TIBCO WebFOCUS®

セキュリティ管理ガイド

バージョン9.0.0
April 2022
DN4501303.0222

目次

1

TIBCO WebFOCUS コンポーネントと展開オプション

TIBCO WebFOCUS では、操作が簡単なレポート作成ツール、ビジネス分析ツール、パフォーマンス管理ツール、および広範囲のセキュリティ統合オプションが提供されます。これらのツールやオプションを使用することで、組織のビジネス知識が強化され、効果的な意思決定が可能になり、競争力の優位性が保持されます。

WebFOCUS は、Web サーバおよび Application Server をオペレーショナルデータに接続することで、既存のネットワークインフラと統合されます。この章では、各種コンポーネントを構成するためのさまざまな方法について説明します。これらの方法により、アプリケーションの開発環境と実稼動環境に応じたシームレスでセキュアな環境が提供されます。

トピックス

WebFOCUS セキュリティモデル

管理者は、WebFOCUS セキュリティモデルを使用して、必要に応じて WebFOCUS リポジトリ内のすべてのリソースを対象に粒度の細かいセキュリティを実装することができます。ユーザの実行操作は、ユーザとリソースの組み合わせごとに許可することができます。アクセス権限は、上位フォルダから継承することも、管理者が特定のグループやユーザに対して許可または拒否することもできます。

セキュリティモデルのハイライトは次のとおりです。

- すべてのコンテンツに使用するリレーショナルデータベースストレージ
- ReportCaster との統合の強化
- すべてのミッドティアコンポーネントのシングルサインオン
- 多様なロール機能
- SaaS (Software as a Service) ベンダーとの統合の強化

- 細分化された管理タスクの委任
- 強化されたセキュリティには次のものがあります。
  - セキュリティ監査
  - アカウントポリシー
  - 複数の認証プロバイダ
  - CSRF (Cross Site Request Forgery) 攻撃から保護するための CSRF フィルタ
  - XSS 攻撃から保護するための XSS (Cross Site Scripting) 防御
  - NULL タイプインジェクション攻撃から保護するための NULL インジェクションフィルタ
  - セッション固定攻撃から保護するためのセッション固定防御
  - クリックジャッキング攻撃から保護するための、カスタマイズ可能な XFrameOptions HTTP レスポンスヘッダ

組織の要求に応じたセキュリティを設計するには、次のことを考慮する必要があります。

- **認証** アプリケーションに関して最初に決定することの 1 つに、そのアプリケーションにアクセスできるユーザを絞り込み、制御する必要があるかどうかという点があります。認証とは、ユーザの本人確認を行うプロセスです。
- **認可** ユーザ認証の完了後、次に行うのはユーザに対して適切なアクセスレベルを選定し、それを適用することです。認可とは、アプリケーション内のリソースやツールへのアクセスを制御するためにユーザ権限を適用するプロセスです。
- **機密性** 機密性とは、情報を特定の環境内のコンポーネント間で転送したり、コンポーネント上に保存したりする場合に、その情報を暗号化することによってプライバシーを保護することです。暗号化の強弱の度合いは調整することができます。また、暗号化のスキームが個人用であるか公共用であるかによってその度合いを変更することができます。どのデータを機密として取り扱うかの判断は、各組織によって異なります。
- **データの整合性** データの整合性とは、所定の承認を得ない限り、情報の変更を行えないようにしてその情報の安全を確保することです。
- **監査** 監査とは、ツールやリソースへのユーザアクセスを追跡し、重要な管理操作 (例、グループへのユーザの追加) を記録することです。

セキュリティポリシーを設計する際には、次の点を考慮する必要があります。

- WebFOCUS リポジトリに格納する情報。

- この情報にアクセスする必要のあるユーザ。
- 各ユーザが必要とする権限の種類。
- 各ユーザに使用を許可するツール。

TIBCO WebFOCUS コンポーネント

WebFOCUS 環境を構成する基本コンポーネントには、次のものがあります。

- **Web ブラウザ**　Web サーバまたは Application Server (Web サーバとしても構成されている場合) への HTTP または HTTPS 接続を使用して、WebFOCUS 環境へのアクセスを可能にします。
- **Web サーバ**　Web エージェント機能および外部認証機能 (例、統合 Windows 認証、SiteMinder エージェント) をサポートする、オプションのコンポーネントです。Web サーバは、Web ブラウザから送信された情報リクエストを受信し、そのリクエストを Application Server に転送します。さらに、Web サーバは、Application Server から送信されたリクエスト応答を受信し、その応答を Web ブラウザに返信します。Web サーバが含まれていない構成では、これらのタスクに Application Server が使用されます。
- **ロードバランサー**　複数のサーバが稼働するインストール環境で、クライアントリクエストを複数のサーバ (クラスタ) に分散させる方法をサポートする、オプションのコンポーネントです。ロードバランサーは、Web ブラウザから送信された入力リクエストを受信し、そのリクエストを複数の異なる Application Server に転送して処理を分散します。
- **Application Server**　ユーザ側とビジネスアプリケーションまたはデータベース側との間で行われるすべてのアプリケーション処理を受け持ちます。多くの場合、Application Server は Web サーバとしても機能します。Application Server の機能の 1 つとして、データベースとの通信があります。また、Application Server は、リクエストの種類に応じて、TIBCO WebFOCUS Reporting Server またはデータベースサーバに接続することもできます。

- **TIBCO WebFOCUS Client** Web サーバと WebFOCUS Reporting Server との間の情報フローを制御します。 - WebFOCUS Client は、Application Server 下で実行されます。WebFOCUS Client は、リポジトリ DBMS または WebFOCUS Reporting Server にアクセスして Web サーバからのリクエストを転送し、これらのコンポーネントからの結果を Web サーバに返信します。WebFOCUS Client は、次のコンポーネントで構成されます。
  - **BI Portal** エンドユーザは、プロフェッショナルな外観を持ち、簡単にカスタマイズできる Web インターフェースで、WebFOCUS レポートにアクセスすることができます。
    - **BI Portal** レポートの作成と表示を行うための WebFOCUS 環境です。BI Portal の重要な機能は、管理者がユーザを新しく登録したり、ユーザにアクセス権限を設定したり、エンドユーザがレポートを作成できることです。BI Portal にアクセスすることにより、レポートの作成や表示が行えます。その際、管理者からアクセス権限が与えられたデータを使用することができます。
  - **ReportCaster** WebFOCUS レポート (セルフサービスおよび BI Portal によるレポート) に対して高度なスケジュールおよび配信機能を提供するほか、アラート、個別のファイルや URL も使用可能になります。
  - **ReportLibrary** ReportCaster が配信したレポート、ファイル、URL コンテンツを格納します。
- **TIBCO WebFOCUS Reporting Server** WebFOCUS がアクセス可能なデータソースのメタデータを格納するとともに、そのデータソースへのアクセスを制御します。Reporting Server は、データソースに対してクエリを実行し、クエリ結果を取得してフォーマットを適用した後、WebFOCUS Client にその結果を送信します。また、Reporting Server が提供する複数のデータアダプタにより、さまざまなデータソースにアクセスすることが可能になります。
- **WebFOCUS データベースリポジトリサーバ** WebFOCUS コンテンツを格納するリレーショナルデータベースシステムです。これらのコンテンツの例として、レポート、グラフ、クエリ、ユーザ、グループ、ロール、ReportCaster スケジュール、リクエスト、イメージ、ReportLibrary スケジュール、保存済みディファードレポートなどがあります。

WebFOCUS 環境に追加できるオプション製品には、次のものがあります。

- **TIBCO WebFOCUS App Studio** Windows ベースの開発環境を使用して WebFOCUS アプリケーションを作成することができます。

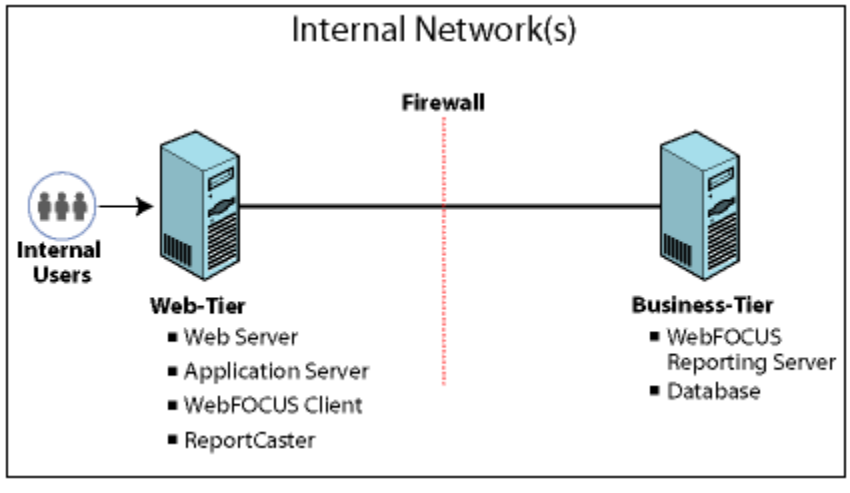
WebFOCUS 展開オプション

WebFOCUS には、コンポーネントを展開する方法がいくつか用意されています。これにより、ユーザはニーズに応じたインストールを計画することができます。

内部展開の基本パターン

内部ユーザ (トラステッドネットワーク上のユーザ) は、標準インストールで WebFOCUS にアクセスします。WebFOCUS Client と Reporting Server は、同一ホストにインストールすることも、ネットワークで接続された 2 つのホストに別々にインストールすることもできます。通常、ReportCaster Distribution Server は、WebFOCUS Client と同一ホストにインストールします。これにより、構成および管理が簡素化されます。

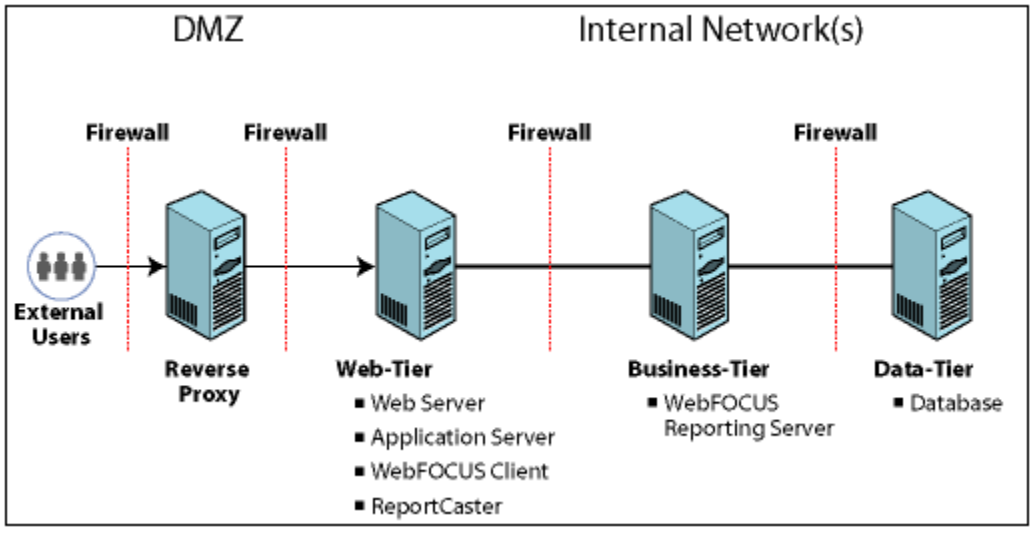
データベースは、ビジネス階層または他のデータ層に配置することができます。異なるマシン上に置く場合は、必要に応じてファイアウォールの背後に配置します。この場合、階層間の通信は、WebFOCUS Reporting Server hub-sub 構成またはベンダーが提供するデータベース接続ソフトにより実行することができます。



外部展開の基本パターン

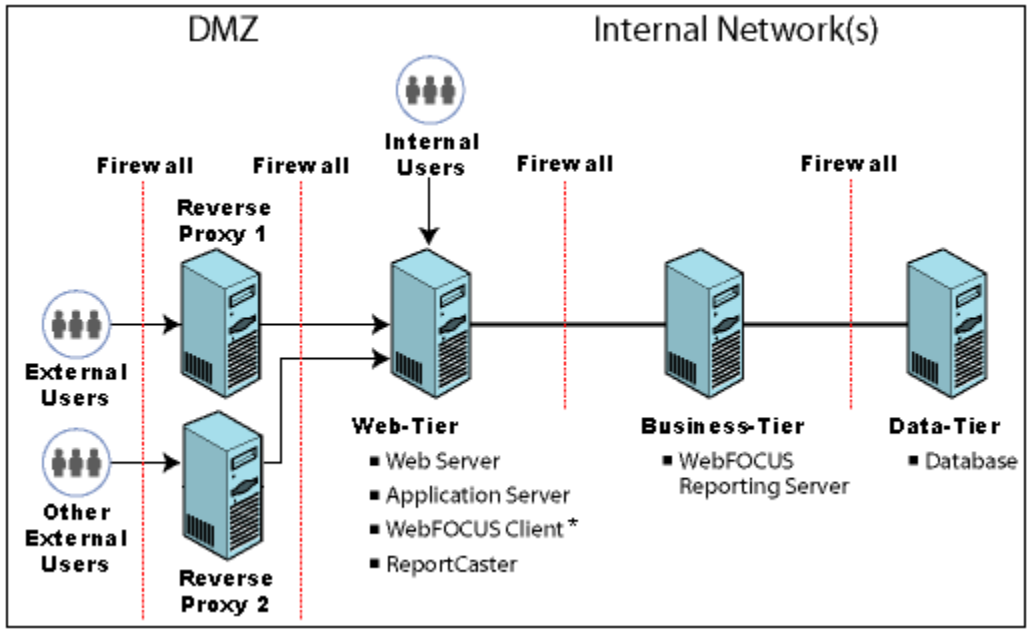
外部ユーザが WebFOCUS にアクセスする場合、必要に応じて外部ユーザがリバースプロキシサーバと交信するよう構成することができます。リバースプロキシサーバとは、WebFOCUS がインストールされた Web サーバと外部ネットワークとを仲介する Web サーバのことです。また、必要に応じて各コンポーネントをファイアウォールで保護することができます。

リバースプロキシサーバを経由する場合、外部ユーザは WebFOCUS に直接アクセスしているかのように操作を行えます。ただし、プロキシサーバが実際に行うのは、入力された HTTP リクエストの受信および WebFOCUS がインストールされた Web サーバへの転送であり、これによりセキュリティ層が別途追加されます。



混合展開のパターン

WebFOCUS は、単一インストールでの複数エントリポイントをサポートします。たとえば、外部ユーザがリバースプロキシサーバを経由し、さらに内部ユーザが直接 Web 階層にアクセスする場合があります。また、下図のように、異なるユーザグループのための複数リバースプロキシサーバが存在する場合があります。



2

TIBCO WebFOCUS Reporting Server の構成

ここでは、TIBCO WebFOCUS Reporting Server を ReportCaster および WebFOCUS Client とともに使用するための構成方法について説明します。WebFOCUS Reporting Server との通信は、さまざまな用途で使用されます。たとえば、次のような用途があります。

- Active Directory や LDAP ディレクトリなどの外部ソースを使用してユーザを認証する。
- ユーザを認可するためのグループメンバーシップ情報を取得する。
- レポートをオンライン実行する。
- レポートをディファード実行する。
- ReportCaster の使用時に、実行するレポートを送信する。

トピックス

TIBCO WebFOCUS Reporting Server のセキュリティモード

WebFOCUS Reporting Server のセキュリティは、次のいずれかのモードで実行されます。

- **PTH (内部)** WebFOCUS Reporting Server へのアクセスは、構成レベルで定義されたユーザリストに対する認証によって制御されます。この場合、ユーザ ID とパスワードを admin.cfg ファイルで構成しておく必要があります。セキュリティを PTH に設定した場合、オペレーティングシステムのセキュリティレベルで偽装されることも、認証されることもありません。オペレーティングシステム側から見ると、すべてのサーバ処理は単一のユーザ ID として実行されます。これがデフォルト認証モードです。

- **LDAP** 外部ディレクトリサービスがユーザを認証します。リソースへのアクセスは、ユーザプロファイルおよびグループプロファイルによって制御されます。WebFOCUS Client 接続から提供されたユーザ認証情報は、確立済みのディレクトリサービスを使用して認証されます。このセキュリティモードでは、ユーザの偽装は適用されません。
- **OPSYS** 各ユーザは、WebFOCUS Reporting Server が稼動しているオペレーティングシステムで定義されます。WebFOCUS Reporting Server は、オペレーティングシステムサービスを使用して接続ユーザを認証し、これらのユーザを偽装することで、ファイルや DBMS オブジェクトなどのリソースへのアクセスを制御します。オペレーティングシステムによるユーザ認証により、Reporting Server ブラウザインターフェースの管理機能へのアクセスが保護されます。

  ユーザの認証情報は、オペレーティングシステムのネイティブセキュリティシステムによって認証されます。次に、WebFOCUS Reporting Server が、ユーザを完全に偽装するデータアクセスエージェントを割り当てます。これにより、ファイルやその他のオブジェクトへのアクセスが、オペレーティングシステムによって管理されます。
- **DBMS** リレーショナルデータベースに格納されたユーザ ID のリストに基づいてユーザの認証を行います。WebFOCUS から提供されたユーザ認証情報がオペレーティングシステムで偽装されることも、認証されることもありません。その代わりに、DBMS サーバまたは WebFOCUS SUB Server で各ユーザを定義することができます。この方法は、「パスワードパススルー」と呼ばれます。これは、WebFOCUS Client から提供されたユーザ ID とパスワードが、認証を行うために次のレベルへ「パス (渡す)」されるためです。
- **CUSTOM** ユーザの認証にカスタムプロシジャを使用します。
- **オフ** ユーザの認証に WebFOCUS Reporting Server のビルトインセキュリティを使用しません。また、WebFOCUS Reporting Server が作成したすべてのエージェントは、その WebFOCUS Reporting Server を開始したユーザのセキュリティプロファイルで実行されます。ユーザ認証の代替方法として、セキュリティプラグインを使用することもできます。

注意：WebFOCUS Reporting Server のロールおよびテンプレートは、WebFOCUS Client のロールおよびテンプレートから独立していますが、その機能は類似しています。特定のユーザを WebFOCUS Reporting Server ではサーバ管理者にする一方、WebFOCUS Client では一般ユーザにすることも、未登録にすることもできます。セキュリティプロバイダを構成する際は、[サーバ管理者] ロールを除いて、その他のサーバロールおよびテンプレートを構成する必要はありません。WebFOCUS Reporting Server のロールおよびテンプレートについての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

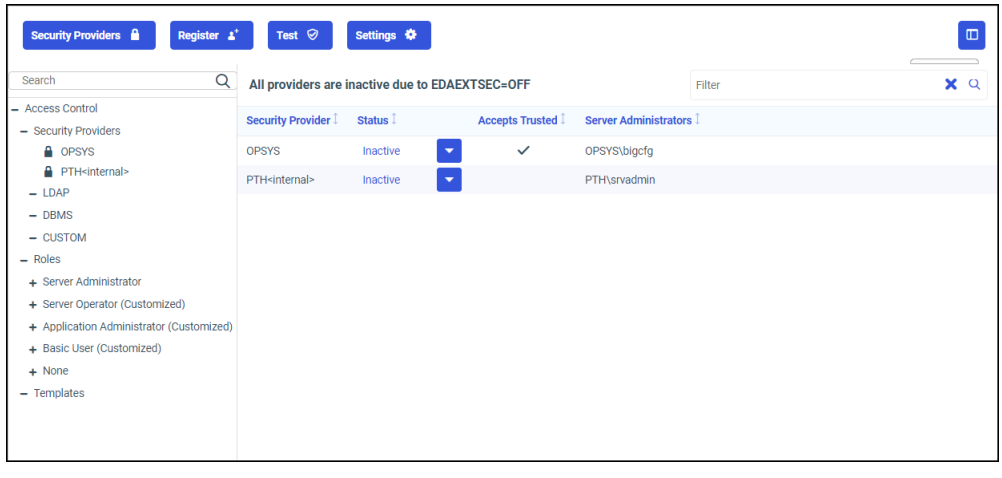
セキュリティプロバイダを作成または編集するには、該当するセキュリティノードをダブルクリックします。メインページに構成オプションが表示されます。別の方法として、セキュリティノードを右クリックし、[新規] を選択して新しいプロバイダを作成するか、[プロパティ] を選択して既存のプロバイダを編集します。プロバイダが構成されていないセキュリティノードで [プロパティ] を選択すると、メインページに新しいプロバイダを構成するためのオプションが表示されます。

[アクセスコントロール] タブをクリックすると、最初に [プロバイダを有効] ページが表示されます。別のページからこのページに戻るには、[アクセスコントロール] フォルダを右クリックして [プロバイダを有効] を選択するか、リボンの [プロバイダを有効] をクリックします。[プロバイダを有効] ページには、現在構成されているプロバイダのリスト、各プロバイダのステータス、サーバ管理者、トラステッド接続を受容するかどうかの設定が表示されます。このページには、現在のサーバ管理者のリストも表示されます。

ユーザのエージェント処理のセキュリティ動作は、WebFOCUS Reporting Server のセキュリティ設定に依存します。詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

TIBCO WebFOCUS Reporting Server ブラウザインターフェース

セキュリティプロバイダを構成するには、Reporting Server ブラウザインターフェースの [アクセスコントロール] タブを使用します。下図は、[アクセスコントロール] タブを示しています。



[アクセスコントロール] タブは、次の要素で構成されています。

- ナビゲーションウィンドウ - セキュリティプロバイダ、テンプレート、ロールを選択します。このページのセキュリティプロバイダリストについての詳細は、25 ページの「 TIBCO WebFOCUS Reporting Server のセキュリティモード 」 を参照してください。
- メインページ - 選択したセキュリティプロバイダ、テンプレート、ロールの設定を構成または表示します。

Reporting Server ブラウザインターフェースへのナビゲート

ブラウザのアドレスバーから Reporting Server ブラウザインターフェースを直接起動するには、次のように URL を入力します。

- 次の URL を入力します。

```
http(s)://host:port
```

説明

`host`

WebFOCUS Reporting Server へのアクセスに使用するホスト名または IP アドレスです。

以下はその例です。

```
server01.ibi.com
```

`port`

WebFOCUS Reporting Server が受信待機するポートの番号です。

以下はその例です。

```
8121
```

ログインが要求された場合は、WebFOCUS Reporting Server の管理権限を持つサーバ管理者の認証情報を入力します。

注意：WebFOCUS Reporting Server 接続に問題がある場合、またはセキュリティが設定された WebFOCUS Reporting Server を実行し、適用するセキュリティモードに関連する要件およびオプションについての詳細が必要な場合は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

ログイン済みの場合は、WebFOCUS Hub のサイドナビゲーションウィンドウから、次のオプションのいずれかを選択することで、Reporting Server ブラウザインターフェースを起動することができます。

- [アプリケーションディレクトリ] を選択し、[アプリケーションディレクトリ] ページを開きます。
- [管理センター] を選択後、[サーバ管理] 下で次のいずれかのリンクを選択します。
  - [サーバのユーザ設定] を選択し、[サーバのユーザ設定] ページを開きます。
  - [アクセスコントロール] を選択し、[アクセスコントロール] ページを開きます。
  - [サーバワークスペース] を選択し、[ワークスペース] ページを開きます。
  - [リソース管理] を選択し、[リソース管理] ページを開きます。
  - [スケーラビリティ] を選択し、[スケーラビリティ] ページを開きます。

注意：[クライアント管理] 下で [管理コンソール] を選択して、管理コンソールから Reporting Server ブラウザインターフェースを開くこともできます。

WebFOCUS ホームページから Reporting Server ブラウザインターフェースを開くには、次の手順を実行します。

- バナーで、[設定]、[WebFOCUS Server] を順に選択します。

  または

- バナーで、プラス (+) ボタンを選択し、[データの準備と管理] を選択します。

レガシーホームページから Reporting Server ブラウザインターフェースを開くには、次の手順を実行します。

- リソースツリーで、[Reporting Server] ノードを展開します。使用する WebFOCUS Reporting Server のノードを右クリックし、[Reporting Server コンソール] を選択します。

  または

- BI Portal のメニューバーで [管理] をクリックし、[管理コンソール] を選択します。管理コンソールから Reporting Server ブラウザインターフェースを起動する手順を実行します。

管理コンソールから Reporting Server ブラウザインターフェースを開くには、次の手順を実行します。

- [構成] タブで、[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。使用する WebFOCUS Reporting Server を右クリックし、[Reporting Server コンソール] を選択します。

ログインが要求された場合は、WebFOCUS Reporting Server の管理権限を持つサーバ管理者の認証情報を入力します。

IP 制限フィルタ

サービスリクエストの実行用に許可する WebFOCUS Reporting Server 接続を、特定の IP アドレスに制限することを強くお勧めします。TCP リスナ (LST_TCP) および HTTP リスナ (LST_HTTP) に必要な IP アドレスへの接続を制限すると、WebFOCUS Reporting Server と WebFOCUS Client 間のトラステッド接続の未承認ユーザによる使用が防止されます。

接続要求に対して許可する IP アドレスは、WebFOCUS Reporting Server 通信構成ファイル (odin.cfg) の RESTRICT_TO_IP キーワードで定義します。odin.cfg ファイルに RESTRICT_TO_IP キーワードが含まれていない場合は、すべての IP アドレスが許可されます。RESTRICT_TO_IP キーワードの使用についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』の「リスナおよびスペシャルサービス」を参照してください。

TIBCO WebFOCUS Reporting Server でのセキュリティプロバイダの構成

事前認証、外部認証、外部認可のいずれかを構成すると、WebFOCUS Client は、WebFOCUS Reporting Server (WFRS) で構成されたセキュリティプロバイダを使用して外部ソースを検索し、ユーザに関する情報を取得します。LDAP または Active Directory セキュリティプロバイダを使用する場合もあれば、カスタム方式で認証または認可を実行する場合もあります。カスタム方式では、たとえば、Web サービスを使用してユーザを認証したり、リレーショナルデータベース管理システム (RDBMS) テーブルに格納されている情報に基づいてユーザを認可したりします。

WebFOCUS Reporting Server は、同時に複数のセキュリティプロバイダをサポートします。プライマリプロバイダは、常に構成する必要があります。また、必要に応じて、1 つまたは複数のセカンダリプロバイダを構成することができます。WebFOCUS ユーザは、プライマリプロバイダで認可することをお勧めします。

WebFOCUS Reporting Server をインストールすると、PTH (内部認証) がデフォルトセキュリティプロバイダとして自動的に構成されます。このデフォルト構成を Reporting Server ブラウザインターフェースで確認するには、[セキュリティオンで開始] コマンドで WebFOCUS Reporting Server を起動する必要があります。インストール時に自動的に作成される PTH サーバ管理者を使用して、事前認証または外部認証に使用する予定の外部ソースを構成することができます。使用する認証方法を構成した後でも、PTH をセカンダリセキュリティプロバイダとして構成することをお勧めします。これにより、プライマリプロバイダが使用不可の場合でも、Reporting Server ブラウザインターフェースへのアクセスが可能になります。

PTH は、WebFOCUS Client との通信に使用される WebFOCUS Reporting Server サービスアカウントのセキュリティプロバイダとしても役立ちます。多くの場合、ガバナンスポリシーでは、外部ソース内のパスワードを定期的に変更すること、パスワードを構成ファイルに格納しないこと、プライマリセキュリティプロバイダに存在するアカウントに無期限のパスワードを使用しないことが規定されています。サービスアカウントのパスワードを定期的に更新するような管理方法を回避するには、外部ソースに存在しない PTH アカウントを指定し、そのアカウントに [サーバ管理者] ロールと無期限のパスワードを割り当てます。

注意：ユーザアカウントのプロバイダを指定しない場合、そのアカウントはプライマリプロバイダからのアカウントとして扱われます。認証に複数の WebFOCUS Reporting Server セキュリティプロバイダを使用するには、セカンダリセキュリティプロバイダに関連付ける各ユーザの WebFOCUS ユーザ ID に、セカンダリセキュリティプロバイダ名を接頭語として追加します。たとえば、WebFOCUS Reporting Server で、LDAP01 というプライマリプロバイダと LDAP02 というセカンダリプロバイダの 2 つの LDAP プロバイダを使用する場合は、WebFOCUS で LDAP01¥user1 および LDAP02¥user2 のユーザアカウントを、それぞれ「user1」および「LDAP2¥user2」として作成する必要があります。

TIBCO WebFOCUS Reporting Server での LDAP または Active Directory セキュリティプロバイダの構成

新しい LDAP または Active Directory セキュリティプロバイダを構成するには、プロバイダを作成し、ユーザ検索およびグループ検索を設定した後、他のアプリケーションからのトラステッド接続を許可するようセキュリティプロバイダを構成します。また、新しいプロバイダを構成すると、自動的に [非アクティブ] ステータスに設定されるため、必要に応じてステータスを [プライマリ] または [セカンダリ] に変更します。

注意：プロバイダのプロパティを変更するには、プロバイダ名を右クリックして [セキュリティの構成] ウィンドウを開きます。

手順　TIBCO WebFOCUS Reporting Server で LDAP セキュリティプロバイダを構成するには

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] ページを開きます。要求された場合は、有効なサーバ管理者 ID およびパスワードを入力し、ログインします。ログインページにセキュリティプロバイダリストが表示された場合は、セキュリティプロバイダを選択します。
2. [セキュリティプロバイダ] 下で [LDAP] を右クリックし、[新規] を選択します。

   または

   バナーで [セキュリティプロバイダ]、[新規プロバイダ]、[LDAP] を順に選択します。

[LDAP セキュリティの構成] タブが表示されます。

3. [続行] をクリックし、[LDAP_PROVIDER] テキストボックスにプロバイダ名を入力します。

   この名前は、[アクセスコントロール] ナビゲーションウィンドウにベンダー名として表示されます。

4. [接続] セクションの各テキストボックスに次のように入力します。

   - [ldap_host] テキストボックスに、LDAP ホストの名前を入力します。
   - [ldap_port] テキストボックスで、デフォルト値を受容するか専用の LDAP ポート番号を入力します。
   - [security] ドロップダウンリストから [Explicit] を選択し、[ldap_princpal] テキストボックスにサービスアカウント名を入力し、[ldap_credentials] テキストボックスに無期限のパスワードを入力します。このバインドは、[ldap_principal] および [ldap_credentials] 構成パラメータで定義されたアカウント下で実行されます。

     [匿名または Windows セキュリティ -NEGOTIATE] オプションは使用しないでください。

   - [ldap_search_timeout] テキストボックスで、デフォルト値の 60 秒を受容するか、LDAP 検索のタイムアウト時間を秒数で入力します。

5. [次へ] をクリックします。

   ページがリフレッシュされ、[ユーザ検索] セクションが展開されます。[グループ検索]、[Trusted 接続]、[環境] セクションも折りたたみ形式で表示されます。

6. WebFOCUS Reporting Server がユーザディレクトリに接続し、そのディレクトリのベンダーおよびバージョン番号を特定した後、[ユーザの検索] ウィンドウおよび [グループの検索] ウィンドウにそのディレクトリの標準的なデフォルト値を入力します。

   注意

   - 特定のウィンドウのテキストボックスが表示されていない場合は、そのウィンドウのタイトルバーの下向き矢印をクリックしてウィンドウを開きます。
   - ディレクトリで使用する値がそのタイプのデフォルト値と異なる場合は、AD または LDAP 管理者に正しい設定を確認してください。

7. [ユーザの検索] ウィンドウおよび [グループの検索] ウィンドウで値を入力した後、[ユーザ認証のテスト] をクリックします。

   [LDAP セキュリティのテスト中] ダイアログボックスが開きます。

8. 外部ディレクトリに存在するアカウントの LDAP ユーザ ID およびパスワードを入力し、[続行] をクリックします。

   認証情報が正しく認証された場合は、そのユーザに対して検索された LDAP または Active Directory グループのリストが表示されます。カスタム属性を使用している場合は、そのユーザの属性値が表示されます。

   認証情報が正しく認証されなかった場合は、エラーメッセージに詳細情報が表示されます。

   注意：通常、このテストは即座に終了します。結果の表示に時間を要する場合は、ディレクトリ管理者およびネットワーク管理者に問い合わせて、現在の環境で接続、ユーザ、グループの構成設定が正しいことを確認してください。

9. [テスト結果] ダイアログボックスを閉じます。このセキュリティプロバイダでトラステッド接続を受容するよう構成する場合は、[Trusted 接続] セクションを展開し、[trust_ext] を [y] に設定します。

10. [保存] をクリックします。

[プロバイダを有効] ウィンドウが開きます。セキュリティプロバイダのリストに、新しいプロバイダが非アクティブプロバイダとして表示されます。

LDAP セキュリティプロバイダプロパティの理解

構成する LDAP プロバイダごとに、接続プロパティ、ユーザプロパティ、グループプロパティを指定する必要があります。

参照　LDAP 接続プロパティの理解

LDAP_PROVIDER

LDAP プロバイダの名前を指定します。

ldap_host

LDAP サーバを実行するホスト名、またはホストの IP アドレスを表すドット表記の IPv4 文字列で構成されたホスト識別子です。
また、[ldap_host] テキストボックスには、ブランクで区切られた複数のホスト識別子のリストを入力することもできます。各ホスト識別子には、末尾のコロン (:) とポート番号を含めることができます。複数のホスト識別子を指定した場合、接続が正しく確立されるまで、各ホスト識別子への接続が順に確認されます。

たとえば、ldap_host 設定値として、次の値はすべて有効です。

```
directory.example.com
192.0.2.0
directory.example.com:1050 people.catalog.com 192.0.2.0
```

ldap_secure_connection

WebFOCUS Reporting Server が LDAP サーバとの通信に SSL 接続を使用するかどうかを指定します。デフォルト値は [いいえ] です。

LDAP セキュリティプロバイダでは、SSL/TLS 接続を確立するための SSL API コールがサポートされます。WebFOCUS Reporting Server は、サーバ認証のみを使用して API コールを開始し、接続先の LDAP サーバが、証明書を提供したサーバと同一であることを確認します。

[ldap_lib_vendor] 設定で IBM、Sun、Novell のいずれかを選択し、SSL 接続を指定した場合、追加のオプションが表示されます。

- Sun および IBM の場合、[ldap_ssl_certificate] 設定が表示されます。
- Novell の場合、[ldap_ssl_certificate] および [ldap_ssl_certification_encoding] 設定が表示されます。

ldap_ssl_certificate

API が SSL/TLS 接続の確立に使用する LDAP 属性を指定します。値は、次のように LDAP ベンダーによって異なります。

- **Novell API** LDAP サーバが認証用に提供する信頼済みルート証明書のファイル名を、パスを含めて指定します。
- **Sun/Netscape API** LDAP サーバが認証用に提供する Netscape 証明書データベース (cert7.db) のパスを、ファイル名を含めずに指定します。
- **IBM API** ldapkey.kdb (LDAP サーバが認証用に提供する IBM データベースファイル) のファイル名を、パスを含めて指定します。ldapkey.sth パスワードスタッシュファイルが同一ディレクトリ内に必要です。

  注意：SSL には、IBM LDAP クライアントライブラリ以外に、GSK (Global Security Kit) が必要です。Windows マシンに GSK をインストールしておく必要があります。
- **Microsoft API** ldap_ssl_certificate 構成を無視します。この構成は、Active Directory では使用されません。サーバ証明書は、証明書ストアにインストールされている必要があります。

ldap_ssl_certification_encoding

Novell の場合、証明書のエンコードに使用する標準を指定します。暗号化の方法およびファイルフォーマットは、API のベンダー仕様により異なります。オプションは B64 と DER です。

ldap_port

LDAP サーバへの接続に使用される TCP ポート番号を定義する正の整数です。ホスト識別子にコロン (:) とポート番号が含まれている場合、ldap_port は無視されます。デフォルトポート番号は、389 または 636 (SSL 接続の場合) です。

security

使用するバインドのタイプを指定します。

- **匿名または Windows セキュリティ - NEGOTIATE**

  認証情報は必要ありません。これがデフォルト値です。

  Reporting Server が Windows マシンにインストールされている場合、このオプションを選択すると、バインドがデフォルト値の NEGOTIATE に設定されます。それ以外の場合、バインドは匿名になります。

  ネゴシエーションでは、Windows 固有の API が、Active Directory に対する WebFOCUS Reporting Server 接続を認証します。バインドは、現在の Windows ユーザ (Reporting Server を開始した Windows アカウント) に基づいて実行されます。WebFOCUS Reporting Server の Windows ホストマシンは、Active Directory サーバと同一のドメインに存在する必要があります。

- **Explicit**

  バインドは、[ldap_principal] および [ldap_credentials] 設定で定義されたアカウントで実行されます。

注意

- Active Directory に対する認証は、[Explicit] オプションを選択した場合にのみサポートされます。内部認証を使用する場合、[匿名または Windows セキュリティ - NEGOTIATE] オプションは選択しないでください。
- [Explicit] または [匿名または Windows セキュリティ - NEGOTIATE] を使用して Active Directory に接続する場合、[ldap_user_attribute] のデフォルト値は sAMAccountName です。この値は、必要に応じてカスタマイズすることができます。

ldap_principal

サービスアカウントの名前を指定します。

注意：この設定は、セキュリティ設定が [Explicit] の場合にのみ表示されます。

ldap_credentials

サービスアカウントのパスワードを指定します。無期限のパスワードを指定することをお勧めします。

注意：この設定は、セキュリティ設定が [Explicit] の場合にのみ表示されます。

ldap_search_timeout
タイムアウトになるまで LDAP が検索を継続する時間を秒単位で指定します。

ldap_referrals
ルートドメインが返す参照に従って子ドメインを検索するかどうかを指定します。デフォルト値は [いいえ] です。

ldap_gchost
Active Directory グローバルカタログのホスト名を指定します。

ldap_gcport
Active Directory グローバルカタログのポート番号を指定します。ldap_gcport は、ldap_port と対で選択する必要があります。非 SSL の組み合わせ (389/3268) または SSL の組み合わせ (636/3269) のいずれかを使用します。このテキストボックスに値を割り当てる場合、正の整数を入力します。

Linux で OpenLDAP を選択した場合は、追加のプロパティとして [ldap_libldap] および [ldap_liblber] が表示されます。これらのプロパティで、Reporting Server が実行時にロードする OpenLDAP ライブラリの名前を指定します。ライブラリ名を指定するよう要求された際は、Reporting Server が実行時にアクセス可能なライブラリのパスを入力する必要があります。その時点でライブラリ名を入力しない場合は、[ldap_libldap] および [ldap_liblber] に入力したライブラリ名が使用されます。

参照　LDAP ユーザプロパティの理解

ldap_user_base
LDAP サーバのユーザ検索の開始点となるエントリの DN を指定します。

ldap_user_scope
WebFOCUS Reporting Server が LDAP ディレクトリ内でユーザ検索を開始する際の範囲を指定します。次のオプションがあります。

subtree　ベース DN 下のすべてを検索します。これがデフォルト値です。

onelevel　ベース DN より 1 レベル下のエントリのみを検索します。

base　ベース DN のみを検索します。

ldap_user_class
ユーザエントリの検索時に使用されるオブジェクトクラスを指定します。

ldap_user_attribute
ユーザエントリの検索時に使用される属性を指定します。一般にデフォルト値を変更する状況として、ユーザ ID の代わりに Email アドレスでユーザがログインできるようにする場合があります。その場合は、[ldap_user_attribute] を mail に設定するか、userPrincipalName に設定します (この名前がディレクトリ内の属性名に一致する場合)。

ldap_user_group_attribute
ユーザオブジェクト内のグループの識別に使用する属性を指定します。

ldap_user_description
オブジェクト (ユーザ、グループ) の説明が値として格納されている属性を指定します。

ldap_user_email
ユーザの Email アドレスが格納されている属性を指定します。

ldap_user_class、ldap_user_attribute、ldap_group_class、ldap_group_attribute は、検索フィルタを構成するパラメータです。検索フィルタの標準構文は、次の構造に従います。

```
(&(Property_Name=Property_Value)(Property_Name=Property_Value))
```

ldap_user_class および ldap_group_class パラメータの値をアスタリスク (*) に変更すると、検索フィルタの構文を次のように簡略化することができます (ただし、グループのサポートは正しく動作しません)。

```
(Property_Name=Property_Value)
```

これらのパラメータにアスタリスク (*) を指定することにより、検索フィルタの構文が簡略化されますが、グループのサポートが無効になります。

参照 **LDAP グループプロパティの理解**

ldap_group_base
LDAP サーバのグループ検索の開始点として機能するエントリの DN を指定します。ldap_group_base は、名前と値の組み合わせで構成され、それぞれの組み合わせをカンマ (,) で区切ります。

ldap_group_scope
WebFOCUS Reporting Server が LDAP ディレクトリ内でグループ検索を開始する際の範囲を指定します。次のオプションがあります。

subtree ベース DN 下のすべてを検索します。これがデフォルト値です。

onelevel ベース DN より 1 レベル下のエントリのみを検索します。

base ベース DN のみを検索します。

ldap_group_class
グループエントリの検索時に使用するオブジェクトクラスを指定します。LDAP のデフォルト値は groupofuniquenames です。Active Directory のデフォルト値は group です。

ldap_group_attribute
グループの名前の識別に使用する 属性を指定します。デフォルト値は cn です。

ldap_member_attribute
グループ内のユーザの識別に使用する属性を指定します。デフォルト値は uniqueMember です。Active Directory のデフォルト値は member です。

ldap_nested_groups
ネストされた LDAP グループのサポートを有効にします。デフォルト値は [いいえ] です。この設定では、ネストされたグループのサポートは無効です。

ldap_group_description
LDAP グループに関する追加情報を指定します。

TIBCO WebFOCUS Reporting Server でのカスタム RDBMS セキュリティプロバイダの構成

ユーザ情報は、リレーショナルデータベース管理システム (RDBMS) から取得することができます。たとえば、Email アドレス、説明、ユーザ認可を WebFOCUS で再作成する代わりに、これらの情報を既存のデータベースから取得したい場合があります。この情報は SQL クエリを使用するか、SQL ストアドプロシジャを使用して取得できますが、いずれの場合でもカスタム FOCUS プロシジャを作成してこの情報を取得します。

RDBMS テーブルを使用した外部認可には、2 つの FOCUS プロシジャが必要です。RDBMS の情報に基づいてユーザの認証も実行する場合は、3 つ目のプロシジャが必要です。RDBMS にユーザ認証情報が格納されていない場合は、外部認可するユーザを識別するために、ユーザを事前認証するよう WebFOCUS Client を構成します。事前認証についての詳細は、236 ページの「 事前認証 」 を参照してください。

カスタムサーバセキュリティプロバイダを有効にするには、WebFOCUS Reporting Server が次のタスクを実行するためのコードを記述する必要があります。

- ユーザ ID とパスワードに基づいてユーザを認証する。
- ユーザが属するグループをすべて取得する。
- システム内のグループをすべて取得する。
- グループのすべてのユーザ、およびシステム内のすべてのユーザを取得する。

WebFOCUS Reporting Server でサンプル SQL セキュリティプロバイダの構成に必要なファイルは、次のサイトから入手することができます。

techsupport.informationbuilders.com/tech/wbf/v8templates/wbf_8_server_custom_provider.html

このページには、プロシジャが情報を返す際に使用する必要のあるフォーマットに関する情報も記載されています。

カスタムプロバイダプロシジャで使用されるシノニムは、EDACONF/catalog/custom ディレクトリに移動する必要があります。WebFOCUS Reporting Server は、サーバ管理者以外のユーザからの接続を拒否することで、カスタムプロシジャで使用されるアダプタ接続を保護します。

手順　TIBCO WebFOCUS Reporting Server でカスタム RDBMS セキュリティプロバイダを構成するには

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] ページを開きます。要求された場合は、有効なサーバ管理者 ID およびパスワードを入力し、ログインします。ログインページにセキュリティプロバイダリストが表示された場合は、セキュリティプロバイダを選択します。
2. [アクセスコントロール] ウィンドウの [セキュリティプロバイダ] 下で、[CUSTOM] を右クリックし、[新規] を選択します。

   または

   バナーで [セキュリティプロバイダ]、[新規プロバイダ]、[CUSTOM] を順に選択します。

   [CUSTOM セキュリティプロバイダの構成] タブが開きます。

3. [CUSTOM_PROVIDER] テキストボックスにカスタムセキュリティプロバイダ名を入力します。

   注意：この名前は小文字で入力することをお勧めします。

4. WebFOCUS Reporting Server が情報を取得するために使用するプロシジャを指定します。

   a. カスタムプロバイダが認証をサポートする場合は、[cust_authenticateuser] テキストボックスに、ユーザを認証するプロシジャの完全修飾名を入力します。たとえば、「_edaconf/catalog/custom/wfsqlauthn」のように入力します。WebFOCUS がユーザを事前認証する場合は、このテキストボックスをブランクにします。

   b. [cust_usersbygroup] テキストボックスに、ユーザに関する情報を返すプロシジャの完全修飾名を入力します。たとえば、「_edaconf/catalog/custom/wfsqlusers」のように入力します。

   c. [cust_groupsbyuser] テキストボックスに、グループに関する情報を返すプロシジャの完全修飾名を入力します。たとえば、「_edaconf/catalog/custom/wfsqlgroups」のように入力します。

   d. [cust_service] リストで、WebFOCUS Reporting Server データサービスを選択します。ユーザ情報を返すプロシジャは、このデータサービス下で実行されます。

   e. このセキュリティプロバイダでトラステッド接続を受容するよう構成するには、[trust_ext] リストから [y] を選択します。

5. [テスト] をクリックし、情報がデータベースに格納されているユーザの名前とパスワードを入力した上で、[続行] をクリックします。

   プロシジャが情報の取得に成功した場合、WebFOCUS Reporting Server からユーザ情報が有効であることを示すメッセージが返されます。

   認証情報が正しく認証されなかった場合は、エラーメッセージに詳細情報が表示されます。

   注意：通常、このテストは即座に終了します。結果の表示に時間を要する場合は、ディレクトリ管理者およびネットワーク管理者に問い合わせて、現在の環境で接続、ユーザ、グループの構成設定が正しいことを確認してください。

6. [テスト結果] ダイアログボックスを閉じ、[保存] をクリックします。

[プロバイダを有効] ウィンドウが開きます。新しいカスタムプロバイダが、非アクティブプロバイダとしてセキュリティプロバイダのリストに表示されます。

参照

CUSTOM セキュリティプロバイダのプロパティ

新しいカスタムセキュリティプロバイダを構成する際は、次のプロパティの値を入力します。

CUSTOM_PROVIDER

カスタムプロバイダの名前を指定します。デフォルト設定では、この設定に「custnn」という値が表示されます。

説明

nn

プロバイダの 2 桁の連続番号です。

cust_authenticateuser

ユーザの認証に使用するプロシジャの名前です。

必要に応じて、認証プロシジャを使用する代わりに、WebFOCUS Reporting Server への接続時に使用するデフォルトサーバ管理者のユーザ ID とパスワードを指定することもできます。

認証プロシジャの作成についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

cust_usersbygroup

すべてのユーザのリストを返すプロシジャ、またはグループ ID がプロシジャに渡される場合は、そのグループ内のすべてのユーザのリストを返すプロシジャの名前です。

ユーザを返すプロシジャの作成についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』 を参照してください。

cust_groupsbyuser

すべてのグループのリストを返すプロシジャ、またはユーザ ID がプロシジャに渡される場合は、そのユーザ ID が属するすべてのグループのリストを返すプロシジャの名前です。グループを返すプロシジャの作成についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』 を参照してください。

cust_service

WebFOCUS Reporting Server データサービスの名前です。このデータサービス下で、ユーザ情報の取得に使用するプロシジャが実行されます。既存のサービスを指定することも、[データサービス] タブで作成したカスタムサービスを指定することもできます。

cust_hashpsswrd

カスタムプロバイダで接続認証にハッシュ形式のパスワードを使用する必要があるかどうかを指定します。デフォルト値は [n] です。

trust_ext

WebFOCUS Reporting Server でトラステッド接続を受容するかどうかを指定します。デフォルト値は [n] です。

セキュリティプロバイダ構成の変更

サーバセキュリティプロバイダには、[プライマリ]、[セカンダリ]、[非アクティブ] のいずれかのステータスを割り当てることができます。プライマリセキュリティプロバイダに指定できるのは、1 つのセキュリティプロバイダのみです。その他すべてのアクティブセキュリティプロバイダは、セカンダリに指定されます。構成済みだが使用されていない上記以外のセキュリティプロバイダは、非アクティブになります。ユーザアカウントのセキュリティプロバイダを指定しない場合、そのアカウントはプライマリプロバイダからのアカウントとして扱われます。

プライマリセキュリティプロバイダのステータスを変更する場合、セカンダリセキュリティプロバイダのいずれかを、新しいプライマリセキュリティプロバイダに指定する必要があります。既存のプライマリプロバイダを置換する新しいセキュリティプロバイダを選択しない場合、WebFOCUS Reporting Server により新しいプライマリセキュリティプロバイダが自動的に指定されます。

セキュリティプロバイダを変更する場合、[PTH<内部>] をセカンダリセキュリティプロバイダとして常に保持することをお勧めします。これにより、管理者は、プライマリセキュリティプロバイダが使用できない場合でも WebFOCUS Server にアクセスすることができます。

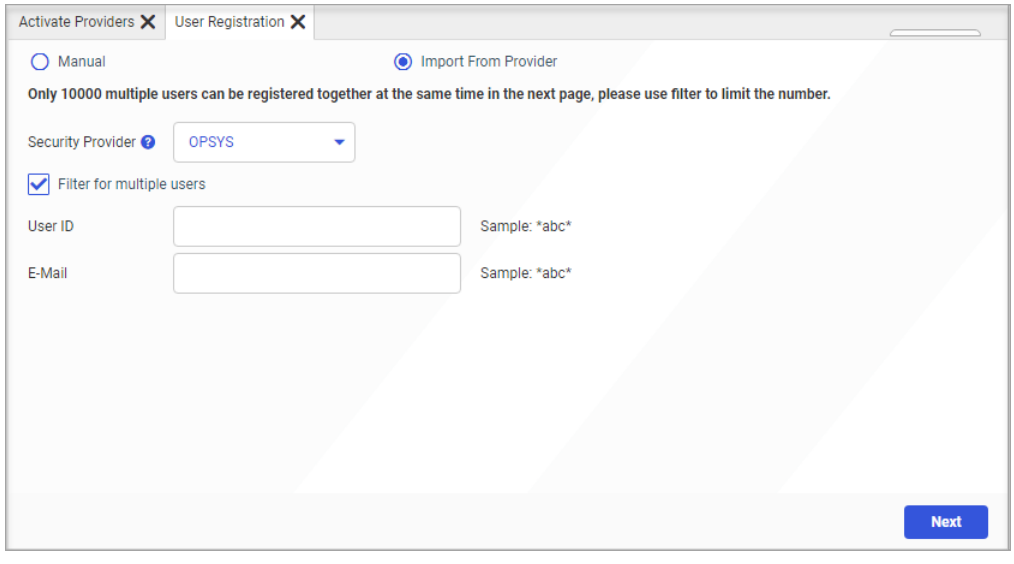
また、admin.cfg ファイル (*drive*:¥ibi¥profiles¥) の最新バージョンのバックアップコピーを保持しておくことをお勧めします。このファイルには、PTH ユーザ情報が格納されます。admin.cfg の主ファイルが破損された場合は、このバックアップファイルを使用して PTH セキュリティプロバイダを復元することができます。

手順　ユーザアカウントをサーバ管理者として登録するには

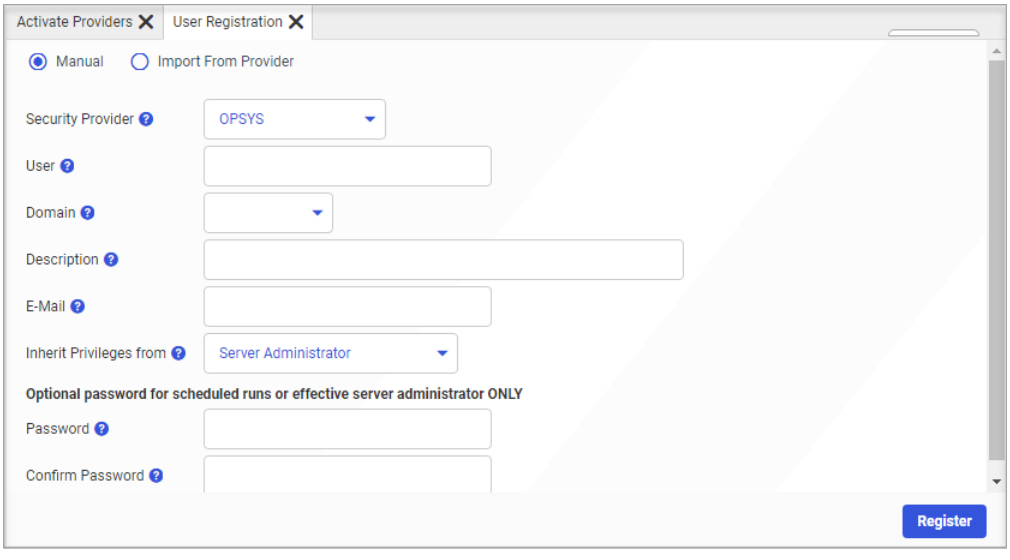
WebFOCUS は、インストール時に、PTH (内部) セキュリティプロバイダのサーバ管理者アカウントを登録します。これらのプロバイダまたは後から追加する他のプロバイダで、別のユーザまたはグループをサーバ管理者として追加登録したい場合があります。

現在の構成で、少なくとも 1 つのアクティブセキュリティプロバイダでサーバ管理者アカウントが登録されている必要があります。ただし、サーバ管理者アカウントが登録されていない場合でも、任意のセキュリティプロバイダをプライマリセキュリティプロバイダに指定することができます。

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] ページを開きます。要求された場合は、有効なサーバ管理者 ID およびパスワードを入力し、ログインします。ログインページにセキュリティプロバイダリストが表示された場合は、セキュリティプロバイダを選択します。
2. 下図のように、[アクセスコントロール] ページで、[登録]、[ユーザ登録] を順に選択して [ユーザの登録] タブを開きます。



3. 下図のように、[手動] を選択して、[ユーザの登録] タブの手動バージョンを開きます。



4. 新しいサーバ管理者を割り当てるセキュリティプロバイダを選択します。

   選択したプロバイダのレイアウトに合わせてページがリフレッシュされます。このレイアウトは各プロバイダで同一ですが、次の手順に示すように若干の違いがあります。

5. 新しいサーバ管理者のユーザ ID を入力します。

   注意：必要に応じて、*domain name¥user ID* フォーマットを使用します。

6. OPSYS セキュリティプロバイダを選択した場合、ユーザのドメイン名を選択します。

7. 必要に応じて、サーバ管理者の説明を入力します (オプション)。

8. このユーザに通知が送信される場合は、Email アドレスを入力します。

9. [権限の継承元] リストのサーバ管理者のデフォルト値を受容します。

   必要な場合のみ、別のサーバロールを選択します。サーバロールについての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

10. [PTH <内部>] セキュリティプロバイダを選択した場合、[パスワード] および [パスワードの確認] テキストボックスに、この管理者のパスワードを入力します。別のセキュリティプロバイダを選択した場合、このパスワードはオプションです。

    注意：WebFOCUS Reporting Server は、スケジュール済みレポート配信の実行時にこのパスワードを使用します。

11. 構成の完了後、ダイアログボックスで [追加と登録] (PTH<内部> セキュリティプロバイダの場合) または [登録] (その他のプロバイダの場合) を選択します。

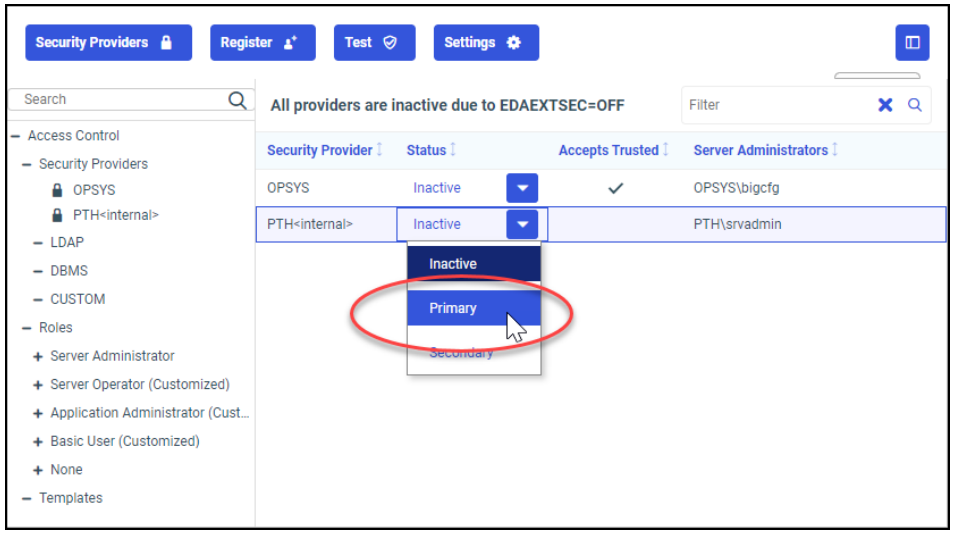
12.「新しいユーザを追加します」というメッセージで [OK] をクリックします。

13. [ユーザの登録] ページがリフレッシュされた後、このページに表示された新規登録ユーザの ID およびその他の情報を確認します。

手順　新規プライマリセキュリティプロバイダを構成するには

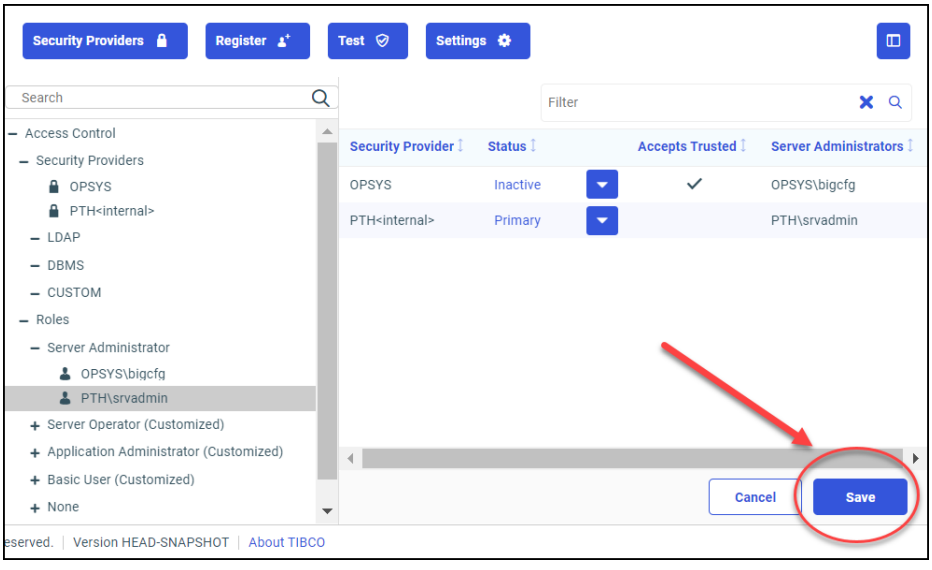
事前の確認事項 - 42 ページの 「 ユーザアカウントをサーバ管理者として登録するには 」 の手順に従って、新しいプライマリセキュリティプロバイダのセキュリティ管理者が作成済みであることを確認します。管理者が作成済みでない場合、新しいプライマリセキュリティプロバイダを指定した後で、Reporting Server ブラウザインターフェースにアクセスできなくなります。

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] ページを開きます。要求された場合、有効なサーバ管理者のユーザ ID とパスワードでログインし、ログインページにセキュリティプロバイダリストが表示された場合は、セキュリティプロバイダを指定します。
2. 下図のように、新しいプライマリセキュリティプロバイダのエントリを特定し、[ステータス] リストで [プライマリ] を選択します。

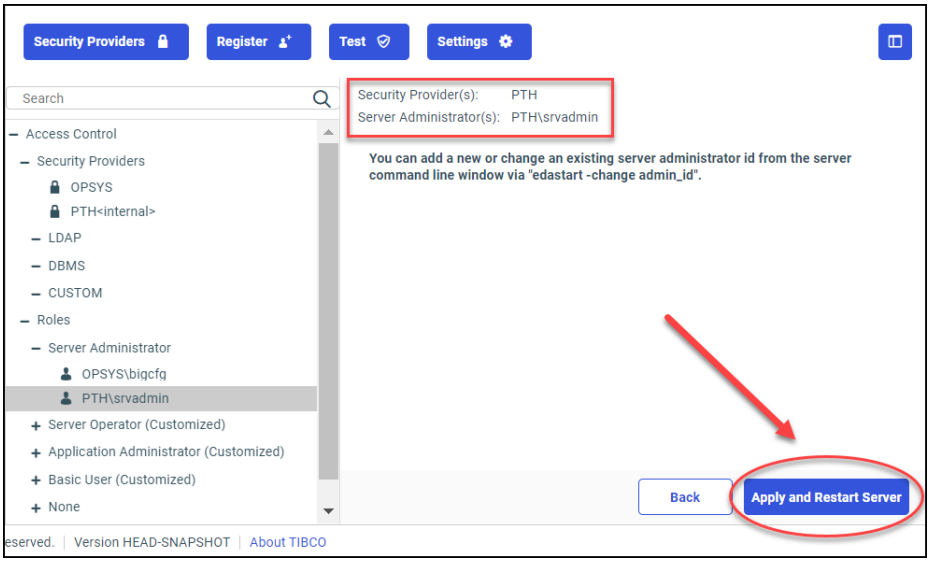


別のプライマリセキュリティプロバイダがすでに選択されていた場合、そのプロバイダのステータスは自動的に [セカンダリ] に変更されます。

3. 変更後の構成を確認し、下図のように、[保存] を選択します。



4. 確認ページで問題がなければ、下図のように、[適用してサーバを再起動] を選択します。



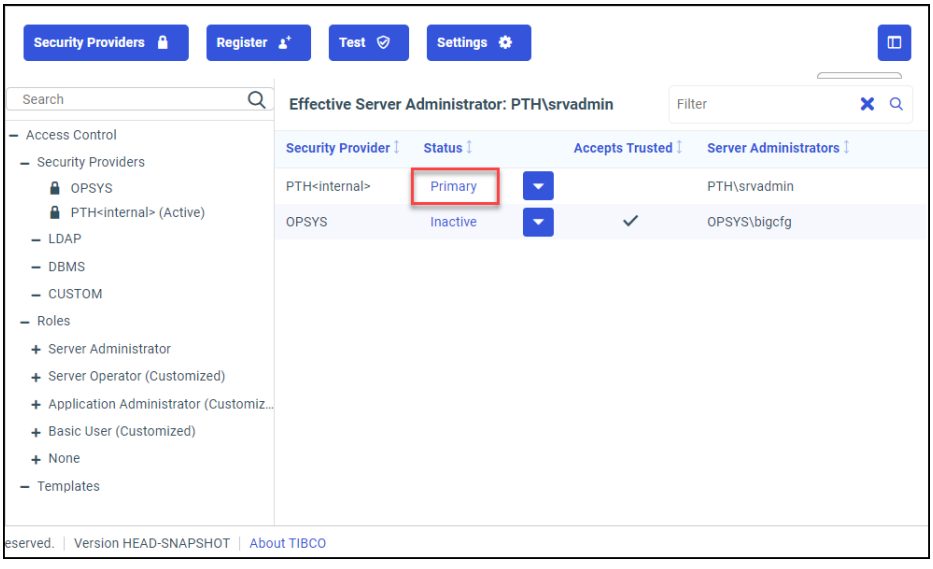
WebFOCUS Reporting Server が再起動中であることを示すメッセージが表示されます。

注意

- OPSYS をプライマリプロバイダに設定している場合は、WebFOCUS Reporting Server を常に手動で再起動する必要があります。
- ブラウザに「ワークスペース再起動中です」というメッセージが 30 秒以上表示された場合は、ブラウザを閉じてから再度開きます。Reporting Server ブラウザインターフェースに再度ログインします。
- この新しいプライマリプロバイダでサーバ管理者が指定されなかった場合、WebFOCUS Reporting Server から新規プロバイダを追加中であることを示すメッセージが表示され、そのプロバイダにサーバ管理者を登録するかどうかの選択が要求されます。42 ページの「 ユーザアカウントをサーバ管理者として登録するには 」の説明に従って、新しいサーバ管理者を登録することができます。

5. WebFOCUS Reporting Server の再起動後、新しいプライマリセキュリティプロバイダのサーバ管理者のユーザ ID とパスワードでログインします。これにより、[アプリケーション] ページが開きます。
6. 次のいずれかの手順を実行し、[アクセスコントロール] ページに移動します。
   - WebFOCUS Hub からは、ブラウザをリフレッシュして [アクセスコントロール] ページを再表示します。
   - Reporting Server ブラウザインターフェースからは、[ツール]、[アクセスコントロール] を順に選択して [アクセスコントロール] ページに戻ります。

7. 下図のように、[アクセスコントロール] ページのセキュリティプロバイダリストで、新しいステータスがセキュリティプロバイダ名の横に表示されていることを確認します。



手順　セキュリティプロバイダのステータスを変更するには

事前の確認事項 - 42 ページの「 ユーザアカウントをサーバ管理者として登録するには 」に、の手順に従って、新しいプライマリセキュリティプロバイダのセキュリティ管理者が作成済みであることを確認します。管理者が作成済みでない場合、新しいプライマリセキュリティプロバイダを指定した後で、Reporting Server ブラウザインターフェースにアクセスできなくなります。

WebFOCUS Reporting Server 構成内でプライマリセキュリティプロバイダに指定できるのは、1 つのセキュリティプロバイダのみです。そのため、既存のプライマリセキュリティプロバイダを別のセキュリティプロバイダで置換する場合、既存のプライマリセキュリティプロバイダは自動的にセカンダリセキュリティプロバイダになります。

セキュリティプロバイダを変更する場合、[PTH<内部>] をセカンダリセキュリティプロバイダとして常に保持することをお勧めします。これにより、プライマリセキュリティプロバイダが使用できない場合でも WebFOCUS Reporting Server へのアクセスを続行することができます。

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] ページに移動します。要求された場合は、有効なサーバ管理者 ID およびパスワードを入力し、ログインします。ログインページにセキュリティプロバイダリストが表示された場合は、セキュリティプロバイダを選択します。

2. 変更するセキュリティプロバイダごとに、次のいずれかの手順を実行します。
   a. プライマリセキュリティプロバイダとしてプロバイダを有効にするには [プライマリ] を選択します。

      注意：別のセキュリティプロバイダがプライマリセキュリティプロバイダとしてすでに指定されている場合は、このセキュリティプロバイダのステータスが自動的に [セカンダリ] に変更されます。

   b. 代替セキュリティプロバイダとしてプロバイダを有効にするには [セカンダリ] を選択します。
   c. プロバイダを無効にするには [非アクティブ] を選択します。

   選択するたびにタブがリフレッシュされます。
3. タブがリフレッシュされた後、[保存] をクリックします。
4. 指定したセキュリティ管理者 ID が、新しく選択したプライマリセキュリティプロバイダで有効であることを確認するよう要求するメッセージで内容を確認し、[適用してサーバを再起動] を選択します。

   注意：OPSYS セキュリティプロバイダを有効にしたが、OPSYS のサーバ管理者を指定していない場合、OPSYS セキュリティプロバイダのサーバ管理者を登録するよう要求するメッセージが表示されます。この場合、42 ページの「 ユーザアカウントをサーバ管理者として登録するには 」 の手順に従います。

   このメッセージが表示されない場合、次の手順へ進みます。

   WebFOCUS Reporting Server が再起動中であることを示すメッセージが表示されます。
5. WebFOCUS Reporting Server が再起動中であることを示すメッセージが表示された場合は、WebFOCUS Reporting Server が再起動されるまで待機します。

   注意

   - OPSYS をプライマリプロバイダに設定している場合は、WebFOCUS Reporting Server を常に手動で再起動する必要があります。
   - ブラウザに「ワークスペース再起動中です」というメッセージが 30 秒以上表示された場合は、ブラウザを閉じてから再度開きます。Reporting Server ブラウザインターフェースに再度ログインします。
6. 要求された場合、有効なサーバ管理者のユーザ ID、パスワード、セキュリティプロバイダで WebFOCUS Reporting Server に再度ログインします。
7. Reporting Server ブラウザインターフェース のホームページで、[ツール]、[アクセスコントロール] を順に選択し、[アクセスコントロール] ページを開きます。

8. [アクセスコントロール] ページのセキュリティプロバイダリストで、更新されたセキュリティプロバイダ名の横に新しいステータスが表示されていることを確認します。

参照　セキュリティプロバイダコール

下表は、WebFOCUS Reporting Server からセキュリティ情報を取得するために使用するリクエストを示しています。

WebFOCUS リクエスト (event.log に表示)	**対応するサーバメッセージ**	**定義**
getProviders()	get all providers	外部認証または外部認可に使用され、WebFOCUS Reporting Server ノードで構成されているセキュリティプロバイダを取得します。
authConnect	authenticate and get user info, u=*userid*	外部認証を使用するようインストールで構成されている場合に、ユーザを認証し、ユーザの説明および Email アドレスをセキュリティプロバイダから取得します。
getGroupsForUser()	get groups, u=*userid*	ユーザの外部グループメンバーシップおよびその他の外部認可情報を取得します。また、セキュリティセンターでユーザのグループメンバーシップレポートを生成します。
getUsersForGroup()	get users, g=*group*	マッピングされた グループに属する ユーザを取得します。

WebFOCUS リクエスト (event.log に表示)	**対応するサーバメッセージ**	**定義**
getGroups() [mask:*searchstring*]	get groups, [g=*searchstring*,] provider=*providerName*	[グループの編集] ダイアログボックスで [参照] ボタンをクリックした際に、外部グループ、または外部認可に使用される他の属性を取得します。
getUsers()	get user info, u=*userid*, provider=*providerName*	事前認証構成でユーザの説明および Email アドレスを取得します。

トラステッド接続の構成

トラステッド接続は、WebFOCUS Client と WebFOCUS Reporting Server 間、および ReportCaster Distribution Server と WebFOCUS Reporting Server 間で構成することができます。

WebFOCUS への接続には、トラステッド接続を使用することをお勧めします。この方法には、複数の利点があります。

- 外部認証の場合、トラステッド接続により WebFOCUS Reporting Server への接続が効率的になるとともに、認証プロバイダに対する追加の認証リクエストが必要なくなります。これにより、システムパフォーマンスが向上します。
- 事前認証の場合、トラステッド接続により、WebFOCUS Reporting Server から認証情報の入力がユーザに要求されなくなります。

注意：WebFOCUS Reporting Server でトラステッド接続を受容するよう構成する必要があります。詳細は、53 ページの 「 TIBCO WebFOCUS Reporting Server でトラステッド接続を受容するよう構成するには 」 を参照してください。

手順　WebFOCUS Client と TIBCO WebFOCUS Reporting Server 間のトラステッド接続を構成するには

1. 管理者としてログインし、管理コンソールを開きます。
2. [構成] タブで、[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。

   既存の WebFOCUS Reporting Server 接続のリストがツリーに表示されます。

3. トラステッド接続を設定する WebFOCUS Reporting Server のノードをクリックします。

   [Client の構成] ページが開きます。

4. [セキュリティ] で、[Trusted] を選択します。トラステッド接続では、WebFOCUS ユーザ ID が WebFOCUS Reporting Server に渡されます。

5. ユーザグループ情報を含めるか、省略するかを選択することができます。

   a. ユーザグループ情報を含めるには、[TIBCO WebFOCUS ユーザ ID とグループを送信] を選択します。これがデフォルト値です。手順 7 へ進みます。

   b. ユーザグループ情報を省略するには、[カスタム] を選択します。手順 6 へ進みます。

6. [ユーザ ID] および [ユーザのグループ] のチェックボックスと関連するオプションが表示されます。

   a. ユーザ ID は WebFOCUS Reporting Server に渡す必要があるため、[ユーザ ID] のチェックは事前にオンに設定されています。

      - TIBCO WebFOCUS スクリプト変数は変更しないでください。この変数には [IBIMR_user] を指定する必要があります。

      - ユーザ ID をスクリプト変数で渡す代わりに、HTTP ヘッダで渡す場合は、[HTTP ヘッダフィールド] のチェックをオンにします。HTTP ヘッダフィールドのファイル名を入力します。

   b. WebFOCUS Reporting Server にグループ情報を渡さない場合は、[ユーザのグループ] のチェックをオフにします。WebFOCUS Reporting Server にグループ情報を渡す場合は、チェックをオンのままにします。

      - デフォルトスクリプト変数の IBIMR_memberof を使用するか、別の変数を入力します。

      - グループ情報をスクリプト変数で渡す代わりに、HTTP ヘッダで渡す場合は、[HTTP ヘッダフィールド] のチェックをオンにします。HTTP ヘッダフィールドのファイル名を入力します。

7. [保存] をクリックします。

ReportCaster を使用する場合は、ReportCaster Distribution Server と WebFOCUS Reporting Server 間のトラステッド接続を構成することもできます。それ以外の場合は、事前認証または外部認証の特定のタイプを構成する手順へ進みます。

手順

ReportCaster Distribution Server と TIBCO WebFOCUS Reporting Server 間のトラステッド接続を構成するには

ReportCaster を使用する場合は、スケジュール済みジョブの実行時に確立する、ReportCaster Distribution Server と Reporting Server のトラステッド接続を構成することができます。

注意: 現在、WebFOCUS での ReportCaster からのトラステッド接続では、WebFOCUS Reporting Server にスケジュールオーナーのユーザ ID は送信されますが、WebFOCUS グループは送信されません。

1. WebFOCUS に管理者としてログインし、ReportCaster コンソールを起動します。
2. リボンの [表示] グループで、[構成] をクリックします。
3. [データサーバ] フォルダを展開し、構成する WebFOCUS Reporting Server のフォルダをクリックします。
4. [セキュリティタイプ] リストから [Trusted] を選択します。
5. リボンの [構成の管理] グループで [保存] をクリックします。
6. ReportCaster 構成の変更を確認するメッセージで、[OK] をクリックします。
7. Distribution Server の再起動と、ReportCaster Web アプリケーションの再ロードを指示するメッセージで、[OK] をクリックします。
8. Reporting Server ブラウザインターフェースのリボンの [構成の管理] グループで、[再起動] をクリックします。

手順

TIBCO WebFOCUS Reporting Server でトラステッド接続を受容するよう構成するには

WebFOCUS Reporting Server でトラステッド接続を受容するようセキュリティプロバイダを構成することができます。各プロバイダは、それぞれ個別に構成します。特定のプロバイダでトラステッド接続を有効にし、他のプロバイダでは無効にすることができます。

注意: トラステッド接続は、Windows サーバ OPSYS プロバイダではサポートされません。

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] ページを開きます。要求された場合は、有効なサーバ管理者 ID およびパスワードを入力し、ログインします。ログインページに [セキュリティプロバイダ] リストが表示された場合は、セキュリティプロバイダを選択します。
2. [アクセスコントロール] ナビゲーションウィンドウの [セキュリティプロバイダ] 下でセキュリティプロバイダを右クリックして、[プロパティ] を選択します。

   そのプロバイダの [セキュリティの構成] ページが開きます。

3. ナビゲーションウィンドウの [セキュリティプロバイダ] フォルダ下で、セキュリティプロバイダをダブルクリックします。
4. [trust_ext] ドロップダウンリストで [y] を選択し、[保存] をクリックします。

   WebFOCUS Reporting Server 再起動中のメッセージが表示された場合は、待機します。
5. WebFOCUS Reporting Server のログインページが表示された場合は、Reporting Server の管理者 ID とパスワードを入力し、[セキュリティプロバイダ] リストが表示された場合は、セキュリティプロバイダを選択して、[ログイン] をクリックします。
6. Reporting Server ブラウザインターフェースホームページで、[ツール]、[アクセスコントロール] を順に選択します。

   セキュリティプロバイダの [Trusted を受容する] 列にチェックマークが表示されます。

TIBCO WebFOCUS での SSL 構成

HTTPS を使用すると、暗号化された SSL 接続が確立されます。WebFOCUS と、エンドユーザに割り当てられたブラウザとの間の通信を保護するには、HTTPS を使用する必要があります。このプロトコルの使用を有効にする構成オプションは多数あります。その 1 つとして、ここでは Apache Tomcat 構成について説明します。

SSL ベースの通信を有効にするには、Java の自己署名証明書を作成します。また、必要に応じて自己署名証明書を認証局に提出し、信頼済み証明書として設定することもできます。証明書を作成する keytool ユーティリティを実行すると、接続タイプがオープンから SSL に変更されます。そのため、Tomcat server.xml ファイルでデフォルトコネクタプロトコル設定をコメントアウトし、代わりに新しい SSL コネクタプロトコル設定を記述する必要があります。

最後に、SSL セキュリティを設定するには、WebFOCUS と内部アプリケーションとの間のデフォルト接続を置き換える必要があります。これらの内部アプリケーションとして、JSCOM3 Java ベースのリスナに接続してグラフを作成するアプリケーションや Excel シートに出力するアプリケーションがあります。この変更を実装するには、WebFOCUS Client の設定で、[Excel Server URL] (EXCELSERVURL) および [グラフサーバ URL] (GRAPHSERVURL) 設定に [Reporting Server JCOM] 値を割り当てる必要があります。

注意：管理者は、WebFOCUS 構成の外部で、SSL を使用するよう IIS を構成することができます。詳細は、IIS、Tomcat、Application Server プロバイダから提供されるマニュアルを参照してください。

手順　自己署名入り証明書を作成するには

Java 自己署名入り証明書を作成するには、次の手順を実行します。

1. [コマンドプロンプト] ウィンドウを開き、コマンドプロンプトを *drive*:¥ibi ¥WebFOCUS82¥jre¥bin ディレクトリに移動します。
2. 次の例のように、keytool コマンドおよび値を入力します。

```
keytool -genkeypair -alias mykey -ext san=dns:dnsName1,dns:dnsName2…
-keyalg RSA -validity 720 -keystore /path_to_keystore/keystore
-keysize 2048 –storepass MyPassword
```

説明

`dnsName`
この証明書を認証用に提示するエンティティ (サブジェクト) の名前またはエイリアスです。すべてのバージョンのサブジェクト名が認識されるよう複数の名前を含めることができます。複数の名前を含めるには、「dns:first_dnsName,dns:second_dnsName,...」構文を使用します。

たとえば、「dns:wfsvr,dns:wfsvr.ibi.com」と入力します。

`MyPassword`
このキーストアのパスワードです。デフォルト値の MyPassword を使用することも、テキストボックスに一意のパスワードを入力してデフォルト値を置換することもできます。

`/path_to_keystore/keystore`
キーファイルの格納先を指定するパス情報です。この値はオプションとして指定します。キーファイルのパスを指定しない場合、Keytool ユーティリティはキーファイルをデフォルトディレクトリに格納します。

注意：認証局の署名入り証明書を要求するために -certreq (証明書リクエスト) を発行する必要がある場合、「mykey」という名前は重要です。

3. Enter キーを押します。

コマンドプロンプトに、一連の質問の第 1 問が表示されます。

4. 次の各質問に回答し、回答後に Enter キーを押します。
   - What is your first and last name? - 証明書所有者の姓名を入力します。
   - What is the name of your organizational unit? - 証明書所有者の組織の部門名を入力します。
   - What is the name of your organization? - 証明書所有者の組織名を入力します。

- What is the name of your City or Locality? - 証明書所有者の都市名または地域名を入力します。
- What is the name of your State or Province? - 証明書所有者の所在地の州名を 2 文字の短縮名で入力します。
- What is the two-letter country code for this unit? - 証明書所有者の所在地の国名を 2 文字の短縮名で入力します。

5. コマンドプロンプトに「Is CN=__, OU=__, O=__, L=__, ST=__, C=__ correct?」という質問が表示されます。値を確認し、正しい場合は「y」を入力します。

   正しくない場合は「n」を入力し、keytool コマンドの手順 2 から再入力します。

   値が正しく入力されると、新しい自己署名入り証明書が使用可能になります。

参照　自己署名証明書の信頼済み証明書としての設定

新しい自己署名証明書がブラウザでの信頼済み証明書として識別されるまで、その自己署名証明をブラウザで使用するとエラーが表示されます。初期テスト時に、テストに含めるブラウザの信頼済み認証局に、新しい自己署名入り証明書を直接追加することができます。ただし、新しい証明書を信頼済み証明書として完全に設定するには、一般に次のリクエストを使用して認証局からの証明書を要求します。

```
keytool -certreq -alias mykey -storepass MyPassword –file ./mykey.csr
–keystore /path_to_keystore/keystore
```

説明

`MyPassword`
: このキーストアのパスワードです。デフォルト値の MyPassword を使用することも、テキストボックスに一意のパスワードを入力してデフォルト値を置換することもできます。

`/path_to_keystore/keystore`
: キーファイルの格納先を指定するパス情報です。この値はオプションとして指定します。キーファイルのパスを指定しない場合、Keytool ユーティリティはキーファイルをデフォルトディレクトリに格納します。

次に証明書リクエストファイル (mykey.csr) を認証局に送信して署名を要求し、認証局から署名入り証明書が返された後、その証明書をキーストアにインポートします。

参照　トラステッド証明書のキーストアへのインポート

外部の認証局 (CA) から証明書をインポートするには、次のコマンドを入力します。

```
keytool –import –alias mykey –file ./mykey.crt –keystore /path_to_keystore/
keystore
```

説明

/path_to_keystore/keystore
キーファイルの格納先を指定するパス情報です。この値はオプションとして指定します。キーファイルのパスを指定しない場合、Keytool ユーティリティはキーファイルをデフォルトディレクトリに格納します。

使用する CA が内部 CA の場合は、次のコマンドを入力して CA から証明書をインポートします。

```
keytool –import –alias CA –trustcacerts –file ./ca.crt –keystore /
path_to_keystore/keystore
```

説明

/path_to_keystore/keystore
キーファイルの格納先を指定するパス情報です。この値はオプションとして指定します。キーファイルのパスを指定しない場合、Keytool ユーティリティはキーファイルをデフォルトディレクトリに格納します。

参照 Tomcat Server.xml ファイルでのコネクタプロトコルの更新

製品のインストール時に Tomcat を使用するよう選択した場合、Tomcat の server.xml ファイルは次のディレクトリに保存されます。

```
C:¥ibi¥tomcat¥conf
```

keytool ユーティリティを実行すると、ポート番号 26000 に割り当てられた http 接続が無効になります。そのため、server.xml ファイルで、この http ベースの接続を定義する Connector タグをコメントアウトする必要があります。コメントアウトするには、開始タグ記号 (<) に続いて感嘆符 (!) を入力します。

```
<Connector connectionTimeout="20000" maxPostSize="-1" port="26000"
protocol="HTTP/1.1" redirectPort="26001" useBodyEncodingForURI="true"/>
```

また、keytool ユーティリティを実行すると、ポート番号 443 に SSL コネクタが設定されます。従来の http ベースの接続は、この接続に置き換えられます。そのため、この接続がファイルに存在しない場合、次の例のように、この最新の Connector タグと、その属性および値を手動で入力する必要があります。

```
<Connector protocol="org.apache.coyote.http11.Http11Protocol"
port="443" SSLEnabled="true"
keystoreFile="C:/users/path_to_keystore/keystore"
keystorePass="MyPassword"
maxThreads="150" scheme="https" secure="true"
clientAuth="false" sslProtocol="TLS"
ciphers="TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA"/>
```

説明

`/path_to_keystore/keystore`
キーファイルの格納先を指定するパス情報です。この値はオプションとして指定します。キーファイルのパスを指定しない場合、Keytool ユーティリティはキーファイルをデフォルトディレクトリに格納します。

`MyPassword`
このキーストアのパスワードです。デフォルト値の MyPassword を使用することも、テキストボックスに一意のパスワードを入力してデフォルト値を置換することもできます。

手順　SSL をサポートする TIBCO WebFOCUS 構成に変更するには

次の手順を開始する前に、WebFOCUS Reporting Server 上で JSCOM サービスが構成され、稼動していることを確認します。詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』の「JSCOM3 リスナの Java サービスを構成するには」を参照してください。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [アプリケーションの設定] 下で、[Client 設定] をクリックします。
3. [Excel Server URL] リストから [Reporting Server JSCOM] を選択します。
4. [グラフサーバ URL] リストから [Reporting Server JSCOM] を選択します。
5. [保存] をクリックします。
6. 「保存しました」というメッセージで [OK] をクリックします。

TIBCO WebFOCUS Reporting Server プロファイル

次のプロファイルを使用して、WebFOCUS Reporting Server のデフォルト動作を構成することができます。

- **WebFOCUS Reporting Server グローバルプロファイル (edasprof.prf)**　グローバルプロファイルは、サーバのインストール時に自動的に作成される起動ファイルです。このファイルには、Reporting Server のデフォルト環境設定が格納されます。グローバルプロファイルは、ユーザセッションが終了するまで有効です。
- **WebFOCUS Reporting Server サービスプロファイル**　サービスプロファイルは、WebFOCUS Reporting Server が特定サービスに関連する接続の環境設定を指定するために使用されるファイルです。Client がサービス修飾子を使用して Reporting Server に接続すると、サービスプロファイルの設定が適用され、ユーザセッションが終了するまで有効になります。サービスプロファイルにはグローバルプロファイルと同じ設定を含めることができます。

- **WebFOCUS Reporting Server グループプロファイル**　グループプロファイルは、Reporting Server が特定のセキュリティグループに属するユーザの環境設定を指定するために使用されるファイルです。グループプロファイルは、ユーザが Reporting Server に接続した際に適用されます。これらの設定は、Reporting Server セッションが終了するまで有効です。グループプロファイルに含める設定の大部分は、グローバルプロファイルで使用する同一のコマンドセットで定義される設定と重複させることができます。このプロファイルは、セキュリティがオンに設定されている場合にのみ有効になります。グループプロファイル処理についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。
- **WebFOCUS Reporting Server ユーザプロファイル (userid.prf)**　ユーザプロファイルは、Reporting Server が特定のユーザ ID の環境設定を指定するために使用されるファイルです。ユーザプロファイルの設定は、ユーザが Reporting Server に接続した際に適用されます。これらの設定は、ユーザセッションが終了するまで有効です。ユーザプロファイルに含める設定の大部分は、グローバルプロファイルで使用する同一のコマンドセットで定義される設定と重複させることができます。

詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

TIBCO WebFOCUS Reporting Server プロファイルへの変数の送信

WebFOCUS Client から Reporting Server に送信されるセキュアリクエストに、Reporting Server プロファイルを有効にする変数および値のリストを追加し、条件付きロジックにより DBMS 設定を切り替えることで、カスタマイズされたサーバ環境を作成することができます。たとえば、1 つ目の値セットでテスト環境を有効にし、2 つ目の値セットで実稼動環境を有効にします。

BI Portal リクエストの場合、これらの変数、各変数の値、および DBMS 接続情報は、リクエスト送信元の BI Portal ワークスペースで定義することができます。APP リクエストの場合、これらはリクエスト送信元の HTTP ホストヘッダで定義することができます。これらの変数および各変数の値は、WebFOCUS Client で設定する必要があります。また、その Client によって変数に割り当てられた値は、URL に含める際に上書きしてはなりません。WebFOCUS Client は、一連の変数および各変数の値を一意のセットとして特定のサーバまたはすべてのサーバに送信することができます。

Client リクエストで変数を使用できるよう構成するには、管理者が [カスタム設定] リストに変数のリストを入力する必要があります。これにより、その Client から Reporting Server に送信されるリクエストにこれらの変数が追加されます。すべての Reporting Server に送信する変数を指定することも、特定の Reporting Server に送信する変数を指定することもできます。また、Reporting Server プロファイル内にこれらの変数が格納されたデータベースを指定することもできます。

手順　TIBCO WebFOCUS Reporting Server リクエストに含める変数を構成するには

Client の変数のリスト、および各変数の値を構成できるのは管理者のみです。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブで [カスタム設定] をクリックします。
3. この Client から送信される変数のリストおよび各変数に割り当てられる値を定義するには、次の手順を実行します。
   a. [カスタム設定] リストに、次のコマンド行を入力します。
      ```
      #variables and values
      ```
   b. 次のフォーマットで変数と値のエントリを入力します。
      ```
      VariableName=Value
      ```
      説明
      VariableName
      この Client から送信する変数の名前です。この変数は、リクエストの受信先 Reporting Server に接続される変数データベースに存在する必要があります。
      Value
      この Client から送信する変数の値です。
      以下はその例です。
      ```
      #variables and values

      IBI_pvar=XPROFILE

      IBI_clientName=Client1

      ABCVar=Test2
      ```
4. すべてのサーバに送信する変数のリストを定義するには、次の手順を実行します。
   a. [カスタム設定] リストに、次のコマンド行を入力します。
      ```
      #List of profile variables to be sent to all eda servers
      ```
   b. 次のコマンドを入力します。
      ```
      IBIC_profileVars=Variable1;Variable2;…
      ```

説明

Variable#

変数と値のリストで定義される変数です。

以下はその例です。

```
#List of profile variables to be sent to all eda servers

IBIC_profileVars=IBI_pvar;IBI_clientName;
```

5. 特定のサーバに送信する変数のリストを定義するには、次の手順を実行します。
   a. [カスタム設定] リストに、次のコマンド行を入力します。

      ```
      #list of profile variables to be sent ONLY to server named ServerName
      ```

      説明

      ServerName

      変数のリストを送信する特定のサーバの名前です。

   b. 次のコマンドを入力します。

      ```
      IBIC_profileVars_ServerName=Variable1;Variable2;
      ```

      説明

      ServerName

      変数のリストを送信する特定のサーバの名前です。

      Variable#

      変数と値のリストで定義される変数です。

      以下はその例です。

      ```
      #list of profile variables to be sent ONLY to server named EDASERVE

      IBIC_profileVars_EDASERVE=ABCVar;
      ```

6. [保存] をクリックします。
7. 「保存しました」というメッセージで [OK] をクリックします。

手順　Client リクエストの変数を受容するよう TIBCO WebFOCUS Reporting Server プロファイルを更新するには

管理者は、次のステートメントをサーバプロファイルリストの末尾に追加することで、サーバプロファイルを更新する必要があります。

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダを展開します。
2. [サーバ接続] フォルダ下で [EDASERVE] を右クリックし、[プロファイル] を選択します。
3. EDASERVE.prf リストに、次の行を入力します。

   ```
   APP FILEDEF &IBI_pvar bugs/DatabaseName.dat
   ```

   説明

   DatabaseName

   Reporting Server に関連付けられているデータベースの名前です。

   以下はその例です。

   ```
   APP FILEDEF &IBI_pvar bugs/edasprof.dat
   ```

4. [保存] をクリックします。
5. 「保存しました」というメッセージで [OK] をクリックします。

3

WebFOCUS Client の構成

管理コンソールを使用して WebFOCUS Client を構成、管理することができます。管理コンソールでは、WebFOCUS 構成設定の更新、ログおよびトレースの有効化、WebFOCUS セッションのモニタ、WebFOCUS コンポーネントの確認を行えます。構成ファイルは、手動で編集することもできます。

トピックス

WebFOCUS 構成ファイル

WebFOCUS 構成ファイルは、*drive:*¥ibi¥WebFOCUS82¥config フォルダに格納されています。これらのファイルを別の環境に移動することで、構成設定を簡単に移植することができます。

WebFOCUS のインストール中に、ユーザが選択したデフォルト構成値がブートストラップファイル (web.xml) およびインストール構成ファイル (install.cfg) に書き込まれます。ほとんどの設定では、構成動作を変更すると、新しい値が webfocus.cfg ファイルに書き込まれます。WebFOCUS を起動すると、最初にブートストラップファイル内の IBI_DOCUMENT_ROOT 設定が確認されます。この設定は、多数のディレクトリの検索先を WebFOCUS に指示するものです。WebFOCUS は、この IBI_DOCUMENT_ROOT 値を使用して、Java コードで指定された製品デフォルト値を特定します。次に install.cfg ファイルで指定されたインストールデフォルト値を確認し、続いて webfocus.cfg ファイルで指定された変更を確認します。これらの処理はすべて、event.log ファイルに記録されます。

event.log ファイルについての詳細は、605 ページの 「 ログの収集 」 を参照してください。

構成ファイル (例、install.cfg、webfocus.cfg) にパスワードを直接入力した場合、次回の WebFOCUS 起動時またはコマンドラインユーティリティ (例、変更管理) の実行時に、WebFOCUS がそのパスワードを自動的に暗号化します。他の暗号化ユーティリティを実行する必要はありません。

webfocus.cfg 以外のファイルに書き込まれるセキュリティ構成設定には、セキュリティゾーン構成ファイル (例、securitysettings.xml) があります。詳細は、525 ページの 「 TIBCO WebFOCUS Client 構成ファイル 」 を参照してください。

構成ファイル内の行の先頭にシャープ記号 (#) を追加すると、その行のテキストがコメントに変換され、WebFOCUS がこのファイルを呼び出した際に、その行の変数やコマンドが実行されなくなります。この機能を使用して、変数をコメントに変換することができます。また、このファイルに記述されている設定や割り当て値に関する注釈、説明、覚書をコメントとして追加することもできます。

変数をコメントに変換するには、変数が記述されている行の先頭にシャープ記号 (#) を入力します。コメントを追加するには、新しい行を作成し、シャープ記号 (#) を追加した後に注釈、説明、覚書を入力します。変更作業の完了後、管理コンソールのメニューバーで [キャッシュのクリア] をクリックし、構成ファイルに加えた変更を保存します。

WebFOCUS 管理コンソールの使用

WebFOCUS 管理コンソールの各種設定を使用して、WebFOCUS Client の構成、内部認証または外部認証設定のカスタマイズ、ReportCaster への接続、機能診断の設定を行えます。

WebFOCUS 管理コンソールの起動

管理コンソールには WebFOCUS 全体の動作に影響する各種設定が表示されるため、管理コンソールにアクセスできるユーザは、システム設定を更新または再構成する権限を所有するユーザに限定されます。

そのため、管理コンソールを起動するには、管理コンソールへのアクセス権限を所有するユーザ ID でログインする必要があります。管理コンソールは、次のいずれかの方法で起動することができます。

WebFOCUS Hub で、次の手順を実行します。

- サイドナビゲーションウィンドウで [管理センター] を選択し、[クライアント管理] 下で [管理コンソール] を選択します。

WebFOCUS ホームページで、次の手順を実行します。

- バナーで [設定] をクリックし、[管理コンソール] を選択します。

ブラウザのアドレスバーで、次の操作を実行します。

❑ 次の URL を入力します。

```
http(s)://host:port/context/admin
```

説明

`host`
WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

`port`
Web サーバまたは Application Server が受信待機するポートの番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

`context`
WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

注意：WebFOCUS にログイン済みで、マシンの ID、ポート番号、コンテキストがアドレスバーにすでに表示されている場合は、コンテキストパスの部分を「/admin」で上書きするだけです。

手順　スタートメニューから管理コンソールにログインするには

1. WebFOCUS が Windows 7 マシンにインストールされている場合は、次の手順を実行します。
   a. [スタート] ボタンをクリックし、[Information Builders] フォルダを展開します。
   b. [WebFOCUS 82] フォルダを展開し、[WebFOCUS 管理コンソール] を選択します。
   c. 手順 3 へ進みます。
2. WebFOCUS が Windows 10 マシンにインストールされている場合は、次の手順を実行します。
   a. [スタート] ボタンをクリックします。
   b. アプリリストを下方向へスクロールし、[Information Builders] フォルダを展開します。
   c. WebFOCUS 統合インストールを使用する場合は、[Windows 統合インストール] フォルダを選択し、Windows 統合インストールのファイルエクスプローラウィンドウを開き、[WebFOCUS の実行] を選択してログインします。

次の手順のいずれかを実行し、管理コンソールを起動します。

- WebFOCUS Hub のサイドナビゲーションウィンドウで、[管理センター] を選択し、[クライアント管理] 下の [管理コンソール] を選択します。

  または

- [ユーザ] メニューから [ホームページの切り替え]、[WebFOCUS ホームページ] を順に選択し、WebFOCUS ホームページのバナーで、[設定]、[管理コンソール] を順に選択します。

d. WebFOCUS 統合インストールを使用しない場合は、[Information Builders] フォルダを展開して [WebFOCUS 管理コンソール] を選択し、管理コンソールの起動権限を所有するユーザ名およびパスワードでログインします。

手順　ブラウザウィンドウから管理コンソールにログインするには

1. 次の URL に移動します。

   ```
   http(s)://host:port/context/admin
   ```

   説明

   `host`
   WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

   `port`
   Web サーバまたは Application Server が受信待機するポートの番号です。

   この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

   `context`
   WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

2. [ログイン] ページで、管理コンソールの起動権限を所有するユーザ名およびパスワードを入力し、[ログイン] をクリックします。

   管理コンソールが自動的に起動します。

   注意：管理コンソールを他の言語で表示するには、[ログイン] ページで [言語の選択] をクリックし、言語のリストから使用する言語を選択します。

ReportCaster コンソールの起動

ReportCaster コンソールを使用して、ReportCaster サーバ環境の構成をグローバルに変更することができます。ReportCaster コンソールには、WebFOCUS Hub のメインメニュー、WebFOCUS ホームページの [ユーティリティ] メニュー、管理コンソールの [ReportCaster] タブからアクセスできます。

ReportCaster コンソールを起動するには、ReportCaster コンソールへのアクセス権限を所有するユーザ ID でログインする必要があります。ReportCaster コンソールは、次のいずれかの方法で起動することができます。

WebFOCUS Hub で、次の手順を実行します。

- サイドナビゲーションウィンドウ上部のメインメニューで、[クイックアクセス] から [ReportCaster ステータス] を選択します。

WebFOCUS ホームページで、次の手順を実行します。

- バナーの [ユーティリティ] から [ReportCaster ステータス] を選択します。

または

- バナーの [設定] から [管理コンソール] を選択します。管理コンソールで [ReportCaster] タブをクリックします。

ReportCaster についての詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』を参照してください。

各種ホームページの使用

製品インストールでログイン時にデフォルト設定で最初に開くページは、[リダイレクト / ibi_apps 先] 設定で定義します。

デフォルト設定のホームページ構成に関係なく、作業セッションを開始後に、これらのホームページのいずれかを開くことができます。この機能は、そのページでのみ使用可能な機能を実行する場合に特に重要です。

ブラウザウィンドウに URL を入力して、各種ホームページにログインすることもできます。ただし、作業セッション中には、[リダイレクト / ibi_apps 先] 設定で定義されたデフォルトホームページに戻ります。

注意：[リダイレクト / ibi_apps 先] 設定で割り当てられる名前は、ユーザの WebFOCUS 構成で使用される主要コンテキストまたはエイリアスに割り当てられた名前によって異なります。この設定には通常、「/ibi_apps」が表示されます。これは、WebFOCUS インストールの主要コンテキストまたはエイリアスとして「/ibi_apps」がよく使用されるためです。組織で別の主要コンテキストまたはエイリアスを使用する場合は、代わりにその値がこの設定に表示されます。割り当てられる主要コンテキスト名に関係なく、この設定は、管理コンソールの [構成] タブの [BI Portal] 設定ページの一番上に表示されます。

手順　ブラウザウィンドウから WebFOCUS Hub を開くには

ブラウザに基本コンテキスト URL を入力して、WebFOCUS Hub を開くことができます。

1. ブラウザのアドレスバーに、次の URL を入力します。

   ```
   http(s)://host:port/context/
   ```

   説明

   `host`
   TIBCO WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

   `port`
   Web サーバまたは Application Server が受信待機するポートの番号です。

   この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

   `context`
   TIBCO WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

   注意：ログインする際に、マシンの ID、ポート番号、コンテキストがアドレスバーにすでに表示されている場合は、コンテキストの後の部分のパスを削除するだけです。

2. 使用中のユーザ認証方法でログインが必要ない場合、またはすでにログイン済みの場合は、WebFOCUS Hub が自動的に開きます。
3. ユーザ認証でログインが必要な場合は、[ログイン] ページに有効なユーザ名とパスワードを入力し、[ログイン] をクリックします。

   これに応答して WebFOCUS Hub が開きます。

手順　ブラウザウィンドウから WebFOCUS ホームページを開くには

ブラウザに URL を入力して WebFOCUS ホームページを開くことができます。

1. ブラウザのアドレスバーに、次の URL を入力します。

   ```
   http(s)://host:port/context/home
   ```

   説明

   `host`
   WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

   `port`
   Web サーバまたは Application Server が受信待機するポートの番号です。

   この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

   `context`
   WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

   注意：ログインする際に、マシンの ID、ポート番号、コンテキストがアドレスバーにすでに表示されている場合は、コンテキストの後のパスの一部を「/home」で上書きするだけです。

   `home`
   WebFOCUS ホームページを開くパスです。このパスでは、大文字と小文字が区別されます。

2. 使用中のユーザ認証方法でログインが必要ない場合、またはすでにログイン済みの場合は、WebFOCUS ホームページが自動的に開きます。
3. ユーザ認証でログインが必要な場合は、[ログイン] ページに有効なユーザ名とパスワードを入力し、[ログイン] をクリックします。

   これに応答して WebFOCUS ホームページが開きます。

手順　ブラウザウィンドウからレガシーホームページを開くには

ブラウザに URL を入力してレガシーホームページを開くことができます。

1. ブラウザのアドレスバーに、次の URL を入力します。

   ```
   http(s)://host:port/context/legacyhome
   ```

説明

`host`

WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

`port`

Web サーバまたは Application Server が受信待機するポートの番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

`context`

WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

`legacyhome`

レガシーホームページを開くパスです。このパスでは、大文字と小文字が区別されます。

以下はその例です。

```
https://Server01:8080/ibi_apps/legacyhome
```

2. 使用中のユーザ認証方法でログインが必要ない場合、またはすでにログイン済みの場合は、レガシーホームページが自動的に開きます。
3. ユーザ認証でログインが必要な場合は、[ログイン] ページに有効なユーザ名とパスワードを入力し、[ログイン] をクリックします。

   これに応答してレガシーホームページが開きます。

手順　ホームページを切り替えるには

[ユーザ] メニューの [ホームページの切り替え] オプションを使用して、異なるホームページを起動して使用することができます。

WebFOCUS Hub で [ユーザ] メニューを展開し、[ホームページの切り替え] オプションを選択後、[WebFOCUS ホームページ] または [レガシーホームページ] のいずれかを選択します。

手順　WebFOCUS ホームページからレガシーホームページを開くには

WebFOCUS ホームページで、[ユーザ] メニューから [レガシーホームページ] をクリックします。

注意：管理コンソールの [構成] タブの [BI Portal] ウィンドウで、[リダイレクト /ibi_apps 先] 設定の [バナーリンクにレガシーホームページオプションを表示] のチェックがオフになっている場合、レガシーホームページのコマンドは表示されません。

手順　ブラウザウィンドウからカスタムようこそページを開くには

ブラウザに URL を入力してカスタムようこそページを開くことができます。

1. ブラウザのアドレスバーに、次の URL を入力します。

   ```
   http(s)://host:port/context/path
   ```

   説明

   `host`
   WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

   `port`
   Web サーバまたは Application Server が受信待機するポートの番号です。

   この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

   `context`
   WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

   `path`
   カスタムようこそページを開くパスです。このパスでは、大文字と小文字が区別されます。

   注意：ログインする際に、マシンの ID、ポート番号、コンテキストがアドレスバーにすでに表示されている場合は、コンテキストの後に表示されるパスの一部をカスタムようこそページのパスの残りの部分で上書きするだけです。

2. 使用中のユーザ認証方法でログインが必要ない場合、またはすでにログイン済みの場合は、カスタムようこそページが自動的に開きます。
3. ユーザ認証でログインが必要な場合は、[ログイン] ページに有効なユーザ名とパスワードを入力し、[ログイン] をクリックします。

   これに応答してカスタムようこそページが開きます。

WebFOCUS 管理コンソールのナビゲート

管理コンソールには、各種設定およびその他の機能のナビゲートを容易にするためのメニューバーと 4 つのタブが表示されます。

これらのタブでは、管理操作が次のカテゴリに分類されています。

- **構成** Reporting Server への接続、アプリケーションの設定、カスタム設定、NLS 設定、出力先変更設定、言語の切り替え、InfoAssist のプロパティを構成します。このタブからは、[ロール更新ユーティリティ] および [HTML5 グラフ拡張機能] にもアクセスできます。
- **セキュリティ** 内部認証と外部認証の全般的なセキュリティ設定、およびセキュリティゾーンの認証、リクエスト一致の設定を構成します。
- **ReportCaster** ReportCaster コンソールを開き、ReportCaster の構成、Distribution Server の再起動、環境パラメータの構成、トレースのオンとオフの切り替えを行えます。管理コンソールでは、ユーザ ID として IBIMR_RC_SVCUSER 値を使用して ReportCaster へのアクセスが認証されます。この認証に失敗した場合、認証情報の入力がユーザに要求されます。
- **機能診断** コンポーネントのインストールと構成の詳細表示、WebFOCUS ログ収集のオンとオフの切り替え、管理者によるログファイルの表示と ZIP コピーの作成を行えます。このタブからは、スタンドアロンユーティリティ実行時に作成されたアプリケーションファイルログ、および LRU キャッシュ統計のページにもアクセスできます。

  トレースは、セッションビューアで確認することができます。セッションビューアには、次のいずれかからアクセスできます。

  - WebFOCUS Hub で、[ツール] メニューから [セッションの表示] を選択します。
  - WebFOCUS ホームページで、[ユーティリティ] メニューから [セッションビューア] を選択します。
  - レガシーホームページで、BI Portal メニューバーの [ツール] メニューから [セッションビューア] を選択します。

メニューバーの各オプションを使用して、TIBCO WebFOCUS およびサードパーティのライセンス情報の確認、キャッシュのクリア、管理コンソールを閉じる (WebFOCUS ホームページまたはレガシーホームページから開いた場合)、ヘルプを開くなどの基本操作を実行することができます。

管理コンソールの設定を更新または確認するには、タブのいずれかをクリックし、選択したタブのメインメニューからフォルダまたはページアイコンをクリックします。メインウィンドウがリフレッシュされ、選択したページに割り当てられた各設定が表示されます。

構成タブのナビゲート

[構成] タブには、Reporting Server 接続を定義する設定および機能と、その他のアプリケーション設定が表示されます。下表は、これらの設定のリストおよびその説明を示しています。

フォルダ [ページ]	使用可能な機能
Reporting Server	[Reporting Server] フォルダ下の各サブフォルダには、WebFOCUS Client から各レポートサーバへのすべての接続を管理するツールが用意されています。次のサブフォルダを使用して、以下のことを行えます。 ❑ **サーバ接続**　リモートサービスの設定を追加、変更します。 ❑ **代替サーバマッピング**　特定の Reporting Server への代替マッピングを構成します。 ❑ **Cluster Manager**　Client から複数のリモートサーバへの詳細接続を構成します。この構成には、セキュリティ設定、暗号化方式、タイムアウト制限があります。 ❑ **レガシークラスタ**　Client から複数のリモートサーバへの基本接続を構成します。この構成には、追加の詳細設定はありません。

フォルダ [ページ]	使用可能な機能
構成 **[アプリケーションの設定]**	[構成] タブの [アプリケーションの設定] フォルダの各ページでは、次の機能エリアの設定を管理します。 ❑ アプリケーションキャッシュ ❑ アプリケーションコンテキスト ❑ アプリケーションディレクトリ ❑ BI Portal ❑ 変更管理 ❑ Client 設定 ❑ ディファードレポート ❑ 機能診断/トレース ❑ 暗号化 ❑ ESRI ❑ フィルタ ❑ 複数レポート ❑ Web ビューア ❑ OLAP* ❑ その他 ❑ パラメータのプロンプト ❑ Quick Data ❑ リポジトリ ❑ ソース管理 ❑ 検索 ❑ テキスト生成サーバ ❑ 検証 * [OLAP] 設定は、[OLAP を有効にする] のチェックをオンにした場合にのみ表示されます。

フォルダ [ページ]	使用可能な機能
構成 **[カスタム設定]**	[構成] タブの [カスタム設定] ページには、テキストベースの入力ボックスが表示され、WebFOCUS Client の高度なカスタム設定を定義することができます。このページを使用して、次のことを行えます。 ❏ WebFOCUS Client 設定をカスタマイズする。 ❏ WebFOCUS Client サイトプロファイルを作成する。 ❏ WebFOCUS Client ユニバーサルプロファイルを作成する。 ❏ Reporting Server のリクエストに含めるカスタム変数を構成する。
構成 **[NLS 設定]**	[構成] タブの [NLS 設定] ページには、国際言語サポートの設定が表示されます。
構成 **[言語の切り替え]**	[構成] タブの [言語の切り替え] ページには、現在の製品インストールに追加可能な言語のリストが表示されます。 [言語の切り替え] 設定は、drive:¥ibi¥WebFOCUS82¥config ディレクトリ内の languages.xml ファイルに格納されます。
構成 **[出力先変更設定]**	[構成] タブの [出力先変更設定] ページには、レポート出力の出力先変更設定を管理する設定が表示されます。
構成 **[InfoAssist のプロパティ]**	[構成] タブの [InfoAssist のプロパティ] ページには、InfoAssist レポートツールのレポートオプションを構成するためのプロパティが表示されます。
構成 **[ロール更新ユーティリティ]**	[構成] タブの [ロール更新ユーティリティ] ページには、リポジトリの各ロールに現在割り当てられている権限と、製品パッケージの各ロールに割り当てられている権限の差異が表示されます。

フォルダ [ページ]	使用可能な機能
構成 **[HTML5 グラフ拡張機能]**	[構成] タブの [HTML5 グラフ拡張機能] ページには、ローカルインストールに現在インストールされているすべての HTML5 グラフ拡張機能が表示されます。このページの機能を使用して、HTML5 グラフ拡張機能をアップロードしたり、これらの InfoAssist および WebFOCUS DESIGNER での使用を有効または無効にしたり、不要になった場合はアンインストールしたりできます。

セキュリティタブのナビゲート

[セキュリティ] タブには、内部セキュリティ設定、外部セキュリティ設定、詳細セキュリティ設定、およびセキュリティゾーンの設定が表示されます。下表は、これらの設定のリストおよび各設定の説明です。

フォルダ [ページ]	使用可能な機能
セキュリティの構成 **[内部]**	[セキュリティ] タブの [内部] ページには、WebFOCUS 内部で管理される認証と認可のログイン設定およびパスワード設定が表示されます。
セキュリティの構成 **[外部]**	[セキュリティ] タブの [外部] ページには、WebFOCUS 外部の他社製アプリケーションで管理される認証と認可の方法および実行先を定義する設定が表示されます。
セキュリティの構成 **[詳細]**	[セキュリティ] タブの [詳細] ページには、WebFOCUS で管理されるセキュリティおよび管理アクティビティをサポートするための設定が表示されます。たとえば、ルートユーザおよび匿名ユーザを識別する設定や Reporting Server 匿名ユーザを識別する設定があります。
セキュリティゾーン **デフォルト** **[認証、リクエスト一致]**	[デフォルトセキュリティゾーン] ページには、他のいずれのゾーンでも処理されないリクエストに使用するデフォルト認証方法の設定が表示されます。

フォルダ [ページ]	使用可能な機能
セキュリティゾーン **モバイル** **[認証、リクエスト一致]**	[モバイルセキュリティゾーン] ページには、TIBCO WebFOCUS モバイル製品 (例、TIBCO WebFOCUS Mobile App) の認証方法を定義する設定が表示されます。
セキュリティゾーン **ポートレット** **[認証、リクエスト一致]**	[ポートレットセキュリティゾーン] ページには、WebFOCUS Open Portal Services 製品 (例、SharePoint) の認証方法を定義する設定が表示されます。
セキュリティゾーン **代替** **[認証、リクエスト一致]**	[代替セキュリティゾーン] ページの設定では、同一 WebFOCUS 内のリクエストのデフォルトセキュリティゾーンで使用される認証方法の代替方法を定義します。

ReportCaster タブのナビゲート

[ReportCaster] タブをクリックすると、デフォルト設定で ReportCaster [サーバステータス] ページが開きます。このページの機能を使用して、ReportCaster サーバ処理の現在ステータスを識別します。詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』を参照してください。

機能診断タブのナビゲート

[機能診断] タブには、システムパフォーマンスとアクティビティを定義する設定および機能が表示されます。下表は、これらの設定のリストおよびその説明を示しています。

フォルダ [ページ]	使用可能な機能
機能診断	管理コンソールの [機能診断] セクションには、次の機能エリアがあります。 ❑ **TIBCO WebFOCUS について**　インストールされた TIBCO WebFOCUS のバージョンおよびリリースに関する情報を表示します。 ❑ **Client の確認**　一般的な処理を実行するためのユーザのディレクトリ権限およびステータスが表示されます。 ❑ **HTTP リクエスト情報**　HTTP リクエストヘッダに関する情報を表示します。 ❑ **JVM プロパティ情報**　Java VM 環境に関する情報を表示します。 ❑ **セッションモニタ**　セッションモニタイベント、および詳細トレースへのリンクを表示します。 ❑ **ログファイル**　WebFOCUS ログファイルへのリンクを表示します。 ❑ **アプリケーションログファイル**　アプリケーションユーティリティから生成されたすべてのログファイルへのリンクを表示します。 ❑ **LRU キャッシュ統計**　現在のキャッシュ使用統計を表示します。

WebFOCUS 管理コンソールのメニューバーの使用

管理コンソールのメニューバーは、管理コンソールの各タブの右上に表示されます。メニューバーのコマンドおよび機能は、管理コンソールのすべてのタブで使用することができます。

ライセンスメニューの使用

[ライセンス] メニューを使用して、現在の TIBCO WebFOCUS ライセンスに関する情報、ユーザとグループのライセンスおよびロールの監査、WebFOCUS に同梱されている他社製ソフトウェア製品すべてのライセンスに関する情報にアクセスすることができます。[ライセンス] メニューの各コマンドを使用して、次のことを行えます。

- 現在のライセンスキー、製品エディション、ライセンスキーの有効期限、ユーザライセンス数を表示する。
- 従来のライセンスで製品を使用する場合は、新しいライセンス番号を追加する。

注意: 製品インストールに同梱されている他社製ソフトウエアのライセンス情報を確認するには、WebFOCUS Hub の [ヘルプ] メニューから [ライセンス] オプションを選択します。

Client ライセンス情報の確認

[TIBCO WebFOCUS Client] メニューオプションから、[ライセンス情報] ダイアログボックスが開きます。このダイアログボックスで、現在のライセンスキー、そのキーで使用可能な各製品コンポーネントが識別されます。レガシーライセンスで製品を使用する場合、このダイアログボックスを使用して、現在のライセンスが期限切れになる場合やライセンスを変更する際に、現在のライセンスを新しいライセンスに切り替えることもできます。

	使用可能な機能
ライセンス情報	[ライセンス情報] ダイアログボックスには、次の情報が表示されます。 ❏ **ライセンスキー** 現在使用中のライセンスキーです。次のいずれかの値が格納されます。 ❏ **Golden_Key** デフォルト値です。ゴールデンキーライセンスで製品を使用します。 ❏ **レガシーライセンスキー番号** 内部管理され、製品のインストール時にユーザに割り当てられたライセンスキー番号です。レガシーライセンスでの使用時に表示されます。 ❏ **ライセンスキーの有効期限** 現在のライセンスの有効期限です。次のいずれかの値が格納されます。 ❏ **期限切れなし** このライセンスには有効期限がないことを示します。ゴールデンキーライセンスでの使用時に、この値が表示されます。 ❏ **有効期限** ライセンスキーが期限切れになる日付です。レガシーライセンスでの使用時に、この値が表示されます。 ❏ **注意：** レガシーライセンスでの使用時に、デフォルト設定で、実際の有効期限の 14 日前から、WebFOCUS Client のライセンスキー有効期限についての警告メッセージが表示されます。このメッセージには、期限が切れる日付と、その日付までの残り日数が表示されます。ライセンス有効期限の警告メッセージは、ログイン時に管理者にのみ表示され、WebFOCUS Client インストールディレクトリ下の logs ディレクトリに格納されている event.log ファイルに書き込まれます。

	使用可能な機能
	❑ **ユーザライセンス** 使用可能なユーザライセンスの総数、および各ユーザカテゴリで使用されているライセンス数が表示されます。次のいずれかの値が格納されます。 ❑ **無制限** ユーザ最大数の上限がないことを示します。ゴールデンキーライセンスでの使用時に表示されます、このライセンスでのデフォルト値です。 ❑ **ライセンス数** 使用可能なユーザライセンスの総数、および各ユーザカテゴリで使用されているライセンス数が表示されます。レガシーライセンスでの使用時に表示されます。次のユーザカテゴリが含まれます。 ❑ 総ユーザ数 ❑ BI Portal ユーザ ❑ DESIGNER/InfoAssist ユーザ ❑ **製品コンポーネント** 現在のライセンスで使用可能な製品コンポーネントです。エントリの右側にチェックボックスが表示され、チェックがオンになっている場合、ユーザはその製品コンポーネントを使用する資格があります。 ❑ TIBCO WebFOCUS Client Self Service ❑ TIBCO WebFOCUS Portal ❑ DESIGNER/InfoAssist ❑ InfoAssist Basic ❑ TIBCO WebFOCUS Mobile ❑ Quick Data ❑ ReportCaster ❑ Web サービス ❑ Enterprise Usage Monitor

	使用可能な機能
	*Performance Management Framework - Performance Management Framework (PMF) インストールで構成 [ライセンス情報] ダイアログボックスには、現在所有するライセンスキーで使用可能な製品コンポーネントのみが表示されるため、レガシーライセンスでの使用時には、上記リストの一部の製品コンポーネントがこのダイアログボックスに表示されない場合があります。 ゴールデンキーライセンスでの使用時には、デフォルト設定ですべての製品コンポーネントが選択されます。 ❏ **新規ライセンスキー** このボタンをクリックすると、[ライセンスの更新] ダイアログボックスが開き、新しいライセンスキーとサイトコードを入力することができます。レガシーライセンスでの使用時にのみ表示されます。

参照 Client ライセンスの管理

製品の各種機能へのアクセスおよびユーザライセンス数は、所有するライセンスキーおよびサイトコードに基づいて決定されます。

ゴールデンキーライセンスでの使用時には、ユーザライセンス数が無制限になり、すべての製品コンポーネントがすべてのユーザに使用可能になります。

レガシーライセンスでの使用時には、ユーザ数がユーザライセンス数を超えると、[ユーザライセンス] セクションの [使用中] ユーザ数が赤色になり、ユーザライセンス数を超えていることを示すメッセージが表示されます。このメッセージは、event.log トレースファイルに記録されます。管理コンソールへのアクセス権限を所有しているユーザには、ログイン時にメッセージが表示されます。

次の 3 つのユーザライセンスカテゴリがあります。

❏ **総ユーザ数** WebFOCUS リポジトリ内で定義されているユーザの総数です。

❏ **BI Portal ユーザ** ポータルの使用権限を所有するユーザ数です。

注意

TIBCO WebFOCUS バージョン 8.2 Enterprise Edition では、ReportCaster スケジュールのみの権限または ReportLibrary のみの権限に限定されたユーザの場合、ユーザ数は無制限です。これらのユーザは、[BI Portal ユーザ (PU)] のユーザ数に含まれません。

TIBCO WebFOCUS バージョン 8.2 Application Edition (WebFOCUS バージョンでは廃止) では、ReportCaster 権限のみを所有するユーザが、[BI Portal ユーザ (PU)] のユーザ数に含まれます。

バージョン 8.0 および 8.1 では、ReportCaster スケジュールのみの権限および ReportLibrary のみの権限を所有するユーザは、WF BI Portal ユーザ数に含まれます。追加の WF BI Portal ユーザを許可するために一時的なライセンスキーが必要な場合は、技術サポートに問い合わせてください。バージョン 8.2 では、ReportLibrary のみの権限のユーザ数が修正されています。[Run] 権限はすべての項目タイプに使用されるため、WebFOCUS リポジトリワークスペース (/WFC) フォルダパス内で [Run] 権限を所有するユーザは、BI Portal ユーザ数に含まれます。

- **DESIGNER/InfoAssist ユーザ** ポータルの使用権限および DESIGNER/InfoAssist の使用権限を所有するユーザ数です。

手順 ライセンスキーを構成するには

ゴールデンキーライセンスでの使用時には (デフォルト構成)、製品の各種機能へのアクセスおよび BI Portal ユーザ数は無制限になります。[新規ライセンスキー] ボタンは、[ライセンスマネジメント] ダイアログボックスで使用できなくなり、この手順は不要になります。

レガシーライセンスでの使用時には、製品の各種機能へのアクセスおよび BI Portal ユーザ数は、所有するライセンスキーおよびサイトコードに基づいて決定されます。これらの値は、[ライセンスマネジメント] ダイアログボックスで変更できます。

1. 管理コンソールのメニューバーで [ライセンス] をクリックし、[TIBCO WebFOCUS Client] を選択します。

   [ライセンス情報] ウィンドウが開き、現在のライセンスで使用可能な機能のリストが表示されます。

2. [新規ライセンスキー] をクリックします。
3. 新しいライセンスキーとサイトコードを入力します。
4. [確認] をクリックします。

   [ライセンス情報] ウィンドウに、現在のライセンスキー、新しいライセンスキー、および新しいライセンスキーで提供される機能のリストが表示されます。

5. [保存] をクリックし、新しいライセンスを実装します。

変更を有効にするには、Web アプリケーションを再ロードする必要があります。また、ユーザが新しい機能へのアクセス権限を取得するには、一度ログアウトし、再度ログインする必要があります。

ユーザ監査情報の確認

[ユーザの監査] コマンドを実行すると、リポジトリライセンスの使用状況が、[総ユーザ数]、[BI Portal ユーザ数]、[DESIGNER/InfoAssist ユーザ数] として評価されます。このコマンドを実行すると、ライセンス分析レポートが生成され、ライセンスタイプ別のライセンス総数、ライセンスタイプ別の使用中ライセンス数、グループ別およびユーザ別のライセンス割り当ての分析に関する情報が表示されます。

また、ローカルマシンの WebFOCUS インストールディレクトリからユーザ監査ユーティリティ (license_audit.bat) を実行することもできます。このユーティリティは、次のディレクトリに格納されています。

drive:¥ibi¥WebFOCUS82¥utilities¥mr (Windows)

install_directory/ibi/WebFOCUS82/utilities/mr (UNIX または Linux)

(標準インストールの場合)

drive:¥ibi¥WebFOCUS_WFI¥WebFOCUS¥utilities¥mr (Windows)

install_directory/ibi/WebFOCUS_WFI/WebFOCUS/utilities/mr (UNIX または Linux)

(統合インストールの場合)

ユーティリティからライセンス分析レポートが作成され、auditUserCounts.htm ファイルに転送されます。このファイルは、プログラムと同一のディレクトリに保存されます。

ライセンス分析レポートには、次の情報が表示されます。

ライセンス分析	
キー	現在のライセンスキーを表示します。デフォルト値は、Golden_Key です。

ライセンス分析	
ユーザライセンス	現在のライセンスキーで許可されているユーザライセンスタイプが表示されます。次のタイプがあります。 ❑ 総ユーザ数 ❑ BI Portal ユーザ ❑ DESIGNER/InfoAssist ユーザ
コード	各ユーザライセンスのコードが表示されます (例、総ユーザ数の場合は TU)。
最大	現在のライセンスキーで使用可能なユーザライセンスの最大数が表示されます。
使用中	現在使用中のライセンス数が表示されます。
利用可能	各ライセンスタイプで使用可能なユーザライセンス数が表示されます。
グループ分析	
グループパス	リポジトリに格納されているグループ名が表示されます。以下は、WebFOCUS リポジトリ作成ユーティリティのデフォルト設定で作成されるグループです。 ❑ /Administrators ❑ /Anonymous ❑ /EVERYONE ❑ /Managers ❑ /SelfServiceDevelopers
ライセンスタイプ	各グループのライセンスタイプが表示されます (例、TU)。
ロール	各グループのロールが表示されます (例、SystemFullControl)。
リソース上	各グループのロールの適用先となるリソースへの IBFS パスが表示されます。

ライセンス分析	
以前のタイプ	各グループの従来のライセンスタイプが表示されます。
グループの概要	次の項目の総数が表示されます。 ❏ グループ数 ❏ グループ数 (ライセンスタイプ設定済み) ❏ グループ数 (ライセンスタイプ未設定) ❏ グループ数 (ユーザタイプ変更済み) ❏ グループ数 (ユーザタイプクリア済み) ❏ グループ数 (タイプ未変更)
ユーザ分析	
ユーザ名	リポジトリに格納されているユーザ名が表示されます。以下は、TIBCO WebFOCUS リポジトリ作成ユーティリティのデフォルト設定で作成されるユーザです。 ❏ admin ❏ public ❏ wfdesktop
ライセンスタイプ	各ユーザに割り当てられているライセンスタイプが表示されます (例、TU)。
ライセンス供与グループ数	ユーザがメンバーとして属するグループの総数が表示されます。
ライセンス供与第 1 グループ	ユーザが割り当てられた 1 つ目のグループの IBFS パスが表示されます。
以前のタイプ	ユーザごとに変更または削除されたライセンスタイプが表示されます。

ライセンス分析	
ユーザの概要	次の項目の総数が表示されます。 ❑ ユーザ数 ❑ ユーザ数 (ライセンスタイプ設定済み) ❑ ユーザ数 (ライセンスタイプ未設定) ❑ ユーザ数 (ユーザタイプ変更済み) ❑ ユーザ数 (ユーザタイプクリア済み) ❑ ユーザ数 (タイプ未変更)

手順　ユーザ監査を管理コンソールから実行するには

管理コンソールのメニューバーで [ライセンス] をクリックし、[ユーザの監査] を選択します。

新しいブラウザウィンドウにライセンス分析レポートが表示されます。

手順　ユーザ監査を TIBCO WebFOCUS インストールのローカルディレクトリから実行するには

1. 次のディレクトリへ移動します。

   drive:¥ibi¥WebFOCUS82¥utilities¥mr (Windows)

   install_directory/ibi/WebFOCUS82/utilities/mr (UNIX または Linux)

2. オペレーティングシステムでサポートされるユーザ監査のユーティリティファイルをダブルクリックします。

   license_audit.bat (Windows)

   license_audit.sh (UNIX または Linux)

3. 最初のプロンプトで、有効な管理者 ID を入力し、Enter キーを押します。
4. 次のプロンプトで、管理者 ID に対応するパスワードを入力し、Enter キーを入力します。

   このバッチファイルの実行により、レポートが生成され、次のディレクトリに格納されます。

   drive:¥ibi¥WebFOCUS82¥utilities¥mr¥auditUserCounts.htm (Windows)

install_directory/ibi/WebFOCUS82/utilities/mr/auditUserCounts.htm (UNIX または Linux)

5. auditUserCounts.htm ファイルをダブルクリックして、ライセンス分析レポートを開きます。

キャッシュのクリア

[キャッシュのクリア] コマンドを実行すると、アプリケーションの状態がリフレッシュされます。これにより、保存された変更の中で、動的に適用されていない変更が適用されます。一部の変更は動的に適用されるか、変更を反映させるために管理ユーザによるキャッシュのクリアのみが必要ですが、管理ユーザによる Web アプリケーションの再起動が必要な変更もあります。この操作を行うと、データ値 (DataValues) キャッシュ、メタデータ (MetaData) キャッシュ、サーバ構成 (ServerConfig) キャッシュに格納されたデータ値もすべてクリアされます。

キャッシュのクリアを実行すると、既存のインデックスリーダーおよびインデックスサーチャーを閉じることでアクティブ検索がすべて終了します。また、collections.xml ファイルおよびスタイルシートファイルの値の更新による Magnify 検索インターフェースへの変更はすべて保存されます。ただし、この操作では、アクティブインデックスライターが閉じられることも、既存の検索結果が削除されることもありません。

WebFOCUS 管理コンソールの終了

WebFOCUS ホームページでの作業中に、[閉じる] コマンドを実行すると、管理コンソールが閉じます。 コンソールを閉じた後でも、管理者としてログインした状態は保持されます。

注意：このコマンドは、WebFOCUS Hub から直接コンソールを開いた場合は、管理コンソールのメニューバーに表示されません。サイドナビゲーションウィンドウから別のオプションを選択すると、管理コンソールを閉じることができます。

WebFOCUS 管理コンソールヘルプの起動

[ヘルプ] アイコンをクリックすると、オンラインヘルプファイルが開き、現在表示されているタブ、設定、または機能についてのトピックが表示されます。

環境の構成およびカスタマイズ

[構成] タブを使用して、次の設定を構成します。

- Reporting Server への Client 接続
- アプリケーションの設定
- カスタム設定

- NLS 設定
- 言語の切り替え
- 出力先変更設定
- InfoAssist のプロパティ

TIBCO WebFOCUS Reporting Server の設定

TIBCO WebFOCUS Reporting Server の設定を開くには、[構成] タブをクリックし、[Reporting Server] を展開します。次のことが可能です。

- Reporting Server と通信するための基本的な Client 設定を構成する。
- 代替サーバのマッピングを作成または変更する。
- サーバパフォーマンス統計をモニタし、最適なサーバにリクエストを送信して処理を実行するための Cluster Manager を作成または変更する。
- レガシークラスタ構成を管理する。

参照 Reporting Server ノードのプロパティ

以下は、[基本] ウィンドウで定義される Reporting Server ノードのプロパティに関する説明です。

基本

ノード名
ノード名には、他のノードと重複する名前を使用することはできません。また、48 バイトを超える名前を指定することはできません。Client がこのサーバにアクセスする際に、この名前が使用されます。

ノードの説明
(オプション) ノードの説明です。この説明が [構成] ウィンドウに表示されます。この説明を省略すると、ノード名が使用されます。

ホスト
ホストサーバのホスト名または IP アドレスです。

TCP/IP ポート
TCP リスナのポート番号です。デフォルトのポート番号は 8120 です。

HTTP(S) ポート
HTTP リスナのポート番号です。通常、TCP/IP ポート番号の次のポート番号です。

デフォルトの HTTP ポート番号は 8121 です。

セキュリティ

Reporting Server 接続に適用するセキュリティオプションです。

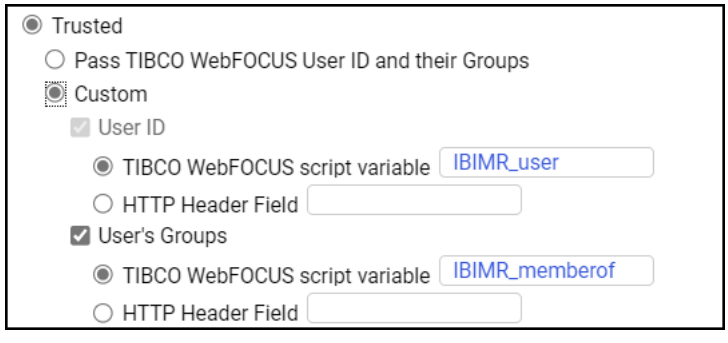
- **認証情報の要求** Client は、[セキュリティ] タブで指定されたユーザ ID とパスワードを使用して Reporting Server との間に明示的な接続を確立します。これがデフォルト値です。
- **HTTP Basic** ユーザ ID とパスワードは、認証ヘッダから抽出されます。 これらの認証情報は、Reporting Server への明示的な接続に使用されます。このオプションは、Web 階層で基本認証を実行する場合にのみ選択します。

  注意：認証ヘッダが有効であるかどうかを確認するには、[機能診断] タブで [HTTP リクエスト情報] を選択します。
- **Kerberos** Client は、ユーザの Kerberos チケットを Reporting Server に渡します。このオプションを使用すると、デスクトップから Client、Client から Reporting Server、Reporting Server からリレーショナルデータベースシステムへのエンドツーエンドのシングルサインオンが可能になります。Kerberos 認証を使用するには、Reporting Server を OPSYS セキュリティモードで実行する必要があります。
- **SAP Ticket** Client は、SAP Enterprise Portal 上で作成されたユーザ MYSAPSSO Cookie を Reporting Server に渡します。Reporting Server は、SAP セキュリティ API を使用して Cookie の有効性を確認します。このオプションを使用すると、SAP Enterprise Portal 上の Open Portal Services を使用する環境で SAP 対応データアダプタを使用するよう Reporting Server が構成されている場合に、Client から Reporting Server へのシングルサインオンが可能になります。
- **サービスアカウント** Reporting Server へのすべての接続に使用するユーザ ID およびパスワードを指定することができます。

  サービスアカウントの認証情報は暗号化され、odin.cfg ファイルの SECURITY キーワードに格納されます。サービスアカウントのユーザ ID およびパスワードを定義すると、この Reporting Server ノードに対して Client が取得するその他すべての認証情報が上書きされ、すべてのユーザが同一の認証情報でこの Reporting Server に接続します。この方法では、BI Portal 展開で Reporting Server 上の特定のリクエストを実行するユーザを識別できないため、この方法を BI Portal 展開で使用することはお勧めしません。
- **Trusted** 未認証リクエストから Reporting Server への接続を信頼済みとして処理することができます。ユーザが事前認証メカニズムまたはログインページ経由で認証された後、それ以降に Reporting Server に送信されるリクエストはすべて信頼済みと見なされます。

このオプションを使用するには、Reporting Server でもトラステッド接続を許可するようセキュリティプロバイダを構成するとともに、未承認クライアントからの接続を拒否するよう制御機能を Reporting Server 側に配置する必要があります。たとえば、Reporting Server の RESTRICT_TO_IP 設定を適用するか、ネットワークファイアウォールを構成して、特定のクライアントのみがサーバに接続できるようにします。

新しい Client 構成を作成する際は、デフォルト設定で [Trusted] オプションが選択され、その下に [TIBCO WebFOCUS ユーザ ID とグループを送信] および [カスタム] オプションが表示されます。[カスタム] オプションを選択すると、画面がリフレッシュされ、[ユーザ ID] および [ユーザのグループ] チェックボックスが表示されます。各チェックボックスの下には、下図のように [TIBCO WebFOCUS スクリプト変数] および [HTTP ヘッダフィールド] オプションが表示されます。



[ユーザ ID] チェックボックス下では、デフォルト設定で [TIBCO WebFOCUS スクリプト変数] オプションに IBIMR_user パラメータが表示されます。[ユーザのグループ] チェックボックス下では、デフォルト設定で [TIBCO WebFOCUS スクリプト変数] オプションに IBIMR_memberof パラメータが表示されます。[TIBCO WebFOCUS スクリプト変数] オプションのデフォルト値を上書きすることも、[HTTP ヘッダフィールド] オプションにユーザ独自の値を入力することもできます。

注意：Client で Reporting Server へのトラステッド接続を構成した場合は、Reporting Server でもトラステッド接続を受容するよう構成する必要があります。

詳細

以下は、[詳細] ウィンドウで定義される Reporting Server ノードのプロパティに関する説明です。

サービス名

Reporting Server ノードの説明です。この説明は、エンドユーザに表示されます。

HTTPS を使用する

Client と Reporting Server の HTTP リスナの間で、暗号化された通信を行うことができます。デフォルト値は off (チェックオフ) です。

Reporting Server HTTP リスナが SSL を使用するよう構成されている場合は、このオプションを選択する必要があります。自己署名入り証明書を使用して Reporting Server との HTTPS 通信を有効にする場合は、Client がインストールされている Java 環境で証明書を構成する必要があります。これにより、Reporting Server と管理コンソール間での HTTPS 通信が有効になります。

圧縮

データ圧縮を有効にします。デフォルト設定では、データ圧縮は無効になっています。

暗号化

データの暗号化機能を有効にし、対称暗号方式を使用するよう設定します。

ドロップダウンリストから、次のオプションのいずれかを選択します。

- **0** オフ。これがデフォルト値です。
- **AES** 高度暗号化標準。AES を選択する場合のフォーマットは次のとおりです。

  `CIPHER(x)(-MODE)`

  説明

  `CIPHER`

  AES128、AES192、AES256 です。

  `x`

  1024 ビットの RSA キー長を定義します (オプション)。この値を指定しない場合、RSA キー長は 512 ビットです。

  `CBC`

  CBC (Cipher Block Chaining) モードを使用することを指定します (オプション)。特定のモードを指定しない場合、ECB (Electronic Code Book) モードが使用されます。

  たとえば、AES256x-CBC は、1024 ビット RSA キーで、CBC モードの AES256 暗号化を表します。AES128 は、512 ビット RSA キーで、ECB モードの AES128 暗号化を表します。

接続制限

Client が待機中の接続を継続する時間 (秒数) を指定します。設定可能な値には、0 (待機なし) と -1 (無期限待機) があります。デフォルト値は -1 です。

最大待ち時間

タイムアウトになるまで Client が待機する時間 (秒数) を指定します。必要に応じて、先頭とそれ以外にそれぞれ異なる待機時間を指定することができます。数字を 1 つ指定すると、その待機時間がすべての行で有効になります。2 つの数字をカンマ区切りで指定した場合、1 つ目の数字が先頭の待機時間を示し、2 つ目の数字が先頭以外の待機時間を示します。デフォルト値は -1 (無期限待機) です。

セキュリティオブジェクト

管理者はあらゆるセキュリティオプションに対して、1 つ以上の HTTP ヘッダ名と Cookie 名のいずれか、または両方を次のように指定できます。

- **Cookie** HTTP Cookie 名それぞれをカンマ (,) で区切って指定します。以下はその例です。

  ```
  cookie_name1, cookie_name2
  ```

- **ヘッダ** HTTP ヘッダ名それぞれをカンマ (,) で区切って指定します。以下はその例です。

  ```
  header_name1, header_name2
  ```

注意

- HTTP Cookie 名およびヘッダ名には、カンマ (,) およびコロン (:) を含めることはできません。これらは予約済み区切り文字です。
- REMOTE_USER は特別なタイプの HTTP ヘッダ変数で、このヘッダ変数の値は Reporting Server に送信されません。そのため、有効な HTTP ヘッダ値ではありません。代わりに、WF_REMOTE_USER 変数を指定します。

Cluster Manager 構成の基本プロパティ

ノード名

サーバのホスト名または IP アドレスです。

ノードの説明

オプションノードの説明です。この説明が [構成] ウィンドウに表示されます。この説明を省略すると、ノード名が使用されます。

リモート CLM ホスト

Cluster Manager のホスト名または IP アドレスです。リモート Cluster Manager (CLM) は、このホストで受信待機します。複数のアドレスを指定した場合は、CLM への接続に成功するまで、アドレスのいずれかがランダムに選択されます。この設定で定義する IP アドレスの個数は、[リモート CLM ポート] で定義するポート番号の個数に一致させる必要があります。複数のホスト名または IP アドレスはカンマ (,) で区切ります。

リモート CLM ポート

Cluster Manager サーバが受信待機するポートの UDP 番号です。デフォルトのポート番号は 8200 です。複数のポート番号を指定する場合は、ポート番号の個数を [リモート CLM ホスト] で定義した IP アドレスの個数と一致させる必要があります。複数のホスト名または IP アドレスはカンマ (,) で区切ります。

セキュリティ

Reporting Server クラスタに適用するセキュリティオプションです。

- **認証情報の要求** Client は、[セキュリティ] タブで指定されたユーザ ID とパスワードを使用して Cluster Manager との間に明示的な接続を確立します。これがデフォルト値です。
- **HTTP Basic** ユーザ ID とパスワードは、認証ヘッダから抽出されます。 これらの認証情報は、Cluster Manager への明示的な接続に使用されます。このオプションは、Web 階層で基本認証を実行する場合にのみ選択します。

  注意：認証ヘッダが有効であるかどうかを確認するには、[機能診断] タブで [HTTP リクエスト情報] を選択します。
- **Kerberos** Client は、ユーザの Kerberos チケットを Cluster Manager に渡します。このオプションを使用すると、デスクトップから Client、Client から Cluster Manager、Cluster Manager からリレーショナルデータベースシステムへのエンドツーエンドのシングルサインオンが可能になります。Kerberos 認証を使用するには、Cluster Manager を OPSYS セキュリティモードで実行する必要があります。
- **SAP Ticket** Client は、SAP Enterprise Portal 上で作成されたユーザ MYSAPSSO Cookie を Cluster Manager に渡します。Cluster Manager は、SAP セキュリティ API を使用して Cookie の有効性を確認します。このオプションを使用すると、SAP Enterprise Portal 上の Open Portal Services を使用する環境で SAP 対応データアダプタを使用するよう Cluster Manager が構成されている場合に、Client から Cluster Manager へのシングルサインオンが可能になります。

- **サービスアカウント** Cluster Manager へのすべての接続に使用するユーザ ID およびパスワードを指定することができます。

  サービスアカウントの認証情報は暗号化され、odin.cfg ファイルの SECURITY キーワードに格納されます。サービスアカウントのユーザ ID およびパスワードを定義すると、この Cluster Manager ノードに対して取得されるその他すべての認証情報が上書きされ、すべてのユーザが同一の認証情報でこの Cluster Manager に接続します。この方法では、BI Portal 展開で Cluster Manager 上の特定のリクエストを実行するユーザを識別できないため、この方法を BI Portal 展開で使用することはお勧めしません。

- **Trusted** 単一ユーザ ID のみによる Cluster Manager への接続を可能にします。このオプションは、ユーザのパスワードを指定しない場合に役立ちます。制御機能を Cluster Manager に設定して、未承認クライアントからの接続を拒否する必要があります。たとえば、Cluster Manager の RESTRICT_TO_IP 設定を適用するか、ネットワークファイアウォールを構成すると、特定のクライアントのみが Cluster Manager に接続することができます。

  注意：Client で Reporting Server へのトラステッド接続を構成した場合は、Cluster Manager でもトラステッド接続を受容するよう構成する必要があります。

Cluster Manager 構成の詳細プロパティ

HTTPS を使用する

Client と HTTP リスナの間で、暗号化された通信を行うことができます。

デフォルト値は OFF です。

Cluster Manager HTTP リスナが SSL を使用するよう構成されている場合は、このオプションを選択する必要があります。自己署名入り証明書を使用して Cluster Manager との HTTPS 通信を有効にする場合は、WebFOCUS Client がインストールされている Java 環境で証明書を構成する必要があります。これにより、Cluster Manager と管理コンソール間での HTTPS 通信が有効になります。

圧縮

データ圧縮を有効にします。デフォルト設定では、データ圧縮は無効になっています。

暗号化

データの暗号化機能を有効にし、対称暗号方式を使用するよう設定します。

ドロップダウンリストから、次のオプションのいずれかを選択します。

- **0** オフ。これがデフォルト値です。
- **AES** 高度暗号化標準。AES を選択する場合のフォーマットは次のとおりです。

```
CIPHER(x)(-MODE)
```

説明

`CIPHER`

AES128、AES192、AES256 です。

`x`

1024 ビットの RSA キー長を定義します (オプション)。この値を指定しない場合、RSA キー長は 512 ビットです。

`CBC`

CBC (Cipher Block Chaining) モードを使用することを指定します (オプション)。特定のモードを指定しない場合、ECB (Electronic Code Book) モードが使用されます。

たとえば、AES256x-CBC は、1024 ビット RSA キーで、CBC モードの AES256 暗号化を表します。AES128 は、512 ビット RSA キーで、ECB モードの AES128 暗号化を表します。

- **IBCRYPT** ユーザ定義の IBCRYPT DLL がロードされます。

接続制限

Client が待機中の接続を継続する時間 (秒数) を指定します。クラスタ展開において、フェールオーバーレスポンスの大幅な遅延が発生することを防止する場合に役立ちます。設定可能な値には、0 (待機なし) と -1 (無期限待機) があります。デフォルト値は -1 です。

最大待ち時間

タイムアウトになるまで Client が待機する時間 (秒数) を指定します。必要に応じて、先頭とそれ以外にそれぞれ異なる待機時間を指定することができます。数字を 1 つ指定すると、その待機時間がすべての行で有効になります。2 つの数字をカンマ区切りで指定した場合、1 つ目の数字が先頭の待機時間を示し、2 つ目の数字が先頭以外の待機時間を示します。デフォルト値は -1 (無期限待機) です。

セキュリティオブジェクト

管理者は、あらゆるセキュリティオプションに対して、1 つ以上の HTTP ヘッダ名または Cookie 名を次のように指定できます。

- **Cookie** HTTP Cookie 名それぞれをカンマ (,) で区切って指定します。以下はその例です。

  cookie_name1, cookie_name2

- **ヘッダ** HTTP ヘッダ名それぞれをカンマ (,) で区切って指定します。以下はその例です。

header_name1, header_name2

注意

- HTTP Cookie 名およびヘッダ名には、カンマ (,) およびコロン (:) を含めることはできません。これらは予約済み区切り文字です。
- REMOTE_USER は特別なタイプの HTTP ヘッダ変数で、このヘッダ変数の値は Reporting Server に送信されません。そのため、有効な HTTP ヘッダ値ではありません。代わりに、WF_REMOTE_USER 変数を指定します。

WebFOCUS Reporting Server の構成

Reporting Server 接続ノードには、Client が Reporting Server に接続してサーバを使用するための情報がすべて格納されます。1 つの Reporting Server の接続ノードからは、1 つのサーバにのみアクセスできます。1 つの Cluster Manager ノードからは、複数のサーバにアクセスすることができます。このセクションで構成に変更を加えた場合、その変更は、Windows では *drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc、UNIX または Linux では *install_directory*/ibi/WebFOCUS82/client/wfc/etc ディレクトリ内の odin.cfg ファイルに書き込まれます。

手順

WebFOCUS 管理コンソールから WebFOCUS Reporting Server コンソールを起動するには

Reporting Server コンソールを使用して、サーバ環境の構成をグローバルに変更することができます。

1. 管理コンソールで、[構成] タブをクリックします。[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。

   既存の Reporting Server のリストが表示されます。

2. Reporting Server のいずれかを右クリックし、[Reporting Server コンソール] を選択します。

   ログインを要求された場合は、Reporting Server 管理者の認証情報を入力します。

   新しいウィンドウに Reporting Server コンソールが開きます。

Reporting Server コンソールについての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照するか、[ヘルプ] ボタンをクリックします。

手順　サーバ接続を追加するには

1. 管理コンソールで [構成] タブをクリックし、[Reporting Server] フォルダを展開します。
2. [サーバ接続] フォルダを右クリックし、[新規作成] を選択します。

   [Client の構成] ウィンドウが開きます。
3. [Client の構成] ウィンドウで、[ノード名]、[ホスト]、[TCP/IP ポート] を入力します。必要に応じて、[ノードの説明]、[HTTP(S) ポート] を指定することもできます。

   注意：ノード名には、他のノードと重複する名前を使用することはできません。また、48 バイトを超える名前を指定することはできません。Client がこのサーバにアクセスする際に、この名前が使用されます。
4. Reporting Server への接続時に使用するセキュリティのタイプを選択します。
   - [認証情報の要求] または [HTTP Basic] を選択した場合は、手順 8 へ進みます。

     注意：HTTP Basic 認証を使用する場合は、[機能診断] タブの [HTTP リクエスト情報] を選択することで、認証ヘッダを確認することができます。
   - [Kerberos] または [SAP Ticket] を選択した場合は、手順 8 へ進みます。

     注意：追加の設定要件についての詳細は、259 ページの 「 シングルサインオンを提供する Kerberos の構成 」 を参照してください。
   - [サービスアカウント] を選択した場合は、手順 5 へ進みます。
   - [Trusted] を選択した場合は、手順 6 へ進みます。

     デフォルト設定では、[Trusted] が選択されています。Reporting Server への接続にはこの方法をお勧めします。
5. [サービスアカウント] を選択した場合は、サービスアカウント ID およびパスワードを入力し、手順 8 へ進みます。
6. [Trusted] を選択した場合は、Client と Reporting Server 間のトラステッド接続の動作を構成します。
   - IBIMR_user および IBIMR_group スクリプト変数を使用して WebFOCUS から Reporting Server にユーザ ID とグループ情報を送信する場合は、手順 8 へ進みます。これがデフォルトの動作です。
   - ユーザ ID のみを送信する場合、ユーザ ID とグループ情報のいずれかまたは両方を別の変数名で送信する場合、またはスクリプト変数の代わりに HTTP ヘッダを使用する場合は、[カスタム] ラジオボタンを選択し、手順 7 へ進みます。

7. [Trusted] - [カスタム] を選択した場合は、Reporting Server に送信する情報、スクリプト変数、HTTP ヘッダをカスタマイズします。

   a. [ユーザ ID] は事前に選択されています。ユーザ ID の送信方法に応じて、[TIBCO WebFOCUS スクリプト変数] または [HTTP ヘッダフィールド] を選択します。デフォルトのスクリプト変数 (IBIMR_User) を受容するか、別のスクリプト変数または HTTP ヘッダフィールドを入力します。

   b. グループ情報を Reporting Server に送信する場合は、[ユーザのグループ] を選択し、グループ情報の送信方法に応じて、[TIBCO WebFOCUS スクリプト変数] または [HTTP ヘッダフィールド] を選択します。デフォルトのスクリプト変数 (IBIMR_memberof) を受容するか、別のスクリプト変数または HTTP ヘッダフィールドを入力します。

   TIBCO WebFOCUS スクリプト変数および HTTP ヘッダについての詳細は、713 ページの「 TIBCO WebFOCUS 変数の操作 」を参照してください。Reporting Server でのトラステッド接続の構成についての詳細は、51 ページの 「 トラステッド接続の構成 」 を参照してください。

8. 必要に応じて [詳細] セクションを展開し、[サービス名]、[HTTPS を使用する]、[圧縮]、[暗号化]、[接続制限]、[最大待ち時間]、[セキュリティオブジェクト] のプロパティをカスタマイズします。これらのオプションをブランクにした場合、デフォルトのプロパティが使用されます。

   注意：Client で Reporting Server へのトラステッド接続を構成した場合は、Reporting Server でもトラステッド接続を受容するよう構成する必要があります。

   [詳細] 設定についての詳細は、89 ページの 「 Reporting Server ノードのプロパティ 」 を参照してください。

9. [保存] をクリックします。

   新しい Reporting Server 接続ノードが、ツリーの [サーバ接続] フォルダ下に表示されます。

手順　TIBCO WebFOCUS 接続を変更するには

1. 管理コンソールで [構成] タブをクリックし、[Reporting Server] フォルダを展開します。
2. 変更するサーバ接続をクリックします。

   [Client の構成] ウィンドウに、接続のプロパティが表示されます。

3. 変更後、[保存] をクリックします。

手順　Reporting Server との暗号化通信を構成するには

この手順は、WFServlet 実装が正しくインストールされ、構成が完了していることが前提になります。

1. Sun JVM で 128 ビットを超える暗号化キーを使用する場合、Java 暗号化拡張機能 (JCE) をインストールする必要があります。JCE は、Oracle のダウンロードサイトから入手することができます。

   注意：JCE は、アプリケーションが使用する JVM ディレクトリにインストールする必要があります。詳細は、JCE のマニュアルを参照してください。

2. .war ファイルのパスを指定する必要がある場合は、webfocus.war ファイルを再展開します。そうでない場合は、WebFOCUS アプリケーションディレクトリを指定します。
3. 管理コンソールで、[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。
4. 暗号化を構成する Reporting Server ノード (例、EDASERVE) を選択します。

   [Client の構成] ウィンドウが開きます。

5. [詳細] の矢印をクリックして [詳細] セクションを開きます。
6. [暗号化] リストから、使用する暗号化方式を選択します。

   注意：AES 暗号化のいずれかを使用すると、クライアントは新しい RSA キーの組 (指定した長さのパブリックキーおよびプライベートキー) をランダムに生成し、パブリックキーをサーバに送信します。サーバは、パブリックキーを受信すると、シークレットキーをランダムに生成します。シークレットキーの長さは、選択した暗号長によって異なります。シークレットキーは、パブリック RSA キーで暗号化され、クライアントに返送されます。クライアントは、それをプライベート RSA キーで復号化します。キーの交換後、クライアントとサーバの両方は同一のシークレットキーを共有し、そのキーを使用して、両者間のすべての通信の暗号化および復号化を行います。

7. [保存] をクリックします。

手順　デフォルトサーバノードを設定するには

[構成] タブでデフォルトサーバノードを選択すると、そのノードが webfocus.cfg ファイル内に IBI_REPORT_SERVER 値として設定されます。ただし、サイトプロファイル、ユニバーサルプロファイル、リクエスト URL のいずれかで別のデフォルトサーバノードが指定されている場合は、その値が優先されます。これらのプロファイルおよびリクエスト URL では、その目的で IBIC_server 設定が使用されます。

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。
2. Reporting Server ノードを右クリックし、[デフォルトとして設定] を選択します。

   サーバアイコンに緑色のチェックマークが表示され、そのサーバがデフォルトノードであることが示されます。

手順　サーバ接続をテストするには

1. 管理コンソールの [構成] タブで [Reporting Servers]、[サーバ接続] を順に展開します。
2. テストする接続を右クリックし、[テスト] を選択します。
   - ❏ サーバ上でテーブルクエリをテストするには、[TABLE リクエスト] を選択します。
   - ❏ サーバ上でグラフクエリをテストするには、[GRAPH リクエスト] を選択します。
   - ❏ サーバ上でストアドプロシジャをテストするには、[ストアドプロシジャ] を選択します。
3. テストページで [実行] をクリックします。
4. [有効な Reporting Server ログイン情報を入力してください] ページが開いた場合は、ユーザ ID とパスワードを入力し、[ログイン] をクリックします。
5. テスト結果を確認します。

   Reporting Server エラーメッセージが表示された場合、サーバ接続に失敗しています。

   テスト結果を表示するページが開いた場合は、サーバ接続は成功しています。
6. テスト結果を確認後、テスト結果のページを閉じ、[キャンセル] をクリックします。

Client のリポジトリへの再接続

ネットワーク、オペレーティングシステム、リレーショナルデータベースシステム、または Application Server で、Client のリポジトリからの接続が一時的に切断された場合、Client は、切断の問題が解決され次第自動的にリポジトリに再接続します。Client とリポジトリとの接続を再度確立するために、Application Server を停止、再起動する必要はありません。

接続が中断された際に、Client セッションにログインした状態のままにできる場合は、接続が復元され次第自動的にリポジトリに再接続されます。中断によって強制的にログアウトされた場合は、再度ログインすると自動的にリポジトリに再接続されます。接続が復元されると、中断された時点から作業を再開することができます。

Client とリポジトリ間の接続の中断および復元のイベント記録は、システムログに書き込まれます

代替サーバマッピング

BI Portal のディファード機能で使用するための代替サーバノードを構成することができます。

ディファードリクエストの処理は、即時実行用の Reporting Server (以下、即時実行用サーバ) を使用するか、ディファードリクエストのみを実行する代替のディファードサーバ (以下、ディファードサーバ) を使用するかのいずれかの方法で行います。ディファードサーバのリソースは、即時実行用サーバから独立して管理されます。ディファードサーバは、即時実行用サーバと同様に、アプリケーション、データソース、マスターファイルにアクセスできること、および同一の環境 (例、UNIX) で実行できることが必要になります。

ディファードリクエストを処理する代替サーバまたはサービスを設定後、ディファードサーバマッピングを設定することで、WebFOCUS Client がそのサーバにリクエストを送信するよう構成します。詳細は、使用するプラットフォームの『TIBCO WebFOCUS インストールガイド』を参照してください。

手順　代替サーバマッピングを追加するには

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダを展開します。
2. [代替サーバマッピング] フォルダを右クリックし、[新規作成] を選択します。

   [代替サーバマッピング] ウィンドウが開きます。
3. [サーバ] リストからメインサーバを選択します。
4. [代替サーバ] リストから代替サーバを選択します。
5. [保存] をクリックします。
6. 「保存しました」というメッセージで [OK] をクリックします。

手順　代替サーバマッピングを変更するには

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダ、[代替サーバマッピング] フォルダを順に展開します。
2. 変更するサーバマッピングのノードをクリックします。

   [Client の構成] ウィンドウに、接続のプロパティが表示されます。
3. 変更後、[保存] をクリックします。

   注意：メインサーバの値を変更すると、代替サーバに割り当てられている値が自動的にクリアされます。そのため、メインサーバ設定の値を変更した場合は、代替サーバも選択する必要があります。
4. 「保存しました」というメッセージで [OK] をクリックします。

手順　ディファードサーバノードを即時実行用サーバへマッピングするには

管理コンソールを使用して、ディファードサーバ用のノードを追加します。この方法は、ディファード以外のサーバにノードを追加する場合と同一です。続いて、次の手順に従って即時実行用サーバノードにディファードサーバをマッピングします。

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダを展開し、[代替サーバマッピング] を右クリックします。
2. [新規作成] をクリックして、新しいマッピングを作成します。

   [代替サーバマッピング] ウィンドウが開き、altdnode.wfs ファイルを編集することができます。
3. [サーバ] リストに利用可能な Reporting Server がすべて表示されます。このリストから即時実行用サーバ名を選択します。
4. [代替サーバ] リストに利用可能な Reporting Server がすべて表示されます (上記で指定した即時実行用サーバを除く)。このリストからディファードサーバ名を選択します。
5. [保存] をクリックします。

注意：上記の手順を繰り返して、複数の即時実行用サーバを同一のディファードサーバにマッピングすることができます。

クラスタサーバの管理

複数のサーバをクラスタ化すると、利用可能なサーバ群の中から最適なサーバにリクエストが自動的に送信されます。

Cluster Manager (CLM) を使用して、複数の Reporting Server が必要に応じて自動的に開始または停止されるクラスタを定義することができます。また、Cluster Manager では、応答時間や送信方法など、クラスタのプロパティを構成することもできます。構成が完了すると、クラスタのパフォーマンスがモニタされ、リクエストの平均応答時間、接続失敗数やエラー数、分単位のリクエスト送信数などの統計が提供されます。

詳細は、89 ページの 「 Reporting Server ノードのプロパティ 」 を参照してください。

手順　Cluster Manager ノードを追加するには

次の手順では、Cluster Manager を使用して単一ノードに複数サーバのクラスタを作成する方法について説明します。

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダを展開します。
2. [Cluster Manager] フォルダを右クリックし、[新規作成] を選択します。

   [Cluster Manager の構成] ウィンドウが開きます。
3. [Cluster Manager の構成] ウィンドウで、[ノード名]、[リモート CLM ホスト]、[リモート CLM ポート] を入力します。必要に応じて、[ノードの説明] を指定することもできます。

   デフォルトのリモート CLM ポート番号は 8120 です。

   注意：管理コンソールの Cluster Manager 構成で指定するノード名は、Reporting Server の Cluster Manager で指定するクラスタ名に一致させる必要があります。
4. この Cluster Manager への接続時に使用するセキュリティのタイプを選択します。

   - [認証情報の要求]、[HTTP Basic]、[kerberos]、[SAP Ticket] のいずれかを選択した場合は、手順 7 へ進みます。
   - [サービスアカウント] を選択した場合は、手順 5 へ進みます。
   - [Trusted] を選択した場合は、手順 6 へ進みます。

   注意

   - HTTP Basic 認証を使用する場合は、[機能診断] タブの [HTTP リクエスト情報] を選択することで、認証ヘッダを確認することができます。
   - Kerberos 認証を使用する場合、追加の設定要件についての詳細は、259 ページの「 シングルサインオンを提供する Kerberos の構成 」 を参照してください。
5. [サービスアカウント] を選択した場合は、[ユーザ ID] および [パスワード] を入力します。手順 7 へ進みます。

6. [Trusted] (デフォルト設定) を選択した場合は、IBIMR_user および IBIMR_group スクリプト変数を使用して、Client から Reporting Server にユーザ ID とグループ情報が送信されます。この動作をカスタマイズするには、別の変数名を使用するか、スクリプト変数の代わりに HTTP ヘッダを使用するか、またはグループ情報を送信しないよう設定します。

   a. デフォルト動作を有効にする場合は、[TIBCO WebFOCUS ユーザ ID とグループを送信] を選択し、手順 7 へ進みます。

   b. TIBCO WebFOCUS スクリプト変数または HTTP ヘッダを使用してユーザ情報またはグループ情報を送信する場合は、[詳細] を選択します。

   c. ユーザ情報は常に送信されるため、[ユーザ ID] は事前に選択されています。ユーザ ID の送信方法に応じて、[TIBCO WebFOCUS スクリプト変数] または [HTTP ヘッダフィールド] を選択します。デフォルトのスクリプト変数 (IBIMR_User) を受容するか、別のスクリプト変数または HTTP ヘッダフィールドを入力します。

   d. グループ情報を Reporting Server に送信する場合は、[ユーザのグループ] を選択し、グループ情報の送信方法に応じて、[TIBCO WebFOCUS スクリプト変数] または [HTTP ヘッダフィールド] を選択します。デフォルトのスクリプト変数 (IBIMR_memberof) を受容するか、別のスクリプト変数または HTTP ヘッダフィールドを入力します。

   注意： Reporting Server でトラステッド接続を受容するようセキュリティプロバイダを構成する必要があります。

   TIBCO WebFOCUS スクリプト変数および HTTP ヘッダについての詳細は、713 ページの「 TIBCO WebFOCUS 変数の操作 」を参照してください。Reporting Server でのトラステッド接続の構成についての詳細は、51 ページの 「 トラステッド接続の構成 」 を参照してください。

7. デフォルトのサービス名、SSL 使用、圧縮、暗号化、接続制限、待機時間を使用し、Cookie およびヘッダを使用しない場合は、手順 8 へ進みます。これらのプロパティをカスタマイズするには、[詳細] セクションを展開し、変更するプロパティのテキストボックスに値を入力します。

8. [保存] をクリックします。

手順　Cluster Manager ノードを変更するには

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダ、[Cluster Manager] フォルダを順に展開します。

2. 編集するノードを右クリックし、[編集] を選択します。

   [Cluster Manager の構成] ウィンドウに、ノードのプロパティが表示されます。

3. 変更後、[保存] をクリックします。

レガシークラスタ構成の管理

[レガシークラスタの構成] ウィンドウでは、以前のサーバのクラスタ実装が引き続きサポートされます。

手順　レガシークラスタを構成するには

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダを展開します。
2. [レガシークラスタ] フォルダを右クリックし、[新規作成] を選択します。

   [レガシークラスタの構成] ウィンドウが開きます。
3. [ノード名] を入力し、必要に応じて [ノードの説明] を入力します。
4. 次の手順に従って、クラスタに含めるサーバを選択します。
   - ❏ [利用可能] リストでサーバを選択し、右矢印をクリックします。
   - ❏ 隣接しない複数のサーバを選択するには、Ctrl キーを押しながらサーバを順に選択し、右矢印をクリックします。
   - ❏ 隣接する複数のサーバを選択するには、最初のサーバを選択し、Shift キーを押しながら最後のサーバを選択した後、右矢印をクリックします。
5. [保存] をクリックします。

Client プロファイルの使用

Client 変数は Reporting Server に送信されないため、これらの変数は Reporting Server プロファイル (edasprof.prf、ユーザプロファイル、グループプロファイル) のいずれにも直接追加することはできません。ただし、サイトプロファイルまたはユニバーサルプロファイルでプロシジャを指定することにより、Client 変数を使用することができます。サイトプロファイルおよびユニバーサルプロファイルは、Reporting Server プロファイルの処理後、レポートリクエストの前に実行されます。サイトプロファイルは Client から実行され、ユニバーサルプロファイルは Client と ReportCaster Distribution Server の両方から実行されます。

サイトプロファイルおよびユニバーサルプロファイルは、webfocus.cfg または site.wfs ファイルに直接追加することもできます。

Client サイトプロファイル

サイトプロファイルは、Client から Reporting Server に送信され、すべての Reporting Server プロファイルの実行直後に Reporting Server 上で実行されます。サイトプロファイルは、Reporting Server プロファイルの設定を上書きし、他のプロファイルで設定された変数値を利用することができます。これにより、(pass) 構文で Client からエクスポートされた変数が Reporting Server で使用可能になります。

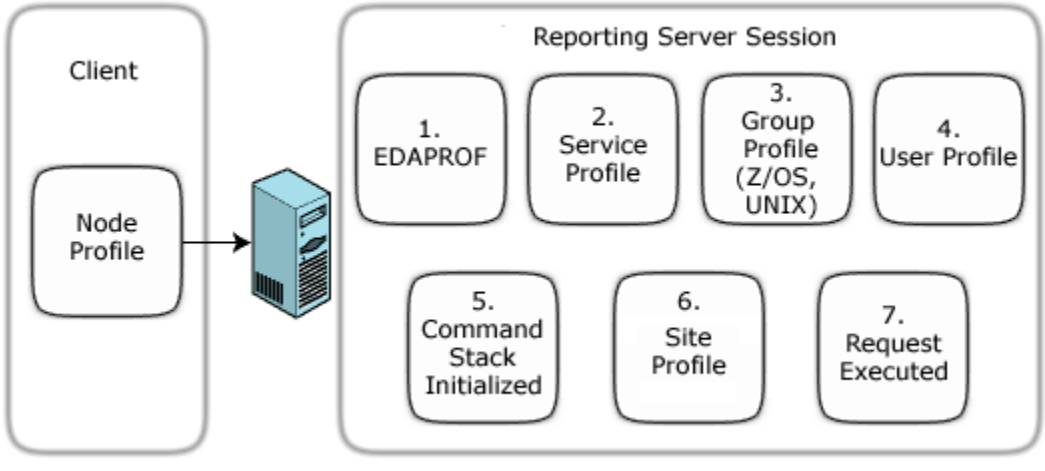
変数の使用についての詳細は、713 ページの 「 TIBCO WebFOCUS 変数の操作 」 を参照してください。Reporting Server プロファイルについての詳細は、58 ページの「 TIBCO WebFOCUS Reporting Server プロファイル 」 を参照してください。

サイトユーザは、次の場合にサイトプロファイルを使用することができます。

- Client が送信した変数に基づいて一連のデータソース接続を確立する。
- Reporting Server のカスタムセキュリティプロシジャで Client 変数 (例、&REMOTE_ADDR、&IBIMR_user) を使用する。これにより、続いて実行するレポート処理に影響する変数をほかにも設定することができます。これは、アプリケーションベースで行うセキュリティの例です。

注意 : サイトプロファイルは、プロシジャが Client によって実行される場合にのみ処理されます。プロシジャが ReportCaster Distribution Server によって実行される際に処理するコマンドを含めるには、ユニバーサルプロファイルを使用します。

下図は、サイトプロファイルの処理手順を示しています。各ファイルの番号は、それぞれのファイルの処理順序を表しています。



手順　サイトプロファイルを作成するには

1. 管理コンソールの [構成] タブで、[アプリケーションの設定] フォルダ下の [Client 設定] をクリックします。
2. [サイトプロファイル] (IBI_SITE_PROFILE) テキストボックスに、実行するプロシジャの名前を入力します。

   [サイトプロファイル] (IBI_SITE_PROFILE) テキストボックスでは、次の構文を使用します。

   ```
   _site_profile=command
   ```

   説明

   `command`
   任意の有効な Reporting Server 構文です。

上記の手順を完了すると、プロファイルプロシジャが自動的に実行されます。Reporting Server を再起動する必要はありません。

ユニバーサルプロファイル

ユニバーサルプロファイルは、Client と ReportCaster Distribution Server の両方から Reporting Server に送信され、Reporting Server 上で実行されます。このプロファイルは、すべての Reporting Server プロファイルの直後に実行されます。

ユニバーサルプロファイルは、サイトプロファイルとは異なり、ReportCaster でのプロシジャの実行時にも処理されます。そのため、ユニバーサルプロファイルには、Client でのみ実行されるロジックやコンストラクトを含めないようにする必要があります。たとえば、HTTP ヘッダ変数は、WebFOCUS Client では使用できますが、ReportCaster Distribution Server では使用できないため、HTTP ヘッダ変数をユニバーサルプロファイルに追加することはできません。

手順　ユニバーサルプロファイルを作成するには

1. 管理コンソールの [構成] タブで、[アプリケーションの設定] フォルダ下の [Client 設定] をクリックします。
2. [Client 設定] で、[ユニバーサルプロファイル] (IBI_UNIVERSAL_PROFILE) テキストボックスに、実行するプロシジャを入力します。

   ユニバーサルプロファイル (IBI_UNIVERSAL_PROFILE) パラメータには、次の構文が使用されます。

   ```
   IBI_UNIVERSAL_PROFILE=command
   ```

説明

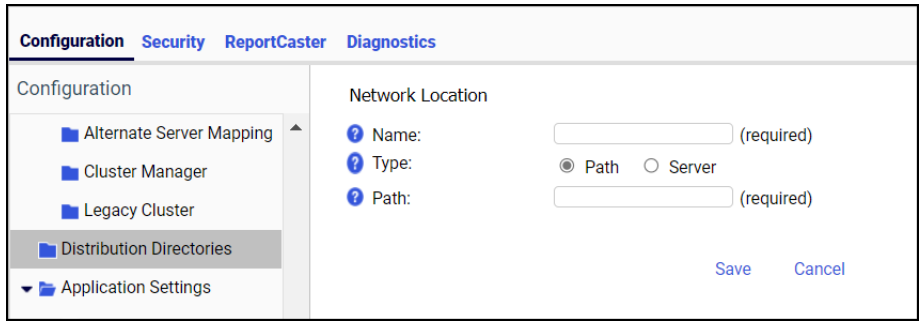
`command`

任意の有効な Reporting Server 構文です。ユニバーサルプロファイルは、Client と Reporting Server Distribution Server の両方によって実行されます。この点がサイトプロファイルと異なります。サイトプロファイルは、Client リクエストによってのみ実行されます。

上記の手順が完了すると、プロファイルプロシジャが自動的に実行されます。Reporting Server を再起動する必要はありません。

配信ディレクトリの管理

[配信ディレクトリ] フォルダには、ReportCaster でのスケジュール済みレポートの配信をサポートする配信ディレクトリノードの構成が格納されます。配信ディレクトリノードは、スケジュール済みレポートの配信から出力を収集する IBFS FILE サブシステム内にフォルダを指定し、下図のように ReportCaster Distribution Server にアクセス可能な既存のファイルシステムディレクトリにマッピングされます。



[配信方法] として [リポジトリ] を使用する場合、ReportCaster Distribution Server は、スケジュール済みのレポート出力を IBFS FILE サブシステムフォルダおよび関連するネットワーク上のディレクトリ、または FTP サーバのディレクトリに送信します。これにより、この出力がその他のツールまたはアプリケーションで使用可能になるため、その他のツールまたは指定されたネットワークまたは FTP サーバのディレクトリから、この出力を取得することが可能になります。

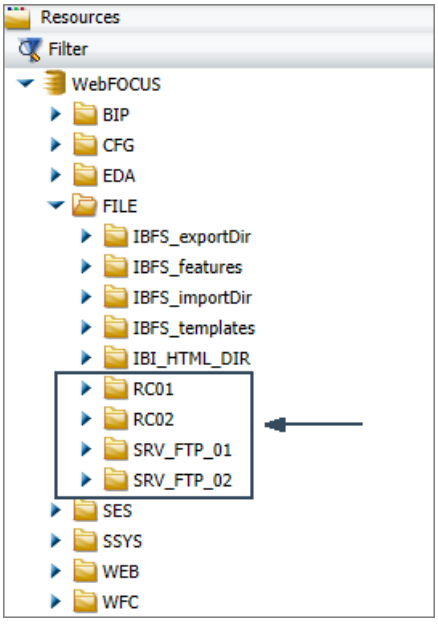
配信ディレクトリは IBFS FILE システム内のフォルダであるため、配信ディレクトリノードには、他の IBFS リソースと同じセキュリティ構成が適用されます。そのため、管理者は配信ディレクトリノードを使用して、スケジュール済みレポートの配信をサポートする IBFS ファイルの使用を特定の許可されたグループおよびユーザに制限することができます。

既存または新しい配信ディレクトリノードを開くと、[ネットワークパス] ページが表示されます。このページには、次のフィールドが表示されます。

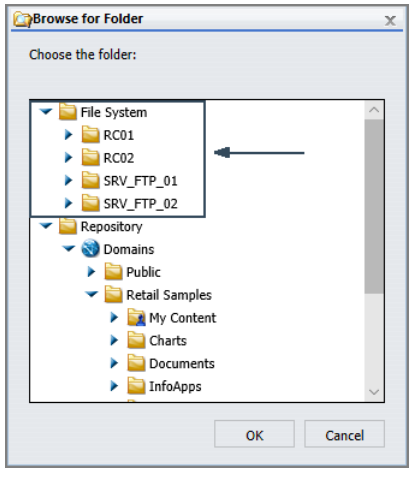
名前

[名前] テキストボックスには、IBFS FILE サブシステム内の配信ディレクトリノードの名前を指定します。このテキストボックスには、一意の値を割り当てる必要があります。同一名で複数の配信ディレクトリノードを作成しようとすると、エラーメッセージが表示されます。

[名前] テキストボックスに割り当てた値は、リソースツリーの配信ディレクトリノードを表すフォルダに表示されます。レガシーホームページでリソースツリーを完全表示モードで表示すると、下図のように、配信ディレクトリノードのフォルダが [FILE] サブシステムフォルダ内のフォルダとして表示されます。



[名前] テキストボックスに割り当てた値は、下図のように、[フォルダの参照] ダイアログボックスで配信ディレクトリノードを表すフォルダにも表示されます。[フォルダの参照] ダイアログボックスは、ReportCaster ベーシックスケジュールツールおよびアドバンストスケジュールツールの [配信] ダイアログボックスから開きます。管理者および許可されたユーザには、リポジトリを使用するレポート配信スケジュールを構成する際にこれらのフォルダが表示されます。



タイプ

管理者は [タイプ] フィールドを使用して、新しい配信ディレクトリでサポートされる配信方法および外部接続のタイプを選択することができます。次の 2 つのオプションがあります。

パス　このオプションを選択した場合、新しい IBFS 配信ディレクトリノードが、Distribution Server にアクセス可能なディレクトリに接続されます。[パス] テキストボックスは [ネットワークパス] ページでも表示が保持され、このディレクトリへのパスが表示されます。

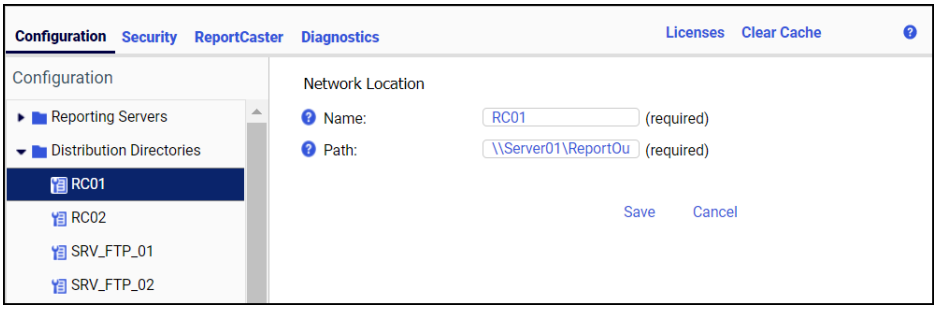
FTP サーバ　このオプションを選択した場合、新しい IBFS 配信ディレクトリノードは、ReportCaster に保持された定義済み FTP の設定構成で指定された FTP サーバに接続されます。[パス] テキストボックスは [FTP サーバ] テキストボックスに置換され、定義済み FTP の設定構成のリストが表示されます。

配信ディレクトリノードは、単一の接続タイプのみサポートできます。そのため、新しい配信ディレクトリノードが作成された場合のみこの項目が表示されます。作成済みの配信ディレクトリノードでは表示されません。

また、配信ディレクトリノードを FTP サーバに割り当てるこのオプションは、定義済み FTP の設定構成が使用できる場合のみ選択可能となるため、この項目およびこれに含まれる 2 つのオプションは、デフォルト設定の構成のほかに少なくとも 1 つの定義済み FTP の設定構成が ReportCaster で使用できる場合のみ表示されます。FTP の設定構成についての詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』を参照してください。

パス

下図のように、[パス] テキストボックスには、IBFS システムの配信ディレクトリノードに対応するネットワーク上のディレクトリへのパスを指定します。このディレクトリは、スケジュール済みレポート出力のファイルシステムターゲットとなるため、Distribution Server がこのパスで指定した場所にファイルを書き込むことができる必要があります。この条件を満たせば、ユーザの要件をサポートする任意の場所にパスを指定することができます。



この値に割り当てるパスのフォーマットは、Distribution Server によって使用されるオペレーティングシステムの要件、または UNC (Universal Naming Convention) の要件に準拠する必要があります。 次のパスのいずれかが使用できます。たとえば、Microsoft Windows ベースのネットワークでは、W:¥ ドライブにマッピングされた「Server01」という名前のサーバ上のファイルシステムディレクトリ「ReportOutput¥Report01」を指定することができます。

- W:¥ReportOutput¥Report01 (Windows)
- /ReportOutput/Report01 (UNIX または Linux)
- ¥¥Server01¥ReportOutput¥Report01 (UNC)

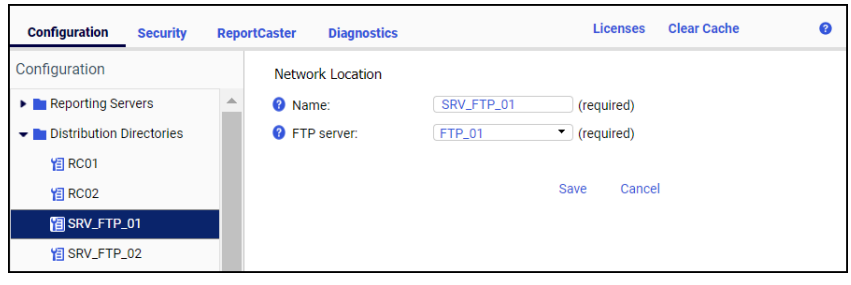
Application Server にもアクセス可能なフォーマットをパスに使用した場合、ファイル配信結果の詳細を Application Server から確認することができます。

パスが、Application Server および Distribution Server をホストしないマシンのディレクトリに指定された場合、Application Server (通常は Tomcat) および Distribution Server がともに、このディレクトリへのアクセス権限を持つユーザ ID で実行される必要があります。Application Server には、ターゲットディレクトリへの読み取り許可が少なくとも必要です。Distribution Server には、ターゲットディレクトリへの読み取り/書き込み許可が少なくとも必要です。これらの許可は、外部ネットワークで構成されるため、本マニュアルでの説明は省略します。

ファイルシステムへのパスは、配信ディレクトリノードの作成前に指定する必要があります。配信ディレクトリノード内のパスが、既存のネットワーク上のディレクトリに指定されていない場合、配信ディレクトリは無効となり、スケジュール済みレポートの配信をサポートできなくなります。

FTP サーバ

下図のように、[FTP サーバ] テキストボックスには、IBFS システムで配信ディレクトリノードがマッピングされる定義済み FTP の設定構成を指定します。



このフィールドに表示されるサーバのリストは、ReportCaster コンソールの [構成] タブで使用可能な一連の定義済み FTP サーバ接続に限定されます。ReportCaster 内で定義されたデフォルト設定の FTP サーバ接続は実際の IBFS ノードではないため、このリストからは除外されます。また、FTP 配信スケジュールに付随するユーザ定義の FTP 接続もリストには表示されません。上記のいずれかで定義された構成を含めるには、管理者が ReportCaster 内に定義済み FTP の設定構成の複製を作成する必要があります。

FTP サーバ構成の詳細には、接続する FTP サーバの名前、この FTP サーバへの接続権限を所有するユーザの ID とパスワード、および使用されるセキュリティプロトコルを指定します。FTP の設定構成についての詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』を参照してください。

配信ディレクトリノードを新規作成する場合、この設定は、[タイプ] 設定で [サーバ] オプションをクリックした後にのみ表示されます。

既存の配信ディレクトリノードを使用する場合、この設定は、作成時に配信ディレクトリノードの FTP サーバ接続をサポートするように構成された場合のみ表示されます。

配信ディレクトリノードへのアクセス許可

通常、リポジトリを使用したスケジュール済みレポート出力の配信は、管理者および指定されたワークスペース内のコンテンツの作成、編集、配信が許可された Developers および Advanced Users グループのユーザに制限されています。これと同じように、スケジュール済みレポートの FILE サブシステムへの配信をサポートする配信ディレクトリノードへのアクセスも、管理者およびノード内のスケジュール済みレポート出力の配信が許可されたユーザに制限されます。ワークスペースベースのセキュリティモデルのツールを使用して、管理者は、これらの許可されたユーザのみが配信ディレクトリを利用できるように設定することができます。

許可されたユーザが配信ディレクトリに完全アクセスできるようにするには、管理者は次のことを行う必要があります。

1. 許可されたグループのユーザが、IBFS FILE サブシステムフォルダのリソースにアクセスできるようにする。
2. 許可されたグループのユーザが使用可能なファイルシステムにスケジュール済みレポート出力を配信できるようにする。
3. グループが個別の配信ディレクトリノードを使用できるようにする。各グループは、配信ディレクトリノードを使用してスケジュール済みレポート配信から作成されたレポート出力を格納します。

上記の要件では、既存の [List] ロールの IBFS システムの [FILE] フォルダへの割り当て、および 2 つの新しいロールの作成が必要です。これら 2 つのロールは、ファイルシステムの配信にアクセス権限を与える [Distribution to File System] ロールと、配信ディレクトリ内のスケジュール済みレポートコンテンツの作成または上書きに必要な権限を与える [Distribution Directory Access] ロールです。

EVERYONE グループのすべてのユーザが [List] ロールを使用できるようにするルールは、デフォルト設定で [FILE] フォルダに割り当てられています。許可されたグループおよびユーザが IBFS FILE サブシステム内に存在する配信ディレクトリノードを使用できるようにするためには、このルールを [FILE] フォルダに割り当てる必要があります。

[Distribution to File System] ロールは、ワークスペース使用時に [Distribute to File System] (opDistributeFileSystem) 権限をユーザに与えるために設定されています。このロールには、必要に応じて他の権限を追加することができます。また、管理者は、他の権限を含む既存のロールにこの権限を追加することもできます。ただし、ファイルシステムの配信アクセスに限定された専用のロールを作成することによって、管理者はこのロールおよびその使用を最も効果的に管理することができます。

[Distribution Directory Access] ロールは、各配信ディレクトリノードの使用に必要な追加のアクセスをユーザに許可します。このロールは、配信ディレクトリノードとそのコンテンツをユーザに表示できる [Access Resource] (opList) 権限、レポートスケジュールを所有するユーザがスケジュール済みレポート出力を含むファイルを配信ディレクトリノードに作成できるようにする [Create Items] (opCreateItem) 権限、およびレポートスケジュールを所有するユーザが、以前のバージョンのファイルでタイムスタンプを含む一意のファイル名が使用されなかった場合に、配信ディレクトリのスケジュール済みレポート出力を含むファイルを上書きできるようにする [Edit Items] (opWrite) 権限で構成されます。スケジュール済みレポート出力を生成する Distribution Server は、レポートスケジュールを所有するユーザの ID を使用して WebFOCUS にログインし、配信ディレクトリノードにスケジュール済みレポート出力を転送するため、[Create Items] および [Edit Items] 権限が必要です。

このロールは、[Distribution to File System] ロールと同じように、必要に応じて他の権限を追加したり、管理者が、他の権限を含む既存のロールにこれらの権限を追加したりできます。ただし、配信ディレクトリノード内のコンテンツの作成と表示に限定された専用のロールを作成することによって、管理者はこのロールおよびその使用を最も効果的に管理することができます。

また、管理者は、スケジュール済みレポート出力を生成するワークスペースにも配信ディレクトリノードを作成する必要があります。すべてのメンバーに、ワークスペースからのスケジュール済みレポート出力の表示または生成が許可されている場合、単一の配信ディレクトリノードにワークスペースからのすべての出力を格納できます。ただし、ワークスペースからの重要性または機密性の高いレポート出力へのアクセスを小規模のグループに制限する場合は、これらの小規模グループにアクセスを制限した追加の配信ディレクトリが必要になります。

権限を持つユーザの配信ディレクトリの使用に必要な構成を完全にするには、管理者は、スケジュール済みレポート出力の IBFS ファイルシステムへの配信をサポートするワークスペースおよび配信ディレクトリに対してルールを作成する必要があります。管理者は、ファイスシステムへの配信用にスケジュール済みレポート出力を生成する各ワークスペースに対して [Distribution to File System] ルールを作成する必要があります。これは、スケジュールを作成時に、このワークスペースのグループメンバーに [ファイルシステム] フォルダおよびワークスペースディレクトリのサブフォルダへのアクセスを許可するために必要です。また、スケジュール済みレポート出力が格納された各配信ディレクトリノードに対して [Distribution Directory Access] ルールを作成する必要もあります。これは、スケジュール済みレポート出力を生成したワークスペースのグループメンバーに配信ディレクトリへのアクセスおよびこれに含まれるスケジュール済みレポート出力の作成を許可するために必要です。

管理者は、次の手順で配信ディレクトリノードを構成することをお勧めします。

1. スケジュール済みレポート出力の配信ディレクトリへのアクセスが必要なワークスペースおよびグループを特定します。

2. スケジュール済みレポートの実行が必要なすべてのユーザが、スケジュール済みレポート出力へのアクセス権限を持つグループに含まれていることを確認します。
3. [Distribution to File System] ロールを作成します。
4. [Distribution Directory Access] ロールを作成します。
5. ワークスペースごとに生成したスケジュール済みレポート出力を格納するために必要な配信ディレクトリノードを作成します。
6. ファイルシステムへの配信用にスケジュール済みレポート出力を生成する各グループを対象に、[Distribution to File System] ルールを作成します。
7. 各ワークスペースからのスケジュール済みレポート出力を格納する配信ディレクトリノードに割り当てられた各グループを対象とする [Distribution Directory Access] ルールを作成します。

以下の説明では、1 つ目および 2 つ目のタスクについての説明は省略されています。これらについては、各組織の要件に基づいて管理者が評価する必要があります。その他のタスクについての詳細は、以下を参照してください。

手順　Distribution to File System ロールを作成するには

このロールは、スケジュール済みレポート出力をワークスペースから IBFS ファイルサブシステムに配信する権限を与えるために設定されます。このロールは、次の手順の説明に従って、単一の権限に制限し、この権限によって特定できるようにすることをお勧めします。ただし、必要に応じてこのロールに他の権限を追加したり、既存のロールに [Distribute to File System] (opDistributeFileSystem) 権限を割り当てたりできます。

1. 管理者としてログインし、セキュリティセンターを起動します。
2. セキュリティセンターで [ロール] タブをクリックします。
3. [新規ロール] アイコンをクリックし、[新規ロール] ダイアログボックスを開きます。
4. [名前] テキストボックスに、この新しいロールの名前を入力します。たとえば、「Distribution to File System」と入力します。
5. [Scheduling and Distribution] 権限カテゴリフォルダ下で、[Distribute to File System] チェックボックスを選択します。
6. [OK] をクリックしてこの新しいロールを保存します。

   ロールのリストに [Distribution to File System] ロールが表示されます。

手順　Distribution Directory Access ロールを作成するには

このロールは、配信ディレクトリノードへのアクセス権限および配信ディレクトリノードでのスケジュール済みレポート出力の作成と上書き権限を与えるために設定されます。このロールは、次の手順の説明に従って、[Access Resource] 権限、[Create Items] 権限、[Edit Items] 権限に制限し、配信ディレクトリへのアクセス権限として特定できるようにすることをお勧めします。ただし、必要に応じてこのロールに他の権限を追加したり、既存のロールにこれらの権限を割り当てたりできます。

1. 管理者としてログインし、セキュリティセンターを起動します。
2. セキュリティセンターで [ロール] タブをクリックします。
3. [新規ロール] アイコンをクリックし、[新規ロール] ダイアログボックスを開きます。
4. [名前] テキストボックスに、この新しいロールの名前を入力します。たとえば、「Distribution Directory Access」と入力します。
5. [Basic Reporting] 権限カテゴリフォルダ下で、[Access Resource] チェックボックスを選択します。
6. [Application Development] 権限カテゴリフォルダ下で、[Create Items] チェックボックスおよび [Edit Items] チェックボックスを選択します。
7. [OK] をクリックしてこの新しいロールを保存します。

   ロールリストに [Distribution Directory Access] ロールが表示されます。

手順　ワークスペースを対象とする Distribution to File System ルールを作成するには

[Distribution to File System] ルールは、ReportCaster を使用してスケジュール済みレポート出力を配信するワークスペースに割り当てられたグループに、IBFS ファイルサブシステムへのアクセス権限を与えます。開始前に、ファイルサブシステムへのアクセスが必要なすべてのユーザが、このルールを割り当てるグループに指定されていることを確認します。

1. 管理者としてログインし、ワークスペース表示を開きます。
2. リソースツリーのワークスペース下またはコンテンツエリアで、スケジュール済みレポートコンテンツに対してリポジトリ配信の使用が必要なワークスペースを右クリックし、[セキュリティ]、[ルール] を順に選択して [セキュリティルール] ダイアログボックスを開きます。
3. [グループとユーザ] タブで、リポジトリ配信へのアクセス権限が必要なグループの名前をクリックします。
4. [グループを対象とするルール] リストで、配信ディレクトリへのアクセス用に作成したロールの名前をクリックします (例、Distribution to File System)。

5. [Distribution to File System] ロールエントリの [アクセス] 列で [許可する] を選択し、[適用先] 列のデフォルト値 [フォルダと下位] を受容します。
6. [適用] をクリック後、[OK] をクリックして新しいルールを保存します。
7. 手順 3 から 6 を繰り返して、追加するワークスペースまたはグループを対象に [Distribution to File System] ルールを作成します。

手順　ワークスペースへの Distribution to File System ルールの割り当てをテストするには

1. [Distribution to File System] ルールが割り当てられたグループのメンバーのユーザ ID とパスワードでログインし、ワークスペース表示を開きます。
2. ワークスペース内のレポートを右クリックし、[スケジュール]、[リポジトリ] を順に選択して ReportCaster スケジューラを開きます。
3. [フォルダパス] をクリックして [フォルダの参照] ダイアログボックスを開きます。
4. [ファイルシステム] フォルダが、[フォルダの選択] ツリー上部に表示された場合は、[OK] をクリックし、ReportCaster スケジューラを閉じます。
5. [ファイルシステム] フォルダが表示されない場合は、[キャンセル] をクリックし、ReportCaster スケジューラを閉じた後、次の手順を実行します。
   a. ワークスペースを右クリックして、[セキュリティ]、[このリソースのルール] を順に選択し、ログインしたグループに [Distribution to File System] ルールが割り当てられていることを確認します。割り当てられていない場合は、このグループに同ルールを割り当てます。
   b. [List] ロールが、EVERYONE グループを対象とする [FILE] サブシステムフォルダに割り当てられていることを確認します。

手順　配信ディレクトリノードを作成するには

配信ディレクトリのノードを作成する場合、既存のネットワーク上のディレクトリへのパスを入力する必要があります。このテキストボックスにパスを入力し、配信ディレクトリノードを保存するだけでは新しいネットワークパスを作成することはできません。パスが、既存のネットワーク上のディレクトリに指定されていない場合、配信ディレクトリノードは無効となり、スケジュール済みレポートの配信をサポートできません。

1. 管理コンソールの [構成] タブで、[配信ディレクトリ] を右クリックし、[新規作成] をクリックして [ネットワークパス] ページを開きます。
2. [名前] テキストボックスに、新しい配信ディレクトリノードを識別する名前を入力します。

3. ネットワークパスに接続する配信ディレクトリノードを作成するには、次の手順を実行します。

   a. [タイプ] フィールドで [パス] をクリックします。

   b. [パス] テキストボックスに、IBFS システムの配信ディレクトリノードに対応する既存のネットワークパスを入力します。この場合、次のいずれかのフォーマットを使用します。

      Windows の場合

      ```
      drive:¥path
      ```

      UNIX または Linux の場合

      ```
      /path
      ```

      UNC (Universal Naming Convention) の場合

      ```
      ¥¥server¥path
      ```

      説明

      `drive`
      サーバがマッピングされたドライブを表す文字です。

      `server`
      [名前] テキストボックスで指定されたノードのスケジュール済みレポートが転送されるディレクトリをホストするサーバの名前です。

      `path`
      [名前] テキストボックスで指定されたノードのスケジュール済みレポートが転送されるディレクトリのネットワークパス名です。

      以下はその例です。

      - W:¥ReportOutput¥Report01 (Windows)
      - /ReportOutput/Report01 (UNIX または Linux)
      - ¥¥Server01¥ReportOutput¥Report01 (UNC を使用した場合)

   c. 手順 5 へ進みます。

4. FTP サーバに接続する配信ディレクトリノードを作成するには、次の手順を実行します。

   a. [タイプ] フィールドで [サーバ] をクリックします。

   b. IBFS システムの配信ディレクトリノードに対応する定義済み FTP の設定構成の名前をクリックします。

c. 手順 5 へ進みます。

5. [保存] をクリックします。
6. 必須情報をすべて入力するよう警告するメッセージが表示された場合は [OK] をクリックし、手順 2 から 5 までに説明した必須情報を入力して保存します。
7. ノードが正常に保存されたことを示すメッセージで [OK] をクリックします。

   [ネットワークパス] ページが閉じられ、新しい配信ディレクトリのノードが [配信ディレクトリ] フォルダ下に表示されます。

手順 配信ディレクトリノードを対象とする Distribution Directory Access ルールを作成するには

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブで [配信ディレクトリ] フォルダを展開します。
3. 更新する配信ディレクトリノードを右クリックし、[セキュリティ]、[ルール] を順に選択して [セキュリティルール] ダイアログボックスを開きます。
4. [グループとユーザ] セクションの [グループ] タブで、配信ディレクトリノードへのアクセス権限が必要なグループ名をクリックします。
5. [グループを対象とするルール] リストで、配信ディレクトリノードへのアクセスを可能にするために作成したロールの名前をクリックします (例、Distribution Directory Access)。
6. [Distribution Directory Access] ロールエントリの [アクセス] 列で [許可する] を選択し、[適用先] 列のデフォルト値 [フォルダと下位] を受容します。
7. [適用] をクリック後、[OK] をクリックして新しいルールを保存します。
8. 手順 3 から 7 を繰り返し、追加の配信ディレクトリノードまたはグループを対象とする [Distribution Directory Access] ルールを作成します。

手順 ワークスペースへの Distribution Directory Access ルールの割り当てをテストするには

1. [Distribution Directory Access] ルールが割り当てられたグループのメンバーのユーザ ID とパスワードでログインします。
2. ワークスペース内のレポートを右クリックし、[スケジュール]、[リポジトリ] を順に選択して ReportCaster スケジューラを開きます。
3. [フォルダパス] をクリックして [フォルダの参照] ダイアログボックスを開きます。
4. [フォルダの選択] ツリー上部に表示される [ファイルシステム] フォルダを展開します。

5. 配信ディレクトリノードの名前が付いたフォルダが [ファイルシステム] フォルダ下に表示された場合は、[OK] をクリックして ReportCaster スケジューラを閉じます。
6. 配信ディレクトリノードのフォルダが表示されない場合は、[キャンセル] をクリックし、ReportCaster スケジューラを閉じた後、次の手順を実行します。
   a. 配信ディレクトリノードを右クリックし、[セキュリティ]、[このリソースのルール] を順に選択して、ログインしたグループに [Distribution Directory Access] ルールが割り当てられていることを確認します。割り当てられていない場合は、このグループに同ルールを割り当てます。
   b. [List] ロールが、EVERYONE グループを対象とする [FILE] サブシステムフォルダに割り当てられていることを確認します。

手順　配信ディレクトリノードを編集するには

[編集] コマンドを使用して、既存の配信ディレクトリノードの値を変更したり、既存のノードをモデルとして新しいノードを作成したりできます。

名前を変更せずに既存の配信ディレクトリノードを保存する場合は、既存のノードが新しいバージョンで上書きされます。新しい名前で既存の配信ディレクトリノードを保存する場合は、新しいノードが自動的に作成され、既存のノードは以前の名前で保持されます。この場合、既存のノードは上書きされません。

既存のノードを新しいノードで置き換える必要がある場合は、新しいノードを作成後に既存のノードを削除します。詳細は、123 ページの 「 配信ディレクトリノードを削除するには 」 を参照してください。

注意 : [タイプ] フィールドは、新しい配信ディレクトリノードの作成時のみ表示されます。そのため、既存の配信ディレクトリノードに割り当てられたタイプを変更することはできません。

1. 管理コンソールの [構成] タブで [配信ディレクトリ] フォルダを展開し、選択した配信ディレクトリを右クリックして [編集] を選択します。
2. 配信ディレクトリノードの名前を変更する必要がある場合は、[名前] テキストボックスに配信ディレクトリノードの新しい名前を入力します。
3. この配信ディレクトリノードが新しいネットワークパスへの接続を必要とする場合は、[パス] テキストボックスに、既存のネットワーク上のディレクトリへの配信ディレクトリの新しいパスを入力します。この場合、次のフォーマットを使用します。

   Windows の場合

   ```
   drive:¥path
   ```

UNIX または Linux の場合

```
/path
```

UNC (Universal Naming Convention) の場合

```
¥¥server¥path
```

説明

`drive`
サーバがマッピングされたドライブを表す文字です。

`server`
[名前] テキストボックスで指定されたノードのスケジュール済みレポートが転送されるディレクトリをホストするサーバの名前です。

`path`
[名前] テキストボックスで指定されたノードのスケジュール済みレポートが転送されるディレクトリのネットワークパス名です。

以下はその例です。

- W:¥ReportOutput¥Report01 (Windows)
- /ReportOutput/Report01 (UNIX または Linux)
- ¥¥Server01¥ReportOutput¥Report01 (UNC を使用した場合)

4. この配信ディレクトリノードが新しい FTP サーバへの接続を必要とする場合は、[FTP サーバ] リストから FTP サーバの名前を選択します。
5. [名前] を変更しなかった場合は、[保存] をクリックします。

   または

   [名前] を変更した場合は、[名前を付けて保存] をクリックします。
6. 必須情報をすべて入力するよう警告するメッセージが表示された場合は [OK] をクリックし、手順 2 と 5 の説明に従ってプロファイルを保存します。
7. ノードが正常に保存されたことを示すメッセージで [OK] をクリックします。

   [ネットワークパス] ページが閉じられます。

   名前を変更しなかった場合は、更新されたノードが [配信ディレクトリ] フォルダ下に表示されます。

名前を変更した場合は、新しいノードおよび既存のノードが [配信ディレクトリ] フォルダ下に表示されます。新しい配信ディレクトリノードには、[Distribution to File System] および [Distribution Directory Access] ルールを割り当て、スケジュール済みレポートの配信に新しい配信ディレクトリノードを使用するグループがこれを使用できるようにする必要があります。

既存のノードを削除する必要がある場合は、123 ページの 「 配信ディレクトリノードを削除するには 」 を参照してください。

手順　配信ディレクトリノードを削除するには

1. 管理コンソールの [構成] タブで [配信ディレクトリ] フォルダを展開し、削除する配信ディレクトリノードを右クリックします。
2. [削除] をクリックします。
3. ノードの削除を確認するメッセージで [はい] をクリックします。

   削除されたノードは、[配信ディレクトリ] フォルダ下に表示されなくなります。

アプリケーション設定の理解

[アプリケーションの設定] では、WebFOCUS Web アプリケーションの構成および動作を設定します。

構成ファイルについての詳細は、525 ページの 「 TIBCO WebFOCUS Client 構成ファイル 」 を参照してください。[アプリケーションの設定] の各設定についての詳細は、527 ページの 「 アプリケーションの設定 」 を参照してください。

手順　アプリケーション設定を表示または編集するには

1. 管理コンソールの [構成] タブで [アプリケーションの設定] フォルダを展開し、表示または編集する設定のカテゴリを選択します。

   右側の構成ウィンドウに各種設定が表示されます。
2. 必要な変更を加え、[保存] をクリックします。

自動ログアウトの管理

アイドル状態を保持した Client セッションは、機密情報やシステムリソースを無許可で使用されるリスクを伴います。Client セッションがアイドル状態を保持する時間を最小限に抑えるために、管理コンソールの [構成] タブの [BI Portal] ページから 2 つの設定を使用して、アイドルセッションの長さを制限することができます (デフォルト設定は 120 分)。

[セッションタイムアウト (分)] (IBI_SESSION_TIMEOUT) 設定は、有効なユーザ ID でログインしたユーザのアイドルセッションの長さを制限します。[パブリックセッションタイムアウト (分)] (IBI_PUBLIC_SESSION_TIMEOUT) 設定は、匿名ユーザ ID でログインしたパブリックユーザのアイドルセッションの長さを制限します。

ベストプラクティスとして、管理者は、上記 2 つの異なるタイプのユーザに対し、セキュリティ上のニーズおよび通常のリソース使用量に見合った最短時間でこれらの設定のデフォルト値を置き換えることをお勧めします。

ユーザにアイドルセッションの期限が近いことを警告するため、[自動ログアウトを有効にする] (IBI_AUTO_SIGNOFF) 設定および [アイドルタイムアウトメッセージまでの期間 (分)] (IBI_AUTO_SIGNOFF_MESSAGE_DURATION) 設定も、[BI Portal] ページに表示されます。[自動ログアウトを有効にする] のチェックをオンにした場合、セッションのアイドル状態が関連する [セッションタイムアウト (分)] 設定の時間 (分) を経過した後にメッセージが表示され、アイドル状態が継続したために現在セッションが期限切れになることが示されます。

このメッセージは、[セッションタイムアウト (分)] 設定で指定された時間 (分) が経過するまで表示された状態になります。この設定のデフォルト値は 2 分です。メッセージがホームページまたはセキュリティセンターに表示された場合、ログアウトまでの残り時間のカウントダウンも表示されます。メッセージがポータルに表示された場合、カウントダウンは表示されません。

セッションを継続するには、[OK] をクリックします。この動作によりメッセージボックスが閉じられ、セッションが復元されます。復元されたセッションがアイドル状態になると、新しいセッションタイムアウトのカウントダウンが開始されます。

ユーザが予定されたタイムアウト前に [OK] をクリックしない場合、メッセージボックスが閉じられ、セッションが終了します。

フォームベース認証または新しいセッションの開始前にユーザの認証を必要とする他の認証方法を使用するゾーンに割り当てられたユーザには、セッション終了後にホームページを表示するウィンドウが自動的にリフレッシュされ、ログインページが表示されます。

シングルサインオンの事前認証方法を使用するゾーンに割り当てられたユーザには、ホームページを表示するウィンドウがリフレッシュされ、[カスタムログアウトターゲット URL] 設定で指定されたログアウトページが代わりに表示されます。

通常、これは、ユーザをログインページに誘導しないデフォルト設定のログアウトページです。ただし、この設定には事前認証のプロバイダが設定したログアウトページの URL も含まれます。この場合、このプロバイダのシングルサインオン製品セッションが終了します。

セキュリティセンターが開いている場合は、セキュリティセンターを表示するウィンドウもリフレッシュされ、ログインページが表示されます。セッションタイムアウト時に開いていた管理コンソールなど他のウィンドウは開いたままで変更されません。ただし、タイムアウト後に最初に使用しようとすると、予期しない動作が発生したことを示すメッセージが表示されます。[OK] をクリックするとこのメッセージがクリアされ、ウィンドウが自動的にリフレッシュされ、ログインページが表示されます。ベストプラクティスとして、新しいセッションで WebFOCUS にログインする前に、1 つのウィンドウを残しそれ以外のウィンドウをすべて閉じることをお勧めします。

ユーザが再度ログインするか、他社製の認証プロバイダの認証を使用してセッションを再開すると、[リダイレクト /ibi_apps 先] 設定で定義されたデフォルトページまたはポータルが開き、ユーザはセッションタイムアウトで中断されたタスクに戻ることができます。

カスタム設定の理解

[カスタム設定] ページでは、標準設定の代わりにカスタム値を入力することで、現在の製品環境をカスタマイズすることができます。

[カスタム設定] テキストボックスに入力した設定変更を保存すると、その変更は *drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc ディレクトリ内の site.wfs ファイルに書き込まれます。このページを使用して設定に新しい値を割り当てると、その設定に割り当てられているデフォルト値が新しい値で上書きされます。新しいバージョンにアップグレードした場合でも、値の上書きは継承されます。

カスタム設定を保存した後でも、入力したテキストがこのページに保持されます。コメントを使用して、特定の更新内容を識別したり、更新内容に関する情報を追加したりできます。

カスタム設定の適用例については、729 ページの 「 Managed Reporting 内部変数 」 を参照してください。

手順　カスタム設定を構成するには

[カスタム設定] ページで設定を構成できるのは管理者のみです。

1. 管理コンソールの [構成] タブで、[カスタム設定] をクリックします。
2. [カスタム設定] テキストボックス上部の最終コメントステートメントまたは最後に入力したカスタム設定エントリの下に、カスタム設定を構成する変数、設定、コマンド、コメントを入力します。

   このコマンドを実行するアプリケーションまたはオペレーティングシステムで要求されるフォーマットを使用します。

   カスタム設定に加えた変更の履歴追跡を容易にするには、変更内容ごとにコメントを使用して各変更を区別します。

3. 暗号化されたフォーマットでカスタム設定を保存するには、[暗号] のチェックをオンにします。

   注意：このチェックをオンにした場合でも、[カスタム設定] テキストボックスに入力した設定は、暗号化されていないフォーマットで保持されます。

4. 構成の完了後、[保存] をクリックします。
5. 確認メッセージのダイアログボックスで [OK] をクリックします。
6. [カスタム設定] ページがクリアされた後、[カスタム設定] テキストボックスで更新したコメント、設定、コマンドを確認するには、[カスタム設定] をクリックします。

NLS 設定の理解

管理コンソールでは、国際言語サポートを構成したり、言語の切り替えを有効にしたりすることができます。

製品でサポートされる各国際言語サポートには、異なるメッセージファイルが存在します。レポート出力に使用する文字セットをカスタマイズする場合は、使用する各言語のコードページを選択する必要があります。

手順　国際言語サポートを構成するには

1. 管理コンソールの [構成] タブで [NLS 設定] をクリックして、NLS 設定のページを開きます。
2. Client が実装されているオペレーティングシステムのオプションを選択します。

   選択したオペレーティングシステムに応じて、リストに表示されるコードページが調整されます。

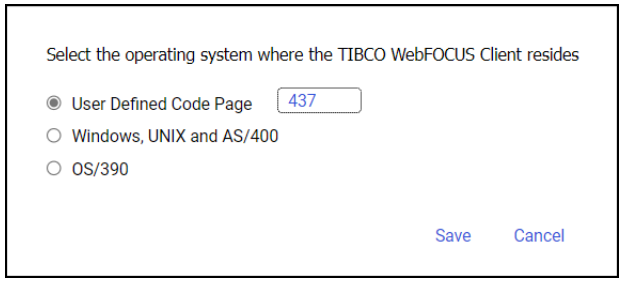
3. ブラウザにレポート出力を正しく表示するために、このリストから Client を構成するコードページを選択します。

   注意：一般に、Client 用に選択する言語は、Reporting Server コンソールで Reporting Server 用に選択する言語に一致させます。

   Reporting Server コンソールで選択した言語が管理コンソールのドロップダウンリストに表示されない場合は、[ユーザ定義コードページ] を選択し、コードページ番号を直接入力します。

   このオプションは、Reporting Server で新しいコードページのサポートが追加されたが、Client でこのサポートがまだ反映されていない場合などに使用します。

下図は、管理者がコードページ 437 を指定したサンプル構成ウィンドウを示しています。



Windows、UNIX オペレーティングシステムでは、Unicode (UTF-8) を使用することができます。

注意：コードページ 137 を使用するよう構成された App Studio では、ISO 8859-1 の Java エンコード制限により、0x80 から 0x9F までの文字がサポートされません。そのため、次の文字をフランス語で正しく表示するには、コードページ 1252 を使用するよう Application Server を構成する必要があります。

- U+0152 Latin 大文字の合字 OE
- U+0153 Latin 小文字の合字 oe

4. [保存] をクリックして、NLS 設定を保存します。Client 構成ファイル (nlscfg.err) が *drive*:¥ibi¥WebFOCUS82¥client¥home¥etc ディレクトリに生成され、新しい CODE_PAGE 設定で更新されます。再度 [NLS 設定] をクリックすると、新しい設定がアクティブなコードページとして反転表示されます。

参照　Client コードページ設定

選択可能なコードページ設定には、次のものがあります。

- * 137 - 英語 (米国)/西ヨーロッパ言語
- 874 - タイ語
- * 942 - 日本語
- * 946 - 中国語 (簡体字)
- 949 - 韓国語
- 1250 - 東ヨーロッパ言語
- 1251 - ロシア語

- ＊1252 - 西ヨーロッパ言語
- 1253 - ギリシャ語
- 1254 - トルコ語
- ＊1255 - ヘブライ語
- 1256 - アラビア語
- 1257 - バルト言語
- 10942 - 日本語 (EUC)
- 10948 - 中国語 (繁体字)
- ＊65001 - Unicode (UTF-8)

注意：現在のリリースで完全にサポートされているコードページは、アスタリスク (*) の付いたコードページのみです。

言語の切り替えのカスタマイズ

ログインページで選択可能にする言語をカスタマイズするには、[言語の切り替え] 設定を有効にします。

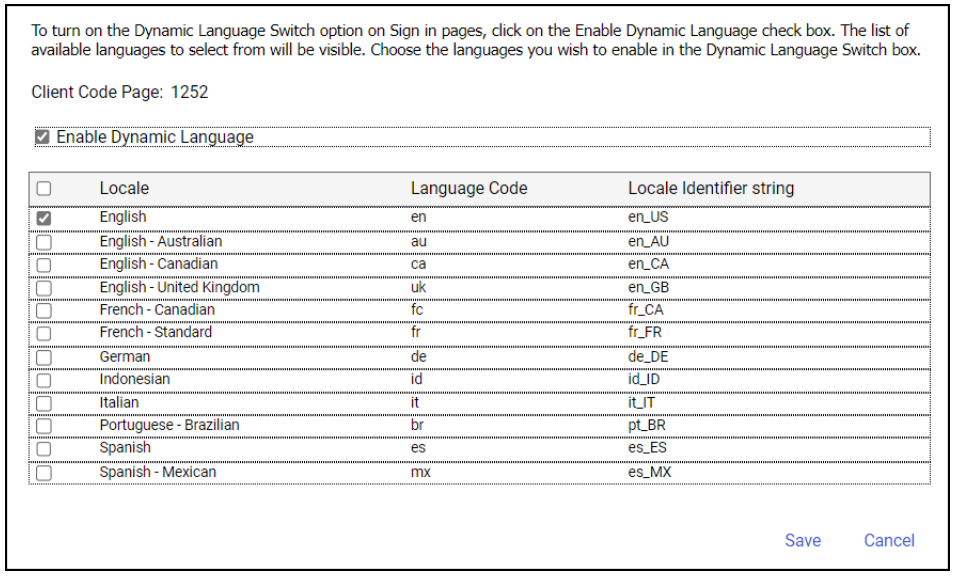
手順　言語の切り替えをカスタマイズするには

1. 管理コンソールの [構成] タブで、[言語の切り替え] をクリックします。

   [言語の切り替え] ページが開き、[NLS 設定] ページで選択したコードページに対して使用可能な言語のリストが表示されます。デフォルト設定では、[言語の切り替えを有効にする] のチェックはオフで、すべての言語のチェックボックスが無効になっています。

   [言語の切り替え] ウィンドウには、126 ページの 「 国際言語サポートを構成するには 」で指定された [Client コードページ] 設定も表示されます。

2. 下図のように、[言語の切り替えを有効にする] のチェックをオンにして、パネル内のすべての言語のチェックボックスを有効にします。

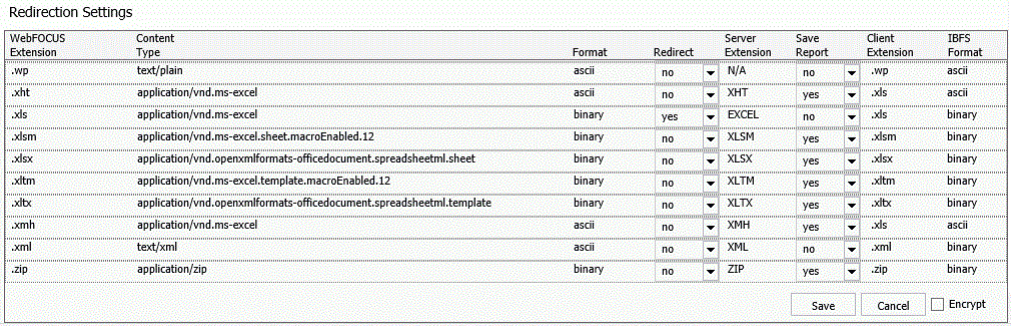


3. ログインページおよび [言語] メニューに表示する言語のチェックをオンにします。
4. ログインページの [言語の選択] ドロップダウンリストおよび [言語] メニューにすべての言語を表示するには、[ロケール] 見出し横のチェックをオンにします。
5. [保存] をクリックします。
6. 「変更が保存されました」というメッセージで [OK] をクリックします。

注意：ログインページの [言語] ドロップダウンリストから言語を除外する場合は、除外する言語のチェックをオフにします。

出力先変更設定の理解

出力先変更設定は、Client がファイル拡張子で出力ファイルを扱う方法を指定します。これらの設定は、管理コンソールの [構成] タブの [出力先変更設定] で確認することができます。下図のように、このページの各エントリは、WebFOCUS 拡張子、コンテンツタイプ、ファイルフォーマット、サーバ拡張子、Client 拡張子、IBFS フォーマットで出力ファイルが識別されています。


Redirection Settings

WebFOCUS Extension	Content Type	Format	Redirect	Server Extension	Save Report	Client Extension	IBFS Format
.wp	text/plain	ascii	no	N/A	no	.wp	ascii
.xht	application/vnd.ms-excel	ascii	no	XHT	yes	.xls	ascii
.xls	application/vnd.ms-excel	binary	yes	EXCEL	no	.xls	binary
.xlsm	application/vnd.ms-excel.sheet.macroEnabled.12	binary	no	XLSM	yes	.xlsm	binary
.xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	binary	no	XLSX	yes	.xlsx	binary
.xltm	application/vnd.ms-excel.template.macroEnabled.12	binary	no	XLTM	yes	.xltm	binary
.xltx	application/vnd.openxmlformats-officedocument.spreadsheetml.template	binary	no	XLTX	yes	.xltx	binary
.xmh	application/vnd.ms-excel	ascii	no	XMH	yes	.xls	ascii
.xml	text/xml	ascii	no	XML	no	.xml	binary
.zip	application/zip	binary	no	ZIP	yes	.zip	binary

Save Cancel Encrypt

注意：上図は [出力先変更設定] ページの下半分に表示されたファイル拡張子およびさまざまな [リダイレクト] と [保存レポート] フィールドの値を示しています。

ディレクトリ *drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc に格納された mime.wfs ファイルには、使用可能なフォーマットタイプに関する情報が保存されています。[出力先変更設定] ページを開くと、mime.wfs ファイルに保存された出力先変更設定が表示され、変更を保存するとこれらが mime.wfs ファイルに保存されます。

[出力先変更設定] に変更を加える前に、アプリケーションおよび組織内でのユーザ操作への影響を評価する必要があります。詳細は、技術サポートに問い合わせてください。

注意

- [Client 設定] ページに表示される [リダイレクト] (IBIWF_REDIRECT) の構成タブの設定についての詳細は、552 ページの 「 Client 設定 」 を参照してください。

ファイル出力のリダイレクトおよび保存

[出力先変更設定] ページの [リダイレクト] および [保存レポート] 設定の値は、リクエストからの出力を処理中に temp フォルダのファイルに保存するかどうか、またこのファイルに自動的に名前を割り当てるかどうかを指定します。これらの 2 つの設定に割り当てられた値の組み合わせによって、リクエストからの出力の表示および保存方法が指定されます。

[リダイレクト] 設定では、リクエストからの出力を Client ディレクトリ下の temp フォルダのファイルに保存するかどうかを指定することができます。

- [リダイレクト] の値が [はい] に設定されている場合、出力は temp フォルダのファイルに保存され、[保存レポート] 設定に割り当てられた値に従って、ファイルに名前が割り当てられます。
- [リダイレクト] の値が [長さ] に設定されている場合は、バッファサイズ設定 (IBIWF_sendbufsize) に割り当てられた値 (デフォルト値は 16384 バイト) を超えた場合のみ、出力が temp フォルダのファイルに保存されます。temp フォルダのファイルに保存する必要のある出力はすべて、追加の HTTP コールは実行されずに、そのままブラウザに送信されます。
- [リダイレクト] の値が [いいえ] に設定されている場合、[保存レポート] 設定に割り当てられた値に従って処理されます。

  [保存レポート] 設定では、レポートファイルの名前を作成時に自動的に割り当てるかどうかを指定することができます。

  - [保存レポート] の値が [いいえ] に設定されている場合、レポート、グラフ、その他の出力はブラウザまたはアプリケーションに直接表示されます。この場合、これを開くか保存するかの選択を要求するプロンプトは表示されません。ユーザは、レポートを開いた後でも保存することができます。レポート出力ファイルには、ランダムに生成される名前が割り当てられます。これは、リクエストの実行元がリソースツリー、InfoAssist、WebFOCUS App Studio、またはその他のアプリケーションツールであっても関係ありません。
  - [保存レポート] の値が [はい] に設定されている場合、レポート、グラフ、その他の出力は、次のように temp フォルダのファイルに保存されます。
    - レポートリクエストで出力ファイル名が指定されている場合、この名前が出力ファイルに割り当てられます。次に、ブラウザが一時的に保存された出力ファイルを取得するために HTTP コールを実行し、ユーザはファイルを開くか、保存するか、キャンセルするかの選択が要求されます。
      - 日付および時間を必要とするレポート、グラフ、その他のコンテンツファイルは、ファイル名の指定およびレポートが Reporting Server で作成された日付と時間の取得に変数を使用する次のコーディング方法を含めることで作成することができます。詳細は、133 ページの 「 PCHOLD AS ファイル名への日付時間の追加 」 の例を参照してください。

- レポートリクエストでファイル名が指定されない場合は、次のようになります。
  - リソースツリーの項目からレポートを実行する場合、この項目の名前の値がリクエストの出力ファイルに割り当てられ、ファイルが作成された日付と時間は自動的にこのファイル名に追加されます。

    注意：項目の名前の値は、[プロパティ] パネルの [名前] テキストボックスに表示されます。
    - ただし、[リダイレクトレポート名にタイムスタンプを追加しない] 設定のチェックもオンの場合は、ファイル名に日付と時間が自動的に追加されません。
  - TIBCO WebFOCUS DESIGNER、InfoAssist、テキストエディタ、App Studio レポートキャンバスなどのツールからレポートを実行する場合、ランダムに生成された名前が出力ファイルに割り当てられ、ファイルが作成された日付と時間は自動的にこのファイル名に追加されます。
    - ただし、[リダイレクトレポート名にタイムスタンプを追加しない] 設定のチェックもオンの場合は、ファイル名に日付と時間が自動的に追加されません。

レポートリクエスト内での出力ファイル名の指定

レポートリクエスト内で出力ファイル名を指定するには、PCHOLD AS ファイル名オプションを使用します。

レポートリクエストで使用される、PCHOLD オプションの構文は次のとおりです。

```
ON TABLE PCHOLD [AS filename] [FORMAT fmt]
```

説明

`AS filename`
PCHOLD ファイルの名前を指定します。

`FORMAT fmt`
PCHOLD ファイルのフォーマットを指定します。たとえば、XLSX と指定します。

注意：レポートリクエストで指定された PCHOLD AS の名前に含まれる文字数が 8 文字以下の場合は、大文字でブラウザに返されます。9 文字以上が含まれる場合は、指定した文字 (大文字または小文字) でブラウザに返されます。

PCHOLD コマンドを使用したレポート作成についての詳細は、『TIBCO WebFOCUS Language リファレンス』を参照してください。

PCHOLD AS ファイル名への日付時間の追加

Microsoft Excel など一部のアプリケーションでは、各ファイルに一意の名前が必要です。この条件に対応するため、[保存レポート] 設定に [はい] の値を割り当てる際に、Reporting Server でレポートが作成された日付と時間を取得するようレポートリクエストに変数を追加し、追加された日付と時間をファイル名に指定し、このファイル名をレポートファイルに割り当てることができます。以下はその例です。

```
-SET &TIME = STRIP(8,&TOD,'.',A8);
-SET &FNAME = OUTPUT_ | &YYMD | _ | &TIME;
TABLE FILE CAR
BY CAR
ON TABLE PCHOLD AS &FNAME FORMAT XLSX
END
XSLX
```

手順　出力先変更設定を変更するには

[出力先変更設定] に変更を加える前に、アプリケーションおよび組織内でのユーザ操作への影響を評価する必要があります。また、必要に応じて、その他の大規模アプリケーションの管理者、または変更によって影響を受ける組織のネットワーク管理者に確認してください。詳細は、技術サポートに問い合わせてください。

1. 管理コンソールの [構成] タブで、[出力先変更設定] をクリックします。
2. [リダイレクト] ドロップダウンリストには次のオプションがあります。
   a. [はい] をクリックすると、指定した拡張子を使用したファイルの出力を一時ディレクトリにリダイレクトします。
   b. [いいえ] をクリックすると、[保存レポート] 設定で割り当てられた値に従って出力を処理することができます。
   c. [長さ] をクリックすると、IBIWF_sendbufsize 設定で定義されたバッファサイズを超える場合のみ、レポートコンテンツを一時ディレクトリにリダイレクトします。
3. [保存レポート] ドロップダウンリストには次のオプションがあります。
   a. [はい] をクリックすると、ブラウザにプロンプトが表示され、指定した拡張子を使用したファイルの出力を開くか保存するかの選択が要求されます。
   b. [いいえ] をクリックすると、出力がブラウザまたはアプリケーションに直接表示され、出力を開くか保存するかの選択は要求されません。
4. 出力先変更設定を暗号化する場合は、ウィンドウ最下部の [暗号] のチェックをオンにします。
5. [保存] をクリックして、[出力先変更設定] パネルで加えた変更を保存します。

GRAPH (PNG、SVG、GIF、JPEG、JPG) リクエストの保存

プロシジャで PNG、SVG、GIF、JPEG、または JPG フォーマットを指定する GRAPH リクエストで [保存レポート] 機能を活用するには、次のことを実行する必要があります。

1. 拡張子 .htm の [保存レポート] は、[はい] に設定します。

   サーバサイド GRAPH リクエストを実行すると、実際のグラフ出力へのリンクを含む HTM ファイルが作成されます。このグラフ出力は、一時イメージファイルとして .jpeg、.jpg、.gif、.svg、.png のいずれかの拡張子で保存されているファイルです。

2. GRAPH リクエスト実行時に、出力を開くか保存するかの選択が要求された場合、[保存] を選択すると、この出力は、グラフイメージの参照のみが含まれた HTM ファイルとして保存されます。このグラフイメージは、Client 構成の一時ファイルの期限切れ設定によって、最終的には期限切れとなり、サーバから削除されます。

3. GRAPH リクエストの出力を保存するには、保存された HTM ファイルを開き、グラフイメージを右クリックして [名前を付けて画像を保存] を選択し、ディスクに永久保存します。これを実行すると、HTM 出力ファイルでは、保存されたイメージファイルを完全参照するよう変更することができます。

InfoAssist プロパティの理解

[InfoAssist のプロパティ] では、すべての InfoAssist ユーザに適用される、システム全体のデフォルト値を設定することができます。これらの設定を更新するには、[構成] タブをクリックし、[InfoAssist のプロパティ] をクリックします。特定の InfoAssist のプロパティについての詳細は、588 ページの 「 InfoAssist のプロパティ 」 を参照してください。

ロール更新ユーティリティの理解

[ロール更新ユーティリティ] ページには、リポジトリの各ロールに現在割り当てられている権限と、製品パッケージの各ロールに割り当てられている権限の差異が表示されます。リポジトリロールはリポジトリ内で定義され、リソーステンプレートで使用されます。パッケージロールは別のファイルで管理され、製品リリース内のロールに標準で割り当てられた権限セットを定義します。

新しいリリースにアップグレードした場合や、セキュリティセンターでロールを更新することでリポジトリロールに割り当てられている権限を変更した場合、このユーティリティを使用すると、リソーステンプレートで使用されるリポジトリロールに割り当てられた権限と、パッケージロールで定義されている一連の標準権限の差異が識別されます。

リポジトリロールに割り当てられた権限セットがパッケージロールの権限セットと異なる場合、このユーティリティのオプションを使用して、差異を無視するか、欠落している権限をリポジトリロールに追加するか、またはリポジトリロール全体をパッケージロールで定義された標準権限セットに置換するかを選択することができます。パッケージロールに含まれていない権限がリポジトリロールに割り当てられている場合、これらの余分な権限をすべて削除するには、リポジトリロールをパッケージロールに置換する必要があります。また、このユーティリティでは、リポジトリロールに割り当てられた権限セットがパッケージロールの権限セットと異なる場合に、これらのリポジトリロールすべてをグローバルに変更することもできます。

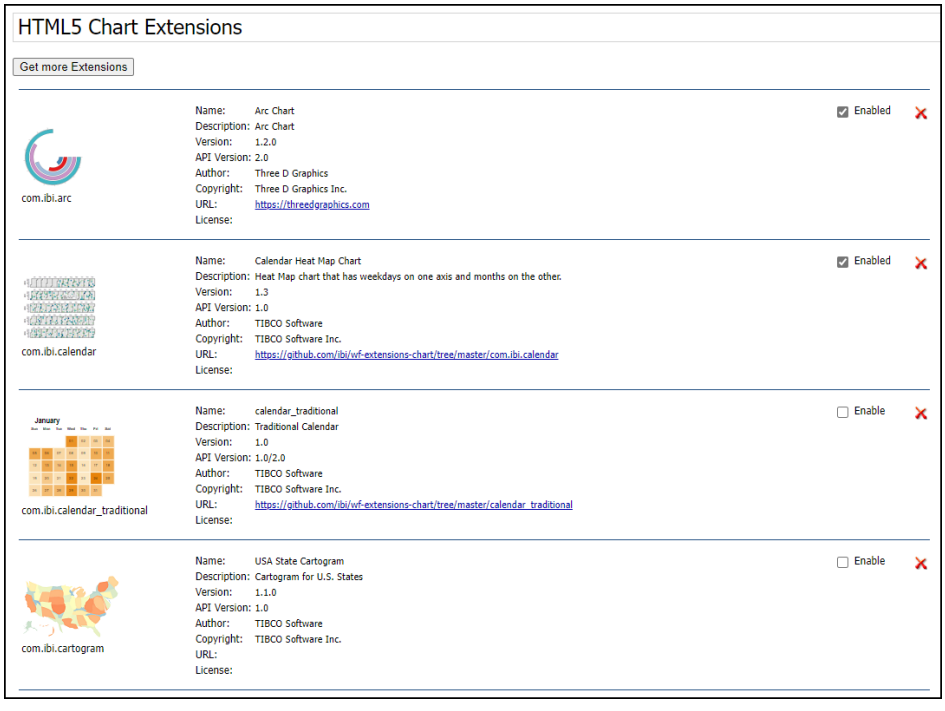
新しいリリースのアップグレードまたはインストールの実行後、このユーティリティを使用して既存のリポジトリロールと新しいパッケージロールの差異を特定し、新しい権限をリポジトリロールに組み込むことも、既存のリポジトリロールを更新せずに保持することもできます。

ロールの権限セットに変更がない場合は、ロールのエントリに「パッケージとリポジトリのロールに違いはありません」というメッセージが表示されます。その場合、リポジトリロールを更新または変更するまで、このユーティリティを使用する必要はありません。

通常のインストール後にロールを更新する方法についての詳細は、『TIBCO WebFOCUS インストールガイド』を参照してください。

HTML5 グラフ拡張機能の操作

[HTML5 グラフ拡張機能] ページには、下図のように、現在インストールされているすべての HTML5 グラフ拡張機能が表示されます。

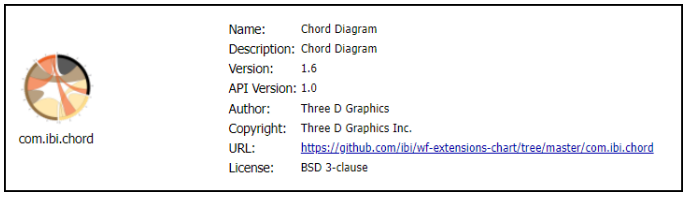


HTML5 グラフ拡張機能は、標準的な グラフを拡張したもので、非常に特殊なレポート作成およびデータ視覚化の要件に合わせてカスタマイズされたグラフが含まれます。グラフ拡張機能についての詳細は、『TIBCO WebFOCUS HTML5 (JSCHART) リファレンス』の「グラフ拡張機能のインストール」を参照してください。

このページの機能を使用して、HTML5 グラフ拡張機能をアップロードしたり、これらの使用を有効または無効にしたり、不要になった場合はアンインストールしたりできます。

HTML5 グラフ拡張機能エントリの理解

HTML5 グラフ拡張機能の各エントリには、グラフ拡張機能およびその作成元を識別する詳細情報が表示され、これに基づいてユーザは各グラフ拡張機能の使用が適切かどうかを判断することができます。



各エントリでは、HTML5 グラフ拡張機能が、[名前]、[説明]、[バージョン]、[API バージョン] で識別されます。これらの詳細情報は、ユーザが使用するグラフ拡張機能を特定したり、ユーザのニーズに最も合ったバージョンを特定したりするのに役立ちます。[作成者] および [著作権] では、各グラフ拡張機能の作成元、および追加コピーの取得先の URL リンクが識別できます。[ライセンス] では、グラフ拡張機能の使用を可能にするライセンスのタイプが識別でき、ユーザはグラフ拡張機能の使用に関する制限およびライセンスを所有するユーザが開発者に対して持つ権利と義務について理解することができます。

HTML5 グラフ拡張機能の有効にする/有効化済みチェックボックスの理解

HTML5 グラフ拡張機能の各エントリには、このグラフ拡張機能が使用できるかどうかを示す [有効にする] / [有効化済み] チェックボックスが表示されています。このチェックボックスを使用して、管理者はこれらのグラフ拡張機能の使用を 2 段階で管理することができます。つまり、実際に使用する HTML5 グラフ拡張機能のみ有効とし、インストール済みの他のすべての HTML5 グラフ拡張機能は必要に応じて使用できるように保持することができます。

このチェックがオフの場合は、下図のように [有効にする] ラベルが表示され、チェックボックスを選択するとこのグラフ拡張機能が使用できるようになることが示されます。

[有効にする] チェックボックスが選択された HTML5 グラフ拡張機能は、インストール済みですが、ユーザに利用可能にはなっていません。

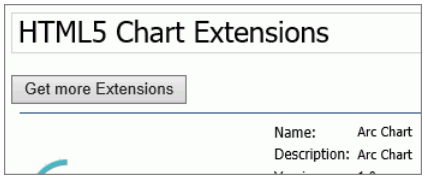
このチェックボックスを選択すると、下図のように [有効化済み] ラベルが表示され、このグラフが使用可能になったことが示されます。

[有効化済み] チェックボックスが選択された HTML5 グラフ拡張機能はインストール済みであり、開発者は InfoAssist を利用したグラフの作成にこれを使用することができます。グラフ拡張機能に含まれたファイルおよびディレクトリは、InfoAssist および DESIGNER からの呼び出し対象として識別されます。グラフ拡張機能のアイコンは、InfoAssist の [フォーマット] タブのリボンの [グラフ] グループで、[その他] コマンドから開く [グラフの選択] メニューに表示されます。

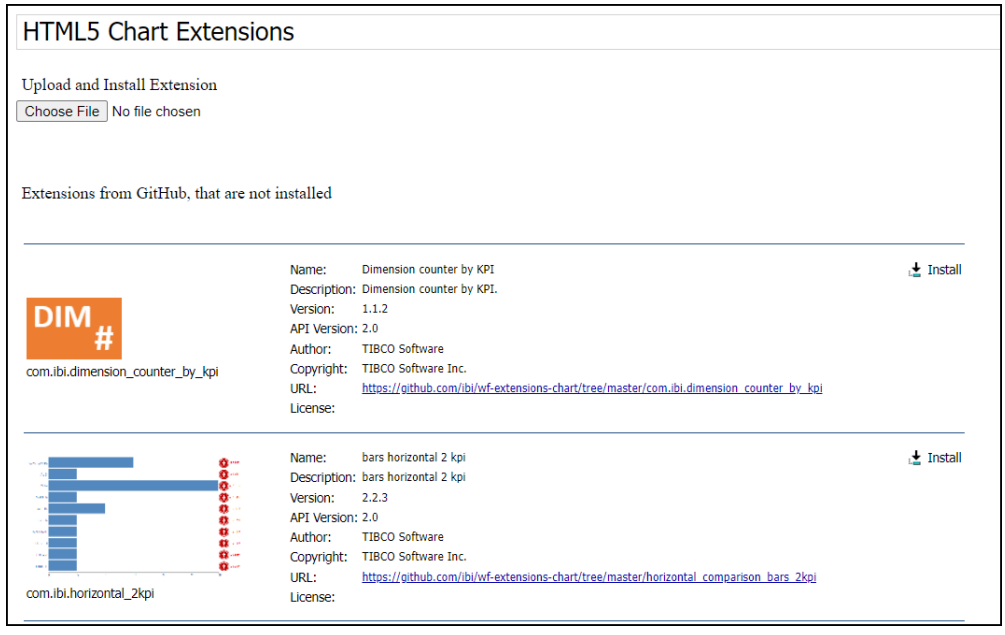
注意：[HTML5 グラフ拡張機能] ページでは、著作権またはライセンス制限が管理されません。アップロードする HTML5 グラフ拡張機能の使用については、ユーザが最終責任を負います。そのため、ページにアップロードする前に HTML5 グラフ拡張機能の使用に関するライセンスまたは許可を所有していることを確認してください。

拡張機能のアップロードとインストールページを使用した追加の HTML5 グラフのアップロード

追加の HTML5 グラフ拡張機能をインストールするには、[拡張機能のアップロードとインストール] ページを使用します。[HTML5 グラフ拡張機能] のメインページから [拡張機能のアップロードとインストール] ページを開くには、下図のように [その他の拡張機能を取得] をクリックします。



下図は、[拡張機能のアップロードとインストール] ページを示しています。



[拡張機能のアップロードとインストール] ページでは、次の 2 つの方法で追加の HTML5 グラフ拡張機能をインストールすることができます。

- [拡張機能のインストール] ボタンをクリック - Install [拡張機能のインストール] ボタンは、Information Builders の GitHub サイトの拡張機能セクション (https://github.com/ibi/wf-extensions-chart) に公開されているが、現在インストールされていないグラフ拡張機能のエントリに表示されます。
- [拡張機能のアップロードとインストール] 横の [ファイルを選択] ボタン Choose File をクリックして、ローカル環境で作成された HTML5 グラフ拡張機能パッケージが .zip ファイルフォーマットで保存されているユーザのローカルファイルシステム上のフォルダに移動します。

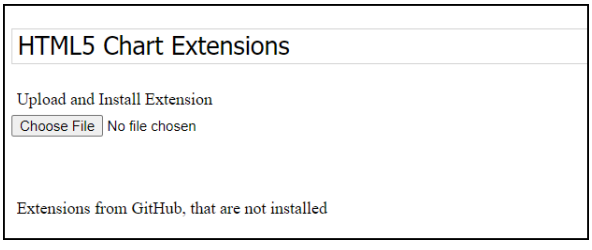
[拡張機能のアップロードとインストール] ページから [HTML5 グラフ拡張機能] のメインページに戻るには、[HTML5 グラフ拡張機能] をクリックするか、ブラウザの [戻る] ボタンをクリックします。

手順　HTML5 グラフ拡張機能をローカルファイルシステムからアップロードするには

次の手順で、HTML5 グラフ拡張機能を含む ZIP ファイルをユーザのローカルシステムからアップロードすることができます。

アップロードする前に、HTML5 グラフ拡張機能の使用に関するライセンスまたは許可を所有していることを確認してください。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [HTML5 グラフ拡張機能] をクリックします。
3. [HTML5 グラフ拡張機能] ページで、[その他の拡張機能を取得] をクリックします。
4. 下図のように、[拡張機能のアップロードとインストール] ページで [ファイルを選択] をクリックします。



[開く] ダイアログボックスが開き、ローカルインストールディレクトリ下の拡張機能フォルダを選択します。通常は、次のフォルダを指定します。

drive:¥ibi¥*install_dir*¥config¥web_resource¥extensions

説明

install_dir
TIBCO WebFOCUS インストールのディレクトリです。

注意：HTML5 グラフ拡張機能の ZIP ファイルを別のディレクトリにダウンロードした場合は、このディレクトリおよびファイルに移動します。

5. アップロードする HTML5 グラフ拡張機能が格納された ZIP ファイルを選択し、[開く] をクリックします。
6. [HTML5 グラフ拡張機能] ページがリフレッシュされ、ページ最上部に戻されます。ここで、新しい HTML5 グラフ拡張機能のエントリが表示されるまで画面を下方向へスクロールします。

注意：ユーザ独自の HTML5 グラフ拡張機能の作成についての詳細は、『TIBCO WebFOCUS HTML5 (JSCHART) リファレンス』の「グラフ拡張機能の作成」を参照してください。

手順　HTML5 グラフ拡張機能を ibi GitHub ページからインストールするには

次の手順で、HTML5 グラフ拡張機能を ibi GitHub サイトの拡張機能セクション (https://github.com/ibi/wf-extensions-chart) からアップロードすることができます。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [HTML5 グラフ拡張機能] をクリックします。
3. [HTML5 グラフ拡張機能] ページで、[その他の拡張機能を取得] をクリックします。
4. 下図のように、[拡張機能のアップロードとインストール] ページで、[GitHub で利用可能な未インストールの拡張機能] 以下のリストを確認します。

5. インストールしたいグラフ拡張機能がリストに表示されている場合は、[拡張機能のインストール] Install をクリックします。
6. [HTML5 グラフ拡張機能] ページがリフレッシュされ、ページ最上部に戻されたます。ここで、画面を下方向へスクロールしてこのグラフ拡張機能がインストールされていることを確認します。

手順　インストール済みの HTML5 グラフ拡張機能を有効にするには

HTML5 グラフ拡張機能のエントリで [有効にする] チェックボックスを選択すると、このグラフ拡張機能が利用可能になります。有効にする前に、HTML5 グラフ拡張機能の使用に関するライセンスまたは許可を所有していることを確認してください。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [HTML5 グラフ拡張機能] をクリックします。
3. [HTML5 グラフ拡張機能] ページで、有効化する HTML5 グラフ拡張機能のエントリまで画面をスクロールします。

注意：ブラウザでサポートされる [検索] または [このページの検索] コマンドを使用して、グラフ拡張機能の名前で検索することもできます。

4. 下図のように、[有効にする] のチェックをオンにします。

5. [HTML5 グラフ拡張機能] ページがリフレッシュされ、ページ最上部に戻されたます。ここで、画面を下方向へスクロールしてこのエントリのチェックボックスが選択されていることを確認します。

   HTML5 グラフ拡張機能のアイコンは、InfoAssist の [フォーマット] タブの [グラフ] グループで [その他] コマンドをクリックすると開く [グラフの選択] メニュー、および DESIGNER キャンバス右側に開くコンテンツの選択オプションの [カスタム] セクションに表示されます。

手順　HTML5 グラフ拡張機能を無効にするには

HTML5 グラフ拡張機能のエントリで [有効化済み] のチェックをオフにすると、このグラフ拡張機能が利用不可能になります。ただし、このグラフ拡張機能は [HTML5 グラフ拡張機能] ページにインストールされた状態で保持され、必要に応じて再度有効にすることができます。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [HTML5 グラフ拡張機能] をクリックします。
3. [HTML5 グラフ拡張機能] ページで、無効にする HTML5 グラフ拡張機能のエントリまで画面をスクロールします。

   注意：ブラウザでサポートされる [検索] または [このページの検索] コマンドを使用して、グラフ拡張機能の名前で検索することもできます。

4. 下図のように、[有効化済み] のチェックをオフにします。

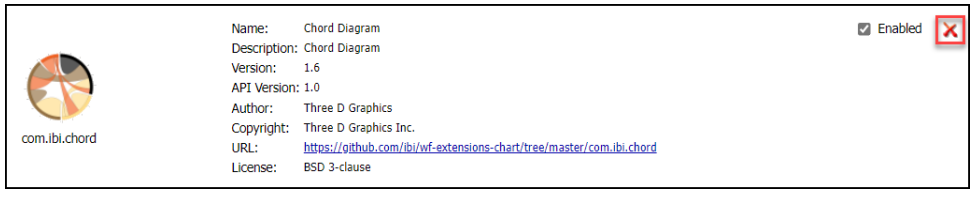
5. [HTML5 グラフ拡張機能] ページがリフレッシュされ、ページ最上部に戻されたます。ここで、画面を下方向へスクロールしてこのエントリのチェックボックスの選択が解除されていることを確認します。

   この HTML5 グラフ拡張機能のアイコンは、InfoAssist のリボンから開く [グラフの選択] メニュー、または DESIGNER キャンバス右側から開くコンテンツの選択オプションの [カスタム] セクションに表示されなくなります。

手順　HTML5 グラフ拡張機能をアンインストールするには

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [HTML5 グラフ拡張機能] をクリックします。
3. [HTML5 グラフ拡張機能] ページで、アンインストールする HTML5 グラフ拡張機能のエントリまで画面をスクロールします。

   注意：ブラウザでサポートされる [検索] または [このページの検索] コマンドを使用して、グラフ拡張機能の名前で検索することもできます。
4. 下図のように、[削除 (グラフ名)] をクリックします。



5. 「この拡張機能を完全に削除してよろしいですか」というメッセージで [OK] をクリックします。
6. [HTML5 グラフ拡張機能] ページがリフレッシュされ、ページ最上部に戻されたます。ここで、画面を下方向へスクロールしてこのエントリが削除されていることを確認します。

   この HTML5 グラフ拡張機能のエントリの表示がページからなくなります。HTML5 グラフ拡張機能が GitHub サイトからインストールされていた場合、[拡張機能のアップロードとインストール] ページに表示され、このページから再インストールすることができます。ローカルファイルシステムからインストールされていた場合はこのページに表示されません。このグラフ拡張機能をローカルファイルシステムから再ロードするためには、[拡張機能のアップロードとインストール] ページの [ファイルを選択] ボタンを使用する必要があります。

TIBCO WebFOCUS セキュリティの構成

管理コンソールでは、ユーザ環境の認証と認可を制御するセキュリティ設定を構成することができます。

セキュリティは、リポジトリ内部で構成することも、TIBCO WebFOCUS 外部のディレクトリを使用して構成することもできます。内部セキュリティの設定を構成するには、[内部] ページの設定を使用します。TIBCO WebFOCUS 外部のディレクトリ (例、Microsoft Active Directory または LADP ディレクトリ) への接続を構成するには、[外部] ページを使用します。

内部セキュリティページ設定の理解

デフォルト設定では、内部認証および内部認可が有効になっています。必要に応じて、[内部] ページの設定を使用して、ログインおよびパスワードポリシーを構成することもできます。

ログインの設定 ([ログインの設定] セクションの有効化)

[内部] セキュリティページの [ログインの設定] セクションに割り当てられたデフォルト値を有効にします。

デフォルト設定では、このチェックはオフ (False) になっています。[ログインの設定] セクションは無効 (選択不可) です。各設定には 0 (ゼロ) が表示されます。

このチェックをオン (True) にすると、[ログインの設定] セクションが有効になります。各設定には構成済みの値が自動的に割り当てられますが、これらの値は変更することができます。このチェックをオンにした状態で各設定を個別に無効にするには、0 (ゼロ) を入力または選択します。後からこのチェックをオフにすると、[ログインの設定] セクションに割り当てられた値がすべて 0 (ゼロ) に戻り、これらの設定が無効になります。

この設定は、[パスワードの期限切れの結果] オプションの値には影響しません。

ログインの最大試行回数 (IBI_Max_Bad_Attempts)

アカウントのステータスをロックに変更するまでに許可するログイン失敗回数を指定します。[ログインの設定] のチェックをオフにした場合、デフォルト値は 0 (ゼロ) です。この場合、ログイン回数に制限はありません。[ログインの設定] のチェックをオンにした場合、デフォルト値は 5 です。管理者は、別の値を入力または選択することができます。[ログインの設定] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

ロックアウト期間 (分) (IBI_Account_Lockout_Duration)

アカウントのステータスをロックからアクティブに変更するまでの時間を分単位で指定します。[ログインの設定] のチェックをオフにした場合、デフォルト値は 0 (ゼロ) です。[ログインの設定] のチェックをオンにした場合、デフォルト値は 3 分です。管理者は、別の値を入力または選択することができます。[ログインの設定] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

ロックアウト期間のリセット (分) (IBI_Account_Lockout_Duration_Reset)

[ログインの最大試行回数] 設定で指定したログイン最大回数の超過後、ログイン試行回数のカウンタを 0 (ゼロ) に戻すまでに必要な経過時間を分単位で指定します。指定可能な範囲は 1 分から 99,999 分です。[ログインの設定] のチェックをオフにした場合、デフォルト値は 0 (ゼロ) です。[ログインの設定] のチェックをオンにした場合、デフォルト値は 3 分です。管理者は、別の値を入力または選択することができます。[ログインの設定] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

パスワード期限切れまでの日数 (IBI_Password_Expire)

パスワードをアクティブにする日数を指定します。[ログインの設定] のチェックをオフにした場合、デフォルト値は 0 (ゼロ) です。この場合、パスワードは期限切れになりません。[ログインの設定] のチェックをオンにした場合、デフォルト値は 90 日です。パスワードが期限切れになると、ユーザは [パスワード期限切れの結果] (IBI_Password_Expire_Action) 設定で指定されたアクションを実行する必要があります。管理者は、別の値を入力または選択することができます。[ログインの設定] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

パスワード期限切れ警告までの日数 (IBI_Password_Expire_Warning)

期限切れの前に、ユーザに警告を表示する日数を指定します。[ログインの設定] のチェックをオフにした場合、デフォルト値は 0 (ゼロ) です。この場合、警告は表示されません。[ログインの設定] のチェックをオンにした場合、デフォルト値は 75 日です。この値は、[パスワード期限切れまでの日数] (IBI_Password_Expire) 設定に割り当てられた値以下にする必要があります。管理者は、別の値を入力または選択することができます。[ログインの設定] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

パスワード期限切れの結果 (IBI_Password_Expire_Action)

パスワード期限切れの際に必要なアクションを指定します。次のオプションのいずれかを選択します。

- パスワード期限切れユーザのログイン前にパスワードの変更を強制 (MUSTCHANGE) - これがデフォルト値です。

- パスワード期限切れユーザのステータスを非アクティブに変更 (DISABLE-USER) - ユーザは、管理者がパスワードをリセットするまでログインできません。

パスワードの複雑さを有効にする (IBI_Password_Complexity)

[内部] セキュリティページの [パスワードの設定] に割り当てるデフォルト値を指定します。

デフォルト設定では、このチェックはオフ (False) になっています。[パスワードの設定] セクションは無効 (選択不可) で、各設定には 0 (ゼロ) が表示されます。

このチェックをオン (True) にすると、[パスワードの設定] セクションの各設定が有効になり、これらの値を変更することができます。各設定には、構成済みの値が自動的に割り当てられます。

後からこのチェックをオフにすると、[パスワードの設定] セクションに割り当てられた値がすべて 0 (ゼロ) に戻り、これらの設定が無効になります。

このチェックをオン (True) にした場合、パスワードには次の要件も適用されます。

- パスワードの連続する 6 文字以上がユーザアカウント名またはユーザのフルネームの一部と一致しない。
- 長さが最低でも 6 文字、または [パスワードの最低の長さ] 設定で指定された長さのいずれか大きい方である。
- 次の 4 つのカテゴリのうち、3 つの文字を含む。
  - 英大文字 (A から Z)。
  - 英小文字 (a から z)。
  - 数字 (0 から 9)。
  - アルファベット以外の文字 (例、!、$、#、%)。
  - パスワードの複雑さの要件は、パスワードの変更または作成時に適用されます。

パスワードの最低の長さ (IBI_Password_Minimum_Length)

パスワードの最低の長さを定義します。[パスワードの複雑さを有効にする] のチェックをオフにした場合、デフォルト値は 0 (ゼロ) 文字です。[パスワードの複雑さを有効にする] のチェックをオンにした場合、デフォルト値は 6 文字です。[パスワードの複雑さを有効にする] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

パスワードの再使用 (IBI_Password_Reuse)

最近使用したパスワードの再使用を禁止する個数を指定します。たとえば、[パスワードの再使用] を 6 に設定した場合、新規パスワードを作成する際に、最近のパスワード変更 6 回分の履歴が追跡され、これらのパスワードの再使用が禁止されます。[パスワードの複雑さを有効にする] のチェックをオフにした場合、変更回数のデフォルト値は 0 (ゼロ) です。この場合、ユーザは以前に割り当てた任意のパスワードを再使用することができます。[パスワードの複雑さを有効にする] のチェックをオンにした場合、変更回数のデフォルト値は 2 です。[パスワードの複雑さを有効にする] のチェックをオンにした状態でこの設定のみを無効にするには、0 (ゼロ) を入力または選択します。

手順　ログイン設定を構成するには

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティ] ページの [セキュリティの構成] フォルダ下で、[内部] をクリックします。
3. [ログインの設定] のチェックをオンにします。

   [内部] ページに次のデフォルト値が表示されます。

   - ログインの最大試行回数 - 5
   - ロックアウト期間 (分) - 3
   - ロックアウト期間のリセット (分) - 3
   - パスワード期限切れまでの日数 - 90
   - パスワード期限切れ警告までの日数 - 75

4. これらの設定に割り当てられたデフォルト値を変更するには、各テキストボックスに別の値を入力または選択します。
5. すべての設定をクリアするには、[ログインの設定] のチェックをオフにします。すべての値が自動的に 0 (ゼロ) に戻ります。
6. [パスワード期限切れの結果] セクションでは、デフォルトオプションの [パスワード期限切れユーザのログイン前にパスワードの変更を強制] を受容するか、別オプションの [パスワード期限切れユーザのステータスを非アクティブに変更] をクリックします。
7. [内部] セキュリティページで設定の更新を継続するか、変更内容を保存します。

手順　パスワード設定を構成するには

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティ] ページの [セキュリティの構成] フォルダ下で、[内部] をクリックします。

3. [パスワードの複雑さを有効にする] のチェックをオンにします。

   [内部] ページに次のデフォルト値が表示されます。

   - パスワードの最低長さ - 6
   - パスワードの再使用 - 2

4. これらの設定に割り当てられたデフォルト値を変更するには、各テキストボックスに別の値を入力または選択します。
5. すべての設定をクリアするには、[パスワードの複雑さを有効にする] のチェックをオフにします。すべての値が自動的に 0 (ゼロ) に戻ります。
6. [内部] セキュリティページで設定の更新を継続するか、変更内容を保存します。

手順　内部セキュリティページの構成変更を保存するには

1. [内部] セキュリティページで構成の変更をすべて完了後、[保存] をクリックします。
2. 確認メッセージのダイアログボックスで [OK] をクリックします。
3. キャッシュのクリアを要求するメッセージで [OK] をクリックします。
4. 管理コンソールのメニューバーの [キャッシュのクリア] をクリックし、確認メッセージで [OK] をクリックします。

外部セキュリティページ設定の理解

[外部] ページは、TIBCO WebFOCUS 外部のディレクトリでセキュリティを構成する場合に使用します。

外部セキュリティを有効にする
このチェックをオンにすると、内部セキュリティ設定が無効になり、このページで指定した外部システムに、すべての認証アクティビティおよび認可が委任されます。このチェックボックス下側のセクションでテキストボックスおよび機能が有効になり、管理者が選択した値に応じて表示内容が変わります。

外部セキュリティタイプ (IBI_Authentication_Type)
このドロップダウンリストには、次の値が表示されます。

- **Reporting Server** (現在、この項目の説明はありません)
- **Legacy LDAP**　AD または LDAP ディレクトリを使用してユーザを認証します。技術サポートから指示がない限り、このオプションは選択しないでください。
- **Custom Java Plug-In** (このオプションは現在利用できません)　技術サポートから指示がない限り、このオプションは選択しないでください。

Reporting Server ノード
外部認証プロバイダアプリケーションとの通信を管理する Reporting Server の名前を指定します。

サーバ管理者 ID
外部セキュリティサーバの管理者 ID を指定します。[ユーザ認可] セクションを使用可能にするには、このテキストボックスに、外部セキュリティサーバで定義済みの有効なユーザ ID を入力する必要があります。通常、インストール時にサーバ管理者に割り当てたユーザ ID です。

パスワード
外部セキュリティサーバの管理者に割り当てられたパスワードを指定します。外部セキュリティサーバの管理者 ID とパスワードの有効性を確認するには、[接続] をクリックします。有効な ID とパスワードが送信されると、[ユーザ認可] セクションが使用可能になります。

ユーザ認可
ユーザ認可を管理する場所を指定します。このセクションのオプションおよびチェックボックスは、[サーバ管理者 ID] テキストボックスに有効なユーザ ID とパスワードを入力し、[接続] をクリックした後に使用可能になります。

- **内部** ユーザ認可タスクのすべてを TIBCO WebFOCUS で管理します。
- **内部と外部** 認可タスクの管理を TIBCO WebFOCUS と外部アプリケーションで分担します。
- **外部のみ** ユーザ認可タスクのすべてを外部アプリケーションで管理します。
- **グループプロバイダ優先** このチェックをオンにした場合、チェックボックス横のテキストボックスで、グループ認可を上書きする外部プロバイダを指定します。

  注意：このチェックボックスは、[内部と外部] または [外部のみ] オプションを選択した場合にのみ表示され、[グループプロバイダ優先] チェックボックスとともにテキストボックスが有効になります。

ログイン時にアカウントを作成
初回のログイン試行時に作成するユーザアカウントの範囲を指定します。

- **All** 初回のログイン試行時に、すべてのユーザのアカウントを作成します。
- **Mapped External Groups** 初回のログイン試行時に、マッピングされた外部グループのユーザのみのアカウントを作成します。
- **OFF** ユーザアカウントの自動作成を無効にします。

ユーザ情報の同期

TIBCO WebFOCUS へのログイン時に [説明] および [Email] テキストボックスのユーザ情報を自動取得する機能を有効にします。これにより、常に最新のユーザ情報が取得されます。

このチェックをオフにすると (デフォルト設定)、ユーザがログインした際にそのユーザの [説明] および [Email] テキストボックスは更新されません。

このチェックをオンにすると、ユーザがログインした際にそのユーザの [説明] および [Email] テキストボックスが更新されます。次のオプションのいずれかを選択して、この情報のソースを指定します。

- **認証プロバイダを使用**　このオプションを選択すると、[説明] および [Email] テキストボックスの最新情報が認証プロバイダから取得されます。このオプションは、デフォルト設定で選択されています。
- **認可プロバイダを使用**　このオプションを選択すると、[説明] および [Email] テキストボックスの最新情報が認可プロバイダから取得されます。

外部セキュリティが使用されている限り、この設定に割り当てられた値は、フォームベース認証および事前認証を使用するセキュリティゾーンにログインする各ユーザに同等に適用されます。

詳細設定の使用

管理コンソールの [セキュリティ] タブの [詳細] ページでは、WebFOCUS インストール全体に適用される特定の管理ユーザ ID、パスワード、その他のセキュリティ機能を指定する設定にアクセスすることができます。

[詳細] ページの設定では、匿名ユーザの ID を指定することができます。これは、ログイン画面からユーザが [パブリックアクセスリンク] を選択した際に呼び出されます。また、このページの設定では、ルートユーザの ID とパスワードを指定することもできます。ルートユーザは、WebFOCUS への無制限アクセスを保持するスーパーユーザです。ルートユーザは、他のすべてのユーザがロックアウトされた場合や、システムの保守管理としてすべてのアクセス権限を必要とする場合の代替ユーザとして機能します。

同一ユーザによる多重ログイン (IBI_MULTIPLE_LOGINS_PER_USER)

同一ユーザによる複数ログインセッション (認証済み) を同時に許可するかどうかを指定します。このチェックがオンの場合 (True)、ユーザは、複数の認証済みセッションを同時に開くことができます。このチェックがオフの場合 (False)、ユーザは、一度に単一の認証済みセッションのみ開くことができます。

ルートユーザ (IBI_ADMIN_NAME)

管理者またはスーパーユーザのユーザ ID を指定します。[ルートユーザ] (IBI_Admin_Name) および [ルートパスワード] (IBI_Admin_Pass) を設定した場合、システム内で設定されている他のポリシーに関係なく、このユーザにはすべての権限が付与されます。通常、この ID は特定の状況でのみ使用し、必要のなくなった時点で削除します。

ルートパスワード (IBI_ADMIN_PASS)

管理者またはスーパーユーザのパスワードが格納されます。

Reporting Server 匿名ユーザ ID (IBI_ANONYMOUS_WFRS_USER)

WebFOCUS Client が WebFOCUS Reporting Server に接続して匿名 (未認証) リクエストを処理する際に使用するユーザ ID を指定します。このユーザ ID は、パブリックユーザとしてログインする際に使用されます。Reporting Server の構成についての詳細は、89 ページの 「 TIBCO WebFOCUS Reporting Server の設定 」 を参照してください。

Reporting Server 匿名パスワード (IBI_ANONYMOUS_WFRS_PASS)

Reporting Server への接続に使用する匿名ユーザのパスワードを指定します。これは、すべての認証タイプに適用されます。このユーザ ID は、パブリックユーザとしてログインする際に使用されます。

匿名ユーザ ID (IBI_ANONYMOUS_USER)

WebFOCUS Client が未認証リクエストに使用するユーザ ID を指定します。デフォルト値は public です。

デフォルト設定で、WebFOCUS Client は Anonymous グループのユーザに使用可能なリソース、および WebFOCUS Reporting Server 上のプロシジャへの匿名アクセス (未認証アクセス) をサポートします。この設定で指定されたユーザが使用する Reporting Server 認証情報は、[Reporting Server 匿名ユーザ ID] (IBI_Anonymous_WFRS_User) および [Reporting Server 匿名ユーザパスワード] (IBI_Anonymous_WFRS_Pass) で指定します。

匿名外部ユーザ (IBI_ANONYMOUS_EXTERNAL_USER)

この値を設定する場合は、外部セキュリティプロバイダから匿名ユーザの認可情報を取得する際に使用するユーザ ID を指定します。

匿名ユーザ名 (IBI_NAMED_ANONYMOUS_USERS)

このチェックがオン (True) に設定され、現在の WebFOCUS 環境で外部認証または事前認証が使用される場合は、指定された匿名ユーザによるログインが許可されます。このユーザがリポジトリに存在せず、IBI_ALLOW_LOGIN_EXTERNAL_GROUPS 設定にも該当しない場合、ログインは成功しますが、このユーザには WebFOCUS 内のパブリックユーザと同一の認可が与えられます。このユーザは、データベースには追加されません。また、いずれのグループにも追加できず、共有相手として指定することもできません。このようなユーザは WebFOCUS 内ではパブリックユーザと見なされますが、そのユーザ ID はセッションモニタで追跡されます。Reporting Server 上での認可は、明示的なユーザ ID に基づいて決定されます。デフォルト値は False (チェックオフ) です。

このユーザが WebFOCUS に登録されているが、IBI_ALLOW_LOGIN_EXTERNAL_GROUPS 設定に該当しない場合、このユーザは引き続き指定された匿名ユーザとして扱われます。

パスワードの変更を有効にする (IBI_USER_PASSWORD_CHANGE)

デフォルト値は True です (チェックオン)。この設定では、ユーザが各自のパスワードを変更することができます。特定の状況下では、この機能を無効にしたい場合があります。たとえば、使用中のシステムでユーザ認証を外部システムに依存し、ユーザが WebFOCUS で各自のパスワードを変更できないようにする場合があります。

グループ管理者によるユーザの作成時にネームスペースを追加 (IBI_USER_NAMESPACE)

グループ管理者が管理対象のグループでユーザを作成できるマルチテナント展開で使用します。この設定では、グループ管理者がユーザを作成する際に、ネームスペースを接頭語または接尾語としてユーザ名に追加するかどうかを指定します。

- [(なし)] に設定すると (デフォルト設定)、ユーザ名にネームスペースは追加されません。
- [プレフィックス] に設定すると、ユーザ名の先頭にネームスペースと円記号 (¥) が追加されます。

  たとえば、グループ管理者が「tenant1¥groupadmin」としてログインした場合、このグループ管理者のネームスペース、およびこのグループ管理者が管理するユーザすべてのネームスペースは「tenant1」になります。ユーザを作成すると、新しいユーザ名の先頭にグループ管理者のネームスペースが自動的に追加され、ユーザ名が「tenant1¥username」として作成されます。
- [サフィックス] に設定すると、ユーザ名の末尾に @ 記号とネームスペースが追加されます。

  たとえば、グループ管理者が「groupadmin@tenant1.com」としてログインした場合、そのグループ管理者のネームスペースは「tenant1.com」になります。ユーザを作成すると、新しいユーザ名の末尾にグループ管理者のネームスペースが自動的に追加され、ユーザ名が「username@tenant1.com」として作成されます。

ネームスペースを使用することで、複数のグループでユーザに同一名が割り当てられた場合の競合が回避できるとともに、ユーザを複数のテナントグループに割り当てる SaaS 実装がサポートされます。

セキュリティゾーンの構成

[セキュリティ] タブでは、4 つのセキュリティゾーンのそれぞれで使用する事前認証タイプを構成することができます。[セキュリティゾーン] フォルダ下のページでは、各セキュリティゾーンの構成を表示、更新することができます。

4 つのゾーンは次のとおりです。

- **デフォルトゾーン**　その他 3 つのゾーンで処理されないリクエストすべての認証方法を定義します。
- **モバイルゾーン**　WebFOCUS Mobile App などの WebFOCUS モバイル製品の認証方法を定義します。
- **ポートレットゾーン**　SharePoint などの WebFOCUS Open Portal Services 製品の認証方法を定義します。
- **代替ゾーン**　同一の WebFOCUS 環境でリクエストに使用する代替認証方法を定義します。

デフォルトゾーン構成の理解

デフォルトゾーンでは、ほとんどのユーザに適用される認証タイプを設定します。

[デフォルトゾーン] の [認証] ページは、デフォルト設定で [フォームベース認証] および [匿名認証] 設定を受容するよう構成されています。フォームベース認証セキュリティは、内部ポータルセキュリティまたは外部セキュリティ (WFRS) に基づいて有効にすることができます。[フォームベース認証] 設定を有効にすると、ユーザが WebFOCUS にアクセスするたびにログインページがユーザに提示されます。匿名認証プロファイルで定義されたパブリックユーザにより、パスワードの有無に関係なく、WebFOCUS ですべてのユーザが受容可能になります。このデフォルト構成により、ユーザの範囲が最大になります。ただし、管理者はこのページで各認証方法の有効と無効を切り替えることで、ユーザの要件に応じて、この構成を最適な認証レベルにまで上げることができます。

[デフォルトゾーン] の [リクエスト一致] ページは、[リクエスト URL パターン] および [IP アドレスパターン] で指定されたパターンをすべて受容するよう構成されています。[リクエスト一致] ページは、このデフォルトゾーンに使用する IP アドレスを編集する以外は、変更しないことをお勧めします。

モバイルゾーン構成の理解

[モバイルゾーン] では、モバイルデバイスから WebFOCUS にアクセスするユーザに要求される、高度なセキュリティレベルに適した認証方法が提供されます。このゾーンでは、管理者はモバイルユーザに対して、WebFOCUS 内で設定された認証方法のいずれかを設定することができます。

[モバイルゾーン] の [認証] ページは、デフォルト設定で [フォームベース認証] および [Remember Me 認証] 設定を受容するよう構成されています。これらの設定では、ユーザが WebFOCUS にアクセスするたびにログインページが表示されます。また、[Remember Me 認証] プロファイルにより、複数セッション間で WebFOCUS へのトラステッドアクセスが保持されます。管理者は、このページの各認証方法を有効または無効にすることができます。

[モバイルゾーン] の [リクエスト一致] ページでは、リクエスト URL が「/MobileController/**」と「/MobileFavsController/**」の 2 パターンに制限されます。リクエスト URL パターンおよび IP アドレスは、追加することも、削除、編集することもできません。

ポートレットゾーン構成の理解

[ポートレットゾーン] では、WebFOCUS Open Portal Services 製品 (例、SharePoint) から WebFOCUS にアクセスするリモートユーザに要求される、高度なセキュリティレベルに適した認証方法が提供されます。

[ポートレットゾーン] の [認証] ページは、デフォルト設定で [フォームベース認証] および [Remember Me 認証] 設定を受容するよう構成されています。これらの設定では、ユーザが WebFOCUS にアクセスするたびにログインページが表示されます。また、[Remember Me 認証] プロファイルにより、複数セッション間で WebFOCUS へのトラステッドアクセスが保持されます。管理者は、このページの各認証方法を有効または無効にすることができます。

[ポートレットゾーン] の [リクエスト一致] ページでは、リクエスト URL が「/tool/portlets/**」のパターンのみに制限されます。リクエスト URL パターンおよび IP アドレスは、追加することも、削除、編集することもできません。

代替ゾーン構成の理解

[代替ゾーン] を使用すると、管理者がデフォルトゾーンとは異なる認証方法でログインすることができます。管理者は、[代替ゾーン] を使用して認証方法をカスタマイズし、その認証方法をユーザサポートに使用することができます。

[代替ゾーン] の [認証] ページは、デフォルト設定で [フォームベース認証] 設定を受容するよう構成されています。この設定では、ユーザがセッションを開始するたびにログインページが表示されます。管理者は、このページの各認証方法を有効または無効にすることができます。代替認証方法を設定するには、2 つのデフォルト方法を無効にし、デフォルトゾーンで使用されていない方法を有効にします。

[代替ゾーン] の [リクエスト一致] ページでは、リクエスト URL パターンおよび IP アドレスパターンを追加して、認証をサポートする有効な URL の範囲を制限することができます。デフォルト設定では、[リクエスト URL パターン] には、任意の URL レイアウトをすべて受容する「/**」パターンが表示されます。[クライアント/最終プロキシの IP アドレス] パターンページには、「127.0.0.1」、「0:0:0:0:0:0:0:1」および「::1」の 3 パターンが表示されます。これらは、それぞれ IPV4 および IPV6 でのローカルホスト IP を表します。

セキュリティゾーンの有効化

[代替ゾーン] 以外のセキュリティゾーンはすべて、デフォルト設定で有効になっています。[代替ゾーン] を使用するには、このゾーンを有効にする必要があります。セキュリティゾーンを有効にするには、[セキュリティゾーン] ページでそのゾーンのステータスを [無効] から [有効] に変更します。

手順 **セキュリティゾーンを有効にするには**

1. [セキュリティゾーン] ページで、[無効] に設定されているセキュリティゾーンエントリの任意の位置をクリックし、[アクション] セクションで [有効にする] をクリックします。

   ステータスが [無効] から [有効] に変更され、そのセキュリティゾーンが使用可能になります。

認証ページの使用

[認証] ページでは、セキュリティゾーン内で使用可能にする認証方法を定義します。各ゾーンのデフォルト設定では、それぞれのゾーンでよく使用されるユーザ認証方法が指定されていますが、管理者は、[認証] ページでこれらの認証方法を別の認証方法に置き換えたり、他の認証方法で補足したりすることができます。

各認証方法には、それぞれ固有の構成があり、ユーザの認証方法が異なります。特定のゾーン内で使用可能な認証方法は、[有効] (チェックマーク付き) ステータスで識別されます。使用不可の認証方法は、[無効] ステータスで識別されます。

[認証] ページの [アクション] セクションには、特定ゾーンのすべての認証方法に影響する各種ダイアログボックスおよびアクションへのリンクが表示されます。[セキュリティゾーン] セクションには、認証ページ設定の [保存]、[エクスポート]、[インポート] のリンクが表示されます。

[オプション] リンクをクリックすると、[認証オプション] ダイアログボックスが開きます。管理者は、このダイアログボックスで、WebFOCUS からログアウトしたユーザの移動先を示すカスタム URL を指定することができます。

[キー管理] リンクをクリックすると、[キー管理] ダイアログボックスが開きます。管理者は、このダイアログボックスで、証明書ベースの認証方法をサポートするセキュアキーを識別するためのキーストアファイルのパスを構成することができます。

[CORS 設定] リンクをクリックすると、[CORS 設定] ダイアログボックスが開きます。管理者は、このダイアログボックスで、WebFOCUS リソースを外部アプリケーションで使用できるよう構成することができます。これにより、外部アプリケーションの Web ページに WebFOCUS コンテンツおよびリソースを埋め込むことで、外部アプリケーションでの WebFOCUS ビジネスインテリジェンスの活用が可能になります。このダイアログボックスの [埋め込みの許可] のチェックをオンにすると、カンマ区切りホワイトリスト URL で指定された Web ページへの WebFOCUS リソースの埋め込みがサポートされます。[CORS (クロスオリジンリソース共有) の許可] のチェックをオンにすると、カンマ区切りホワイトリスト URL を使用するユーザが埋め込み WebFOCUS リソースをインタラクティブ操作するための Ajax リクエストおよびレスポンスメッセージの使用がサポートされます。クロスオリジン設定の構成は、各ゾーンでそれぞれ独立して管理されます。

[有効にする] / [無効にする] リンクをクリックして、[無効] に設定されている認証方法を有効にしたり、[有効] に設定されている認証方法を無効にしたりできます。このリンクは、認証方法のいずれかを選択した後にのみ使用可能になります。

[編集] リンクをクリックすると、選択した認証方法をサポートするダイアログボックスが開きます。このダイアログボックスで、その認証方法で必要な構成設定を作成または更新することができます。このリンクは、認証方法のいずれかを選択した後にのみ使用可能になります。

手順　認証方法を有効にするには

1. [認証] ページで、[無効] に設定されている認証方法エントリの [名前] または [ステータス] 列を右クリックし、[有効にする] を選択します。

   または

2. [無効] に設定されている認証方法エントリの任意の位置をクリックし、[アクション] セクションで [有効にする] をクリックします。

ステータスが [無効] から [有効] (チェックマーク付き) に変更され、その認証方法がセキュリティゾーンで使用可能になります。

手順　認証方法を無効にするには

1. [認証] ページで、[有効] に設定されている認証方法エントリの [名前] または [ステータス] 列を右クリックし、[無効にする] を選択します。

   または

2. [有効] に設定されている認証方法エントリの任意の位置をクリックし、[アクション] セクションで [無効にする] をクリックします。

   ステータスが [有効] から [無効] (チェックマークなし) に変更され、その認証方法がセキュリティゾーンで使用不可になります。

手順　認証ページの変更を保存するには

1. [認証] ページの [アクション] セクションで、[セキュリティゾーン] 下の [保存] をクリックします。
2. 確認メッセージのダイアログボックスで [OK] をクリックします。
3. Web アプリケーションの再ロードを要求するメッセージダイアログボックスで [OK] をクリックします。
4. 現在のセッションからログアウトし、管理者として再度ログインして、管理コンソールに戻ります。
5. [セキュリティ] タブをクリックし、[セキュリティゾーン] フォルダ下で、構成済みゾーンの [認証] をクリックします。

   新しい設定または更新された設定が、構成済みの設定として表示されます。

手順　カスタムログアウトアドレスを構成するには

各セキュリティゾーンは、デフォルト設定でフォームベース認証を使用するよう構成されています。フォームベース認証のセキュリティゾーンでユーザがログアウトすると、ログアウトページが開き、ユーザをログインページに誘導するリンクが表示されます。一方、外部認証または事前認証を使用するゾーンでは、ログアウト後にユーザをログインページに誘導する必要はありません。これらのゾーンでは、カスタムログアウトアドレスを構成することで、デフォルトログアウトページを表示する代わりに、代替ログアウトページの URL に置き換えることができます。

1. [認証] ページの [アクション] セクションで、[オプション] をクリックします。

2. [認証オプション] ダイアログボックスで、[カスタムログアウトターゲット URL を有効にする] のチェックをオンにします。
3. カスタムログアウトターゲット URL を入力します。
   - セキュリティゾーンが IWA (Integrated Windows Authentication) を使用するよう構成されている場合は、デフォルトのログアウト URL の「/signout」を受容します。
   - セキュリティゾーンが他社製の事前認証プロバイダを使用するよう構成されている場合は、そのプロバイダの SSO 製品セッションを終了するログアウト URL を入力します (URL が存在する場合)。たとえば、WebSeal では、ログアウト URL を次のように指定します。

     ```
     http://webseal.domain.com/pkmslogout
     ```

     SiteMinder では、URL を次のように指定します。

     ```
     http://siteminder.domain.com/logout.html
     ```

     シングルサインオン環境で作業しているユーザを元のポータルに自動的に戻すには、末尾の語句をブランクにします。たとえば、WebSeal では、ログアウト URL を次のように指定します。

     ```
     http://webseal.domain.com
     ```

4. [OK] をクリックします。

許可するホスト名リストの管理

WebFOCUS の内部通信では、ユーザリクエストは、HTTP リクエストメッセージの形式でブラウザから WebFOCUS Reporting Server に送られます。通常、HTTP リクエストメッセージは、仮想ホストの URL (リクエストを処理するサーバでホストされるアプリケーションまたは Web サイト) をホストヘッダフィールドで特定する必要があります。正規ユーザからのメッセージでは、ターゲットサーバ上の既存のホストの URL が特定されます。一方、潜在的な攻撃者からのメッセージでは、ターゲットサーバに存在しないホストの URL が特定できます。

HTTP リクエストメッセージのホストヘッダ URL の認証を必要としないサーバでは、通常、未定義ホストの URL を含むリクエストは、最初に処理可能なホストアプリケーションにリダイレクトされます。次に、このホストが認識されない URL を含むメッセージを処理し、Web キャッシュの [Location] フィールドの正当な URL に置き換え、この有害なコンテンツを含むメッセージをキャッシュから返します。後続のメッセージはすべて、攻撃者により導入された URL にリダイレクトされ、サーバから悪意のあるコードを含むメッセージが送信者に返されます。

これらの HTTP レスポンスヘッダインジェクション攻撃を防御するため、管理者は、アクティブセキュリティゾーンごとに有効なホスト名のホワイトリストを作成する必要があります。作成後は、リクエストメッセージからのホストヘッダ URL に対し、このホワイトリストで検証することができます。

ホワイトリストの作成後、WebFOCUS Reporting Server は、このリスト上の URL を含む HTTP リクエストメッセージのみを受容し、他のすべてのメッセージに対しては、リソースが正常に処理できませんでしたというエラーメッセージを返します。

管理者は、[認証オプション] ダイアログボックスの [許可するホスト名] フィールドに、組織で許可されたホスト名のリストを定義することができます。デフォルト設定では、このフィールドにアスタリスク (*) がワイルドカードとして表示され、すべてのホスト名 URL にリダイレクトされる HTTP リクエストメッセージを受容します。WebFOCUS Reporting Server で受容される前に、HTTP リクエストヘッダのホスト名を検証する独立したアプリケーションを導入済みの場合のみ、このオプションを受容することをお勧めします。

手順　許可するホスト名リストを構成するには

セキュリティゾーン内の HTTP リクエストメッセージの受容を、WebFOCUS Reporting Server 上の既存の仮想ホストの URL を含むリクエストに制限するには、管理者は、[認証オプション] ダイアログボックスの [許可するホスト名] フィールドのアスタリスク (*) ワイルドカード文字を、WebFOCUS Reporting Server 上に存在する仮想ホスト、Web サイト、アプリケーションの URL のカンマ区切りホワイトリストで置き換える必要があります。HTTP リクエストメッセージのホストヘッダフィールドの URL が受容されるためには、このリストの URL と一致する必要があります。

1. 管理コンソールで [セキュリティ] タブを選択します。
2. [セキュリティ] タブで、[許可するホスト名] リストを構成するセキュリティゾーンのフォルダを展開し、[認証] ページノードを選択します。
3. [認証] ページの [アクション] セクションで [オプション] を選択し、[認証オプション] ダイアログボックスを開きます。
4. WebFOCUS Reporting Server で定義され、HTTP リクエストメッセージの処理が許可された各仮想ホストの URL を [許可するホスト名] フィールドに入力します。

   ❑ 完全修飾 URL を入力して単一ホスト名を示すことができます。たとえば、「www.samplehost.com」と入力します。完全修飾 URL との一致は完全一致で、大文字と小文字が区別されます。

- ホスト名の範囲を表すために、ワイルドカードとしてピリオド (.) を使用することもできます。 たとえば、.ibi_apps.com URL のワイルドカードは www.ibi_apps.com、www.server1.ibi_apps.com、および ibi_apps.com の前に文字を含むその他の URL と一致します。
- このフィールドに複数の URL を表示する場合は、各 URL をカンマ (,) 区切りで入力します。

5. 期限切れまたは許可切れの URL は削除します。
6. [OK] を選択してリストを保存します。
7. [認証] ページの [セキュリティゾーン] セクションで、[保存] を選択します。
8. 「Web セキュリティ構成データは正常に保存されました」というメッセージで、[OK] をクリックします。
9. 「これらの変更を有効にするには、Web アプリケーションを再起動してください」というメッセージで、[OK] をクリックします。
10. 現在のセッションからログアウトします。
11. WebFOCUS Reporting Server を停止し、再起動します。
12. 管理者として再度ログインし、新しい構成をテストします。

クロスオリジン設定の構成

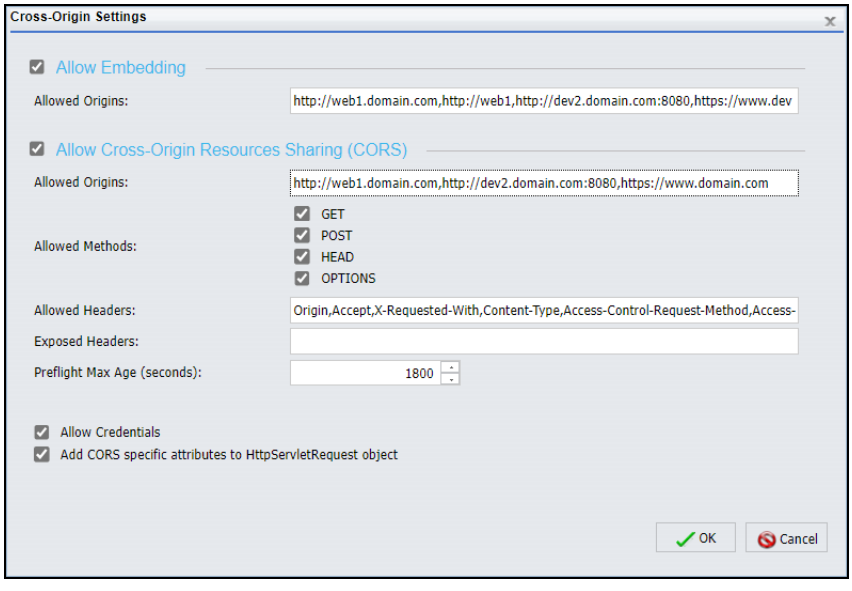
外部アプリケーションの Web ページに WebFOCUS コンテンツおよびリソースを埋め込むことで、外部アプリケーションでの WebFOCUS ビジネスインテリジェンスの活用が可能になります。たとえば、カスタマサービスを提供するための外部アプリケーションに、WebFOCUS でデザインされた作成済みポータルを埋め込むことで、カスタマサービスの評価指標やアカウントサービスの履歴情報にレポート、グラフ、分析リソースを追加することができます。

ただし、提供元が不明または未承認の外部アプリケーションから要求される WebFOCUS リソースやコンテンツの埋め込みリクエストから WebFOCUS を保護するために、デフォルト設定では埋め込みを許可しないよう構成されています。管理者は、[CORS 設定] ダイアログボックスの [埋め込みの許可] のチェックをオンにすることで、このデフォルト構成を無効にし、信頼される外部アプリケーションの Web ページ内のフレームまたは iframe にポータルやページなどのリソースを埋め込むリクエストを受容するよう WebFOCUS を構成することができます。

また、外部アプリケーションに埋め込まれた WebFOCUS コンテンツやリソースのインタラクティブ操作を可能にすることで、外部アプリケーションでの WebFOCUS ビジネスインテリジェンスの活用を可能することもできます。埋め込みアプリケーションユーザのブラウザから発行される非同期 Ajax リクエストは、WebFOCUS リソースやコンテンツを動的に取得または更新するため、常に最新情報が提供されるとともに、埋め込みコンテンツのインタラクティブなユーザ操作が可能になります。

クロスオリジンリソース共有 (CORS) を有効にすると、Web ページからリクエストを送信し、リソースの作成元ドメインの外部にある別のドメインから、制限されたリソースを取得することができます。クロスオリジンリソース共有のポリシー構成を使用して、Web ページに別のドメインからのクロスオリジンイメージ、スタイルシート、スクリプト、iframe、ビデオを埋め込むことを許可する一方で、より慎重を要するクロスドメインリクエスト (例、Ajax リクエスト) を禁止することができます。このポリシー構成では、リソース側でクロスオリジンリクエストを特定のドメインやメッセージに制限できるため、CORS 基準では、クロスオリジンリクエストの許可が安全かどうかを判断するために、ブラウザとサーバがどのように交信できるかを示した方法が定義されています。この方法では、同一オリジンリクエストより自由度や機能性が高くなりますが、単純にすべてのクロスオリジンリクエストを許可するより安全になります。これは、W3C コンソーシアムの勧告基準です。詳細は、https://en.wikipedia.org/wiki/cross-origin_resource_sharing、および W3C コンソーシアムから提供される CORS 推奨事項 (http://www.w3.org/TR/cors/) を参照してください。

下図のように、WebFOCUS で埋め込みの使用およびクロスオリジンリソース共有の使用を有効するには、[CORS 設定] ダイアログボックスを使用します。[埋め込みの許可] のチェックをオンにすると、外部 Web ページのフレームまたは iframe 内にコンテンツを埋め込むためのリクエストがサポートされます。[CORS (クロスオリジンリソース共有) の許可] のチェックをオンにすると、Ajax クロスオリジンリソース共有リクエストの使用がサポートされます。



注意：[CORS 設定] ダイアログボックスには [埋め込みの許可] チェックボックスと [CORS (クロスオリジンリソース共有) の許可] チェックボックスの両方が表示され、これらが連動して埋め込み BI アプリケーションの要件全体をサポートしますが、これらの 2 つの設定は互いに独立しています。たとえば、クロスオリジンリソース共有は使用するが、フレームまたは iframe に WebFOCUS コンテンツを埋め込む必要がない外部アプリケーションをサポートするよう WebFOCUS を構成することができます。別の例として、フレームまたは iframe にポータルを埋め込むが、クロスオリジン Ajax リクエストを使用しない単純なアプリケーションをサポートするよう WebFOCUS を構成することもできます。

オリジンの定義

クロスオリジンリソース共有の標準仕様では、オリジンは、URL のスキーム、ホスト、ポートで定義されます。スキームは、ホストのプロトコルを識別し、通常は「http://」または「https://」です。ホストは、ホストの登録名 (ホスト名を含むが、ホスト名のみに限定されない)、またはホストの IP アドレスを識別します。ポートは、ホストの通信に使用されるエンドポイントを識別します。

これらの 3 つのコンポーネントが事実上同一であれば、その URL で同一のオリジンが定義されます。たとえば、次の例では、2 つ目のリソース URL のホストコンポーネントには追加のパス情報が含まれていますが、両方のリソースは同一のオリジンとして定義されます。

- http://example.com/
- http://example.com/path/file/

一方、次の例では、各リソースはそれぞれ異なるオリジンとして定義されます。

- http://example.com/
- http://example.com/8080/
- http://www.example.com/
- https://example.com:80/
- https://example.com/
- http://example.org/
- http://ietf.org/

上記の例では、各リソースではスキーム、ホスト、ポートの少なくとも 1 つのコンポーネントが異なります。詳細は、「https://tools.ietf.org/html/rfc6454」を参照してください。

埋め込みの許可

外部アプリケーション Web ページのフレームまたは iframe 内にコンテンツを埋め込むリクエストが許可されるかどうかは、[埋め込みの許可] チェックボックスで制御します。このチェックをオンにした場合、チェックボックス下側の [許可するオリジン] テキストボックスで、WebFOCUS コンテンツの埋め込みを許可するアプリケーションの範囲を定義します。

TIBCO WebFOCUS は、埋め込みコンテンツを要求するリクエストに応答して、WebFOCUS から送信するメッセージの X-Frame-Options ALLOW-FROM ヘッダまたは Content-Security-Policy ヘッダに特定の値を割り当てることで、埋め込みを許可または拒否します。使用されるレスポンスヘッダは、リソースを要求するブラウザのタイプに応じて異なります。[埋め込みの許可] チェックボックスおよびこのチェックボックスに関連する [許可するオリジン] テキストボックスの値は、これらのレスポンスヘッダに割り当てられます。

デフォルト設定では、[埋め込みの許可] のチェックはオフです。この設定では、WebFOCUS はレスポンスヘッダに SAMEORIGIN 値を割り当てます。これにより、外部アプリケーションのフレームまたは iframe 内への WebFOCUS リソースの埋め込みが防止されます。

[許可するオリジン] テキストボックスには、デフォルト設定でアスタリスク (*) ワイルドカード文字が入力されています。[埋め込みの許可] のチェックをオンにし、[許可するオリジン] テキストボックスにアスタリスク (*) ワイルドカード文字を入力した場合、レスポンスメッセージから ALLOW-FROM または Content-Security-Policy ヘッダが除外されます。これにより、すべての他社製アプリケーションでコンテンツの埋め込みが許可されます。

TIBCO WebFOCUS リソースの埋め込みを許可する外部アプリケーションの範囲を制限するには、[許可するオリジン] テキストボックスのアスタリスク (*) ワイルドカード文字の代わりに、TIBCO WebFOCUS がサポートする特定オリジンのホスト URL (カンマ区切りのホワイトリスト) を入力する必要があります。ホワイトリストの各 URL には、外部ホストのスキーム、ホスト名、ポートを含める必要があります。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

[埋め込みの許可] のチェックをオンにし、[許可するオリジン] テキストボックスに特定の URL または複数の URL のカンマ区切りホワイトリストを入力した場合、TIBCO WebFOCUS は [許可するオリジン] テキストボックスのホワイトリストをレスポンスヘッダに割り当てます。割り当てる値は、リクエストを発行したブラウザのタイプに応じて異なります。この設定により、そのホワイトリストで指定された特定のホストのみが TIBCO WebFOCUS コンテンツを埋め込むことができます。

埋め込みを許可するかどうかは、セキュリティゾーンごとに個別に指定することができます。この機能により、外部アプリケーションからのリクエストをサポートするセキュリティゾーンのみで埋め込みを許可し、サポートしないセキュリティゾーンでは埋め込みを禁止することができます。

[埋め込みの許可] 設定は、外部 Web ページのフレームまたは iframe 内へのコンテンツの埋め込みのみをサポートします。一方、[CORS (クロスオリジンリソース共有) の許可] 設定は、Web ページ内のリソースおよびコンテンツを取得または更新するクロスオリジンリクエストの使用をサポートします。詳細は、166 ページの 「 クロスオリジンリソース共有 (CORS) の有効化 」 を参照してください。

埋め込み BI アプリケーションについての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

手順　セキュリティゾーンで埋め込みを許可するには

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、埋め込み BI アプリケーションをサポートするゾーンの [認証] ノードをクリックします。

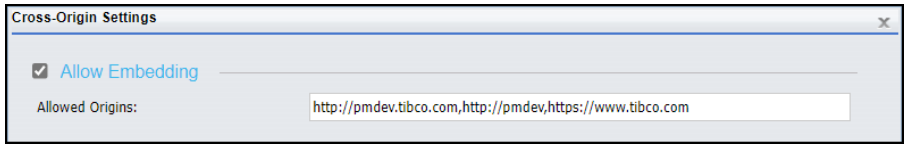
ほとんどの WebFOCUS 環境では、この構成をデフォルトセキュリティゾーンに割り当てますが、埋め込み BI アプリケーションのサポートにデフォルトセキュリティゾーンを使用しない環境では、代替セキュリティゾーンを使用することもできます。

3. [認証] ページで [CORS 設定] をクリックします。
4. 下図のように、[CORS 設定] ダイアログボックスで [埋め込みの許可] のチェックをオンにします。

5. すべてのアプリケーションからの HTTP リクエストおよびレスポンスを許可するには、[埋め込みの許可] チェックボックス下側の [許可するオリジン] テキストボックスのアスタリスク (*) ワイルドカード文字を受容します。
6. 特定のアプリケーションからの HTTP リクエストおよびレスポンスを許可するには、[埋め込みの許可] チェックボックス下側の [許可するオリジン] テキストボックスに、許可する各アプリケーションの URL を入力します。

   このテキストボックスに URL を入力する際は、次の要件を考慮する必要があります。

   - 各 URL には、スキーム (「http:」または「https:」) を含める必要があります。
   - 「http://hostname.domain.com」または「http://hostname」フォーマットの URL を使用してネットワーク上の Web サイトにアクセスする場合は、ホワイトリストに両方の URL を含める必要があります。
   - 下図のように、ホワイトリストに複数の URL を含める場合は、各 URL をカンマ (,) で区切る必要があります。



   - ポートは、デフォルトポート (http の場合は 80、https の場合は 443) を使用しない URL のみに追加します。ポート 80 は、すべての HTTP サービスのポートを識別し、ポート 443 は、すべての HTTP セキュアサービスのポートを識別します。そのため、URL のスキームが http で、ポートが 80 の場合は、ポートを含める必要はありません。同様に、スキームが https で、ポートが 443 の場合は、ポートを含める必要はありません。

7. [OK] をクリックします。

   外部アプリケーションのクロスオリジンリソース共有 (CORS) を有効にする方法については、168 ページの 「 セキュリティゾーンでクロスオリジンリソース共有を許可するには 」 を参照してください。

   埋め込み BI アプリケーションの構成についての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

クロスオリジンリソース共有 (CORS) の有効化

外部アプリケーションからコンテンツまたはリソースを要求するクロスオリジンリソース共有リクエストを TIBCO WebFOCUS で許可するかどうかは、[CORS (クロスオリジンリソース共有) の許可] チェックボックスで制御します。このチェックをオンにした場合、チェックボックス下側の [許可するオリジン] テキストボックスで、クロスオリジンリソース共有リクエストの送信を許可するアプリケーションの範囲を定義します。

TIBCO WebFOCUS は、クロスオリジンリソース共有を要求する Ajax メッセージに応答して、送信されるメッセージの Access-Control-Allow-Origin ヘッダに特定の値を割り当てることで、クロスオリジンリソース共有を許可または拒否します。このレスポンスヘッダに割り当てられる値は、[CORS (クロスオリジンリソース共有) の許可] チェックボックスの値、および関連する [許可するオリジン] テキストボックスの値に基づいて定義されます。

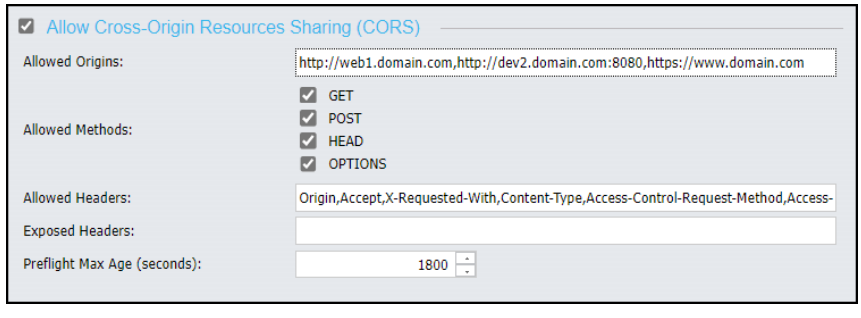
デフォルト設定では、[CORS (クロスオリジンリソース共有) の許可] のチェックはオフです。この設定では、TIBCO WebFOCUS はクロスオリジンリソース共有リクエストに対して HTTP 403 エラーメッセージで応答します。これにより、外部アプリケーションとの TIBCO WebFOCUS リソースの共有が防止されます。

[許可するオリジン] テキストボックスには、デフォルト設定でアスタリスク (*) ワイルドカード文字が入力されています。[CORS (クロスオリジンリソース共有) の許可] のチェックをオンにし、[許可するオリジン] テキストボックスにアスタリスク (*) ワイルドカード文字を入力した場合、TIBCO WebFOCUS はこのワイルドカード文字を Access-Control-Allow-Origin レスポンスヘッダに割り当てることで、リソースの共有をすべての外部アプリケーションに対して許可します。

TIBCO WebFOCUS リソースの共有を許可する外部アプリケーションの範囲を制限するには、[許可するオリジン] テキストボックスのアスタリスク (*) ワイルドカード文字の代わりに、TIBCO WebFOCUS がサポートする特定オリジンのホスト URL (カンマ区切りのホワイトリスト) を入力する必要があります。ホワイトリストの各 URL には、外部ホストのスキーム、ホスト名、ポートを含める必要があります。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

[CORS (クロスオリジンリソース共有) の許可] のチェックをオンにし、[許可するオリジン] テキストボックスに特定の URL または複数 URL のカンマ区切りホワイトリストを入力した場合、TIBCO WebFOCUS は Access-Control-Allow-Origin レスポンスヘッダに [許可するオリジン] テキストボックスのホワイトリストを割り当てます。この設定により、Ajax リクエストメッセージに応答して TIBCO WebFOCUS がリソースを共有するのは、そのホワイトリストで指定された特定のホストのみに制限されます。

下図のように、CORS の許可を有効にした後、残りの機能を使用して、セキュリティゾーンでサポートされる埋め込みアプリケーションのクロスオリジンリソース使用に対する標準的な保護を設定します。



このダイアログボックスの各種設定により、クロスオリジンリソース共有仕様でサポートされる機能のすべてが組み込まれます (例、URL、リクエストメソッド、ヘッダ、認証情報)。また、プレフライトリクエストが完了するまでの許容最大時間も定義します。

クロスオリジンリソース共有を許可するかどうかは、セキュリティゾーンごとに個別に指定することができます。この機能により、外部アプリケーションからのリクエストをサポートするセキュリティゾーンのみでクロスオリジンリソース共有を許可し、サポートしないセキュリティゾーンではクロスオリジンリソース共有を禁止することができます。

[CORS (クロスオリジンリソース共有) の許可] 設定は、Web ページ内のリソースおよびコンテンツを取得または更新するクロスオリジンリクエストの使用をサポートするのみです。一方、[埋め込みの許可] 設定は、外部アプリケーション Web ページのフレームまたは iframe 内にコンテンツを埋め込むリクエストをサポートします。詳細は、163 ページの 「 埋め込みの許可 」 を参照してください。

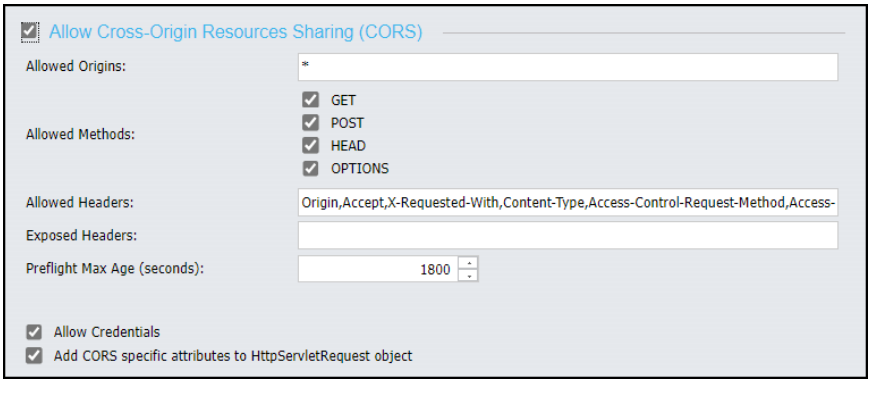
埋め込み BI アプリケーションについての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

手順　セキュリティゾーンでクロスオリジンリソース共有を許可するには

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、埋め込みアプリケーションをサポートするゾーンの [認証] ノードをクリックします。

   ほとんどの WebFOCUS 環境では、この構成をデフォルトセキュリティゾーンに割り当てますが、埋め込み BI アプリケーションのサポートにデフォルトセキュリティゾーンを使用しない環境では、代替セキュリティゾーンを使用することもできます。
3. [認証] ページで [CORS 設定] をクリックします。
4. [CORS 設定] ダイアログボックスで、[CORS (クロスオリジンリソース共有) の許可] のチェックをオンにします。

   下図のように、このダイアログボックスの各種設定が使用可能になります。



5. [CORS (クロスオリジンリソース共有) の許可] チェックボックス下側の [許可するオリジン] テキストボックスに、TIBCO WebFOCUS へのクロスオリジンリソース共有リクエストの発行を許可する各アプリケーションの URL を入力します。

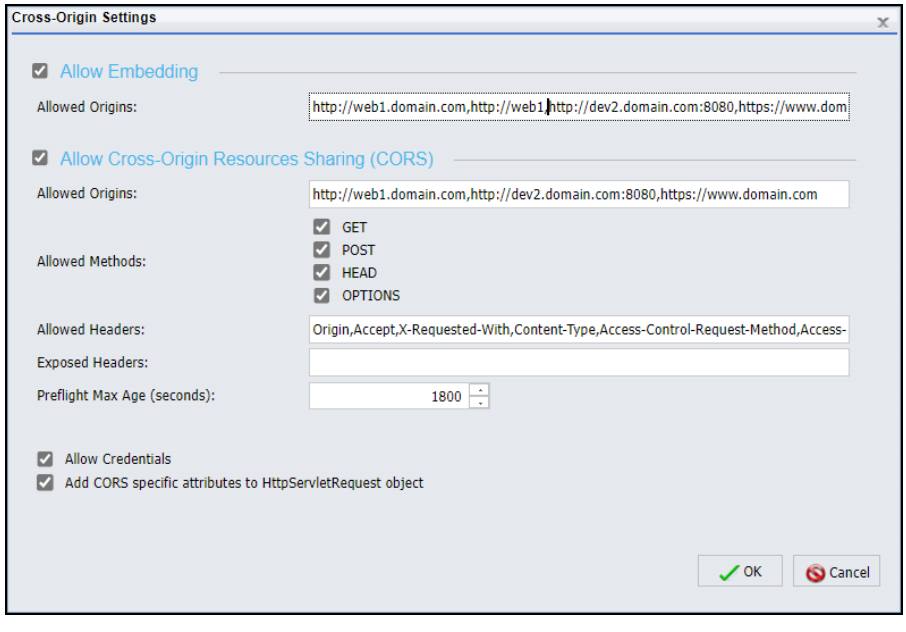
このテキストボックスに URL を入力する際は、次の要件を考慮する必要があります。

- 各 URL には、スキーム (「http:」または「https:」) を含める必要があります。
- 「http://hostname.domain.com」または「http://hostname」フォーマットの URL を使用してネットワーク上の Web サイトにアクセスする場合は、ホワイトリストに両方の URL を含める必要があります。
- 下図のように、ホワイトリストに複数の URL を含める場合は、各 URL をカンマ (,) で区切る必要があります。

- ポートは、デフォルトポート (http の場合は 80、https の場合は 443) を使用しない URL のみに追加します。ポート 80 は、すべての HTTP サービスのポートを識別し、ポート 443 は、すべての HTTP セキュアサービスのポートを識別します。そのため、URL のスキームが http で、ポートが 80 の場合は、ポートを含める必要はありません。同様に、スキームが https で、ポートが 443 の場合は、ポートを含める必要はありません。

6. 残りのすべてのテキストボックスおよびチェックボックスでは、割り当てられたデフォルト値を受容します。

構成が完了すると、ダイアログボックスは下図のようになります。



7. [OK] をクリックします。

   埋め込み BI アプリケーションの構成についての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

セキュリティゾーンでの HTTP Strict Transport Security (HSTS) の構成

[HTTP Strict Transport Security の設定] リンクから [HTTP Strict Transport Security の設定] ダイアログボックスが開き、選択したセキュリティゾーンで HSTS セキュリティポリシーの使用を実装することができます。このポリシーでは、各ユーザに割り当てられたブラウザと Application Server とのすべての通信に TSL (SSL) レベルのセキュリティの使用が要求されます。そのため、この設定は、TLS (SSL) セキュリティの使用が構成済みの組織にのみ関連します。詳細は、54 ページの 「 TIBCO WebFOCUS での SSL 構成 」 を参照してください。

HTTP Strict Transport Security (HSTS) ポリシーはサーバによるセキュリティ強化であり、すべての入力リクエストで HTTPS プロトコルの使用を要求します。このポリシーが有効な場合、Web サイトのホストサーバは、HTTPS プロトコルを使用しないブラウザからの最初のリクエストに対して、Strict-Transport-Security フィールドを含むレスポンスヘッダが表示されたメッセージを返します。レスポンスヘッダ内のこのフィールドは、このサーバでは、HTTPS 接続を使用しないブラウザからのリクエストが受容されないことを示します。

レスポンスヘッダには、このポリシーが適用される期間 (通常は 1 年間) を指定するフィールドも含まれます。このプロトコルを使用しないブラウザからの後続のリクエストでは、レスポンスにエラーメッセージが表示されます。

Strict-Transport-Security フィールドを含むレスポンスヘッダが表示されたメッセージを受信することで、ブラウザは、このサイトへのメッセージの送信には HTTPS プロトコルの使用が必要だと理解します。また、同一のサイト名を使用するが、このプロトコルの使用を要求しない他のサイトについては正規のサイトと認めず、リクエストは HTTPS プロトコルの使用を要求するサイトに自動的にリダイレクトされます。

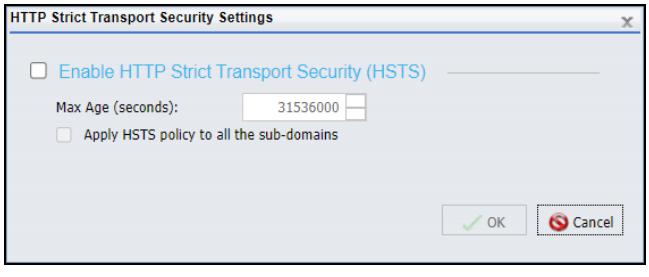
セキュリティゾーン内でこのポリシーを設定することで、このゾーンのユーザと Application Server 間のすべての通信に、この高度なセキュリティが導入されます。このポリシーでは、ゾーン内のすべての通信で HTTPS プロトコルを使用するようにします。そのため、これらの通信は暗号化され、パブリック鍵証明書で認証されます。また、これにより、このゾーンのユーザからのリクエストが、HTTPS プロトコルを要求しない非正規サイトに誤ってリダイレクトされることが回避されます。

[HTTP Strict Transport Security の設定] ダイアログボックスへのリンクおよびその構成は、管理コンソールの [セキュリティ] タブの [認証] ページに表示されます。このポリシーは構成されたゾーンにのみ適用されるため、適用するセキュリティゾーンごとにポリシーを設定する必要があります。ベストプラクティスとして、TSL (SSL) セキュリティを使用するよう構成された環境内のすべてのセキュリティゾーンで HSTS ポリシーを適用することをお勧めします。

HTTP Strict Transport Security の設定ダイアログボックスの理解

[HTTP Strict Transport Security の設定] ダイアログボックスでは、選択したセキュリティゾーンの HSTS ポリシーを有効にすることができます。追加の設定では、ポリシーを適用する期間、およびホストサーバ URL 内のサブドメインに送信されたメッセージにもこのポリシーを適用するかどうかを定義します。

HTTP Strict Transport Security は、デフォルト設定ではすべてのセキュリティゾーンで無効になっています。そのため、このダイアログボックスの機能は、[HTTP Strict Transport Security (HSTS) を有効にする] のチェックボックスを選択するまで使用不可になっています。



[HTTP Strict Transport Security (HSTS) を有効にする] チェックボックスを選択すると、[セキュリティ] タブの左側ウィンドウで選択したセキュリティゾーンの HSTS ポリシーが有効になります。このチェックをオンにすると、ダイアログボックスの他の機能が使用可能になります。

[最大期間 (秒)] のリストには、デフォルト設定で 1 年間の秒数が表示されます。この値は、組織の基準に準拠するよう増減させることができます。

[HSTS ポリシーをすべてのサブドメインに適用] のチェックは、デフォルト設定でオフになっています。ただし、Application Server をホストするサイトのすべてのサブドメインに送信されるメッセージで、HTTPS プロトコルの使用を要求するようにするためには、このチェックをオンにすることをお勧めします。

手順　セキュリティゾーンで HSTS セキュリティを構成するには

この構成は、内部通信で TLS (SSL) の使用を構成済みの場合のみ関係します。詳細は、54 ページの 「 TIBCO WebFOCUS での SSL 構成 」 を参照してください。

1. 管理者としてログインして管理コンソールを起動し、[セキュリティ] タブを選択します。
2. [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、HSTS を有効にするゾーンの [認証] ノードを選択します。

   TIBCO WebFOCUS が HTTPS を使用するよう構成されている場合、現在の環境で使用するすべてのセキュリティゾーンでこの機能を有効にすることをお勧めします。
3. [認証] ページで、[HTTP Strict Transport Security の設定] を選択し、[HTTP Strict Transport Security の設定] ダイアログボックスを開きます。
4. [HTTP Strict Transport Security (HSTS) を有効にする] のチェックをオンにします。
5. [最大期間 (秒)] テキストボックスで、デフォルト値の 31536000 を受容し、HTTP Strict-Transport-Security の 1 年間の使用を設定します。

   このテキストボックス右側の上下矢印を使用して、この値 (秒数) を調整することができます。
6. [HSTS ポリシーをすべてのサブドメインに適用] のチェックをオンにし、Application Server 内のサブドメインへのすべてのリクエストに対する HTTPS プロトコルの使用要件を追加します。
7. [OK] を選択し、構成を保存します。
8. 157 ページの 「 認証ページの変更を保存するには 」 の説明に従って、セキュリティゾーンへの変更を保存します。

リクエスト一致ページの理解

[リクエスト一致] ページでは、セキュリティゾーンの正規の URL および IP アドレスの範囲を定義します。このページには、[リクエスト URL パターン] および [クライアント/最終プロキシの IP アドレス] タブが表示されます。これらのタブでは、信頼できるユーザの URL および IP アドレスのパターンを識別します。パターンは、さまざまな URL および IP アドレスを含めた広範囲のパターンにすることも、有効なリクエストを少数の URL および IP アドレスに制限する厳密なパターンにすることもできます。セキュリティゾーンでの構成が完了すると、[リクエスト一致] ページの各タブで設定された信頼済み URL および IP アドレスのパターンに一致するリクエストメッセージのみが受容され、その他すべてのリクエストメッセージは除外されます。[リクエスト一致] ページを使用して、信頼できない送信元からのリクエストを除外することで、潜在的に悪意のあるリクエストから WebFOCUS 処理を保護することができます。

リクエスト URL パターンには、次の Java Ant パスパターンを使用します。

- URL パターンのすべての要素は、スラッシュ (/) で区切ります。
- 疑問符 (?) は、単一文字を表します。
- 1 つのアスタリスク (*) は、0 (ゼロ) 個以上の文字列を表します。
- 2 つのアスタリスク (**) は、パス内の 0 (ゼロ) 個以上のディレクトリ名を表します。

技術サポートの指示がない限り、このページの設定は変更しないでください。

リクエスト URL パターンタブの理解

[リクエスト URL パターン] タブでは、ユーザリクエストの正規の送信元として受容する URL の範囲を定義します。

このタブのデフォルト設定は、セキュリティゾーンごとに異なり、各ゾーンで要求されるセキュリティ制限の相違が反映されています。たとえば、モバイルセキュリティゾーンおよびポートレットセキュリティゾーンは、リモートサイトまたはポートレット経由で作業するユーザをサポートします。そのため、これらのデフォルト構成では、受容可能な URL の範囲が少数のパターンに厳しく制限されています。一方、デフォルトセキュリティゾーンおよび代替セキュリティゾーンは、社内のサイトで作業するユーザすべてをサポートし、デフォルト構成で適用される制限はほとんどありません。

クライアント/最終プロキシの IP アドレスタブの理解

[リクエスト URL パターン] および [クライアント/最終プロキシの IP アドレス] タブでは、ユーザリクエストの正規の送信元として受容する、クライアントとプロキシサイトの IP アドレスの範囲を定義します。プロキシサイト (プロキシサーバ) は、ユーザと Application Server 間で交信されるメッセージすべての中継点として機能するサーバです。

このタブのデフォルト設定は、セキュリティゾーンごとに異なり、各ゾーンで要求されるセキュリティ制限の相違が反映されています。デフォルトゾーン、モバイルゾーン、ポートレットゾーンでは、このタブに値は設定されていません。また、クライアントまたは最終プロキシの IP アドレスの評価に無関係な [追加]、[編集]、[削除] リンクは使用できません。

一方、代替セキュリティゾーンの IP アドレスパターンには、3 つのデフォルトパターンが定義されています。これらのパターンは、「127.0.0.1」、「0:0:0:0:0:0:0:1」、「::1」です。これらのパターンは、それぞれ IPV4 および IPV6 のローカルホスト IP アドレスを表し、代替セキュリティゾーンで受容するリクエストを、ローカルユーザから発行されたリクエストのみに制限します。このゾーンでは、[追加]、[編集]、[設定の編集]、[削除] リンクを使用することもできます。これらの機能の構成はすべて、代替ゾーンに割り当てられたユーザにのみ影響します。

セキュリティゾーン設定のインポートとエクスポート

各セキュリティゾーンの設定は、4 つのセキュリティ構成ファイルに保存されます (securitysettings.xml、securitysettings-mobile.xml、securitysettings-portlet.xml、securitysettings-zone.xml) 。ゾーンの認証方法を変更する前に、そのゾーンページの [エクスポート] リンクを使用して、セキュリティゾーン構成のバックアップ ZIP ファイルを保存します。セキュリティゾーン設定を以前の構成に戻す必要がある場合は、[インポート] リンクを使用して構成ファイルから設定を取得し、サーバ上のセキュリティ構成ファイルをその設定に戻します。

手順　セキュリティ構成ファイルをエクスポートするには

[エクスポート] リンクを使用すると、サーバの 4 つのセキュリティ構成ファイルの ZIP コピーが作成され、指定したネットワークディレクトリに保存されます。この機能を使用して、現在のセキュリティ構成設定を更新する前に、これらの構成設定のバックアップを作成します。

1. セキュリティゾーンの [認証]、[リクエスト一致] ページの [アクション] セクションで、[エクスポート] をクリックします。
2. ZIP ファイルを開くかどうかを選択するメッセージで、[開く] をクリックします。
3. WinZip ダイアログボックスのメニューバーで [ファイル] をクリックし、[名前を付けて保存] をクリックします。
4. ファイルのデフォルト名を受容するか、新しい名前を入力します。
5. 新しいファイルの格納先に移動し、[保存] をクリックします。
6. WinZip ダイアログボックスのメニューバーで [ファイル] をクリックし、[終了] をクリックします。

手順　セキュリティ構成ファイル設定をインポートするには

[インポート] 機能を使用して、以前のセキュリティ構成設定が格納されたセキュリティ構成ファイルからテキストをコピーし、WebFOCUS Server の 4 つのセキュリティファイルに貼り付けることができます。以前のセキュリティ構成設定に戻す必要がある場合は、この機能をいつでも使用することができます。

1. セキュリティゾーンの [認証]、[リクエスト一致] ページの [アクション] セクションで、[インポート] をクリックします。
2. [Web セキュリティ構成データのインポート] ダイアログボックスで、[securitysettings.xml]、[securitysettings-mobile.xml]、[securitysettings-portlet.xml]、[securitysettings-zone.xml] タブのいずれかをクリックして、新しい構成データの格納先とする構成ファイルを指定します。
3. ソースファイルから構成テキストをコピーします。

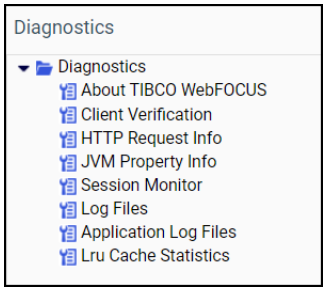
4. [Web セキュリティ構成データをローカルファイルからコピーし、ここに貼り付けてください] ボックスに、ソースファイルのテキストを貼り付けます。
5. [OK] をクリックします。
6. 確認ダイアログボックスで、[OK] をクリックしてインポートを完了します。
7. 「入力 Web 構成データを貼り付けられません」というメッセージが表示された場合は、[OK] をクリックした上で、必要に応じてテキストを調整し、手順 5 および 6 を繰り返します。

TIBCO WebFOCUS 機能診断の使用

管理コンソールの表示権限を所有するユーザは、管理コンソールの [機能診断] メニューを使用して次のことを行えます。

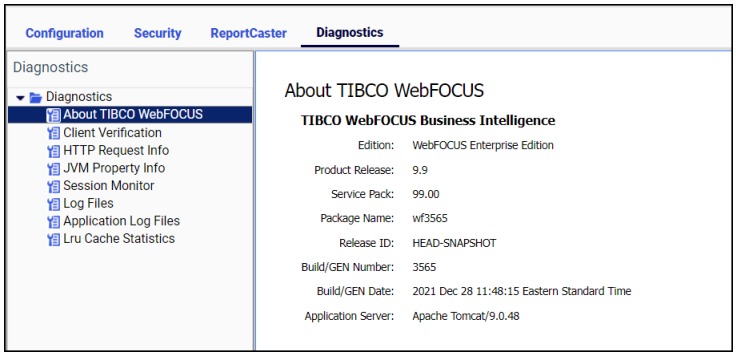
- バージョン情報の表示
- Client コンポーネントのインストールと構成の確認
- TIBCO WebFOCUS セッションのモニタ
- ログのオンとオフの切り替え、ログファイルの表示
- 別のアプリケーションで作成したログファイルの表示
- LRU キャッシュ統計のモニタ

下図は、[機能診断] メニューを示しています。



バージョン情報の確認

[TIBCO WebFOCUS について] ページには、下図のように、使用している製品のリリース番号、および製品に同梱されているオプションコンポーネントに関する情報が表示されます。



技術サポートに問い合わせる際は、このページの情報を使用して、製品のリリース番号やサービスパックの情報を識別することができます。

[TIBCO WebFOCUS について] をクリックすると、次の情報がメインウィンドウに表示されます。

製品リリース　リリース番号です (例、8.2)。

サービスパック　サービスパック番号です (例、05.0.1)。最初の 2 桁はバージョン番号を表します。最後の 2 桁は中間リリース番号です。

パッケージ名　インストールファイルのパッケージ名です (例、wf032019a)。

リリース ID　製品のリリース ID です (例、8.2.05)。

ビルド/GEN 番号　特定の製品ビルド番号です (例、74)。

ビルド/GEN 日時　このビルドの生成日時です (例、March 20, 2019 8:04:35 PM EDT)。

Application Server　Application Server 名です (例、Apache Tomcat/8.5.32)。

[機能診断] タブから [TIBCO WebFOCUS について] ページにアクセスできるのは、管理コンソールの表示権限を所有しているユーザのみです。

ただし、このページの製品およびサーバに関する情報は、[TIBCO WebFOCUS Business Intelligence について] ウィンドウの表示権限を所有するユーザにも表示されます。このウィンドウを開くには、[ヘルプ] をクリックし、[WebFOCUS について] を選択します。

Client の確認

[Client の確認] ページには、Client 構成の現在ステータス、およびアプリケーションの設定が表示されます。このページを開くと、構成およびアプリケーション設定の確認に必要なテストが表示され、自動的に実行することができます。

使用可能な設定には [パス] が表示されます。使用不可の設定には [失敗] が表示されます。

この自動確認プロセスには、クライアント通信モードの各タイプ (CGI、WFServlet、または ISAPI) に対する Web サーバエイリアスおよびディレクトリアクセス許可の検証が含まれます。

Client 確認ツールの確認ログのデフォルトパスは、*drive*:¥ibi¥WebFOCUS82¥logs です。これらのツールは、ログディレクトリの読み取り、書き込み、削除権限のテストを実行します。また、*drive*¥:ibi¥WebFOCUS82¥config ディレクトリに対する読み取り権限および書き込み権限のテストも実行されます。

Reporting Server 接続、および Reporting Server から提供されるグラフ機能またはテーブル機能の現在ステータスをテストするには、[構成] タブを開き、テストする Reporting Server のアイコンを右クリックします。各サーバノードのコンテキストメニューの [テスト] オプションには、3 種類のテストが表示されます。

手順　Client の確認テストを実行するには

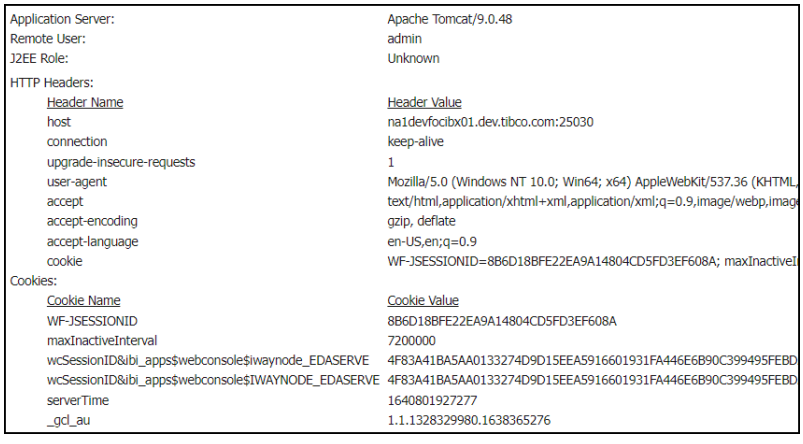
管理コンソールで [機能診断] タブをクリックし、[Client の確認] をクリックします。

[Client の確認] ページには、さまざまなディレクトリアクセス許可が表示されます。たとえば、アプリケーションの作成と削除、管理者としてのログイン、標準ディレクトリの読み取りと書き込み、ワークスペースの作成と削除、レポートの作成と削除に関するアクセス許可です。

注意： このテストを製品のインストール直後に実行した場合、クライアントアプリケーションをサポートする Tomcat Web アプリケーションの初期化に時間を要するため、テスト結果の表示が遅くなる場合があります。

HTTP リクエスト情報ページのモニタ

[HTTP リクエスト情報] ページには、下図のように、ブラウザに返される HTTP ヘッダまたは HTTPS ヘッダに関する情報が表示されます。



Application Server:	Apache Tomcat/9.0.48
Remote User:	admin
J2EE Role:	Unknown
HTTP Headers:	
Header Name	Header Value
host	na1devfocibx01.dev.tibco.com:25030
connection	keep-alive
upgrade-insecure-requests	1
user-agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
accept	text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,imag
accept-encoding	gzip, deflate
accept-language	en-US,en;q=0.9
cookie	WF-JSESSIONID=8B6D18BFE22EA9A14804CD5FD3EF608A; maxInactiveI
Cookies:	
Cookie Name	Cookie Value
WF-JSESSIONID	8B6D18BFE22EA9A14804CD5FD3EF608A
maxInactiveInterval	7200000
wcSessionID&ibi_apps$webconsole$iwaynode_EDASERVE	4F83A41BA5AA0133274D9D15EEA5916601931FA446E6B90C399495FEBD
wcSessionID&ibi_apps$webconsole$IWAYNODE_EDASERVE	4F83A41BA5AA0133274D9D15EEA5916601931FA446E6B90C399495FEBD
serverTime	1640801927277
_gcl_au	1.1.1328329980.1638365276

この情報は、特に Web サーバまたは Application Server のセキュリティを TIBCO WebFOCUS に統合したり、Web サーバまたは Application Server が仮想ホスト (HTTP ヘッダ) を使用したりする場合のトラブルシューティングや HTTP ヘッダ構成に役立ちます。このページには次の情報が表示されます。

Application Server　Application Server の名前およびバージョンを示します (例、Apache Tomcat/9.0.26)。Apache Tomcat は、デフォルト設定で製品インストールに同梱されていますが、インストールで異なる Application Server プラットフォームが使用される場合は、別の名前がこのエントリに表示されます。

リモートユーザ　セッションに現在ログインしているユーザの名前を示します。

J2EE ロール　デフォルト値の「不明」が表示されます。通常、J2EE ロールは関係ありません。

[**HTTP ヘッダ**] セクションには、最初のリクエストに応答して Application Server から、ユーザに割り当てられたブラウザに返されるレスポンスのフィールドおよびデフォルト値が表示されます。これらは、HTTP セッションの受容可能なオペレーティングパラメータを定義します。

- **host**　Application Server のドメイン名とポート番号を示します (例、hostsrvr01.companyname.com:25150)。
- **connection**　接続状況を示します。デフォルト設定では、アイドル状態でもセッションの表示を保持するために、この値が keep-alive に設定されています。

- **upgrade-insecure-requests**
- **user-agent**　受容可能なブラウザを示します (例、Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko)。
- **accept**　受容可能なメディアタイプを示します (例、text/html, application/xhtml+xml, image/jxr, */*)。
- **accept-encoding**　トランザクション内の情報の圧縮に使用する受容可能なエンコーディングフォーマットを示します (例、gzip, deflate)。
- **accept-language**　受容可能な言語コードを示します (例、en-US)。
- **cookie**　リクエスト送信元に返される一連の値を示します。これには、セッションの現在の状態に関する情報が含まれます。Application Server からユーザに返される cookie に含まれる典型的なパラメータについての詳細は、[Cookie] セクションを参照してください。

[**Cookie**] セクションには、現在のセッションで Application Server から返される cookie に含まれる次の情報が表示されます。

- **WF-JSESSIONID**　ユーザのリクエストで開始された現在のセッションの一意の ID を示します。
- **maxInactiveInterval**　サーバとブラウザ間の通信でアイドル状態を保持できる最大秒数を示します。デフォルト設定では、この値は 7200000 に設定されています。
- **wcSessionID&ibi_apps$webconsole$iwaynode_EDASERVE**
- **serverTime**　アイドル状態が続いた場合に、現在のセッションが期限切れになる時間を示します。この値は、エポック時間 (UNIX 時間 とも呼ばれる) で表示されます。通常は、最後のレスポンスメッセージの時間に、[MaximumInactiveInterval] に割り当てた秒数を加算した時間に等しくなります。
- **_ga**　Application Server に割り当てられた Google Analytics Client ID を示します。
- **_fbp**
- **_gcl_au**
- **apt.uid**　Application Server に割り当てられた Linux ユーザ ID を示します。

JVM プロパティ情報ページのモニタ

[JVM プロパティ情報] ページには、使用する製品インストールでサポートされる Java 仮想マシン (JVM) についての情報が表示されます。JVM は、Application Server および Client をホストするマシンのランダムアクセスメモリ (RAM) 内に存在します。このページに表示される統計は、このインストールのパフォーマンスを表します。

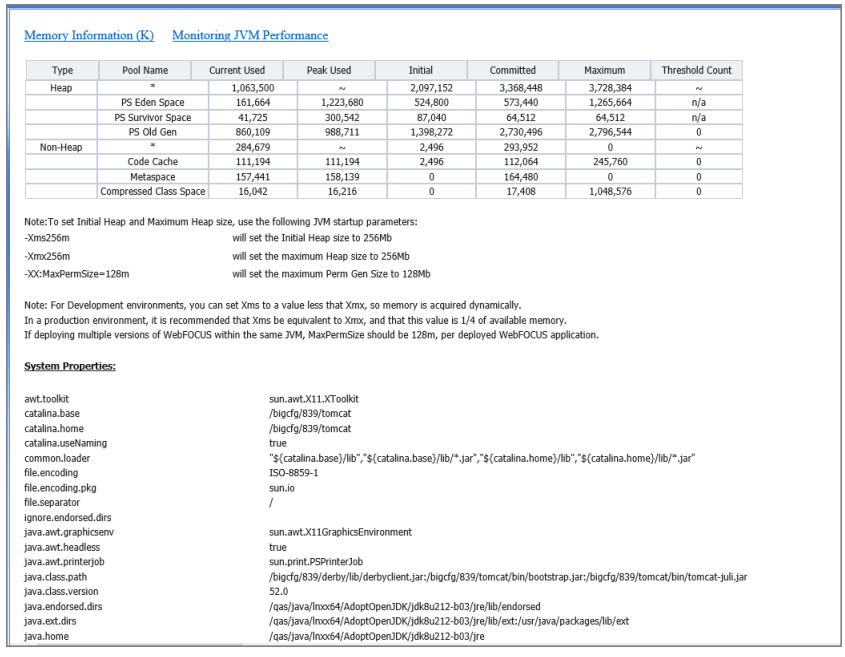
このページの情報は、TIBCO WebFOCUS Web アプリケーションの Java 環境およびメモリやリソースの問題に関する分析およびトラブルシューティングをサポートします。

このページには、2 つのタブへのリンクが表示されます。[メモリ情報 (K)] タブには、現在の JVM メモリ使用の統計およびシステムプロパティが表示されます。[JVM パフォーマンスモニタ] タブには、前の 1 時間のメモリ使用パターンを示す一連のグラフが表示されます。

この情報は、Java VM 環境でアクセス可能な JConsole モニタツールでも確認できます。ただし、[JVM プロパティ情報] ページを管理コンソール内に表示することで、Apache Tomcat またはホストサーバから直接この情報にアクセスするための時間と労力が節減されます。

メモリ情報 (K) タブのモニタ

[メモリ情報 (K)] タブには、下図のように、現在のメモリ使用分析および TIBCO WebFOCUS のインストールを実行する Java 仮想マシンの追加のシステムプロパティが表示されます。



Memory Information (K)　Monitoring JVM Performance

Type	Pool Name	Current Used	Peak Used	Initial	Committed	Maximum	Threshold Count
Heap	*	1,063,500	~	2,097,152	3,368,448	3,728,384	~
	PS Eden Space	161,664	1,223,680	524,800	573,440	1,265,664	n/a
	PS Survivor Space	41,725	300,542	87,040	64,512	64,512	n/a
	PS Old Gen	860,109	988,711	1,398,272	2,730,496	2,796,544	0
Non-Heap	*	284,679	~	2,496	293,952	0	~
	Code Cache	111,194	111,194	2,496	112,064	245,760	0
	Metaspace	157,441	158,139	0	164,480	0	0
	Compressed Class Space	16,042	16,216	0	17,408	1,048,576	0

Note:To set Initial Heap and Maximum Heap size, use the following JVM startup parameters:

-Xms256m　will set the Initial Heap size to 256Mb

-Xmx256m　will set the maximum Heap size to 256Mb

-XX:MaxPermSize=128m　will set the maximum Perm Gen Size to 128Mb

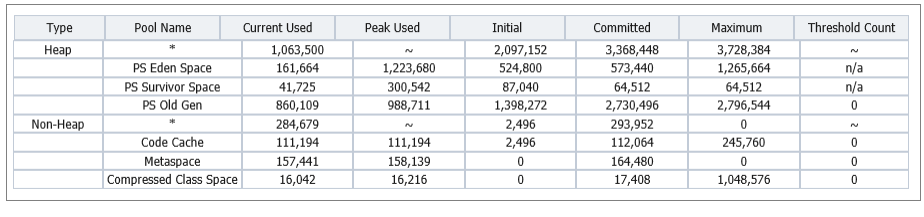
Note: For Development environments, you can set Xms to a value less that Xmx, so memory is acquired dynamically.
In a production environment, it is recommended that Xms be equivalent to Xmx, and that this value is 1/4 of available memory.
If deploying multiple versions of WebFOCUS within the same JVM, MaxPermSize should be 128m, per deployed WebFOCUS application.

System Properties:

awt.toolkit	sun.awt.X11.XToolkit
catalina.base	/bigcfg/839/tomcat
catalina.home	/bigcfg/839/tomcat
catalina.useNaming	true
common.loader	"${catalina.base}/lib","${catalina.base}/lib/*.jar","${catalina.home}/lib","${catalina.home}/lib/*.jar"
file.encoding	ISO-8859-1
file.encoding.pkg	sun.io
file.separator	/
ignore.endorsed.dirs	
java.awt.graphicsenv	sun.awt.X11GraphicsEnvironment
java.awt.headless	true
java.awt.printerjob	sun.print.PSPrinterJob
java.class.path	/bigcfg/839/derby/lib/derbyclient.jar:/bigcfg/839/tomcat/bin/bootstrap.jar:/bigcfg/839/tomcat/bin/tomcat-juli.jar
java.class.version	52.0
java.endorsed.dirs	/qas/java/lnxx64/AdoptOpenJDK/jdk8u212-b03/jre/lib/endorsed
java.ext.dirs	/qas/java/lnxx64/AdoptOpenJDK/jdk8u212-b03/jre/lib/ext:/usr/java/packages/lib/ext
java.home	/qas/java/lnxx64/AdoptOpenJDK/jdk8u212-b03/jre

メモリ使用統計テーブル

タブ上部のテーブルには、下図のように、Application Server および Client を実行するホストの Java 仮想マシンインストールについて、現在のメモリ使用統計が表示されます。



Type	Pool Name	Current Used	Peak Used	Initial	Committed	Maximum	Threshold Count
Heap	*	1,063,500	~	2,097,152	3,368,448	3,728,384	~
	PS Eden Space	161,664	1,223,680	524,800	573,440	1,265,664	n/a
	PS Survivor Space	41,725	300,542	87,040	64,512	64,512	n/a
	PS Old Gen	860,109	988,711	1,398,272	2,730,496	2,796,544	0
Non-Heap	*	284,679	~	2,496	293,952	0	~
	Code Cache	111,194	111,194	2,496	112,064	245,760	0
	Metaspace	157,441	158,139	0	164,480	0	0
	Compressed Class Space	16,042	16,216	0	17,408	1,048,576	0

このテーブルの値は、次の JVM メモリ領域ごとに現在使用されているメモリ量を示します。

[**Heap**] メモリ領域には、実行時に JVM にロードされるすべてのクラスインスタンスおよび配列が含まれます。そのため、ヒープに割り当てられるメモリ量は、ユーザのアクティビティによって異なります。

JVM では、内部ガベージコレクション処理により、使用されていないクラスインスタンスまたは配列が自動的にクリアされます。この処理で残ったクラスおよび配列は、Eden Space (すべての新しいクラスおよび配列が最初にロードされる) から Survivor Space に移動し、次に Old Gen Space に移動します。このため、テーブルでは、ヒープ全体の概要統計が 1 行に表示され、ヒープ内の次の 3 つのプール (メモリ領域) の統計が 3 行に表示されます。

- **PS Eden Space**　すべての新しいクラスインスタンスおよび配列が含まれます。
- **PS Survivor Space**　継続して使用されているため、Eden Space でのガベージコレクション処理で残ったクラスインスタンスおよび配列が含まれます。
- **PS Old Gen**　継続して使用されているため、Survivor Space でのガベージコレクション処理で残ったクラスインスタンスおよび配列が含まれます。

[**Non-Heap**] メモリ領域には、内部 JVM 処理の維持に必要なすべてのスレッドおよびメモリが含まれます。通常、この領域はガベージコレクションの対象外となり、この領域のサイズは変わりません。

テーブルでは、非ヒープ領域全体の統計が 1 行に表示され、次の 3 つのプールの統計が 3 行に表示されます。

- **Code Cache**　ネイティブコードをコンパイルおよび保存するために使用するメモリが含まれます。
- **Metaspace**　ユーザが作成したクラスから自動的にロードされたメタデータが含まれます。
- **Compressed Class Space**　アプリケーションでロードされた Java クラスのメタデータが含まれます。

このテーブルのカラムは、各メモリ領域の次の統計を示します。

- **プール名**　各行の統計が適用されるメモリ領域の名前を指定します。
- **現在使用中**　現在使用中のメモリ量がキロバイト単位で示されます。これには、アクセス可能とアクセス不可の両方を含むすべてのオブジェクトで使用されるメモリが含まれます。
- **ピーク時**　セッション中の任意の時点でプールにより使用されるメモリの最大使用量がキロバイト単位で示されます。
- **初期**　セッション開始時にプールで使用されるメモリ量がキロバイト単位で示されます。
- **コミット済み**　プールでの使用が保証されたメモリ量がキロバイト単位で示されます。

- **最大** プールで使用可能な最大メモリ量がキロバイト単位で示されます。
- **しきい値** メモリ使用量のしきい値がキロバイト単位で示されます。

下図のように、[Heap] 行および [Non-Heap] 行の [ピーク時] 列と [しきい値] 列には、数値ではなくチルダ記号 (~) が表示されます。

Type	Pool Name	Current Used	Peak Used	Initial	Committed	Maximum	Threshold Count
Heap	*	1,063,500	~	2,097,152	3,368,448	3,728,384	~
	PS Eden Space	161,664	1,223,680	524,800	573,440	1,265,664	n/a
	PS Survivor Space	41,725	300,542	87,040	64,512	64,512	n/a
	PS Old Gen	860,109	988,711	1,398,272	2,730,496	2,796,544	0
Non-Heap	*	284,679	~	2,496	293,952	0	~
	Code Cache	111,194	111,194	2,496	112,064	245,760	0
	Metaspace	157,441	158,139	0	164,480	0	0
	Compressed Class Space	16,042	16,216	0	17,408	1,048,576	0

このチルダ記号 (~) は、これらのカテゴリの概要統計が、[Heap] および [Non-Heap] メモリ領域全体には関係しないことを示します。その他すべてのカラムでは、[Heap] 行と [Non-Heap] 行に表示されるキロバイト数は、後続の 3 行に表示されるキロバイト数の合計に等しくなります。

エントリハイライトの理解

[使用中] および [ピーク時] 列の各エントリは、それぞれのカテゴリの値が、プールに割り当て可能な最大メモリ量 ([最大] 列) の 90% を超えると、ハイライト表示されます。

たとえば、ヒープの [PS Old Gen] プールの現在使用中のバイト数が [最大] 量の 90% を超えた場合、このエントリは背景色がハイライト表示され、使用中の既存クラスの数値がこのプールに割り当てられた最大メモリ量に近づいていることが警告されます。

メモリ割り当てガイドライン

下図のように、メモリ使用統計の下に、標準ガイドラインが表示されます。このリストには、Java 初期パラメータの最適なメモリサイズを設定するために、JVM インストールに追加する初期パラメータについての推奨が記載されています。このリストの詳細は、各インストールで変わりません。

このセクションでは、「Xms」は、ヒープの初期メモリ割り当てを定義する -Xms パラメータのことです。「Xmx」は、ヒープの最大メモリ割り当てを定義する -Xmx パラメータのことです。「XX」は、最小ヒープフリー率と最大ヒープフリー率を定義する XX パラメータのことです。

システムプロパティリスト

[システムプロパティ] リストは、ページ下部に表示されます。このリストには、Java 仮想マシン内で定義された関連パラメータが表示され、Application Server および Client のローカルインストールでこれらのパラメータに割り当てられた値が示されます。

System Properties:

awt.toolkit	sun.awt.X11.XToolkit
catalina.base	/bigcfg/839/tomcat
catalina.home	/bigcfg/839/tomcat
catalina.useNaming	true
common.loader	"${catalina.base}/lib","${catalina.base}/lib/*.jar","${catalina.home}/lib","${catalina.home}/lib/*.jar"
file.encoding	ISO-8859-1
file.encoding.pkg	sun.io
file.separator	/
ignore.endorsed.dirs	
java.awt.graphicsenv	sun.awt.X11GraphicsEnvironment
java.awt.headless	true
java.awt.printerjob	sun.print.PSPrinterJob
java.class.path	/bigcfg/839/derby/lib/derbyclient.jar:/bigcfg/839/tomcat/bin/bootstrap.jar:/bigcfg/839/tomcat/bin/tomcat-juli.jar
java.class.version	52.0

このリストに表示された特定のプロパティについての詳細は、使用する Java バージョンの「Java Toolkit and Java® Virtual Machine Specification」を参照してください (https://docs.oracle.com/javase/specs/index.html)。

このリストの最後の 4 つのエントリには、TIBCO WebFOCUS 内で定義され、現在のインストールで使用されるエンコードスキーマが示されます。

- **System.in Encoding**　現在のコードページおよび Application Server で使用されるエンコードを示します。
- **System.out Encoding**　現在のコードページおよび Application Server で使用されるエンコードを示します。
- **Method setCharacterEncoding**　文字エンコードの使用が実装済みかどうかを示します。
- **Available Processors**　JVM をサポートするマシンに割り当てられたプロセッサのサイズ (ビット単位) です。

JVM パフォーマンスモニタ

[JVM パフォーマンスモニタ] タブには、CPU、メモリ、ヒープメモリ、非ヒープメモリの過去 1 時間のリソース使用量の変化を示す 4 つのグラフが表示されます。

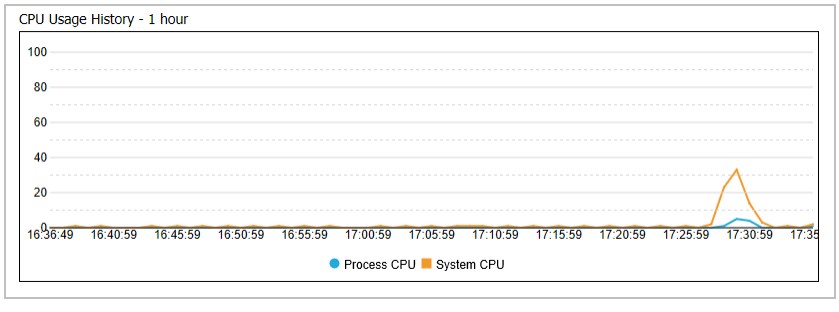
ページ上部の [リフレッシュ] ボタンをクリックすると、グラフがリセットされ、ボタンクリック時から 1 時間前までの動作が表示されます。このボタンを使用してグラフを更新し、最新の画面動作を把握することができます。

[リフレッシュ間隔] チェックボックスおよびリフレッシュ間隔の [秒] テキストボックスを使用して、自動リフレッシュ間隔をリセットすることができます。[リフレッシュ間隔] は、デフォルトで 10 秒に設定されています。この値は、1 から 99,999,999 までの任意の数値で置換できます。自動リフレッシュを有効にするには、[リフレッシュ間隔] のチェックをオンにします。

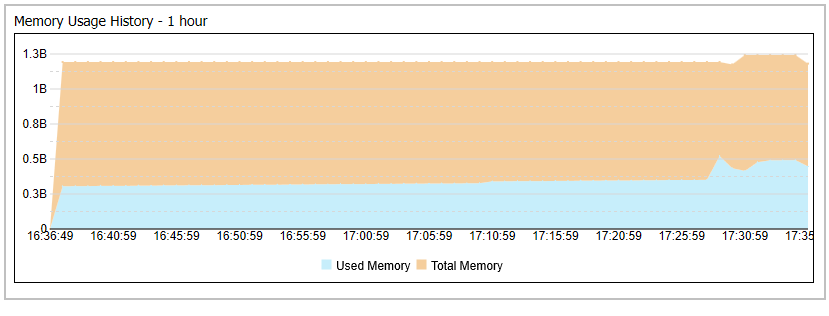
このタブのグラフは、予期しないリソース使用の波および過去 1 時間以内の発生時点をすばやく特定することで、ユーザのパフォーマンスモニタおよびトラブルシューティングをサポートします。

CPU 使用履歴 - 1 時間　下図のように、過去 1 時間の CPU リソース使用パーセントの変化を示します。

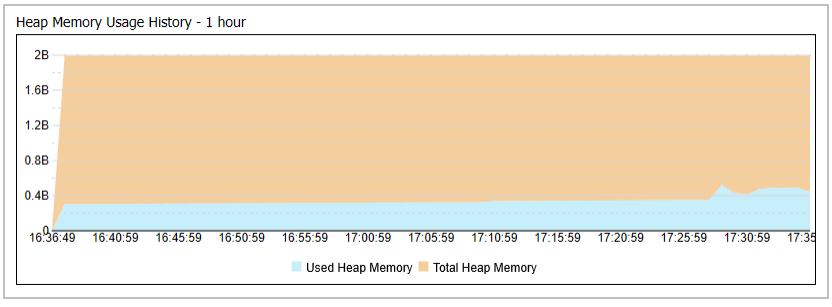
- **プロセス CPU**　特定期間に JVM プロセスで使用された CPU リソースの変化 (パーセント) を示します。
- **システム CPU**　特定期間にオペレーティングシステムプロセスで使用された CPU リソースの変化 (パーセント) を示します。



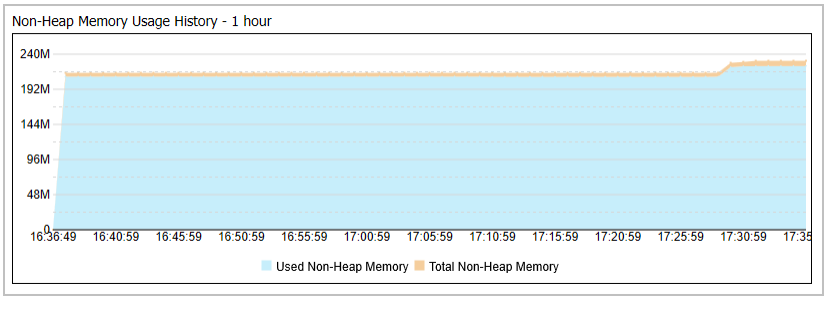
メモリ使用履歴 - 1 時間　下図のように、過去 1 時間の JVM アプリケーション全体のメモリ使用量の変化をキロバイト単位で示します。このグラフの上位エントリは、メモリに割り当てられた合計メモリ (キロバイト) を示します。



ヒープメモリ使用履歴 - 1 時間　下図のように、過去 1 時間のヒープメモリ使用量の変化をキロバイト単位で示します。このグラフの上位エントリは、ヒープメモリに割り当てられた合計メモリ (キロバイト) を示します。

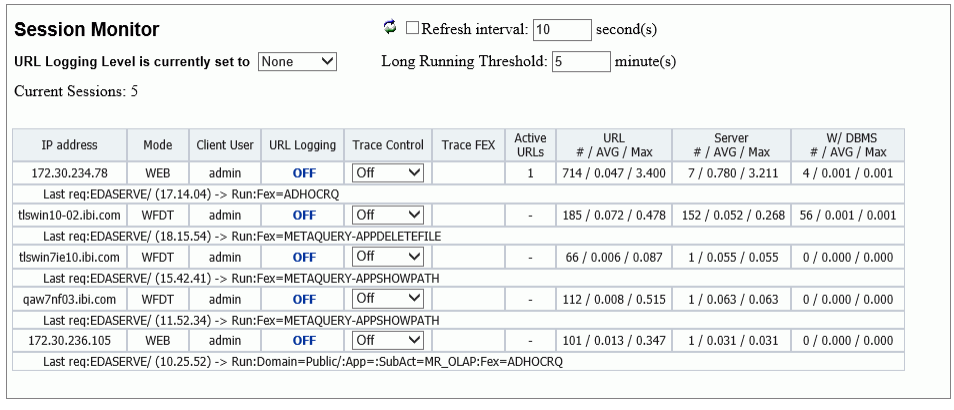


非ヒープメモリ使用履歴 - 1 時間　下図のように、過去 1 時間の非ヒープメモリ使用量の変化をキロバイト単位で示します。このグラフの上位エントリは、非ヒープメモリに割り当てられた合計メモリ (キロバイト) を示します。



セッションのモニタ

管理者は、[セッションモニタ] ページを使用して、すべての Client セッション、および Reporting Server の接続とアクティビティのトラッキングを行えます。下図のように、[セッションモニタ] ページには、接続中のユーザ、レポートリクエスト、Reporting Server のノードが表示されます。



表示された情報をリフレッシュするには、[リフレッシュ] アイコンをクリックします。自動リフレッシュを設定するには、[リフレッシュ間隔] のチェックをオンにし、デフォルト設定の 10 秒を受容するか、別の値を秒数で入力します。このテキストボックスの値を変更した場合、その値が有効になるのは、[セッションモニタ] ページを開いている間のみです。このページを閉じて、後から再び開くと、デフォルト値に戻ります。

管理者は、[現在の URL ログレベル] 横の [すべて]、[なし]、[選択] のいずれかをクリックして、現在のすべてのセッションログを有効または無効にすることができます。特定のセッションのログを有効または無効にするには、[選択] をクリックし、そのセッションの [URL ログ] 列で [オン] または [オフ] をクリックします。デフォルト設定では、すべてのログ情報は、*drive*:¥ibi¥WebFOCUS82¥logs (Windows) または *install_directory*/ibi/WebFOCUS82/logs (UNIX または Linux) に格納されます。

非アクティブセッションが無限に継続しないようにするには、[長時間実行しきい値] テキストボックスのデフォルト値 (5 分) を受容するか、別の値を入力してセッション期間を増減します。このテキストボックスの値を変更した場合、その値が有効になるのは、[セッションモニタ] ページを開いている間のみです。このページを閉じて、後から再び開くと、デフォルト値に戻ります。次の情報がセッションごとに表示されます。

IP アドレス

セッションを開始したコンピュータまたは他のデバイスに割り当てられる数値ラベルです。

このアドレスを使用して、セッションを開始したコンピュータまたは他のデバイスに割り当てられているユーザを識別することができます。

モード
セッションを開始した製品コンポーネントを識別し、すべてのアクティブリクエストに関する情報を表示します。製品コンポーネントの値は、次のとおりです。

WEB
Client です。

WSRV
Reporting Server です。

WFC
管理コンソールです。

WFRQ
セルフサービスアプリケーションのレポートリクエストです。

WFDT
App Studio です。

IBFS
Information Builders ファイルシステム です。

Client ユーザ
クライアントセッションを開始したユーザ ID です。Null 値は、セルフサービスアプリケーションから送信されたリクエストであることを示します。

URL ログ
個々のセッションまたは現在ユーザのログを有効または無効にします。

トレースの制御
特定の IP アドレス (ユーザ) のトレースを特定の詳細レベルで有効または無効にします。

プロシジャトレース
セッションの WFServlet、Client コネクタ、Reporting Server のトレースを有効にするかどうかを指定します。トレースを有効にした場合は、[トレースの表示] アイコンが表示されます。このアイコンをクリックしてトレースを確認します。

アクティブ URLs
セッション中にアクティブに使用されている URL の件数を示します。この値は、現在開いているアクティブ状態のセッションにのみ関連します。各 URL は、リクエストがブラウザ経由で Application Server に送信された際の送信元ワークステーションを表します。

URL

HTTP リクエストで送信された動的 URL の番号、平均継続時間、最大継続時間が表示されます。平均継続時間は、秒単位で測定され、ミリ秒に換算されます。HTTP リクエストの URL にはサーバに転送されないものがあり、また、サーバに転送されるリクエストには DBMS には転送されないものがあります。

Server

Reporting Server で実行されるレポートの動的 URL の番号、平均継続時間、最大継続時間を表示します。平均継続時間は、秒単位で測定され、ミリ秒に換算されます。HTTP リクエストの URL にはサーバに転送されないものがあり、また、サーバに転送されるリクエストには DBMS には転送されないものがあります。

W/DBMS

外部データベースで実行されるレポートの動的 URL の番号、平均継続時間、最大継続時間を表示します。平均継続時間は、秒単位で測定され、ミリ秒に換算されます。HTTP リクエストの URL にはサーバに転送されないものがあり、また、サーバに転送されるリクエストには DBMS には転送されないものがあります。

手順　セッションモニタログをエクスポートするには

セッションモニタログをエクスポートして、トラブルシューティングに活用したい場合があります。

1. 管理コンソールで [機能診断] タブをクリックし、[セッションモニタ] をクリックします。

   右側ウィンドウに現在のセッションが表示されます。

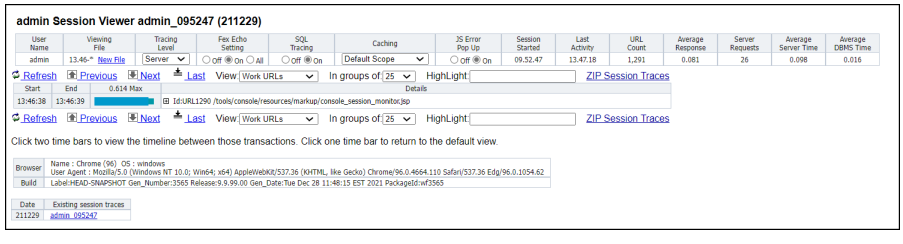
2. 特定のセッションの [トレースの制御] オプションを [詳細] に設定します。

   [プロシジャトレース] 列に情報アイコンが表示されます。

3. 必要に応じて、ログを記録するリクエストを実行し、管理コンソールに戻ります。

4. [トレースの表示] アイコン をクリックします。

   下図のように、セッションビューアが表示されます。



5. [セッショントレース ZIP] リンクをクリックし、ZIP ファイルを保存します。
6. セッションビューアを閉じ、[セッションモニタ] ウィンドウに戻ります。
7. [トレースの制御] オプションを元の値に設定します。通常、この値は [オフ] です。

   これに応答して、セッションモニタテーブルの上部に、トレースが変更または停止されたことを示す確認メッセージが表示されます。

セッションの表示

セッションビューアを使用して、最近の作業セッション中に発生したシステムイベントのトレースを確認し、これらのトレースをシステム管理者や技術サポート担当者が利用できるようエクスポートすることができます。セッションビューアではシステムイベントおよびエラーメッセージのトレースが収集されるため、システムの使用状況が明確になるほか、システム障害やパフォーマンス問題の原因の調査が可能になります。

セッションビューアでは、確認するセッションの範囲を現在アクティブのセッションから過去に実行されたセッションにまで拡張することで、[セッションモニタ] ページの情報を補足することができます。セッションビューアでセッションに関する情報を保持する日数を定義するには、[トレース削除までの日数] (IBI_Trace_Retain_Days) パラメータを使用します。また、セッションの範囲をユーザ自身が開始したセッションと、他のユーザが開始したセッションの中でセッションアクティビティの表示権限を所有するセッションに限定することで、確認するセッションを絞り込むことができます。

セッションビューアにアクセス可能なユーザは、[Development Traces (opDevTraces)] 権限が割り当てられているユーザのみです。この権限が割り当てられたユーザは、現在および過去の作業セッションのトレースを表示することができます。この権限を所有するユーザは、セッションビューアを開くことができます。WebFOCUS Hub からこれを実行するには、[ツール] メニューを開き、[セッションの表示] を選択します。WebFOCUS ホームページからは、[ユーティリティ] をクリックし、[セッションビューア] を選択します。

管理者としてログインした場合は、ユーザ自身のセッション以外に、他のユーザのセッションを表示することができます。管理者以外のユーザとしてログインした場合、表示可能なセッションは、[Development Traces (opDevTraces)] 権限で許可されている範囲に限定されます。

セッションビューアメインページの表示

下図のように、セッションビューアのメインページには、現在の作業セッションに関する情報が表示されます。また、最近完了したセッションの中で、ユーザが表示権限を所有するセッションのリストも表示されます。

セッションビューアのメインページを開くには、[Session Traces] (opDevTraces) 権限を所有するユーザとしてログインします。WebFOCUS Hub から、[ツール] および [セッションの表示] を選択します。WebFOCUS ホームページでは [ユーティリティ] をクリックし、[セッションビューア] を選択します。セッション ID のフォーマットは「username_HHMMSS」です。セッション ID は、表示中セッションのユーザ名、開始時間、開始日付で構成されます。次の情報がセッションごとに表示されます。

ユーザ名

この作業セッションにログインしたユーザの名前です。

表示ファイル

表示ファイルの名前です。ファイル名は、HH.MM フォーマットの開始時間と終了時間で識別されます。終了時間にアスタリスク (*) が表示されている場合、そのファイルへの現在トレースの転送が継続中であることを示しています。

[新規ファイル] をクリックすると、一連のトレースを新しいファイルに収集することができます。これにより、確認する URL の範囲を調整することができます。このリンクをクリックすると、セッションビューアが新しいファイルを自動的に作成し、後続のすべてのトレースをそのファイルに割り当てます。以前のトレースを確認するには、[表示ファイル] リストから、完了済みトレースが格納されているファイルを選択します。

トレースレベル

現在のセッションで収集されたトレースのレベルです。このフィールドのデフォルト値は [オフ] ですが、リストから別の値を選択することもできます。この選択値はセッションビューアを閉じる際に保存され、次のセッションのデフォルト設定として使用されます。

4 つのトレースレベルは累加的に機能し、上位のトレースレベルには、それより下位のトレースレベルのトレース情報がすべて含まれます。これらのレベルには次のものがあります。

- **基本** 各 URL のトレースを生成します。これには、IBFS トレースおよびプロシジャトレースが含まれます。
- **出力** [基本] レベルのトレースと、Reporting Server でリクエストを実行した URL の出力が含まれます。このトレースレベルは、出力トレースの収集に必要なディスク領域に影響しますが、システムパフォーマンスには影響しません。
- **デバッグ** [出力] レベルのトレースと、セッションビューアに書き込まれる log4j デバッグレベルのトレースが含まれます。
- **詳細** [デバッグ] レベルのトレースと、レガシー WFServlet トレースが含まれます。このトレースレベルは、セッションパフォーマンスに影響します。
- **サーバ** [詳細] レベルのトレースと、現在の作業セッションでの Reporting Server アクティビティのトレースが含まれます。

プロシジャ ECHO 設定

プロシジャファイルコマンドの実行から取得される ECHO トレースのレベルです。プロシジャファイルコマンドが実行されると、プロシジャファイルの &ECHO 変数によって、プロシジャのテストやデバッグを目的としてコマンドラインが表示されます。これらのレベルには次のものがあります。

- **オフ** スタックコマンドとダイアログマネージャコマンドの両方をトレースに表示しません。これがデフォルト値です。
- **オン** 実行用に展開およびスタックされた TIBCO WebFOCUS コマンドをトレースに表示します。
- **すべて** 実行用に展開およびスタックされたダイアログマネージャコマンドおよび TIBCO WebFOCUS コマンドをトレースに表示します。

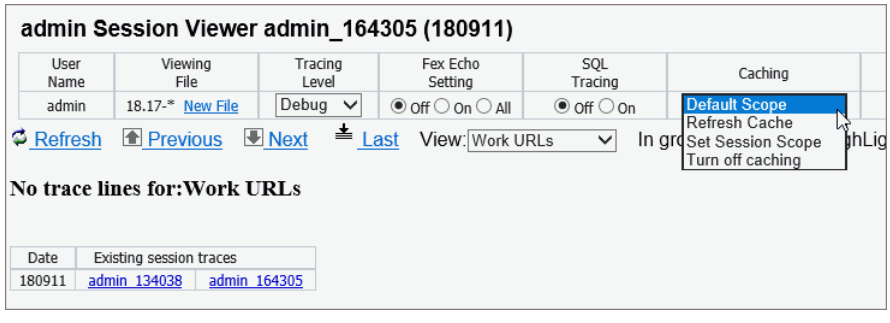
SQL トレース

SQL イベントから取得されるトレースのレベルです。これらのレベルには次のものがあります。

- **オフ** SQL リクエストおよびレスポンスイベントのトレースを表示しません。
- **オン** すべての SQL リクエストおよびレスポンスイベントのトレースを表示します。この設定を選択した場合でも、SQL データベースに対して発行されたリクエストが存在しない場合は、セッションビューアに SQL イベントトレースは表示されません。

キャッシュ

現在のセッションのキャッシュ構成です。下図のように、このリストのオプションは、管理コンソールの [構成] タブの [アプリケーションキャッシュ] ページで定義されたデフォルト設定のキャッシュ構成を上書きします。



このリストのオプションは、現在のセッションのキャッシュ処理のみに影響します。これにより、管理者および開発者は、アプリケーション作成セッション中のキャッシュを一時的に中断することができます。

次のセッションが開始されると、[デフォルト範囲] オプションがこのリストに自動的に割り当てられます。このオプションは、新しいセッションのキャッシュを永続状態にリセットし、実稼働セッションで使用できるようにします。

リストには次のオプションがあります。

デフォルト範囲

ユーザ範囲とも呼ばれるこのオプションを選択すると、データソースの値がキャッシュに保存され、セッションが終了しても LRU キャッシュ統計がクリアされません。これが、[キャッシュ] リストのデフォルト設定のオプションです。これにより、キャッシュされたデータおよびキャッシュ統計をセッション間で永続的に保持することができます。

このオプションでは、選択時には [デフォルト範囲] ラベルが表示され、選択されていない場合は [デフォルト範囲に戻す] ラベルが表示されます。

セッション範囲

選択時には [セッション範囲] ラベルが表示され、選択されていない場合は [セッション範囲に設定] ラベルが表示されます。

キャッシュしない

現在のセッションでキャッシュを停止します。このオプションを選択すると、[セッション範囲に設定] または [デフォルト範囲に戻す] を選択するまでセッション内でキャッシュが停止されます。このオプションでは、選択時には [キャッシュしない] ラベルが表示され、選択されていない場合は [キャッシュオフ] ラベルが表示されます。

キャッシュのリフレッシュ

キャッシュがリフレッシュされ、以前に選択したオプションが即時復元されます。

JS エラーポップアップ

セッショントレースでの JS エラーポップアップメッセージの取得を有効にします。このオプションは、デフォルト設定で [オフ] が選択されています。これは、JS エラーポップアップメッセージがセッショントレースに含まれないことを示します。

セッション開始
アクティブセッションの開始時間が HH.MM.SS フォーマットで表示されます。

最新アクティビティ
アクティブセッション内の最新アクティビティの開始時間が HH.MM.SS フォーマットで表示されます。

URL 回数
表示中の セッションで発行された URL の総数です。

平均レスポンス
表示中の セッションで発行された URL すべての平均レスポンス時間 (秒数) です。

サーバリクエスト
アクティブセッション中に Reporting Server に送信されたリクエスト数です。

平均サーバ時間
Reporting Server がリクエストへの応答に要した平均時間 (秒数) です。

平均 DBMS 時間
TIBCO WebFOCUS 以外のデータベースまたは RDBMS データベースに転送されたリクエストに対して Reporting Server が応答に要した平均時間 (秒数) です。

現在のセッションファイルが存在しない場合、ステータスバーの下に次のメッセージが表示されます。

セッションファイルがありません。

現在のセッションファイルが存在する場合は、ステータスバーの下にそのファイルのトレースがリスト表示されます。

管理者としてログインした場合は、最近完了したセッションがリンクとして表示されるテーブルを開くこともできます。表示可能な複数のセッションが特定の日付で発生した場合、これらのセッションは、発生日付の古い順からテーブルの左から右に表示されます。

完了したセッションの情報は、[トレース削除までの日数] (IBI_TRACE_RETAIN_DAYS) で定義された期間だけ保持されます。

別のセッションを表示するには、メインページまたはセッション詳細ページでセッションリンクをクリックします。選択したセッションのトレースが新しいページに表示されます。

注意：セッションリンクから表示可能なセッションは、完了済みセッションのみです。現在のセッションを表示するには、管理コンソールから [セッションモニタ] ページを開き、[情報] アイコンをクリックします (情報アイコンが表示されている場合)。

セッション詳細ページの表示

セッション詳細ページを開くには、[既存のセッショントレース] 列でセッションリンクをクリックします。下図のように、セッション詳細ページが開きます。

このページの一連の機能を使用して、選択したセッションに関連する詳細を確認したり、そのセッションで作成されたトレースの概要を表示したりできます。また、別のセッションに移動することもできます。

選択したセッションを確認した後、セッション詳細ページを閉じ、メインページに戻ります。

セッション詳細ページを開くと、画面上部にユーザのログイン情報と、選択したセッションの ID が表示されます。

セッション ID の下側のテーブルには、確認するセッションの詳細がリスト表示されます。[ユーザ名] 列のエントリで、表示中のセッションを開始したユーザ名が識別されます。

[表示ファイル] 列のエントリで、表示中のトレースエントリの開始時間を基準にした範囲が識別されます。デフォルト設定では、トレースエントリは開始時間から未定義の終了時間までの全範囲が対象になります。ドロップダウンリストが表示されている場合は、別の時間範囲をドロップダウンリストから選択することができます。

確認するトレース情報の表示を変更するには、次のオプションを使用します。

- **リフレッシュ**　アクティブセッションを開いた後に生成されたトレースをリストに追加します。このオプションは、完了済みセッションに対しては無効です。
- **戻る**　トレース情報の前の画面に戻ります。
- **次へ**　トレース情報の次の画面へ進みます。
- **最後**　セッション終了直前に収集された最終のトレース情報の画面に移動します。
- **表示**　表示するトレースのリストを特定のタイプに限定します。
  - **すべての URL**　静的コンテンツを返す URL (例、.css ファイル、.html ファイル、.js ファイル)、Client アクションを実行する動的 URL、および Reporting Server でアクションを実行する URL を表示します。
  - **作業 URL**　動的 URL および Reporting Server リクエストのみを表示します。この設定がデフォルト値です。
  - **サーバリクエスト**　Reporting Server にアクセスする URL のみを表示します。
- **グループ**　単一ページに表示するトレースエントリ数を指定します。選択可能な値には、1、5、10、25、50、100、200 があります。このフィールドで選択した値は、[戻る]、[次へ]、[最後] オプションに影響します。大きい値を選択すると、前のページまたは次のページに移動する操作回数が減ります。
- **ハイライト**　このテキストボックスに検索文字列を入力し、Enter キーを押すと、その文字列を含むトレースエントリの [開始] 列が黄色でハイライト表示されます。

  たとえば、「short」という文字列を入力すると、次のように「short」を含むトレースエントリの [開始] 列が黄色でハイライト表示されます。

```
IBFS checkPolicy Success
IBFS:/EDA/ACTWIN7/ibisamp/short.mas
```

注意：ハイライトをクリアするには、[ハイライト] テキストボックスから値を削除し、Enter キーを押します。

- **セッショントレース ZIP**　選択したセッションのトレースすべてを単一の ZIP ファイルに保存します。このリンクをクリックすると、プログラムでファイルを開くか、ファイルを保存するかの選択が要求されます。[ファイルを保存する] をクリックして ZIP ファイルの保存先を指定し、[保存] をクリックします。

  この ZIP ファイルのデフォルト名は、ユーザ名の後に、このファイルに含まれるトレースファイルとログファイルの個数が付加された名前になります (例、admin_140841)。

上記のオプションは、トレース情報テーブルの下にも表示されます。

注意：下図のように、2 つのタイムバーをクリックすると、ページがリフレッシュされ、これらのバーが表す 2 つのトランザクション間のタイムラインが表示されます。

確認後、2 つのタイムバーのいずれかを選択し、デフォルト表示に戻ります。

トレース情報テーブルでは、さらに詳細なセッショントレースを個別に確認することができます。このテーブルには、セッション中に収集されたトレース 1 件につき 1 つの概要エントリが表示されます。これらの概要エントリを展開して、トレースで収集された詳細イベントメッセージを表示することができます。

トレース情報テーブルおよび上記のオプションの下には、セッションを開始したユーザエージェントおよびビルドが表示されます。ユーザエージェントを識別する詳細情報として、ブラウザ、オペレーティングシステム、サポートアプリケーションが表示されます。ビルドを識別する詳細情報として、そのセッションの接続先製品のバージョン番号、ビルド番号、生成日付が表示されます。

ページの下部には、最近完了したセッションのリストが表示されます。このリストは、メインページのセッションリストと同一のものですが、セッション詳細ページから別のセッションに直接移動できるようにこのページにも表示されています。

トレースエントリの表示

下図のように、セッション詳細ページのトレースリストの各エントリは、システムアクティビティ 1 件のレコードを表します。

1 つのアクティビティに複数のイベントが含まれている場合があります。トレース横のアイコンをクリックすると、そのトレースの詳細情報が表示されます。

トレースごとに次の情報が表示されます。

開始
トレース内のイベントの開始時刻 (時間、分、秒) です。時間は、24 時間制で表されます。

終了
トレース内のイベントの終了時刻 (時間、分、秒) です。時間は、24 時間制で表されます。

最大 (秒数)
この列タイトルの数字は、リスト内のトレースの中で、完了までに最長の時間を要したトレースの秒数を表します。

下図のように、この列のエントリには、トレース内の各イベントの相対時間を表す時間バーが表示されます。

- バーの青色の部分は、このトレースでイベントの処理に要した Web CPU 時間 (秒数) を表します。また、この色のバーから、作業 URL コンポーネントが含まれたトレースであることが分かります。
- バーの黒色の部分は、データベースからのレスポンスの取得に要した Web 待機時間 (秒数) を表します。また、この色のバーから、作業 URL コンポーネントが含まれたトレースであることが分かります。
- バーの茶色の部分は、このトレースでイベントの処理に要した Reporting Server 時間 (秒数) を表します。また、この色のバーから、サーバリクエストコンポーネントが含まれたトレースであることが分かります。

バーの各部分にマウスポインタを置くと、それぞれの正確な秒数がツールヒントに表示されます。現在のセッションのアクティブトレースを表示している場合、列幅全体に青緑色のバーが表示されます。バーの上にマウスポインタを置くと、そのイベント中に経過した秒数を示すツールヒントが表示されます。

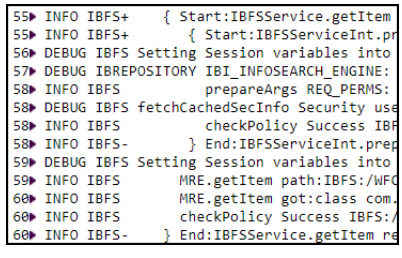
詳細

トレースの ID です。この ID は、トレースイベントを開始したリクエストメッセージの移動先 URL です。URL の最初の語句で、リクエストを開始した Servlet またはその他のアプリケーションが識別されます。各トレース ID は一意です。

URL の ID 番号がオレンジ色でハイライト表示されている場合、そのトレースイベントには 1 つまたは複数のエラーメッセージが含まれています。詳細トレース表示では、エラーメッセージが含まれているイベントもオレンジ色でハイライト表示されるため、エラーの発生時間を簡単に識別することができます。

展開された URL 詳細の表示

トレース詳細リストの各エントリを展開すると、ネストされたリストが開き、システムが生成したメッセージが表示されます。これらのメッセージで、そのトレースで収集されたイベントと、各イベントの発生時間 (ミリ秒) が識別されます。これらのイベントには、Client と Reporting Server 間または Reporting Server と Application Server 間で送受信されたリクエストと応答メッセージが含まれます。また、アプリケーションプログラムがコマンドを実行した際に生成されたエラーメッセージ、情報メッセージ、システムステータスメッセージも含まれます。下図のように、反復イベントまたは従属イベントを表すエントリはネスト形式で表示されるため、これらのイベントを簡単に識別することができます。



トレースエントリはイベント開始時間から始まり、後続のイベント発生時のエントリは、トレース開始時間からのミリ秒で表されます。この値により、各イベントの区別が容易になり、トレース内での各イベントが時系列で表示されます。

イベント開始時間の後に、トレースイベントの IBFS ステータスコードが続きます。

この列には、次のシンボルのいずれかが表示されます。

アイコン	説明
IBFS+	プログラムの開始イベント、あるいはプログラム間またはアプリケーション間でのデータ交換の開始イベントです。
IBFS-	プログラムの終了イベント、あるいはプログラム間またはアプリケーション間でのデータ交換の終了イベントです。
IBFX*	エラーメッセージです。
IBFSX	管理メッセージまたは情報メッセージです。

次に、そのイベントを記述したアプリケーションまたはプログラムによって生成されたメッセージのテキストが表示されます。このセクションに表示されるテキストのタイプは、[表示] ドロップダウンリストから選択したトレースタイプに応じて異なります。

- [すべての URL] または [作業 URL] を選択した場合、URL エントリを展開すると、プログラムの実行時に生成されたステータスメッセージおよびエラーメッセージが表示されます。

  注意：エントリに Reporting Server メッセージが含まれている場合、トレースエントリの下線付きリクエスト ID のリンクから Reporting Server トレースの詳細を表示したり、下線付きレスポンス ID のリンクから Reporting Server レスポンストレースの詳細を表示したりできます。

- [サーバリクエスト] を選択した場合、URL エントリを展開すると、Reporting Server リクエストプロシジャと、そのプロシジャの実行時に生成されたステータスメッセージまたはエラーメッセージのリストが表示されます。これは、セッションモニタの情報アイコンからサーバリクエストリンクを開く場合に表示されるものと同一です。

Reporting Server リクエスト詳細の表示

下図のように、Reporting Server リクエストから収集されたトレースでは、セッション中に Client から Reporting Server に送信されたクエリやその他のリクエスト処理の詳細が識別されます。

```
Plain text:---Focexec-Start--- RequestID=URL56Req1 UrlID=URL56 ReqInfo="Run:Domain=Sales/:App=sales:SubAct=MR_STD_REPOR
....:SET PCHOLD-FMT=XML
....:*WF
....:GKE %MRE USERID admin
....:GKE %MRE DOMAIN Sales/
....:GKE %MRE BASEDIR IBFS:/WFC/Repository/Sales
....:GKE %MRE APPDIR sales
....:GKE %WF FEXNAME cost_of_goods_ytd
....:GKE %WF FULLFEXNAME Cost of Goods YTD
....:GKE %IP 10.98.96.234
....:
0001:EX -LINES 6 EDAPUT FOCEXEC,mrheader,C,MEM,-* mr header include start
0002:-* mr as NOT html
0003:-SET &FOCEXURL=&FOCEXURL | 'IBIMR_drill=IBFS,RUNFEX,IBIF_ex,true' | '&';
0004:SET FOCEXURL='&FOCEXURL'
0005:-* mr header include end
0006:-*
0001:EX -LINES 47 EDAPUT FOCEXEC,cost_of_goods_ytd,C,MEM,ENGINE INT CACHE SET ON
0002:SET PAGE-NUM=NOLEAD
0003:SET SQUEEZE=ON
0004:-DEFAULTH &WF_HTMLENCODE=ON;
0005:SET HTMLENCODE=&WF_HTMLENCODE
0006:
0007:SET HTMLCSS=ON
0008:-DEFAULTH &WF_EMPTYREPORT=ON;
0009:SET EMPTYREPORT=&WF_EMPTYREPORT
0010:
0011:SET EMBEDHEADING=ON
0012:SET GRAPHDEFAULT=OFF
0013:SET COMPONENT=TableChart_1
0014:SET ARVERSION=2
0015:-DEFAULTH &WF_TITLE='WebFOCUS Report';
0016:GRAPH FILE retail_samples/wf_retail_lite
0017:-* Created by Designer for Graph
0018:SUM WF_RETAIL_LITE.WF_RETAIL_SALES.COGS_US
0019:BY WF_RETAIL_LITE.WF_RETAIL_TIME_SALES.TIME_YEAR
0020:ON GRAPH PCHOLD FORMAT JSCHART
0021:ON GRAPH SET VZERO OFF
0022:ON GRAPH SET HAXIS 770.0
0023:ON GRAPH SET VAXIS 405.0
0024:ON GRAPH SET LOOKGRAPH LINE
0025:ON GRAPH SET EMBEDHEADING ON
0026:ON GRAPH SET AUTOFIT ON
0027:ON GRAPH SET STYLE *
0028:*GRAPH_JS
0029:    "injectedRevision" : "$Revision: 1.2 $",
0030:    "dataSetLimits": {"enabled": true},
0031:    "catchErrors" : true
0032:*END
0033:-INCLUDE  __c/theme
0034:TYPE=REPORT, TITLETEXT='Chart1', ARREPORTSIZE=DIMENSION, ARFILTER_TARGET='*', ARGRAPHENGINE=JSCHART, $
0035:TYPE=DATA, COLUMN=N1, BUCKET=x-axis, $
0036:TYPE=DATA, COLUMN=N2, BUCKET=y-axis(1), $
0037:*GRAPH_SCRIPT
0038:
0039:*GRAPH_JS_FINAL
0040:"blaProperties": {
0041:"seriesLayout": "absolute"
0042:}
0043:
0044:*END
0045:ENDSTYLE
0046:END
```

この情報から、リクエストの処理中に送信された変数およびコマンドが識別されます。通常、これらのリクエストは、Client から Reporting Server に送信された TABLE リクエストまたは -HTMLFORM BEGIN/END リクエストです。

プロシジャ上部の先頭行の ID により、そのプロシジャと、トレース生成元のサーバから収集された URL トレースが関連付けられます。たとえば、この ID が URL101 の場合、このプロシジャと、トレース URL101 で収集されたアクティビティ内のサーバリクエストイベント行が関連付けられます。

変数およびコマンドのリストの末尾には、クエリまたはその他の処理の結果を示すステータスメッセージのリストが表示されます。

```
....:SET PCHOLD-FMT=BINARY
     --------End-------- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" Lines=851
     ---Server-Report--- RequestID= URL170Req12 ReportID= URL170Req12Rep Mime= .HTM OutputSizeK= 2 OutputLines= 4 File= URL170Req12Rep.htm N
     ---Message-Start--- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" FocMsgs=0
....:0 NUMBER OF RECORDS IN TABLE=       10  LINES=     10
....:0 HOLDING HTML FILE ON PC DISK ...
     --------End-------- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" FocMsgs=0
     ---Server--Times--- RequestID=URL170Req12 UrlID=URL170 ReqInfo="Run:Domain=Public/:SubAct=MR_STD_REPORT:Fex=WebFOCUS_Report" Reports=1
```

Reporting Server レスポンス詳細の表示

Reporting Server レスポンスから収集されたトレースでは、作業セッション中に Reporting Server から Client に送信されたクエリまたはその他の処理に応答して返された情報が識別されます。

出力トレースを表示するには、URL トレースエントリ内の下線付き URL リクエストレスポンスエントリのリンクをクリックします。以下はその例です。

URL103Req4Resp

下図のように、この表示の最初の部分では、レスポンス処理中に Client に返されたフォーマット変数が識別されます。

```
<!DOCTYPE html>
<html>
<head>
<meta name="HandheldFriendly" content="True">
<meta name="PalmComputingPlatform" content="True">
<meta name='viewport' content='width=device-width, initial-scale=1, maximum-scale=5, user-scalable=1'><title>Report1</title>
<script type="text/javascript">
</script>
<style type='text/css'>
#IBI_popupHere { position:absolute; visibility:hidden; z-index:200; }
</style>
<script language='javascript'>
var ibiOptions = new Array("popupdesc");
var focexurl = "/ibi_apps/WFServlet?IBIF_webapp=/ibi_apps&IBIC_server=EDASERVE&IBIAPP_app=sales&IBIMR_drill=IBFS,RUNFEX,IBIF_ex,true&";
var fochtmlurl = "/ibi_apps/ibi_html";
var serverLanguage='en';
</script>
<script language='javascript' src='/ibi_apps/ibi_html/javaassist/nls.js'></script>
<script language='javascript' src='/ibi_apps/ibi_html/javaassist/ibi/html/js/ibigbl.js'></script>
<style type="text/css">
<!--
TABLE { border-collapse:collapse; }
BODY { background-color:#FFFFFF }
TD { vertical-align:top; padding-left:6pt; padding-right:6pt; }
.x7 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414;
 border-top: 1.00pt SOLID #DBDBDB; border-bottom: NONE; border-right: NONE; border-left: NONE; }
.x6 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414; padding-top:3pt; padding-bottom:3pt;
 border-style: NONE; }
.x4 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414; padding-top:3pt; padding-bottom:3pt;
 border-top: 1.00pt SOLID #DBDBDB; border-bottom: NONE; border-right: NONE; border-left: NONE; }
.x5 { font-family:ARIAL; font-size:9pt; font-weight:normal; font-style:normal; text-decoration:none; color:#141414; padding-top:3pt; padding-bottom:3pt;
 border-top: 1.00pt SOLID #DBDBDB; border-bottom: NONE; border-right: NONE; border-left: NONE; }
.x2 { font-family:ARIAL; font-size:9pt; font-weight:bold; color:#141414;
 border-style: NONE; }
.x3 { font-family:ARIAL; font-size:9pt; font-weight:bold; color:#141414;
 border-style: NONE; }
-->
</style>
<script language='javascript'>
ibigblloadCss(null);
</script>
</head>
```

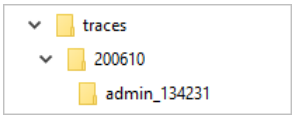
下図のように、この表示の後続の部分では、レスポンス処理中に Client に返されたデータが識別されます。

```
<tr>
<td style="vertical-align:bottom" class='x2'>
COUNTRY</td>
<td style="vertical-align:bottom" class='x3'>
CAR</td>
</tr>
<tr>
<td class='x4'>
ENGLAND</td>
<td class='x5'>
JAGUAR</td>
</tr>
<tr>
<td class='x6'>
</td>
<td class='x5'>
JENSEN</td>
</tr>
<tr>
<td class='x6'>
</td>
<td class='x5'>
TRIUMPH</td>
</tr>
<tr>
<td class='x4'>
FRANCE</td>
<td class='x5'>
PEUGEOT</td>
</tr>
<tr>
<td class='x4'>
ITALY</td>
<td class='x5'>
ALFA ROMEO</td>
</tr>
<tr>
<td class='x6'>
</td>
<td class='x5'>
MASERATI</td>
</tr>
```

デフォルト設定では、「URL###Req##Rep」リンクをクリックすると、セッションビューアにレポート自体が表示されます。結果を HTML フォーマットで表示するには、このファイルをテキストファイルとして保存し、再度開きます。通常、Reporting Server レスポンスには、SQL ベースのクエリ、更新、またはその他のデータベース関連処理に応答して返されたデータまたはステータスメッセージが含まれます。

トレースファイルの保存

セッションビューアでは、下図のように、[traces] ディレクトリ内の一連のファイルにトレース情報が保持されます。これらは、*drive*:¥ibi¥WebFOCUS_WFI¥WebFOCUS¥traces (Windows) または *install_directory*/ibi/WebFOCUS_WFI/WebFOCUS/traces (UNIX または Linux) に格納されています。



このディレクトリ内には、[ログ削除までの日数] (IBI_TRACE_RETAIN_DAYS) 設定で定義された期間に発生したユーザセッションの日付ごとにセッションアクティビティフォルダが作成されています。これらを識別しやすくするために、フォルダのタイトルには作成日 (YYMMDD 形式) が使用されています。

日付ごとのセッションアクティビティフォルダ内には、この日に発生したセッションごとにフォルダが作成されています。このフォルダには、このセッション中に作成されたすべてのファイルが格納され、フォルダ名にはセッション ID の短縮バージョンが使用されます。

セッションレコードの自動収集およびファイリングにより、過去のセッションが検索しやすくなると同時に、ユーザのシステムリソースから過剰なトレースレコードを除外することができます。単一日付のすべてのセッションを含むフォルダのタイトルに日付を使用することで、期限切れトレースファイルを検索し、最大保持期間を超え、削除が可能なフォルダを特定することができます。

セッショントレースをこの自動検索で削除せずに保存する必要がある場合は、トレースディレクトリ内に別のフォルダを作成し、「save」または別の識別しやすい単語を使用して名前を付ける必要があります。この場合、YYMMDD 形式の日付は使用しないでください。次に、セッショントレースファイルの ZIP ファイルを作成し、上記で作成した別のフォルダにこれらを手動で保存します。これらのファイルは、ユーザが削除しない限り、後から確認することができます。

セッションフォルダのコンテンツ

セッションフォルダには、session.log ファイルおよび procedure.log ファイルが、セッション中に呼び出された URL の .trace ファイル、.dat ファイル、.header ファイル、.xml ファイルとともに格納されます。

- .trace ファイルには、URL コールで収集されたシステムイベントのレコードが格納されます。
- .dat ファイルには、URL コールで定義された .html データが格納されます。
- .header ファイルには、URL コールで発生したメッセージのヘッダに含まれるデータが格納されます。
- .xml ファイルには、コールで呼び出された関連パラメータがすべて格納されます。

これらのファイル内の詳細なレコードについては、このセクションの前の項に記載されています。

手順　セッションビューアのトレースファイルをエクスポートするには

名前に YYMMDD 日付フォーマットを使用しないフォルダが [traces] フォルダに作成済みであることを確認します。このフォルダは、*drive:*¥ibi¥WebFOCUS_WFI¥WebFOCUS¥traces (Windows) または *install_directory*/ibi/WebFOCUS_WFI/WebFOCUS/traces (UNIX または Linux) に格納されています。このようなフォルダが存在しない場合は、次の手順を開始する前に作成します。

1. [セッションビューア] を開きます。
2. [セッショントレース ZIP] のリンクをクリックし、現在のセッションを保存します。

   または

   現在のセッションテーブル下部のセッションリストで、前のセッションのリンクをクリックし、[セッショントレース ZIP] を選択してこれを保存します。
3. ブラウザのプロンプトでファイルを開くか保存するかを確認された場合、[名前を付けて保存] を選択します。
4. トレースファイルの次の場所に移動します。

   ```
   drive:¥ibi¥WebFOCUS_WFI¥WebFOCUS¥traces¥undatedfolder¥username_time¥
   ```

   (Windows の場合)

   または

   ```
   install_directory/ibi/WebFOCUS_WFI/WebFOCUS/traces/undatedfolder/
   sessionID
   ```

(UNIX または Linux の場合)

説明

`undatedfolder`
[ログ削除までの日数] (IBI_TRACE_RETAIN_DAYS) パラメータで指定した日数を超えて保持する必要がある、ZIP 化されたセッションファイルを格納するフォルダの名前です。この名前には、YYMMDD フォーマットの日付を使用しないでください。

`sessionID`
セッションに割り当てられたユニーク ID です。セッションを開始したユーザの名前とセッション発生日の時間を組み合わせ、区切り文字にアンダースコア (_) を使用します。

5. ZIP ファイルがターゲットディレクトリに保存されたことを確認し、セッションビューアを終了します。

ログファイルの使用

[ログファイル] ページには、すべてのログファイルへのリンクが一覧表示されます。ここから各ログファイルのページに移動し、ログファイルの内容を即座に確認できるほか、ログファイルのコピーを作成してシステムイベントのレコードを技術サポートに送信し、システム問題発生時のトラブルシューティングやシステム分析に役立てることができます。

このページには、各ログファイルが名前のアルファベット順で表示されます。[ログ名] 列の各エントリの横には、ロガー名のリストが表示されます。各ログファイルのページに表示されるイベントは、ログの記録に関与したイベントがロガーによって収集されたものです。たとえば、audit.log ファイルには、com.ibi.uoa、com.ibi.config、com.ibi.content などのロガーが収集したイベントが記録されます。

ログファイルには、システムイベントのレコードが記録されています。各ロガーの横には、[ログレベル] 列が表示されます。このログレベルで、ロガーが収集するイベントのレベルが識別されます。

ログの各レベルは累加的に機能します。上位のレベルには、それより下位のレベルで収集されるイベントがすべて含まれます。たとえば、レベルを [警告] に設定した場合、収集されるイベントには、警告を生成するイベント以外に、[重大] レベルおよび [エラー] レベルで収集されるイベントも含まれます。

これらのレベルには次のものがあります。

- **オフ**　イベントを収集しません。
- **重大**　システム処理を中断するイベントのみを収集します。

- **エラー**　重大イベント以外に、エラーメッセージを生成するイベントを収集します。
- **警告**　エラーイベントおよび重大イベント以外に、警告メッセージを生成するイベントを収集します。
- **情報**　警告イベント、エラーイベント、重大イベント以外に、情報メッセージを生成するイベントを収集します。
- **デバッグ**　情報イベント、警告エラーイベント、エラーイベント、重大イベント以外に、デバッグメッセージを生成するイベントを収集します。
- **トレース**　デバッグイベント、情報イベント、警告エラーイベント、エラーイベント、重大イベント以外に、トレースメッセージを生成するイベントを収集します。

ログファイルおよびトレースファイルについての詳細は 605 ページの 「 ログの収集 」 を参照してください。

audit ログファイルにはログレベルが事前に割り当てられ、ログレベルを変更することはできません。その他のログファイルでは、ログレベルを調整することができます。ただし、Application Server を再起動すると、すべてのログレベルがデフォルト値に戻ります。

問題の状況をすばやく簡単に特定できるよう、警告イベント、エラーイベント、重大イベントのログエントリが、次のように強調表示されます。

- **警告** - イエロー
- **エラー** - オレンジ
- **重大** - コーラル

色コードで色分けされた強調表示は、エラーまたは問題発生イベントを収集するログエントリと、ルーチンのシステムイベントを収集するログエントリを区別することによって、確認作業やトラブルシューティングをサポートします。3 つのイベントカテゴリのそれぞれに一定の色を使用することで、特定の重大度に関する問題イベントの検索範囲を絞り込むことができます。

これらの強調表示は、ログファイルビューアに適用されるため、[ログファイル] ページからログファイルを開いて参照する場合のみ表示されます。強調表示はログファイルの ZIP ファイルには保存されません。また、別のテキストエディタでログファイルを開いたり参照したりしても表示されません。

[すべて ZIP 化] ボタンをクリックすると、すべてのログファイルおよび systeminfo.xml が単一の ZIP ファイルに保存されます。このボタンを使用して、必要に応じてシステムイベントレコードおよびシステム情報を収集することができます。

[すべてデフォルトに戻す] ボタンを使用して、すべての設定についてログレベルをデフォルト設定に戻し、ログレベルを調整することができます。

ログファイルには、現在の日付の開始時間から ZIP ファイルが作成された時間までのイベントレコードが含まれます。ログファイルに収集されたイベントレコードは、トラブルシューティングや分析に役立ちます。

systeminfo.xml ファイルには、ファイル作成時のシステム情報設定に割り当てられた値のスナップショットが含まれます (例、[JVP プロパティ情報] ページの値、[アプリケーションの設定] ページの値、ライセンス情報)。ファイルの先頭の info-date タグには、ファイル作成時の日付と時間および収集された値が記録されます。

注意：[ログファイル] ページには、Web サービストレースおよび Client トレースは表示されません。これらのトレースを表示するには、セッションビューアまたはセッションモニタを開きます。これらの機能についての詳細は、190 ページの 「 セッションの表示 」 および 187 ページの 「 セッションのモニタ 」 を参照してください。

ログページの使用

ログページには、ログファイルに収集されたシステムイベントレコードが、ログ記録日の古いイベントから最新のイベントの時間順で表示されます。

ログファイルを開いてログを確認するには、[ログファイル] ページで [ログ名] 列のリンクをクリックします。選択したログファイルのページが別のウィンドウで開きます。

ページ上部にログファイル名が表示されます。また、ページ上部のドロップダウンリストには、日付の古いログファイル名が表示されます。このドロップダウンリストに表示される古いログファイル名は、*drive*:¥ibi¥WebFOCUS82¥logs ディレクトリに格納されているログファイルです。ログファイルが保持される日数は、管理コンソールの [構成] タブの [アプリケーションディレクトリ] ページの [ログ削除までの日数] (IBI_LOG_RETAIN_DAYS) 設定で定義されます。

ファイル名の下に [新規トレース行] リンクが表示されます。このリンクをクリックするとログページがリフレッシュされ、現在のログページを開いた後に発生したシステムイベントのエントリが表示されます。新しいレコードは自動的にログファイルに記録されます。この情報の完全性を保持するために、どのユーザもログファイルレコードを更新、変更することはできません。

[最下行へ] リンクをクリックすると、ファイルの最終エントリに直接移動します。このリンクは、エントリ数が多いファイルを確認する際に、最新イベントのエントリに直接移動する場合に役立ちます。同様に、最終エントリの下に表示される [先頭行へ] リンクをクリックすると、ログファイルの最初のエントリに戻り、各機能がページの最上部に表示されます。

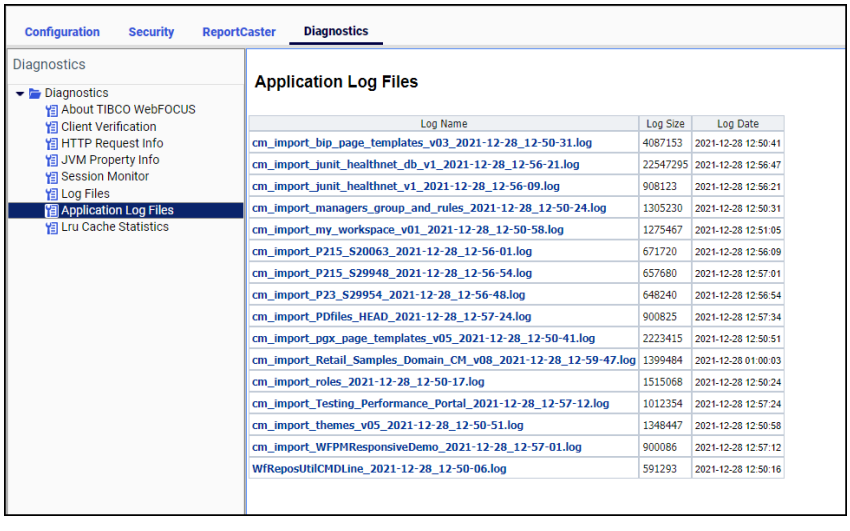
各イベントエントリのリストは、[最下行へ] リンクの下に表示されます。各エントリの名前は、イベントが発生した日付と時間 (時間、分、秒、ミリ秒) から始まります。日付と時間の後に、イベントのカテゴリを示すコード名と、イベント自体の名前が続きます。その次にイベントの説明が続きます。この説明には、イベントに応答してシステムによって生成されたメッセージが含まれます。

技術サポートからの問い合わせに応じて、ログページで特定イベントのレコードを確認、検索することができます。ブラウザの [検索] コマンドを使用して、特定のメッセージ、イベント名、タイムスタンプでイベントを検索することもできます。レコードのリストを上下にスクロールしてイベントを検索こともできます。

確認の完了後、ログページを閉じます。ブラウザの [保存] または [印刷] コマンドを使用してログページのコピーを保存または印刷したり、[ログファイル] ページの [すべて ZIP 化] ボタンを使用してログページの ZIP ファイルを保存したりできます。

アプリケーションログファイルの使用

下図のように、[アプリケーションログファイル] ページには、アプリケーションユーティリティから生成されたログファイルすべてのリンクが表示されます。



アプリケーションユーティリティの実行時に発生したエラーや処理上の問題を分析する必要がある場合、このページでアプリケーションログファイルを特定し、そのファイルに書き込まれたレコードを検証することができます。[アプリケーションログファイル] ページでアプリケーションログ情報を簡単に特定して検証できるため、変更管理のインポートやエクスポートなどのスタンドアロンユーティリティ処理のトラブルシューティングに要する時間が節約されます。このページは、発生した問題の早期解決に役立つとともに、ユーティリティ処理のレコードを技術サポートと共有する手段として利用することもできます。

このページには、各ログファイルが名前順で表示されます。通常、[ログ名] エントリには、ログファイルを生成したアプリケーションユーティリティの名前およびログファイルを作成したユーティリティが実行された日付と時間が表示されます。

たとえば、cm_import_bip_page_templates_v03_2018-06-06_23-50-51.log ファイルは、2018 年 6 月 6 日に発生した BIP ページテンプレート CM パッケージの変更管理インポートからイベントを収集します。ただし、[ログ名] エントリに割り当てられた値は、ログファイルを作成するユーティリティで選択されたデータおよびフォーマットによって異なります。その結果、各ログ名の情報およびフォーマットも異なります。

[ログサイズ] エントリには、ログファイルのサイズがキロバイト単位で表示され、[ログ日付] には、アプリケーションログファイルが作成された日付と時間が YYYY-MM-DD HH:MM:SS フォーマットで表示されます。

このページに表示されるログは、以下のシステムフォルダに格納されているユーティリティによって作成されます。

drive:¥ibi¥WebFOCUS82¥utilities

これらのユーティリティは、変更管理インポートやデータベースの更新などのタスクを実行します。標準的なユーティリティは、製品インストール時にこのシステムフォルダにロードされます。ただし、インストール後にこのフォルダに追加されたその他のユーティリティで作成されたログも [アプリケーションログファイル] ページに表示されます。

アプリケーションログ自体は、システムフォルダに保存されます。

drive:¥ibi¥WebFOCUS82¥application_log

アプリケーションログファイルが保持される日数は、[ログ削除までの日数] (IBI_LOG_RETAIN_DAYS) 設定で定義されます。これは、管理コンソールの [構成] タブの [アプリケーションディレクトリ] ページから設定できます。

アプリケーションログページの使用

アプリケーションログページには、アプリケーションユーティリティの実行時に発生したシステムイベントの詳細な記録が表示されます。イベントは、発生日時によって古いイベントから最新のイベントの順に表示されます。ユーザは、アプリケーションログページを使用して、特定のイベントの記録を確認したり検索したりできます。

アプリケーションログページを開いてログを確認するには、[アプリケーションログファイル] ページで [ログ名] 列のリンクをクリックします。選択したアプリケーションログファイルが新しいウィンドウに開きます。

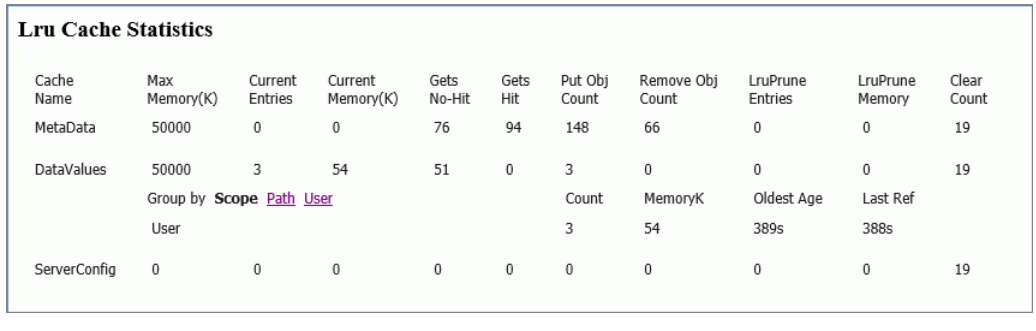
ページ上部にログファイル名が表示されます。[最下行へ] リンクをクリックすると、ファイルの最終エントリに直接移動します。このリンクは、エントリ数が多いファイルを確認する際に、ログ末尾に表示された最新イベントのエントリに直接移動する場合に役立ちます。同じように [先頭行へ] リンクが、最終ログエントリ下部に表示されます。このリンクを使用して、ログファイルの先頭の一番古いエントリに戻ることができます。

イベントのリストは、[最下行へ] リンクの下に表示されます。通常、各エントリは、先頭にイベントが発生した日付と時間 (時間、分、秒、ミリ秒) が表示されます。日付と時間の後に、イベントのカテゴリを示すコード名と、イベント自体の名前が続きます。その次にイベントの説明が続きます。この説明には、イベントに応答してシステムによって生成されたメッセージが含まれます。特に他社製のユーティリティやインストール後に追加されたユーティリティなど一部のユーティリティでは、このパターンに従ってエントリが生成されない場合があります。

確認の完了後、アプリケーションログページを閉じます。ブラウザの [保存] または [印刷] コマンドを使用して、アプリケーションログページのコピーを保存したり印刷したりできます。

LRU キャッシュ統計の使用

LRU (- 最長時間未使用) キャッシュ統計ページには、下図のように、現在のキャッシュ使用統計が表示されます。



Lru Cache Statistics

Cache Name	Max Memory(K)	Current Entries	Current Memory(K)	Gets No-Hit	Gets Hit	Put Obj Count	Remove Obj Count	LruPrune Entries	LruPrune Memory	Clear Count
MetaData	50000	0	0	76	94	148	66	0	0	19
DataValues	50000	3	54	51	0	3	0	0	0	19
	Group by **Scope** Path User					Count	MemoryK	Oldest Age	Last Ref	
	User					3	54	389s	388s	
ServerConfig	0	0	0	0	0	0	0	0	0	19

このページから、各キャッシュに割り当てられた現在リソース量、キャッシュ内のエントリ数、キャッシュに割り当てられたメモリ量、キャッシュにデータを追加したオブジェクト/イベントの数、キャッシュからデータを取得したオブジェクト/イベントの数、キャッシュからデータをクリアしたオブジェクト/データの数、新規データの容量確保のためにキャッシュから古い未使用データを削除したオブジェクト/イベントの数を把握することができます。

ユーザは、これらの統計情報に基づいて、キャッシュ内のアクティビティの現在ステータスを推察したり、メタデータまたはデータソースの値がキャッシュに正しくロードされているかどうかを判断したり、キャッシュ使用量のピーク時を特定し、データまたはメタデータがキャッシュから削除またはクリアされたかどうかを確認したりできます。

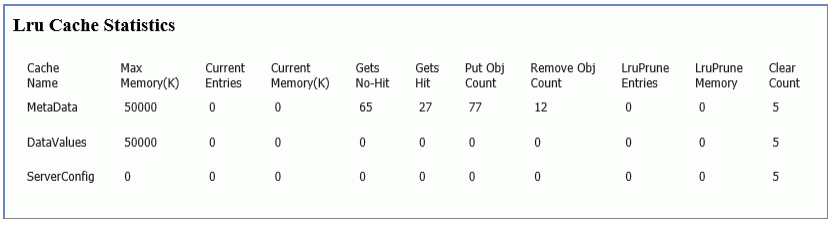
「LRU キャッシュ」は、すべてのキャッシュが「Least Recently Used」という最長時間未使用ルールに従うことを意味します。このルールでは、新規リソースの追加によりキャッシュ使用量が割り当てメモリ量を超える場合、使用されていない期間が最も長いリソースが最初にキャッシュからクリアされます。

[LRU キャッシュ統計] ページを開くには、管理コンソールの [機能診断] タブをクリックし、[LRU キャッシュ統計] を選択します。

このページの統計に割り当てられた値は、キャッシュの処理中に発生したイベントの結果を反映し、このページのエントリレイアウトは、Application Server メモリ内の合計キャッシュ使用量を構成する各キャッシュの構造および各キャッシュ内のレコードの構造に従います。

キャッシュ統計ページレイアウトの理解

[LRU キャッシュ統計] ページのエントリは、下図のようにキャッシュごとに行単位で整理されています。



Lru Cache Statistics

Cache Name	Max Memory(K)	Current Entries	Current Memory(K)	Gets No-Hit	Gets Hit	Put Obj Count	Remove Obj Count	LruPrune Entries	LruPrune Memory	Clear Count
MetaData	50000	0	0	65	27	77	12	0	0	5
DataValues	50000	0	0	0	0	0	0	0	0	5
ServerConfig	0	0	0	0	0	0	0	0	0	5

キャッシュエントリの理解

[LRU キャッシュ統計] ページには、デフォルト設定で次のキャッシュのエントリが表示されます。

メタデータ (MetaData)

このキャッシュは、ユーザがグラフの実行にインサイトモードを選択するたびに Client によって自動的に開始される Reporting Server の呼び出しから生成されるメタデータ値を収集します。これらの呼び出しには、すべてのインサイトグラフで共有される情報、フォント、メタデータに関するサーバへのリクエストが含まれます。このキャッシュにメタデータを配置するリソースへのパス、およびこのキャッシュに割り当てられるメモリ量は事前定義されています。そのため、ユーザがインサイトモードのグラフを選択するとこのキャッシュが自動的に起動されます。このキャッシュおよびその処理を構成する設定は事前定義されており、管理者が設定することはできません。このキャッシュの再構成または調整が必要な場合は、技術サポートに問い合わせてください。

データ値 (DataValues)

このキャッシュは、レポート、グラフ、ポータル、ダッシュボード、その他のコンテンツを作成するユーザが開始したプロシジャのクエリからデータ値を収集します。このキャッシュにデータを配置するリソースへのパスは、[データ値グローバルキャッシュパス] (IBI_DATAVALUES_CACHE_GLOBALPATHS) 設定および [データ値ユーザキャッシュパス] (IBI_DATAVALUES_CACHE_INCLUDEPATHS) 設定で定義されています。これらの設定は、管理コンソールの [構成] タブの [アプリケーションキャッシュ] ページにあります。

サーバ構成 (ServerConfig)

このキャッシュは、ユーザが開始したプロシジャのクエリに明示的に関連しないサーバ処理で使用されたメタデータ値を収集します。このキャッシュにメタデータを配置するリソースへのパス、およびこのキャッシュに割り当てられるメモリ量は事前定義されており、管理者が設定することはできません。このキャッシュの再構成または調整が必要な場合は、技術サポートに問い合わせてください。

キャッシュ統計の理解

[LRU キャッシュ統計] ページの最上部の列は、各キャッシュについて収集された統計を識別します。[Current Entries] および [Current Memory] を除き、これらの統計は複数セッションの累積動作を反映します。これらはキャッシュを終了した場合のみクリアされます。[Current Entries] および [Current Memory] の統計は、[キャッシュのクリア] を実行するとクリアされます。

各キャッシュについて、次の統計が使用できます。

Max Memory (K)

このキャッシュに割り当てられた、Application Server をホストするマシンの最大メモリ量です。[DataValues] キャッシュについては、この列の値は、[DataValues] 行の [データ値最大キャッシュメモリ (MB)] (IBI_DATAVALUES_CACHE_MAXMEG) 設定に割り当てられた値で決定されます。[MetaData] キャッシュおよび [ServerConfig] キャッシュの最大メモリ量は事前定義されており、管理者が設定して再構成することはできません。これらの設定に割り当てられたメモリ量は、[アプリケーションキャッシュ] ページの設定ではメガバイト単位で表示されますが、この統計では同じメモリ量がキロバイト単位で表示されます。そのため、[データ値最大キャッシュメモリ (MB)] (IBI_DATAVALUES_CACHE_MAXMEG) 設定で 50 と表示された値は、このエントリでは 50,000 と表示されます。この値は、管理者が [データ値最大キャッシュメモリ (MB)] (IBI_DATAVALUES_CACHE_MAXMEG) 設定の値を変更しない限り、セッション終了まで保持されます。

Current Entries

現在キャッシュ内に保存されているデータエントリ数です。各エントリには、クエリによって取得されたデータを含むリソースへの IBFS パス、次に各データソース値、このキャッシュにデータを配置するプロシジャを実行したユーザ名、キャッシュにデータが追加された時間および再使用のためにデータが最後に取得された時間を表すタイムスタンプが含まれます。この値は、エントリがキャッシュに追加されたり、キャッシュから削除またはクリアされたりすると変更されます。

Current Memory (K)

キャッシュ内のデータ値による現在のメモリ使用量です。この統計の値を [Max Memory (K)] 統計の値から差し引いた値が、追加のデータに使用可能なメモリ量になります。この値は、データエントリがキャッシュに追加されたり、キャッシュから削除またはクリアされたりすると変更されます。

Gets No-Hit

キャッシュからメタデータまたはデータ値を取得できなかった GET オブジェクトの数です。この数字は、実行されたがクエリからのデータが事前に追加されていなかったためにキャッシュからデータを取得できなかったプロシジャの数を示します。GET オブジェクトによるデータまたはメタデータのキャッシュからの取得が失敗するたびにこの値が増加します。この値が減少することはなく、複数のセッションで累積されます。キャッシュを終了した場合のみ、値がゼロに戻ります。

Gets Hit

キャッシュから値を取得できた GET オブジェクト の数です。この数字は、キャッシュに保存されていたデータを取得できた実行済みプロシジャの数を示します。GET オブジェクトがデータまたはメタデータをキャッシュから取得するたびにこの値が増加します。この値が減少することはなく、複数のセッションで累積されます。キャッシュを終了した場合のみ、値がゼロに戻ります。

Put Obj Count

プロシジャからキャッシュに取得されたデータ値をロードした PUT オブジェクトの現在の数です。PUT オブジェクトがデータまたはメタデータをキャッシュに追加するたびにこの値が増加します。この値が減少することはなく、複数のセッションで累積されます。キャッシュを終了した場合のみ、値がゼロに戻ります。

Remove Obj Count

LRU のプルーニングプロセスに対応して、キャッシュからデータ値を削除した REMOVE オブジェクトの現在の数です。REMOVE オブジェクトがキャッシュからのデータまたはメタデータを削除するたびにこの値が増加します。この値が減少することはなく、複数のセッションで累積されます。キャッシュを終了した場合のみ、値がゼロに戻ります。

LruPrune Entries

新しいプロシジャから発行されたクエリに応答してキャッシュに追加する必要があるメタデータまたはデータの容量確保のために、キャッシュから削除された最長時間未使用 (LRU) エントリの数です。最長時間未使用エントリは、プロシジャによる再使用のために Get Objects でリクエストされることがなかったキャッシュ内の最も古いエントリです。この値は、Put Objects からの新しいデータまたはメタデータ用のメモリ領域を空にするために、キャッシュからデータエントリが削除されるたびに増加します。この値が減少することはなく、複数のセッションで累積されます。キャッシュを終了した場合のみ、値がゼロに戻ります。

LruPrune Memory

新しいプロシジャから発行されたクエリに応答して追加する必要があるメタデータまたはデータソース値の容量確保のために、最長時間未使用 (LRU) エントリがキャッシュから削除された際に解放されたメモリ量です。最長時間未使用エントリは、プロシジャによる再使用のために Get Objects でリクエストされることがなかったキャッシュ内の最も古いエントリです。この値は、各 LRU の削除処理で解放されたメモリ量の累積値を表します。現在の空きメモリ容量を表すものではありません。

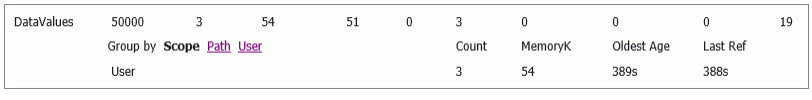
Clear Count

現在のセッション中にユーザが開始した [キャッシュのクリア] イベントの数です。ユーザが、管理コンソールのメニューバーで [キャッシュのクリア] コマンドをクリックするたびにこの値が増加します。キャッシュをクリアするコマンドを含むプロシジャの実行によってもこの値は増加します。この値が減少することはなく、複数のセッションで累積されます。キャッシュを終了した場合のみ、値がゼロに戻ります。

キャッシュグループエントリの理解

キャッシュエントリは、ユーザ ID またはエントリのデータ取得元のマスターファイルへのパスによってグループ化することができます。どちらのグループも、キャッシュに転送されたデータの取得元を示し、キャッシュ内のデータの最新の割り当てまたは取得を評価するために役立ちます。

サブセクションによるグループは、下図のように各アクティブキャッシュ行のすぐ下に表示されます。このサブセクションは、現在のセッション中にユーザアクティビティによって値が追加されると表示され、ユーザがキャッシュをクリアするか Application Server のシャットダウンによってキャッシュが終了するまで表示が保持されます。



このサブセクションには、[Scope]、[Path]、[User] でグループ化された追加のキャッシュ統計の概要が表示されます。[Scope] でグループ化された場合、このセクションの統計は、キャッシュ内のすべてのユーザおよびパスについて概要統計を示します。[User] でグループ化された場合、このセクションの統計は、キャッシュにデータまたはメタデータを追加した各ユーザについて概要統計を示します。セクションは、ユーザごとに 1 行で表示されます。[Path] でグループ化された場合、このセクションの統計は、キャッシュにデータまたはメタデータを追加した各リソースについて概要統計を示します。セクションは、パスごとに 1 行で表示されます。

これらのグループ化オプションを使用して、このセッションのクエリで取得された IBFS パスを特定し、このサブセクションの統計をセッション別、ユーザ別、またクエリ別 (IBFS パスで表示) に評価することができます。

各オプションは次のグループ統計を示します。

Count

各ユーザまたはパスのキャッシュに現在保存されているメタデータまたはデータソースのエントリ数です。これは選択した [Group by] オプションによって異なります。[Group by] オプションが [Global] に設定されている場合、この値はキャッシュ全体の値と一致します。

MemoryK
各セッション、ユーザまたはパスのキャッシュに現在保存されているメタデータまたはデータソースが使用するメモリ量です。これは選択した [Group by] オプションによって異なります。[Group by] オプションが [Global] に設定されている場合、この値はキャッシュ全体の値と一致します。

Oldest Age
各ユーザまたはパスのキャッシュに保存されたメタデータまたはデータソースの最長保有時間 (分数) です。

Last Ref
キャッシュからの最後のデータ呼び出しからの経過時間 (分数) です。

キャッシュは、システム処理で開始されると統計の表示が開始され、Application Server のシャットダウンで終了すると統計の表示が終了します。

このページの統計は、記録または保存されません。[Group by] サブセクションの統計および [Current Entries]、[Current Memory] の統計以外の統計は累積値で表され、セッション間で保持されます。現在の統計は、キャッシュの現在の状態のスナップショットとして機能します。累積統計は、各キャッシュの存続期間中に発生したアクティビティの継続的な記録として機能します。

DBA パスワードの設定

DBA パスワードは、Reporting Server 上のデータソースへのアクセスを定義します。各データソースの記述には、データソースへのアクセスに適切なパスワードを指定することができます。必要に応じて、各パスワードを特定のアクセスタイプ、条件、および規則と関連付けることもできます。これにより、行レベルまでアクセスを制限することができます。

SET PERMPASS=*password* コマンドは、データソースへのアクセス用のパスワードを確立します。ユーザはこのパスワードを変更することはできません。サーバでこのコマンドに値を割り当てるには、SET PERMPASS=&FOCSECUSER を使用します。[DBA ソース] (IBIF_DBAPASS_SRC) 設定を使用して、PERMPASS コマンドをリクエストごとに Reporting Server に送信するかどうかを制御することができます。

データベースセキュリティについての詳細は、『TIBCO WebFOCUS メタデータリファレンス』を参照してください。

各リクエストに DBA パスワードを設定して、BI Portal から Reporting Server 上のデータソースへのシングルサインオンを確立します。

TIBCO ReportCaster は、TIBCO ReportCaster へ暗号化されて送信される DBA パスワードもサポートします。単一パスワードを複数のグループに関連付けることが可能であるため、DBA パスワードにはグループ ID を割り当てることはできません。DBA パスワードは、ドメイン ID、ユーザの HREF、ユーザ指定の変数のいずれかに設定されます。

手順　DBA パスワードを設定するには

1. 管理コンソールの [構成] タブで、[アプリケーションの設定] フォルダ下の [Client 設定] をクリックします。
2. [DBA ソース] (IBIF_DBAPASS_SRC) 設定をデフォルト値の [オフ] にすると、Reporting Server データベースリクエストとともに、Client から BI Portal ユーザ ID が送信されなくなります。
3. [DBA ソース] (IBIF_DBAPASS_SRC) 設定のリストから [IBIMR_user] を選択すると、データベースリクエストとともに、BI Portal ユーザ ID が Reporting Server に送信されます。
4. [保存] をクリックします。

   変更が保存されたことを示すメッセージで [OK] をクリックします。

ユーザ ID の取得

レポートリクエストでユーザ ID にアクセスするには、保護された Reporting Server 変数 &FOCSECUSER を使用します。この変数には、Reporting Server セキュリティがオフの場合を除いて、接続中のユーザ ID が格納されます。GETUSER や CNCTUSR サブルーチンなどの従来の方法より、&FOCSECUSER を使用することをお勧めします。

プロシジャまたは構成ファイルで変更ができない DBA パスワードを接続済みのユーザ ID から設定するには、次のサンプルコードを Reporting Server プロファイル (edasprof.prf) の任意の位置に配置します。

```
SET PERMPASS = &FOCSECUSER
```

DBA セキュリティについての詳細は、『TIBCO WebFOCUS メタデータリファレンス』を参照してください。

ディファード処理

ディファードは BI Portal 機能の 1 つで、ユーザはバックグラウンドで実行する BI Portal プロシジャを送信することができます。その後、実行済みレポート出力を BI Portal の [ディファードレポートステータス] インターフェースで表示することができます。これは、ブラウザがリクエストの終了を待機する即時実行プロシジャとは対照的です。

セキュリティの観点からは、ディファードリクエストは、Reporting Server では即時リクエストと同様に受け入れられます。Reporting Server セキュリティが有効な場合、ディファードリクエストは、Reporting Server の有効なユーザ ID とパスワードで接続する必要があります。

リクエストが完了すると、その出力は Reporting Server の *drive*:¥ibi¥srv*nn*¥wfs ディレクトリ内のファイルに格納されます。ここで、*nn* は現在のリリース番号を表します。出力とともに、リクエストやその他の情報を送信したユーザ ID を含むファイルが作成されます。Reporting Server では、出力ファイルの取得と削除、ステータスの確認ができるのは、ディファードジョブを送信したユーザのみです。Reporting Server 管理者 (edaserve.cfg ファイルにキーワード server_admin_id で識別されたユーザ) もディファード出力を表示、削除できますが、これはファイルレベルまたは Reporting Server コンソールからのみ可能です。

注意：デフォルト設定では、ディファードリクエストを削除する際に確認メッセージが表示されます。この場合、削除を確定するまでに 2 回のクリックが必要です。削除の確認を省略するよう設定することもできます。その場合は、1 回のクリックで削除が確定されます。この設定についての詳細は、557 ページの 「 ディファードレポート設定 」 を参照してください。確認メッセージを省略すると、削除回数が多い場合に時間を短縮できます。

Reporting Server を起動したユーザ ID のみが読み取りおよび書き込みアクセスを持つよう、dfm_dir へのアクセスを制限する必要があります。認証されていないユーザがディレクトリへアクセスできないよう、読み取りアクセスを制御する必要があります。

ディファードチケットは、ユーザのディファードリクエストごとに BI Portal リポジトリに格納されます。チケットは BI Portal ユーザごとに格納されます。管理者 ID でマネージャモードを使用する場合を除き、ユーザには各自のディファードチケットのみが表示されます。チケットには、出力の格納先の Reporting Server ノードが記述されています。

ユーザがディファードステータスを要求すると、ユーザのチケットはすべて一度に処理されます。サーバからのステータスの取得に認証情報が必要な場合、動的なサーバログインフォームが表示されます。1 つ以上のサーバが一時的に利用できない場合、これらのチケットのステータスは「unknown (不明)」として表示されます。

たとえば、あるユーザが「user1」というユーザ ID でディファードリクエストを送信し、翌日、同一ユーザが「user2」というユーザ ID で同一リクエストを送信後、ディファードステータスを確認すると、ユーザは前日のリクエストにアクセスすることができず、エラーメッセージが表示されます。

最初のレポートにアクセスするには、ユーザはセッションを終了し、Reporting Server に「user1」としてログインする必要があります。

レポートリクエストの停止

管理者は、URL にリクエストパラメータを使用することで、実行中のレポートリクエストを停止することができます。

参照　レガシー環境でのセルフサービスリクエストの停止

次のリクエストパラメータを使用して、ユーザはレガシーセルフサービスアプリケーションまたはレガシー環境で、任意のレポートリクエスト、またはリクエストグループを停止することができます。このパラメータは、リクエストの URL で、次のように指定します。

```
http://server:port/context/WFServlet?
IBIWF_action=STOPREQ&IBIWF_USER_REQUEST_ID=ALL
```

現在のブラウザセッションから開始された、すべてのリクエストを停止します。

```
http://server:port/context/WFServlet?
IBIF_ex=procedure_name&IBIWF_USER_REQUEST_ID=value
```

IBIF_ex で指定されたレポートプロシジャを実行し、IBIWF_USER_REQUEST_ID パラメータで指定された任意の値を割り当てます。ここで、「ALL」はすべてのリクエストを停止するキーワードとして予約されているため、IBIWF_USER_REQUEST_ID パラメータの値として使用することはできません。

リクエストに IBIWF_USER_REQUEST_ID パラメータの任意の値が含まれている場合、ユーザは、次の URL を使用し、停止するリクエストの IBIWF_USER_REQUEST_ID 値を指定することで、リクエストまたはリクエストグループを停止することができます。

```
http://server:port/context/WFServlet?
IBIWF_action=STOPREQ&IBIWF_USER_REQUEST_ID=value
```

リクエストの URL に、IBIWF_USER_REQUEST_ID 値が同一のプロシジャ名が複数存在する場合、すべてのリクエストが停止されます。

リクエストがキャンセルされると、次のメッセージが表示されます。

```
リクエストがオペレータにより中止されました。
```

データの出力中にリクエストが停止されると、次のメッセージがレポート出力に表示されます。

```
このレポートは無効です。データ抽出がキャンセルされたか、
ジョブが停止されています。
```

注意：[リクエストの停止] メニューオプションを使用した場合でも、ディファードリクエストおよび TIBCO ReportCaster ジョブは停止されません。

4

認証と認可

ここでは、WebFOCUS Client で認証および認可を構成する方法について説明します。認証は、ユーザまたはプログラムを識別するプロセスです。認可は、認証済みのユーザまたはプログラムが実行可能な機能およびアクセス権限を決定するプロセスです。

認証は、WebFOCUS で実行することも、LDAP ディレクトリなどの外部ソースで実行することもできます。また、ユーザやプログラムを事前認証することもできます。この認証方法では、特定のシステムが認証を実行し、別のシステムがその認証を信頼するという関係になります。認可は、内部認可にすることも、外部認可にすることもできます。複数の認証ソースと認可ソースの同時使用がサポートされます。

トピックス

認証の理解

認証とは、システムでユーザやプログラムを識別するためのプロセスです。認証には、個別ユーザにより対話的に入力される場合、またはプログラムにより自動的に入力されたユーザ ID とパスワードの確認が含まれる場合があります。これらの方法は、フォームベース認証と呼ばれます。また、ユーザやプログラムを事前認証することもできます。この認証方法では、特定のシステムが認証を実行し、別のシステムがその認証を信頼するという関係になります。

ユーザ認証には多数のオプションがあります。デフォルト設定では、内部リポジトリに格納された情報に基づいてユーザの認証が行われます。WebFOCUS アカウントポリシーを使用した内部認証は安全性の高い方法ですが、多くの組織では、従来からユーザアカウント情報を製品の外部で一元的に管理しています。

WebFOCUS では、これらの外部ソース (例、Microsoft Active Directory (AD)、LDAP ディレクトリ) を使用してユーザを認証するよう 構成することも、リレーショナルデータベース管理システム (RDMBS) テーブルに格納されている情報を使用するよう構成することもできます。また、事前認証を使用するよう WebFOCUS を構成することもできます。事前認証では、WebFOCUS は別のシステムで実行された認証を信頼します。別のシステムの例として、Web サーバ、インターネットアイデンティティプロバイダ、Web アクセス管理システム、別のアプリケーションなどがあります。

アプリケーション内の異なるポイントに、異なる認証の要件が存在する場合がよくあります。計画時の早い段階で次のことを考慮しておくことが大切です。

- 認証の実行場所

  通常、認証を実行する場所は、最も強力なセキュリティ実装を提供し、最も機密性の高いデータを格納するプラットフォームを基準に選定します。認証の実行場所をオペレーティングシステムへのログイン時にすると、特定のアプリケーションにアクセスする際に、認証レイヤがさらに必要になる場合があります。一方、オペレーティングシステムへのログイン時の認証で、要件がすべて満たされる場合もあります。この場合、ユーザを再認証することなく、すべての認証済みユーザのリソースへのアクセスが許可されることになります。

- パスワードの管理方法

  格納するパスワード、および環境内でパスワードを格納する場所を決定します。パスワードの有効期限を設定します。パスワードの長さや許容する文字など、パスワードに適用する複雑性の要件を指定します。

- システムへのログイン時にユーザに要求する認証情報の入力回数

操作性を向上させるには、処理の中断回数を最小限に抑え、パスワードを記憶させておく方法も考慮します。

環境ごとに異なるセキュリティモデルのサポート

企業では、開発環境、テスト環境、実稼動環境のそれぞれで異なるセキュリティモデルを実装している場合がよくあります。たとえば、実稼働環境では、WebFOCUS Reporting Server は通常、複数の認証済みユーザに代わって、データへのアクセスに単一サービスアカウントを使用します。これにより、レポートシステムを使用するユーザがリクエストを送信し、ユーザごとのログインユーザ ID を持たない RDBMS 内のデータからレポートを生成することが可能になります。一方、開発環境では、開発者が独自の RDBMS ログインユーザ ID を使用して、機密性の高い開発データへのアクセスを制御している場合もあります。これらの要件をサポートするために、開発環境では WebFOCUS Reporting Server に対してユーザを認証し、実稼動環境では通常のセキュリティプロバイダまたはシングルサインオンアプリケーションを使用してユーザを認証することができます。

ほとんどの場合、テスト環境と実稼動環境では同一のセキュリティモデルが使用されます。

「ユーザを記憶する」機能

内部認証または外部認証を使用するよう環境を構成した場合は、[ユーザをこのコンピュータに記憶する] 機能を有効にすることで、ログインページを省略するオプションをユーザに提供することができます。認証に成功した後、信頼済みログイン Cookie がローカルのワークステーションに保存されます。デフォルト設定では、保存期間は 14 日間です。このログイン Cookie には、ユーザパスワードは格納されません。

注意：事前認証を使用する場合は、この機能を有効にしないでください。[ユーザを記憶する] チェックボックスは、ユーザがログインする際にのみ表示されるため、認証済みユーザにこの機能が表示されることはありません。

手順　「ユーザを記憶する」機能を有効にするには

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。

1. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
2. [認証] ページで [Remember Me 認証] を選択し、[編集] をクリックします。
3. [ログインリクエストは、常に Remember Me リクエストです] のチェックをオンにします。

注意：[Cookie 名] テキストボックス、および [ログインリクエストで Remember-Me が要求されたかどうかを確認するパラメータ名] テキストボックスの値は、技術サポートからの指示がない限り変更しないでください。

4. すべての Remember Me ログインにセキュア Cookie を使用するには、[セキュア Cookie の使用] のチェックをオンにします。

   注意：このチェックをオンにすると、この Cookie に「/secure」フラグが設定され、HTTPS 接続経由でのみ送信されます。

5. [OK] をクリックします。
6. [アクション] セクションで [有効にする] をクリックし、次に [保存] をクリックします。
7. 確認メッセージのダイアログボックスで [OK] をクリックします。
8. Web アプリケーションの再ロードを要求するメッセージダイアログボックスで [OK] をクリックします。
9. 現在のセッションからログアウトします。
10. サーバを停止し、再起動します。
11. 管理者として再度サインインし、管理コンソールに戻って新しい構成をテストします。

手順　「ユーザを記憶する」機能を無効にするには

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
3. [認証] ページで [Remember Me 認証] を選択し、[編集] をクリックします。
4. [ログインリクエストは、常に Remember Me リクエストです] のチェックをオフにします。
5. [セキュア Cookie の使用] のチェックがオンになっている場合は、オフにします。

   注意：[Cookie 名] テキストボックス、および [ログインリクエストで Remember-Me が要求されたかどうかを確認するパラメータ名] テキストボックスの値は、技術サポートからの指示がない限り変更しないでください。

6. [OK] をクリックします。
7. [アクション] セクションで [無効にする] をクリックし、次に [保存] をクリックします。

8. 確認メッセージで [OK] をクリックします。
9. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
10. 現在のセッションからログアウトします。
11. サーバを停止し、再起動します。
12. 管理者として再度ログインし、管理コンソールに戻って新しい構成をテストします。

事前認証、外部認証、外部認可の構成

事前認証、外部認証、外部認可を構成するには、次のタスクを実行する必要があります。

1. 外部認証ソース内のアカウントに一致する名前で、WebFOCUS 管理者アカウントを作成します。
2. 事前認証または外部認証を構成する前に、WebFOCUS へのバックアップアクセスを確保しておくことを強くお勧めします。外部認証または外部認可の場合、スーパーユーザを構成します。事前認証の場合、代替ゾーンを有効にする方法もあります。
3. WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続を構成します。
4. デフォルト認証、代替認証、モバイル認証、ポートレット認証にそれぞれ異なる認証方法を使用するには、その要件をサポートするようセキュリティゾーンを構成します。
5. 事前認証の場合、組織での要求に応じて適切な事前認証を構成します。外部認証または外部認可の場合、WebFOCUS Reporting Server でセキュリティプロバイダを構成した後、WebFOCUS Reporting Server へのログインを認証するよう WebFOCUS Client を構成します。
6. 外部認可の場合、外部グループをマッピングします。

手順　外部ソース用の TIBCO WebFOCUS 管理者アカウントを作成するには

通常、WebFOCUS 管理者アカウント「admin」は外部ソースに存在しないため、事前認証または外部認証が正しく構成された後では、この管理者アカウントでは認証されなくなります。これから作成するアカウントは WebFOCUS と外部ソースの両方に存在することになるため、新しい認証構成で WebFOCUS を再起動した後は、WebFOCUS への管理者アクセスにそのアカウントを使用できるようになります。

作成する WebFOCUS 管理者アカウントのユーザ ID は、外部ソース内のアカウントに一致させる必要があります。ただし、そのアカウントは、外部ソース内の管理者である必要はありません。たとえば、Web アクセス管理システムによる事前認証を構成する場合は、WebFOCUS ユーザ名を Web アクセス管理システムのユーザ ID に一致させる必要があります。

LDAP による外部認証を構成する場合は、WebFOCUS ユーザ名を LDAP のユーザ名に一致させる必要があります。Windows による事前認証を構成する場合は、Windows アカウントからドメイン名を除いた名前を指定します。

1. セキュリティセンターの [ユーザ] ウィンドウで [新規ユーザ] をクリックします。
2. 外部ソースのアカウントのユーザ ID と同一のアカウント名を入力します。
3. パスワードを入力し、確認用にパスワードを再入力します。

   注意：事前認証または外部認証を使用して WebFOCUS にログインする場合、このパスワードは無視されます。ただし、デフォルトゾーンで事前認証を構成し、代替ゾーンを有効にしている場合、[外部セキュリティタイプ] をブランクにすると、代替ゾーンからログインした際にこのパスワードが確認されます。
4. 必要に応じて、説明および Email アドレスを入力します。
5. [作成先グループ] ドロップダウンリストから [GroupAdmins] を選択します。アカウントのステータスは [アクティブ] のままにします。
6. [OK] をクリックして変更内容を保存し、[新規ユーザ] ダイアログボックスを閉じます。
7. セキュリティセンターを閉じるか、セキュリティセンターから移動ます。

ここで作成した WebFOCUS アカウントは、新しい認証構成で WebFOCUS を再起動した後、管理者アクセスに使用します。次に、WebFOCUS へのスーパーユーザアクセスを有効にする手順へ進みます。

手順　スーパーユーザアクセスを有効にするには

スーパーユーザアクセスは、その他すべてのセキュリティルールを上書きします。スーパーユーザアカウントは、事前認証、外部認証、または外部認可が正しく構成されていない場合や使用できない場合でも、WebFOCUS へのアクセスが内部認証されます。スーパーユーザアカウントは、認証を構成する際に管理者アカウントでログインの問題が発生した場合にのみ使用します。事前認証または外部認証が正しく構成されていることが確認された後、スーパーユーザアクセスを無効にするか、スーパーユーザパスワードを保護する必要があります。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティの構成] フォルダ下の [詳細] をクリックします。
3. [ルートユーザ] テキストボックスに、スーパーユーザのアカウント名を入力します。[ルートパスワード] テキストボックスに、スーパーユーザのパスワードを入力し、[保存] をクリックします。

   注意：構成完了後に使用するために作成した WebFOCUS 管理者アカウントは指定しないでください。

4. 変更が保存されたことを示すメッセージで [OK] をクリックします。
5. キャッシュのクリアを要求するメッセージで [OK] をクリックします。
6. 管理コンソールのメニューバーで [キャッシュのクリア] をクリックします。
7. キャッシュのクリアを確認するメッセージで [OK] をクリックします。

これで、指定したアカウントのスーパーユーザアクセスが有効になりました。事前認証を構成する場合は、必要に応じて代替ゾーンを有効にすることができます。これにより、事前認証が正しく構成されていない場合でも、スーパーユーザでのログインが可能になります。

外部認証を構成する場合は、ログアウト後に新しいスーパーユーザ認証情報で再度ログインすることで、スーパーユーザアクセスをテストすることができます。

スーパーユーザアクセスを確認した後、WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続を構成する手順へ進みます。

手順　Apache Tomcat のリバースプロキシを構成するには

Apache Tomcat Application Server でリバースプロキシ構成を使用する場合は、server.xml ファイルの設定を構成し、すべての URL コールが、内部サーバではなく Web 側プロキシサーバのアドレスを使用するようにします。このように構成しない場合、Microsoft Excel 2007 レポートへのドリルダウンなど、一部の機能がプロキシサーバではなく、内部ホストマシンから情報を取得します。

Apache Tomcat の server.xml ファイルを変更するには、次の手順を実行します。

1. 次のディレクトリへ移動します。

   ```
   <Tomcat_Home>¥conf
   ```

   説明

   `<Tomcat_Home>`
   システムで、Apache Tomcat がインストールされているパスです。

2. server.xml ファイルをテキストエディタで開きます。
3. 次のように、proxyName パラメータおよび proxyPort パラメータを追加します。

   ```
   <!-- Define a Coyote/JK2 AJP 1.3 Connector on port 8009 -->
   <Connector port="8009"
       enableLookups="false" redirectPort="8443" debug="0"
       protocol="AJP/1.3" proxyName="WEB-FACING PROXY_SERVER"
       proxyPort="WEB FACING PROXY_PORT" />
   ```

4. proxyName パラメータ値に、Web 側プロキシサーバの完全修飾ホスト名を指定します。
5. proxyPort パラメータの値に、Web 側プロキシサーバのポート番号を指定します。

6. server.xml ファイルに加えた変更を保存します。
7. Apache Tomcat Application Server を再起動します。

セキュリティゾーン

一部の WebFOCUS 展開では、単一環境で複数の認証方法をサポートすることが便利な場合があります。たとえば、エンドユーザは Web アクセス管理システムで事前認証するが、管理者はユーザ ID とパスワードでログインできるようにする場合があります。別の例として、社内の従業員は Windows 認証で事前認証する必要があるが、顧客には各自の LDAP ユーザ ID とパスワードを入力するログインページを提示する場合があります。

WebFOCUS モバイルおよびポータルのオプションには、特別な認証要件もあります。
WebFOCUS では、セキュリティゾーンを使用することで、構成可能な条件に応じてさまざまな認証方法がサポートされます。各ゾーンは、*drive*:¥ibi¥WebFOCUS82¥config ディレクトリ (Windows)、または *installdirectory*/ibi/WebFOCUS82/config ディレクトリ (UNIX または Linux) に格納されている構成ファイルで定義します。

下表は、各セキュリティゾーンについての説明です。

ゾーン	構成ファイル	説明
デフォルトゾーン	securitysettings.xml	デフォルト設定では、他のゾーンのいずれかで処理されないリクエストのフォームベース認証をサポートします。 **ヒント：**このゾーンは、ユーザベースで使用されるプライマリ認証タイプに対して構成します。
代替ゾーン	securitysettings-zone.xml	デフォルト設定では、WebFOCUS Client マシンにインストールされた Web ブラウザで WebFOCUS にアクセスする管理者のフォームベース認証をサポートします。
ポートレットゾーン	securitysettings-portlet.xml	SharePoint などの WebFOCUS Open Portal Services 製品の認証方法を定義します。

デフォルトゾーンは常に有効になっています。このゾーンでは、プライマリ認証方法を構成します。

デフォルトゾーンでは、フォームベース認証以外に、1 つの事前認証方法を構成することができます。このゾーンでは 2 つの認証方法を構成できるため、このゾーンでユーザの事前認証情報を管理できる一方、ユーザの事前認証情報を上書きする必要がある場合は、デフォルトログインページまたはカスタムログインページでユーザにログイン認証情報の入力を要求することができます。

たとえば、デフォルトゾーンにフォームベース認証以外に IWA 認証を割り当てる場合、ユーザが自身のワークステーションからログインする際は IWA 事前認証を信頼し、ユーザが他のワークステーションからログインする際はフォームベース認証を使用するよう構成することができます。

ユーザが他のワークステーションからログインする際は、ログイン試行ごとにユーザに認証情報の入力が要求されます。これにより、そのワークステーションで設定されているデフォルト IWA 認証情報が上書きされるため、そのワークステーションを使用する未認証ユーザがデフォルト認証情報に基づいてアクセスできなくなります。ユーザが自身のワークステーションからログインする際は、ログイン試行ごとにユーザ ID とパスワードを入力する必要はなく、代わりに IWA 認証を信頼します。

ただし、デフォルトゾーンで 2 つの異なる認証方法を構成し、事前認証方法にカスタムログアウトページを定義した場合、そページがデフォルトログアウトページの代わりに使用されます。この構成を採用する場合、構成可能なカスタムログアウトページは 1 つのみです。

代替ゾーンでは、ユーザのネットワーク上の場所に基づいて使用されるセカンダリ認証方法を設定することができます。デフォルト設定では、代替ゾーンは無効になっています。代替ゾーンはネットワークアドレス localhost (TCP/IPv4 では 127.0.0.1、TCP/IPv6 では 127:0:0:1::1) から送信されたリクエストを処理するよう事前に構成されています。ただし、この構成は変更することができます。管理者のワークステーションアドレス、リバースプロキシ、リモートデスクトップ接続に適した別マシンなどのアドレスを追加または削除することができます。

構成済みのアドレスではワイルドカードがサポートされるため、アドレスを個別に指定する以外に、IP アドレスの範囲を指定することもできます。アスタリスク (*) は任意の数の文字に一致し、疑問符 (?) は単一文字に一致します。次の例は、サンプル securitysettings-zone.xml ファイルの一部を示しています。

```
<property name="filterChainEnabled" value="true"/>
<property name="filterChainPatternEnabled" value="true"/>
         <property name="filterChainPatterns">
            <list>
                  <value>/**</value>
             </list>
       </property>
<property name="filterChainIPAddresseEnabled" value="true"/>
<property name="filterChainIPAddresses">
             <list>
                  <value>127.0.0.1</value>
                  <value>172.30.240.1</value>
                  <value>172.30.???.??1</value>
                  <value>172.30.239.*</value>
             </list>
</property>
```

注意：監査ログファイルには、各ユーザセッションに関連する TCP/IP アドレスが記録されます。この情報は、セキュリティゾーンの構成に関する問題が発生した際のトラブルシューティングに役立ちます。

代替ゾーンでユーザにログインページを提示する場合、そのユーザは WebFOCUS ログインページにリダイレクトされます。次の例のように、ログイン URL にゾーンインジケータが追加されます。

```
http://localhost/ibi_apps/zone/signin
```

モバイルゾーンおよびポートレットゾーンは、これらのオプション製品をサポートするよう事前に構成されており、通常はこの構成を変更する必要はありません。

ゾーン別のログアウト URL の指定

各ゾーンにそれぞれ異なるログアウト URL を指定することができます。ゾーンのログアウト URL を指定しない場合、この URL は、デフォルト値の「/signout」になります。このデフォルト値は、[認証オプション] ダイアログボックスの [カスタムログアウトターゲット URL] で設定された値です。ただし、この設定は、各ゾーンの [カスタムログアウトターゲット URL を有効にする] のチェックをオンにするまで有効になりません。

部分修飾 URL は、ibi_apps フォルダ下の場所を暗示的に指定する不完全 URL です。このような URL は、パブリックアクセスを有効にした場合にのみ、この設定に割り当てることができます。パブリックアクセスが無効な場合、部分修飾 URL は期待どおりに動作しないため、この設定では、ibi_apps フォルダ下の場所を明示的に指定する完全修飾 URL を使用する必要があります。

シングルサインオン (SSO) 環境では、認証情報が外部の認証プロバイダに保持されるため、WebFOCUS からログアウトしても、必ずしもユーザが認証済みの SSO 製品セッションからログアウトしたことにはなりません。この場合、ログアウトのリダイレクト URL には、SSO 製品セッションを終了する URL を指定します (その URL が存在する場合)。たとえば、WebSeal では、ログアウト URL を次のように指定します。

```
http://webseal.domain.com/pkmslogout
```

SiteMinder では、URL を次のように指定します。

```
http://siteminder.domain.com/logout.html
```

匿名アクセス

匿名アクセス (パブリックアクセスとも呼ばれる) は、認証もパーソナライズも必要としないアプリケーションを使用する場合に役立ちます。匿名アクセスでは、未承認ユーザが WFC/Repository/Public フォルダに格納されたリソースを表示したり、実行したりできますが、それ以外のリソースの作成や編集などの権限は与えられません。このアクセス方法に設定された制限によって、管理者は一般使用向けのリソースの整合性を保護すると同時に、すべてのユーザがこれらのリソースを使用できるようにできます。

匿名アクセスは、デフォルト設定で無効になっています。 匿名アクセスを有効にするには、匿名アクセスが必要な [セキュリティゾーン] で [匿名認証] 設定を有効にする必要があります。

セキュリティゾーンで [匿名認証] を有効にすると、WebFOCUS Client で WFC/Repository/Public フォルダのリソースへの匿名アクセスまたは未認証アクセスがサポートされます。また、WebFOCUS Reporting Server のプロシジャへのアクセスも同様にサポートされます。匿名ユーザに、リポジトリ内に格納された他のコンテンツへのアクセスを許可する場合は、235 ページの 「 匿名ユーザのセキュリティポリシーの変更 」 の説明に従って、その他のリソースへのアクセスを匿名ユーザに許可するルールを作成することができます。[匿名ユーザ ID] (IBI_ANONYMOUS_USER) 設定で指定されたユーザが使用する WebFOCUS Reporting Server 認証情報は、[Reporting Server 匿名ユーザ ID] (IBI_ANONYMOUS_WFRS_USER) および [Reporting Server 匿名ユーザパスワード] (IBI_ANONYMOUS_WFRS_PASS) で指定します。これらの設定はすべて、[セキュリティ] タブの [詳細] ページに表示されます。

匿名ユーザごとに個別のセッションが作成されます。これらのセッションは、Web ブラウザに格納される非永続的な WF-JSESSIONID Cookie に基づいて各ユーザに関連付けられます。また、foccache トークンやグローバル変数など、匿名ユーザごとに固有の情報もトラッキングされます。すべての匿名セッションには、[匿名ユーザ ID] (IBI_ANONYMOUS_USER) 設定で指定されたユーザアカウントの有効なポリシーと同一のポリシーが適用されます。

事前認証を使用するよう WebFOCUS を構成した場合は、匿名認証を無効にする必要があります。これは、この構成では特定の事前認証済みユーザにアクセスが限定されるためです。外部認証を使用するよう WebFOCUS を構成した場合、パブリックアクセスはサポートされますが、考慮事項がいくつかあります。

外部認証でのパブリックアクセスの構成についての詳細は、327 ページの 「 外部認証 」 を参照してください。

[セキュリティ] タブの [詳細] ページの [匿名ユーザ ID] (IBI_ANONYMOUS_USER) 設定を使用して、未認証アクセスのデフォルトユーザ ID を指定することができます。デフォルト設定では、このユーザ ID は「public」です。

手順　特定のセキュリティゾーンで匿名アクセスを有効にするには

匿名アクセスは、デフォルト設定で無効になっています。デフォルトセキュリティゾーンまたは代替セキュリティゾーンで匿名アクセスを有効にするには、[匿名認証] 設定を有効にする必要があります。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。

3. [匿名認証] エントリをクリックします。[アクション] セクションで [有効にする] をクリックし、次に [保存] をクリックします。

   または

   [匿名認証] エントリを右クリックし、[有効にする] を選択します。[アクション] セクションで [保存] をクリックします。

4. 確認メッセージで [OK] をクリックします。
5. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
6. 現在のセッションからログアウトします。
7. Application Server を停止し、再起動します。
8. 管理者として再度ログインし、新しい構成をテストします。

手順　特定のセキュリティゾーンで匿名アクセスを無効にするには

特定のセキュリティゾーンで匿名アクセスを有効にした後、[匿名認証] 設定を無効にすることでこのゾーンの匿名アクセスを無効にすることができます。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
3. [匿名認証] エントリをクリックします。[アクション] セクションで [無効にする] をクリックし、次に [保存] をクリックします。

   または

   [匿名認証] エントリを右クリックし、[無効にする] を選択します。[アクション] セクションで [保存] をクリックします。

4. 確認メッセージで [OK] をクリックします。
5. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
6. 現在のセッションからログアウトします。
7. Application Server を停止し、再起動します。
8. 管理者として再度ログインし、新しい構成をテストします。

手順　すべてのセキュリティゾーンで匿名アクセスを無効にするには

アプリケーション全体で匿名アクセスを無効にするには、[セキュリティ] タブの [詳細] ページで、匿名ユーザ設定に割り当てられている名前およびパスワードをすべて削除し、さらにセキュリティセンターで Public ユーザを削除します。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティの構成] フォルダ下の [詳細] をクリックします。
3. [Reporting Server 匿名ユーザ ID] および [Reporting Server 匿名ユーザパスワード] テキストボックスに割り当てられている値をクリアします。
4. [セキュリティの構成] セクションで [保存] をクリックします。
5. 「変更を保存しました」というメッセージで、[OK] をクリックします。
6. 「これらの変更を有効にするには、キャッシュをクリアしてください」というメッセージで、[OK] をクリックします。
7. 管理コンソールのメニューバーで [キャッシュのクリア] をクリックします。
8. キャッシュのクリアを確認するメッセージで、[OK] をクリックします。
9. セキュリティセンターに移動します。
10. [ユーザ] ウィンドウの [USERS] フォルダ下で [public] エントリを右クリックし、[削除] を選択します。

    確認メッセージで [はい] をクリックし、ユーザの削除を確定します。
11. [閉じる] をクリックします。

手順　匿名ユーザに別のアカウントを指定するには

匿名ユーザに別のユーザアカウントを指定するには、新しいユーザアカウントを作成し、[匿名ユーザ ID] (IBI_Anonymous_User) 設定に割り当てられている名前を、作成したユーザアカウントに割り当てた名前に変更します。

1. [セキュリティセンター] の [ユーザとグループ] タブで、[新規ユーザ] をクリックします。
2. [新規ユーザ] ダイアログボックスで、新しい匿名ユーザアカウントのユーザ名を入力し、必要に応じて説明を追加します。

    注意：このアカウントに Email アドレスおよびパスワードは指定しないでください。
3. [作成先グループ] リストから [Anonymous] を選択し、[ステータス] リストから [アクティブ] を選択します。
4. [OK] をクリックします。

これで、匿名ユーザの新しいアカウントが作成されました。

5. 管理コンソールを開き、[セキュリティ] タブをクリックします。
6. デフォルト匿名ユーザ ID に新しいユーザを指定するには、次の手順を実行します。
   a. [セキュリティの構成] フォルダ下の [詳細] をクリックします。
   b. [匿名ユーザ ID] (IBI_ANONYMOUS_USER) テキストボックスに、セキュリティセンターで作成したユーザアカウント名を入力します。

   これで、新しいユーザアカウントが匿名ユーザとして使用されるよう WebFOCUS が構成されました。

参照　匿名ユーザのセキュリティポリシーの変更

デフォルト設定では、匿名ユーザには [Public] フォルダ内のリソースへのアクセスが許可されています。匿名ユーザに、これ以外のフォルダまたはポータルへのアクセスを許可する場合は、アクセスを有効にするための新しいルールを作成することができます。匿名ユーザのセキュリティポリシーを管理する場合は、セキュリティゾーンの [匿名認証] 設定の [ユーザ名] テキストボックスで指定されたユーザアカウントにルールを直接適用するのではなく、Anonymous グループに対してルールを作成し、上記のユーザアカウントを Anonymous グループに追加する方法をお勧めします。

ルールの作成についての詳細は、484 ページの 「 グループ、ユーザ、ロールに対してルールを作成するには 」 を参照してください。

フォームベース認証

フォームベース認証は、各セキュリティゾーンのデフォルト認証方法です。この方法では、ユーザリクエストを認証するために、WebFOCUS Client が通常のログインページをユーザに提示し、ログインプロセス中に収集されたユーザ ID とパスワードを検証するために、HTML フォームタグを使用して認証情報を WebFOCUS Reporting Server に転送します。

手順　フォームベース認証設定をカスタマイズするには

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
3. [フォームベース認証] エントリをクリックします。

4. [アクション] セクションで [有効] をクリックし、[フォームベース認証] をダブルクリックして [フォームベース認証設定の編集] ダイアログボックスを開きます。

   このダイアログボックスでは、デフォルト設定で 3 つの設定のチェックがすべてオフになっています。

5. [OK] をクリックして、デフォルト設定を受容します。
6. [アクション] セクションで [保存] をクリックします。
7. 確認メッセージのダイアログボックスで [OK] をクリックします。
8. Web アプリケーションの再ロードを要求するメッセージダイアログボックスで [OK] をクリックします。
9. 現在のセッションからログアウトします。
10. Application Server を停止し、再起動します。
11. 管理者として再度ログインし、新しい構成をテストします。

内部認証

デフォルト設定では、リポジトリに格納された情報に基づいてユーザの認証が行われます。ユーザがログインすると、ユーザパスワードの Salt ハッシュが生成され、リポジトリに格納されているパスワードハッシュと比較されます。 ユーザパスワード自体は格納されておらず、格納されているハッシュ値からパスワードを特定することはできません。

デフォルト設定では、ユーザアカウントのパスワード設定は必須ではありませんが、内部認証プロセスの他の動作と同様に、このパスワード設定の動作をカスタマイズすることができます。要件に応じてカスタムログインページを作成し、そのページにスタイルを適用することができます。また、パスワードやアカウントのポリシーを構成することもできます。これらのポリシーには、パスワード設定を必須にするかどうか、パスワードの最小長さの設定、ユーザ本人によるパスワード変更を可能にするか、ユーザログイン情報を記憶するかどうかなどの構成があります。

事前認証

事前認証では、トラステッド認証が構成済みで、後述の認証方法のいずれかでユーザ認証情報が渡されることを前提としています。この構成では、ユーザにログインページが表示されません。匿名アクセスやユーザ本人によるパスワード変更など一部の機能は無効になります。

事前認証には、いくつかの利点があります。たとえば、ユーザにはシングルサインオン (SSO) 機能が提供されます。また、認証が一元的に実行されるため、管理者が WebFOCUS と別のソースとの間でパスワードを同期する必要がなくなります。選択した事前認証方法によっては、事前認証の構成で安全性が侵害されないよう、追加の手順が必要になる場合があります。たとえば、事前認証のユーザ ID が HTTP ヘッダで渡される場合、このヘッダ値の安全性を確保するよう対策を講じる必要があります。

CAS による事前認証の構成

Central Authentication Service (CAS) による事前認証を使用すると、ユーザセキュリティ認証情報にアクセスせずに、Web アプリケーションなどのクライアントでのユーザ認証が可能になります。代わりに、WebFOCUS Client が CAS サーバに対して認証され、その接続の安全性が有効であることを確認するセキュリティチケットが WebFOCUS Client に返されます。WebFOCUS Client は、そのチケットと独自のサービス ID を CAS サーバに送信することでチケットの有効性を確認します。CAS は、各ユーザが認証されたかどうかに関する信頼情報を返します。

CAS サーバが自己署名証明書を使用する場合、認証局署名証明書を、WebFOCUS で使用される JVM の信頼されたルート証明書に追加する必要があります。

手順　CAS による事前認証を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
3. [CAS 認証] エントリをクリックします。
4. [アクション] セクションで [編集] をクリックします。
5. [CAS 認証設定の編集] ダイアログボックスで、CAS ログインサーバの URL を次の形式で入力します。

   ```
   https://CASSERVER.domain.com:port/cas/login
   ```

説明

CASSERVER.domain.com
CAS 処理のホストサーバのネットワーク名または IP アドレスです。

port
CAS サーバの接続先ポート番号です。

6. CAS サービスチケット検証の URL を次の形式で入力します。

   `https://CASSERVER.domain.com:port/cas`

   説明

   CASSERVER.domain.com
   CAS 処理のホストサーバのネットワーク名または IP アドレスです。

   port
   CAS サーバの接続先ポート番号です。

7. CAS サービスの URL を次の形式で入力します。

   `https://WebFOCUSServer.domain.com:port/ibi_apps`

   説明

   WebFOCUSSERVER.domain.com
   WebFOCUS 処理のホストサーバのネットワーク名または IP アドレスです。

   port
   WebFOCUS Reporting Server の接続先ポート番号です。

8. [OK] をクリックします。
9. [CAS 認証] エントリを右クリックし、[有効にする] を選択します。
10. [アクション] セクションで [保存] をクリックします。
11. 確認メッセージで [OK] をクリックします。
12. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
13. 現在のセッションからログアウトします。
14. WebFOCUS Reporting Server を停止し、再起動します。
15. 管理者として再度ログインし、接続をテストします。

手順　TIBCO WebFOCUS cacerts ファイルに CAS CA 証明書を追加するには

CAS サーバに自己署名証明書を使用する場合は、このサーバの CA 証明書を、WebFOCUS で使用される JVM の信頼済みルート証明書に追加する必要があります。

注意：信頼される認証局署名証明書を使用する場合、この作業は必要ありません。

1. CAS サイトから CA 証明書をエクスポートし、その CA 証明書を WebFOCUS 環境に保存します。
2. Tomcat Server を停止します。
3. Tomcat JDK に移動し、cacerts ファイルを特定します。

   通常、cacerts フィルは *drive*:¥ibi¥JDK¥jre¥lib¥security フォルダ (Windows) または *installdirectory*/ibi/JDK/jre/lib/security フォルダ (UNIX または Linux) に格納されています。

   a. cacerts ファイルが格納されているフォルダで、[コマンドプロンプト] ウィンドウを開き、次のコマンドを実行します。

      ```
      ..¥..¥..¥bin¥keytool -import
      -alias youralias -keystore cacerts -file path¥to¥yourca.cert
      ```

      説明

      `youralias`
      証明書に割り当てられたエイリアスです。

      `yourca.cert`
      証明書ファイルです。

   b. パスワードの入力を要求するプロンプトで「changeit」と入力します。証明書のインポートを要求するプロンプトで「yes」と入力します。
4. Tomcat サーバを再起動します。

例 CAS 検証エラー

CAS 検証エラーは、信頼された証明書ストアに追加されていない自己署名証明書を使用する場合に発生します。その場合、次のようなエラーが表示されます。

```
[YYYY-MM-DD hh:mm:ss,sss] ERROR
org.jasig.cas.client.validation.Cas20ServiceTicketValidator
http-apr-8080-exec-2 - javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Unknown Source)
.
.
.
... 60 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(Unknown
Source)
at java.security.cert.CertPathBuilder.build(Unknown Source)
... 66 more
```

HTTP Basic 認証による事前認証の構成

HTTP Basic 認証を使用すると、ユーザ名とパスワードが含まれたメッセージがクライアントからサーバに転送されます。サーバは、このメッセージの 2 つの値と、指定されたレルム (認証情報を要求する一連の Web ページ) で有効なユーザのデータベース内のユーザ ID とパスワードを比較します。この処理の結果に応じて、サーバから認証ステータスを示すメッセージが返されます。

HTTP Basic 認証では、メッセージを暗号化する代わりに、双方向変換を簡単に行える Base64 エンコードが使用されるため、SSL とともに使用しない限り、セキュリティで保護されません。HTTP Basic 認証を構成するには、HTTP Basic 認証の影響を受けるレルムの名前を指定する必要があります (通常は「WebFOCUS」)。この設定により、認証リクエストがデータベースのそのセクション (そのレルムでページを表示して操作する資格のあるユーザのリスト) に送信されます。

注意：バージョン 8.2 SP01 では、HTTP Digest 認証は使用できません。

手順　HTTP Basic 認証を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
3. [HTTP Basic 認証] エントリを右クリックし、[編集] を選択します。
4. [Realm 名] テキストボックスで、デフォルト値の「WebFOCUS」を受容するか、別の名前を入力します。
5. [OK] をクリックします。
6. [HTTP Basic 認証] エントリを右クリックし、[有効にする] を選択します。
7. [アクション] セクションで [保存] をクリックします。
8. 確認メッセージで [OK] をクリックします。
9. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
10. 現在のセッションからログアウトします。
11. WebFOCUS Reporting Server を停止し、再起動します。
12. 管理者としてログインし、新しい構成をテストします。

Java コンテナセキュリティによる事前認証の構成

WebFOCUS でユーザを認証する代わりに、Apache Tomcat、IBM WebSphere、Oracle WebLogic などの Java コンテナで認証を実行するよう構成することができます。Java コンテナは、getRemoteUser() 呼び出しを使用して、WebFOCUS にユーザ ID を提供します。

手順　JEE コンテナベース認証を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

また、ユーザ認証をサポートするための Java コンテナも作成する必要があります。詳細は、インストール済み Java の提供元ベンダーのマニュアルを参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し (通常はデフォルトセキュリティゾーン)、[認証] をクリックします。
3. [認証] ページの [アクション] セクションで、[オプション] をクリックします。
4. [認証オプション] ダイアログボックスで、[カスタムログアウトターゲット URL を有効にする] のチェックをオンにします。
5. [カスタムログアウトターゲット URL] テキストボックスで、デフォルト値の「/signout」を受容するか、別のカスタムログアウトターゲット URL を入力し、[OK] をクリックします。
6. [認証] ページで [JEE コンテナベース認証] を右クリックし、[有効にする] を選択します。

   他の認証設定はすべて自動的に無効になります。
7. 更新後のセキュリティゾーン構成にフォームベース認証を追加するには、[フォームベース認証] を右クリックし、[有効にする] を選択します。

   このセキュリティゾーンからフォームベース認証を除外するには、[フォームベース認証] を [無効] のままにします。
8. J2EE 認証を有効にする方法についての詳細は、Java コンテナのマニュアルを参照してください。
9. [認証] ページの [セキュリティゾーン] セクションで、[保存] をクリックします。
10. 「Web セキュリティ構成データは正常に保存されました」というメッセージで、[OK] をクリックします。
11. 「これらの変更を有効にするには、Web アプリケーションを再起動してください」というメッセージで、[OK] をクリックします。
12. 現在のセッションからログアウトします。
13. WebFOCUS Reporting Server を停止し、再起動します。
14. 管理者として再度ログインし、新しい構成をテストします。

OpenID Connect による事前認証の構成

Google や Keycloak などの ID プロバイダは、OpenID Connect プロトコルの仕様に準拠した認証サービスを提供します。

OpenID Connect による事前認証が有効化されると、¥ibi_apps コンテキストにナビゲートするユーザには、WebFOCUS ログイン画面ではなくそれらの ID プロバイダのログイン画面が表示されます。ユーザは、この画面に認証情報を入力し、OpenID Connect ID プロバイダに送信します。WebFOCUS およびエンドユーザが示した認証情報が ID プロバイダに認証されると、ユーザは WebFOCUS にリダイレクトされます。

WebFOCUS は、独自の Client ID を ID プロバイダに返すクライアント認証メッセージを用意します。このメッセージには、エンドユーザの追加情報をリクエストする範囲 ID を含めることもできます。

WebFOCUS が提示した認証情報の認証時に、ID プロバイダは要求されたユーザ情報を返し、認証済みユーザは WebFOCUS でセッションを開始することができます。

セッションを終了したユーザには、WebFOCUS の標準ログアウトページではなく ID プロバイダが使用するログアウトページが表示されます。ID プロバイダのログアウトページから、ユーザは、OpenID Connect ID プロバイダに再度ログインするか、他の Web サイトまたはアプリケーションに移動するかを選択することができます。

ID プロバイダでの OpenID Connect による認証設定の構成

OpenID Connect 認証を受容するアプリケーションとして、WebFOCUS インストールはクライアントまたは OpenID Connect 認証プロセスのリレーパーティとして機能します。この場合、管理者は、OpenID Connect ID プロバイダにこの利用者のアカウントを作成する必要があります。

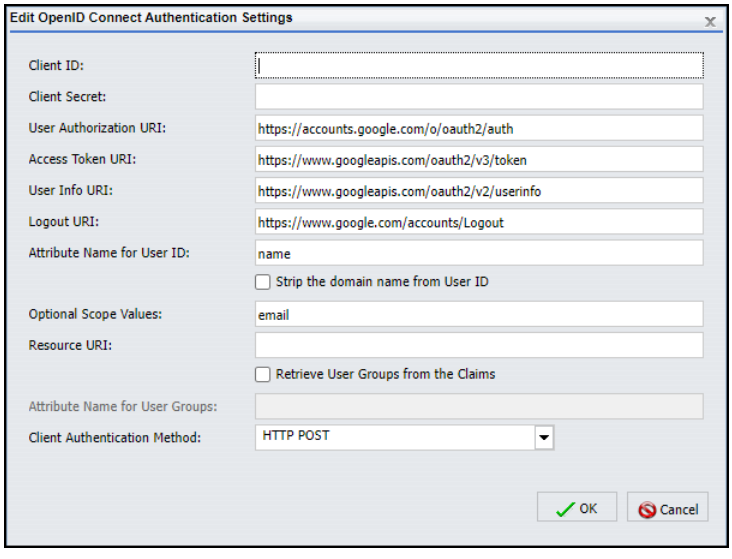
OpenID Connect ID プロバイダはそれぞれに若干異なる構成および要件を保持していますが、すべてのプロバイダが OpenID Connect の標準に準拠する必要があります。

管理者は、ユーザの WebFOCUS インストールを一意に識別するクライアント名およびその他の情報を ID プロバイダに提供する必要があります。これらの情報には、WebFOCUS インストールのルート URL、およびログイン処理中に ID プロバイダから送信されるレスポンスを処理するリソースの場所を特定する 1 つまたは複数の有効なリダイレクト URI が含まれます。

ID プロバイダは、WebFOCUS の各インストールに固有のクライアント ID およびクライアントシークレットを作成し、管理者に提供します。また、ID プロバイダは、カスタムログアウトターゲット URL を特定します。WebFOCUS セッションを終了したユーザはこの URL に転送され、ユーザはここで ID プロバイダに再度ログインすることも他のタスクに移動することもできます。管理者は、これらの値をすべて OpenID Connect 構成に入力します。

TIBCO WebFOCUS 内部での OpenID Connect による認証設定の構成

[OpenID Connect 認証設定の編集] ダイアログボックスには、下図のように、WebFOCUS からクライアント認証メッセージで OpenID Connect ID プロバイダに送信する必要がある認証情報およびエンドポイント URI の設定が含まれています。



OpenID Connect ID プロバイダと通信するためには、有効なリレーパーティ (エンドユーザの ID を認証する必要がある Web サイトまたはアプリケーション) として WebFOCUS を指定する認証情報を ID プロバイダに設定する必要があります。これらの値は、認証済みユーザへのアクセス許可リクエストに対するリレーパーティからのレスポンスに含める必要があります。

- **クライアント ID**　OpenID Connect ID プロバイダに対してユーザの WebFOCUS インストールを識別するユニーク ID です。この値は、ID プロバイダがサポートする各アプリケーションに対して一意の値にする必要があります。
- **クライアントシークレット**　この値は、WebFOCUS と ID プロバイダで共有され、両者のメッセージの認証を有効にします。OpenID Connect ID プロバイダへのリクエストのたびに提供する必要があります。クライアントシークレットに割り当てる値は、推測されないランダムな値にする必要があります。以下はその例です。

  ```
  sGBAyfVL7YWtP6gudLIjbRZV_N0dW4f3xETiIxqtokEAZ6FAsBtgyIq0MpU1uQ7J08xOTO2zwP0OuO3pMVAUTid
  ```

  ID プロバイダは、この値の表示と抽出を管理者に許可する前に、別のログインを要求する場合があります。

OpenID 認証リクエストが適切なエンドポイントに確実に送信されるためには、[OpenID Connect 認証設定の編集] ダイアログボックスに次の URI 情報も含める必要があります。

- **ユーザ認可 URI** エンドユーザの認証が可能な、ID プロバイダ認可サーバの HTTP エンドポイントを指定します。ユーザ認証のリクエストは、このエンドポイントに送信されます。
- **アクセストークン URI** アクセストークンの発行が可能な、ID プロバイダ認可サーバの HTTP エンドポイントを指定します。認証済みユーザに対するトークンのリクエストは、このエンドポイントに送信されます。
- **ユーザ情報 URI** ユーザ情報を保持し、クライアントによるアクセストークンの提供時に現在のユーザに関する認証情報の送信が可能な、ID プロバイダの保護されたリソースを指定します。
- **ログアウト URI** OpenID プロバイダが認証したすべてのセッションからログアウトをした際に転送される、ID プロバイダの HTTP エンドポイントを指定します。通常、これは Open ID プロバイダのログインページです。このページでは、ユーザは再度ログインして別の OpenID Connect ID プロバイダのセッションを開始することも、ログアウトしたままにすることも可能です。ログアウトリダイレクト URI はこのテキストボックスで定義済みのため、[認証オプション] ダイアログボックスの [カスタムログアウトターゲット URL] テキストボックスにログアウト URL を定義する必要はありません。
- **ユーザ ID の属性名** WebFOCUS ユーザ ID にマッピングされる特定の属性を指定します。このテキストボックスのデフォルト値は name です。多くの場合は、name の代わりに email を使用します。この場合、email は、local_part@domain_name のフォーマットを使用した Email アドレスを示し、ユーザ ID として機能します。これ以外の属性名をこのテキストボックスに使用することもできます。使用する値についての詳細は、ID プロバイダに問い合わせてください。この属性に割り当てる値は、一意の値である必要があります。
  - **ユーザ ID からドメイン名を除外** このチェックがオンの場合、ログインプロセスで ID プロバイダに送信されるユーザ ID からドメイン名接頭語が自動的に除外されます。このチェックボックスは、ユーザ名に「domain name¥user ID」フォーマットを使用し、ドメイン名接頭語を使用したユーザ ID を受容しない OpenID Connect プロバイダを使用するユーザにのみ関連します。
- **範囲値 (オプション)** 必須の範囲 ID (openid) 以外に ID プロバイダに送信可能なオプションの範囲 ID の名前を指定します。範囲 ID は、Client へのアクセスを要求するエンドユーザに関する特定タイプの情報のリクエストです。有効な範囲 ID の値には、Open ID Connect の標準 (email、address、phone、profile) で定義された値が含まれます。このテキストボックスには、デフォルト設定で email の範囲 ID が表示されますが、ユーザおよび ID プロバイダがこれを使用しない場合は削除することができます。

- **クライアント認証方法** ID プロバイダのサーバ接続でクライアント認証メッセージが使用する HTTP リクエストメソッドを指定します。デフォルト設定では、HTTP POST リクエストメソッドが選択されています。このメソッドを使用した場合、クライアント認証情報がメッセージ本文に含まれます。HTTP Basic 認証スキームリクエストメソッドを選択することもできます。この場合、クライアント認証情報は HTTP 認証ヘッダに含まれます。[なし] オプションの選択は推奨されません。ただし、ID プロバイダがこのリストで定義されていない別のリクエストメソッドの使用を求めた場合は除きます。

Google による OpenID Connect 事前認証の構成

[OpenID Connect 認証設定の編集] ダイアログボックスは、デフォルト設定で、Google からの事前認証済みユーザログインリクエストのサポートに必要な情報で構成されています。管理者は、Google から提供されるクライアント ID とクライアントシークレット、および属性名のみ追加する必要があります。

Google OpenID Connect API についての詳細は、「https://developers.google.com/identity/protocols/OpenIDConnect」を参照してください。

手順 Google の OpenID Connect 認証設定を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で [デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
3. [OpenID Connect 認証] エントリをダブルクリックし、[OpenID Connect 認証設定の編集] ダイアログボックスを開きます。
4. [クライアント ID] テキストボックスに、OpenID Connect プロバイダの有効なクライアントとして WebFOCUS を識別する名前を入力します。

   以下はその例です。

   ```
   292085223830.apps.googleusercontent.com
   ```

5. Google が提供する [クライアントシークレット] の値を入力するか、コピーして貼り付けます。

   以下はその例です。

```
GBAyfVL7YWtP6gudLIjbRZV_N0dW4f3xETiIxqtokEAZ6FAsBtgyIq0MpU1uQ7J08xOTO2zw
P0OuO3pMVAUTid
```

6. OpenID プロバイダとして Google を設定するには、次のテキストボックスでデフォルト値を受容します。
   - **ユーザ認可 URI** https://accounts.google.com/o/oauth2/auth
   - **アクセストークン URI** https://www.googleapis.com/oauth2/v3/token
   - **ユーザ情報 URI** https://www.googleapis.com/oauth2/v2/userinfo
   - **ログアウト URI** https://www.google.com/accounts/Logout
7. [ユーザ ID の属性名] テキストボックスに有効な属性名を入力します。

   注意：多くの場合は、デフォルト値の name を email で置換します。ただし、他の属性名をこのテキストボックスに使用することもできます。使用する値についての詳細は、ID プロバイダに問い合わせてください。
8. ID プロバイダに送信されたすべてのユーザ ID からドメイン名接頭語が除外されていることを確認する必要がある場合、[ユーザ ID からドメイン名を除外] のチェックをオンにします。それ以外の場合は、このチェックをオフのままにします。

   注意：このチェックボックスは、ユーザ名に「domain name¥user ID」フォーマットを使用し、ドメイン名接頭語を使用したユーザ ID を受容しない OpenID Connect プロバイダを使用するユーザにのみ関連します。
9. [範囲値 (オプション)] テキストボックスに表示されたデフォルト値 email を受容します。
10. [クライアント認証方法] リストに表示されたデフォルト選択 HTTP POST を受容します。
11. 構成の完了後、[OK] をクリックします。
12. 252 ページの 「 セキュリティゾーンで OpenID Connect 認証を有効にするには 」 の説明に従って、新しい構成を有効にします。
13. 253 ページの 「 OpenID Connect 構成を保存するには 」 の説明に従って、新しい構成を保存します。

Keycloak による OpenID Connect 事前認証の構成

Keycloak は、オープンソースのアイデンティティ管理およびアクセス管理ソリューションで、OpenID Connect 標準を使用したシングルサインオン事前認証を WebFOCUS に提供します。Keycloak およびその機能についての詳細は、「https://www.keycloak.org/about.html」を参照してください。

OpenID 認証の Keycloak クライアントとして WebFOCUS インストールを構成する方法についての詳細および説明は、『Keycloak Getting Started Guide』(https://www.keycloak.org/docs/latest/getting_started/index.html) を参照してください。

手順　Keycloak の OpenID Connect 認証設定を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で [デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
3. [OpenID Connect 認証] エントリをダブルクリックし、[OpenID Connect 認証設定の編集] ダイアログボックスを開きます。
4. WebFOCUS のクライアント ID を入力します。この ID は、Keycloak の WebFOCUS クライアントページの [設定] タブの [クライアント ID] テキストボックスで識別されます。

   たとえば、「WebFOCUS-HEAD」と入力します。
5. Keycloak が提供する [クライアントシークレット] の値を入力するか、コピーして貼り付けます。通常、この値は、ランダムに生成された値の 16 進数表現です。

   以下はその例です。

   ```
   43b89579-ea9c-4101-b321-56b9dc6ae0f8
   ```
6. [認証 URI] テキストボックスには、次のように入力します。

   ```
   http://host:port/auth/realms/realm-name/protocol/openid-connect/auth
   ```

   説明

   `host`
   Keycloak が使用するホストの名前または IP アドレスです。

   `port`
   Keycloak ID プロバイダが待ち受けるポート番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

`realm-name`

Keycloak で WebFOCUS に適用したレルムの名前です。たとえば、WebFOCUSRealm と入力します。

以下はその例です。

```
http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-connect/auth
```

7. [アクセストークン URI] テキストボックスに、次のように入力します。

   ```
   http://host:port/auth/realms/realm-name/protocol/openid-connect/token
   ```

   この場合の host、port、realm-name は、手順 6 で説明したように、Keycloak で使用されるホストを指定します。

   以下はその例です。

   ```
   http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-connect/token
   ```

8. [ユーザ情報 URI] テキストボックスに、次のように入力します。

   ```
   http://host:port/auth/realms/realm-name/protocol/openid-connect/userinfo
   ```

   この場合の host、port、realm-name は、手順 6 で説明したように、Keycloak で使用されるホストを指定します。

   以下はその例です。

   ```
   http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-connect/userinfo
   ```

9. [ログアウト URI] テキストボックスに、次のように入力します。

   ```
   http://host:port/auth/realms/realm-name/protocol/openid-connect/logout?redirect_uri=https://wfhost.ibi.com/context/service/wf_security_logout.jsp
   ```

   この場合の host、port、realm-name は、手順 6 で説明したように、Keycloak が使用するホストを識別し、wfhost は、WebFOCUS が使用するホストの名前または IP アドレスを識別します。また、context には、WebFOCUS インストールで使用するコンテキストを指定します (通常は、¥ibi_apps)。

以下はその例です。

```
http://server01.ibi.com:8080/auth/realms/WebFOCUSRealm/protocol/openid-
connect/logout?redirect_uri=https://wfserver01.ibi.com/ibi_apps/
service/ wf_security_logout.jsp
```

10. [ユーザ ID の属性名] テキストボックスに有効な属性名を入力します。

    注意：多くの場合は、デフォルト値の name を email で置換します。ただし、他の属性名をこのテキストボックスに使用することもできます。使用する値についての詳細は、ID プロバイダに問い合わせてください。

11. ID プロバイダに送信されたすべてのユーザ ID からドメイン名接頭語が除外されていることを確認する必要がある場合、[ユーザ ID からドメイン名を除外] のチェックをオンにします。それ以外の場合は、このチェックをオフのままにします。

    注意：このチェックボックスは、ユーザ名に「domain name¥user ID」フォーマットを使用し、ドメイン名接頭語を使用したユーザ ID を受容しない OpenID Connect プロバイダを使用するユーザにのみ関連します。

12. [範囲値 (オプション)] テキストボックスに表示されたデフォルト値 email を受容します。
13. [クライアント認証方法] リストに表示されたデフォルト選択 HTTP POST を受容します。
14. 構成の完了後、[OK] をクリックします。
15. 252 ページの 「 セキュリティゾーンで OpenID Connect 認証を有効にするには 」 の説明に従って、新しい構成を有効にします。
16. 253 ページの 「 OpenID Connect 構成を保存するには 」 の説明に従って、新しい構成を保存します。

その他の OpenID Connect ID プロバイダによる事前認証の構成

他のサードパーティ OpenID Connect プロバイダで WebFOCUS ユーザの事前認証を行うこともできます。WebFOCUS および ID プロバイダで構成が必要な情報は、OpenID Connect の標準に準拠する必要がありますが、特定の構成要件は ID プロバイダによって異なります。詳細は、使用する OpenID プロバイダのマニュアルを参照してください。

手順　その他の OpenID Connect ID プロバイダの OpenID Connect 認証設定を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で [デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
3. [OpenID Connect 認証] エントリをダブルクリックし、[OpenID Connect 認証設定の編集] ダイアログボックスを開きます。
4. OpenID Connect ID プロバイダでクライアント ID が割り当てられている場合は、この値をコピーして [クライアント ID] テキストボックスに貼り付けます。

   または

   ユーザが、OpenID Connect ID プロバイダ内でユーザの構成にクライアント ID を割り当てた場合は、[クライアント ID] テキストボックスにこの値を入力するか、コピーして貼り付けます。
5. ID プロバイダが提供する [クライアントシークレット] の値をコピーして、[クライアントシークレット] テキストボックスに貼り付けます。
6. 次のテキストボックスに URL を入力するか、コピーして貼り付けます。これらの値はすべて、ID プロバイダからユーザに提供されます。

   - **ユーザ認可 URI** ID プロバイダがエンドユーザの認証を行う HTTP エンドポイントの URL です。
   - **アクセストークン URI** ID プロバイダがアクセストークンを発行する HTTP エンドポイントの URL です。
   - **ユーザ情報 URI** ID プロバイダがユーザ情報を保持する HTTP エンドポイントの URL です。有効なアクセストークンなど、現在のユーザに関する追加情報を求めるクライアントアプリケーションからのリクエストは、このエンドポイントに送信されます。
   - **ログアウト URI** ユーザがセッションからログアウトする際に転送される HTTP エンドポイントの URL です。
7. [ユーザ ID の属性名] テキストボックスに有効な属性名を入力します。

   注意：多くの場合は、デフォルト値の name を email で置換します。ただし、他の属性名をこのテキストボックスに使用することもできます。使用する値についての詳細は、ID プロバイダに問い合わせてください。

8. ID プロバイダに送信されたすべてのユーザ ID からドメイン名接頭語が除外されていることを確認する必要がある場合、[ユーザ ID からドメイン名を除外] のチェックをオンにします。それ以外の場合は、このチェックをオフのままにします。

   注意：このチェックボックスは、ユーザ名に「domain name¥user ID」フォーマットを使用し、ドメイン名接頭語を使用したユーザ ID を受容しない OpenID Connect プロバイダを使用するユーザにのみ関連します。

9. ユーザと ID プロバイダで使用を合意したオプションの範囲 ID の名前を [範囲値 (オプション)] に入力します。各値を区切るにはブランクを 1 つ挿入します。

   注意：ユーザおよび ID プロバイダが使用しない場合は、このテキストボックスにデフォルト設定で表示される値 email を削除することができます。

10. [クライアント認証方法] リストのデフォルト選択 HTTP POST を受容するか、[HTTP Basic 認証スキーム] を選択して、エンドユーザの認証メッセージで ID プロバイダが要求する HTTP 通信メソッドを指定します。

    注意：ID プロバイダから要求がない限り、[なし] オプションの選択は推奨されません。

11. 構成の完了後、[OK] をクリックします。
12. 252 ページの 「 セキュリティゾーンで OpenID Connect 認証を有効にするには 」 の説明に従って、新しい構成を有効にします。
13. 253 ページの 「 OpenID Connect 構成を保存するには 」 の説明に従って、新しい構成を保存します。

手順　セキュリティゾーンで OpenID Connect 認証を有効にするには

各インストールでサポート可能な OpenID Connect プロバイダは 1 つのみです。

セキュリティゾーンで OpenID Connect 認証を有効にする際は、そのセキュリティゾーンの他の認証方法をすべて無効にする必要があります。

他の事前認証方法と同じように、[デフォルトセキュリティゾーン] でこの方法を使用し、管理操作にはフォームベース認証をサポートするよう [代替ゾーン] を許可します。

1. 管理コンソールの [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、[デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
2. [認証] ページで、次の手順を実行します。
   a. [フォームベース認証] エントリを選択し、[無効にする] をクリックします。
   b. [匿名認証] エントリを選択し、[無効にする] をクリックします。
   c. [OpenID Connect 認証] エントリを選択し、[有効にする] をクリックします。

3. 253 ページの 「 OpenID Connect 構成を保存するには 」 の手順に従って、[認証] ページで Open ID Connect 構成を保存します。

手順　OpenID Connect 構成を保存するには

1. [認証] ページの [アクション] セクションで、[保存] をクリックします。
2. 確認メッセージのダイアログボックスで [OK] をクリックします。
3. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
4. 現在のセッションからログアウトします。
5. WebFOCUS Reporting Server を停止し、再起動します。
6. OpenID Connect ID プロバイダからの有効な ID を使用してログインし、新しい構成をテストします。

Web アクセス管理システムによる事前認証の構成

Web アクセス管理システム (例、CA SiteMinder、Oracle Access Manager (従来の Oblix)、IBM Tivoli Access Manager WebSEAL) を使用して、WebFOCUS でシングルサインオン (SSO) を有効にすることができます。これらのシステムは、WebFOCUS へのリクエストを代行受信し、WebFOCUS にアクセスするユーザを認証、認可した後、事前認証されたユーザ ID を HTTP ヘッダで WebFOCUS に渡します。これらのシステムがリクエストを代行受信し、リクエストごとに HTTP ヘッダに値を挿入するため、WebFOCUS は、HTTP ヘッダに挿入されたユーザ ID が有効であることを信頼することができます。

手順　Web アクセス管理システムによる事前認証を構成するには

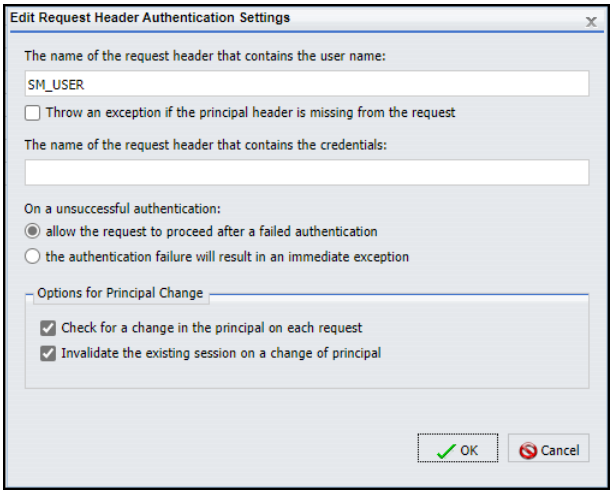
次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティ] タブで、Web アクセス管理システムによる事前認証をサポートするセキュリティゾーンのフォルダ下で [認証] をクリックします。

   通常、これはデフォルトセキュリティゾーンです。
3. [リクエストヘッダ認証] エントリを右クリックし、[編集] を選択します。

4. 下図のように、Web アクセス管理システムから提供されたデフォルト名を [ユーザ名の格納先リクエストヘッダ名] テキストボックスに入力します。



   - CA SiteMinder の場合、この値には通常「SM_USER」を使用します。
   - IBM Tivoli Access Manager WebSEAL の場合、この値には通常「iv-user」を使用します。
   - Oracle Access Manager の場合、Oracle Access Manager のマニュアルを参照してください。

5. [OK] をクリックします。
6. [認証] ページの [アクション] セクションで、[オプション] をクリックします。
7. [認証オプション] ダイアログボックスで、[カスタムログアウトターゲット URL を有効にする] のチェックをオンにします。
8. Web アクセス管理システムから提供されたカスタムログアウトターゲット URL を入力します。
   - Siteminder の場合、この値は通常「http://siteminder.domain.com/logout.html」です。
   - IBM Tivoli Access Manager WebSEAL の場合、
     この値には通常「http://webseal.domain.com/pkmslogout」です。
   - Oracle Access Manager の場合、Web Access Management のマニュアルまたはシステム管理者に問い合わせてください。
9. [OK] をクリックします。
10. [認証] ページで [リクエストヘッダ認証] を右クリックし、[有効にする] を選択します。

11. [認証] ページの [セキュリティゾーン] セクションで、[保存] をクリックします。
12. 「Web セキュリティ構成データは正常に保存されました」というメッセージで、[OK] をクリックします。
13. 「これらの変更を有効にするには、Web アプリケーションを再起動してください」というメッセージで、[OK] をクリックします。
14. 現在のセッションからログアウトします。
15. WebFOCUS Reporting Server を停止し、再起動します。
16. 管理者として再度ログインし、新しい構成をテストします。

手順　リクエストヘッダ認証を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティゾーン] フォルダ下で、変更するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
3. [リクエストヘッダ認証] エントリを右クリックし、[編集] を選択します。
4. [リクエストヘッダ認証の編集] ダイアログボックスが開きます。
   a. CA Site Minder を使用する場合は、ユーザ名を格納するリクエストヘッダの名前としてデフォルト名 (SM_USER) を受容します。
   b. IBM Tivoli Access Manager WebSEAL を使用する場合は、「iv-user」と入力します。
   c. Oracle Access Manager を使用する場合は、Oracle Access Manager 管理者から提供された値を入力します。

   この値の大文字と小文字は区別されませんが、値の綴りが、管理コンソールで指定した値の綴りに一致する必要があります。
5. [リクエストにプリンシパルヘッダが存在しない場合、例外をスロー] のチェックはオフのままにします。このチェックボックスは、認証プロセスでこのイベントが発生した際に例外を記録する場合にのみオンにします。
6. [認証情報の格納先リクエストヘッダ名] テキストボックスに、ユーザ ID を入力します。

   たとえば、「SM_USER」、「iv-user」と入力します。

7. [認証失敗時の動作] セクションで、次のように指定します。
   a. 認証の失敗時に例外を生成するには、[認証の失敗時に例外をスロー] のチェックをオンにします。
   b. 認証に失敗した場合でもリクエストの実行を続行するには、デフォルト設定の [認証失敗後もリクエストの続行を許可する] を受容します。
8. 各認証リクエストにユーザ名の変更の確認を含めるには、[各リクエストでプリンシパルの変更を確認する] のチェックをオンにします。
9. ユーザ名が変更された場合にセッションを無効にするには、[各リクエストでプリンシパルの変更を確認する] のチェックをオンにします。
10. 構成の完了後、[OK] をクリックします。
11. [リクエストヘッダ認証] エントリを右クリックし、[有効にする] を選択します。
12. [アクション] セクションで [保存] をクリックします。
13. 「変更は正常に保存されました」というメッセージで、[OK] をクリックします。
14. 「Web アプリケーションを再起動してください」というメッセージで、[OK] をクリックします。
15. 現在のセッションからログアウトします。
16. WebFOCUS Reporting Server を停止し、再起動します。
17. 管理者としてログインし、新しい構成をテストします。

統合 Windows 認証による事前認証の構成

統合 Windows 認証を使用した事前認証の場合、WebFOCUS は、Microsoft Internet Information Services (IIS) を WebFOCUS の Windows 認証オプションまたは Basic 認証オプションとともに使用して、Microsoft Windows ユーザを認証します。この構成では、WebFOCUS のホストである Java Web アプリケーションコンテナにユーザ ID を安全に渡すために、IIS のプラグイン構成が必要です。IIS と Tomcat の構成および IIS と WebSphere の構成についての追加情報は、次の手順の末尾に記載されています。

手順　Windows 認証による事前認証を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

Windows 認証を使用する場合に、管理タスクを実行するために Windows 認証をバイパスする必要のある管理者のフォームベース内部認証を継続してサポートするには、代替セキュリティゾーンを有効にすることをお勧めします。詳細は、155 ページの 「 セキュリティゾーンを有効にするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [デフォルト] セキュリティゾーンフォルダ下で [認証] をクリックします。
3. [認証] ページの [アクション] セクションで、[オプション] をクリックします。
4. [認証オプション] ダイアログボックスで、[カスタムログアウトターゲット URL を有効にする] のチェックをオンにし、[カスタムログアウトターゲット URL] テキストボックスのデフォルト値である「/signout」を受容して [OK] をクリックします。
5. [認証] ページで [JEE コンテナベース認証] をクリックします。

   通常、IIS はユーザ ID の先頭にユーザの Windows ドメイン名を追加し、「domain name ¥user ID」の形式で WebFOCUS に渡します。デフォルト設定では、WebFOCUS はこの値からドメイン名とバックスラッシュ (¥) を除外してユーザ ID のみにします。このユーザ ID が、ログイン処理に使用されます。

   このデフォルト動作を受容し、変更を加えずに次の手順へ進むことをお勧めします。この動作を変更する必要がある場合は、[JEE コンテナベース認証設定の編集] ダイアログボックスで [JEE ユーザプリンシパル名からドメイン名を除外] のチェックをオフにし、[OK] をクリックして変更内容を保存します。
6. [JEE コンテナベース認証] エントリが選択された状態で [有効にする] をクリックします。

   その他すべての認証は、自動的に無効になります。
7. [認証] ページの [セキュリティゾーン] セクションで、[保存] をクリックします。
8. 「Web セキュリティ構成データは正常に保存されました」というメッセージで、[OK] をクリックします。
9. 「Web アプリケーションを再起動してください」というメッセージで、[OK] をクリックします。
10. 現在のセッションからログアウトします。
11. コネクタから渡されたユーザ ID を信頼するよう JEE コンテナを有効にします。

    - Tomcat の場合、server.xml ファイル (Windows の場合は *drive*:¥tomcat¥conf、UNIX または Linux の場合は *installdirectory*/tomcat/conf に格納) を開き、次の例のように、APJ Connector ブロックに tomcatAuthentication キーワードを追加し、false に設定します。

```
<!-- Define an AJP 1.3 Connector on port 8009 -->
<Connector port="8009" protocol="AJP/1.3"
tomcatAuthentication="false" redirectPort="8443" />
```

- WebSphere の場合、WebSphere のマニュアルを参照し、WebSphere REMOTE_USER 変数を使用して、IIS コネクタから WebFOCUS に渡されたユーザ ID を読み取る方法を確認してください。

12. WebFOCUS Reporting Server を停止し、再起動します。
13. 管理者として再度ログインし、新しい構成をテストします。
    - 代替ゾーンを有効にした場合 (推奨)、WebFOCUS マシンにログインする際に、内部認証を使用して WebFOCUS にアクセスすることができます。この URL は「http://localhost/ibi_apps」です。また、任意のワークステーションで「http://machinename/ibi_apps」からログインすると、事前認証で WebFOCUS にアクセスすることができます。Web ブラウザの設定で、ドメイン名を使用した Windows 認証が自動的に使用されるよう構成していない場合、「http://machinename.domain.com/ibi_apps」からログインすると、ユーザに対して認証情報の入力が要求されます。
    - デフォルト設定では、Internet Explorer は Web サイトアドレスが「http://machinename」の形式の場合にのみ、自動的に Windows 認証を使用します。「http://machinename.domain.com」の形式で WebFOCUS にアクセスするユーザの Windows 認証を有効にするために、ユーザマシンの Internet Explorer でローカルイントラネットゾーン設定の再構成が必要になる場合があります。

カスタムシングルサインオン (SSO) を提供する事前認証の構成

WebFOCUS に他のアプリケーションを統合することで、ユーザにシングルサインオン (SSO) 機能を提供することができます。たとえば、ユーザが既存の Web アプリケーションにログインし、入力した認証情報がその Web アプリケーションで確認されるとします。ユーザがこの Web アプリケーションで ポータルに移動するボタンやリンクをクリックすると、パスワードの再入力が要求されずに、WebFOCUS に自動的にログインした状態になります。

この統合を実現する最良の方法は、WebFOCUS Web アプリケーション内部でカスタム Java Servlet フィルタを展開することです。技術サポートに依頼して、IBIServletFilter に基づいたカスタムソリューションを作成することができます。別の方法として、ユーザが IIS 経由で WebFOCUS にアクセスする場合は、ASP.NET を使用して HTTP モジュールを IIS にインストールすることもできます。

カスタムソリューションでは、一般に共有シークレット手法を使用します。この手法では、ユーザが既存の Web アプリケーション内のリンク、ボタン、タブのいずれかをクリックすることで、WebFOCUS への接続を開始します。Web アプリケーションがユーザ ID を設定し、ユーザ ID とタイムスタンプが含まれた AES 暗号化トークンを作成します。次に Web アプリケーションがこのトークンを WebFOCUS に渡します。

WebFOCUS では、IBIServletFilter がトークンを復号化し、タイムスタンプと現在時間を比較して、そのトークンが特定の時間間隔を超えたかどうかを特定します。IBIServletFilter は、この時間チェックを実行することで、リプレイ攻撃 (期限切れトークンに基づいて未承認ユーザの認証を試みる不正な攻撃) が発生しなかったことを確認します。

トークンが特定の時間間隔を超えてない場合、IBIServletFilter はそのトークンからのユーザ ID と、保持されているユーザ ID を比較します。これらのハッシュが一致した場合、そのユーザ ID は信頼されます。一致しない場合、接続は拒否されます。

シングルサインオンを提供する Kerberos の構成

WebFOCUS は、Windows 環境で Web ブラウザ、WebFOCUS Client、および Kerberos 事前認証を使用するネットワークの WebFOCUS Reporting Server 間のシングルサインオン (SSO) をサポートします。これには、WebFOCUS Reporting Server 上での偽装サポートも含まれます。つまり、Microsoft SQL Server などの、トラステッド接続をサポートする RDBMS アダプタを使用することで、SSO 機能を拡張することができます。

ここでは、Active Directory のネイティブ Kerberos サポートを使用した SSO 環境で WebFOCUS を構成する方法について説明します。この操作では、Windows Active Directory、WebFOCUS、および WebFOCUS に割り当てられたブラウザのアップデートが必要です。Active Directory の構成では、WebFOCUS Client および WebFOCUS Reporting Server をサポートするサーバのアカウントを含めること、また Kerberos 認証の委任方法を定義することが必要です。WebFOCUS の構成では、関連する各セキュリティゾーンで Kerberos 認証のサポートが必要です。ユーザに割り当てられた各ブラウザの構成では、Kerberos 認証の使用をサポートするサーバおよびクライアント URL の特定が必要です。以下は、これらのタスクの詳細な説明です。

Kerberos を使用した事前認証の制限事項

- **ReportCaster** ReportCaster は、Kerberos 環境で使用することができます。構成および追加のリリースレベル要件についての詳細は、297 ページの 「 ReportCaster サポートの構成 (Kerberos 認証) 」 を参照してください。

- **同一マシン上の WebFOCUS Client と WebFOCUS Reporting Server**　両方のコンポーネントが同一マシンに存在する場合は、ノードの HOST キーワードをコンピュータ名の形式で指定する必要があります。localhost または完全修飾ドメイン名を使用すると、ランタイムエラーが発生します。これらのコンポーネントがそれぞれ異なるマシンに存在する場合は、コンピュータ名または完全修飾ドメイン名の形式を使用することができます。HOST キーワードは、管理コンソールの [サーバ接続] セクションで指定します。

- **Web ブラウザ**　Web ブラウザと WebFOCUS が同一の Windows マシンに存在する場合は、これらの 2 つのコンポーネント間で Kerberos はサポートされません。

- **複数グループに属するユーザ**　Kerberos 実装では、ユーザが属する各グループは、それぞれの Kerberos チケット内に格納されます。そのため、ユーザが多数のグループに属する場合にチケットのサイズが増大します。詳細は、298 ページの 「 大規模チケットサポートの構成 (Kerberos 認証) 」 を参照してください。

- **ユーザ ID のフォーマット**　Kerberos 事前認証を使用する場合は、Kerberos が各ユーザに割り当てる認証情報の ID と一致した WebFOCUS ユーザ ID を作成する必要があります。Kerberos では通常、ユーザの Windows ドメインをユーザ ID の末尾に追加しますが、WebFOCUS では、デフォルト設定でこのドメインを除外するよう構成されています。そのため、組織では多くの場合、Kerberos ユーザ ID からドメインサフィックスを除外するだけで、WebFOCUS ユーザ ID になります。

  ただし、ユーザの組織でこのデフォルト構成が無効化されている場合は、ユーザ ID に次のフォーマットを使用する必要があります。

  ```
  user_ID @ domain.com
  ```

  説明

  `user_ID`
  Kerberos チケットで WebFOCUS に渡されるユーザ ID です。

  `domain.com`
  利用可能なドメインおよび拡張子です。

- **ドメイン接尾語**　通常、Kerberos は、WebFOCUS に渡されたユーザ ID の末尾にユーザの Windows ドメインを追加し、「user ID@domain.com」のフォーマットにします。デフォルト設定では、この連結された値からドメイン部分が除外され、ユーザ ID のみになります。残ったユーザ ID のみを使用して、ログイン処理が完了します。

このデフォルト構成を上書きし、WebFOCUS によるドメインの除外を回避するには、[Kerberos/SPNEGO 認証設定の編集] ダイアログボックスの [DNS サフィックスの除外を有効にする] のチェックをオフにします。このダイアログボックスは、管理コンソールの [セキュリティ] タブで [認証] ページを選択すると表示されます。

制約付き委任と制約なしの委任についての理解

WebFOCUS では、Kerberos 事前承認で許可されるアカウント認証情報について、制約なしの委任と制約付き委任がともにサポートされます。

制約なしの委任では、アカウント認証情報の委任がドメイン内のすべてのサービスに許可されます。制約付き委任では、アカウント認証情報の委任が特定のサービスのみに制限されます。

いずれの場合も構成は同一の基本パスに従います。ただし、WebFOCUS Reporting Server のみへの制約付き委任または WebFOCUS Reporting Server とデータベースサーバへの制約付き委任を設定するには、次の構成タスクを追加する必要があります。

- アカウントが、サービスプリンシパル名 (SPN) を使用して委任されるマシンを特定する。
- [サービスの種類] として [HTTP] を指定し、Kerberos 認証が委任される特定のコンピュータを特定する。

Kerberos 認証を WebFOCUS Reporting Server からリレーショナルデータベース管理システム (RDBMS) に委任する必要がある場合は、この委任をサポートする接続を WebFOCUS Reporting Server に構成する必要があります。詳細は、Reporting Server ブラウザインターフェースオンラインヘルプのコンテンツを参照してください。

Windows Active Directory での Kerberos 実装のインストール前の作業

Windows Active Directory に WebFOCUS を追加するために必要なインストール前の作業は、Kerberos 認証について制約付き委任を使用するか制約なしの委任を使用するかによって異なります。

制約付き委任を使用する場合、ドメインの管理権限を所有するネットワーク管理者は、インストールの前に次の作業を実行する必要があります。

- WebFOCUS Reporting Server でサービスプリンシパル名 (SPN) が使用可能なことを確認します。
- Active Directory で WebFOCUS Client のサービスアカウントを作成します。
- KTPASS.EXE ユーティリティの ktpass コマンドを使用して、WebFOCUS Client の Kerberos keytab ファイルを生成します。

- ❑ Active Directory で制約付き委任のサービスユーザアカウントを構成します。

制約なしの委任を使用する場合、ドメインの管理権限を所有するネットワーク管理者は、インストールの前に次の作業を実行する必要があります。

- ❑ Active Directory で WebFOCUS Client のサービスアカウントを作成します。
- ❑ KTPASS.EXE ユーティリティの ktpass コマンドを使用して、WebFOCUS Client の Kerberos keytab ファイルを生成します。
- ❑ Active Directory で制約なしの委任のサービスユーザアカウントを構成します。

注意：いずれの場合も、Windows Server 2008 を稼動している場合は、Kerberos keytab ファイルの使用をサポートするために、ドメインコントローラ用の次の Microsoft パッチのインストールが必要になる場合があります。
http://support.microsoft.com/kb/951191

手順　WebFOCUS Reporting Server のサービスプリンシパル名 (SPN) を確認するには

Kerberos 認証について制約なしの委任の使用を選択した場合は、WebFOCUS Reporting Server のサービスプリンシパル名は必要ないため、この手順を省略できます。266 ページの「Windows Active Directory でサービスアカウントユーザを作成するには」の手順へ進みます。

Kerberos 認証について制約付き委任の使用を選択した場合は、Kerberos 認証を委任する前に WebFOCUS Reporting Server のサービスプリンシパル名 (SPN) を確認する必要があります。次の手順を実行することで、WebFOCUS Reporting Server に割り当てられた SPN を特定することができます。

ただし、WebFOCUS Reporting Server の SPN が予めわかっている場合は、この手順を省略して、266 ページの「Windows Active Directory でサービスアカウントユーザを作成するには」へ進むことができます。

1. ドメインコントローラ、または Windows ドメインにログインされた別のマシンで、ドメイン管理者としてログインし、[コマンドプロンプト] ウィンドウを開きます。
2. 次のコマンドを入力、実行し、サービスプリンシパル名が WebFOCUS Reporting Server をホストするマシンに作成されたかどうかを確認します。

   ```
   setspn -l hostname
   ```

   説明

   `hostname`
   WebFOCUS Reporting Server のマシン名です (例、rs-kerb)。
3. 出力結果に次のメッセージが表示された場合

```
Could not find account hostname
```

説明

`hostname`
: WebFOCUS Reporting Server のマシン名です (例、rs-kerb)。

WebFOCUS Reporting Server がドメインに追加されなかったことを示します。

WebFOCUS Reporting Server をドメインに追加する方法についての詳細は、「Adding Users and Computers to the Active Directory Domain」(https://support.microsoft.com/en-us/help/324753/how-to-create-an-active-directory-server-in-windows-server-2003) の手順を参照してください。

4. 出力結果に次のメッセージが表示された場合

```
Registered ServicePrincipalName...
```

ただし、次のエントリが含まれない場合

```
HTTP/hostname.ibi.com
```

説明

`hostname.ibi.com`
: WebFOCUS Reporting Server の完全な SPN です。*hostname* は、WebFOCUS Reporting Server のマシン名です (例、rs-kerb.ibi.com)。

制約付き委任をサポートする SPN は、WebFOCUS Reporting Server では使用できません。

この場合、264 ページの 「 サービスプリンシパル名 (SPN) を作成するには 」 に説明する手順に従って WebFOCUS Reporting Server の SPN を新規作成する必要があります。

5. 出力結果に次のメッセージが表示された場合

```
Registered ServicePrincipalName...
```

また、次のエントリが含まれる場合

```
HTTP/hostname.ibi.com
```

説明

`hostname.ibi.com`
: WebFOCUS Reporting Server の完全な SPN です。*hostname* は、WebFOCUS Reporting Server のマシン名です (例、rs-kerb.ibi.com)。

WebFOCUS Reporting Server では、制約付き委任をサポートする SPN が使用できます。

次のトピック (266 ページの 「 Windows Active Directory でサービスアカウントユーザを作成するには 」) へ進みます。

サービスプリンシパル名 (SPN) の確認結果の例

次の結果例は、rs-kerb という WebFOCUS Reporting Server のサービスプリンシパル名が確認できたことを示します。2 行目に、この WebFOCUS Reporting Server の完全な SPN として HTTP/rs-kerb.ibi.com が特定されています。

```
setspn -l rs-kerb
Registered ServicePrincipalNames for CN=RS-KERB, OU=Workstations,DC=ibi,DC-
com:
     HTTP/rs-kerb.ibi.com
     TERMSRV/rs-kerb.ibi.com
     TERMSRV/RS-KERB
     WSMAN/rs-kerb.ibi.com
     WSMAN/rs-kerb
     RestrictedKrbHost/rs-kerb.ibi.com
     RestrictedKrbHost/RS-KERB
     HOST/RS-KERB
     HOST/rs-kerb.ibi.bom
```

次の結果例には、setspn ステートメントで rs-kerb という名前のアカウントが見つからなかったことを示すメッセージが含まれています。

```
setspn -l rs-kerb
FindDomainForAccount: Call to DsGetDcNameWithAccountW failed with return
value 0x00000525
Could not find account rs-kerb
```

手順　サービスプリンシパル名 (SPN) を作成するには

setspn コマンドを使用して、WebFOCUS Reporting Server のサービスプリンシパル名 (SPN) を作成します。

1. ドメインコントローラ、または Windows ドメインにログインされた別のマシンで、ドメイン管理者としてログインし、[コマンドプロンプト] ウィンドウを開きます。
2. 次のコマンドを入力、実行します。

   注意：WebFOCUS Reporting Server の完全な SPN に指定する値には、先頭に大文字の HTTP、次にスラッシュ (/) を追加します。

   コマンドのフォーマットは、次のとおりです。

   ```
   setspn -a HTTP/hostname.ibi.com hostname
   ```

説明

`hostname.ibi.com`
WebFOCUS Reporting Server の完全な SPN です。*hostname* は、WebFOCUS Reporting Server のマシン名です (例、rs-kerb.ibi.com)。

出力結果は次のとおりです。

```
Registering ServicePrincipalNames for CN=hostname,
CN=Computers,DC=ibi,DC=com
        HTTP/hostname.ibi.com
Updated object
```

説明

`hostname`
WebFOCUS Reporting Server のコンピュータ名です。*hostname* は、WebFOCUS Reporting Server のマシン名です (例、rs-kerb.ibi.com)。

3. 次のコマンドを入力、実行して、新規作成した SPN が存在することを確認します。

```
setspn -l hostname
```

説明

`hostname`
作成した 新しい SPN です (例、rs-kerb)。

作成できた場合は、次のメッセージが表示されます。

```
Registered ServicePrincipalNames for
CN=hostname,CN=Computers,DC=ibi,DC=com
```

メッセージの後に、次のエントリを含む結果のリストが表示されます。

```
HTTP/hostname.ibi.com
```

説明

`hostname.ibi.com`
作成した新しい SPN です。*hostname* は、WebFOCUS Reporting Server のマシン名です (例、rs-kerb.ibi.com)。Kerberos 委任に関連する値はこの値のみです。

正常なサービスプリンシパル名 (SPN) 登録の例

次の例は、コンピュータ名 rs-kerb の新しいサービスプリンシパル名として HTTP/rs-kerb.ibi.com が登録されたことを示します。

```
Registering ServicePrincipalNames for CN=RS-KERB,CN=Computers,DC=ibi,DC=com
     HTTP/rs-kerb.ibi.com
Updated object
```

次のレスポンスメッセージは、新規作成された SPN の存在を確認するもので、コンピュータ名 rs-kerb の登録済みサービスプリンシパル名がすべて表示されます。

```
Registered ServicePrincipalNames for CN=RS-KERB,CN=Computers,DC=ibi,DC=com:
     HTTP/rs-kerb.ibi.com
     WSMAN/rs-kerb
     WSMAN/rs-kerb.ibi.com
     TERMSRV/RS-KERB
     TERMSRV/rs-kerb.ibi.com
     RestrictedKrbHost/RS-KERB
     HOST/RS-KERB
     RestrictedKrbHost/rs-kerb.ibi.com
```

手順　Windows Active Directory でサービスアカウントユーザを作成するには

この手順では、Active Directory で WebFOCUS SSO 機能のサービスアカウントを作成します。これにより、Kerberos 処理の WebFOCUS Client が特定されます。

1. ドメインコントローラで、Windows の [Active Directory ユーザーとコンピューター] ウィンドウを開きます。
2. 新しいユーザを追加するフォルダに移動し、これを開きます。
3. ユーザリストの任意の場所で右クリックし、[新規ユーザー] を選択します。
4. 下図のように、[新しいオブジェクト - ユーザー] ウィザードの最初のページで、[名] および [フルネーム] テキストボックスに WebFOCUS がインストールされたマシンの名前を入力します。

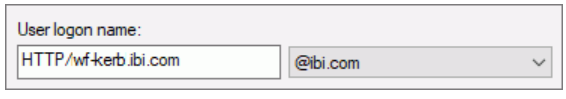
[名] および [フルネーム] に指定する値には、先頭に小文字の http、次にアンダースコア (_) を追加する必要があります。フォーマットは、次のとおりです。

```
http_hostname
```

説明

`hostname`
WebFOCUS がインストールされたマシンのコンピュータ名です (例、wf-kerb)。

5. 下図のように、[ユーザーログオン名] テキストボックスに、WebFOCUS がインストールされたマシンの名前を入力します。



[ユーザーログオン名] に指定する値は、先頭に大文字の HTTP、次にスラッシュ (/) を追加します。フォーマットは、次のとおりです。

```
HTTP/hostname.domain.ext
```

説明

`hostname.domainext`
WebFOCUS Client がインストールされたマシンの完全修飾ドメイン名です。

6. 下図のように、自動的に割り当てられた [ユーザーログオン名 (Windows 2000 より前)] テキストボックスの値を、WebFOCUS Client がインストールされたマシン名で上書きします。

[ユーザーログオン名] に指定する値には、先頭に小文字の http、次にアンダースコア (_) を追加します。フォーマットは、次のとおりです。

```
http_hostname
```

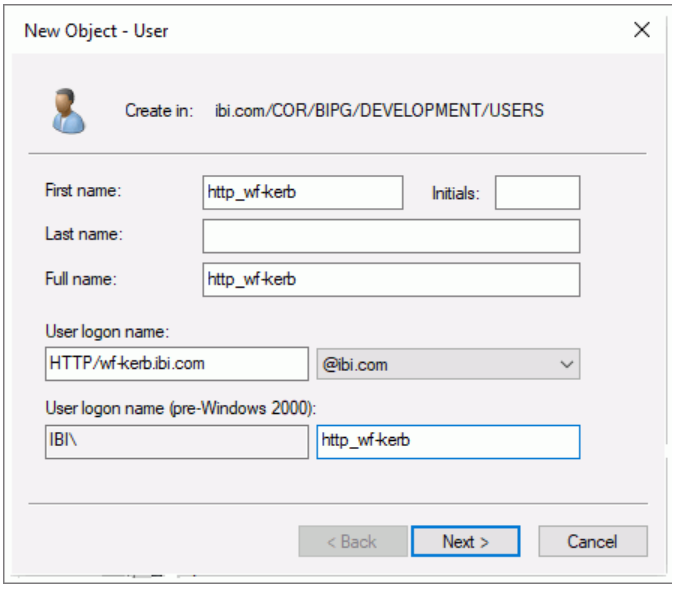
説明

`hostname`
WebFOCUS Client がインストールされたマシンの名前です (例、wf-kerb)。

[ユーザーログオン名 (Windows 2000 より前)] に指定した値が、このサービスアカウントの sAMAccountName 属性になります。

7. 入力した内容を確認後、下図のように [次へ] をクリックします。

   この例では、[新しいオブジェクト - ユーザー] ダイアログボックスに推奨されるフォーマットで値が入力されており、WebFOCUS Client が wf-kerb という名前のマシンにインストールされていることを示しています。

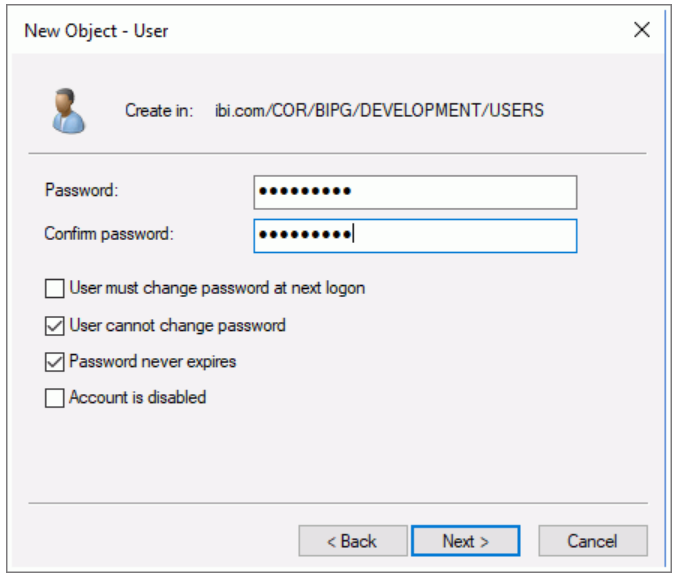


8. 下図のように、次のページでパスワードの入力が要求された場合は、次の手順を実行します。

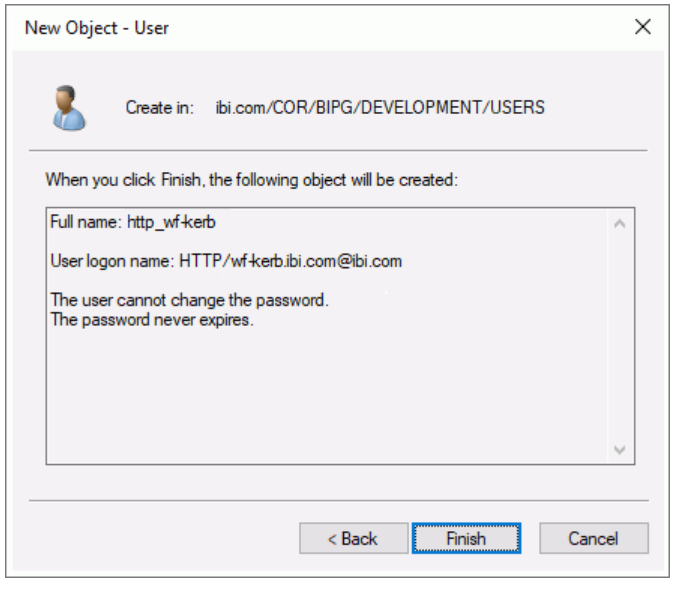
   a. [パスワード] および [パスワードの確認入力] テキストボックスに、サービスアカウントユーザのパスワードを入力します。

   b. [ユーザーは次回ログオン時にパスワードの変更が必要] のチェックをオフにします。

c. [ユーザーはパスワードを変更できない] および [パスワードを無期限にする] のチェックボックスを選択し、[次へ] をクリックします。



9. 下図のように、確認ページが表示された場合は、作成するサービスアカウントユーザのプロパティのリストを確認し、[完了] をクリックします。



手順　サービスアカウントユーザの ktpass コマンドを実行するには

サービスアカウントの servicePrincipalName (SPN) 属性を設定し、WebFOCUS の Kerberos keytab ファイルを生成するには、ドメインコントローラの [コマンドプロンプト] ウィンドウから ktpass コマンドを実行する必要があります。このコマンドおよびすべての引数と値を単一行に入力します。後でトラブルシューティングに対応できるよう、このコマンド構文のコピーを保存しておくことをお勧めします。

1. ドメインコントローラで [コマンドプロンプト] ウィンドウを開きます。
2. [コマンドプロンプト] ウィンドウに、次のフォーマットで ktpass コマンドを入力します。

```
ktpass /out filename /mapuser user_ID /princ principal /crypto
encryption /pass password /ptype KRB5_NT_PRINCIPAL
```

説明

`filename`
ktpass コマンドが Kerberos keytab ファイルの作成に使用する名前です。推奨値は http_*hostname*.keytab です。

説明

`hostname`
WebFOCUS Client サービスアカウントの完全名です (例、wf-kerb.ibi.com」) 。

`user_ID`
サービスアカウントの [ユーザーログオン名 (Windows 2000 より前)] テキストボックスに入力した sAMAccountName の値です。

`principal`
サービスアカウントの [ユーザーログオン名] テキストボックスに入力したユーザログオン名の値に「*@REALM*」を連結した値です。ここで、REALM は Kerberos レルムを表します。Kerberos レルムには通常、Active Directory DNS サフィックスと同一の値を使用します。ただし、Kerberos レルムの値はすべて大文字で入力します。

`encryption`
keytab ファイルの作成時に使用する暗号化オプションです。場合によっては、推奨値である All をサポートする ktpass コマンドを使用するために、最新の Microsoft サポートツールをダウンロードする必要があります。

注意：ネットワーク上のマシンのいずれかで Windows Server 2008 R2、Windows 7、またはそれ以降が稼動している場合、これらのマシンが Kerberos とともに正しく機能するよう All を選択する必要があります。Microsoft は、これ以降の Windows バージョンで DES のサポートをすべて廃止しました。

`password`
サービスアカウントに関連付けられている Windows パスワードをテキストで指定します。

次の例は、このセクションで先に示した例に適用された正しいフォーマットの ktpass コマンドを示しています。

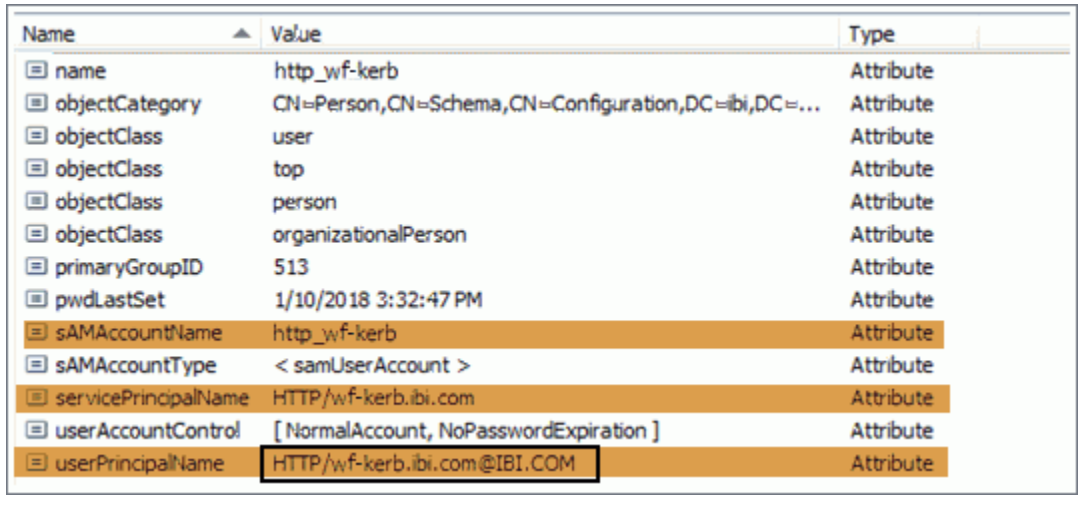
```
C:¥>ktpass /out http_wf-kerb.keytab /mapuser http_wf-kerb /princ
HTTP/wf-kerb.ibi.com@IBI.COM /crypto All /pass password1
/ptype KRB5_NT_PRINCIPAL
```

3. ktpass コマンドが成功した場合は、次の例のように、[コマンドプロンプト] ウィンドウに「Successfully mapped」というレスポンスメッセージが表示されます。

```
Targeting domain controller: ibidca.ibi.com
Successfully mapped HTTP/wf-kerb.ibi.com to http_wf-kerb.
Key created.
Output keytab to http_wf-kerb.keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x0df97e7355555817c828671454137af0)
```

4. Active Directory サービスアカウントのプロパティの表示を許可するユーティリティを開き、新しいサービスアカウントのプロパティを開きます。

下図のように、プロパティ名をスクロールし、ktpass コマンドに、servicePrincipalName (SPN) という名前の属性が追加され、sAMAccountName および userPrincipalName (UPN) 属性が変更されていることを確認します。

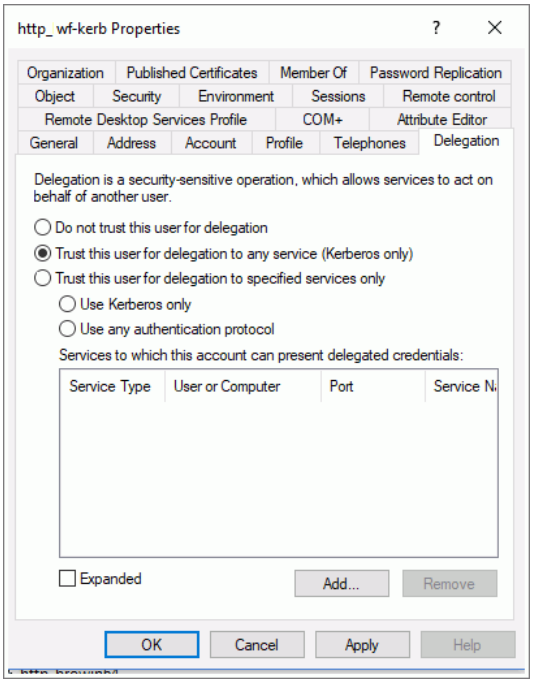


手順　Active Directory で委任のサービスアカウントユーザを構成するには

サービスアカウントユーザの [プロパティ] ダイアログボックスの [委任] タブを使用して、Windows Active Directory で Kerberos に制約付き委任または制約なしの委任を構成することができます。

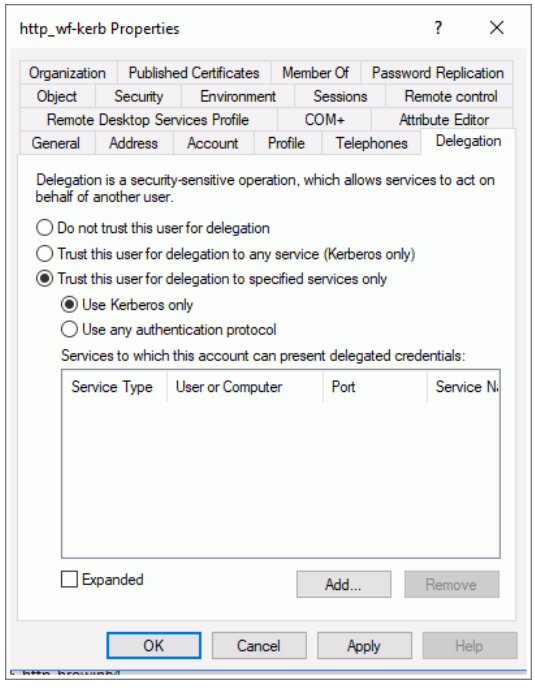
1. [Active Directory ユーザーとコンピューター] ウィンドウのユーザリストでサービスアカウントユーザを右クリックし、[プロパティ] を選択します。
2. [プロパティ] ダイアログボックスの [委任] タブをクリックします。

   注意：[委任] タブは、ktpass コマンドの実行後にのみ表示されます。詳細は、270 ページの 「 サービスアカウントユーザの ktpass コマンドを実行するには 」 を参照してください。
3. 制約なしの委任を使用する場合は、下図のように、デフォルト設定で選択された [任意のサービスへの委任でこのコンピューターを信頼する] オプションを受容し、手順 9 へ進みます。

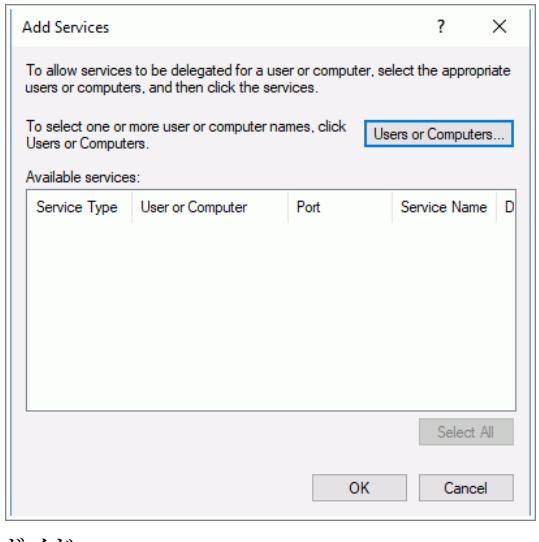


4. 制約付き委任を使用する場合は、下図のように、[このコンピューターを信頼する] を選択し、[追加] をクリックします。

   注意：[Kerberos のみを使う] オプションは、デフォルト設定で選択されています。



5. 下図のように、[サービスの追加] ダイアログボックスで [ユーザーまたはコンピューター] をクリックします。



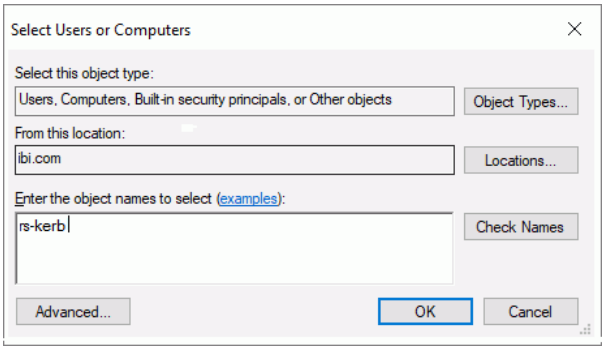
6. 下図のように、[ユーザーまたはコンピューターの選択] ダイアログボックスで、[選択するオブジェクト名を入力してください] テキストボックスに、[このアカウントが委任された資格情報を提示できるサービス] の SPN を入力し、[OK] をクリックします。

   通常は、次の値を使用します。

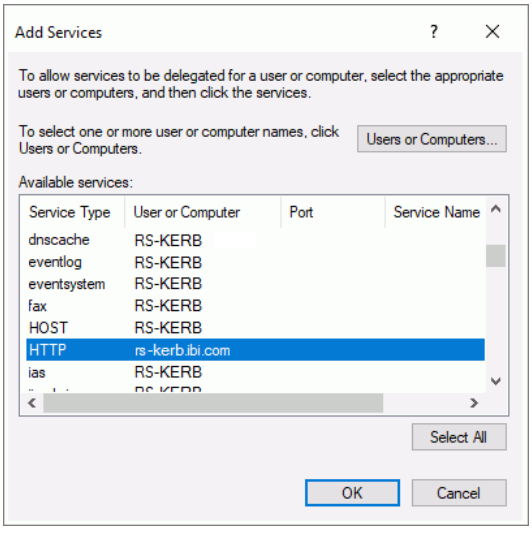
   ```
   hostname
   ```

   説明

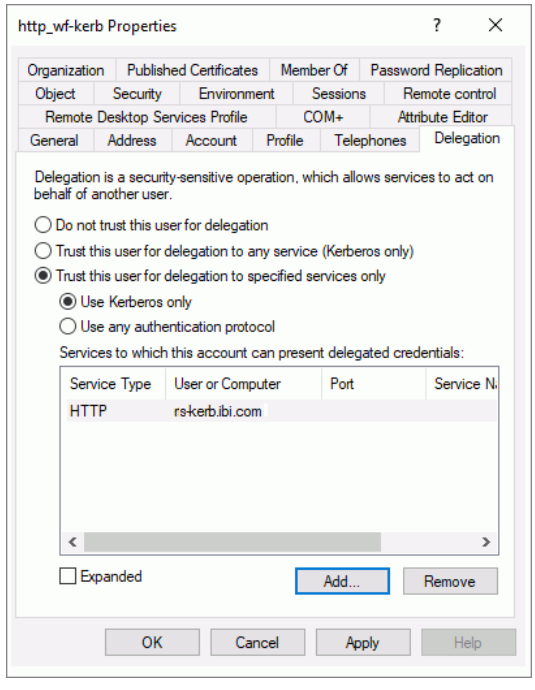
   `hostname`
   : このアカウントが委任された資格情報を提示できる WebFOCUS Reporting Server の SPN です。



7. 下図のように、[サービスの追加] ダイアログボックスの [利用可能なサービス] リストの [サービスの種類] 列で [HTTP] を選択し、[OK] をクリックします。



8. 下図のように、選択した [サービスの種類] と [サービスアカウント名] が、[このアカウントが委任された資格情報を提示できるサービス] リストに表示されていることを確認し、[OK] をクリックします。



9. ホストヘッダを使用しない場合は、作成された keytab ファイル (例、http_wf-kerb.keytab) を、WebFOCUS をインストールするマシンにコピーします。ホストヘッダを使用する場合は、275 ページの 「 ホストヘッダサポート (Kerberos 認証) 」 へ進みます。

ホストヘッダサポート (Kerberos 認証)

1 つまたは複数のホストヘッダを使用する場合は、次の手順を実行する必要があります。

手順 **ホストヘッダサポートを実装するには (Kerberos 認証)**

次の手順では、wf-kerb1 および wf-kerb2 という 2 つのホストヘッダ名が存在することを前提にしています。

1. DNS に各ホストヘッダの A レコードを追加し、NetBIOS 名と同一の IP アドレスを指定します。

   注意：C レコードは作成しないでください。

2. 次のフォーマットを使用して、ホストヘッダごとに ktpass コマンドを実行します。

```
ktpass /in filename /out filename /princ principal /crypto encryption/
pass password /ptype KRB5_NT_PRINCIPAL
```

a. wf-kerb1 では、次の ktpass コマンドを実行します。

```
ktpass /in c:¥keytab¥http_wf-kerb.keytab
/out c:¥keytab¥http_wf-kerb.keytab
/princ HTTP/wf-kerb1.ibi.com@IBI.COM /crypto All
/pass password1 /ptype KRB5_NT_PRINCIPAL
```

出力結果は次のとおりです。

```
Existing keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
NOTE: creating a keytab but not mapping principal to any user.
      For the account to work within a Windows domain, the
      principal must be mapped to an account, either at the
      domain level (with /mapuser) or locally (using ksetup)
      If you intend to map HTTP/wf-kerb1.ibi.com@IBI.COM to an
      account through other means or don't need to map the
      user, this message can safely be ignored.
WARNING: pType and account type do not match. This might cause
problems.
Key created.
Output keytab to c:¥keytab¥http_wf-kerb.keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
keysize 64 HTTP/wf-kerb1.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 1 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
```

b. wf-kerb2 では、次の ktpass コマンドを実行します。

```
ktpass /in c:¥keytab¥http_wf-kerb.keytab
/out c:¥keytab¥http_wf-kerb.keytab
/princ HTTP/wf-kerb2.ibi.com@IBI.COM /crypto All
/pass password1 /ptype KRB5_NT_PRINCIPAL
```

出力結果は次のとおりです。

```
Existing keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
keysize 64 HTTP/wf-kerb1.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 1 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
NOTE: creating a keytab but not mapping principal to any user.
      For the account to work within a Windows domain, the
      principal must be mapped to an account, either at the
      domain level (with /mapuser) or locally (using ksetup)
      If you intend to map HTTP/wf-kerb2.ibi.com@IBI.COM to an
      account through other means or don't need to map the
      user, this message can safely be ignored.
WARNING: pType and account type do not match. This might cause
problems.
Key created.
Output keytab to c:¥keytab¥http_wf-kerb.keytab:
Keytab version: 0x502
keysize 63 HTTP/wf-kerb.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 2 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
keysize 64 HTTP/wf-kerb1.ibi.com@IBI.COM ptype 1 (KRB5_NT_PRINCIPAL)
vno 1 etype
0x17 (RC4-HMAC) keylength 16 (0x5835048ce94ad0564e29a924a03510ef)
```

3. 次の setspn コマンドを実行します。

   注意：各ホストヘッダは、完全修飾ドメイン名を使用するか、1 部構成名を使用することで参照することができます。たとえば、最初のホストヘッダを wf-kerb1.ibi.com (完全修飾ドメイン名) で参照することも、wf-kerb1 (1 部構成名) で参照することもできます。その結果、この手順の setspn コマンドを実行する際は、4 つのエントリになります。

   a. 次のように実行します。

      ```
      setspn -A HTTP/wf-kerb1.ibi.com ibi¥http_wf-kerb
      ```

      出力結果は次のとおりです。

      ```
      Registering ServicePrincipalNames for CN=http_wf-
      kerb,OU=USERS,OU=DEVELOPMENT,
      O=BIPG,OU=COR,DC=ibi,DC=com
             HTTP/wf-kerb1.ibi.com
      Updated object
      ```

   b. 次のように実行します。

      ```
      setspn -A HTTP/wf-kerb1 ibi¥http_wf-kerb
      ```

      出力結果は次のとおりです。

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
       HTTP/wf-kerb1
Updated object
```

c. 次のように実行します。

```
setspn -A HTTP/wf-kerb2.ibi.com ibi¥http_wf-kerb
```

出力結果は次のとおりです。

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
       HTTP/wf-kerb2.ibi.com
Updated object
```

d. 次のように実行します。

```
setspn -A HTTP/wf-kerb2 ibi¥http_wf-kerb
```

出力結果は次のとおりです。

```
Registering ServicePrincipalNames for CN=http_wf-
kerb,OU=USERS,OU=DEVELOPMENT,
O=BIPG,OU=COR,DC=ibi,DC=com
       HTTP/wf-kerb2
Updated object
```

Kerberos 制約付き委任の WebFOCUS Reporting Server 構成要件

Kerberos 事前認証で制約なしの委任を使用する場合は、このセクションを参照する必要はありません。この構成は、制約なしの委任には関係しません。

- Kerberos 事前認証で制約付き委任を使用する場合は、接続タイプとして Kerberos を指定し、オペレーティングシステムセキュリティで実行するよう WebFOCUS Reporting Server を構成する必要があります。
- WebFOCUS Reporting Server が Windows オペレーティングシステムで実行される場合、オペレーティングシステムセキュリティで実行するよう Reporting Server を構成する必要があります。
- WebFOCUS Reporting Server が UNIX または Linux で実行される場合、OPSYS セキュリティプロバイダで実行するよう Reporting Server を構成する必要があります。詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

TIBCO WebFOCUS Client の構成手順 (Kerberos 認証)

WebFOCUS Client で Kerberos 事前認証を構成するには、次の手順を実行します。

デフォルトゾーン、ポータルゾーン、代替ゾーンで Kerberos 事前認証がサポートされます。ただし、ローカル管理アクセスに代替ゾーンを使用する場合は、Kerberos 事前認証を構成しないでください。これは、WebFOCUS Client とブラウザが同一マシンにインストールされている場合、Kerberos が認証をサポートできないためです。

インストールプロセスで作成された場合、一般に管理ユーザには有効な Kerberos ユーザ ID が割り当てられません。そのため、構成の前半で、既存の管理ユーザを、有効な Kerberos ユーザ ID を割り当てた新しい管理ユーザで置き換えます。その後、WebFOCUS は、Kerberos 事前認証およびその他すべての認証タスクをこの新しい管理ユーザで管理することができます。

管理ユーザおよび Kerberos 事前認証の対象となるすべてのユーザに割り当てる ID は、製品インストールで設定された Kerberos ユーザ ID のフォーマット規則に従う必要があります。デフォルト設定では、WebFOCUS はすべての Kerberos ユーザ ID の名前からドメインを除外します。このデフォルト構成を受容した場合、管理ユーザまたは Kerberos 事前認証の対象となるその他のユーザの ID に名前を割り当てるだけです。ただし、[Kerberos/SPNEGO 認証設定の編集] ダイアログボックスで [DNS サフィックスの除外を有効にする] のチェックをオフにしてこの機能を無効にした場合、ユーザ ID には、ユーザが割り当てられたドメイン名および名前を追加し、所定のフォーマット (User ID@domain.com) に従う必要があります。

Kerberos ユーザ名およびそのフォーマット要件についての詳細は、259 ページの 「 Kerberos を使用した事前認証の制限事項 」 を参照してください。

構成の後半では、次の項目の名前またはパスを指定します。

- サービスプリンシパル名
- KeyTab のパス
- krb5.conf 構成ファイルのパス

これらの各項目は、Kerberos 事前認証のキーコンポーネントの名前またはパスを表し、すべて指定する必要があります。

注意：krb5 構成ファイルの名前は、Windows では krb5.ini 、UNIX では krb5.conf となります。

Kerberos 事前認証をサポートするセキュリティゾーンにこれらの値を割り当てるには、[Kerberos/SPNEGO 認証設定の編集] ダイアログボックスにこれらの値を入力する必要があります。このダイアログボックスは、管理コンソールの [セキュリティ] タブのセキュリティゾーン別の各 [認証] ページにあります。デフォルトセキュリティゾーンの設定は、securitysettings.xml ファイルに保存されます。代替セキュリティゾーンの設定は、securitysettings-zone.xml ファイルに保存されます。ポータルゾーンの設定は、securitysettings-portlet.xml ファイルに保存されます。

手順　Kerberos 事前認証の管理ユーザを作成するには

この手順では、WebFOCUS を内部認証から Kerberos 事前認証に変換後、デフォルト設定の管理者を置換する管理ユーザのアカウントを作成します。

1. 管理者としてログインします。
2. [セキュリティセンター] を開きます。
3. [ユーザ] ウィンドウの [USERS] フォルダを選択し、[新規ユーザ] をクリックします。
4. 次のフォーマットのいずれかを使用して、[ユーザ ID] テキストボックスに有効な Kerberos ユーザの ID を入力します。
   - ❏ Kerberos 認証の構成で、ユーザ ID から自動的にドメインが除外されている場合は、ユーザ ID のみを入力します。
   - ❏ Kerberos 認証で、ユーザ ID から自動的にドメインが除外されない場合は、管理ユーザのユーザ ID とドメインを「User ID@domain.com」のフォーマットで [名前] テキストボックスに入力します。
5. [作成先グループ] リストから [Administrators] を選択し、[OK] をクリックします。
6. [ユーザ] ウィンドウの [USERS] フォルダ下で、以前に作成された管理ユーザを選択し、[削除] をクリックします。
7. セキュリティセンターから移動します。

手順　TIBCO WebFOCUS Client を構成するには (Kerberos 認証)

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールを開きます。
2. [セキュリティ] タブをクリックします。
3. [セキュリティゾーン] フォルダ下で、更新するセキュリティゾーンのフォルダを展開し、[認証] をクリックします。
4. [Kerberos/SPNEGO 認証] エントリをダブルクリックします。

   または

   [Kerberos/SPNEGO 認証] エントリを右クリックし、[編集] を選択します。
5. [KERBEROS/SPNEGO 認証設定の編集] ダイアログボックスが開きます。
   a. [サービスプリンシパル名] テキストボックスに Kerberos サービスプリンシパル名を入力します。

      たとえば、「HTTP/wf-kerb.ibi.com」と入力します。
   b. [KeyTab のパス] テキストボックスに keytab ファイルのパスを入力します。

      このファイルは、config ディレクトリに保存することをお勧めします。

      以下はその例です。

      ```
      drive:/ibi/WebFOCUS82/config/http_wfkerb.keytab
      ```

      説明

      `drive`
      WebFOCUS アプリケーションをホストするドライブを表す文字です。
   c. [krb5.conf 構成ファイルのパス] テキストボックスに、krb5 構成ファイルのパスを入力します。

      このファイルは、config ディレクトリに保存することをお勧めします。

      以下はその例です。

      ```
      drive:/ibi/WebFOCUS82/config/krb5configfilename
      ```

      説明

      `drive`
      WebFOCUS アプリケーションをホストするドライブを表す文字です。

`krb5configfilename`
Windows では krb5.ini、UNIX では krb5.conf です。

注意：これらの値の入力はすべて必須です。上記の例では、各属性の一般的な値が示されています。組織で異なる Kerberos サービスプロバイダ名を使用する場合、またはその他のコンポーネントを異なるパスに格納している場合は、上記の手順で呼び出された名前やパスでなく、それらの名前やパスをテキストボックスに入力してください。

d. [DNS サフィックスの除外を有効にする] および [FORM 認証からのフォールバックを有効にする] のチェックはオンのままにします (デフォルト設定を受容)。

2 つ目の設定のチェックをオンにすると、Kerberos 認証に失敗した場合の補助的な認証方法として、このセキュリティゾーンで [フォームベース認証] も有効になります。

e. [OK] をクリックします。

6. [Kerberos/SPNEGO 認証] エントリを右クリックし、[有効にする] を選択します。

   または

   [Kerberos/SPNEGO 認証] エントリをクリック後、[アクション] セクションで [有効にする] を選択します。

7. [アクション] セクションで [保存] をクリックします。
8. 確認メッセージで [OK] をクリックします。
9. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
10. 現在のセッションからログアウトします。
11. WebFOCUS Reporting Server を停止し、再起動します。
12. 管理者としてログインし、構成をテストします。

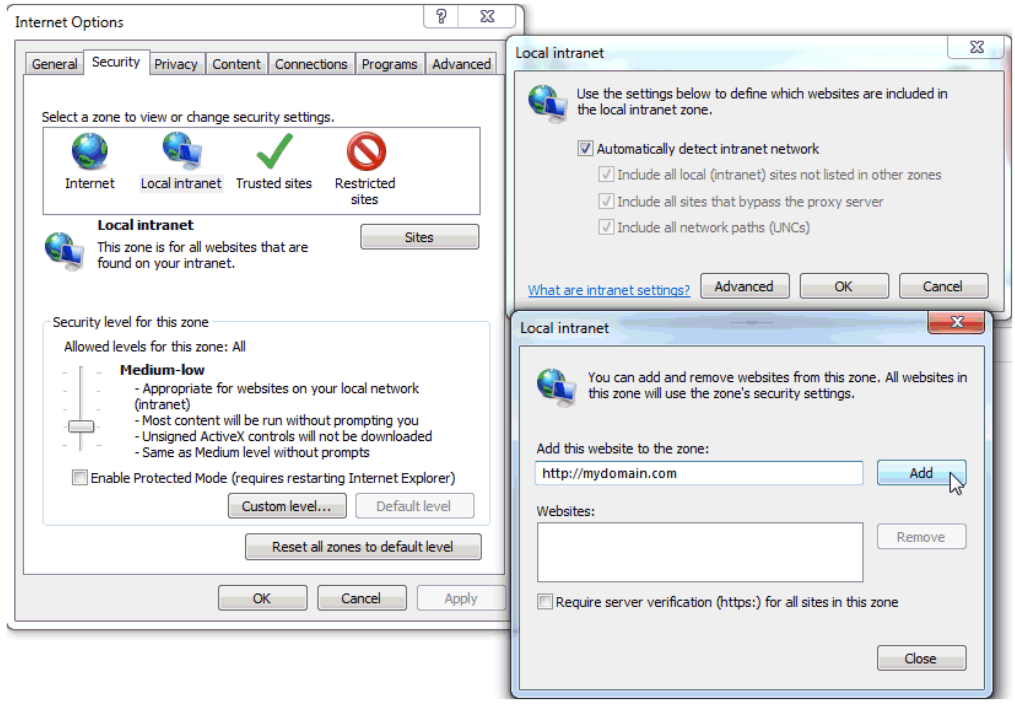
Web ブラウザの構成 (Kerberos 認証)

SSO 機能には、Windows 2000 の機能レベル以上での Active Directory ドメインが必要です。次のブラウザがサポートされます。

- Microsoft Internet Explorer 10 以降
- Google Chrome 53 (以前のバージョンでも動作可能)
- Microsoft Edge 44 以降
- Mozilla Firefox 49 以降 (以前のバージョンでも動作可能)

手順　Internet Explorer を構成するには (Kerberos 認証)

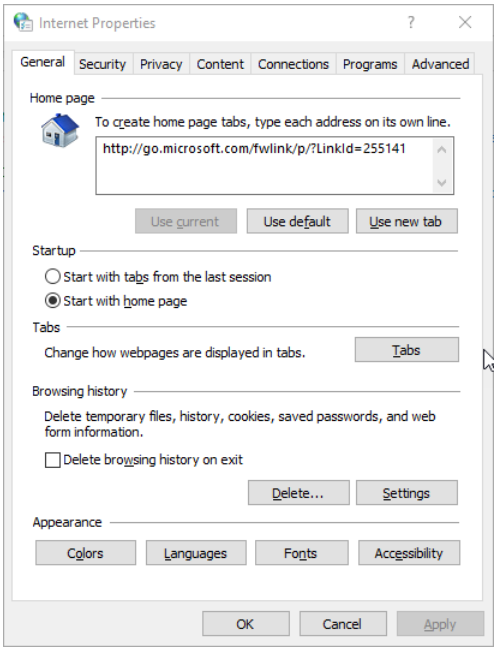
1. Internet Explorer のブラウザメニューを開いて [ツール] をクリックし、[インターネットオプション] を選択します。
2. [セキュリティ] タブで、[ローカルイントラネット] ゾーンを選択し、[サイト] をクリックします。
3. [詳細設定] をクリックします。
4. DNS 内のすべてのホスト名をローカルイントラネットの一部と見なす場合は、ワイルドカードを入力します。または、下図のように、WebFOCUS を実行するマシン名のみを入力し、[追加] をクリックします。



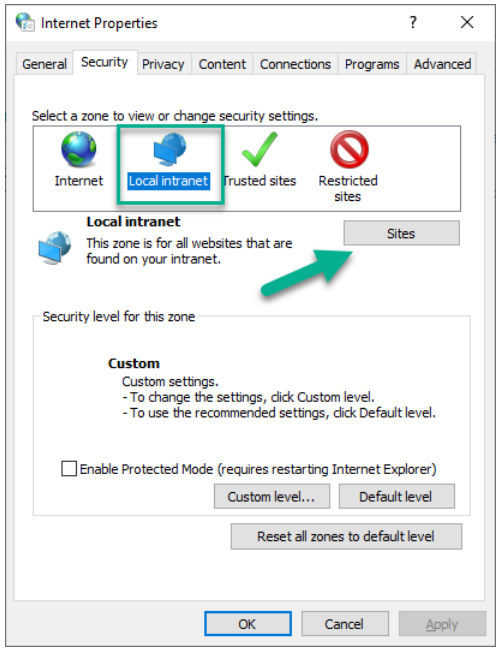
5. [閉じる]、[OK] を順にクリックします。[インターネットオプション] ダイアログボックスで、再度 [OK] をクリックして変更を保存します。
6. [インターネットオプション] ダイアログボックスを再度開き、[詳細設定] タブをクリックします。[セキュリティ] セクションまで下方向へスクロールし、[統合 Windows 認証を使用する] のチェックがオンになっていることを確認します。

手順　Microsoft Edge を構成するには (Kerberos 認証)

1. Windows の検索ボックスに「インターネットオプション」と入力し、下図のように、[インターネットのプロパティ] ダイアログボックスを開きます。

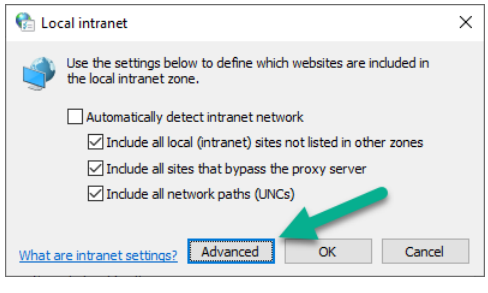


2. 下図のように、[セキュリティ] タブを選択し、[ローカルイントラネット] を選択し、[サイト] ボタンをクリックします。



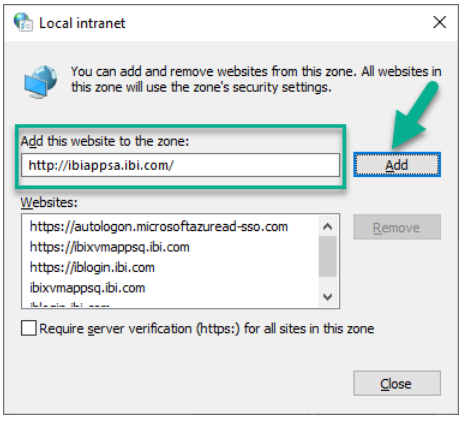
[ローカルイントラネット] ダイアログボックスが開きます。

3. 下図のように、[詳細設定] を選択します。



2 つ目の [ローカルイントラネット] ダイアログボックスが開き、詳細設定が表示されます。

4. DNS 内のすべてのホスト名をローカルイントラネットの一部と見なす場合は、ワイルドカードを入力します。または、下図のように、WebFOCUS を実行するマシン名のみを [この Web サイトをゾーンに追加する] テキストボックスに入力し、[追加] をクリックします。



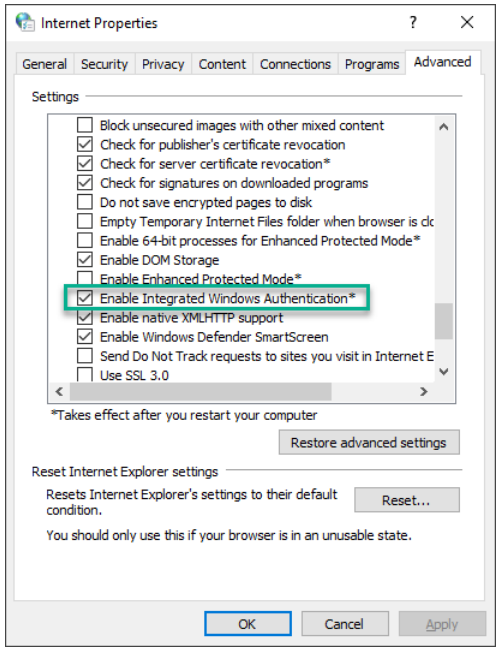
   リストに追加する必要がある Web サイトごとに、この手順を繰り返し実行します。

5. 許可する Web サイトのリストの完成後、[閉じる] をクリックして、詳細設定を含む [ローカルイントラネット] ダイアログボックスを閉じ、[OK] をクリックして 1 つ目の [ローカルイントラネット] ダイアログボックスを閉じます。

6. [インターネットのプロパティ] ダイアログボックスで [OK] を選択してダイアログボックスを閉じ、変更を保存します。

7. [インターネットのプロパティ] ダイアログボックスを再度開き、[詳細設定] タブをクリックします。

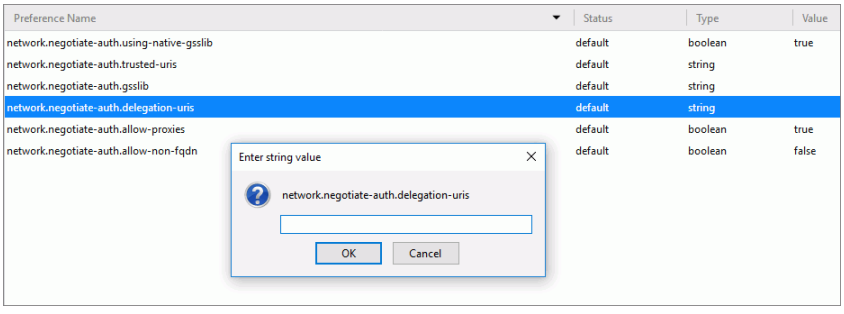
8. 下図のように、[セキュリティ] セクションまで下方向へスクロールし、[統合 Windows 認証を使用する] のチェックがオンになっていることを確認します。



9. このチェックボックスが選択されていることを確認後、[OK] を選択して [インターネットのプロパティ] ダイアログボックスを閉じます。

手順　Mozilla Firefox を構成するには (Kerberos 認証)

1. Mozilla Firefox のアドレスバーに「about:config」と入力し、Enter キーを押します。
2. 「動作保証対象外になります」という警告メッセージが表示された場合は、「危険性を承知の上で使用する」をクリックします。
3. [検索] テキストボックスに「network.negotiate」と入力し、2 つの信頼設定を特定します。これらの 2 つの設定にドメインを追加します。
4. 下図のように、[network.negotiate-auth.delegation-uris] エントリをダブルクリックします。



5. ドメイン情報を追加し、[OK] をクリックします。
6. [network.negotiate-auth.trusted-uris] エントリをダブルクリックし、WebFOCUS Reporting Server のドメイン情報を追加した後、[OK] をクリックします。

Google Chrome の構成 (Kerberos 認証)

Google Chrome で Kerberos 認証を使用するには、Google が提供するセキュリティポリシーテンプレートを管理者がダウンロードし、インストールする必要があります。

Windows で稼働するマシンでホストされるブラウザの場合、セキュリティポリシーテンプレートにより次の 2 つの設定がレジストリに追加されます。

- **AuthServerWhitelist**　統合認証に使用するサーバをホワイトリストで指定します。WebFOCUS 構成で統合認証用に含めるサーバの名前およびドメインをこのレジストリ値に割り当てます。たとえば、「webfocus.ibi.com」と指定します。複数のサーバ名を含める場合は、サーバ名をカンマ (,) で区切ります。ワイルドカード文字 (*) を使用することもできます。
- **AuthNegotiateDelegateWhitelist**　Google Chrome が認証タスクを委任することのできるサーバを指定します。認証タスクをサポートするサーバの名前とドメインをこのレジストリ値に割り当てます。たとえば、「webfocus.ibi.com」と指定します。複数のサーバ名を含める場合は、サーバ名をカンマ (,) で区切ります。ワイルドカード文字 (*) を使用することもできます。

  この値にデータを割り当てない場合、Chrome は、イントラネットサーバからの統合認証リクエストのみに応答し、インターネットサーバからのリクエストは無視します。

このセキュリティポリシーテンプレートは、Apple macOS または Linux で稼働するマシンでホストされるブラウザにも同様の影響を与えます。セキュリティポリシーテンプレートのダウンロードおよび Apple macOS または Linux での展開についての詳細は、https://www.chromium.org/administrators/policy-templates を参照してください。

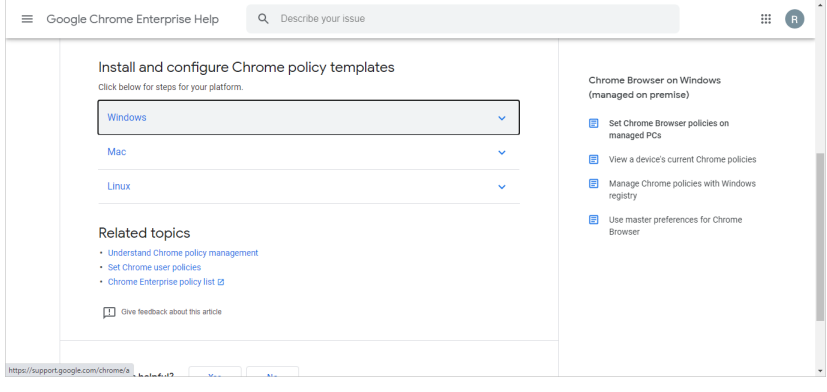
Windows で Kerberos 認証をサポートするためには、次の 3 つの手順で Google Chrome の構成を行います。

1. Google Chrome の Web サイトから適切なセキュリティテンプレートまたはバンドルをダウンロードします。
2. セキュリティテンプレートまたはポリシーを、WebFOCUS へのアクセスに使用する Google Chrome ブラウザをホストするマシンにインストールします。
3. Kerberos 認証で使用可能なすべてのサーバの名前および URL を、Windows レジストリに保持されたホワイトリストにすべて追加します。

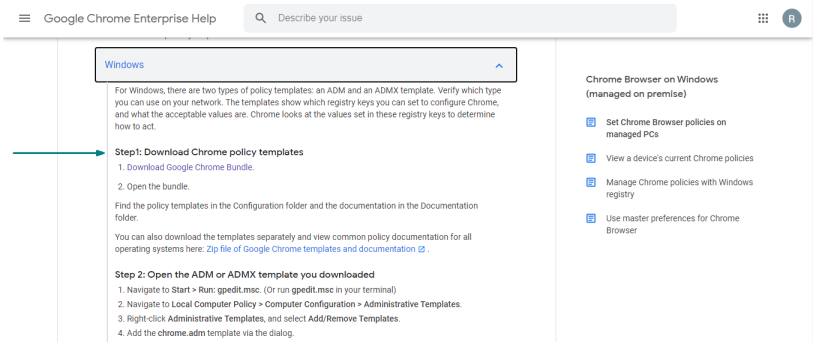
手順 Google Chrome (Kerberos 認証) のセキュリティポリシーテンプレートをダウンロードするには

WebFOCUS への接続に Google Chrome ブラウザを使用する各ユーザは、次のことを行います。

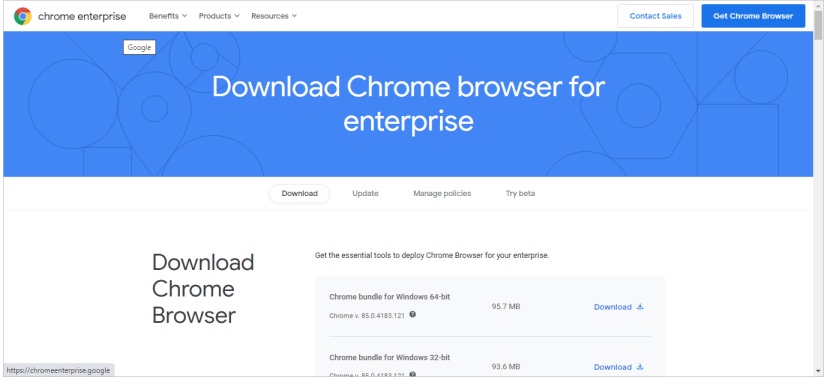
1. Google Chrome ブラウザを起動し、[Google Chrome Enterprise ヘルプ] サイトの [管理対象パソコンに Chrome ブラウザのポリシーを設定する] ページ (https://support.google.com/chrome/a/answer/187202?hl=en) に移動します。
2. 下図のように、[Chrome ポリシーテンプレートのインストールと設定] セクション見出しまで下方向へスクロールし、Google Chrome ブラウザをホストするデバイスのオペレーティングシステムに合った中間見出しを特定します。



3. [Google Chrome バンドルをダウンロードします] リンクをクリックし、Chrome バンドルをダウンロードします。下図のように、この手順は、[Windows] 中間見出し下のステップ 1 に記載されています。



4. 下図のように、使用するオペレーティングシステムをサポートする Google Chrome バンドル横のダウンロードリンクを選択し、ブラウザのプロンプトに従ってダウンロードを完了します。



手順 Windows で Google Chrome (Kerberos 認証) のセキュリティポリシーテンプレートをインストールするには

1. Google Chrome のサポートサイトからダウンロードした Chrome バンドル ZIP ファイルをローカルマシンに保存し、格納されたファイルを抽出します。
2. 抽出ファイルから次の場所にナビゲートします。

   `drive:¥path¥Configuration¥adm¥language¥chrome.adm`

説明

`drive:¥path¥`
: ZIP ファイルの抽出先のドライブ名とパスです。

`language`
: Google Chrome ブラウザのホストマシンが使用する言語のコード名です。

以下はその例です。

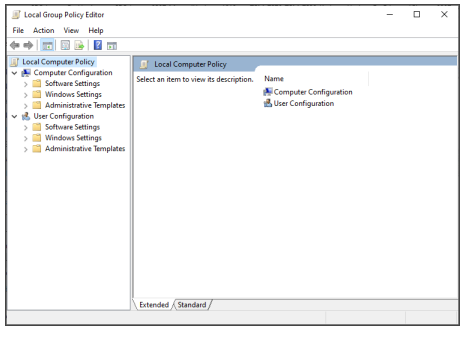
```
C:¥temp¥KerberosUpdatesForEdgeandChrome8207¥Configuration¥adm¥en-US
```

3. 次のいずれかの手順を実行し、ローカルグループポリシーエディターを起動します。

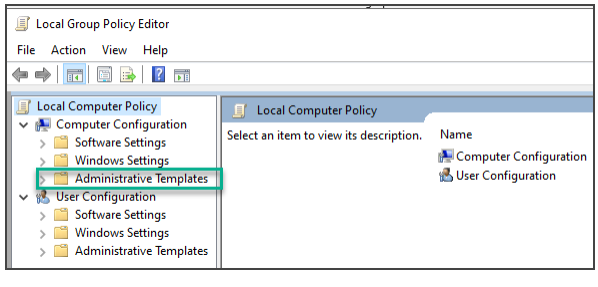
   ブラウザをホストするマシンの検索トレイに「グループポリシーの編集」と入力してアプリケーションパネルを開き、[開く] を選択してローカルグループポリシーエディターを表示します。

   または

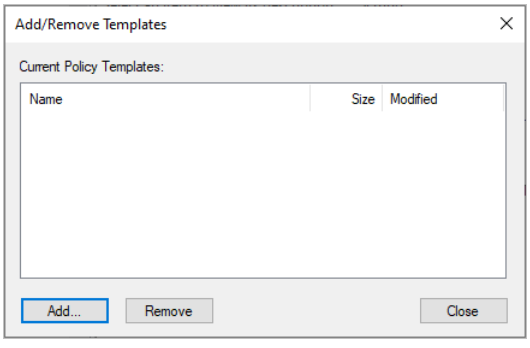
   [スタート] メニューから [設定] を選択し、[設定の検索] テキストボックスに「gpedit.msc」と入力します。下図のように、[検索結果] 見出し下で [グループポリシーの編集] を選択し、[設定] ウィンドウを閉じてローカルグループポリシーエディターを表示します。



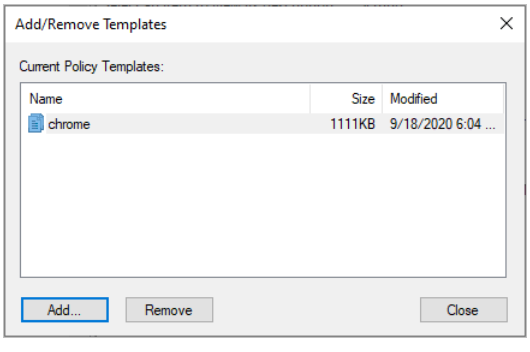
4. 下図のように、ローカルグループポリシーエディターで、[ローカルコンピューターポリシー]、[コンピューターの構成]、[管理用テンプレート] を順に展開します。



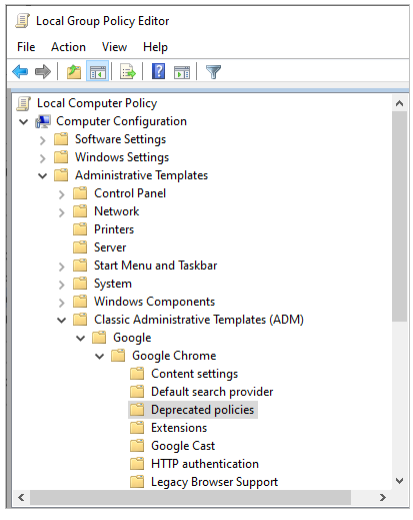
5. [管理用テンプレート] を右クリックし、コンテキストメニューから [テンプレートの追加と削除] を選択して、[テンプレートの追加と削除] ダイアログボックスを開きます。



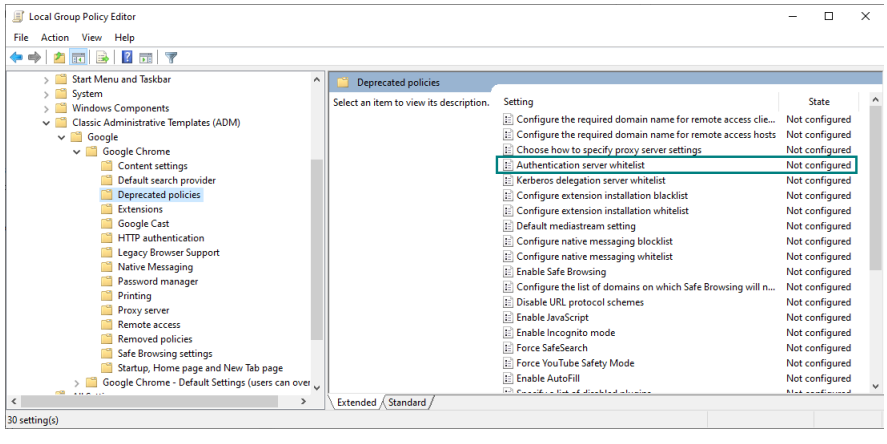
6. [追加] を選択し、chrome.adm ファイルを保存したネットワークパスに移動します。
7. 下図のように、ファイルをハイライト表示し、[閉じる] を選択して [テンプレートの追加と削除] ダイアログボックスを閉じ、[従来の管理用テンプレート] (ADM) フォルダをローカルグループポリシーエディターに追加します。



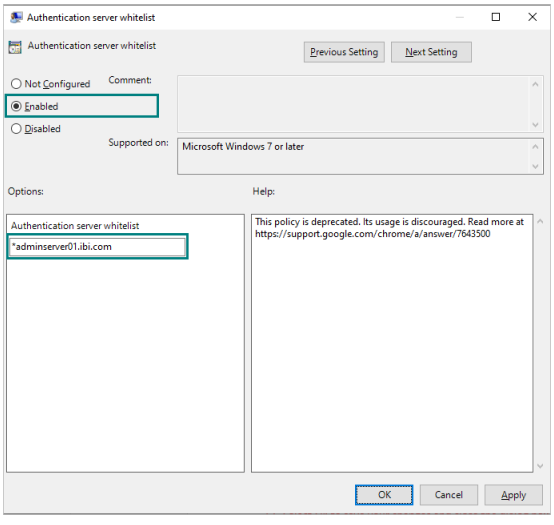
8. 下図のように、ローカルグループポリシーエディターのナビゲーションツリーの [コンピューターの構成] ノード下で、[管理用テンプレート]、[従来の管理用テンプレート (ADM)]、[Google]、[Google Chrome]、[非推奨ポリシー] を順に展開します。



9. 下図のように、[非推奨ポリシー] フォルダで、[認証サーバーのホワイトリスト] 設定をダブルクリックします。



10. [認証サーバーのホワイトリスト] ダイアログボックスで [有効] を選択し、[オプション] セクションに、統合認証用ホワイトリストに表示されたサーバの名前を入力します。



通常、サーバ名には「`serverdomain`.com」のフォーマットを使用します。

説明

`server`
WebFOCUS 構成で統合認証用のホワイトリストに追加するサーバの名前です。

`domain`
WebFOCUS 構成で統合認証用のホワイトリストに追加するドメインの名前です。

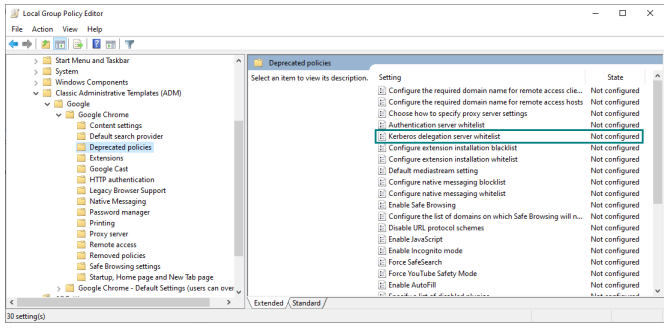
以下はその例です。

```
adminserver.ibi.com
```

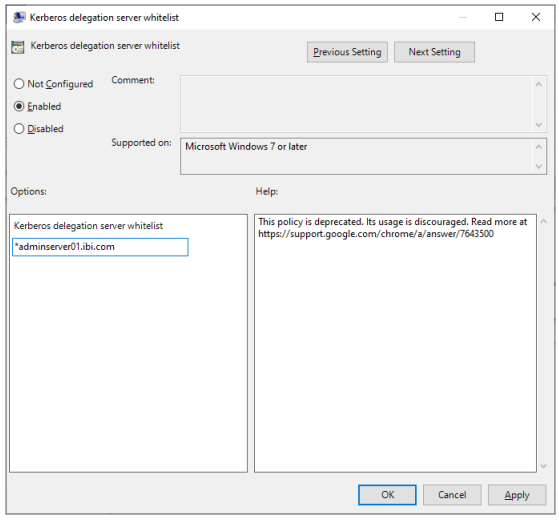
サーバ名のフォーマットでは、ワイルドカード文字が使用できます。複数のサーバ名を入力する必要がある場合は、区切り文字としてカンマ (,) を使用します。

11. [OK] を選択して変更を保存し、ダイアログボックスを閉じます。

12. 下図のように、[非推奨ポリシー] フォルダで、[Kerberos 委任サーバーのホワイトリスト] 設定を選択します。



13. 下図のように、[Kerberos 委任サーバーのホワイトリスト] ダイアログボックスで [有効] を選択し、[オプション] セクションに、許可するサーバの名前 (ワイルドカード文字を受容) を入力します。



通常、サーバ名には「`serverdomain`.com」のフォーマットを使用します。

説明

`server`
: Google Chrome が認証タスクを委任することのできるサーバの名前です (ホワイトリストに登録されているサーバ)。

`domain`
: Google Chrome が認証タスクを委任することのできるドメインの名前です (ホワイトリストに登録されているドメイン)。

以下はその例です。

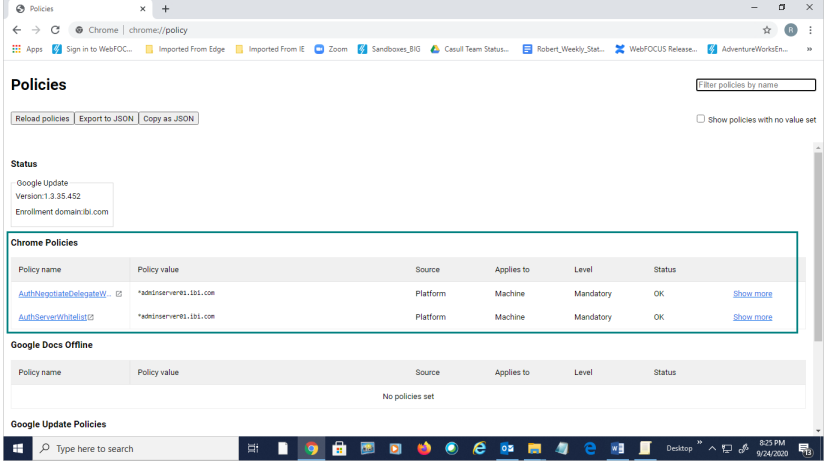
```
adminserver.ibi.com
```

サーバ名のフォーマットでは、ワイルドカード文字が使用できます。複数のサーバ名を入力する必要がある場合は、区切り文字としてカンマ (,) を使用します。

14. [OK] を選択して変更を保存し、ダイアログボックスを閉じます。
15. [ファイル]、[終了] を順に選択して、ローカルグループポリシーエディターを閉じます。
16. ユーザのブラウザをホストするマシンを再起動します。

手順　Google Chrome ブラウザの Kerberos 認証対応を確認するには

1. Chrome ブラウザを開き、アドレスバーに「chrome://policy」と入力し、ポリシーページを開きます。
2. 下図のように、リストを見て、[認証サーバーのホワイトリスト] ポリシーおよび [Kerberos 委任サーバーのホワイトリスト] ポリシーが実装されていることを確認します。



3. 両方のポリシーエントリで、Kerberos 認証でアクセス可能にするすべての URL が[Policy value] 列に表示されていることを確認します。
4. 両方のポリシーが存在し、Kerberos 認証でアクセス可能な URL がすべてリストに表示されている場合は、ブラウザを閉じます。
5. 1 つまたは両方のポリシーが存在しない場合および 1 つまたは複数の URL が欠落している場合は、ブラウザを閉じ、前の項の説明に従ってポリシーを編集するか再度インストールします。

手順 **WebFOCUS 構成をテストするには (Kerberos 認証)**

1. Kerberos シングルサインオン構成をテストするには、構成済みのブラウザのいずれかで BI Portal にアクセスします。

   構文は次のとおりです。

   ```
   http://server.url.domain:port/context
   ```

   Kerberos が正しく構成され、BI Portal にユーザ ID が追加されている場合は、Kerberos 認証情報により BI Portal にログインした状態になります。

2. Kerberos が構成されたノードを使用してレポートを実行することで、WebFOCUS Client が WebFOCUS Reporting Server に認証を委任できることを確認します。

   WebFOCUS Reporting Server の edaprint ログファイルには、「request by cmrpip0000xx for Kerberos connect to agent」が記録され、Windows ログイン ID が UPN フォーマットで示されます。

ReportCaster サポートの構成 (Kerberos 認証)

Kerberos 認証では、WebFOCUS Reporting Server とユーザのブラウザセッション間での同期接続が必要ですが、ReportCaster はスケジュール済みレポートの実行時にブラウザセッションを使用しません。そのため、ReportCaster は、レポートを有効にするためにユーザ ID およびパスワードを Kerberos に提供する必要があります。

Distribution Server の構成インターフェースで、ReportCaster の通信先として設定されているデータサーバをそれぞれ個別に構成する必要があります。[セキュリティタイプ] を [ユーザ] に設定して、エンドユーザに対してユーザ ID およびパスワードの入力がノードごとに 1 回要求されるようにします。

別の方法として、[セキュリティタイプ] を [静的] に設定し、その WebFOCUS Reporting Server でのすべてのスケジュールに使用されるユーザ ID およびパスワードを指定します。

手順 **ReportCaster データサーバを構成するには (Kerberos 認証)**

1. ReportCaster コンソールで [構成] タブをクリックし、[データサーバ] フォルダを展開します。
2. 構成するノードを選択し、次の設定を変更します。
   a. [セキュリティタイプ] ドロップダウンリストから、[ユーザ] または [静的] を選択します。
   b. [静的] を選択した場合は、[ユーザ] テキストボックス右横のボタンをクリックします。

c. [ユーザ] ダイアログボックスで、ユーザ ID およびパスワードを入力し、[OK] をクリックします。

d. [保存] ボタンをクリックして、変更を保存します。

大規模チケットサポートの構成 (Kerberos 認証)

Kerberos の Microsoft Windows 実装では、Windows グループ識別子が各ユーザの Kerberos チケット内に配置されます。その結果、ユーザが多数のグループに属する場合、そのユーザのチケットサイズが増大します。Kerberos チケットは HTTP ヘッダ内で転送されますが、チケットサイズが増大すると、いくつかの技術的問題を引き起こします。ユーザが 100 を超えるグループに属する場合は、次の特別な構成作業の一部またはすべてを実行する必要があります。

- Tomcat Server の HTTP ヘッダバッファサイズを増加します。これを行うには、maxHttpHeaderSize="*xx*" 設定を追加します。ここで、*xx* は 4096 の倍数で表したバイト数です。この設定は、必要に応じて 65,536 バイトにまで増加します。Tomcat の server.xml ファイルで、使用するコネクタブロックに応じて、8080 または 8009 ブロックにこの設定を追加します。
- 多数のグループに属するユーザのアクセス先ワークステーションごとに、次の作業を実行します。
  - Kerberos 認証に、UDP ではなく、TCP を使用するよう Windows を構成します。これを行うには、レジストリで MaxPacketSize を 1 に設定します。詳細は、Microsoft Knowledge Base Article 244474 (https://support.microsoft.com/en-us/help/244474/how-to-force-kerberos-to-use-tcp-instead-of-udp-in-windows) を参照してください。
  - MaxTokenSize を 65535 に設定します。
- さらに、ドメインコントローラの MaxTokenSize を設定する必要があります。

複数ドメイン環境での Kerberos 実装の WebFOCUS 設定

ここでは、複数ドメインまたは複数サブドメイン環境で Kerberos が正しく動作するために必要な追加手順について説明します。

たとえば、ユーザが SUBA.MYDOMAIN.COM、SUBB.MYDOMAIN.COM、MYDOMAIN.COM のメンバーで、これらのユーザすべてが Kerberos 環境にアクセスする必要がある場合は、この手順に従う必要があります。

複数ドメイン環境で Kerberos が正しく動作するために必要な追加の構成設定を行うには、「krb5.ini」という Kerberos 構成ファイルを作成する必要があります。このファイルには、複数のドメインを使用する際に Kerberos が正しく動作するために必要な追加情報がすべて格納されます。

Java の一部のバージョンでは、krb5.ini 構成ファイルを使用した場合でも複数のドメインが正しく動作しないという不具合があります。その場合は、現在の Java を新しいバージョンに更新する必要があります。Java の不具合についての詳細は、次の Java バグレポートを参照してください。

http://bugs.sun.com/view_bug.do?bug_id=6670362

手順　Kerberos 設定を構成する krb5.ini ファイルを作成するには

1. 新しいテキストファイルを作成し、「krb5.ini」という名前を付けます。

   このファイルの参照先は後から明示的に指定できるため、ファイルシステム上の任意の場所で作成することができます。この例では、次の場所でファイルを作成します。

   ```
   drive:¥ibi¥WebFOCUS82¥config¥krb5.ini
   ```

2. krb5.ini ファイルの先頭に、[libdefaults] セクションのコード行を以下のように追加します。

   この例の最終行の default_realm 名 MYDOMAIN.COM を、マシン上で WebFOCUS Client が参加しているドメインの完全修飾 DNS 名に置き換えます。

   default_realm 名は、大文字で入力します。この名前には、大文字と小文字の区別があります。

   ```
   [libdefaults]
       ticket_lifetime = 600
       default_tgt_enctypes = rc4-hmac
       default_tgs_enctypes = rc4-hmac
       default_checksum     = rsa-md5
       forwardable = true
       default_realm = MYDOMAIN.COM
   ```

3. [libdefaults] セクションの後に、[realms] セクションのコード行を以下のように追加します。次の例のように、使用するすべてのドメインおよびサブドメインのエントリを追加します。

   ドメインおよびサブドメインがドメインコントローラを共有している場合は、ここで [realms] セクションを作成した後、次の [domain_realm] セクションでその関係を指定します。[domain_realm] セクションの説明は、手順 4 に記載されています。

```
[realms]
MYDOMAIN.COM = {
   kdc = dc1.mydomain.com:88
   kdc = dc2.mydomain.com:88
   kdc = dc3.mydomain.com:88
   default_domain = mydomain.com
}
SUBA.MYDOMAIN.COM = {
   kdc = dc1.suba.mydomain.com:88
   kdc = dc2.suba.mydomain.com:88
   default_domain = suba.ibi.com
}
SUBB.MYDOMAIN.COM = {
   kdc = dc1.subb.mydomain.com:88
   kdc = dc2.subb.mydomain.com:88
   default_domain = subb.ibi.com
}
```

[libdefaults] セクションと同様に、[realms] セクションの値でも大文字と小文字が区別されます。たとえば、この例の先頭ブロックの MYDOMAIN.COM のように、最初の参照名は大文字にし、default_domain の値は小文字にする必要があります。

kdc の各エントリは、それぞれ対応するドメインのドメインコントローラの DNS 名を表す必要があります。ドメインごとに必要な kdc エントリは 1 つですが、冗長性を確保するために複数の kdc エントリを使用することができます。

4. この手順は、必要に応じて実行します。追加のドメインまたはホスト名を特定の realm にマッピングするには、オプションの [domain_realm] セクションで次のコード行を追加します。

   各ドメインを同一名の realm にマッピングしますが、realm 名は大文字で指定します。結果的に、次のエントリが冗長になります。

   ```
   [domain_realm]
      .suba.mydomain.com = SUBA.MYDOMAIN.COM
      .subb.mydomain.com = SUBB.MYDOMAIN.COM
      .mydomain.com = MYDOMAIN.COM
   ```

   [domain_realm] セクションについての詳細は、次の Web サイトで MIT Kerberos の仕様を参照してください。

   http://web.mit.edu/kerberos/krb5-1.4/krb5-1.4.1/doc/krb5-admin/domain_realm.html

5. この手順は、必要に応じて実行します。サイトで適用可能な場合は、オプションの [capaths] セクションで次のコード行を追加します。

   [capaths] セクションは、親ドメインが子ドメインすべてと一方向の信頼関係を持たない環境、または複数ドメイン階層が使用されている環境でのみ必要です。

これらの状況では、Kerberos プロトコルが、一方のドメインのユーザを他方のドメインのリソースに対して認証する方法を特定することができません。そのため、Kerberos がどのパスを経由してユーザを認証するかを特定できるよう、認証に必要な関係をマッピングする必要があります。次の信頼関係が適用されます。

- SUBA.MYDOMAIN.COM ドメインは、SUBB.MYDOMAIN.COM を一方向で信頼します。
- SUBB.MYDOMAIN.COM ドメインは、MYDOMAIN.COM を一方向で信頼します。
- SUBA.MYDOMAIN.COM ドメインは、MYDOMAIN.COM を信頼しません。

この例では、Kerberos が、SUBA.MYDOMAIN.COM のすべてのユーザを、SUBB.MYDOMAIN.COM のすべてのリソースに対して直接認証することができます。SUBA.MYDOMAIN.COM のユーザを MYDOMAIN.COM で認証するには、そのユーザを SUBB.MYDOMAIN.COM 経由で認証する必要があります。これは、SUBA.MYDOMAIN.COM が、MYDOMAIN.COM との間で直接的な信頼関係を持たないためです。

```
[capaths]
SUBA.MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
SUBB.MYDOMAIN.COM {
SUBA.MYDOMAIN.COM = .
MYDOMAIN.COM = .
}
MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
SUBA.MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
```

最初のブロックは、SUBA.MYDOMAIN.COM のユーザを認証するための情報です。ピリオド (.) で示されているとおり、Kerberos は SUBA.MYDOMAIN.COM のユーザを SUBB.MYDOMAIN.COM に対して直接認証することができます。SUBA.MYDOMAIN.COM のユーザを MYDOMAIN.COM に対して認証するには、Kerberos が SUBB.MYDOMAIN.COM 経由で認証する必要があります。これは、コードに「MYDOMAIN.COM =SUBB.MYDOMAIN.COM」と記述されているためです。

2 つ目のブロックは、SUBB.MYDOMAIN.COM のユーザを認証するための情報です。Kerberos は SUBB.MYDOMAIN.COM のユーザを、SUBA.MYDOMAIN.COM と MYDOMAIN.COM の両方に対して認証できるため、両方の列にピリオド (.) が指定されています。

3 つ目のブロックは、MYDOMAIN.COM のユーザを認証するための情報です。ピリオド (.) で示されているとおり、Kerberos は MYDOMAIN.COM のユーザを SUBB.MYDOMAIN.COM のリソースに対して直接認証することができます。Kerberos が SUBA.MYDOMAIN.COM のユーザを認証するには、最初に SUBB.MYDOMAIN.COM を経由する必要があります。

Kerberos プロトコルで [capaths] セクションを使用する方法についての詳細は、MIT の次の説明を参照してください。

http://web.mit.edu/kerberos/krb5-1.5/krb5-1.5.4/doc/krb5-admin/capaths.html

すべての手順が完了すると、krb5.ini ファイルは次のようになります。

```
[libdefaults]
   ticket_lifetime = 600
   default_tgt_enctypes = rc4-hmac
   default_tgs_enctypes = rc4-hmac
   default_checksum = rsa-md5
   forwardable = true
   default_realm = MYDOMAIN.COM
[realms]
MYDOMAIN.COM = {
   kdc = dc1.mydomain.com:88
   kdc = dc2.mydomain.com:88
   kdc = dc3.mydomain.com:88
   default_domain = mydomain.com
}
SUBA.MYDOMAIN.COM = {
   kdc = dc1.suba.mydomain.com:88
   kdc = dc2.suba.mydomain.com:88
   default_domain = suba.ibi.com
}
SUBB.MYDOMAIN.COM = {
   kdc = dc1.subb.mydomain.com:88
   kdc = dc2.subb.mydomain.com:88
   default_domain = subb.ibi.com
}
[domain_realm]
   .suba.mydomain.com = SUBA.MYDOMAIN.COM
   .subb.mydomain.com = SUBB.MYDOMAIN.COM
   .mydomain.com = MYDOMAIN.COM
```

```
[capaths]
SUBA.MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
SUBB.MYDOMAIN.COM {
SUBA.MYDOMAIN.COM = .
MYDOMAIN.COM = .
}
MYDOMAIN.COM {
SUBB.MYDOMAIN.COM = .
SUBA.MYDOMAIN.COM = SUBB.MYDOMAIN.COM
}
```

手順　Apache Tomcat で krb5.ini のパスを指定するには

通常、WebFOCUS Kerberos 構成には krb5.ini ファイルが必要です。以下の Java オプションを使用して、このファイルのパスを指定する必要があります。次の手順を実行して、Tomcat で -Djava.security.krb5.conf オプションを指定することができます。

1. Tomcat の bin ディレクトリに移動します。

   通常、bin ディレクトリは次の場所にあります。

   ```
   drive:¥ibi¥tomcat¥bin¥
   ```

2. tomcat8WFw.exe をダブルクリックして、[Apache Tomcat Properties] ダイアログボックスを開きます。
3. [Java] タブを選択し、Java オプションのリストの末尾に次のエントリを追加します。

   ```
   -Djava.security.krb5.conf=drive:¥ibi¥WebFOCUS82¥config¥krb5.ini
   ```

   krb5.ini ファイルの格納先として別のディレクトリを選択した場合は、次の例に示すディレクトリを、そのディレクトリで読み替えてください。
4. [適用] をクリックして、設定を保存します。
5. 設定を有効にするには、Tomcat を停止してから再起動します。

SAML による事前認証の設定

SAML (Security Assertion Markup Language) 認証は、他社製 ID プロバイダに依存し、サービスプロバイダのサービスを要求するユーザの認証をアサートします。プリンシパル (例、WebFOCUS ユーザ) がサービスプロバイダ (例、WebFOCUS) のサービスをリクエストすると、サービスプロバイダがそのリクエストを ID プロバイダに転送します。次に ID プロバイダがプリンシパルを認証し、リクエストを許可します。SAML 事前認証を使用することで、管理者は、ユーザアカウント管理に関する負担をこのタスクを専門に行う ID プロバイダに転換することができます。また、ユーザは、WebFOCUS およびその他のアプリケーションを起動するために、作業セッション中に複数回ログインする必要がなくなります。WebFOCUS では、内部セキュリティおよび認証情報ベース認証の各種要件に対応した、さまざまな ID プロバイダがサポートされます。これらの ID プロバイダの特殊なサポート要件に関する追加情報が必要な場合は、技術サポートに問い合わせてください。

SAML 認証を完全に構成するには、次の操作が必要です。

1. カスタムキーストアを作成します。

   注意：この手順はオプションですが、実行することをお勧めします。

   WebFOCUS に同梱されているデフォルトキーストアを使用して SAML 認証をサポートすることも、カスタムキーストアを作成することもできます。キーストアを SAML 認証サポートのみに限定することも、キーストアを必要とする他のセキュリティ機能 (例、Trusted チケット認証) をサポートするために使用することもできます。カスタムキーストアを作成する場合は、そのキーストアを [キー管理] ダイアログボックスに追加する必要があります。また、[SAML 認証設定の編集] ダイアログボックスで定義する SAML サービスプロバイダメタデータに、キーストアに割り当てる値を追加する必要があります。

2. 代替セキュリティゾーンを有効にします。

   デフォルトセキュリティゾーンで SAML 認証を構成した後でも、管理者は構成タスクや保守管理タスクを実行するために SAML 認証をバイパスする必要があります。代替セキュリティゾーン (デフォルト設定でフォームベース認証が構成済み) を有効にすると、管理者が自身のマシンからログインし、SAML 認証をバイパスして管理者自身を適切に認証することが可能になります。

3. カスタムキーストアを WebFOCUS に割り当てます。

   注意：この手順はオプションですが、実行することをお勧めします。

カスタムキーストアを作成する場合は、[キー管理] ダイアログボックスの [証明書エイリアスとパスワードのマッピング] ボックスにカスタムキーストアを追加し、デフォルトキーストアのパスとパスワードをカスタムキーストアのパスとパスワードに置換して、そのカスタムキーストアを WebFOCUS で使用可能にする必要があります。ただし、デフォルトキーストアを使用する場合は、この操作を省略することができます。デフォルトキーストアは、このダイアログボックスですでに構成されています。

4. SAML サービスプロバイダのメタデータファイルをダウンロードして構成します。

   [SAML 認証設定の編集] ダイアログボックスで SAML サービスプロバイダメタデータにキーストア証明書エイリアスとパスワードを追加します。これらの値および [エンティティ ID] と [エンティティベース URL] を使用してメタデータファイルを生成します。このメタデータファイルにより、SAML 認証をサポートする ID プロバイダに対して、WebFOCUS が信頼されるサービスプロバイダとして識別されます。

5. ID プロバイダメタデータファイルを WebFOCUS にダウンロードして構成します。

   ID プロバイダから提供されたメタデータファイルを WebFOCUS 構成に追加して、WebFOCUS でそのプロバイダを使用したユーザ ID 認証を有効にします。

6. デフォルトセキュリティゾーンで SAML 認証を有効にします。

   WebFOCUS ユーザのデフォルト認証方法として SAML 認証を設定するには、デフォルトセキュリティゾーンでその他すべての認証方法を無効にした上で、SAML 認証を有効にする必要があります。

7. SAML 認証構成を保存します。

   [認証] ページの [保存] リンクをクリックして、[SAML 認証設定の編集] ダイアログボックスで構成した設定を保存します。WebFOCUS からログアウトし、WebFOCUS Reporting Server を再起動して SAML 認証の実装を完了します。

   実稼働環境の主な認証方法として SAML 認証を設定した場合でも、代替セキュリティゾーンを有効にしてフォームベース認証の使用を保持し、フォームベース認証を使用するための構成を残しておくことをお勧めします。フォームベースでログインし、システム管理タスクに継続して代替セキュリティゾーンを使用することができます。

注意

- WebFOCUS は、OASIS 標準に従って、ID プロバイダが開始した SAML 認証リクエスト <AuthnRequest> メッセージに <SubjectConfirmationData>要素が含まれていない場合にそのメッセージを拒否します。また、HTTP 401 未承認エラーを発行し、ターゲットリソースに対する有効な認証情報が欠落しているためにリクエストが適用されなかったことを提示します。<AuthnRequest> メッセージに関する OASIS 標準についての詳細は、https://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf の 18 ページおよび 19 ページを参照してください。
- WebFOCUS は、Spring Security SAML Extension 標準に従って、サービスプロバイダが開始した認証リクエストを処理、検証する場合と同一の方法で、ID プロバイダが開始した認証済みログインリクエスト (非要請応答メッセージまたは IDP 開始 SSO メッセージとも呼ばれる) を処理、検証します。WebFOCUS は、リクエストとともに提供された認証情報を評価し、ID プロバイダによるリクエスト送信者 ID の検証結果に基づいて、プリンシパルにアクセスを許可するか、エラーを返します。<AuthnRequest> メッセージに関する Spring Security SAML Extension 標準についての詳細は、http://docs.spring.io/spring-security-saml/docs/1.0.2.release/reference/pdf/spring-security-saml-reference.pdf の 32 ページを参照してください。

SAML 認証の要件

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

WebFOCUS での SSL 構成などの追加要件を伴う場合があります。SSL 構成で必要な手順についての詳細は、54 ページの 「 TIBCO WebFOCUS での SSL 構成 」 を参照してください。その他の要件についての詳細は、技術サポートに問い合わせてください。

[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの 「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

手順　カスタムキーストアを作成するには

この手順は必要に応じて実行します。デフォルトキーストア (wfKeystore.jks) およびそのキーストア内のデフォルトエイリアスを使用して、SAML 認証処理をサポートすることができます。

- デフォルトキーストアおよびエイリアスを使用する場合は、次の手順を省略します。[キー管理] ダイアログボックスおよび [SAML 認証設定の編集] ダイアログボックスのデフォルト設定を使用します。
- カスタムキーストアおよびエイリアスを使用する場合は、次の手順を実行します。また、[キー管理] ダイアログボックスに新しいキーストアの設定を追加するとともに、[SAML 認証設定の編集] ダイアログボックスのデフォルト設定を、カスタムキーストアの作成に使用する設定に置き換える必要があります。

1. [コマンドプロンプト] ウィンドウを開き、コマンドプロンプトを *drive:*¥ibi¥WebFOCUS82¥config¥was ディレクトリに移動します。
2. 次の例のように、Java keytool コマンドおよび値を入力します。

   ```
   keytool -genkey -alias aliasname -keyalg RSA -keysize 2048 -keypass
   keypass -storepass storepass -validity 3650 -keystore keystorename.jks
   ```

   説明

   aliasname
   　キーストア内のプライベートキーに割り当てる一意のエイリアスです。

   RSA
   　キーストアに割り当てるアルゴリズムです。

   2048
   　キーサイズです。

   keypass
   　プライベートキーエイリアスに割り当てるパスワードです。

   storepass
   　キーストアファイルに割り当てるパスワードです。

   3650
   　キーの有効日数です。

   keystorename.jks
   　キーストアファイルに割り当てる名前です。

   注意：keytool は、通常 Java bin ディレクトリに格納された Java コマンドです。
3. Enter キーを押します。

   コマンドプロンプトに、一連の質問の第 1 問が表示されます。

4. 次の各質問に回答します。
   - What is your first and last name? - 証明書所有者の姓名を入力します。

     たとえば、「John Doe」と入力します。
   - What is the name of your organizational unit? - 証明書所有者の組織の部門名を入力します。

     たとえば、「Technical Content Manager」と入力します。
   - What is the name of your organization? - 証明書所有者の組織名を入力します。

     たとえば、「TIBCO」と入力します。
   - What is the name of your City or Locality? - 証明書所有者の都市名または地域名を入力します。

     たとえば、「New York」と入力します。
   - What is the name of your State or Province? - 証明書所有者の所在地の州名を 2 文字の短縮名で入力します。

     たとえば、「NY」と入力します。
   - What is the two-letter country code for this unit? - 証明書所有者の所在地の国名を 2 文字の短縮名で入力します。

     たとえば、「US」と入力します。
5. コマンドプロンプトに「Is CN=__, OU=__, O=__, L=__, ST=__, C=__ correct?」という質問が表示されます。値を確認し、正しい場合は「y」を入力します。

   たとえば、「Is CN= John Doe, OU= Technical Content Management, O= TIBCO, L= New York, ST= NY, C= US correct?」という質問が表示されます。

   正しくない場合は「n」を入力し、keytool コマンドの手順 2 から再入力します。

   値が正しく入力されると、新しいキーストアが使用可能になります。
6. 次の例のように、keytool コマンドを再入力して新しいキーストアの詳細を確認します。

   ```
   keytool -list -v -keystore keystorename.jks -storepass storepass
   ```

   説明

   keystorename.jks
   キーストアファイルに割り当てる名前です。

   storepass
   キーストアファイルに割り当てるパスワードです。

7. 新しいキーストアファイルが、次のディレクトリに保存されていることを確認します。

   drive:¥ibi¥WebFOCUS82¥config¥was

手順　TIBCO WebFOCUS にカスタムキーストアを割り当てるには

デフォルトキーストア (wfKeystore.jks) およびデフォルトエイリアスを使用して ID プロバイダ用の WebFOCUS 証明書に署名して暗号化することができます。また、ID プロバイダの要件に応じてカスタムキーストアおよびエイリアスに置き換えることもできます。

- ❏ デフォルトキーストアおよびエイリアスを使用する場合は、次の手順を省略し、[キー管理] ダイアログボックスのデフォルト設定を使用します。
- ❏ カスタムキーストアおよびエイリアスを使用する場合は、次の手順を実行し、[キー管理] ダイアログボックスのデフォルト設定を、カスタムキーストアの作成に使用した設定に置き換えます。

1. 管理コンソールの [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、[デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
2. [認証] ページで、[キー管理] をクリックします。
3. [キー管理] ダイアログボックスで、[キーストアファイルのパス] テキストボックスのデフォルト値を受容します。

   このパスは、キーストアを作成した際に、そのキーストアを保存した *drive*:¥ibi¥WebFOCUS82¥config¥was ディレクトリに対応します。
4. [キーストアのパスワード] テキストボックスに、キーストアに割り当てたパスワードを入力します。

   これは、キーストアを作成した際に storepass オプションに割り当てたパスワードです。
5. [追加] をクリックします。
6. [キーストアの証明書エイリアス] テキストボックスに、キーストアに割り当てたエイリアスを入力します。
7. [パスワード] テキストボックスに、キーストアエイリアスに割り当てたパスワードを入力します。
8. [デフォルト証明書エイリアス] のチェックをオンにします。
9. [OK] をクリックします。

   [証明書エイリアスとパスワードのマッピング] ボックスに、新しいキーストアのエントリが表示されます。

10. [OK] をクリックします。

手順　SAML 認証プロバイダの TIBCO WebFOCUS メタデータを構成、生成するには

この構成を開始する前に、次のディレクトリでキーストアが使用可能なことを確認します。

drive:¥ibi¥WebFOCUS82¥config¥was

デフォルトキーストア (wfKeystore.jks) およびデフォルトエイリアスを使用して ID プロバイダ用の WebFOCUS 証明書に署名して暗号化することも、ID プロバイダの要件に応じてカスタムキーストアおよびエイリアスに置き換えることもできます。

- デフォルトキーストアおよびエイリアスを使用する場合は、[SAML 認証設定の編集] ダイアログボックスのデフォルト設定を使用します。
- カスタムキーストアおよびエイリアスを使用する場合は、[SAML 認証設定の編集] ダイアログボックスのデフォルト設定を、カスタムキーストアの作成に使用した設定に置き換えます。

1. 管理コンソールの [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、[デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
2. [SAML 認証] エントリをダブルクリックします。

   [SAML 認証設定の編集] ダイアログボックスが開きます。
3. [サービスプロバイダ (SP) メタデータ] タブの [メタデータファイルのパス] テキストボックスで、デフォルトのパスおよびファイル名を受容するか、別のパスおよびファイル名を入力します (WebFOCUS で別のファイルを使用する必要がある場合)。

   デフォルトのパスは、次のとおりです。

   file:{IBI_CONFIGURATION_DIRECTORY}/was/saml/wfspMetadata.xml

   説明

   IBI_CONFIGURATION_DIRECTORY
   ルートディレクトリからこの設定までのサブフォルダを含めたパスを識別する値です。以下はその例です。

   drive:¥ibi¥WebFOCUS82¥config¥
4. [エンティティエイリアス] テキストボックスで、デフォルト値をホスト名など認識しやすい名前で上書きします。この名前には、文字と数字のみ使用できます。
5. 製品インストールに同梱されたデフォルトキーストアを使用する場合は、[署名証明書エイリアス] および [暗号化証明書エイリアス] テキストボックスのデフォルト値を受容します。デフォルトキーストアを使用しない場合は、これらのテキストボックスに、カスタムキーストアに追加したエイリアスを入力します。

これらの値により、SAML ID プロバイダに対して、署名証明書および暗号化証明書の提出者として WebFOCUS エイリアスが識別されます。

6. [SSL/TLS 証明書エイリアス]、[セキュリティプロファイル]、[SSL/TLS セキュリティプロファイル] の各テキストボックスに割り当てられたデフォルト値を受容します。
7. [メタデータに署名] のチェックは、デフォルト設定でオフになっています。このチェックボックスは、ID プロバイダに送信する WebFOCUS メタデータにデジタル署名する必要がある場合のみ選択します。
8. [シングルログアウトのサポート] および [署名済みログアウトリクエストが必要] チェックボックスに割り当てられたデフォルト設定を受容します。
9. [署名済みログアウトレスポンスが必要] のチェックは、デフォルト設定でオフになっています。このチェックボックスは、ID プロバイダからのレスポンスの認証が必要な場合にのみ選択します。
10. [メタデータの生成] をクリックします。

    [サービスプロバイダ (SP) メタデータの生成] ダイアログボックスが開きます。
11. [エンティティ ID] テキストボックスで、デフォルト URL を受容するか、サービスプロバイダが WebFOCUS Client との通信時に使用する URL を入力します。

    注意：このテキストボックスに「localhost」の値が表示された場合は、この値を WebFOCUS へのアクセスに使用する完全修飾 URL で置き換える必要があります。以下はその例です。

    ```
    https://SERVER.DOMAIN.COM/ibi_apps/sp
    ```
12. [エンティティベース URL] テキストボックスで、デフォルト URL を受容するか、サービスプロバイダが WebFOCUS Client との通信時に使用するベース URL を入力します。

    注意：代替セキュリティゾーンの SAML 認証時に、このテキストボックスに「localhost」の値が表示された場合は、この値を WebFOCUS へのアクセスに使用する完全修飾 URL で置き換える必要があります。以下はその例です。

    ```
    https://SERVER.DOMAIN.COM/ibi_apps
    ```
13. 残りの選択不可の設定は無視します。これらに割り当てられた値を更新または変更する必要がある場合は、[サービスプロバイダ (SP) メタデータの生成] ダイアログボックスを閉じ、[SAML 認証設定の編集] ダイアログボックスの対応するテキストボックスの値を更新します。
14. [サービスが認証リクエストに署名する] および [署名済み認証アサーションが必要] チェックボックスのデフォルト設定を受容します。
15. [シングルサインオンバインディング] および [サポートされる NameID] セクションのデフォルト設定を受容します。

16. [生成] をクリックします。
17. ブラウザに表示される指示に従って、wfspMetadata.xml ファイルをデスクトップにダウンロードします。
18. wfspMetadata.xml ファイルをデスクトップから、WebFOCUS マシンの次のディレクトリにコピーします。

    drive:¥ibi¥WebFOCUS82¥config¥was¥saml

19. [キャンセル] をクリックして、[サービスプロバイダ (SP) メタデータの生成] ダイアログボックスを閉じます。
20. wfspMetadata.xml ファイルを ID プロバイダに転送します。このファイルは、WebFOCUS 環境との信頼関係の確立に使用されます。
21. [SAML 認証設定の編集] ダイアログボックスで、ID サービスプロバイダのメタデータファイルの追加を続行します。

    ID サービスプロバイダからメタデータファイルが提供されない場合がまれにありますが、その場合は [OK] をクリックして [SAML 認証設定の編集] ダイアログボックスを閉じ、314 ページの 「 SAML 構成を保存するには 」 の手順に従って [認証] ページを保存します。

手順　SAML 構成に ID サービスプロバイダメタデータファイルをダウンロードして構成するには

この構成を開始する前に、SAML ID プロバイダからメタデータファイルが提供されていることを確認します。

1. SAML ID プロバイダから提供されるメタデータファイルをダウンロードします。
2. ID プロバイダから提供されたメタデータファイルを次の場所にコピーします。

   drive:¥ibi¥WebFOCUS82¥config¥was¥saml

3. [SAML 認証設定の編集] ダイアログボックスを開き、[ID プロバイダ (IdP) メタデータ] タブをクリックします。
4. [ID プロバイダ (IdP) メタデータ] タブの [メタデータファイルのパス] テキストボックスに、ID プロバイダから提供されるメタデータファイルの名前を入力します。

   次のフォーマットを使用します。

   file:{IBI_CONFIGURATION_DIRECTORY}/was/saml/idpMetadata.xml

説明

`IBI_CONFIGURATION_DIRECTORY`
ルートディレクトリからこの設定までのサブフォルダを含めたパスを識別する値です。以下はその例です。

drive:¥ibi¥WebFOCUS82¥config¥

5. [ID プロバイダ (IdP) メタデータ] タブの残りの設定はすべてデフォルト値を受容します。

   これらの設定は、ID プロバイダに要求された場合のみ変更します。

6. [詳細] タブをクリックします。

   注意：[詳細] タブの各設定は、メタファイルを生成する際に自動的に構成されます。通常、これらの設定を調整する必要はありません。ただし、次のチェックボックスは必要に応じて選択したり、選択解除したりできます。

   a. [ユーザ名を SAML アサーション属性から取得する] のチェックは、デフォルト設定でオフになっています。認証プロバイダによって、ユーザ名を SAML アサーション属性のいずれかから取得するよう要求された場合のみ、このチェックボックスを選択し、ユーザ名を取得する属性の名前を [SAML アサーション属性名] テキストボックスに入力します。

   b. [署名アルゴリズムに SHA256withRSA、ダイジェストアルゴリズムに SHA-256 を使用] のチェックは、デフォルト設定でオフになっています。ID プロバイダが SHA256 ハッシュアルゴリズムをサポートするか、これを信頼できる証明書利用者に使用するよう構成されている場合は、このチェックボックスを選択します。

   c. デフォルト設定では、[サービスプロバイダ (SP) が開始するシングルサインオンを無効にする] のチェックがオフになっています。サービスプロバイダの WebFOCUS が開始するシングルサインオン認証リクエストをブロックする必要がある場合のみ、このチェックボックスを選択します。

7. [OK] をクリックして [SAML 認証設定の編集] ダイアログボックスを閉じ、変更を保存します。

手順　デフォルトゾーンで SAML 認証を有効にするには

セキュリティゾーンで SAML 認証を有効にする際は、そのセキュリティゾーンの他の認証方法をすべて無効にする必要があります。

1. 管理コンソールの [セキュリティ] タブの [セキュリティゾーン] フォルダ下で、[デフォルト] セキュリティゾーンフォルダを展開し、[認証] をクリックします。
2. [認証] ページで、次の手順を実行します。
   a. [フォームベース認証] エントリを選択し、[無効にする] をクリックします。

b. [匿名認証] エントリを選択し、[無効にする] をクリックします。

c. [SAML 認証] エントリを選択し、[有効にする] をクリックします。

3. 314 ページの 「 SAML 構成を保存するには 」 に記載されている手順に従って、SAML 認証が構成された [認証] ページを保存します。

手順 代替セキュリティゾーンを有効にするには

代替セキュリティゾーンを有効にすると、管理者が構成タスクや管理タスクを実行するために SAML 認証をバイパスする必要がある場合に、フォームベース認証による管理者の認証が可能になります。

1. 管理コンソールの [セキュリティ] タブで、[セキュリティゾーン] フォルダをクリックします。
2. [セキュリティゾーン] ページで、[代替セキュリティゾーン] エントリをクリックし、[アクション] セクションの [有効にする] をクリックします。

   ステータスが [無効] から [有効] に変更され、代替セキュリティゾーンが使用可能になります。

手順 SAML 構成を保存するには

1. [認証] ページの [アクション] セクションで、[保存] をクリックします。
2. 確認メッセージのダイアログボックスで [OK] をクリックします。
3. Web アプリケーションの再ロードを要求するメッセージダイアログボックスで [OK] をクリックします。
4. 現在のセッションからログアウトします。
5. WebFOCUS Reporting Server を停止し、再起動します。
6. 管理者としてログインし、新しい構成をテストします。

埋め込み BI アプリケーションの Trusted チケット認証の構成

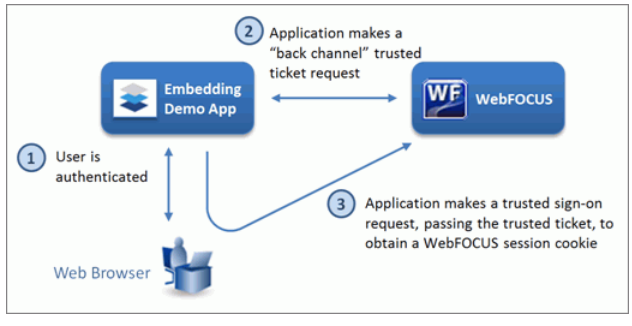
Trusted チケット事前認証では、Trusted チケットを使用して、信頼される埋め込み BI アプリケーションに埋め込まれた WebFOCUS コンテンツおよびリソースへのアクセスを要求するユーザの ID を認証します。WebFOCUS は、ログインプロセス中にこの Trusted チケットを埋め込み BI アプリケーションに提供します。

Trusted チケット認証を使用した場合、埋め込み BI アプリケーションのユーザがシングルサインオン (SSO) 機能を活用することができます。また、Trusted チケット認証を使用すると、WebFOCUS から提供されるリソースの使用が定義済みロールとアクセス権限を所有する既存ユーザに限定されるため、WebFOCUS が保護されます。

この方法をサポートするには、埋め込み BI アプリケーションと WebFOCUS の両方が埋め込み BI アプリケーションユーザのレコードを保持していること、およびこれらのユーザが外部アプリケーションに埋め込まれたコンテンツおよびリソースの格納先ドメインのグループに割り当てられていることが必要になります。埋め込み BI アプリケーションは、Trusted チケット認証をサポートする変数を送信するよう構成する必要があります。また、WebFOCUS は、埋め込み BI アプリケーションをサポートするセキュリティゾーンでこれらの変数を受容するよう構成する必要があります。

Trusted チケット認証のワークフロー

下図のように、Trusted チケット認証では 3 回のメッセージ交換が必要です。



埋め込み BI アプリケーションへのユーザログイン

1 回目の交換では、ユーザが埋め込み BI アプリケーションにログインします。ログインするには、ユーザはそのアプリケーション内での作業権限を所有する有効なユーザとして識別されるための認証情報 (例、ユーザ ID とパスワード) を提示します。埋め込み BI アプリケーションがその認証情報を認証し、作業セッションを開始します。

Trusted チケットリクエスト

2 回目の交換では、埋め込み BI アプリケーションが WebFOCUS からの Trusted チケットを取得するための HTTP GET または POST リクエストメッセージを送信します。以下はその例です。

```
GET http://host:port/ibi_apps/service/wf_security_trusted.jsp?
IBIB_userid=userone
```

注意：このリクエストには「http://」または「https://」を使用することができます。

埋め込み BI アプリケーションと WebFOCUS 間で行われる 2 回目のメッセージ交換は、一般に「バックチャネル」のリクエストと呼ばれます。これは、埋め込み BI アプリケーションのホストサーバと WebFOCUS のホストサーバ間で接続が直接確立されるためです。そのため、この接続は、ユーザの Web ブラウザを実行するネットワークからは見えません。

この Trusted チケットリクエストには、1 つの必須パラメータと 2 つのオプションパラメータが含まれています。

- IBIB_userid パラメータは必須です。このパラメータには、新規に認証されたユーザの ID が格納されます。
- IBIB_appname パラメータはオプションです。このパラメータには、[Trusted チケット認証設定の編集] ダイアログボックスの [アプリケーションリスト] ボックスで指定されたアプリケーションのいずれかの名前が格納されます。このパラメータは Trusted チケットリクエストに含めることができますが、このパラメータがリクエストに含まれず、セキュリティゾーンでデフォルトアプリケーションが指定されていない場合、WebFOCUS は、[Trusted チケット認証設定の編集] ダイアログボックスで指定されたデフォルトアプリケーション名を使用します。
- IBIB_useripaddr パラメータもオプションです。このパラメータは、埋め込み BI アプリケーションの [Trusted チケットのアプリケーション設定] ダイアログボックスで [クライアント IP 一致を有効にする] のチェックをオンにした場合にのみ必要です。このパラメータには、ログインリクエストを開始したユーザが使用するブラウザの IP アドレスが格納されます。

WebFOCUS が Trusted チケットリクエストを受信すると、そのリクエストに IBIB_appname パラメータが含まれているかどうかを特定します。このパラメータがリクエストに含まれている場合、WebFOCUS は、そのアプリケーションが [Trusted チケット認証設定の編集] ダイアログボックスの [アプリケーションリスト] ボックスで指定された有効なアプリケーションのいずれかであることを確認します。

IBIB_appname パラメータのアプリケーション名に一致するアプリケーションが存在しない場合、その Trusted チケットリクエストは拒否されます。

一致するアプリケーションが存在する場合、WebFOCUS は、Trusted チケットの要求元アプリケーションの IP アドレスと、そのアプリケーションの [受容 IP アドレス] リストを比較します。IP アドレスがそのリストに含まれていない場合、そのリクエストは拒否されます。IP アドレスがそのリストに含まれている場合、Trusted チケットが作成されます。

Trusted チケットリクエストに IBIB_appname パラメータが含まれていない場合、WebFOCUS は、リスト内のアプリケーションのいずれかがデフォルトアプリケーションとして指定されているかどうかを特定します。

デフォルトアプリケーションが存在しない場合、そのリクエストは拒否されます。

デフォルトアプリケーションが存在する場合、WebFOCUS は、Trusted チケットの要求元アプリケーションの IP アドレスが、デフォルトアプリケーションの [受容 IP アドレス] リストに含まれているかどうかを特定します。IP アドレスがリストに含まれていない場合、そのリクエストは拒否されます。IP アドレスがリストに含まれている場合、Trusted チケットが作成されます。

Trusted チケットには暗号化された情報が格納され、この情報が WebFOCUS でのその後の Trusted ログインリクエストの処理に使用されます。Trusted チケットは、Trusted チケットリクエスト内のパラメータ (必須の IBIB_userid パラメータ、オプションの IBIB_appname および IBIB_useripaddr パラメータ) の値と、そのチケットが作成された時間を取得します。その後の Trusted ログインリクエストで、WebFOCUS はこれらのパラメータの暗号化された値を使用して、ユーザ認証および Trusted ログインリクエスト自体を検証します。Trusted チケットは、そのアプリケーションのチケット有効期間で指定された時間内に、Trusted ログインリクエストの一部として WebFOCUS に返される必要があります。この有効期間は、埋め込み BI アプリケーションごとの [Trusted チケットのアプリケーション設定] ダイアログボックスの [チケットの有効期間 (秒)] テキストボックスで定義されます。

Trusted チケットが作成されると、WebFOCUS がそのチケットを埋め込み BI アプリケーションに返します。次にこのアプリケーションが、ログインリクエストを開始したユーザのブラウザに返します。

Trusted ログインリクエスト

3 回目の交換では、埋め込み BI アプリケーションのユーザのブラウザから、Trusted ログインリクエストが WebFOCUS に送信されます。このリクエストは、HTTP GET または POST リクエストメッセージの形式で WebFOCUS に送信されます。以下はその例です。

```
GET http://host:port/ibi_apps/service/wf_security_trusted.jsp
```

説明

`host`
: WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

`port`
: Web サーバまたは Application Server が受信待機するポートの番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

注意：このリクエストには「http://」または「https://」を使用することができます。

この Trusted ログインリクエストには、1 つの必須パラメータと 2 つのオプションパラメータが含まれています。

- IBIB_ticket パラメータは必須です。このパラメータには、埋め込み BI アプリケーションから取得された Trusted チケット値が格納されます。
- IBIB_appname パラメータはオプションです。このパラメータには、[Trusted チケット認証設定の編集] ダイアログボックスの [アプリケーションリスト] ボックスで指定されたアプリケーションのいずれかの名前が格納されます。このパラメータは Trusted ログインリクエストに含めることができますが、このパラメータがリクエストに含まれず、セキュリティゾーンでデフォルトアプリケーションが指定されていない場合、WebFOCUS は、[Trusted チケット認証設定の編集] ダイアログボックスで指定されたデフォルトアプリケーション名を使用します。
- IBIB_Destination パラメータもオプションです。このパラメータには、ログイン後に WebFOCUS がユーザをリダイレクトする URL が格納されます。このリダイレクト先は、WebFOCUS ホームページにすることも、相対 URL で指定されるポータルにすることもできます。

WebFOCUS が Trusted ログインリクエストを受信すると、WebFOCUS は、そのリクエストが Trusted ログインリクエストの開始ユーザの埋め込み BI アプリケーションで定義されたチケット有効期間内に受信されたこと、およびそのリクエストの開始ユーザが WebFOCUS 内に存在することを確認します。チケット有効期間の期限切れ後に Trusted ログインリクエストが受信された場合、そのリクエストは拒否されます。

チケット有効期間内にリクエストが受信された場合、WebFOCUS は、Trusted チケットリクエスト検証に記載されている方法で、リクエスト元アプリケーションの名前を検証します。IBIB_appname パラメータから提供された名前が [アプリケーションリスト] ボックスに存在しない場合、その Trusted ログインリクエストは拒否されます。Trusted ログインリクエストに IBIB_appname パラメータが含まれておらず、デフォルトアプリケーションが指定されていない場合、そのリクエストは拒否されます。

Trusted ログインリクエストの検証に成功した場合、WebFOCUS は Trusted チケットから IBIB_userid、IBIB_appname、IBIB_useripaddr パラメータを取得して暗号化します。

WebFOCUS が IBIB_userid パラメータで識別されるユーザ ID の既存アカウントを特定できない場合、WebFOCUS は [ログイン時にアカウントを作成] 設定の値を確認します。この値が [すべて] の場合、このユーザの新しいアカウントが自動的に作成されます。この設定には、[オフ] または [マッピング済み外部グループ] 値を使用することもできます。これらの構成オプションについての詳細は、334 ページの 「 AUTOADD 」 を参照してください。

Trusted チケットに IBIB_useripaddr パラメータのユーザ IP アドレスが含まれ、埋め込み BI アプリケーションの設定で [クライアント IP 一致を有効にする] のチェックがオンになっている場合、WebFOCUS は、Trusted チケットの IP アドレスと、Trusted チケットリクエストを送信した埋め込み BI アプリケーションユーザのブラウザの IP アドレスが一致していることを確認します。これらの IP アドレスが一致していない場合、その Trusted ログインリクエストは拒否されます。これらの IP アドレスが一致している場合、その Trusted ログインリクエストは受容されます。

WebFOCUS が Trusted ログインリクエストを受容すると、ユーザのセッションが開始され、IBIB_Destination パラメータで識別される URL にユーザがリダイレクトされます。埋め込み BI アプリケーションは、URL リクエストまたは WebFOCUS RESTful Web サービス API を使用して、このユーザの代わりに WebFOCUS からコンテンツおよびリソースを要求することができます。

埋め込み BI アプリケーションから WebFOCUS リソースを作成または更新する POST リクエストを送信する必要がある場合は、クロスサイトリクエストフォージェリ (CSRF) トークンを WebFOCUS から取得し、これらのリクエストとともに送信する必要があります。通常、Trusted ログインリクエストへのレスポンスでは、このセッションで使用可能な CSRF トークン名と値の組み合わせを含む XML が返されます。

Trusted チケット認証用の代替セキュリティゾーンの使用

一般に、埋め込み BI アプリケーション展開をサポートするために代替セキュリティゾーンを有効にする必要はありません。代替セキュリティゾーンを有効にすると、Trusted チケット認証構成のトラブルシューティングが複雑になる可能性があるため、有効にする必要がない限り、代替セキュリティゾーンは無効にしておくことをお勧めします。

ただし、代替セキュリティゾーンを有効にする必要があり、Trusted チケット認証をサポートする場合は、最初に WebFOCUS が代替セキュリティゾーン構成でクライアントリクエストを処理するかどうかを特定します。デフォルト設定では、代替セキュリティゾーンは、localhost IP アドレスの「127.0.0.1」および「0:0:0:0:0:0::1」に送信されたリクエストを受信するよう構成されています。この構成を作成するには、代替セキュリティゾーンで Trusted チケット認証を有効にし、埋め込み BI アプリケーションが存在するホストの IP アドレスを追加します。

Trusted チケット認証構成の概要

Trusted チケット認証を構成するには、管理者は、埋め込み BI アプリケーションと WebFOCUS が情報を交換し、Trusted チケットリクエストおよび Trusted ログインリクエストを認証するよう構成する必要があります。

埋め込み BI アプリケーションが Trusted チケット認証をサポートするよう準備するには、埋め込み BI アプリケーション開発者が次のように構成する必要があります。

1. 埋め込み BI アプリケーションの必須パラメータ ID 情報が含まれた Trusted チケットを WebFOCUS に送信するためのバックチャネルリクエストを発行するよう埋め込み BI アプリケーションを構成します。
2. WebFOCUS ホストのアドレスを識別する Trusted チケットを使用してフロントチャネルログインリクエストを発行するよう埋め込み BI アプリケーションを構成します。

Trusted チケットリクエストおよび Trusted ログインリクエストを送信するよう埋め込み BI アプリケーションを構成する方法についての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

この構成および埋め込み BI アプリケーションから送信される ID 情報は、管理者が WebFOCUS で Trusted チケット構成に外部アプリケーションを追加する前に準備しておく必要があります。

Trusted チケット認証をサポートするよう WebFOCUS を準備するには、管理者は次のように構成する必要があります。

1. 埋め込み BI アプリケーションをサポートするセキュリティゾーンで、Trusted チケット認証を構成して有効にします。
2. 埋め込み BI アプリケーションと WebFOCUS が異なるオリジンからアクセスされる場合は、埋め込み BI アプリケーションをサポートするセキュリティゾーンでクロスオリジン (CORS) 設定を構成します。詳細は、160 ページの 「 クロスオリジン設定の構成 」 を参照してください。
3. 構成の完了後、Tomcat を再起動して、WebFOCUS が Trusted チケット接続を受容する構成を有効にします。

Trusted チケット認証の評価

Fintoso 埋め込み BI デモアプリケーションは、drive:¥ibi¥WebFOCUS82¥samples ¥embedded_demo に格納され、Trusted チケット機能の評価に役立つ次の 2 つのページが含まれています。

- Trusted チケットの作成ページ

  `http(s):/host:port/embeddemo/tester/create_trusted_ticket.jsp`

- Trusted チケットログインリクエストのテスト

  ```
  http(s):/host:port/embeddemo/tester/test_trusted_ticket.jsp
  ```

説明

`host`
WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

`port`
Web サーバまたは Application Server が受信待機するポートの番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

これらのページでは、2 つのトランザクションのそれぞれについて、必須テキストボックスとオプションテキストボックスが識別されています。

これら 2 つのページについての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

注意: create_trusted_ticket.jsp ページにリクエストを発行するブラウザをホストするマシンのアドレスが、[Trusted チケット認証設定の編集] ダイアログボックスの [アプリケーションリスト] に表示されます。このアドレスが表示されない場合は、[Trusted チケットの作成] ページで、Trusted チケットを作成するリクエストが受容されません。このリストへのアドレスの追加についての詳細は、321 ページの 「 Trusted チケット認証を構成するには 」 を参照してください。

手順　Trusted チケット認証を構成するには

次の手順を開始する前に、事前認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

WebFOCUS での SSL 構成などの追加要件を伴う場合があります。この構成に必要な手順についての詳細は、54 ページの 「 TIBCO WebFOCUS での SSL 構成 」 を参照してください。その他の要件についての詳細は、技術サポートに問い合わせてください。

埋め込み BI アプリケーションの開発者と連携して、Trusted チケットリクエストおよび Trusted ログインリクエストをサポートするよう埋め込み BI アプリケーションを構成します。詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』を参照してください。

また、[認証] ページで変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップを作成しておくことをお勧めします。詳細は、174 ページの「 セキュリティ構成ファイルをエクスポートするには 」 を参照してください。

1. 管理コンソールで [セキュリティ] タブをクリックします。
2. [セキュリティ] ページの [セキュリティゾーン] フォルダ下で、次の手順を実行します。
   a. デフォルトセキュリティゾーンで埋め込み BI アプリケーションをサポートする場合は、[デフォルト] セキュリティゾーンフォルダ下で [認証] をクリックし、次の手順へ進みます。
   b. 代替セキュリティゾーンで埋め込み BI アプリケーションをサポートする場合は、[代替セキュリティゾーン] フォルダ下で [認証] をクリックし、次の手順へ進みます。

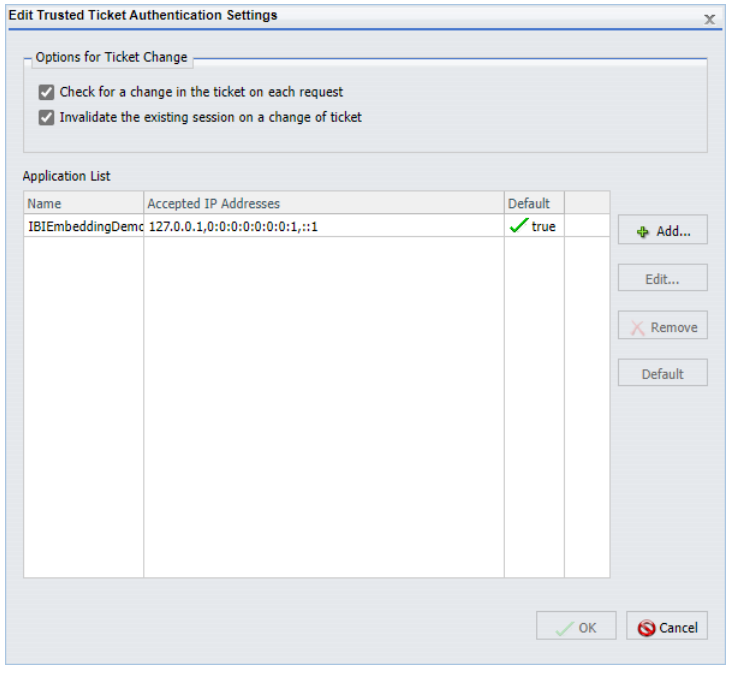
   注意：両方のゾーンで埋め込み BI アプリケーションをサポートする場合は、最初にデフォルトセキュリティゾーンの Trusted チケット認証を構成し、次に代替セキュリティゾーンの Trusted チケット認証を構成します。
3. [Trusted チケット認証] エントリをクリックし、[アクション] セクションで [編集] をクリックします。

   または

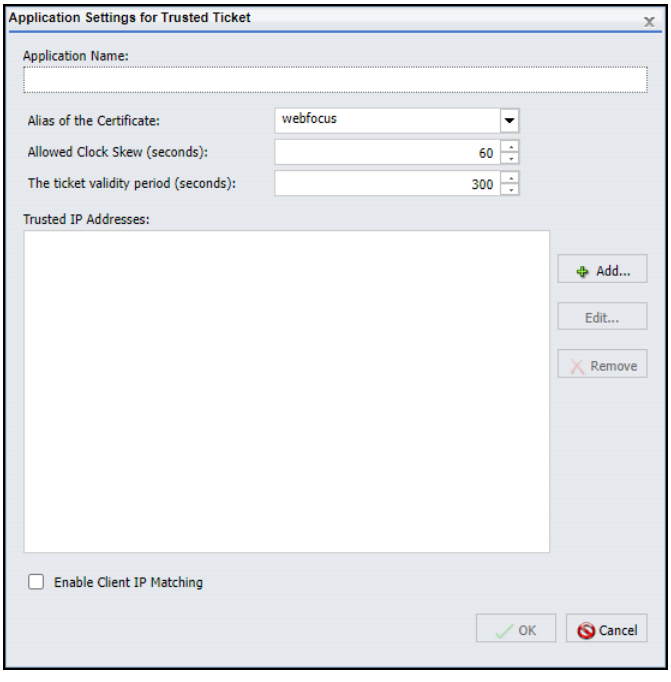
   [Trusted チケット認証] エントリを右クリックし、[編集] を選択します。
4. [Trusted チケット認証設定の編集] ダイアログボックスで、[各リクエストでチケットの変更を確認する] および [チケットの変更時に既存のセッションを無効にする] チェックボックスのデフォルト設定を受容します。

   これらの設定は、同時セッションの数を最小限にするために構成されています。そのために、現在開いているセッションの中で新しい Trusted チケットログインリクエストを受信した際に既存ユーザをログアウトし、新しいログインリクエストを送信したユーザでログインします。これらのチェックをオフにすることはお勧めしません。

5. 下図のように、[追加] をクリックします。



6. 下図のように、[Trusted チケットのアプリケーション設定] ダイアログボックスで、[アプリケーション名] テキストボックスに埋め込み BI アプリケーションの名前を入力します。

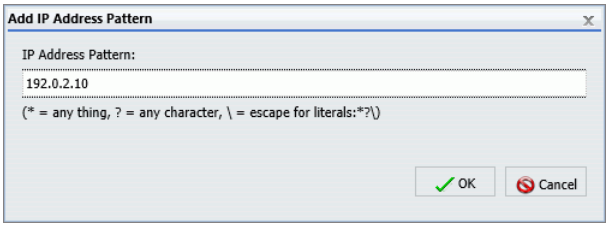


HTTP リクエストメッセージで送信されるアプリケーション名と同一の綴りおよび大文字小文字で名前を入力します。

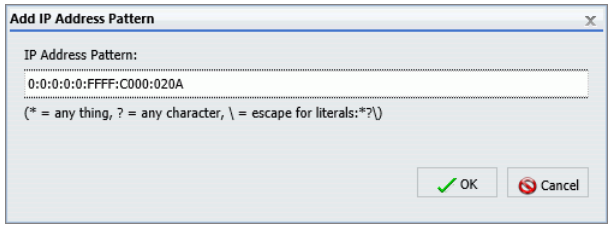
注意：セキュリティを強化するには、新しい証明書を作成して WebFOCUS キーストアに追加し、そのキーストアのエイリアスを作成した上で、[証明書のエイリアス] リストでそのエイリアスの名前をクリックします。

7. [追加] をクリックします。
8. [IP アドレスパターンの追加] ダイアログボックスで、[IP アドレスパターン] テキストボックスに埋め込み BI アプリケーションの IP アドレスを入力します。

   下図のように、IPv4 フォーマットを使用することができます。



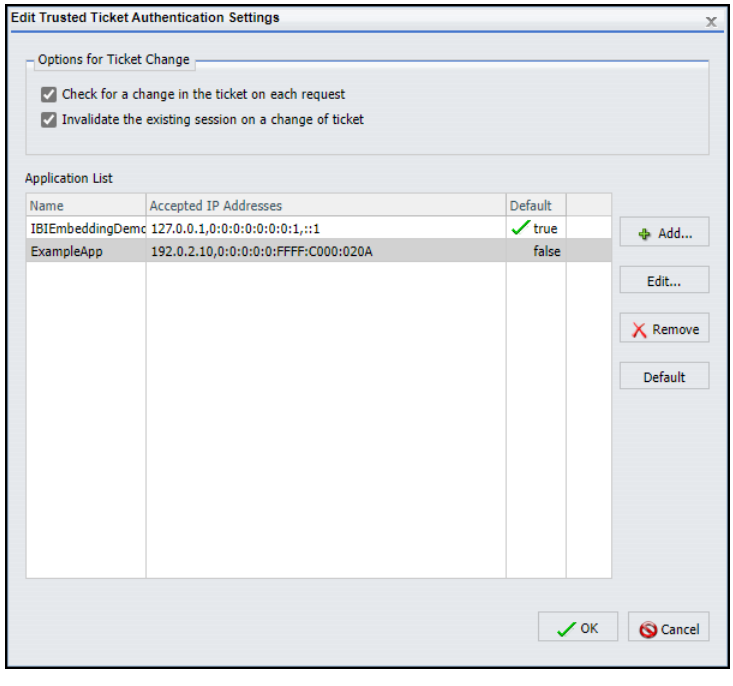
下図のように、IPv6 フォーマットを使用することもできます。



[IP アドレスパターン] テキストボックスには 1 つのアドレスのみを入力します。

9. アドレスを入力した後、[OK] をクリックします。
10. 同一のアプリケーションに対して別の IP アドレスを追加する必要がある場合は、手順 7 から 9 を繰り返します。
11. [Trusted チケットのアプリケーション設定] ダイアログボックスにすべてのアドレスを入力した後、[OK] をクリックします。

    下図のように、[アプリケーションリスト] ボックスに新しい埋め込み BI アプリケーションが表示されます。



12. 別のアプリケーションを追加する必要がある場合は、手順 5 から 11 を繰り返します。

13. [Trusted チケット認証設定の編集] ダイアログボックスにすべてのアプリケーションを入力した後、[OK] をクリックします。
14. [認証] ページの [アクション] セクションで、[保存] をクリックします。
15. 確認メッセージのダイアログボックスで [OK] をクリックします。
16. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
17. 現在のセッションからログアウトします。
18. WebFOCUS Reporting Server を停止し、再起動します。
19. 管理者として再度ログインし、新しい構成をテストします。

    埋め込み BI アプリケーションと WebFOCUS が 2 つの異なるサーバ上で展開されている場合は、埋め込み BI アプリケーションをサポートするゾーンで、埋め込みを許可するよう WebFOCUS を構成します。詳細は、164 ページの「 セキュリティゾーンで埋め込みを許可するには 」 を参照してください。

    埋め込み BI アプリケーションから WebFOCUS リソースを作成または更新する POST リクエストを送信する必要がある場合は、埋め込み BI アプリケーションをサポートするゾーンで、CORS (クロスオリジンリソース共有) を設定する必要があります。詳細は、168 ページの「 セキュリティゾーンでクロスオリジンリソース共有を許可するには 」 を参照してください。

手順　クロスサイトリクエストフォージェリトークンの名前を変更するには

1. 管理コンソールの [構成] タブの [アプリケーションの設定] フォルダ下で、[フィルタ] をクリックします。
2. [フィルタ] ページで、[クロスサイトリクエストフォージェリ保護] のチェックがオンになっていることを確認します。
3. [クロスサイトリクエストフォージェリセキュリティトークン] テキストボックスに [IBIWF_SES_AUTH_TOKEN] 値が入力されていることを確認します。
4. [保存] をクリックします。
5. 管理コンソールのメニューバーで [キャッシュのクリア] をクリックします。
6. 確認メッセージのダイアログボックスで [OK] をクリックします。

外部認証

外部認証では、ユーザにログインページが提示され、ユーザがこのページでユーザ ID およびパスワードを入力します。WebFOCUS Client は、これらの認証情報を WebFOCUS Reporting Server に渡します。次に Reporting Server は、これらの認証情報を外部ソースに基づいて検証します。WebFOCUS では、Active Directory、LDAP ディレクトリ、カスタム RDBMS テーブル情報、Web サービスなどの外部ソースを使用してユーザを認証することができます。外部ソースによるユーザ認証は、ユーザが WebFOCUS Client にアクセスする際と、Reporting Server ブラウザインターフェースに直接アクセスする際の両方で実行されます。

注意：現在、WebFOCUS では WebFOCUS Reporting Server 経由でのユーザパスワード変更はサポートされません。外部認証を構成する際は、[セキュリティ] タブの [詳細] ページで [パスワードの変更を有効にする] のチェックをオフにします。

Active Directory および LDAP 認証の理解

WebFOCUS では、Active Directory および LDAP ディレクトリに基づいてユーザを認証することができます。この方法では、WebFOCUS Reporting Server でユーザを認証し、次に WebFOCUS Reporting Server LDAP セキュリティプロバイダを使用して外部ディレクトリによりユーザ認証情報を検証します。

必要に応じて、WebFOCUS リポジトリ内のユーザアカウント情報を、外部ディレクトリの Email アドレスおよび説明で更新することもできます。

手順　Active Directory および LDAP 認証を構成するには

次の手順を開始する前に、外部認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページに変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップコピーを保存しておくことをお勧めします。

1. WebFOCUS Reporting Server で、LDAP をプライマリプロバイダ、PTH をセカンダリプロバイダとして構成します。

   詳細は、30 ページの 「 TIBCO WebFOCUS Reporting Server でのセキュリティプロバイダの構成 」 を参照してください。

2. 管理者としてログインし、管理コンソールを起動します。
3. 管理コンソールの [セキュリティ] タブの [セキュリティの構成] フォルダ下で、[外部] をクリックします。
4. [外部セキュリティを有効にする] のチェックをオンにします。

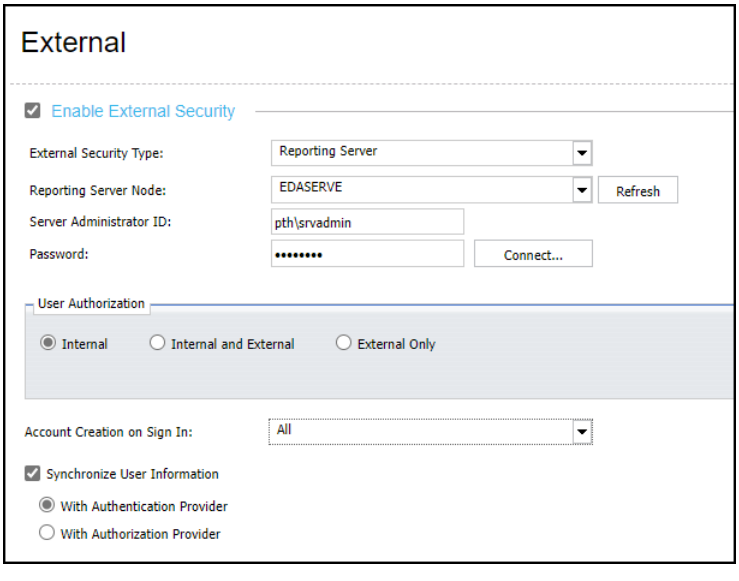
[外部] ページに、WebFOCUS Reporting Server に現在割り当てられている設定が表示されます。

5. [サーバ管理者 ID] テキストボックスに「pth¥srvadmin」と入力します。
6. [パスワード] テキストボックスに、セキュリティユーザに割り当てられているパスワードを入力します。

   このアカウントのパスワードは、インストールプロセス中に、元の管理者アカウントに対して指定したパスワードと同一になるよう事前に構成されています。
7. [接続] をクリックします。

   確認ダイアログボックスで [OK] をクリックします。
8. [ユーザ認可] グループで [内部] オプションを選択します。
9. [ログイン時にアカウントを作成] リストから [OFF] を選択します。
10. 認証中に WebFOCUS アカウントを Active Directory または LDAP ユーザの説明および Email で更新するには、[ユーザ情報を認証プロバイダと同期] のチェックをオンにします。
    a. ユーザの説明および Email の最新情報を認証プロバイダから取得するには、デフォルトオプションの [認証プロバイダを使用] を選択します。
    b. ユーザの説明および Email の最新情報を認可プロバイダから取得するには、[認可プロバイダを使用] を選択します。

すべての構成が完了すると、このページは下図のようになります。



11. [セキュリティの構成] セクションで [保存] をクリックします。
12. 確認メッセージで [OK] をクリックします。
13. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
14. 現在のセッションからログアウトします。
15. WebFOCUS Reporting Server を停止し、再起動します。
16. 管理者としてログインし、新しい構成をテストします。

RDBMS テーブル情報による認証の構成

WebFOCUS Reporting Server で CUSTOM セキュリティプロバイダを使用することで、RDBMS テーブルのデータに基づいてユーザを認証するよう WebFOCUS を構成することができます。CUSTOM プロバイダは、カスタム FOCUS プロシジャを使用して認証を実行します。認証比較を行う前に、ユーザパスワードのハッシュを RDBMS に格納し、実行時にカスタム FOCUS プロシジャでそのハッシュを計算することをお勧めします。

必要に応じて、リポジトリ内のユーザアカウント情報を、データベースの Email アドレスおよび説明で更新することもできます。

手順　RDBMS テーブル情報による認証を構成するには

次の手順を開始する前に、外部認証に必要な構成を完了しておく必要があります。詳細は、225 ページの 「 事前認証、外部認証、外部認可の構成 」 を参照してください。

[認証] ページに変更を加える前に、[エクスポート] コマンドを使用してセキュリティ設定構成ファイルのバックアップコピーを保存しておくことをお勧めします。

1. WebFOCUS Reporting Server で、カスタムプロバイダをプライマリプロバイダ、PTH をセカンダリプロバイダとして構成します。
2. 管理者としてログインし、管理コンソールを起動します。
3. [セキュリティ] タブをクリックし、[セキュリティの構成] フォルダ下の [外部] をクリックします。
4. [外部セキュリティを有効にする] のチェックをオンにします。

   [外部] ページに、WebFOCUS Reporting Server に現在割り当てられている設定が表示されます。
5. [サーバ管理者 ID] テキストボックスに、WebFOCUS Reporting Server 管理者アカウントサービス名を「ProviderName¥serviceUserName」の形式で入力します。

説明

`ProviderName`
RDBMS の名前です。

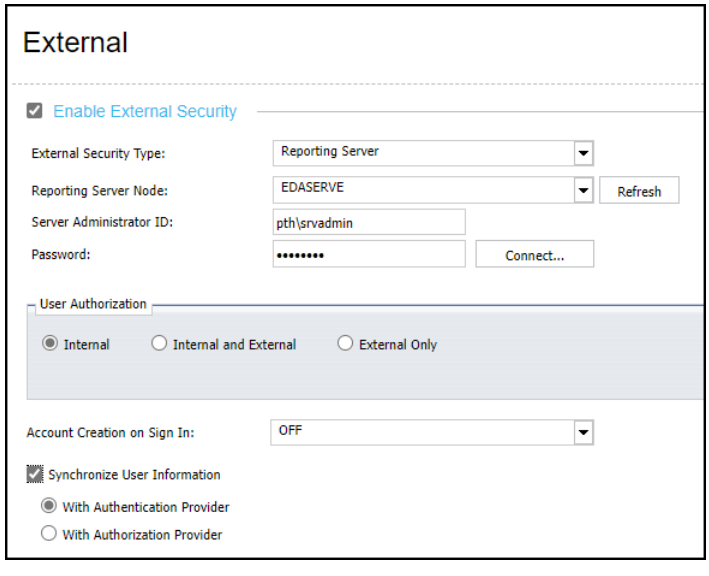
`serviceUserName`
RDBMS のユーザ ID です。

6. [パスワード] テキストボックスに、セキュリティユーザに割り当てられているパスワードを入力します。
7. [接続] をクリックします。

   確認ダイアログボックスで [OK] をクリックします。
8. [ユーザ認可] グループで [内部] オプションを選択します。

   RDBMS を使用して他の認可方法 (例、AD、LDAP) を無効にする場合は、[内部と外部] オプションを選択し、[グループプロバイダ優先] リストから、認可方法を提供する RDBMS プロバイダの名前を選択します。
9. [ログイン時にアカウントを作成] リストから [OFF] を選択します。
10. 認証中に WebFOCUS アカウントを RDBMS ユーザの説明および Email で更新するには、[ユーザ情報を認証プロバイダと同期] のチェックをオンにします。

    すべての構成が完了すると、このページは下図のようになります。



11. 現在のセッションからログアウトします。

12. Application Server を停止し、再起動します。
13. RDBMS のユーザ ID とパスワードを使用して再度ログインします。

    ログインに成功した場合、外部認証が正しく構成されています。

認可の理解

認可は、認証済みのユーザまたはプログラムが実行可能な機能およびアクセス権限を決定するプロセスです。WebFOCUS ソフトウェアには、ユーザを認可する複数のオプションが用意されています。デフォルト設定では、WebFOCUS は内部認可を使用するよう構成されています。この構成では、ユーザが実行可能な機能およびリソースへのアクセス権限は、WebFOCUS リポジトリに格納されている情報のみに基づいて決定されます。また、WebFOCUS は外部認可を使用するよう構成することもできます。この構成では、ユーザが実行可能な機能およびアクセス権限は、WebFOCUS ソフトウェアの外部で管理されている情報に基づいて決定されます。

外部認可は、次の情報に基づいて処理されます。

- LDAP (Lightweight Directory Access Protocol) をサポートする任意のディレクトリ (例、Microsoft Active Directory (AD)) から取得されたグループ、ロール、およびユーザプロファイル属性値。
- リレーショナルデータベース管理システム (RDBMS) から取得されたデータ。
- 任意の WebFOCUS Reporting Server データアダプタから取得されたデータ (例、Web サービスや ERP システムから取得された情報)。

WebFOCUS では、さらに柔軟に、一部のユーザを内部認可し、その他のユーザを外部認可することも可能です。外部認可されたユーザがログインする際に内部ユーザアカウントが存在しない場合は、WebFOCUS がそのアカウントを自動的に作成します。

内部認可の理解

デフォルト設定では、WebFOCUS は内部認可を使用するよう構成されています。この構成では、ユーザが実行可能な機能およびリソースへのアクセス権限は、WebFOCUS リポジトリに格納されている情報のみに基づいて決定されます。管理者は、セキュリティセンターを使用して、ユーザの作成やグループへのユーザの追加を行えます。外部アプリケーションでは、Web サービス API を使用して、ユーザやグループの作成、グループメンバーシップの管理を行えます。

通常、セキュリティルールはグループに関連付けられるため、ユーザのアクセス権限は、そのユーザが属する WebFOCUS グループに基づいて決定されます。ただし、特別な要求に応えるために、特定のユーザのセキュリティルールを個別に作成することも可能です。

内部認可は、内部認証、外部認証、事前認証などの、任意の認証方法と組み合わせて使用することができます。

外部認可の理解

外部認可を使用するよう WebFOCUS を構成すると、WebFOCUS は、WebFOCUS Reporting Server (WFRS) で構成されたセキュリティプロバイダを使用して、ユーザログイン時にユーザに関する情報を外部ソースから取得します。この情報には、ユーザの Email アドレス、説明、外部グループメンバーシップなどがあります。次に、WebFOCUS Reporting Server はこの情報を WebFOCUS に返します。WebFOCUS は、この情報に基づいて、ユーザアカウントを作成、更新したり、ユーザ認可情報を定義したりします。また、セキュリティプロバイダは、すべての外部グループのリストや外部グループに属するユーザのリストを取得するなどの管理機能をサポートするために、ユーザおよびグループに関するその他の外部情報も WebFOCUS に返します。

注意：認可データの管理に LDAP グループを使用するのではなく、LDAP ユーザプロファイル属性やロールを使用して認可データを外部で管理している組織もあります。WebFOCUS ではこの方法もサポートされます。

WebFOCUS でサポートされる外部認可の一例として次の方法があります。

- 事前認証と外部認可
  - Windows 認証を使用してユーザを識別し、これらのユーザを Active Directory グループメンバーシップに基づいて認可します。
  - Web アクセス管理システムを使用してユーザを認証し、これらのユーザをリレーショナルデータベース管理システム (RDBMS) に格納されている情報に基づいて認可します。
  - WebFOCUS に SaaS (Software as a Service) アプリケーションを統合して、ユーザにシングルサインオン (SSO) 機能を提供します。これらのユーザを RDBMS または Web サービスから取得された情報に基づいて認可します。
- 外部認証と外部認可
  - LDAP ディレクトリを使用してユーザを認証するとともに、グループまたはロールの情報を取得してユーザを認可します。
  - カスタム SQL ストアドプロシジャを使用してユーザを認証、認可します。

EXTERNAL および EXTERNALONLY オプション

WebFOCUS グループを外部ディレクトリの認可データにマッピングする場合、2 つの構成オプションがあります。これらのオプションは、[外部] ページの [ユーザ認可] グループに表示されます。[外部] ページを開くには、管理コンソールの [セキュリティ] タブで [外部] をクリックします。

EXTERNAL

WebFOCUS グループを外部ソースにマッピングしますが、マッピングされるグループとマッピングされないグループがあります。ユーザは、次のいずれかに該当する場合に認可されます。

- ユーザが、WebFOCUS グループにマッピングされた外部グループのメンバーである場合。
- ユーザが、マッピングされていない WebFOCUS グループに明示的に配置されている場合。

この設定は、[外部セキュリティタイプ] (IBI_Authentication_Type) が [Reporting Server] に設定されている場合に使用することをお勧めします。

EXTERNALONLY

ユーザは、WebFOCUS グループにマッピングされた外部グループのメンバーである場合にのみ認可されます。

このオプションを選択した場合は注意が必要です。WebFOCUS の Administrators グループに外部認可情報がマッピングされていない場合、ユーザが WebFOCUS からロックアウトされる可能性があります。

EXTERNALONLY オプションの認可を指定した場合、WebFOCUS で管理者権限を保持するには、次のいずれかを実行する必要があります。

- EXTERNALONLY オプションを構成した後、スーパーユーザアカウントで WebFOCUS にログインし、Administrators グループを外部グループにマッピングします。その後、外部グループに属するユーザで WebFOCUS にログインします。
- 最初に EXTERNAL オプションを構成した後、管理者アカウントで WebFOCUS にログインし、Administrators グループを外部グループにマッピングします。次に、EXTERNALONLY オプションを構成し、外部グループに属するユーザで WebFOCUS にログインします。

注意：WebFOCUS の親グループが外部ソースにマッピングされている場合は、子グループのメンバーシップがマッピングされているか、直接割り当てられているかに関係なく、ユーザがその子グループのメンバーであると見なされるには、その親グループのメンバーである必要があります。

AUTOADD

WebFOCUS には、ユーザアカウントが外部ソースに存在するが WebFOCUS には存在しない場合に、事前認証または外部認証されたユーザを WebFOCUS に自動的に追加するオプションがあります。自動的に追加されたユーザは、WebFOCUS に正常にログインすることができます。外部ソースには存在するが WebFOCUS には存在しないユーザのうち、自動的に追加されないユーザは、WebFOCUS へのアクセスが拒否されます。

セキュリティセンターでは、ログインプロセスで自動的に作成されたアカウントは、[ACTIVE] ではなく、[AUTOADD] ステータスになります。

外部認証と外部認可を構成する際の制限事項

外部認証と外部認可とを構成する場合は、次の制限が適用されます。

- インストールした WebFOCUS ごとに、外部認証、外部認可、またはその両方に使用可能な WebFOCUS Reporting Server ノードは 1 つです。
- 各ユーザの認証と認可の両方に、同一の WebFOCUS Reporting Server セキュリティプロバイダを使用する必要があります。
- ユーザアカウントのプロバイダを指定しない場合、そのアカウントはプライマリプロバイダからのアカウントとして扱われます。認証または認可に複数の WebFOCUs Reporting Server セキュリティプロバイダを使用するには、セカンダリセキュリティプロバイダに関連付ける各ユーザの WebFOCUS ユーザ ID に、セカンダリセキュリティプロバイダ名を接頭語として追加します。たとえば、WebFOCUS Reporting Server で、LDAP01 というプライマリプロバイダと LDAP02 というセカンダリプロバイダの 2 つの LDAP プロバイダを使用する場合は、WebFOCUS で LDAP01¥user1 および LDAP02¥user2 のユーザアカウントを、それぞれ「user1」および「LDAP2¥user2」として作成する必要があります。

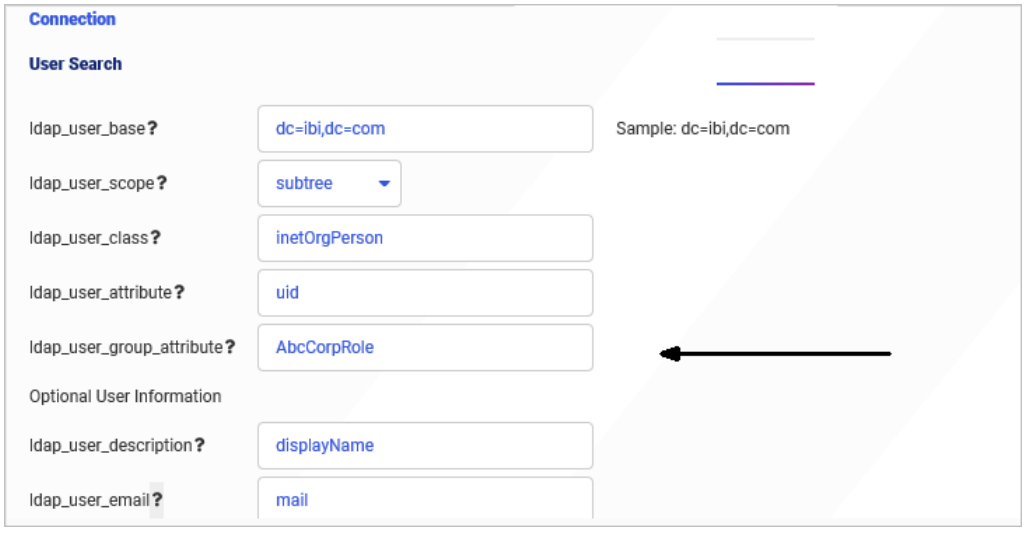
認可にユーザプロファイル属性を使用する際の特別な考慮事項

LDAP ディレクトリまたは Microsoft Active Directory から取得したグループ、ロール、またはユーザプロファイル属性値に基づいてユーザを認可するには、WebFOCUS Reporting Server で LDAP セキュリティプロバイダを構成します。構成後、WebFOCUS Reporting Server は外部ユーザディレクトリからユーザ、グループ、ロール、またはユーザプロファイル属性に関する情報を取得し、それを WebFOCUS Client に渡します。この LDAP セキュリティプロバイダを使用して、WebFOCUS Client のユーザ認証情報を認証することもできます。

通常、LDAP および Active Directory ユーザディレクトリで管理されているグループメンバーシップ情報は、他のアプリケーションでユーザを認可するためにも使用されます。ただし、組織によっては、このディレクトリに格納されている他の情報 (例、ロール、ユーザプロファイル属性) に依存する場合もあり、その場合は必要な認可情報が属性に挿入されます。これらの属性には、単一値の属性と複数値の属性があり、外部ディレクトリ内の他のオブジェクトと関係を設定する必要はありません。これらの認可方法がすべてサポートされます。

注意：ベンダーおよびバージョンによっては、WebFOCUS のすべての外部認可機能をサポートするために、LDAP ディレクトリにユーザメンバーシッププラグインが必要になる場合があります。Active Directory は、独自のユーザメンバーシップをサポートします。詳細は、LDAP 管理者に問い合わせてください。

下図のように、ユーザプロファイル属性から認可データを取得し、それを WebFOCUS に渡して認可を行うよう LDAP プロバイダを構成することができます。ここでは、[ldap_user_group_attribute] で指定された AbcCorpRole がユーザ認可に使用されます。



LDAP グループとは異なり、カスタム属性には対応するディレクトリオブジェクトが存在しないため、次の制限が適用されます。

- WebFOCUS セキュリティセンターでは、カスタム属性にマッピングされた WebFOCUS グループに属するユーザは表示されません。
- セキュリティセンターの [グループの編集] ダイアログボックスで [参照] ボタンを使用しても、カスタム属性値は検索されません。ただし、属性値を手動で入力することは可能です。

外部認可の構成

外部認可の設定は、次の手順で構成されます。

1. WebFOCUS Reporting Server で、認可に使用する外部ソースのセキュリティプロバイダを構成します。セキュリティプロバイダとして、LDAP、Active Directory、またはカスタムプロバイダを使用することができます。カスタムプロバイダには、リレーショナルデータベース管理システム (RDBMS) や Web サービスでユーザを認可するプロバイダなどがあります。
2. WebFOCUS Reporting Server で外部認可を使用するよう WebFOCUS を構成します。
3. WebFOCUS Web アプリケーションを再起動します。
4. WebFOCUS グループを外部認可データにマッピングします。

手順　TIBCO WebFOCUS で外部認可を使用するよう構成するには

WebFOCUS で外部認可を使用するよう構成する前に、WebFOCUS Reporting Server で外部認可ソースをセキュリティプロバイダとして構成しておく必要があります。また、WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続を構成することを強くお勧めします。

セキュリティプロバイダについての詳細は、30 ページの「 TIBCO WebFOCUS Reporting Server でのセキュリティプロバイダの構成 」 を参照してください。トラステッド接続の構成についての詳細は、51 ページの「 WebFOCUS Client と TIBCO WebFOCUS Reporting Server 間のトラステッド接続を構成するには 」 を参照してください。

1. 管理コンソールの [セキュリティ] タブの [セキュリティの構成] フォルダ下で、[外部] をクリックします。
2. [外部セキュリティを有効にする] のチェックをオンにします。

   [外部] ページに、WebFOCUS Reporting Server に現在割り当てられている設定が表示されます。

3. [サーバ管理者 ID] テキストボックスに、WebFOCUS Reporting Server 管理者アカウントサービス名を「ProviderName¥serviceUserName」の形式で入力します。
4. [パスワード] テキストボックスに、セキュリティユーザに割り当てられているパスワードを入力します。
5. [接続] をクリックします。
6. 確認メッセージのダイアログボックスで [OK] をクリックします。
7. 認証中に WebFOCUS アカウントを Active Directory または LDAP ユーザの説明および Email で更新するには、[ユーザ情報を認証プロバイダと同期] のチェックをオンにします。
8. [ユーザ認可] グループで、[外部のみ] を選択して、認可タスクのすべてを外部プロバイダに割り当てるか、[外部と内部] を選択して、WebFOCUS と外部プロバイダ間で認可タスクを分担します。
9. 変更を保存します。
10. [セキュリティの構成] セクションで [保存] をクリックします。
11. 確認メッセージで [OK] をクリックします。
12. Web アプリケーションの再ロードを要求するメッセージで [OK] をクリックします。
13. 現在のセッションからログアウトします。
14. WebFOCUS Reporting Server を停止し、再起動します。
15. 管理者としてログインし、新しい構成をテストします。
16. 必要に応じて、新しい構成で発生する問題のトラブルシューティングのために、セキュリティトレースを有効にします。

    - WebFOCUS とともに Apache Tomcat をインストールした場合は、*drive*:¥ibi ¥WebFOCUS82¥webapps¥webfocus¥WEB-INF¥classes¥log4j.xml ファイルのバックアップコピーを作成し、log4j.xml ファイルを編集して、com.ibilog のレベル値を info から trace に変更します。
    - webfocus.war を使用して Web アーカイブから WebFOCUS Web アプリケーションを展開した場合は、元のディレクトリで log4j.xml ファイルを編集し、webfocus.war ファイルを再作成する必要があります。
    - 別の方法として、webfocus.war を使用して Web アーカイブから WebFOCUS Web アプリケーションを展開した場合は、拡張ディレクトリ内の展開先ディレクトリで、log4j.xml ファイルを編集することができます。このディレクトリの場所が不明な場合や、log4j.xml ファイルを変更するアクセス権限を所有していない場合は、Java アプリケーション管理者に確認してください。

17. Web アプリケーションを停止し、再起動します。

    注意：再起動する前に、必要に応じて、*drive*:¥ibi¥WebFOCUS82¥logs¥event.log ファイルを削除するか、名前を変更します。これにより、WebFOCUS が外部認可モードで再起動された際に、新しいログファイルが使用されます。

18. 作成済みのユーザアカウントを使用してログインします。

    ヒント：event.log ファイルには、WebFOCUS Reporting Server セキュリティプロバイダから取得した外部認可情報が記録されます。

    手順 16 でセキュリティトレースを有効にした場合、event.log の記録は次の例のようになります。

```
-WFRS.authenticate userName:userName
 - EDA.authConnect node:EDASERVE User:userID
security:EXPLICIT-DYNAMIC
 - EDA.authConnect node() provider:null reqName:userID
 - edaAuth for node:EDASERVE user:userID returned:1000
 - edaAuth for user:userID returned email:userEmail
 - edaAuth for user:userID returned description:userDescription userID
 - EDA.getGroupsForUser() node:EDASERVE userName:userID
 - EDA.getGroupsForUser() provider:null reqName:userID userID
 - group 1=#WF-ALL description=WF-ALL MAILING LIST userID
 - group 2=#SharePointSiteAdmins description=SharePoint AdminsuserID
 - group 3=#Summit_Lab_Staff description=#Summit_Lab Mailing List userID
 - group 4=CORP-WF-DEV description=WF Product Team userID
 - EDA.getGroupsForUser() from provider:null group count:4 userID
 - User:userID has 4 external groups
```

    ログインに失敗した場合は、[ルートユーザ] (IBI_Admin_Name) 設定で指定したアカウントで再度ログインします。

ここで、WebFOCUS グループを外部認可データにマッピングすることができます。

グループマッピング

マッピングは、外部グループメンバーシップ、外部ユーザプロファイルデータ、RDBMS に格納されたユーザ情報などの外部認可データを WebFOCUS グループに関連付けるプロセスです。外部認可は、次の情報に基づいて処理されます。

- LDAP (Lightweight Directory Access Protocol) をサポートする任意のディレクトリ (例、Microsoft Active Directory (AD)) から取得されたグループ、ロール、およびユーザプロファイル属性値。
- リレーショナルデータベース管理システム (RDBMS) から取得されたデータ。
- 任意の WebFOCUS Reporting Server データアダプタから取得されたデータ (例、Web サービスや ERP システムから取得された情報)。

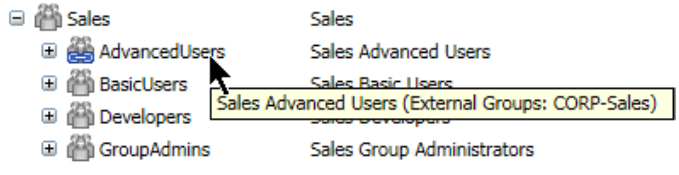
外部認可を使用するよう WebFOCUS を構成した場合、WebFOCUS グループのそれぞれは、マッピングされたグループまたはマッピングされていないグループのいずれかになります。

注意：WebFOCUS グループを外部認可データにマッピングするには、[Group Mapping (opExternalGroupMapping)] 権限が必要です。デフォルト設定では、この権限は Administrators グループのメンバーにのみ割り当てられています。

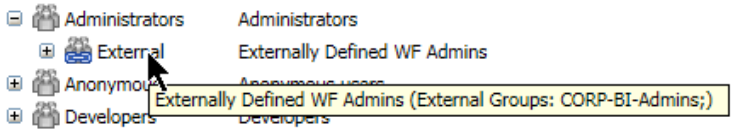
マッピングに使用する認可データは、セキュリティセンターで構成することも、Web サービスを使用して外部認可属性をプログラムで設定することもできます。Web サービスについての詳細は、『TIBCO WebFOCUS 埋め込みアプリケーションガイド』の「WebFOCUS RESTful Web サービス」セクションを参照してください。

マッピングは、WebFOCUS グループに設定されるプロパティの 1 つです。このプロパティ値は、外部ディレクトリ内の認可データ属性を指定する文字列です。WebFOCUS グループを複数の外部グループやロール属性値にマッピングするには、これらの値をセミコロン (;) で区切るか、複数の外部グループに一致するワイルドカード記号を使用することができます。たとえば、WebFOCUS グループを「SALES-*」にマッピングすると、その WebFOCUS グループが、「SALES-」で始まる外部グループすべてにマッピングされます。この文字列の最大文字数は、セミコロン (;) を含めて 2,000 バイトです。

セキュリティセンターでは、マッピングされたグループは、グループ名の横に表示された青色の鎖アイコンで識別されます。グループ名のツールヒントには、マッピングされている外部データまたはユーザ属性が表示されます。下図の構成では、Sales グループ下の「AdvancedUsers」という WebFOCUS グループが「CORP-Sales」という外部グループにマッピングされていますが、Sales グループ下のその他のサブグループはマッピングされていません。



WebFOCUS グループのメンバーを WebFOCUS 内部で定義し、かつセキュリティプロバイダの外部ソースでも定義する必要がある場合は、内部認可するメンバーにはマッピングされていないグループを使用し、外部認可するメンバーにはマッピングされたグループを使用することができます。下図の例では、WebFOCUS グループである Administrators グループ下の「External」というサブグループが、「CORP-BI-Admins」という外部グループにマッピングされています。

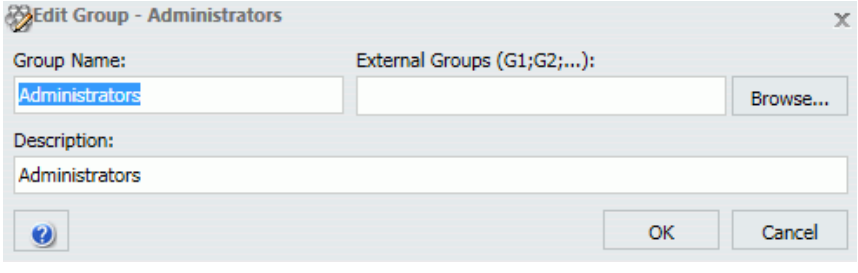


上記の親グループとサブグループのメンバーは、マッピングされていない親グループのセキュリティポリシーを共有しますが、これらのグループのメンバーシップはそれぞれ個別に管理することができます。

手順　TIBCO WebFOCUS グループを外部認可データにマッピングするには

1. [セキュリティセンター] で、外部グループにマッピングする WebFOCUS グループを選択し、[グループの編集] をクリックします。

   下図のように、[グループの編集] ダイアログボックスが表示されます。

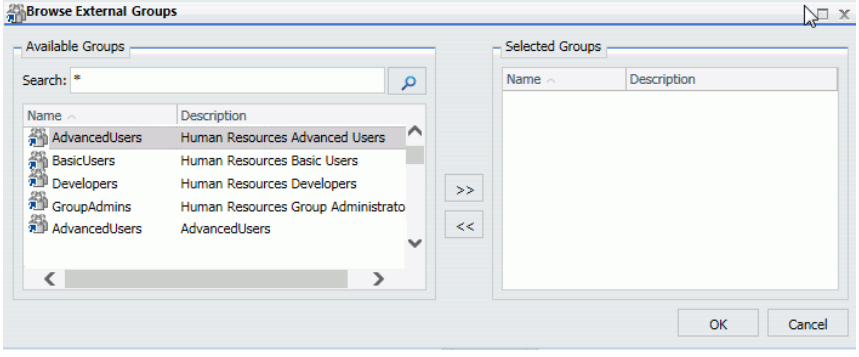


   ヒント：[参照] ボタンが表示されない場合は、外部認可を使用するよう WebFOCUS が構成されていません。外部認可の構成方法についての詳細は、336 ページの 「 TIBCO WebFOCUS で外部認可を使用するよう構成するには 」 を参照してください。

2. 外部認可に使用する属性値が分かっている場合は、その値を直接入力することができます。それ以外の場合は、[参照] をクリックします。

   注意：認可にカスタムユーザプロファイル属性を使用する場合は、その値を手動で入力する必要があります。

   下図のように、[外部グループの参照] ダイアログボックスが表示されます。



3. 検索語句を入力し、[検索] をクリックします。

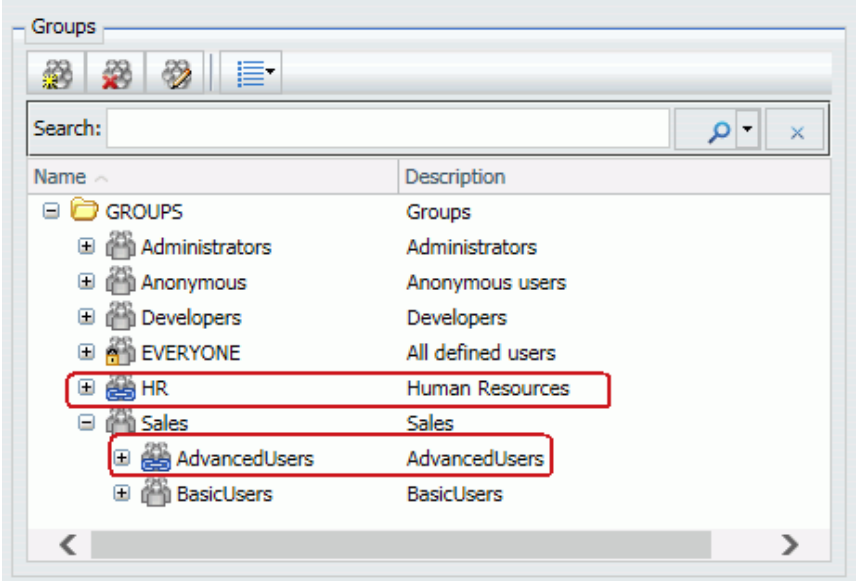
   注意：デフォルト設定では、プライマリセキュリティプロバイダのみを対象として検索が実行されます。セカンダリセキュリティプロバイダを対象としてデータを検索するには、クエリにそのプロバイダ名を含める必要があります。たとえば、セカンダリ PTH プロバイダの Sales グループを検索するには、「PTH¥*Sales」と入力して検索を実行します。すべてのセキュリティプロバイダを対象にグループを検索するには、「*¥*」と入力します。

4. WebFOCUS グループにマッピングする値を選択し、[OK] をクリックします。

   注意：複数の値を選択することもできます。

5. [グループの編集] ダイアログボックスに戻ると、選択した外部グループが [外部グループ] テキストボックスに表示されます。[OK] をクリックし、変更を保存します。

セキュリティセンターに戻ると、下図のように、マッピングされたグループの名前とリンクアイコンが表示されます。



グループ名の上にマウスポインタを置くとツールヒントが表示され、WebFOCUS グループ名の後に、マッピングされた外部認可データが括弧表記で示されます。

Microsoft Office ドリルダウンリンクに関する特別な考慮事項

ドリルダウンリンクのターゲットとして Microsoft Office 製品を選択すると、ドリルダウンに失敗します。これは、ターゲットに設定されたこれらの製品がブラウザの外部で起動されているためです。この場合、セキュリティコンテキストや以前に確立されたセッション関連の Cookie、およびこれらに基づくユーザ認可がターゲット製品で保持されません。

WebFOCUS バージョン 7.7 のドリルダウン機能は、Microsoft Office 製品で正常に機能していました。これは、ドリルダウンの匿名アクセスが許可されていたためです。WebFOCUS バージョン 8 でこの機能を有効にするには、組織で最適なオプションを次のいずれかから選択してください。

- Application Server のホストマシンのレジストリに ForceShellExecute サブキーを追加し、この値を 1 に設定します。

  このレジストリの変更により、Excel で使用されるデフォルト設定の URL 処理方法が上書きされ、WebFOCUS 外部で問題が発生します。

  レジストリの更新方法および Microsoft Office 製品のセッションに関連する動作についての詳細は、以下の Microsoft Office サポートサイトを参照してください。

  http://support.microsoft.com/kb/218153

- レポートのドリルダウンに必要な権限をパブリックユーザに与えるよう WebFOCUS セキュリティを構成します。

  このオプションでは、ドリルダウンリンクでターゲットに設定されたコンテンツをパブリックユーザが使用できるようにする必要があります。最低限必要なコンテンツセキュリティを保持したいユーザには、この設定はお勧めできません。

- ログインページで [ユーザを記憶する] 機能を有効にします。エンドユーザが [ユーザを記憶する] 機能を選択した場合、永続 Cookie が確立されます。

  [ユーザを記憶する] 機能ではログインの成功に一貫性がなく、永続 Cookie により新しいセッションが誤って作成される可能性があります。これにより、foccache ディレクトリに依存するアプリケーションで処理の問題が発生する場合があります。自動ログイン機能も、セキュリティを重視するユーザにとって許容できない脆弱性要因になる可能性があります。

- シングルサインオン (SSO) を IIS/Tomcat 統合 Windows 認証とともに使用します。ログイン認証情報の再ネゴシエーションが自動的に発生し、Excel レポートが正しく表示されます。

  SSO システムによって、ユーザが新しいセッションに自動的にログインされない可能性があります。また、新しい WebFOCUS セッションでは、foccache ディレクトリに依存するアプリケーションで問題が発生する可能性があります。

ReportCaster が別マシンにインストールされた TIBCO WebFOCUS 展開での特別な考慮事項

ReportCaster Distribution Server と WebFOCUS Client がそれぞれ異なるマシンにインストールされている場合に、管理コンソールで WebFOCUS 構成ファイルを更新すると、ReportCaster からその構成ファイルにアクセスできなくなります。WebFOCUS 構成の変更が ReportCaster にも反映されるようにするには、追加の構成手順を実行する必要があります。この追加手順は、外部認証または外部認可を構成する際に特に重要になります。これは、ReportCaster と WebFOCUS Client で同一のセキュリティ設定が使用されていない場合、ReportCaster ジョブが正しく実行されない場合があるためです。

手順 ReportCaster Distribution Server 設定が TIBCO WebFOCUS 設定に一致するよう構成するには

WebFOCUS 構成の変更が正しく動作することを確認した後、WebFOCUS がインストールされているマシンの構成ファイルを、ReportCaster Distribution Server がインストールされているマシンにコピーします。

1. WebFOCUS Client 設定を変更した場合は、WebFOCUS マシンの *drive*:¥ibi¥WebFOCUS82¥config¥webfocus.cfg ファイルを、ReportCaster マシンの *drive*:¥ibi¥WebFOCUS82¥config ディレクトリにコピーします。
2. WebFOCUS Reporting Server への WebFOCUS Client 接続の設定を変更した場合は、WebFOCUS マシンの drive:¥ibi¥WebFOCUS82¥client¥home¥etc¥odin.cfg ファイルを、ReportCaster マシンの drive:¥ibi¥WebFOCUS82¥client¥etc ディレクトリにコピーします。
3. リポジトリ設定を変更した場合は、WebFOCUS マシンの *drive*:¥ibi¥WebFOCUS82¥client¥etc¥install.cfg ファイルおよび webfocus.cfg ファイルを、ReportCaster マシンの *drive*:¥ibi¥WebFOCUS82¥client¥etc ディレクトリにコピーします。

   リポジトリ設定が install.cfg ファイルに格納されていない場合は、この手順を実行する必要はありません。
4. Distribution Server を再起動し、スケジュール済みジョブを実行して、期待どおりにジョブが実行されることを確認します。

5

TIBCO WebFOCUS 管理

ここでは、WebFOCUS で使用するセキュリティポリシーを作成、管理する方法について説明します。また、セキュリティの基本概念、リポジトリファイル構造、および WebFOCUS セキュリティモデルの基本要素についても説明します。これらの基本要素には、ユーザ、グループ、ロール、権限、リソース、セキュリティルール、セキュリティポリシーなどがあります。

トピックス

セキュリティ要件の評価

セキュリティポリシーを設計または実装する前に、組織のセキュリティ要件を明確にしておく必要があります。次の考慮事項は、検討項目の一部を示していますが、セキュリティ要件を明確にする上で役に立つ項目です。また、組織でカスタムポリシーを作成する場合でも、同梱されているリソーステンプレートを評価することで、ソフトウェアでどのようなセキュリティポリシーを設計できるかを見極めることもできます。

セキュリティポリシーの考慮事項は次のとおりです。

- どのユーザグループ間でレポート作成要件やアクセス要件が類似していますか。

多くの場合、これらのグループは、エンタープライズ展開では部門になり、SaaS 展開ではテナントになります。また、管理者グループや、レポートのスケジュールを一元的に管理するグループなど、リポジトリ内のすべてのリソースへのアクセス権限を所有する最上位グループが存在する場合もあります。

- ユーザはどのレポートツール、権限、ロールを必要としていますか。

  たとえば、独自のレポートを作成するユーザもいれば、作成済みレポートの実行のみを行うユーザもいます。ユーザがレポートをスケジュールできる場合でも、スケジュール機能のすべてを使用できるユーザもいれば、一部の機能のみを使用できるユーザもいます。マネージャには他のユーザが利用できない権限が必要です。

  注意：構造を複雑にすると、管理者によるシステム管理やユーザによるシステムの理解がより困難になります。ユーザや管理者の操作を簡素化するために、作成するロール数を制限することも必要になります。

- いくつの WebFOCUS 環境が必要ですか。環境ごとに要件が異なりますか。

  エンタープライズ展開では、多くの場合 WebFOCUS 実装の開発環境、テスト環境、実稼動環境が分離されますが、テスト環境および実稼動環境に開発者ロールが存在しない場合があります。一方、SaaS 展開では、テナント開発者が、組織で使用する新しいレポートコンテンツを実稼動環境で直接開発する場合もあります。

- WebFOCUS BI Portal 内でコンテンツを展開しますか。

  各部門またはテナントがそれぞれ独自のポータルを所有する場合もあれば、すべてのユーザが単一ポータルにアクセスする場合もあります。管理を容易にするには、1 つのエンタープライズポータルを作成し、一部のページをすべてのユーザに提供する一方、部門またはテナント専用のページを各組織のユーザのみに限定します。

- 集中型の管理モデルを使用しますか、または一部の管理権限をグループ管理者に委任しますか。

  たとえば、システム管理者がユーザをレポート作成ロールに割り当てる代わりに、販売グループ管理者にこの権限を委任することができます。

IBFS ファイルシステムとサブシステム

WebFOCUS では、リソースに関する情報は「WebFOCUS リポジトリ」と呼ばれるリレーショナルデータベースに格納されます。これらのリソースはすべて、IBFS ファイルシステム内で編成されています。IBFS は、オブジェクトの格納と取得に使用する論理アドレスシステムです。

階層構造の IBFS は、リポジトリ内でオブジェクトを容易に編成できるように、一連のサブシステムを基盤として構築されています。オブジェクトごとに一意の IBFS パスが存在します。IBFS パスは、グループメンバーシップの管理、ドリルダウンプロシジャへの参照の制御、特定のリソースへのユーザのアクセス権限の確認など、さまざまな目的で使用されます。特に、セキュリティルールでは IBFS パスが参照されます。これらのルールに基づいて作成されるセキュリティポリシーは、階層の IBFS パスを経由して下位に継承されます。つまり、サブシステムに新しいポリシーが明示的に適用されていない限り、サブシステムにはその親システムのポリシーが継承されます。

注意

- 次の文字を IBFS パス内に使用することはできません。

  ブランク、& * ( ) | : ; " , ?

- スラッシュ (/) はパス指定では有効ですが、フォルダや項目の名前に使用することはできません。

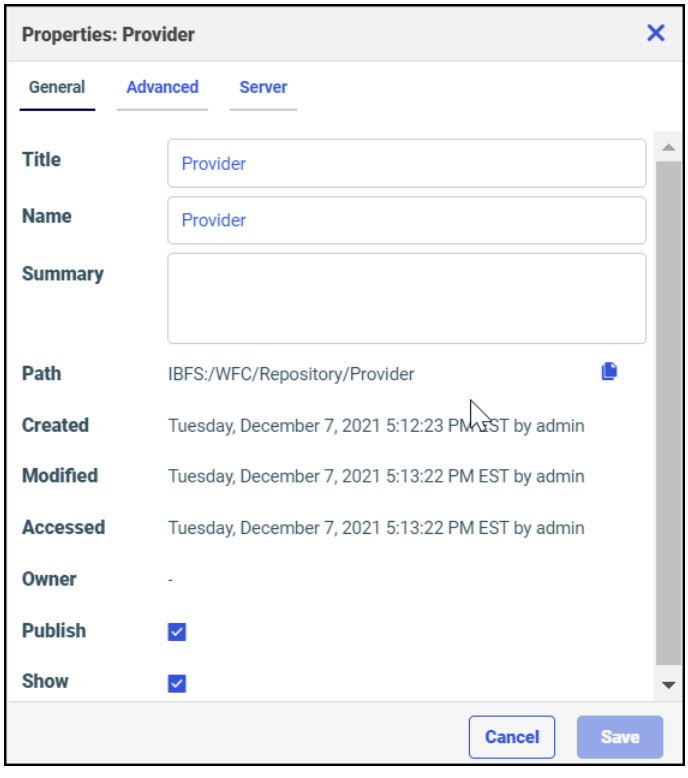
  新しいフォルダまたは項目を作成する際に、[タイトル] に禁止文字を使用すると、その文字が [フォルダ名] または [ファイル名] の名前から自動的に削除されます。

- UNIX または Linux 環境を使用する組織では、メタデータ、プロシジャなど WebFOCUS Reporting Server リソースのファイル名およびディレクトリ名を作成する場合に小文字を使用することをお勧めします。

- /bi という用語を主要エイリアスまたはコンテキストとして、または IBFS パス内で使用しないようにします。これは予約語であり、エイリアスまたはコンテキストとして使用すると、管理コンソールおよびセキュリティセンターの正しい表示ができなくなります。

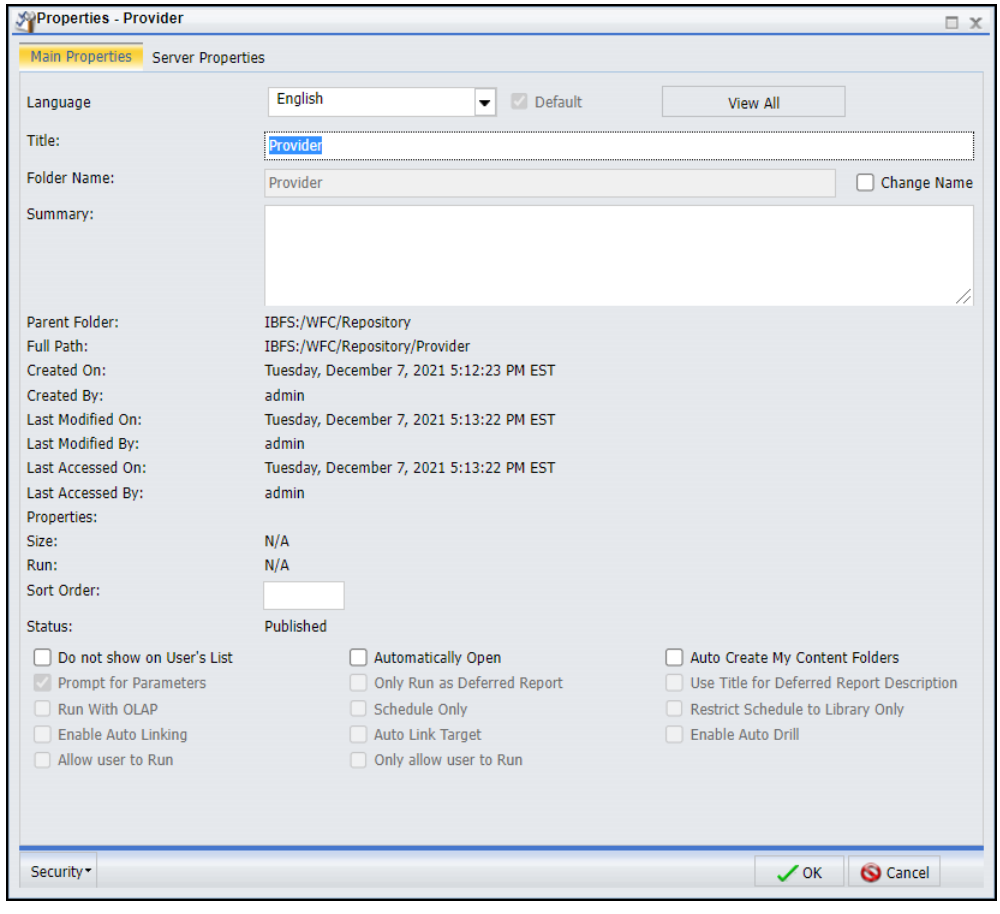
WebFOCUS Hub のビューまたは WebFOCUS ホームページを使用する場合、項目を右クリックし、[プロパティ] を選択して [プロパティ] パネルを開きます。

下図のように、オブジェクトの IBFS パスが [プロパティ] パネルの [パス] ラベルに表示されます。



レガシーホームページを使用する場合は、オブジェクトを右クリックして [プロパティ] を選択し、[プロパティ] ダイアログボックスを開きます。

下図のように、オブジェクトの IBFS パスが [プロパティ] ダイアログボックスの [フルパス] ラベルに表示されます。



レガシーホームページでは、BI Portal のリソースツリーのデフォルト表示形式は、[リポジトリ表示] です。この表示形式では、各要素がユーザフレンドリなラベルで表示されます。リソースツリーの IBFS サブシステムを表示するには、[ワークスペース] ノードを右クリックし、[表示]、[完全表示] を順に選択します。リポジトリ表示に戻すには、[TIBCO WebFOCUS] ノードを右クリックし、[表示]、[リポジトリ表示] を順に選択します。

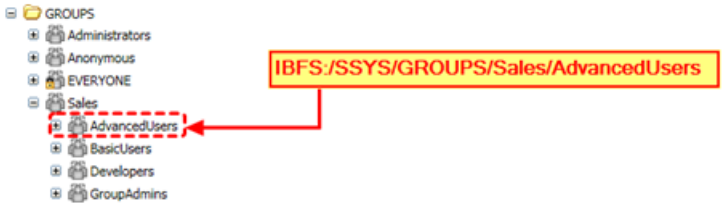
注意：カスタムリソーステンプレートの場合にのみ [完全表示] を使用します。その他すべての機能には、デフォルトの [リポジトリ表示] を使用します。

IBFS パスは、「IBFS:」というネームスペース指定で始まり、IBFS サブシステムが続きます。パス内に変数を使用すると、リソースを呼び出すユーザのワークスペース、フォルダ、グループ、言語に基づいて、関連するリソースが動的に選択されます。レポートプロシジャ、スケジュール、ReportLibrary コンテンツはすべて、WFC サブシステムに格納されます。

WFC サブシステム内のリソースには、名前およびタイトルが含まれています。名前はオブジェクトの IBFS 名を表し、タイトルはリソースツリーでの表示名を表します。

注意：リソースツリーに表示される [ワークスペース] ノードの IBFS 名は「ワークスペース」です。IBFS パスでは、このノードは IBFS:¥WFC¥Repository で参照されます。

USERS、GROUPS、ROLES サブシステムはすべて、SSYS サブシステム下で編成されています。下図のように、GROUPS サブシステムでは、サブグループが親グループにネストされているように、サブグループの IBFS アドレスに親グループの名前が含まれています。



上の例では、管理者が [Sales] グループ下に [AdvancedUsers]、[BasicUsers]、[Developers]、[GroupAdmins] サブグループを作成しています。AdvancedUsers の IBFS パスは、IBFS:/SSYS/GROUPS/Sales/AdvancedUsers です。

EDA および FILE サブシステムは、リポジトリ外部のリソースを参照します。EDA サブシステムにルールを設定して、ユーザグループに対して特定の WebFOCUS Reporting Server ノードを非表示にしたり、FILE サブシステムにルールを設定して、WebFOCUS ファイルシステムベースのリソース (例、WebFOCUS82¥cm 下の import および export ディレクトリ) へのアクセスにセキュリティを設定したりできます。

下図のように、ロールを作成または表示する際に、そのロールの権限ごとに [サブシステム] 列が表示されます。

[サブシステム] 列には、権限の適用先となるサブシステムが表示されるほか、その権限がセッション権限、ローカル権限、ハイブリッド権限のいずれに該当するかが示されます。

注意：[サブシステム] 列のアスタリスク (*) は、権限がすべてのサブシステムに適用されることを示しています。

IBFS パスでの変数の使用

ほとんどの IBFS パスは、リポジトリ内の単一エンドポイントを直接指定します。ただし、開発者は、すべてのユーザを対象とした単一リソースではなく、コンテキスト上適切なリソースに転送可能なポータルまたはその他アプリケーションのパスを作成する必要があります。

たとえば、ポータルの IBFS パスに変数を使用して、マルチテナントでカスタムスタイルを適用することができます。具体的には、同一の基本情報を利用する単一ポータルを作成し、組織に合ったロゴや配色を使用して、各テナントアプリケーションのユーザに配信することができます。

動的な IBFS パスに対応するには、リポジトリに一連の変数を追加します。これらの変数は、先頭に 2 つのシャープ記号 (##) を追加した場合に、グループ名やユーザ名などユーザが指定する値を置換します。これにより、変数が示すグループ、フォルダ、その他の特性の条件に適合したリソースに移動することができます。

次のような変数があります。

- **WF_MyContentFolder** 変数が、IBFS パスを呼び出したユーザの [MyContent] フォルダで置換されることを示します。
- **WF_PersonalFolder** 変数が、IBFS パスを呼び出したユーザの [UserInfo] フォルダで置換されることを示します。
- **WF_PrimaryGroup** 変数が、IBFS パスを呼び出したユーザがメンバーが属する最上位グループの名前で置換されることを示します。
- **WF_Language2** 変数が、IBFS パスを呼び出したユーザの 2 バイト文字 (大文字) 言語コードで置換されることを示します。

変数名では、大文字と小文字が区別されません。

手順 IBFS パスに変数を追加するには

実行時にユーザが示す特性によって異なるリソースへのパスを入力する必要がある場合は、次の手順をガイドラインとして使用します。たとえば、次の手順を使用して、マルチテナントグループで使用されるポータルの実行時に、各テナントグループが使用するロゴファイルまたは CSS テーマファイルを呼び出すためのパスを入力します。

1. パスは、「IBFS:/」で開始し、ワークスペースおよびフォルダの名前を入力します。各ワークスペースおよびフォルダはスラッシュ記号 (/) で区切り、実行時にユーザが指定する特性に依存するフォルダまたはその他のリソースを示すパスのレベルまで入力します。

   たとえば、「IBFS:/Sales/Month」と入力します。

2. ユーザが指定する特性によって異なるパスのレベルに達した場合、関連する変数を次のフォーマットで入力します。

   ```
   ##{variablename}
   ```

   説明

   `variablename`
   プロシジャまたはポータルを実行して IBFS パスを呼び出したユーザの特性を表す変数です。変数のリストについては、351 ページの 「 IBFS パスでの変数の使用 」 を参照してください。

   たとえば、「IBFS:/Sales/Month/##{WF_PrimaryGroup}」と入力します。

   注意：変数名では、大文字と小文字が区別されません。

3. このレベル以下で同一パスが使用される場合、変数からエンドポイントのリソース名までパスを継続します。

たとえば、「IBFS:/Sales/Month/##{WF_PrimaryGroup}/Hidden_Content/theme.css」と入力します。

4. パスをテストし、異なる認証情報のユーザが適切なリソースに移動できることを確認します。

セキュリティシステムの基本要素

セキュリティシステムの基本要素は、権限、リソース、ルールです。各ユーザのセキュリティポリシーは、各リソースでユーザに対して適用されるルールの組み合わせで決定されます。それぞれの状況で各ユーザに設定可能な権限は、ルールによって制御されます。たとえば、ユーザが特定のフォルダでリソースを編集する権限を所有している場合でも、別のフォルダではリソースの編集を行えない場合があります。

権限

ツールおよびリソースへのアクセスや、ユーザが実行可能な操作は、権限に基づいて制御されます。たとえば、次のリソースやツールへのアクセスは、それぞれ異なる権限で制御されます。

- プロシジャ、ReportLibrary コンテンツ、アクセスリスト、スケジュールなどのリソースを格納するフォルダ。
- プロシジャの実行、フォルダの削除などのコンテキストメニューオプション。
- メニューバーの [管理] および [ツール] メニューと、そのメニュー内に表示されるメニュー項目。
- ポータル、変更管理パッケージ、WebFOCUS Reporting Server などのリソースにアクセスするためのリソースツリーノード。
- エンタープライズ展開でのグループ管理者または SaaS 展開でのテナント管理者に対してセキュリティセンターに表示されるユーザリスト。

複数の類似した権限を 1 つのロールとして定義しておくと、セキュリティルールでそのロールが使用可能になります。権限およびロールは、ユーザやグループをリソースに関連付けるためのルールで使用されます。たとえば、基本ユーザに許可する権限がすべて含まれたロールや、開発者に許可する権限がすべて含まれたロールを作成します。

すべての権限のリストについては、643 ページの 「 権限 」 を参照してください。

権限のタイプ

ロールやルールを作成または変更する際は、関連する各権限がどのように機能するか、どのように使用されているか、どのリソースに適用されるかを理解しておくことが重要です。

ローカル権限

ローカル権限は、1 つまたは複数のサブシステムでユーザに割り当て可能な機能的権限を定義します。レポートの [実行] やフォルダの [削除] などのコンテキストメニューオプションを有効にするには、ローカル権限が使用されます。また、ローカル権限に基づいて、さまざまなツールに表示される項目が決定されます。たとえば、セキュリティセンターに表示されるユーザや、ReportCaster に表示されるスケジュールは、ローカル権限に応じて異なります。たとえば、グループ管理者が表示可能なユーザは、システム内のすべてのユーザではなく、管轄するグループ内のユーザのみに限定される場合があります。

ローカル権限は、サブシステム内の各レベルでユーザごとに評価されます。ユーザのローカル権限を特定のフォルダで許可する一方で、別のフォルダで拒否することもできます。たとえば、ユーザの [Access Resource] および [Run Procedures] 権限を [Sales] ワークスペースフォルダで許可し、これらの権限をサブフォルダで拒否することができます。このユーザは、[Sales] フォルダ内のレポートを実行することはできますが、このフォルダ下のサブフォルダを表示することも、サブフォルダ内のレポートを実行することもできません。ユーザが複数のグループに属している場合、特定のグループでローカル権限が許可される一方、別のグループで権限が拒否される場合もあります。その場合、このユーザの権限は拒否されます。

ローカル権限は、ツリーのコントロールやツールのユーザインターフェースなどの機能が表示される際に評価されます。ローカル権限に加えた変更は即座に反映されますが、変更を確認するためにインターフェースのリフレッシュまたは再ロードが必要になる場合があります。たとえば、特定のユーザに対して [Access Resource] 権限が [Sales] サブフォルダで拒否されていたが、今回の変更でこの権限が許可された場合、[Sales] サブフォルダを表示するために、このフォルダのリフレッシュが必要になる場合があります。

セキュリティセンターでは、ローカル権限の [サブシステム] 列には、1 つまたは複数の IBFS サブシステム名が表示されます。この列のアスタリスク (*) は、そのローカル権限をあらゆるサブシステムで使用できることを示しています。

セッション権限

セッション権限は、ログインプロセスでユーザに割り当て可能な機能的権限を定義します。メニューバーのドロップダウンリスト項目、リソースツリーのノード、およびその他のグローバルユーザ機能 (例、デスクトップ製品の多くのボタン) を有効にするには、セッション権限が使用されます。

セッション権限は、ログイン時にユーザごとに評価されます。この場合、[ワークスペース] ノード (WFC/Workspaces)、およびそのノード下の特定の深さまでのサブフォルダに設定されているルールが評価されます。この深さは、[セッション権限検索の深さ] (IBI_SESSION_PRIVILEGE_SEARCH_DEPTH) 設定で指定されます。この設定のデフォルト値は 1 です。この設定では、[ワークスペース] ノード直下のワークスペースフォルダのセッション権限のみが評価されます。

注意：[セッション権限検索の深さ] (IBI_SESSION_PRIVILEGE_SEARCH_DEPTH) 設定の値を増加させると、ユーザのログイン時に表示するリソースを取得するために、リポジトリ内でより深い検索が行われます。その結果、ログイン処理に要する時間が長くなる場合があります。パフォーマンスの問題を回避するには、[セッション権限検索の深さ] (IBI_SESSION_PRIVILEGE_SEARCH_DEPTH) 設定の値を 2 以下に設定することを強くお勧めします。[セッション権限検索の深さ] (IBI_SESSION_PRIVILEGE_SEARCH_DEPTH) 設定についての詳細は、538 ページの 「 BI Portal の設定 」 を参照してください。

セッション権限が競合する場合、たとえば、ユーザが 2 つのグループに所属し、一方のグループでセッション権限が許可されているが、他方のグループでそのセッション権限が拒否されている場合、ユーザにはそのセッション権限が許可されます。たとえば、ユーザが属する一方のグループで [Display Favorites Node] (opFavorites) 権限が許可されている場合、他方のグループでこの権限が拒否されている場合でも、ユーザはリソースツリーで [お気に入り] ノードを表示することができます。

注意：これは、ローカル権限が競合する場合と逆の結果です。ローカル権限が [許可する] と [拒否する] で競合する場合、その権限は [拒否する] として評価されます。

セッション権限に加えた変更は、ユーザの次回ログイン時に反映されます。

セキュリティセンターでは、セッション権限は [サブシステム] 列に「Session」と表示されます。

ハイブリッド権限

ハイブリッド権限は、ローカル権限とセッション権限の両方に該当する権限です。ハイブリッド権限は 2 つの目的に使用されます。1 つ目は一部のグローバル機能を有効にすること、2 つ目はオプションとしてサブシステム内のローカル機能を有効にすることです。

たとえば、ハイブリッド権限の [Run Procedures Deferred] には、「Session, WFC」と表示されます。このハイブリッド権限の一部であるセッション権限は、[ツール] メニューに [ディファードステータス] を表示するかどうかを決定する権限として使用され、ローカル権限は、[ワークスペース] ノード下のプロシジャのコンテキストメニューで [ディファード実行] オプションを有効にするかどうかを決定する権限として使用されます。

通常の展開では [セッション権限検索の深さ] (IBI_SESSION_PRIVILEGE_SEARCH_DEPTH) が 1 に設定されているため、ハイブリッド権限を含むルールは、少なくとも 1 つの最上位ワークスペースフォルダで「許可する」に設定する必要があります。ただし、別の最上位フォルダまたはサブフォルダでは、ハイブリッド権限のルールを「拒否する」に設定することも可能です。この構成により、ユーザがプロシジャをディファード実行できるのにも関わらず、その後でディファードリクエストの出力を取得できないという状況が回避されます。

セキュリティセンターでは、ハイブリッド権限には「Session」と表示される以外に、1 つ以上のサブシステム名が表示されます。

リソース

リソースとは、アクセスの制御や実行操作の許可の対象にすることが可能な、すべてのフォルダ、項目、ReportLibrary コンテンツ、ポータル、権限、レポートプロシジャ、ロール、ユーザ、グループのことです。

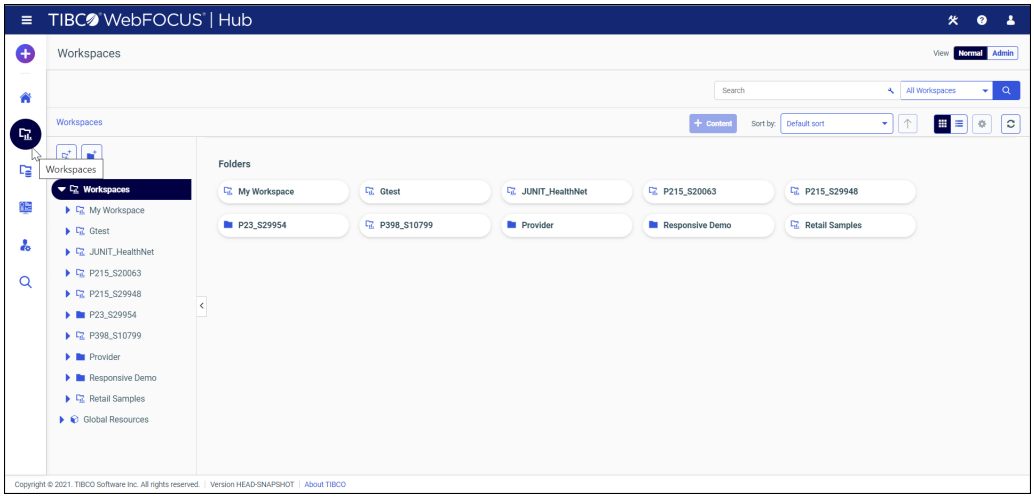
リソースタイプに応じて、制御される権限が異なります。たとえば、すべてのリソースタイプは削除の対象になり得ますが、レポートリクエストリソースをグループのメンバーにしたり、ユーザリソースを実行やスケジュールの対象にしたりすることはできません。

ユーザは、リソースツリーに表示された項目またはコンテンツエリアに表示された項目からリソースにアクセスできます。レガシーライセンスを使用するユーザの場合、製品にインストールされたライセンスキーに基づいて、ライセンスで管理されたコンポーネントが表示されます。

リソースコンポーネントの表示

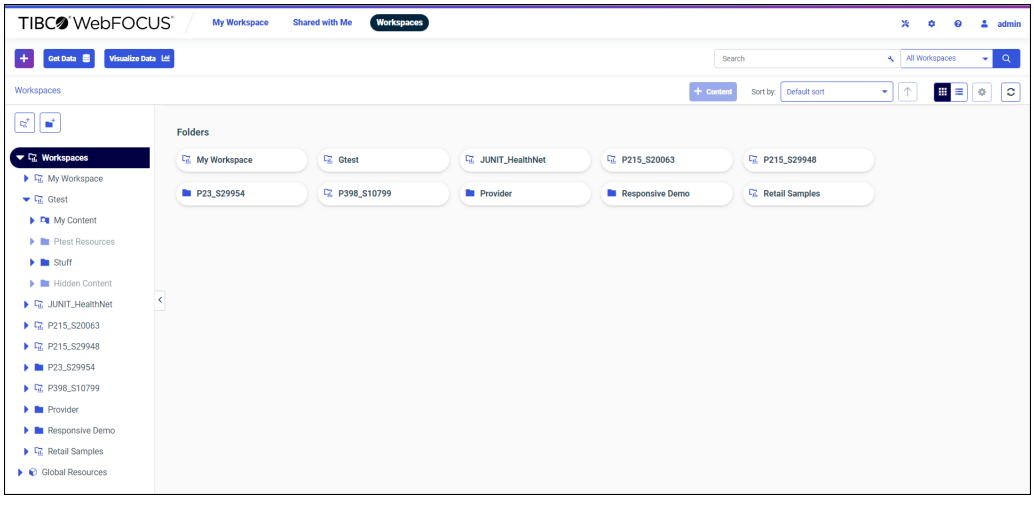
[ワークスペース] エリアには、ライセンスで管理されたコンポーネントがすべて表示されます。

WebFOCUS Hub から直接 [ワークスペース] エリアを開くには、下図のように、サイドナビゲーションウィンドウから [ワークスペース] を選択します。

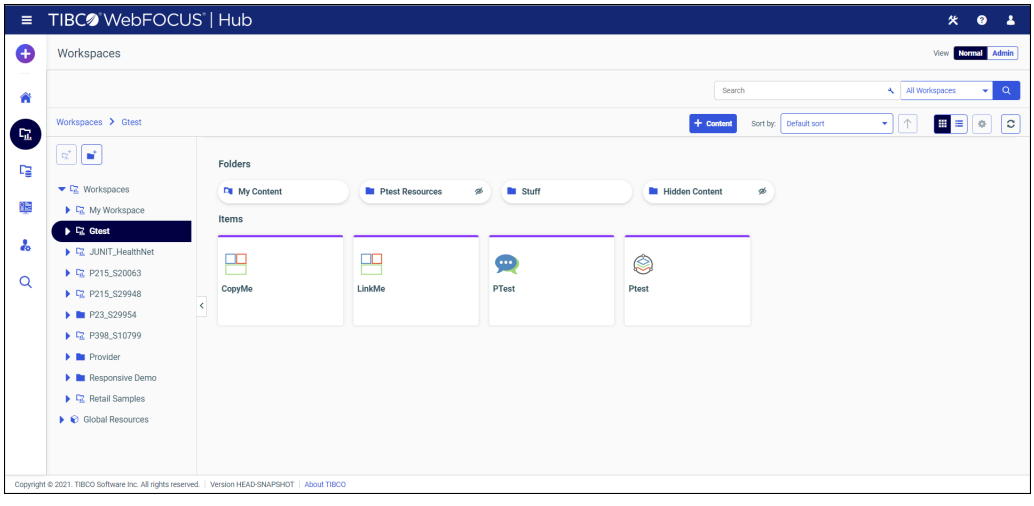


また、WebFOCUS ホームページから [ワークスペース] エリアを開くこともできます。この場合、下図のように、バナーの [ワークスペース] を選択します。

下図のように、WebFOCUS エクスプローラが開き、既存のワークスペースおよびフォルダへのリンクが表示されます。

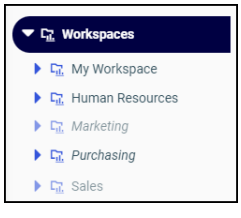


フォルダを開くと、下図のように、このフォルダに格納された項目が WebFOCUS エクスプローラに表示されます。



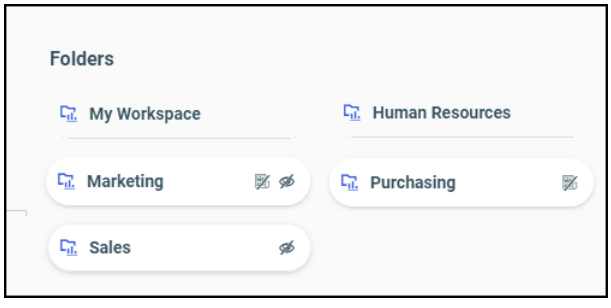
ビジュアルキューは、リソース項目のプライベート/公開済み、表示/非表示、共有/非共有のステータスを示します。[ワークスペース] エリアでは、表示リソースは、これらを使用してコンテンツを作成することができないユーザにも表示されます。非表示リソースは、このようなユーザにも表示されません。

リソースツリーでは、プライベートワークスペースは斜体で表示されます。公開済みワークスペースは斜体で表示されません。非表示ワークスペースは、淡色表示されます。表示ワークスペースは、淡色表示されません。下図は、これらのバリエーションを示しています。



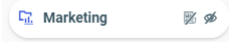
この例では、[Human Resources] エントリの表示には、淡色表示も斜体も使用されていません。この外観は、フォルダが公開済みで表示されることを示します。[Marketing] エントリの表示には、淡色表示と斜体が使用されています。この外観は、フォルダがプライベートで非表示であることを示します。[Purchasing] エントリの表示には、淡色表示は使用されていないが斜体が使用されています。この外観は、フォルダがプライベートだが表示されることを示します。[Sales] エントリの表示には、淡色表示が使用されているが斜体は使用されていません。この外観は、フォルダが公開済みだが非表示であることを示します。

コンテンツエリアでも、同じように状態に応じて項目の外観が変わります。プライベートフォルダにはプライベートアイコンが表示されます。 プライベートアイコンには、公開書類と取り消し線 が描画されます。公開フォルダには、このアイコンは表示されません。 非表示フォルダには非表示アイコンが表示されます。 非表示アイコンには、目と取り消し線 が描画されます。表示フォルダには、このアイコンが表示されません。 下図は、これらのバリエーションを示しています。

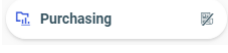


この例では、[Human Resources] フォルダ 

にはアイコンが表示されていません。 これは、フォルダが公開済みで表示されることを示します。

[Marketing] フォルダ 

には非表示とプライベートのアイコンが表示されています。 これは、フォルダがプライベートで非表示であることを示します。

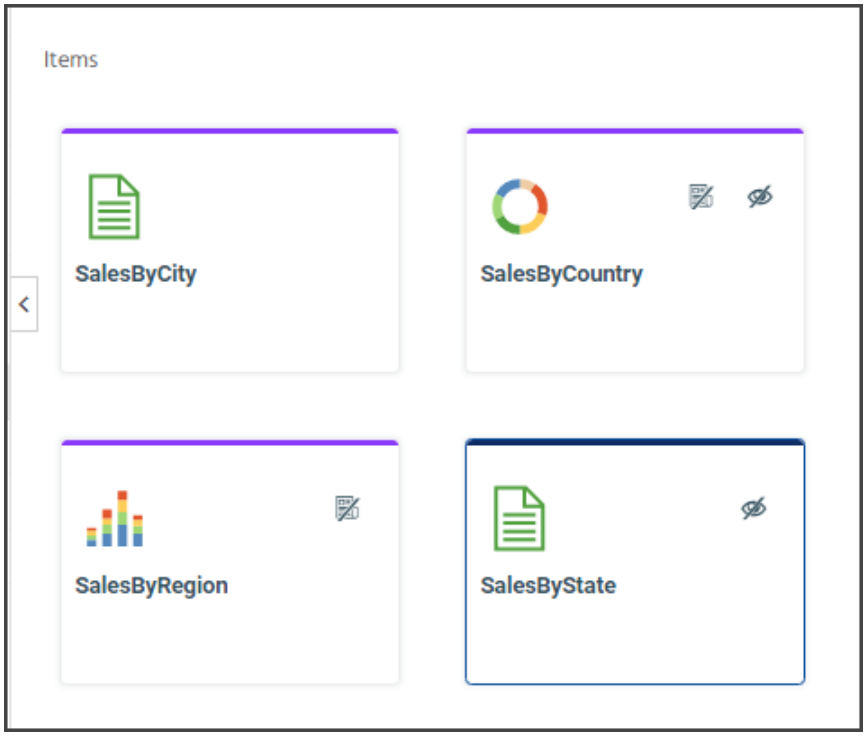
[Purchasing] フォルダ 

にはプライベートアイコンが表示されています。これは、フォルダがプライベートで表示されることを示します。

[Sales] フォルダ 

には非表示アイコンが表示されます。 これは、フォルダが公開済みで非表示であることを示します。

下図のように、フォルダ内の項目にも同じようなビジュアルキューが適用されます。



この例では、[SalesByCity] レポートのタイルには、レポートのサムネール以外のアイコンは表示されていません。この外観は、レポートが公開済みで表示されることを示します。

[SalesByCountry] グラフのタイルには、プライベートアイコンおよび非表示アイコンが表示されています。プライベートアイコンには、公開書類と取り消し線が描画されます。 非表示アイコンには、目と取り消し線が描画されます。 この外観は、グラフがプライベートで非表示であることを示します。

[SalesByRegion] 項目のタイルには、グラフサムネール横にプライベートアイコンのみが表示されています。この外観は、グラフがプライベートで表示されることを示します。

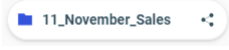
[SalesByState] 項目のタイルには、レポートサムネール横に非表示アイコンのみが表示されています。この外観は、レポートが公開済みだが非表示であることを示します。

リソースを右クリックすると表示されるオプションは、ユーザの権限および項目のステータスに基づきます。公開済みの項目を右クリックした場合、[非公開] オプションが表示されます。項目がプライベートの場合、[公開] オプションが表示されます。

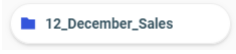
また、[プロパティ] ダイアログボックスから項目の公開または表示ステータスを確認することもできます。項目を開くには、リソースツリーまたはコンテンツエリアで項目を右クリックし、[プロパティ] を選択します。項目が公開済みの場合は、[公開] 設定で [はい] オプションが選択され、項目がプライベートの場合は [いいえ] オプションが選択されています。同じように、項目を使用したコンテンツの作成ができないユーザにも項目が表示される場合は、[表示] 設定で [はい] オプションが選択され、このようなユーザには項目が表示されない場合は、[いいえ] オプションが選択されています。

[マイコンテンツ] フォルダまたはそのサブフォルダ内のプライベートフォルダおよびリソースは共有することができます。これらのフォルダのコンテンツエリア内で、共有リソースは共有アイコン で識別されます。

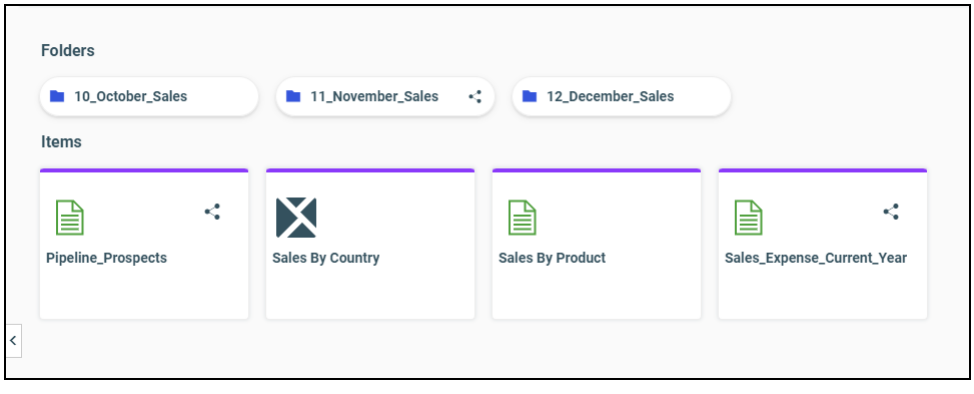
共有されるリソースのアイコンには、このアイコンが重ねて表示されます。



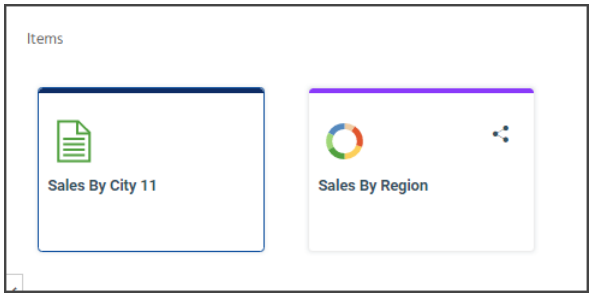
非共有リソースのアイコンには、このアイコンが重ねて表示されません。



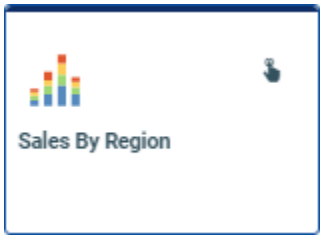
このアイコンの重ね合わせは、フォルダにも個別項目にも適用されます。下図のように、[11_November_Sales] フォルダ、[Pipeline_Prospects] レポート、[Sales_Expense_Current_Year] レポートはすべて共有されています。



下図のように、[SalesByRegion] グラフは共有されていますが、[SalesByCity] レポートは共有されていません。



注意：下図のように、インサイト実行用に構成されたリソースを表すタイルには、インサイト実行アイコンも表示されます。



インサイト実行アイコン は、ボタンまたは画面上のオプションを選択する人差し指を表します。詳細は、『TIBCO WebFOCUS 利用ガイド』を参照してください。

ユーザおよびグループリソース

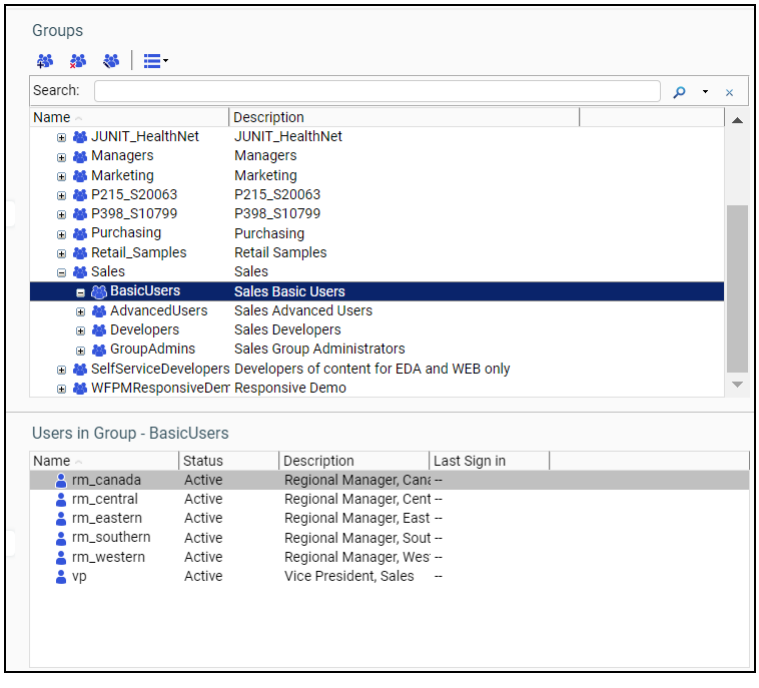
ユーザは、一意の ID で識別されます。また、ユーザの説明、Email アドレス、パスワード、グループメンバーシップ、ステータス (アクティブ、非アクティブ、AUTOADD) などのプロパティを追加することもできます。グループは、類似した権限や同一リソースへのアクセス許可をすべてのメンバーが必要とする複数のユーザまたはサブグループで構成されます。すべてのユーザは、EVERYONE グループのメンバーになります。このグループには、システム内で定義されたすべてのユーザが属しています。

注意：マルチテナント SaaS 展開では、テナントユーザはサービスプロバイダユーザとともに EVERYONE グループに属しますが、各テナントユーザが認識できる他のユーザは、ユーザ自身の組織内のユーザに限られます。

明示的グループと暗示的グループ

ユーザが割り当てられたグループは、「明示的グループ」と呼ばれます。すべてのユーザは EVERYONE グループに属しているため、各ユーザには常に少なくとも 1 つの明示的グループが存在します。グループを別のグループにネストして階層構造にすることで、管理を容易にすることもできます。階層構造でサブグループが親グループにネストされている場合、サブグループのメンバーであるユーザは、親グループのメンバーであると見なされます。この場合、サブグループはそのメンバーの明示的グループであり、親グループは暗示的グループになります。

下図では、Sales グループは暗示的グループで、Sales グループ下の BasicUsers グループは明示的グループです。



セキュリティルールは、明示的グループと暗示的グループの両方に適用されます。つまり、暗示的グループに適用されたルールは、そのグループにネストされた明示的グループにも適用されます。

注意：マルチテナント SaaS 展開では、EVERYONE グループおよびそのメンバーは、テナントユーザには表示されません。

プライベートリソースと公開済みリソース

ポータル、レポート、プロシジャなどのコンテンツリソースは、プライベートまたは公開済みのいずれかになります。プライベートコンテンツは、そのコンテンツのオーナーと、共有が許可されたユーザのみに表示されます。公開済みコンテンツは、許可されたユーザと共有することもできますが、公開済みコンテンツへのユーザアクセスは、ユーザの判断で共有するかどうかを決定するのではなく、ルールによって制御されます。公開済みコンテンツは、信頼性のあるコンテンツと見なされます。通常、公開済みコンテンツは、品質保証の検査とテスト後にユーザコミュニティに公開されます。

プライベートリソース

すべてのリソースは、初期状態ではプライベートリソースとして作成されます。プライベートリソースのセキュリティポリシーでは、次のことが規定されます。

- リソースのオーナーは、そのリソースを作成したユーザです。
- リソースは、その親リソースからセキュリティポリシーを継承しません。
- オーナーは、リソースに対してフルコントロールを所有します。
- オーナーが属するグループに対して Manage Private Resources 権限を持つ管理者は、そのオーナーのリソースを管理することができます。これにより、無効なユーザまたは削除済みユーザがリソースを所有する場合でも、管理者がそのユーザのリソースを管理することが可能になります。たとえば、リソースの削除、リソースの公開、他のユーザやグループへのオーナーシップの移動などの操作を行えます。
- プライベートリソースは、グループまたはユーザがそのオーナーになることができますが、複数のオーナーがそのリソースを同時に所有することはできません。プライベートリソースのオーナーがグループの場合、権限を所有するユーザ (例、オーナー、権限を持つ管理者) はオーナーシップをユーザからグループに移動する必要があります。

プライベートコンテンツには、次のような形態があります。

マイコンテンツ
: ユーザが作成したレポート、出力、スケジュールです。このコンテンツは、ユーザ専用のプライベートコンテンツとして保持されます。ただし、共有権限を持つユーザがコンテンツを他のユーザと共有したり、ユーザのプライベートコンテンツを管理できる管理ユーザがコンテンツを公開したりした場合を除きます。

その他のプライベートコンテンツ
: プライベートコンテンツの中には、特定の開発者グループのみがアクセス可能なコンテンツや、公開用に準備されているコンテンツがあります。これにより、新しいコンテンツが実稼動環境で作成された場合でも、そのコンテンツを公開前にテストすることが可能になります。その典型的な例として、テナント開発者が単一環境のみにアクセスできる SaaS 展開があります。

ユーザがプロシジャやレポートなどの項目を保存するために、[マイコンテンツ] フォルダが自動的に作成されます。親フォルダで [[マイコンテンツ] フォルダの自動作成] プロパティを有効にしておくこと、およびユーザが [My Content Folder] 権限を所有していることが必要です。

注意：このプロパティは、[コンテンツ] ノード (WFC¥Repository) 下の最上位フォルダでのみ設定することをお勧めします。

公開済みリソース

権限を所有するユーザは、プライベートコンテンツを公開することで、正式なコンテンツとして多くのユーザに提供することができます。公開済みリソースのセキュリティポリシーでは、次の条件が規定されます。

- 公開済みリソースのオーナーはシステムです。
- 公開済みリソースには、その親フォルダで定義されたセキュリティポリシーが適用されます。

共有リソース

共有とは、ユーザが [マイコンテンツ] フォルダ内のプライベートコンテンツを、許可されたユーザと共有する際に一般に使用される機能です。

共有されたリソースは、専用の [共有コンテンツ] フォルダから他の適切なユーザにも利用可能になります。[共有コンテンツ] フォルダは、フォルダ内に共有コンテンツが存在する場合に、自動的に表示される仮想フォルダです。

オーナーがリソースを共有できるユーザおよびグループは、[Content Sharing Scope] 権限に基づいて決定されます。また、コンテンツオーナーには、次の 1 つまたは複数の権限が付与されている必要があります。これらの権限は、[ロール] ダイアログボックスの [Advanced Reporting] フォルダ下にあります。

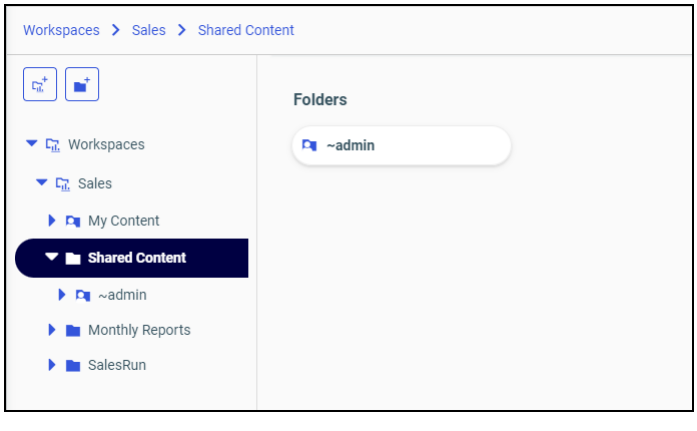
`Share Private Resources`
: ユーザは、リソースのコンテキストメニューから [共有] を選択することで、そのリソースを共有することができます。リソースは、格納先のフォルダにアクセス可能なすべてのユーザと共有されます。これは、ReportLibrary コンテンツには適用されません。

`Share Private Resources with Specific Users`
: ユーザは、リソースのコンテキストメニューから [共有の設定] を選択し、利用可能なユーザ、グループ、またはその両方のリストから共有相手を選択することで、そのリソースを共有することができます。これは、ReportLibrary コンテンツには適用されません。

`Share Private Library Content`
: ユーザは、ReportLibrary コンテンツを共有することができます。

[マイコンテンツ] フォルダまたはそのサブフォルダのプライベートリソースを共有するには、次の 2 つの方法があります。[共有する] メニューオプションを使用して、すべてのユーザとリソースを自動的に共有することも、[共有の設定] メニューオプションを使用して、[共有の設定] ダイアログボックスから特定のユーザまたはグループとリソースを共有することもできます。[共有する] オプションを使用する場合、リソースは EVERYONE グループと共有され、すべてのユーザに一般ユーザ権限が与えられます。[共有の設定] オプションを使用する場合、リソースは限られたユーザおよびグループとのみ共有され、リソースが表示されるワークスペースで設定されたロールに基づいて権限が与えられます。[共有する] オプションを使用して、作成中のリソースを一般に利用できるようにすることも、[共有の設定] オプションを使用して、リソースを一般には利用できるようにせず、リソースの作成タスクを特定のユーザと共有することもできます。

[マイコンテンツ] フォルダまたはその下位フォルダのリソースを共有する場合、作成者以外のすべてのユーザには、[共有コンテンツ] フォルダにこれらのリソースが表示されます。[共有コンテンツ] フォルダを開くと、コンテンツを共有したユーザごとにサブフォルダが表示されます。この機能により、ユーザ自身が作成して [マイコンテンツ] フォルダに表示されるコンテンツと、別のユーザが作成して共有されたコンテンツを識別することができます。下図では、管理者が各ユーザの使用を許可したコンテンツを格納する [Administrator] フォルダが、[共有コンテンツ] フォルダ下に表示されています。これは、コンテンツ表示に表示されます。



共有による階層内のフォルダおよびリソースへの影響の理解

共有リソースへの適切なアクセスの付与を継続しながら、ワークスペース内の非共有リソースの完全性を保持するため、リソースが格納されたフォルダおよび上位フォルダでは、その共有ステータスが自動的に調整されます。

フォルダ内のリソースを共有する場合、このフォルダおよびその上位フォルダは [マイコンテンツ] まですべて自動的に共有されます。この自動更新により、新しく共有されたリソースが共有フォルダに格納されていない場合も使用できるようになります。階層内でフォルダを共有する場合も同じ動作が発生します。共有フォルダの上位フォルダは [マイコンテンツ] フォルダまですべて自動的に共有されます。この動作により、階層内の非共有フォルダによって、その下位の共有フォルダまたはフォルダ内のリソースへのアクセスがブロックされることを自動的に回避します。

共有後にフォルダの共有を解除する場合、表示されるフォルダの非共有ステータスに従って、フォルダ内の共有リソースの共有も自動的に解除されます。階層内の上位フォルダの共有を解除する場合も同じ動作が発生します。新しく共有が解除されたフォルダ下のフォルダおよびリソースもすべて自動的に共有が解除されます。この動作により、非共有フォルダ内のすべてのフォルダおよびリソースが使用できなくなり、フォルダとそのフォルダ内のリソースを他のユーザに使用不可にする決定が強化されます。

共有の解除後に再度フォルダを共有する場合、このフォルダ内のリソースは自動的に共有されません。この場合、フォルダを開き、このフォルダ内のリソースを個別に共有にする必要があります。共有の解除後に階層内の上位フォルダを共有する場合も同じ動作が発生します。再度共有されたフォルダ内のフォルダおよびリソースはいずれも、自動的に再度共有されることはありません。ユーザは、これらを開いて個別に共有する必要があります。ただし、同一階層内でリソースを共有する場合は、このリソースを格納するフォルダおよび上位フォルダもすべて自動的に共有されます。この動作により、同一フォルダ内で共有リソースと非共有リソースを保持することができ、共有フォルダ内に格納された場合も非共有リソースを使用不可として維持することができます。

共有フォルダ内の各リソースの共有を解除する場合、表示されるフォルダの共有が自動的に解除されることはありません。この場合、フォルダ全体の共有を解除するまでフォルダは共有され続けます。この機能により、フォルダ内の 1 つまたは複数のリソースの共有が解除された場合も、フォルダは共有リソースへのアクセスを継続的に提供することができます。階層内のフォルダの共有を解除した場合も同じ動作が発生し、このフォルダの上位フォルダは、ユーザがこれらのフォルダの共有ステータスを個別に変更するまで共有され続けます。

原則として、リソースまたはフォルダを共有すると、その上位フォルダも自動的に共有されます。フォルダの共有を解除すると、その下位フォルダおよびリソースの共有も自動的に解除されます。この原則の唯一の例外は、最下位の個別リソースまたはフォルダです。これらの項目の共有を解除した場合、階層内のどこにも影響は及びません。

個別リソースを共有すると、このリソースの共有を解除するか、このリソースが格納されたフォルダまたは上位フォルダの共有を解除するまで共有され続けます。フォルダを共有すると、このフォルダまたは上位フォルダの共有を解除するまで共有され続けます。個別リソースは、格納されるフォルダの共有を解除せずに共有を解除することができます。この動作により、共有が解除されたリソースを含むフォルダに格納されている場合も、共有リソースは継続して使用することができます。

リソースの共有

プライベートリソースの共有または共有の解除機能は、ワークスペースの [マイコンテンツ] フォルダまたは [マイコンテンツ] フォルダ内の下位フォルダのいずれかに格納されたリソースにのみ適用されます。

ルール

ユーザが特定の場所で実行できる操作、および実行できない操作は、ルールに基づいて決定されます。ルールを使用することで、特定のリソースに対象 (ユーザまたはグループ)、ロール、アクション (例、[許可する]、[拒否する])、適用先 (例、[フォルダのみ]、[下位のみ]、[フォルダと下位]) が関連付けられます。これらのルールに基づいて、ロール内のさまざまな権限がユーザに許可されたり、拒否されたりします。

注意: 通常、ルールの適用対象はグループです。ルールは単一ユーザに直接適用することもできますが、ユーザ単位でのルールの管理は複雑になるため、この方法はお勧めしません。

有効なポリシー

ユーザが特定のツール、リソース、機能にアクセスできるかどうかは、ルールの組み合わせに基づいて決定されます。複数のグループに属するユーザは、一方のグループで特定のツールの使用が許可され、他方のグループでそのツールの使用が拒否される場合があります。フォルダにはルールが明示的に適用されていない場合がありますが、ルールはその親フォルダから継承されます。ユーザがリソースにアクセスする際に、関連するセキュリティルールがすべて評価され、これらのルールを組み合わせた結果が、そのリソースに対するユーザのルールとして決定されます。この結果が、そのリソースに対するユーザの有効なポリシーです。

特定の対象およびリソースに関連するルールには、次のものがあります。

- ユーザが属する明示的および暗示的なグループに関連して、リソースに適用されているルール。
- ユーザアカウントに直接関連して、リソースに適用されているルール。
- ユーザまたはグループに関連して、リソースの親に適用されているルールから継承されたルール。

ユーザが何らかの理由で特定の機能にアクセスできない場合は、ユーザの有効なポリシーを確認することで、トラブルシューティングに役立てることができます。

優先順位

複数のルール間の競合は、優先順位に基づいて解決されます。優先順位は次のとおりです (上位から下位の順)。

- 継承のクリア
- 最上級の許可
- 拒否する
- 許可する
- 設定しない

一般に、ルールは権限を許可するために使用します。これは、デフォルト設定では権限は許可されていないためです。権限を [許可する] または [最上級の許可] に設定して明示的に許可しない限り、その権限は拒否されます。デフォルト設定では、権限は [設定しない] に指定されています。これは、許可されていないことを意味します。ユーザの特定のリソースに対する権限がルールで許可されている場合でも、別のルールでその権限が拒否されている場合、一般にその権限は拒否されます。ただし、後述のように、セッション権限に関しては取り扱いが異なります。[許可する] ルールは [設定しない] ルールより優先されるため、[許可する] に設定すると、有効なポリシーでその権限が許可されます。[拒否する] ルールは [許可する] ルールより優先されるため (セッション権限を除く)、[拒否する] に設定すると、有効なポリシーでその権限が拒否されます。[最上級の許可] ルールは [拒否する] ルールより優先されるため、[最上級の許可] に設定すると、有効なポリシーでその権限が許可されます。

特定のグループが別のグループに優先することはなく、またユーザのルールがグループのルールに優先することもありません。ユーザが属するグループで権限が [拒否する] に設定されているが、その権限を特定のユーザのみに [許可する] に設定したい場合、選択したリソースに対してそのユーザの権限を許可するルールを作成するだけではその権限は許可されません。これは、ユーザの有効なポリシーが、ユーザの権限を許可するルールより、ユーザの属するグループの権限を拒否するルールを優先的に評価して決定されるためです。この場合、ユーザの権限を [最上級の許可] に設定するルールを作成する必要があります。[最上級の許可] ルールはグループの権限の [拒否する] ルールより優先されるため、そのユーザのみに権限が許可されます。

通常、[最上級の許可] ルールは、特別な状況に対処するために使用します。たとえば、特定のリソースへのアクセス権限がグループで拒否されているが、そのグループに属するメンバーがそのリソースにアクセスする必要がある場合です。[最上級の許可] ルールを使用する別の状況として、他のルールが適用されているかどうかに関係なく、特定のグループに権限を常に許可する場合があります。たとえば、WebFOCUS には、Administrators グループのメンバーに SystemFullControl ロールを [最上限の許可] で許可するルールが組み込まれています。このルールにより、IBFS:/ リソース (システムリソース全体) の [フォルダと下位] を対象としてアクセスが許可されます。このルールは、EVERYONE グループに [拒否する] ルールが適用された場合でも、管理者がシステム内のリソースの制御を失わないようにするための予防手段です。

[継承のクリア] ルールに設定すると、リソース上でロールに継承されているルールがすべて取り消され、そのリソースに対するアクセスが [設定しない] に変更されます。ユーザが複数のロールに属しており、それらのロールで権限が重複している場合、クリアされたロールで共有されていた権限はすべて、[設定しない] として評価されます。

セッション権限では、メニューバーのドロップダウンリスト項目、リソースツリーのノード、およびその他のグローバルユーザ機能 (例、デスクトップ製品の多くのボタン) が有効になります。セッション権限は複数の場所で必要になる各種ツールへのアクセスを制御するため、セッション権限が一方のルールで拒否されている場合でも、他方のルールで許可されていれば、そのセッション権限は許可されます。たとえば、[Sales] フォルダでプロシジャのディファード実行が許可されているユーザは、[Finance] フォルダでディファード実行が拒否されている場合でも、[Sales] フォルダから実行されたディファードレポートを表示するために [ディファードステータス] インターフェースにアクセスする必要があります。

手順　リソースに対するユーザの有効なポリシーを表示するには

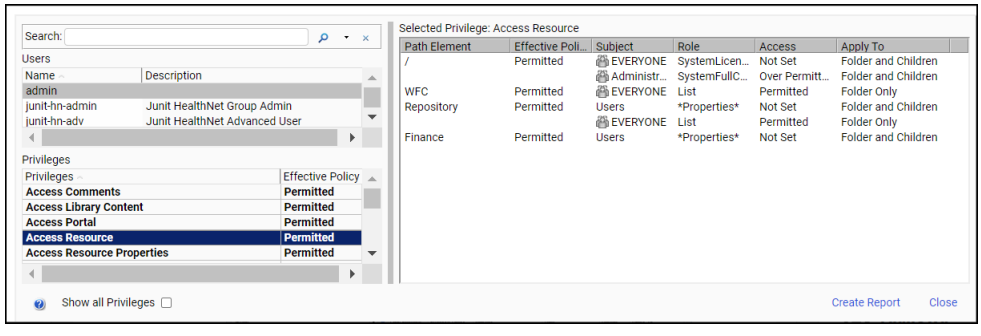
[有効なポリシー] ダイアログボックスには、ユーザに特定の実行権限が許可または拒否されている理由が示されています。別のユーザの有効なポリシーを表示するには、次の権限が付与されている必要があります。

- View Rules on a Resource (opViewRulesOn) - [セキュリティ] コンテキストメニューに、[このリソースのルール] および [有効なポリシー] オプションを表示します。
- Manage Rules on Resources (opManageRulesOn) - [セキュリティ] コンテキストメニューに、[ルール] オプションを表示します。

[View Rules on a Resource] 権限のみを所有するユーザは、特定のリソースに対して、そのユーザ自身に関連する有効なポリシーのみを表示することができます。ユーザが適切な権限を所有していない場合、ルールおよび有効なポリシーを表示または管理するオプションはコンテキストメニューに表示されません。

1. リソースを右クリックし、[セキュリティ]、[有効なポリシー] を順に選択します。

   [有効なポリシー] ダイアログボックスが開き、選択したリソースに対するルールの権限ごとに、評価された有効なポリシーが表示されます。



   ユーザが適切な権限を所有している場合、[ユーザ] ドロップダウンリストから別のユーザを選択して、そのユーザの有効なポリシーを表示することができます。

2. 選択したリソースに対してこのユーザに関連する権限すべて (このリソースに適用されていない権限を含む) の有効なポリシーを表示するには、[すべての権限を表示] のチェックをオンにします。

3. 権限の有効なポリシーの評価結果を表示するには、[権限] ボックスでその権限を選択します。

   [有効なポリシー] ダイアログボックスには、ユーザが属するグループすべてを対象に、選択したリソースより上位すべての階層レベルのポリシー評価結果が表示されます。レベルごとに表示される情報には次のものがあります。

   - パス要素
   - 有効なポリシー. - 適用されたすべてのルールの組み合わせに基づいてこのフォルダに設定されたアクセスです。
   - 対象
   - ロール
   - アクセス - この階層レベルに直接適用されたルールに基づいてこのフォルダに設定されたアクセスです。

- ❑ 適用先 - ポリシーは、パス要素のみのフォルダに適用される場合もあれば、パス要素のフォルダとその下位、またはフォルダの下位のみに適用される場合もあります。

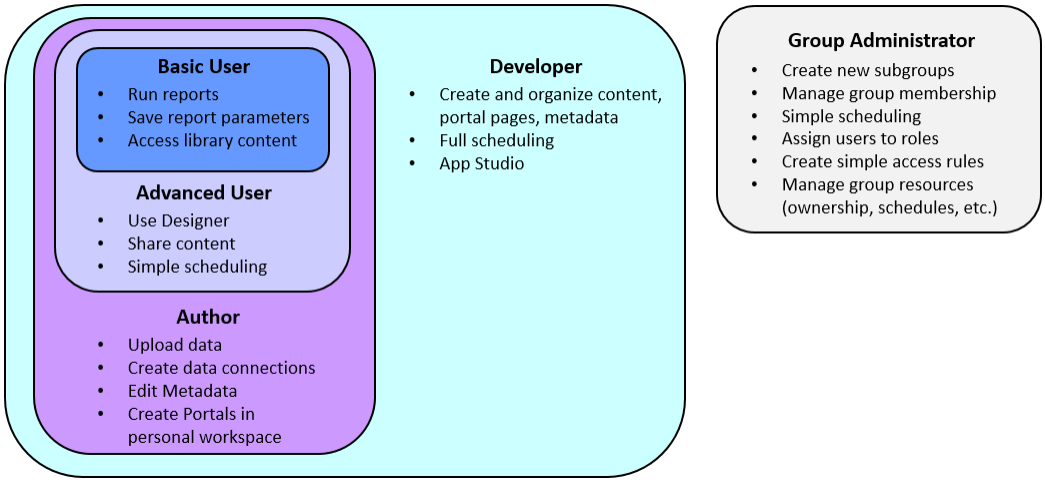
4. ダイアログボックスに表示された情報をリッチテキスト形式のレポートで出力するには、権限を選択し、[レポートの作成] をクリックします。

ポリシーの設計

セキュリティポリシーは、組織のビジネスニーズに応じてレポートリソースへのアクセスを制御します。ポリシーを設計する際は、作成するグループ、ロール、ルールを決定します。

グループの設計

リソーステンプレートを使用すると、4 つのロール (Basic Users、Advanced Users、Developers、Group Administrators) が定義されます。これらのロールは、ワークスペースの親グループ下にネストされたサブグループとして実装されます。Basic Users グループのユーザの権限は、Basic Users ロールに関連付けられたルールに基づいて決定されますが、Advanced Users グループのユーザの権限は、Basic Users ロールに関連付けられたルールと Advanced Users ロールに関連付けられたルールに基づいて決定されます。下図のように、Advanced Users ロールの権限には、Basic Users ユーザの権限が含まれ、Developer ロールの権限には、Advanced Users ロールの権限が含まれています。Group Administrators ロールには、レポートの実行権限および ReportLibrary 出力の表示権限が許可されていないため、このロールの権限は、他のサブグループの権限と重複しません。



グループをネストすると、ポリシーの設計が簡素化されます。ユーザは、これらのグループのいずれかに属しているだけで、そのユーザタイプの権限がすべて割り当てられます。ユーザにこれらのグループの権限を組み合わせて割り当てる必要がある場合は、そのユーザを Group Administrators グループや他のグループのいずれかに追加することもできます。ルールを親グループに適用することで、そのグループ内のすべてのユーザがコンテンツを互いに共有できるようにしたり、グループ管理者に親グループとサブグループを管理する権限を与えたりすることもできます。

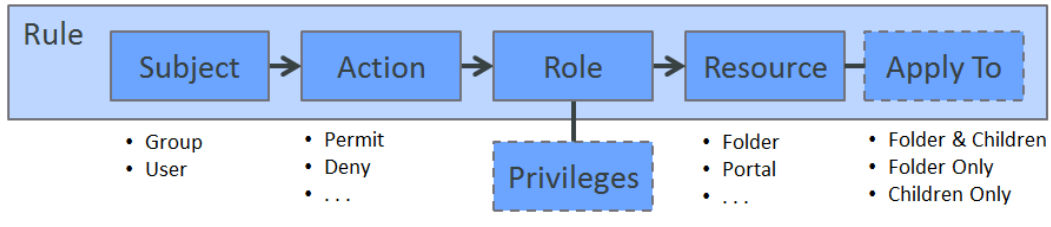
また、ユーザの権限を複数の異なるロールに分割して、それぞれのロールで権限が重複しないようにすることもできます。このモデルでは柔軟性が向上しますが、各ユーザの権限が多数のロールとルールを合成したものになるため、管理がより困難になります。

さらに、システム内のすべてのリソースへのアクセスが必要なユーザを管理する「インフラグループ」が必要となる場合があります。たとえば、Administrators グループがこれに該当します。また、リポジトリ内でリソースの実行や削除は行えないが、リソースをエクスポートできる「変更管理グループ」が必要になる場合もあります。

グループについての詳細は、454 ページの 「 ユーザの管理 」 を参照してください。

ロールの設計

よく使用する一連の権限をグループ化するには、ロールを使用します。次に、セキュリティルールに基づいて、下図のように特定のリソースに対して対象者 (ユーザまたはグループ) のロールを許可または拒否します。



ユーザをグループに分類する方法を決定した後、これらのグループに割り当てるロールを設計します。リソーステンプレートで作成されるグループのように、ユーザタイプごとにグループが 1 つの場合は、ユーザタイプごとにロールを 1 つ作成する方法が簡単です。次に、特定のリソースに対して、各グループのロールを許可するか、拒否するかを決定するルールを作成します。

たとえば、リソーステンプレートにより自動的に作成されるルールは、ワークスペースフォルダとその下位フォルダに対して、BasicUser グループの DomainBasicUser ロールを許可します。AdvancedUser グループの DomainAdvancedUser ロールは、ワークスペースフォルダとその下位フォルダに対して許可されています。同様のルールを設計して、作成するカスタムサブグループにワークスペースポータルへのアクセスや、共通ポータルのワークスペースページへのアクセスを許可することができます。開発者が Reporting Server にアクセスできるようにするには、リソースツリーの Reporting Server ノードに対して、Developers グループの DomainDeveloper ロールを許可するルールを作成します。

1 つのロールを、複数のルールで使用することができます。たとえば、さまざまなタイプのリソースに対して、特定のグループに複数の権限を許可する場合などです。フォルダ、ポータル、Reporting Server ノードのそれぞれのリソースに対する権限を開発者に許可する場合は、関連する権限がすべて含まれたロールを 1 つ作成した上で、そのロールを各リソースに適用する別のルールを作成します。特定のサブシステムに適用されない権限は無視されます。また、開発者用のロールとして、特定の IBFS サブシステムに関連する権限のみが含まれた別のロールをリソースごとに作成する方法もあります。この方法では、フォルダを指定する開発者用のロール、ポータルを指定する開発者用のロール、Reporting Server ノードを指定する開発者用のロールを作成することになります。ただし、ロールを 1 つだけ作成する方が管理が容易になります。

注意：セッション権限が含まれたロールは、WFC サブシステムの下位で設定するルールには使用しないことをお勧めします。デフォルト設定では、特定の深さより下位にあるセッション権限は確認されません。これは、システムリソースの負荷を軽減するためです。システム管理者は検索の深さを変更できますが、この変更はお勧めしません。

ロールについての詳細は、474 ページの 「 ロールの管理 」 を参照してください。

ルールの設計

システムで使用するルール数を少なくすると、ルールの理解や管理が容易になります。セキュリティポリシーを構成するルール数は、さまざまな要因に左右されます。たとえば、ユーザに提供するサブシステムの種類、組織で必要なロール数、使用するワークスペース数などが影響します。システムで使用するルール数を最小限に抑えるには、IBFS 階層内で可能な限り最上位に近いレベルでルールを適用します。一般に、可能な限り上位で権限を許可し、可能な限り下位で権限を拒否します。

ここでは、一例として、すべてのユーザがすべてのリソースにアクセスし、レポート作成またはレポート実行のいずれかの操作のみを実行する必要があるという単純なシナリオについて考察します。このシナリオは、単に 2 つのグループと 2 つのルールを使用することで実装することができます。2 つのグループは、Report Developer グループおよび Report Runner グループです。2 つのルールは、IBFS ルートノードに適用します。これにより、これらのルールが、コンテンツフォルダ、ポータル、Reporting Server リソースのすべてに適用されます。一方のルールで、IBFS ルートフォルダに対して Report Developer グループの Report Developer ロールを許可します。他方のルールで、同一範囲のリソースに対して Report Runner グループの Report Runner ロールを許可します。Report Runner グループに Reporting Server ノードが表示されないようにするには、別のルールを 1 つ追加し、Reporting Server ノードに対してこのグループの List ロールを拒否します。

多くの場合、グループが異なれば、アクセスが必要なリソースも異なります。リソーステンプレートから提供されるセキュリティポリシーは、この要件をサポートします。各ワークスペースでは、グループにそれぞれ独自のリソースへのアクセスが許可されていますが、各ワークスペースフォルダおよびポータルの上位では、どのグループにもルールは関連付けられていません。特定のフォルダやポータルページを非表示にするなど、追加要件をサポートする特別なルールを適用することで、ポリシーを調整することができます。

一般的な例として、ユーザが特定のコンテナのコンテンツを操作できるようにするが、その操作がコンテナ自体には影響しないようにするという要件があります。たとえば、開発者が [Sales] フォルダ下でフォルダの作成と削除を行う必要があるが、[Sales] フォルダ自体の削除は行えないようにするという場合があります。この要件に対処するには、そのフォルダのみで使用されるルールを適用して、特定の権限を制限します。リソーステンプレートは、この方法で ワークスペース Developers および Group Administrators グループを制限します。その結果、これらのグループが管理権限を持つフォルダなど、セキュリティ境界を定義するコンテナを削除できなくなります。

ルールについての詳細は、482 ページの 「 ルールの管理 」 を参照してください。

フォルダの使用

フォルダには、すべてのリポジトリコンテンツが格納されます。ユーザが作成するフォルダは、常にプライベートフォルダとして作成されます。作成者に必要な権限が付与されている場合、フォルダおよびフォルダ内のコンテンツを他のユーザと共有したり、一般使用向けに公開したりできます。

フォルダには、タイトルとフォルダ名の両方が定義されています。フォルダのタイトルは、一般にユーザに表示される情報です。フォルダ名は、フォルダが格納するコンテンツの一義的な内容を表す内部参照として WebFOCUS で使用されます。コンテナ内では同一のタイトルを使用できますが、重複したフォルダ名を使用することはできません。

フォルダパスのパス情報には最大で 1,040 バイト (オブジェクト名を含まない)、オブジェクト名には最大で 64 バイトの文字を使用することができます。たとえば、フォルダ名を /WFC/Repository/AmericaBank/Finance と指定することができます。この例では、パス情報の /WFC/Repository/AmericaBank/ が 28 バイト、フォルダ名の Finance が 7 バイトです。

注意：WebFOCUS バージョン 8 より前のリリースでは、公開済みコンテンツはスタンダードレポート、プライベートコンテンツはマイレポートと呼ばれていました。

手順　フォルダのプロパティを表示するには

フォルダのプロパティを表示するには、リソースツリーまたはコンテンツエリアでフォルダを右クリックし、[プロパティ] を選択します。[プロパティ] パネルが表示されます。下表は、プロパティの説明です。

項目	説明
全般タブ	
タイトル	リソースツリーまたはコンテンツエリアに表示されるフォルダのタイトルです。エンドユーザは、このタイトルでフォルダを識別します。通常は、フォルダ内のコンテンツに基づいています。
名前	フォルダに対する一意の内部参照を示します。この名前を使用して、内部処理でフォルダを識別します。このテキストボックスは灰色で表示され、デフォルトで使用不可に設定されています。テキストボックス横の [名前の変更] アイコンをクリックすると、このテキストボックスを使用して名前を変更することができます。
概要	フォルダに関する詳細説明が表示されます。
パス	親フォルダのリポジトリのフルパスが表示されます。
作成日時	フォルダが作成された日時およびフォルダを作成したユーザ ID が表示されます。
更新日時	フォルダが最後に変更された日時および、フォルダを最後に変更したユーザ ID が表示されます。

項目	説明
アクセス日時	[プロパティ]、[実行]、[ディファード実行] コマンド、またはフォルダの変更に使用される編集ツールのいずれかでフォルダが最後にアクセスされた日時が表示されます。フォルダに最後にアクセスしたユーザ ID またはツールも表示されます。
オーナー	フォルダが現在割り当てられているユーザ ID が表示されます。
公開	フォルダおよびそのコンテンツが公開済みかどうかを指定します。
表示	フォルダ内でのコンテンツの作成が許可されていないユーザに、このフォルダを表示するかどうかを指定します。このオプションは、フォルダ内のコンテンツの表示および使用が許可されているユーザに対してフォルダを一時的に使用不可にする場合に使用します。
詳細タブ	
フォルダのプロパティ	
[マイコンテンツ] フォルダの自動作成	このチェックがオンの場合、[My Content Folder] 権限を所有するユーザの [マイコンテンツ] フォルダが作成されます。これにより、ユーザは WebFOCUS DESIGNER、InfoAssist およびその他のレポート機能や配信機能を使用して作成する個人用のレポート、グラフ、ドキュメント (例、保存済みパラメータレポート) をそのフォルダに保存することができます。
自動的に開く	このチェックがオンの場合、WebFOCUS Hub の [ワークスペース] ビュー、WebFOCUS ホームページまたはレガシーホームページを開くと、リソースツリーがロードされます。 ❑ リソースツリーのこのワークスペースのフォルダが自動的に展開され、[マイコンテンツ] フォルダおよび同フォルダ内の他のフォルダが表示されます。 ❑ WebFOCUS Hub の [ワークスペース] ビューまたは WebFOCUS ホームページでは、このワークスペースのフォルダがコンテンツエリアにも自動的に表示され、フォルダおよびフォルダに割り当てられた項目が表示されます。
エクスプローラ/ポータルのプロパティグループ	

項目	説明
ソート順	リソースツリーおよびコンテンツエリアにフォルダを表示する順序を指定します。
言語	フォルダおよびそのコンテンツの作成に使用された言語が表示されます。
すべて表示	[言語のプロパティ] ダイアログボックスが開き、フォルダおよびそのコンテンツの作成、表示に使用するデフォルト設定の言語が表示されます。ユーザの環境が複数の言語をサポートする場合、このダイアログボックスには、選択したコードページで使用可能な他の言語のエントリも表示されます。
メニューアイコン	このフォルダを表すために使用されるアイコンの CSS クラス名を、フルサイズのホームページ画面上部のタブ、または画面がフルサイズより小さい場合はサイドメニューに表示します。詳細は、『WebFOCUS BI Portal 利用ガイド』の「ポータルレベルへのアイコンの追加」を参照してください。
下位項目のメニューアイコンを表示	このチェックがオンの場合、このフォルダ内のフォルダおよびポータルのメニューアイコンが、フルサイズのホームページ画面上部のタブ、または画面がフルサイズより小さい場合はサイドメニューに表示されます。
サーバタブ	
サーバの割り当て	割り当てサーバおよび利用可能なすべてのサーバが表示されます。このチェックがオンの場合、デフォルト設定の WebFOCUS Reporting Server が使用されておらず、利用可能なサーバのいずれかを選択する必要があります。 このチェックがオフで、WebFOCUS Reporting Server が指定されていない場合、レポートリクエストは、WebFOCUS Client 構成で指定されたデフォルト WebFOCUS Reporting Server に送信されます。

項目	説明
アプリケーションパスの割り当て	割り当てアプリケーションパスおよび利用可能なすべてのアプリケーションパスが表示されます。このチェックがオンの場合、デフォルト設定のアプリケーションパスが使用されておらず、利用可能な他のアプリケーションパスのいずれかを選択する必要があります。 このチェックがオフで、アプリケーションパスが指定されていない場合、WebFOCUS Client 構成および WebFOCUS Reporting Server 構成の処理中に定義されたデフォルト設定のアプリケーションパスが使用されます。

手順　フォルダを作成するには

1. リソースツリーで、新しいフォルダを保存するワークスペースまたはフォルダに移動します。

   または

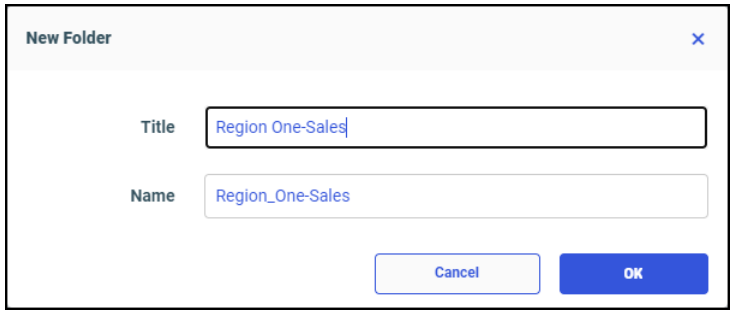
   階層リンクで、新しいフォルダを格納するワークスペースまたはフォルダへのリンクをクリックします。

2. WebFOCUS Hub で、リソースツリー上部の [新規フォルダ] を選択します。

   または

   WebFOCUS ホームページのアクションバーで [その他] タブをクリックし、[フォルダ] を選択します。

3. 下図のように、[新規フォルダ] ダイアログボックスに新しいフォルダのタイトルを入力します。



入力すると同時に、[タイトル] テキストボックスの値から取得された一意の値が [名前] テキストボックスに入力されます。[タイトル] テキストボックスに入力したブランクまたは特殊文字はすべて、[名前] テキストボックスでアンダースコア (_) に自動的に変換されます。複数の特殊文字で構成される連続した文字列 (例、&&&) を [タイトル] テキストボックスに入力すると、[名前] テキストボックスでこれらが単一のアンダースコア (_) に自動的に変換されます。必要に応じて、後から名前を変更することもできます。

4. [OK] をクリックします。

   新しいフォルダが、リソースツリーおよびコンテンツエリアの指定したディレクトリに表示されます。

5. フォルダにオプションの概要説明を追加するには、次の手順を実行します。
   a. 新しいフォルダを右クリックし、[プロパティ] を選択します。
   b. [プロパティ] パネルで、[概要] テキストボックスに説明を入力します。
   c. [保存] をクリックして説明を保存します。その後、[キャンセル] をクリックして [プロパティ] パネルを閉じます。

手順　フォルダを公開するには

リソースツリーまたはコンテンツエリアで、フォルダを右クリックし、[公開] を選択します。

リソースツリーがリフレッシュされ、フォルダ名は斜体表示でなくなります。コンテンツエリアがリフレッシュされ、フォルダから境界線が削除され、フォルダアイコンはフルカラーで表示されます。

手順　フォルダを非公開にするには

リソースツリーまたはコンテンツエリアで、フォルダを右クリックし、[非公開] を選択します。

リソースツリーがリフレッシュされ、フォルダ名が斜体で表示されます。コンテンツエリアがリフレッシュされ、フォルダを囲む境界線が表示されます。フォルダアイコンは灰色で表示されます。

手順　フォルダの複製を作成するには

リソースツリーまたはコンテンツエリアで、フォルダを右クリックし、[複製の作成] を選択します。

リソースツリーでは、元のフォルダの下にフォルダの複製が表示されます。コンテンツエリアでは、元のフォルダの右隣または真下にフォルダの複製が表示されます。複製フォルダの名前およびタイトルは、元のフォルダの名前およびフォルダにアンダースコア (_) と、複製が作成されるたびに増加する整数値が追加されます。

注意

- [複製の作成] メニューオプションでは、元のフォルダと同じディレクトリにフォルダの複製が作成されます。フォルダの複製を別のディレクトリに移動する場合は、[コピー] および [貼り付け] のオプションを使用してください。
- ワークスペースの複製を作成することはできません。

手順　フォルダを切り取りまたはコピーして貼り付けるには

1. リソースツリーまたはコンテンツエリアでフォルダを右クリックします。フォルダを移動する場合は [切り取り] を選択し、フォルダを元の場所に残す場合は [コピー] を選択します。
2. リソースツリーで、移動先を示すフォルダをクリックします。必要に応じて、ツリーを展開して移動先を表示します。

   または

   移動先が階層リンクで表示される場合は、移動先を示すフォルダをクリックします。
3. リソースツリーで、移動先を示すフォルダを右クリックし、[貼り付け] を選択します。

   または

   移動先のコンテンツエリアの任意の場所で右クリックし、[貼り付け] を選択します。

   リソースツリーおよびコンテンツエリアがリフレッシュされ、フォルダが表示されます。

   指定した場所でフォルダ名が一意である必要があります。フォルダを別の親フォルダに貼り付けた場合、その親フォルダ内に同一の名前が存在しない限り、元のフォルダ名が保持されます。その名前のフォルダがすでに存在する場合、または貼り付けたフォルダ内に元のフォルダと同一名のフォルダが含まれている場合、コピーしたフォルダの名前は、元のフォルダの名前にアンダースコア (_) と、フォルダを貼り付けるたびに増加する整数値が追加されます。フォルダのタイトルは、フォルダ名と同じように更新されます。

   注意：ワークスペースを切り取り、貼り付けることはできません。

手順　フォルダタイトルを変更するには

1. リソースツリーまたはコンテンツエリアで、フォルダを右クリックし、[プロパティ] を選択します。

2. [プロパティ] パネルの [タイトル] テキストボックスに新しいタイトルを入力し、[保存] をクリックします。

   フォルダタイトルが更新されます。フォルダ名のアルファベット順で新しいフォルダの位置が変わる場合は、リソースツリーおよびコンテンツエリア内のフォルダの配置も変更されます。

3. 更新の完了後、[キャンセル] をクリックして [プロパティ] パネルを閉じます。

手順　フォルダを削除するには

1. リソースツリーまたはコンテンツエリアで、フォルダを右クリックし、[削除] を選択します。
2. フォルダの削除を確認するメッセージで、[OK] をクリックします。

   リソースツリーおよびコンテンツエリアがリフレッシュされ、フォルダが削除されます。

ワークスペースの理解

ワークスペースは、WebFOCUS コンテンツ構造を形成する最上位の基本要素です。各ワークスペースでは、一連のユーザグループ、ワークスペース内のコンテンツの作成元メタデータへのリンク、およびこれらが一体的に機能するための一連のルールが統合されます。ユーザは、ワークスペースを使用して、プライベートコンテンツの管理、コンテンツの共有 (ユーザロールで許可されている場合)、他のユーザが公開したコンテンツへのアクセスを行えます。

リソースツリーでは、各ワークスペースは [ワークスペース] ノード下のルートレベルのフォルダとして表示されます。これらのフォルダにより、コンテンツがセクション別に分類されるため、コンテンツの識別が容易になるとともに、ワークグループ用に体系化されたコンテンツ構造が作成されます。

ワークスペースには、エンタープライズとテナントの 2 つの種類があります。エンタープライズワークスペースは、単一の企業に影響する環境をサポートし、その企業内の部門別およびコンテンツ別に分類されます。テナントワークスペースは、複数の企業に影響する環境をサポートし、サービスベンダーとしてソフトウェアのテナントクライアント別に分類されます。

テナントワークスペースは、同一テナントに割り当てられたユーザのみ使用できます。他のテナントに割り当てられたユーザは使用できません。

ポータル、共有ポータルページ、WebFOCUS Reporting Server テンプレートなどのリソースもワークスペースの一部です。これらのリソースを作成するには、最初にワークスペースを作成する必要があります。ワークスペースを作成すると、これらのリソースで使用されるコンテンツと、そのコンテンツの利用対象ユーザが関連付けられます。また、ワークスペース内で定義されたルールに基づいて、各リソース内のコンテンツへのユーザアクセスが制御されます。リソースが必要なくなった場合、これらのリソースが割り当てられているワークスペースを削除すると、リソースも削除されます。

デフォルト設定では、すべての新規ワークスペースの基盤としてリソーステンプレートが使用されます。新しいワークスペースを作成する際に、ユーザが選択したワークスペースタイプ、およびワークスペースに含めるよう選択したリソースに適合するリソーステンプレートが呼び出されます。リソーステンプレート内で事前に構成されているグループおよびルールに基づいて、コンテンツの利用範囲 (最大限のアクセスレベルから最小限のアクセスレベル) が定義されます。WebFOCUS では一連の基本的なテンプレートが定義されていますが、管理者は独自のリソーステンプレートを作成し、利用可能なリソーステンプレートのリストにそのテンプレートを追加することができます。

マイワークスペースの理解

マイワークスペースは、ユーザがアクセスしやすい便利な場所を提供する特別なワークスペースです。マイワークスペースでは、ユーザ自身で使用するコンテンツを作成したり、コンテンツを他のユーザと共有したり作成できます。マイワークスペースは、デフォルトで製品環境に設定されており、ホームページから直接作成したコンテンツまたは他の定義済みワークスペースの外部で作成したコンテンツの格納先ワークスペースとして設定されています。

他のワークスペースと同様に、マイワークスペースは、リソーステンプレートから作成され、すべてのテンプレートに割り当てられたルールと同一のセキュリティルールを使用します。ただし、ワークスペースには通常 4 つのグループが割り当てられるのに対し、このグループには Basic Users グループと Authors グループのみが含まれます。

他のワークスペースと同様に、管理者は、[マイワークスペース] 内の 2 つのグループへのユーザの割り当てを積極的に管理する必要があります。[マイワークスペース] のユーザに与えられる権限は、他のワークスペースのユーザに与えられる権限とは完全に独立したものです。

[マイワークスペース] 内の [マイコンテンツ] フォルダは、Authors グループのメンバーが新規コンテンツを作成できる専用フォルダとして機能します。[共有] フォルダも設定されており、ユーザが [マイワークスペース] の自身のインスタンス内のプライベートコンテンツを共有すると表示されます。

[マイワークスペース] というタイトルのワークスペースは、[マイワークスペース] というタイトルのビューとは区別されることに注意してください。ビューとワークスペースの両方に、現在ログインしているユーザが作成したプライベートコンテンツが表示されます。

ただし、ワークスペースには、現在ログインしているユーザが作成または保存したコンテンツのみが格納されます。ビューには、このユーザが利用可能なすべてのワークスペースの [マイコンテンツ] フォルダからプライベートコンテンツが表示されます。つまり、[マイワークスペース] ビューには、[マイワークスペース] というタイトルのワークスペースより広範囲のコンテンツが表示されます。

新規コンテンツのデフォルトワークスペースとして別のワークスペースを使用する必要がある場合は、管理者は [マイワークスペース] を別のワークスペースで置換することができます。この場合、[BI Portal] ページの [デフォルトワークスペースリポジトリパス] (IBI_DEFAULT_WORKSPACE_PATH) 設定に表示されるパスを変更します。

ただし、別のワークスペースがデフォルトワークスペースとして指定された場合も、ユーザは [マイワークスペース] というタイトルのワークスペースで作業することができます。[マイワークスペース] は、WebFOCUS Hub または WebFOCUS ホームページのコンテンツ表示から開くことができます。

開始ワークスペースの理解

[開始] ワークスペースは、WebFOCUS Hub または製品のクラウドインスタンスの WebFOCUS ホームページ上部に表示される [開始] カルーセルのコンテンツを格納する特別なワークスペースです。このワークスペースには、製品をはじめてインストールした際に、WebFOCUS ソフトウェアの機能をはじめてのユーザに紹介するためのコンテンツが格納されます。管理者は、このワークスペースに独自のコンテンツを追加し、組織のニーズに合わせて導入コンテンツをカスタマイズすることができます。割り当てられた開始ワークスペースグループの権限に基づいて、各ユーザはこのワークスペースおよび関連するカルーセル内の項目の実行、編集、作成、スケジュールが行えます。

[開始] ワークスペースは、デフォルト設定で製品のクラウドインスタンスに含まれていますが、オンプレミスインスタンスには含まれていません。他のワークスペースと同様に、このワークスペースは、リソーステンプレートから作成され、すべてのテンプレートに割り当てられたルールと同一のセキュリティルールを使用します。

[開始] ワークスペースには、ワークスペースに通常割り当てられる 4 つのユーザグループに加えて Authors グループが含まれます。リソーステンプレートで作成された 5 つのグループをすべて含めることで、管理者は、新しいユーザが通常行う作業の役割に最適な権限範囲にこのユーザを割り当てることができます。

他のワークスペースと同様に、管理者は、[開始] ワークスペース内のグループへのユーザの割り当てを積極的に管理する必要があります。[開始] ワークスペースのユーザに与えられる権限は、他のワークスペースのユーザに与えられる権限とは完全に独立したものです。

[開始] ワークスペース内にデフォルトで設定されたフォルダも、リソーステンプレートから作成された他のワークスペースとは異なります。[開始] ワークスペースには、[マイコンテンツ] フォルダは表示されません。ただし、[ビジュアライゼーション] フォルダが表示されます。このフォルダには、[開始] カルーセルに表示されないが、WebFOCUS コンテンツのサンプルとしてユーザが使用可能な事前にパッケージ化されたビジュアライゼーションが格納されています。

管理者は、[開始] ワークスペースを別のワークスペースで置換することができます。この場合、管理コンソールの [構成] タブの [BI Portal] 設定で、[デフォルトリストリポジトリパス] (IBI_DYNAMIC_LIST_PATH) 設定に割り当てられた値を変更します。この設定は、WebFOCUS ホームページのホーム表示で最上位カルーセルに表示されるワークスペースも定義します。

管理者が、この設定で、[開始] ワークスペースのデフォルトパスを置換すると、上位カルーセルの名前がこの別のワークスペースの名前で置換され、このワークスペースに格納されたコンテンツが上位カルーセルに表示されます。管理者は、最上位カルーセルに表示されるコンテンツが利用できるよう、このワークスペース内のグループにユーザを割り当てる必要があります。Authors グループは、[開始] ワークスペースを置換するワークスペースには含まれません。

この設定の値がブランクの場合、[開始] カルーセルはホーム表示上部に表示されませんが、[開始] ワークスペースおよびそのグループ設定は保持されます。

この設定に別のワークスペースを指定した場合、またはワークスペースを指定しなかった場合も、ユーザは、WebFOCUS ホームページのコンテンツ表示から [開始] というタイトルのワークスペース内で作業することができます。

リソーステンプレートの理解

管理者は、WebFOCUS セキュリティモデルを使用することで、複雑なセキュリティポリシーを柔軟に作成することができます。一方、多くの組織では、ごく少数の標準ユーザロールと、単純なパターンのアクセス権限でセキュリティ要件を満たすことができます。WebFOCUS でワークスペースを作成する際は、部門や部署で構成される企業向けのリソーステンプレートと、共通のレポートリソースおよびテナント独自のレポートリソースを必要とする SaaS プロバイダ向けのリソーステンプレートが提供されます。

WebFOCUS から提供される一連のリソーステンプレートを使用すると、一般的なエンタープライズ展開または SaaS 展開で使用可能なフォルダ、グループ、ロール、ルールが作成されます。これらのテンプレートをそのまま実装することも、組織の要求に適合させることもできます。また、組織の要件に適合するカスタムリソーステンプレートを作成することもできます。

リソーステンプレートグループの理解

リソーステンプレートから新しいワークスペースを作成すると、セキュリティセンターにそのワークスペース自体の新しいグループが自動的に作成されるとともに、そのグループ内に 4 つのユーザタイプ (BasicUsers、AdvancedUsers、Developers、GroupAdmins) それぞれのサブグループが作成されます。管理者がこれらのグループのいずれかにユーザを割り当てると、そのワークスペースで作業する際に、そのユーザにはユーザロールに割り当てられた権限が自動的に付与されます。

BasicUsers グループのメンバーは、所属するワークスペース内のコンテンツを表示することができます。これらのメンバーは、[マイコンテンツ] フォルダ内にフォルダを作成し、ディファードレポートを保存することができます。また、以前に作成されたレポートからオートリンクパラメータをコピーし、それらのパラメータをメンバー自身のフォルダに保存することができます。ただし、フォルダおよびコンテンツの共有、公開、コピー、貼り付けを行うことはできません。

AdvancedUsers グループのメンバーは、BasicUsers グループの権限をすべて所有する以外に、メンバー独自のコンテンツおよびフォルダを作成、共有することができます。

Developers グループのメンバーは、BasicUsers グループおよび AdvancedUsers グループの権限をすべて所有する以外に、データのアップロードとデータへの接続、メタデータの編集、ワークスペースコンテンツの作成、管理を行えます。また、他のユーザが閲覧可能なコンテンツを管理することもできます。さらに、メンバー自身のワークスペースからフォルダまたはコンテンツをコピーし、別のワークスペースに貼り付けることができます。ただし、この操作のターゲットワークスペースで、コピー元コンテンツの作成時に使用されたメタデータと同一のメタデータへの接続が可能である必要があります。

GroupAdmins グループのメンバーは、4 タイプのユーザグループにユーザを追加したり、ユーザを削除したりすることで、ワークスペース内での各ユーザのロールを決定します。また、ワークスペースに割り当てられた全般アクセス権限を変更することもできます。

ワークスペースで作業する際に大部分のユーザが必要とする基本アクセスレベルは、上記 4 タイプのユーザグループで十分なため、管理者がユーザごとにアクセスレベルのプロファイルを構成する必要がなくなり、これらのユーザグループへのユーザ割り当てのみに集中することができます。

手順　ワークスペースを作成するには

1. 管理者としてログインし、WebFOCUS Hub でサイドナビゲーションウィンドウから [ワークスペース] アイコンを選択し、ワークスペースエリアを開きます。

   または

WebFOCUS ホームページを開き、バナーで [ワークスペース] を選択し、ワークスペースエリアを開きます。

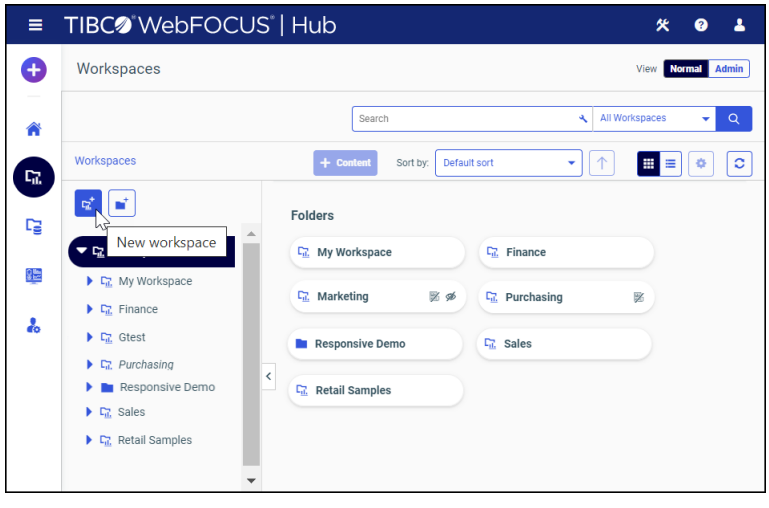
注意：デフォルト設定で開かない場合は、コンテンツエリアの左側でリソースツリーを展開します。

2. リソースツリーで、[ワークスペース] をクリックします。

   または

   階層リンクで、[ワークスペース] をクリックします。

3. 下図のように、WebFOCUS Hub のリソースツリー上部で、[新規ワークスペース] を選択します。

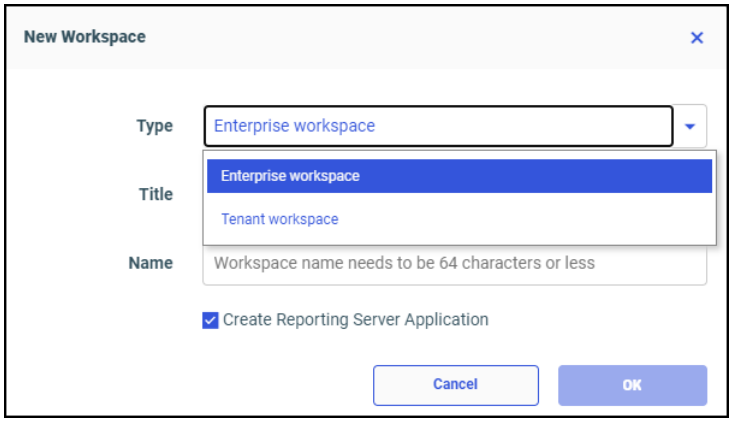


または

WebFOCUS ホームページでワークスペースビューを開き、リソースツリー上部で、[新規ワークスペース] を選択します。

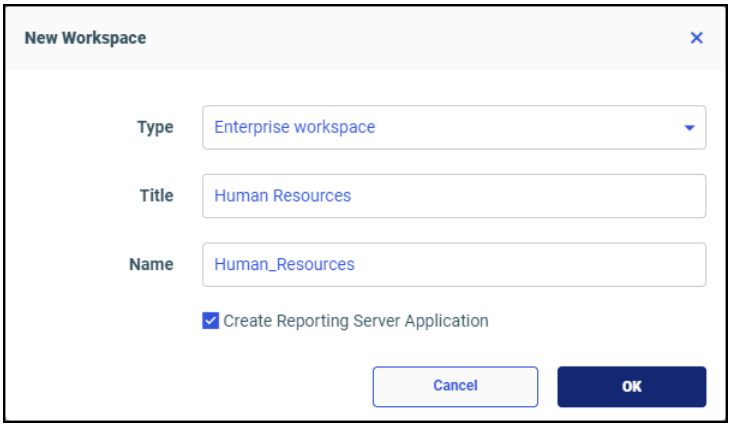
4. [新規ワークスペース] ダイアログボックスの [タイプ] ドロップダウンリストから、次のいずれかを選択します。

   - 下図のように、[エンタープライズワークスペース] を選択すると、企業の部門や部署のワークスペースが作成されます。



   - [テナントワークスペース] を選択すると、SaaS プロバイダのテナントワークスペースが作成されます。

5. 下図のように、[タイトル] テキストボックスにワークスペースの説明を入力します。



[タイトル] テキストボックスに説明を入力すると、同一の文字が [名前] テキストボックスにも同時に入力されますが、[名前] の文字は IBFS 規則に準拠するよう自動的に調整されます。

管理者は、ワークスペース作成後に [プロパティ] パネルを開き、別の表示言語にローカライズされたタイトルを [言語のプロパティ] ダイアログボックスに追加することで、タイトルをさまざまな言語にローカライズすることができます。[言語のプロパティ] ダイアログボックスは、[すべて表示] ボタンで [プロパティ] パネルにリンクされています。

6. WebFOCUS Reporting Server 上に関連するアプリケーションディレクトリを作成するには、[Reporting Server アプリケーションの作成] のチェックをオンにします。

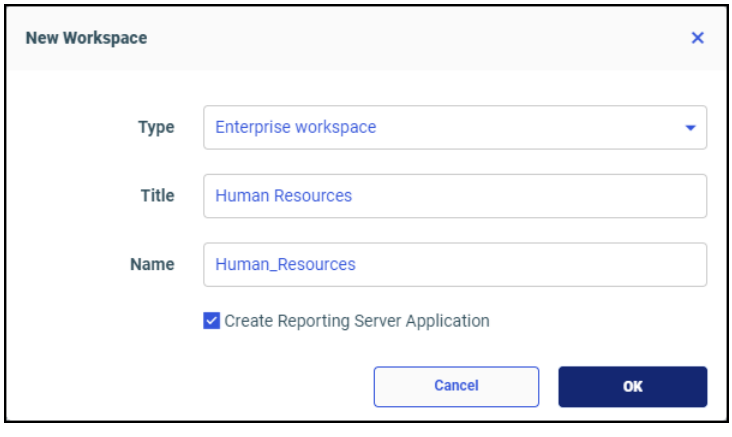
   注意：[Reporting Server アプリケーションの作成] オプションを含める場合は、ワークスペースユーザに WebFOCUS Reporting Server 上のアプリケーションディレクトリへのアクセス権限を付与する認可方法を作成、実装する必要があります。詳細は、410 ページの 「 アクセスコントロールテンプレートの理解 」 を参照してください。

   このチェックをオンまたはオフにすると、[名前] テキストボックスの値が動的に更新され、リソース名に使用できない文字が削除されます。

7. すべて選択した後、[OK] をクリックします。

新規ワークスペースの名前指定

[新規ワークスペース] ダイアログボックスの [タイトル] テキストボックスに新規ワークスペースのタイトルを入力すると、そのタイトルと同一の文字が [名前] テキストボックスに自動的に入力されます。[名前] テキストボックスに入力された文字が IBFS 名前規則に準拠するかどうかが自動的に検証されます。[タイトル] テキストボックスに使用制限文字を入力すると、[名前] テキストボックスでその文字が使用可能文字に置換されます。たとえば、下図のように [タイトル] テキストボックスにブランクを入力すると、[名前] テキストボックスではブランクが自動的にアンダースコア (_) に置換されます。

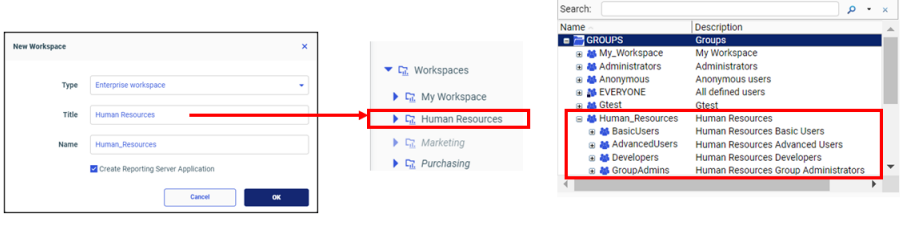


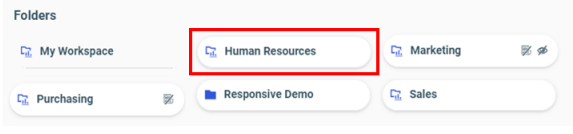
[タイトル] テキストボックスの値がエンドユーザに自動的に表示され、[名前] テキストボックスの値は内部処理に使用されます。

新規ワークスペースの作成結果の表示

新しいワークスペースを作成すると、その結果が [ワークスペース] ビューおよびセキュリティセンターに表示されます。選択したオプションに基づいて所定のリソースが作成されます。

[ワークスペース] エリアからワークスペースを作成する場合、新規ワークスペースのフォルダがリソースツリーおよびコンテンツエリアの [フォルダ] セクションに表示されます。セキュリティセンターの [ユーザとグループ] タブの [グループ] ウィンドウに、新規ワークスペースのグループが表示されます。リソースツリーおよびコンテンツエリアでは、デフォルト設定で [タイトル] が表示されます。セキュリティセンターの [グループ] リストには、ワークスペースの名前とタイトルの両方が表示されます。下図のように、作成結果は [ワークスペース] エリアにもセキュリティセンターにも表示されます。





WebFOCUS Hub の [ワークスペース] エリアまたは WebFOCUS ホームページからワークスペースを作成した場合、ワークスペースとともにポータルまたは共有ポータルページを作成するオプションがないため、これらの作成結果は表示されません。ただし、レガシーホームページからワークスペースを作成した場合は、このプロセスにポータルまたは共有ポータルページを含めるオプションが使用できます。

レガシーホームページの [新規ワークスペース] ダイアログボックスで [ワークスペースポータル] オプションを選択した場合、他の作成結果とともにポータルが使用可能になります。新規ワークスペースのフォルダが、リソースツリーおよびコンテンツエリアの [フォルダ] セクションに表示されます。ポータルのアイコンは、[ポータル] カルーセルにも表示されます。セキュリティセンターの [ユーザとグループ] タブの [グループ] ウィンドウに、新規ワークスペースのグループが表示されます。リソースツリー、コンテンツエリア、[ポータル] カルーセルでは、デフォルト設定でタイトルが表示されます。セキュリティセンターの [グループ] リストには、ワークスペースの名前とタイトルの両方が表示されます。これらの結果は、[ワークスペース] エリア、[ポータル] カルーセル、およびセキュリティセンターに表示されます。

[共有ポータルのワークスペースページ] オプションを選択した場合、他の作成結果とともに共有ポータルページが使用可能になります。このオプションを選択すると、共有ポータル内にブランクの [可変キャンバス] ページが作成されます。共有エンタープライズポータルでは、共有ページのフォルダがリソースツリーに表示されます。これらの結果は、WebFOCUS ホームページに表示されます。

エンタープライズリソーステンプレートとテナントリソーステンプレートの相違点の理解

各リソーステンプレートを実行すると、複数のグループ、ロール、セキュリティルール、フォルダが作成され、オプションとしてポータル、ポータルページ、WebFOCUS Reporting Server アプリケーションの作成を選択した場合は、これらのリソースも同時に作成されます。ただし、エンタープライズリソーステンプレートとテナントリソーステンプレートには、いくつかの相違点があります。

- どちらのテンプレートを実行した場合でも、[ワークスペース] ノード下にフォルダが作成されます。
- エンタープライズグループ管理者は、システム内のユーザをすべて表示することも、管理するグループに任意のユーザを追加することもできます。テナントグループ管理者は、管理するグループに所属するユーザのみを表示することができます。
- エンタープライズリソーステンプレートを実行すると、タイトルが「共有エンタープライズポータル」、名前が「enterprise」、URL が「.../ibi_apps/bip/portal/enterprise」の共有エンタープライズポータルが作成されます
- 一方、テナントリソーステンプレートを実行すると、タイトルが「共有マルチテナントポータル」、名前が「multitenant」、URL が「.../ibi_apps/bip/portal/multitenant」の共有テナントポータルが作成されます。

どちらのテンプレートを実行した場合でも、次のグループが作成されます。

- Basic Users

- Advanced Users
- Developers
- Group Administrators

これらのグループに適用されたルールから、デフォルトセキュリティポリシーが生成されます。ワークスペース内での操作権限の範囲は、Basic Users、Advanced Users、Developers の順に増加します Group Administrators グループは、レポートを実行することはできませんが、リソースのオーナーシップを管理したり、ワークスペース内のグループメンバーシップを管理したりできます。1 名の社員が複数の役割を担うような組織では、その役割の実行に必要な権限がすべて割り当てられるよう、その社員のユーザアカウントを複数のグループに追加することができます。

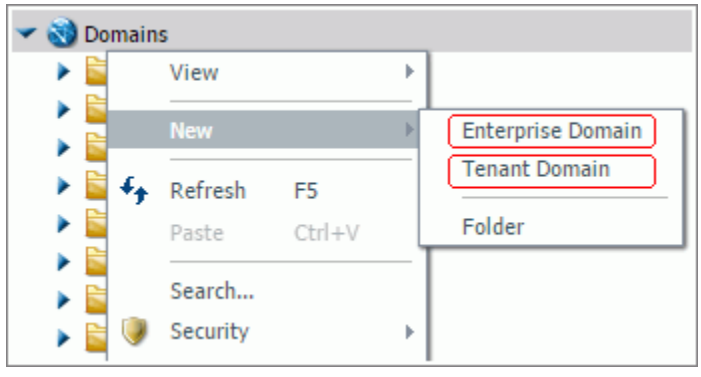
これらのテンプレートを実行すると、ワークスペース、ポータル、Reporting Server ノードに適用されるルールも作成されます。デフォルトルールについての詳細は、399 ページの 「 カスタムリソーステンプレートの作成 」 を参照してください。

ビルトインリソーステンプレートの有効化と無効化

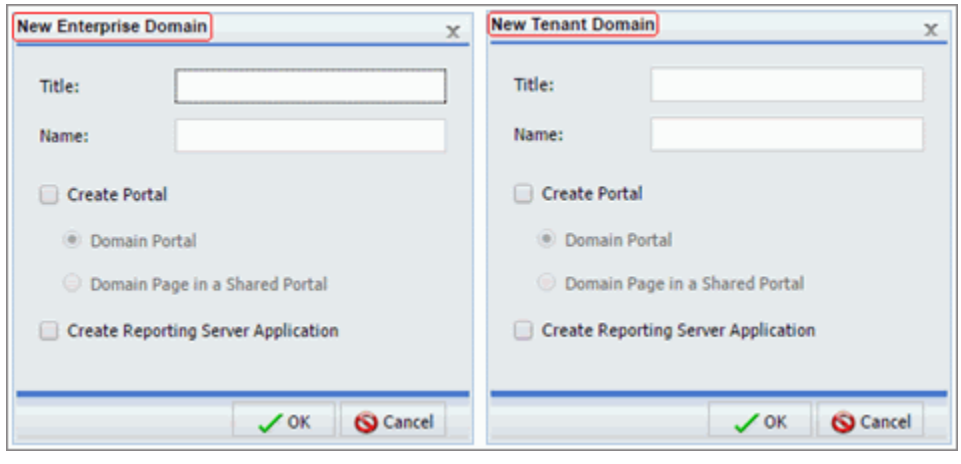
WebFOCUS には、エンタープライズワークスペース用に 6 つのリソーステンプレートのセット、およびテナントワークスペース用に 6 つのリソーステンプレートのセットが同梱されています。両方のセットは、デフォルト設定で有効になっています。ワークスペースの作成時に選択するワークスペースタイプおよびオプションに基づいて、実行されるリソーステンプレート、およびそのリソーステンプレートによって作成されるリソースが決定されます。

WebFOCUS ホームページからも新規ワークスペースは作成できますが、作成時にすべてのリソースを利用するためには、レガシーホームページからの作成をお勧めします。

新しいエンタープライズワークスペースまたはテナントワークスペースを作成するには、管理者としてログインし、レガシーホームページを起動します。下図のように BI Portal のリソースツリーで [ワークスペース] ノードを右クリックし、[新規作成] を選択します。



選択したワークスペースタイプに応じて、下図のようなダイアログボックスのいずれかが表示されます。



最初に [エンタープライズワークスペース] または [テナントワークスペース] を選択し、次にダイアログボックスで追加オプションを選択すると、次のリソーステンプレートのいずれかが呼び出されます。

エンタープライズワークスペース

- ❏ エンタープライスワークスペース
- ❏ エンタープライズワークスペース (共有ポータル)

- ❏ エンタープライズワークスペース (ポータル)
- ❏ エンタープライスワークスペースとアプリケーション
- ❏ エンタープライズワークスペースとアプリケーション (共有ポータル)
- ❏ エンタープライズワークスペースとアプリケーション (ポータル)

テナント ワークスペース

- ❏ テナント ワークスペース
- ❏ テナントワークスペース (共有ポータル)
- ❏ テナントワークスペース (ポータル)
- ❏ テナントワークスペースとアプリケーション
- ❏ テナントワークスペースとアプリケーション (共有ポータル)
- ❏ テナントワークスペースとアプリケーション (ポータル)

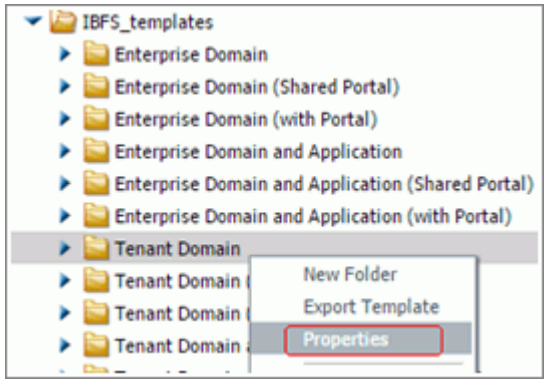
通常、WebFOCUS 環境は、エンタープライズ展開モデルと SaaS テナント展開モデルの両方をサポートするのではなく、これらの展開モデルのいずれかをサポートするよう構成されます。そのため、管理者は、サポートしない展開モデルが [ワークスペース] ノードのコンテキストメニューに表示されないようリソーステンプレートのセット全体を無効にすることができます。すべての SaaS テナントリソーステンプレートまたはすべてのエンタープライズリソーステンプレートを無効にするには、セット内のいずれか 1 つのテンプレートの [有効] 設定に [False] 値を割り当てる必要があります。

手順　ビルトインリソーステンプレートのセット全体を無効にするには

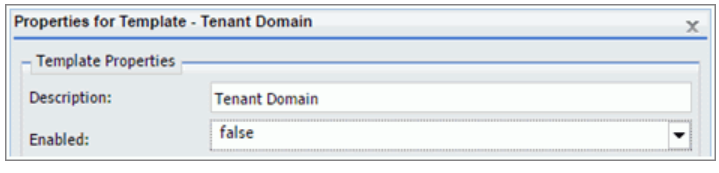
この機能は、レガシーホームページからのみ使用できます。

1. 管理者としてログインし、レガシーホームページを開きます。
2. リソースツリーで [ワークスペース] ノードを右クリックし、[表示]、[完全表示] を順に選択します。
3. リソースツリーで、[FILE] フォルダ、[IBFS_templates] フォルダを順に展開します。

4. フォルダを右クリックし、[プロパティ] を選択します。たとえば、下図のように [テナントワークスペース] フォルダを右クリックします。

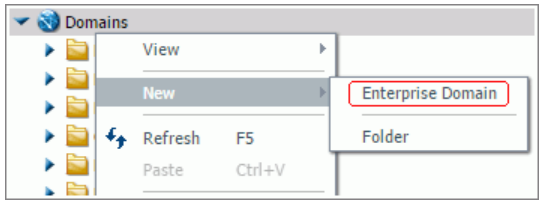


5. 下図のように、[テンプレートのプロパティ] ダイアログボックスの [有効] リストから [False] を選択します。



6. [OK] をクリックします。
7. [ワークスペース] ノードを右クリックし、[表示]、[リポジトリ表示] を順に選択して、リソースツリーを元の表示形式に戻します。
8. [ワークスペース] ノードを右クリックし、[新規作成] を選択します。

   下図のように、コンテキストメニューには [エンタープライズワークスペース] コマンドのみが表示されます。

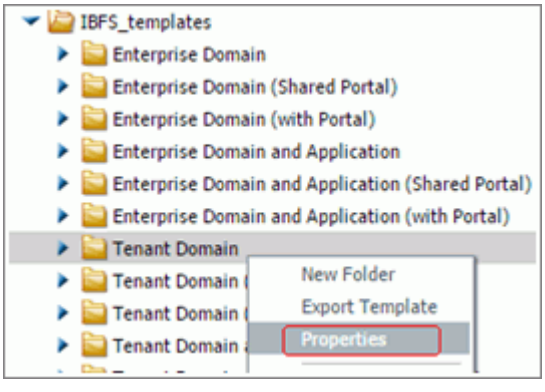


手順　ビルトインリソーステンプレートのセット全体を再度有効にするには

リソーステンプレートのセット全体を非表示にした後、そのセット全体を再度有効にする場合、管理者は、以前に無効にしたリソーステンプレートの [有効] リストの値を [True] に再設定する必要があります。

この機能は、レガシーホームページからのみ使用できます。

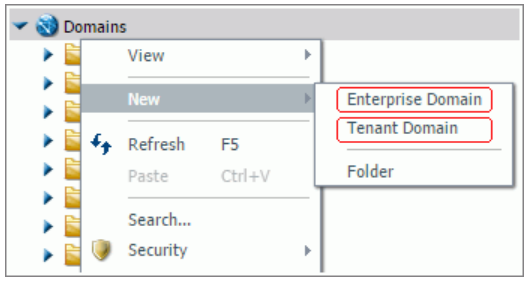
1. 管理者としてログインし、レガシーホームページを開きます。
2. リソースツリーで [ワークスペース] ノードを右クリックし、[表示]、[完全表示] を順に選択します。
3. [FILE] フォルダ、[IBFS_templates] フォルダを順に展開します。
4. 以前にテンプレートセット全体を非表示にするために [有効] プロパティを [False] に設定したフォルダを右クリックし、[プロパティ] を選択します。たとえば、下図のように [テナントワークスペース] フォルダを右クリックします。



5. 下図のように、[テンプレートのプロパティ] ダイアログボックスの [有効] リストから [True] を選択します。

6. [OK] をクリックします。
7. [WebFOCUS] ノードを右クリックし、[表示]、[リポジトリ表示] を順に選択して、リソースツリーを元の表示形式に戻します。
8. [ワークスペース] ノードを右クリックし、[新規作成] を選択します。

下図のように、コンテキストメニューに [テナントワークスペース] コマンドと [エンタープライズワークスペース] コマンドの両方が表示されます。



ワークスペースの削除

ワークスペースを削除できるのは、ワークスペース内のリソースすべての削除権限を所有する管理者のみです。

ワークスペースを削除すると、そのワークスペースに関連付けられているリソースも削除されます。つまり、ワークスペースグループおよびそのサブグループが削除されます。そのワークスペースに関連して作成された他のリソースがある場合、そのリソースも削除されます。たとえば、ワークスペースが参照する以下の項目です。

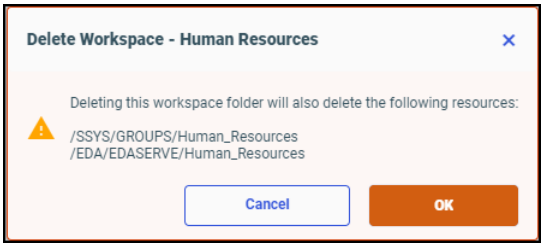
- ポータル - そのワークスペースから作成されたポータルが削除されます。
- 共有ポータルのページ - そのワークスペースから作成されたページが削除されます。
- WebFOCUS Reporting Server アプリケーション - そのワークスペースから作成されたアプリケーションが削除されます。

注意：このカスケード削除プロセスでは、ワークスペース内のグループからユーザが削除されるのみです。ユーザ自体は削除されません。

手順　ワークスペースを削除するには

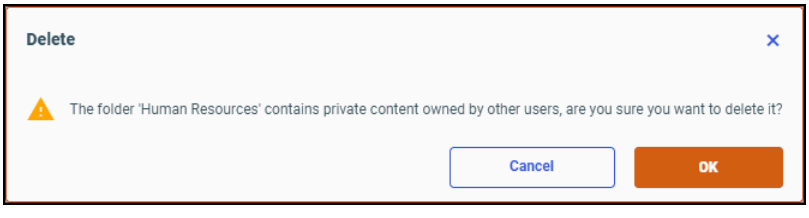
1. 管理者としてログインします。
2. WebFOCUS Hub または WebFOCUS ホームページから [ワークスペース] ビューを開き、リソースツリーを展開します。
3. リソースツリーの [ワークスペース] 下またはコンテンツエリアの [フォルダ] 下で、ワークスペースフォルダを右クリックして [削除] を選択します。

4. 下図のように、このワークスペースフォルダで作成されたリソースがすべて削除されることを確認するメッセージが表示されます。[OK] をクリックして、ワークスペースおよび関連するリソースを削除します。



注意：このメッセージには、最初にワークスペースに含まれていたリソースに基づいて、削除されるリソースのリストが表示されます。そのため、このメッセージに表示される詳細は、削除するワークスペースごとに異なります。

5. 下図のように、フォルダにプライベートコンテンツが格納されていることを警告するメッセージが表示された場合、[OK] をクリックしてワークスペースおよびプライベートコンテンツを削除するか、[キャンセル] をクリックしてワークスペースを削除せずに処理を終了します。



ワークスペース削除後のワークスペースユーザの管理

ワークスペースを削除すると、そのワークスペースに関連付けられているグループも自動的に削除されますが、この操作ではそのグループに割り当てられたユーザは削除されません。削除されたグループに属するユーザは、セキュリティセンターの [ユーザ] ウィンドウに残ります。削除されたグループのユーザを残す必要がない場合は、管理者がリポジトリからユーザを削除することができます。詳細は、463 ページの 「 ユーザを削除するには 」 を参照してください。

リソーステンプレートのカスタマイズ

リソーステンプレートを実行して作成された定義済みロールは、セキュリティセンターでカスタマイズすることができます。たとえば、AdvancedUsers グループに対して、レポートオブジェクトから InfoAssist の使用のみは許可するが、メタデータの使用を許可しない場合は、AdvancedUsers グループのロールから [InfoAssist from Metadata] 権限を削除することができます。

リソーステンプレートの実行により、既存のロールが上書きされることはありません。ワークスペースロールに加えた変更は保持され、作成済みのユーザを含め、すべてのワークスペース内のユーザに適用されます。

注意：ユーザのログイン時にロールが確認されます。そのため、ユーザロールに加えた変更は、ロール変更の保存後にログインしたユーザに即座に反映されます。ロールの変更時にすでにログインしていたユーザは、変更を有効にするために一度ログアウトし、再度ログインする必要があります。

ロールの変更方法についての詳細は、474 ページの 「 ロールの管理 」 を参照してください。

カスタムリソーステンプレートの作成

カスタムリソーステンプレートは、標準リソーステンプレートをカスタマイズし、使用する環境に固有のビジネス要件や運用要件をサポートするよう設計されたテンプレートです。カスタムリソーステンプレートを実行して作成されるワークスペースは、ルールとリソースの特殊な組み合わせに適合します。カスタムリソーステンプレートを使用すると、特定のグループやアクティビティで要求される権限およびリソースが、作成されるワークスペースすべてに自動的に組み込まれます。

カスタムリソーステンプレートを作成するには、管理者は、リソースと展開タイプ (作成予定のカスタムリソーステンプレートに最も適合する展開タイプ) を統合するワークスペースを作成し、そのワークスペースのフォルダを作成した後、ワークスペースのリソースと展開タイプの組み合わせに最も近い標準テンプレート scenario.xml ファイルのコピーを作成します。

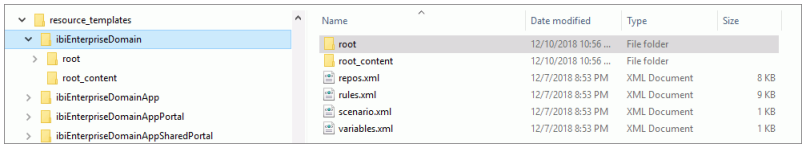
これらの 3 つのコンポーネントの準備が完了すると、管理者はカスタムテンプレートフォルダ内の scenario.xml ファイルをエクスポートして、リソーステンプレートに必要なファイル一式を作成します。ワークスペースに割り当てられるタイトルと名前は、新しいテンプレートのタイトルと名前になります。これらは、[ワークスペース] ノードのコンテキストメニューに追加され、ユーザが新しいワークスペースを作成する際に、そのカスタムリソーステンプレートがコンテキストメニューから選択可能になります。

管理者は、これらの基本手順を実行する以外に、カスタムリソーステンプレートに割り当てられる権限やロールをカスタマイズしたり、変数の調整やその表示順序を変更したりすることができます。

カスタムテンプレートを作成する前に、権限、ロール、リソース、グループ、IBFS サブシステムなどの概念を理解しておくことが重要です。これらの機能についての詳細は、453 ページの 「 ユーザの管理 」 の各トピックを参照してください。また、権限、ロール、ルールのどのような組み合わせが可能かを知るために、インストールに同梱されているリソーステンプレートを参照することをお勧めします。

リソーステンプレートの格納先およびファイル

デフォルト設定では、ビルトインリソーステンプレートおよびカスタムリソーステンプレートは、resources_templates フォルダに格納されます。このフォルダのディレクトリは、Windows では drive:¥ibi¥WebFOCUS82¥config¥、UNIX または Linux では install_directory/ibi/WebFOCUS82/config/ です。



統合インストールを使用する場合は、*drive*:¥ibi¥WebFOCUS_WFI¥WebFOCUS¥config¥resource_templates¥ibiEnterpriseDomain (Windows) または *directory*/ibi/WebFOCUS_WFI/WebFOCUS/config/resource_templates/ibiEnterpriseDomain (UNIX または Linux) に格納されます。

IBFS システムでは、リソーステンプレートは、レガシーホームページの WebFOCUS /FILE/IBFS_templates 下のリソースツリーに格納されます。このディレクトリは、リソースツリーを完全表示モードにした場合に表示されます。

下表は、各リソーステンプレートフォルダに作成されるリソースの説明です。

名前	タイプ	用途
root	ディレクトリ構造	レポートプロシジャやポータルページなどのリソースを格納します。一部のサブディレクトリは空ですが、これらのサブディレクトリも必要です。
repos.xml	ファイル	テンプレートにより作成されたすべてのリソースのプロパティを格納します。

名前	タイプ	用途
reposTree.xml	ファイル	テンプレートにエクスポートされたリソースのリストを格納します。トラブルシューティングや記録用として使用します。このファイルはテンプレートの作成時に自動的に作成されますが、テンプレートの実行時には必要ありません。 **注意：**このファイルはリソーステンプレートには含まれていません。
rules.xml	ファイル	テンプレートにより作成されたセキュリティルールを格納します。
scenario.xml	ファイル	リソーステンプレートの作成に必要な情報を格納します。このファイルはリソーステンプレートとともに提供され、カスタムテンプレートの作成時に使用されますが、テンプレートの実行時には必要ありません。
variables.xml	ファイル	リソーステンプレートの実行時に必要情報の入力を要求する方法を指定します。指定する項目には、各プロンプトの名前、プロンプトソート順、プロンプトフィールドのタイプ (normal または check) があります。

リソーステンプレート変数

ユーザがリソーステンプレートを使用する際に、WebFOCUS がそのテンプレートに変数が含まれているかどうかを特定し、必要に応じて各変数値の入力をユーザに要求します。リソース (例、フォルダ、グループ、ポータル、ポータルページ) の名前、説明、タイトルを指定することができます。また、フォルダおよび項目の概要を入力することもできます。入力した情報は、これらのリソースを閲覧するユーザや管理者に表示されます。

たとえば、テンプレートに名前と説明が事前定義された IBFS コンテンツフォルダを含めることができます。このフォルダは、空にしておくことも、サブフォルダやコンテンツを含めることもできます。また、フォルダ自体に、[ソート順] や [マイコンテンツフォルダの自動作成] プロパティなどのフォルダプロパティを定義しておくこともできます。このリソーステンプレートを実行すると、このフォルダの作成に使用するタイトルおよび名前の入力が要求されます。

[リソーステンプレート管理] インターフェースでは、変数に分かりやすい表示名を指定することができます。また、テンプレートダイアログボックスに表示する変数の順序や変数タイプを指定することもできます。

下表は、リソーステンプレートで使用される変数のタイプについての説明です。

変数タイプ	用途
normal	通常、このタイプの変数は、エンドユーザに提示されるグループの説明や、フォルダおよびポータルページのタイトルに使用します。normal 変数には、任意の文字データを使用できます。
check	通常、このタイプの変数は、IBFS リソースの名前に使用します。変数を確認するために入力されたデータは、IBFS パスのコンポーネントの規則で有効であるかどうかが確認されます。

エンタープライズリソーステンプレートによるモデルの作成

任意の IBFS リソースおよびセキュリティルールを、カスタムリソーステンプレートにエクスポートすることができます。最初に、カスタムテンプレートで使用する リソースおよびルールを作成する必要があります。たとえば、部門固有のコンテンツフォルダを作成するとともに、部門固有のグループと業務ごとのサブグループを作成します。また、共通のコンテンツフォルダやポータルへのアクセスをすべてのユーザに許可したり、テンプレートにカスタムロールを追加したりします。

必要な変更をすべて追加した後、カスタムテンプレートを後から使用できるようエクスポートすることができます。

手順　リソースおよびポリシーモデルを作成するには

この機能は、レガシーホームページからのみ使用できます。

1. レガシーホームページを開きます。
2. BI Portal のリソースツリーで [ワークスペース] ノードを右クリックし、[表示]、[リポジトリ表示] を順に選択します。
3. [ワークスペース] ノードを右クリックし、[新規作成] を選択します。
   - ❏ [エンタープライズワークスペース] を選択すると、企業内の部門および部署ワークスペースのカスタムテンプレートが作成されます。
   - ❏ [テナントワークスペース] を選択すると、SaaS プロバイダのクライアントワークスペースのカスタムテンプレートが作成されます。

4. [タイトル] テキストボックスに、「%%desc%%」と入力します。

   入力と同時に [名前] テキストボックスにも「%%desc%%」が自動的に割り当てられます。

5. [名前] テキストボックスに、小文字で「%%name%%」と入力します。
6. モデルワークスペースにオプションのリソースを含めるには、次の手順を実行します。
   a. ポータルを含めるには、[ポータルの作成] のチェックをオンにし、[ワークスペースポータル] を選択します。
   b. 共有ポータルページを含めるには、[ポータルの作成] のチェックをオンにし、[共有ポータルのワークスペースページ] を選択します。
   c. WebFOCUS Reporting Server 上に関連するアプリケーションディレクトリを追加するには、[Reporting Server アプリケーションの作成] のチェックをオンにします。

      注意：[Reporting Server アプリケーションの作成] オプションを使用する場合、WebFOCUS Reporting Server 上のアプリケーションディレクトリへのアクセス権限をワークスペースユーザに許可する方法を検討しておくことをお勧めします。詳細は、410 ページの 「 アクセスコントロールテンプレートの理解 」 を参照してください。
7. [OK] をクリックします。
8. リソーステンプレート処理が完了したことを示す確認メッセージで、[OK] をクリックします。

   [ワークスペース] ノード下に、「%%desc%%」というタイトルのコンテンツフォルダが表示されます。コンテンツフォルダ下に、[マイコンテンツ] および [非表示のコンテンツ] フォルダが表示されます。追加のリソース (例、ポータル) を含めた場合は、リソースツリーにこれらのリソースも表示されます。
9. 適用されたルールを確認するには、新しいコンテンツまたはポータルリソースを右クリックし、[このリソースのルール] を選択します。

   デフォルト設定では、[このリソースのルール] ダイアログボックスに、4 つの標準ワークスペースユーザグループと Managers グループのルールが表示されます。

手順　カスタムテンプレートフォルダを作成するには

デフォルト設定では、リソーステンプレートを実行、作成する権限は管理者のみに与えられています。

この機能は、レガシーホームページからのみ使用できます。

1. レガシーホームページを開きます。
2. BI Portal のリソースツリーで [ワークスペース] ノードを右クリックし、[表示]、[完全表示] を順に選択します。

3. [FILE] フォルダを展開し、[IBFS_templates] フォルダを右クリックして [新規フォルダ] を選択します。
4. [タイトル] テキストボックスに新しいテンプレートの名前、[概要] テキストボックスにテンプレートの説明を入力します。

   ここで入力した名前が、作成するカスタムリソーステンプレートの IBFS 名になります。テンプレートの表示タイトルは、後から変更することができます。

   注意：入力するテンプレート名は、IBFS の名前規則に準拠する必要があります。たとえば、ブランクはアンダースコア (_) で置き換えられます。IBFS の名前規則についての詳細は、346 ページの 「 IBFS ファイルシステムとサブシステム 」 を参照してください。
5. [OK] をクリックします。

   [IBFS_templates] ノード下に、新しいテンプレート名のフォルダが表示されます。

手順　カスタムテンプレート用の scenario.xml ファイルをコピーするには

scenario.xml ファイルには、カスタムリソーステンプレートにエクスポートされる内容が記述されています。カスタマイズを開始する前に、カスタムリソーステンプレートに必要なリソースに最も適合する scenario.xml ファイルのコピーをモデルテンプレートフォルダからカスタムリソースフォルダに移動する必要があります。標準リソーステンプレート xml ファイルのコピーを作成した後、このテンプレートから作成されるワークスペースに別の名前またはタイトルを使用するには、406 ページの 「 シナリオファイルを更新するには 」 の手順に従って、scenario.xml ファイルで割り当てられている値を更新する必要があります。

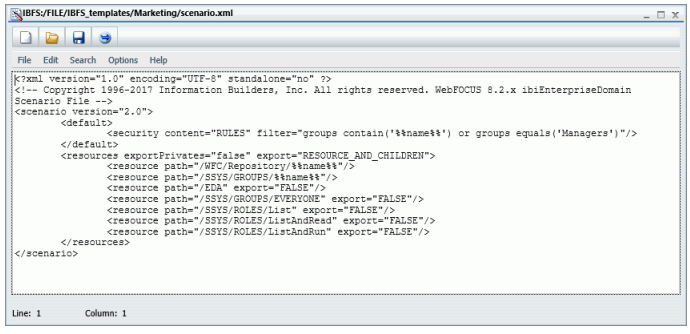
この機能は、レガシーホームページからのみ使用できます。

1. [IBFS_Templates] フォルダ下で、作成するワークスペースタイプとリソースに最も適合するテンプレートが格納されたフォルダを展開します。

   選択するフォルダは、モデルワークスペースの作成時に選択したワークスペースタイプとリソースの構成に一致させる必要があります。たとえば、モデルワークスペースがエンタープライズワークスペース (追加リソースなし) の場合は、[エンタープライズワークスペース] フォルダから scenario.xml ファイルをコピーします。
2. 選択したフォルダで scenario.xml ファイルを右クリックし、[コピー] を選択します。
3. 新しいカスタムテンプレートフォルダを右クリックし、[貼り付け] を選択します。

   scenario.xml ファイルのコピーがカスタムテンプレートフォルダに表示されます。
4. 新しいカスタムテンプレートフォルダで、scenario.xml ファイルを右クリックし、[編集] を選択します。

テキストエディタが開き、選択したテンプレートタイプの scenario.xml ファイルのコンテンツが表示されます。この例では、下図のように、エンタープライズリソーステンプレートの scenario.xml ファイルのコンテンツが表示されます。



セキュリティタグの属性によって追加のフィルタがこれらのルールに適用されます。これらのルールは、このカスタムテンプレートに基づいてワークスペースを作成する際にエクスポートされます。この例では、カスタムテンプレートでエクスポートされるルールは、サブジェクトが「%%name%%」または「Managers」に一致する EDA 上のルールのみです。

resources セクションで、プライベートコンテンツをエクスポートしないこと、および指定したリソースとその下位リソースをエクスポートすることを指定します。テンプレートに関連する各リソースは、それぞれの IBFS フルパスで指定します。場合によっては、リソースのパス名が「/WFC/Repository/%%name%%」のようにパラメータ化されていることがあります。また、「/SSYS/ROLES/List」のように静的なパス名が指定されている場合もあります。 サブシステムに対するルールはエクスポートするが、そのサブシステム内のリソースはエクスポートしない場合、「export="FALSE"」というオプションを使用してリソースパスを指定します。

注意：新しい変数を追加する場合、変数はすべて小文字で指定する必要があります。

5. 確認の完了後、テキストエディタを閉じます。

カスタムリソーステンプレートへのカスタマイズの追加

カスタムテンプレートに割り当てられたロールおよびルールを更新することができます。

この機能は、レガシーホームページからのみ使用できます。

手順　マイコンテンツフォルダの自動作成を無効にするには

エンタープライズリソーステンプレートから作成されたモデルフォルダでは、ユーザが個人のコンテンツを最上位フォルダに保存することができます。必要に応じて、この機能をカスタムテンプレートで無効にすることができます。

この設定は、WebFOCUS Hub の [ワークスペース] エリアまたは WebFOCUS ホームページから開く [プロパティ] パネルの [詳細] タブでも表示されますが、レガシーホームページ環境での変更をお勧めします。

この変更は、カスタムリソーステンプレートに追加可能なカスタマイズの 1 つです。

1. カスタムテンプレートから作成されたワークスペースフォルダを右クリックし、[プロパティ] を選択します。
2. [プロパティ] ダイアログボックスで、[マイコンテンツフォルダの自動作成] のチェックをオフにし、変更を保存します。

手順　共通のポータルまたはフォルダへのアクセスを有効にするには

テンプレートにより作成されたグループに、既存のポータルまたはコンテンツフォルダへのアクセスを許可したい場合があります。すべてのユーザに同一のアクセス権限を付与する場合は、共通リソースにアクセスするためのロールを、SSYS/GROUPS/EVERYONE グループに許可するルールを作成します。このルールをテンプレートに含めずに、後から使用する場合は、このルールや他のルールを後から作成することもできます。

この機能は、レガシーホームページからのみ使用できます。

共通のポータルまたはフォルダへのアクセスを有効にするには、次の手順を実行します。

1. 共通のポータルまたはフォルダを作成します。

   この時点で実際にポータルをデザインしたり、フォルダにコンテンツを追加したりする必要はありません。ここでポータルまたはフォルダを作成するのは、ルールの設定先となるリソースが存在する必要があるためです。
2. リソースを右クリックし、[セキュリティ]、[ルール] を順に選択します。
3. グループを選択し、次にロールおよびアクセスタイプを選択します。
4. [適用] をクリックし、[OK] をクリックしてプロパティを保存します。

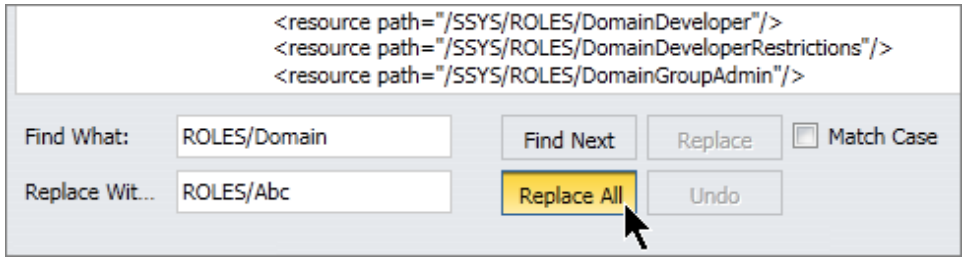
手順　シナリオファイルを更新するには

この機能は、レガシーホームページからのみ使用できます。

1. リソースツリーを [完全表示] モードにし、[FILE] ノード、[IBFS_templates] ノードを順に展開した後、テンプレートフォルダを展開します。

2. scenario.xml ファイルを右クリックし、[編集] を選択します。

   カスタムロールを作成した場合は、検索と置換を使用して、ファイル内のロール名をグローバルに変更することができます。たとえば、下図のように「SSYS/ROLES/Domain」を「SSYS/ROLES/Abc」に置換します。



3. 必要な変更を加えた後、[保存] をクリックします。

   注意：IBFS パス名では、大文字と小文字が区別されます。

4. 変更作業の完了後、[保存] をクリックします。
5. [ファイル] をクリックし、[終了] を選択してファイルを閉じます。

カスタムリソーステンプレートのエクスポート

カスタマイズがすべて完了した後、テンプレートをエクスポートします。

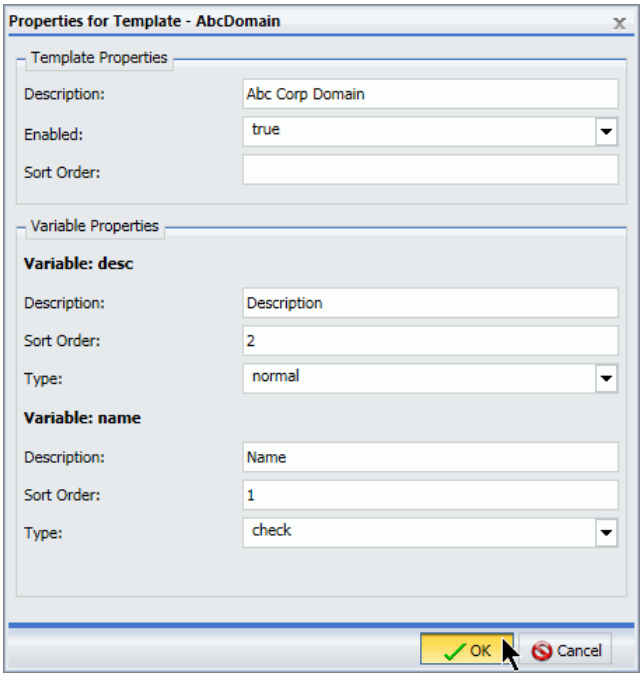
手順　カスタムリソーステンプレートをエクスポートするには

この機能は、レガシーホームページからのみ使用できます。

1. レガシーホームページを開きます。
2. リソースツリーを [完全表示] モードにし、テンプレートフォルダを右クリックして [テンプレートのエクスポート] を選択します。
3. テンプレート処理が完了したことを示す確認メッセージで、[OK] をクリックします。
4. テンプレートフォルダを右クリックし、[リフレッシュ] を選択して新しいリソースを表示します。

リソーステンプレートプロパティの更新

リソーステンプレートのプロパティを更新するには、テンプレートフォルダを右クリックし、[プロパティ] を選択します。下図のように、[テンプレートのプロパティ] ダイアログボックスが表示されます。



[テンプレートのプロパティ] ダイアログボックスでは、テンプレートの説明やソート順を編集したり、テンプレートの有効と無効 (利用可能なテンプレートリストでの表示と非表示) を切り替えたりできます。また、特定のテンプレートダイアログボックスに表示される変数の説明の変更、テンプレートダイアログボックスでの変数のソート順の指定、変数タイプの構成を行うこともできます。

注意：変数が IBFS パス名またはリソースに使用する値の入力を要求する場合は、変数の [タイプ] から [check (チェック)] を選択することで、入力された無効な IBFS 文字が拒否されるよう設定することができます。

モデルの削除

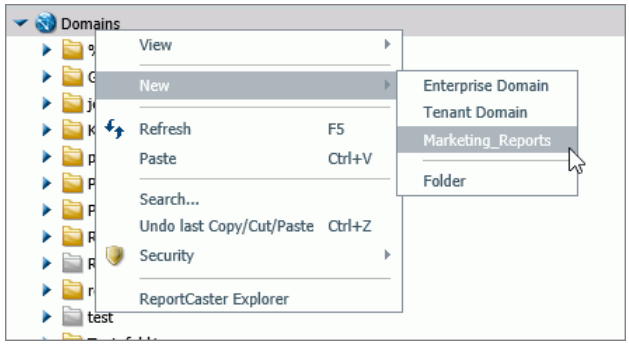
リソーステンプレートをエクスポートした後、リポジトリ内のリソースおよびポリシーモデルのオブジェクトは必要なくなります。テンプレートを再作成する予定がある場合や、テンプレートの別のバリエーションを作成する場合は、モデルオブジェクトを保持しておくことができます。それ以外の場合は、この時点でモデルオブジェクトを削除することができます。これらのモデルオブジェクトは、テンプレートを使用して後からいつでも作成することができます。

手順　新規カスタムリソーステンプレートをテストするには

[ワークスペース] ノード下で新規カスタムリソーステンプレートが存在することをテストするには、[ワークスペース] ノードのコンテキストメニューにそのテンプレートのコマンドが表示されること、および [新規ワークスペース] ダイアログボックス最上部のタイトルバーにカスタムリソーステンプレート名が表示されていることを確認する必要があります。

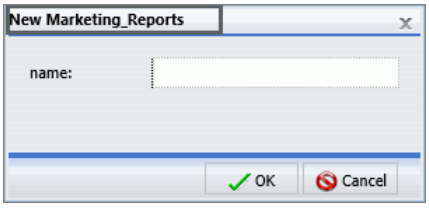
この機能は、レガシーホームページからのみ使用できます。

1. BI Portal のリソースツリーで、[ワークスペース] ノードを右クリックし、[新規作成] を選択します。
2. 下図のように、[新規作成] サブメニューにカスタムリソーステンプレート名が表示されていることを確認します。



3. カスタムリソーステンプレートに割り当てられた名前をクリックします (例、[マーケティング])。

4. 下図のように、[新規ワークスペース] ダイアログボックス最上部のタイトルバーにカスタムリソーステンプレート名が表示されていることを確認します。



5. 386 ページの 「 ワークスペースを作成するには 」 の手順に従ってワークスペースを作成します。

   新しいワークスペースのリソースおよび権限がカスタムリソーステンプレートのリソースおよび権限に適合していることを確認します。

アクセスコントロールテンプレートの理解

WebFOCUS Reporting Server アクセスコントロールテンプレートを WebFOCUS リソーステンプレートと併用すると、エンタープライズ展開または SaaS テナント展開のユーザにアクセスコントロールの統合ソリューションが提供されます。

WebFOCUS Reporting Server で定義されるアクセスコントロールテンプレートは、グループ、ロール、権限で構成されるテンプレートです。Reporting Server でアクセスコントロールテンプレートを定義しておくと、WebFOCUS でこれらのグループに属するユーザに、その Reporting Server 上のアプリケーションディレクトリおよび使用可能な機能への適切なアクセスレベルが自動的に付与されます。たとえば、Marketing/AdvancedUsers グループのみに割り当てられているユーザは、marketing アプリケーションディレクトリに存在するメタデータを使用してレポートを作成することはできますが、finance アプリケーションディレクトリに存在するメタデータを使用することはできません。また、Marketing/Developers グループに割り当てられているユーザは、Reporting Server ブラウザインターフェースのツールを使用して接続やエージェントをモニタすることはできますが、このグループに属していない marketing ユーザはこの操作を実行することはできません。

管理者がサポートするグループ数が少ない場合は、Reporting Server ブラウザインターフェースを使用して各アプリケーションディレクトリを手動で作成し、それぞれのアプリケーションディレクトリへのアクセス権限を構成することができます。一方、グループ名とアプリケーションディレクトリ間のアクセス権限にパターンがある場合は、Reporting Server アクセスコントロールテンプレートを実装する方法が適しています。この方法は使い勝手がよく、時間が節約されるとともに、結果の整合性が確保されます。Reporting Server アクセスコントロールテンプレートを使用すると、Reporting Server アプリケーションディレクトリのアクセス権限と適切なサーバロールへのユーザ割り当てが、 リソーステンプレートに自動的に統合されます。

ただし、明示的に登録されたグループは、アクセスコントロールテンプレートで一致したグループより優先されます。WebFOCUS Reporting Server で明示的に登録されたグループのユーザが WebFOCUS Reporting Server に接続する場合、ユーザ認可は常にそのグループから取得され、アクセスコントロールテンプレートによる一致で最も近いグループからは取得されません。

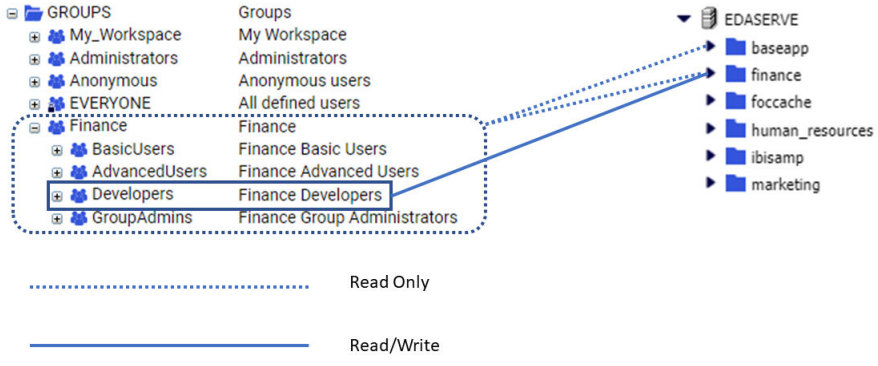
このセクションに記載されているアクセスコントロールテンプレートは、ユーザアクセスの標準モデルに準拠しています。このモデルでは、リソーステンプレートからワークスペースが作成され、デフォルト設定でそのワークスペース下に 4 つのサブグループが作成されます (Basic Users、Advanced Users、Developers、Group Administrators)。管理者は、これらの 4 つのサブグループを使用して、標準的な 4 つのユーザタイプのニーズと役割に応じてワークスペースリソースへのアクセスを可能にするかどうかを調整することができます。

Reporting Server アクセスコントロールテンプレートのビジネス要件の定義

アクセスコントロールテンプレートを作成する最初の手順として、複数のグループ、各グループで使用可能にするコンテンツ、そのコンテンツへの適切なアクセスレベルを識別するビジネス要件を定義します。このセクションで説明するアクセスコントロールテンプレートの場合、次のビジネス要件を考慮します。

1. すべてのユーザは、ibisamp ディレクトリおよび baseapp ディレクトリへの読み取りアクセス権限を所有する。
2. 管理者およびマネージャは、すべてのワークスペースのアプリケーションディレクトリへの読み取り/書き込みアクセス権限を所有する。
3. ワークスペースのユーザは、ユーザ自身が属するワークスペースのアプリケーションディレクトリへの読み取りアクセス権限を所有する。
4. ワークスペースの開発者は、開発者自身が属するワークスペースのアプリケーションディレクトリへの読み取り/書き込みアクセス権限を所有する。
5. ワークスペースのユーザおよび開発者は、ユーザ自身が属するワークスペースのアプリケーションディレクトリ、ibisamp ディレクトリ、baseapp ディレクトリを除いて、その他のアプリケーションディレクトリへのアクセス権限を所有しない。

下図は、これらのビジネス要件を示しています。この例では、ワークスペースのユーザおよび開発者は Finance ワークスペースに割り当てられています。図を分かりやすくするために、管理者およびマネージャのアクセス権限を示す線は省略されています。



アクセスコントロールテンプレートを構成する際は、これらの基本要件を変更することができます。たとえば、すべてのユーザが ibisamp ディレクトリおよび baseapp ディレクトリへのアクセス権限を必要としない場合は、これらのディレクトリへのアクセスを許可するオプションをすべてのユーザから削除することができます。

上記の例に記載されているビジネス要件は、アクセスコントロールテンプレートの基本的な構成を示すもので、このセクションの残りの部分、および後述の「 アクセスコントロールテンプレートテキスト」セクションにも使用されます。

アクセスコントロールテンプレートの正規表現とグループ ID パターン

正規表現とグループ ID パターンを使用すると、アクセスコントロールテンプレートをさまざまな範囲のグループに適用することができます。グループ名がグループ ID パターンに一致すると、そのグループにテンプレート自体およびテンプレートで構成された WebFOCUS Reporting Server のアクセスロールと権限が自動的に適用されます。管理者は、グループ ID パターンの構成に正規表現を使用することで、アクセスコントロールテンプレートの適用範囲を、厳密に定義したパターンに一致する少数のグループに制限したり、最低条件で定義したパターンに一致する多数のグループに拡大したりできます。デフォルト設定では、次の正規表現が使用できます。

- **(.+)** すべてのグループ名を取得します。このパターンには次の要素が含まれます。
  - ワイルドカード **(.)** は、拡張文字セット内の文字を含むすべての文字に一致します。
  - プラス記号 **(+)** は、先行するワイルドカードが 1 つまたは複数の文字に一致することを示します。
- **(.**+)/Developers のパターンは、すべてのワークスペース内の Developers グループを取得します。このパターンでは、**/Developers** という単語により、**(.+)** パターンを /Developers 文字列を末尾に含むグループ名に制限します (例、Retail_Samples/Developers)。

アクセスコントロールテンプレートの構成では、変数として 2 つのプレースホルダ語句が使用されます。

- **modelgrp** この語句が指定された正規表現では、すべてのグループが取得されます。これらのグループは、[一般ユーザ] ロールと見なされます。「modelgrp/developers」というパターンに一致する名前のグループは、[アプリケーション管理者] ロールと見なされます。
- **modelapp** この語句が指定された正規表現では、すべてのアプリケーションが取得されます。

この構成例では、これらの値は WebFOCUS Reporting Server ブラウザインターフェースの [テンプレートの登録] ページの各テキストボックスに割り当てられます。また、これらの値は、アクセスコントロールテンプレート設定が記述された構成ファイルにも割り当てられます。

アクセスコントロールテンプレートの作成

アクセスコントロールテンプレート機能は、認証および認可のさまざまな構成に対応しています。ただし、このセクションの各トピックでは、内部認証を使用し、グループをトラステッド接続経由で WebFOCUS Reporting Server に送信してユーザを認可する方法を前提にしています。

アクセスコントロールテンプレートを作成する方法には、次の 2 種類があります。

- **コピーと貼り付け**　このマニュアルからアクセスコントロールテンプレートのテキストをコピーし、WebFOCUS Reporting Server の admin.cfg ファイルに貼り付けます。

  この方法では、アクセスコントロールテンプレートがすばやく作成されます。サンプルテンプレートに加える変更が微小で、サンプルテンプレート内のグループアクセス権限構成を現在の環境に適用できる場合は、この方法が適しています。

- **手動構成**　Reporting Server ブラウザインターフェースで環境を構成し、このブラウザインターフェースからアクセスコントロールテンプレートを生成します。

  この方法は、より多くの時間と労力を要します。新しいアクセスコントロールテンプレートの要件がこの標準テンプレートに合致しない場合は、この方法が適しています。

アクセスコントロールテンプレートの要件

アクセスコントロールテンプレートの作成方法に関係なく、アクセスコントロールテンプレートを作成する際は、次のことを事前に実行する必要があります。

- WebFOCUS Client の管理コンソールで WebFOCUS Reporting Server セキュリティ設定を構成して、信頼されるユーザ ID とグループを WebFOCUS Client から WebFOCUS Reporting Server に転送可能にする。
- WebFOCUS Reporting Server ブラウザインターフェースでセキュリティプロバイダの [Trusted] 設定を [y] (はい) に変更して、信頼されるユーザ ID とグループを WebFOCUS Reporting Server で受容可能にする。
- Reporting Server ブラウザインターフェースの [サービスのプロセス統計とリスナ] でトラステッド通信をサポートするホストを受容するよう構成を変更して、トラステッド接続を特定のホストに限定する。
- Reporting Server ブラウザインターフェースの [アクセスコントロール] 設定で [prepend_provider_name] を [n] (いいえ) に変更して、グループ名またはユーザ名の登録時にプライマリセキュリティプロバイダ名が自動的に接頭語として追加される機能を無効にする。[アクセスコントロール] 設定には、Reporting Server ブラウザインターフェースの [アクセスコントロール] ページからアクセスできます。この設定を無効にすると、後から別のプライマリセキュリティプロバイダへの切り替えが可能になります。たとえば、これらのユーザやグループのロールを再登録せずに、内部認証から Active Directory によるユーザ認証に切り替えたい場合があります。

これらの要件の構成方法については、以下のトピックに記載されています。

この構成をサポートする機能は、レガシーホームページから簡単に使用できます。

手順 WebFOCUS Client から WebFOCUs Reporting Server へのトラステッド接続を設定するには

次の手順は、デフォルト構成の内部認証および内部認可に基づいています。この手順をサポートする機能は、レガシーホームページでのみ使用できます。

現在の WebFOCUS 環境で内部認証および内部認可が使用されていることを確認するには、管理コンソールの [セキュリティ] タブを開き、[セキュリティの構成] フォルダ下で [外部] をクリックします。[外部セキュリティを有効にする] のチェックがオフの場合、現在の WebFOCUS 環境で内部認証が使用されます。[ユーザ認可] グループで [内部] オプションが選択されている場合、現在の WebFOCUS 環境で内部認可が使用されます。このように構成されていない場合は、技術サポートに問い合わせて、トラステッド接続に関する情報を確認してください。

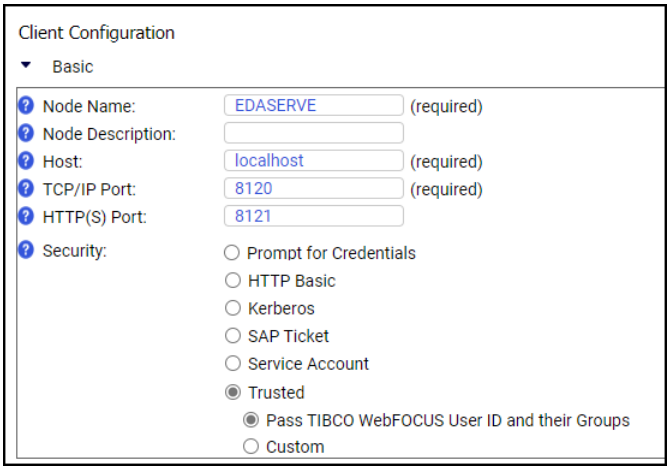
この手順では、「EDASERVE」という WebFOCUS Reporting Server へのトラステッド接続を設定し、他の WebFOCUS Reporting Server へのトラステッド接続は設定しません。この Reporting Server を使用するのは、デフォルトリソーステンプレートの構成でも、WebFOCUS Reporting Server として「EDASERVE」が指定されているためです。別の WebFOCUS Reporting Server へのトラステッド接続を設定する必要がある場合は、デフォルトリソーステンプレートのそれぞれで、「EDASERVE」を別の WebFOCUS Reporting Server の名前に置き換える必要があります。

1. 管理コンソールの [構成] タブで、[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。
2. [EDASERVE] ノードをダブルクリックします。
3. [Client の構成] ページの [セキュリティ] エントリ下で [Trusted] オプションを選択します。

   ページがリフレッシュされ、2 つのオプションが表示されます。[WebFOCUS ユーザ ID とグループの送信] オプションが自動的に選択されます。
4. [ホスト] テキストボックスで、次のように値を指定します。
   a. WebFOCUS Client と WebFOCUS Reporting Server が同一マシンにインストールされている場合は、「localhost」と入力します。
   b. WebFOCUS Client と WebFOCUS Reporting Server が異なるマシンにインストールされている場合は、WebFOCUS Reporting Server のホストマシンの名前または IP アドレスを入力します。

      この値は、他のクライアントからのトラステッド接続を無効にするために、後から WebFOCUS Reporting Server の RESTRICT_TO_IP 設定にも割り当てます。

5. 下図のように構成されたことを確認します。



注意：WebFOCUS Client と WebFOCUS Reporting Server が異なるマシンにインストールされている場合は、「localhost」を WebFOCUS Reporting Server のホスト名に置き換える必要があります。

6. [保存] をクリックします。
7. WebFOCUS Reporting Server 構成の変更が正しく保存されたことを示すメッセージで、[OK] をクリックします。
8. 管理コンソールのメニューバーで、[キャッシュのクリア] をクリックします。
9. すべてのキャッシュがクリアされたことを示すメッセージで、[OK] をクリックします。
10. 現在のセッションからログアウトします。

手順　セキュリティプロバイダをトラステッドセキュリティプロバイダとして指定するには

アクセスコントロール機能が動作するには、セキュリティプロバイダをアクティブにした状態で WebFOCUS Reporting Server を実行する必要があります。このプロバイダは、PTH <内部>、LDAP、OPSYS、DBMS プロバイダのいずれかにすることも、CUSTOM プロバイダ (例、リレーショナルデータベース管理システム (RDBMS) にアクセスするユーザを認可) にすることもできます。

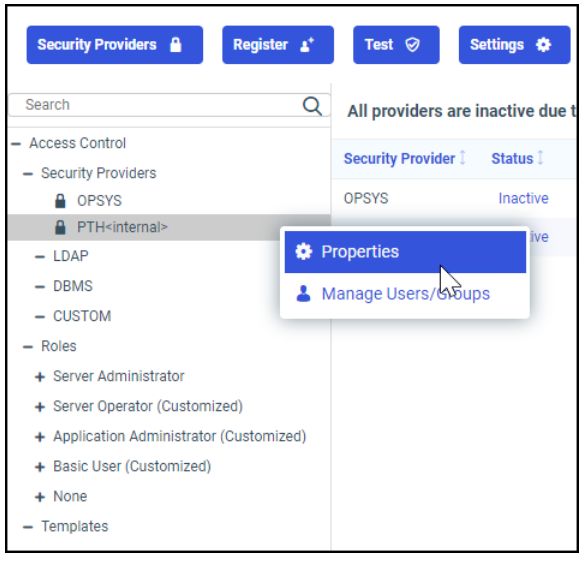
1. WebFOCUS Hub のサイドナビゲーションウィンドウで、[管理センター] をクリックし、[アクセスコントロール] を選択します。

   または

WebFOCUS ホームページで、[設定]、[WebFOCUS Server] を順に選択して、Reporting Server ブラウザインターフェースを開きます。メニューバーで、[ツール]、[アクセスコントロール] を順に選択し、[アクセスコントロール] ページを開きます。

2. [アクセスコントロール] フォルダ下で、WebFOCUS Reporting Server でアクティブ状態のセキュリティプロバイダのノードを右クリックし、[プロパティ] を選択します。

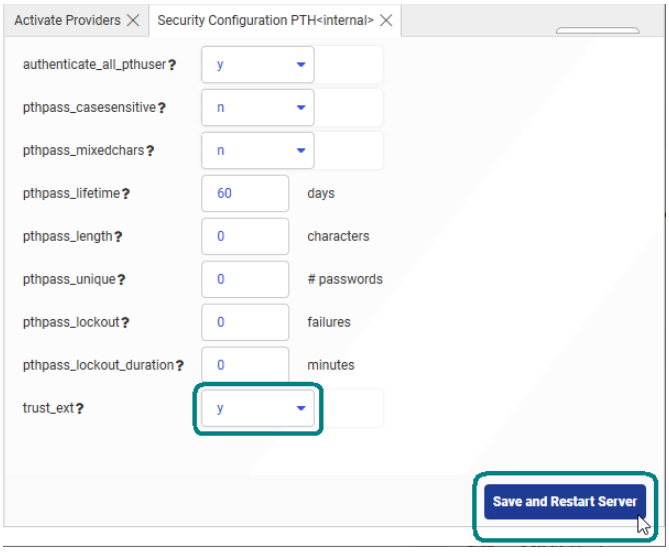
   たとえば、下図のように [PTH <内部> (アクティブ)] を右クリックし、[プロパティ] を選択します。



   注意：Windows プラットフォームの場合、OPSYS プロバイダでトラステッド通信を使用することはできません。

3. 選択したセキュリティプロバイダの構成ページで、[trust_ext] ドロップダウンリストまで下方向へスクロールし、値 [y] が表示されることを確認します。 表示されない場合は、[trust_ext] ドロップダウンリストで [y] を選択し、[保存] をクリックします。

たとえば、下図のように、[セキュリティの構成 PTH <内部>] ページで、[trust_ext] リストから [y] を選択し、[保存] をクリックします。



プロパティパネルが閉じた後、WebFOCUS Reporting Server を手動で再起動します。

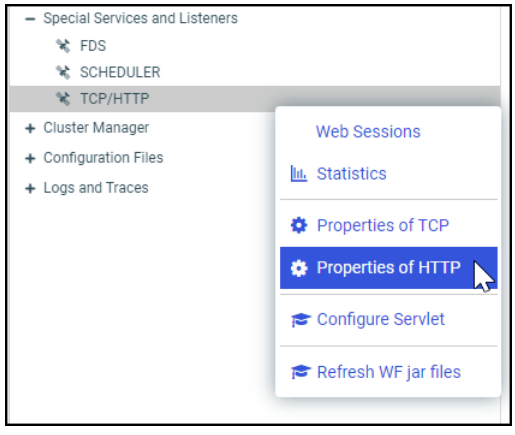
注意：[PTH <内部> (アクティブ)] セキュリティプロバイダは、デフォルト設定でトラステッドセキュリティプロバイダとして設定されています。構成されていない別のセキュリティプロバイダを選択する場合は、最初にセキュリティプロバイダの構成を完了しておく必要があります。詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』の「認証の構成」を参照してください。

4. 「ワークスペース再起動中です」というメッセージでは、待機します。
5. [ツール]、[アクセスコントロール] を順に選択し、[PTH <内部> (アクティブ)] を右クリックして新しいトラステッド構成を確認します。

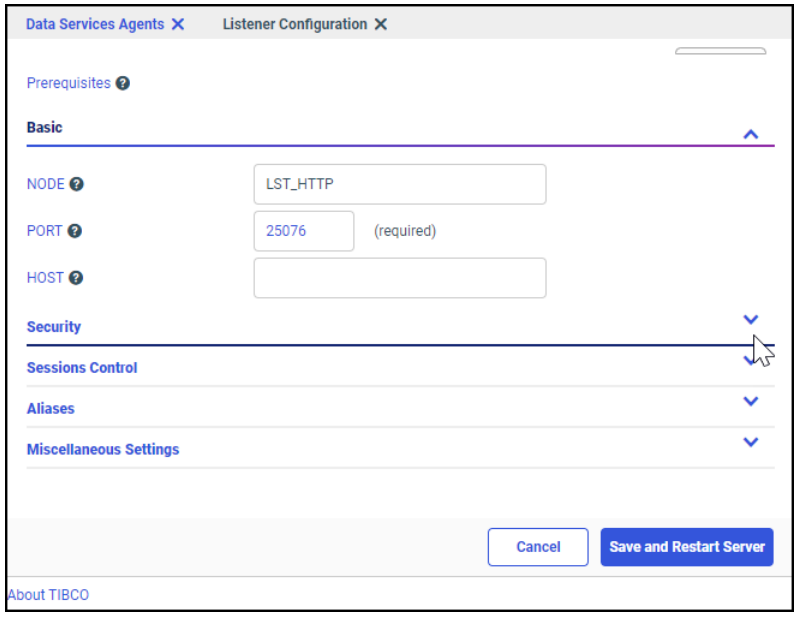
手順　トラステッドアクセスを特定のホストに制限するには

1. Reporting Server ブラウザインターフェースで、[ワークスペース] ページを開きます。
2. ワークスペースツリーで、[サービスのプロセス統計とリスナ] を展開します。

3. 下図のように、[TCP/HTTP] ノードを右クリックし、[TCP のプロパティ] を選択します。



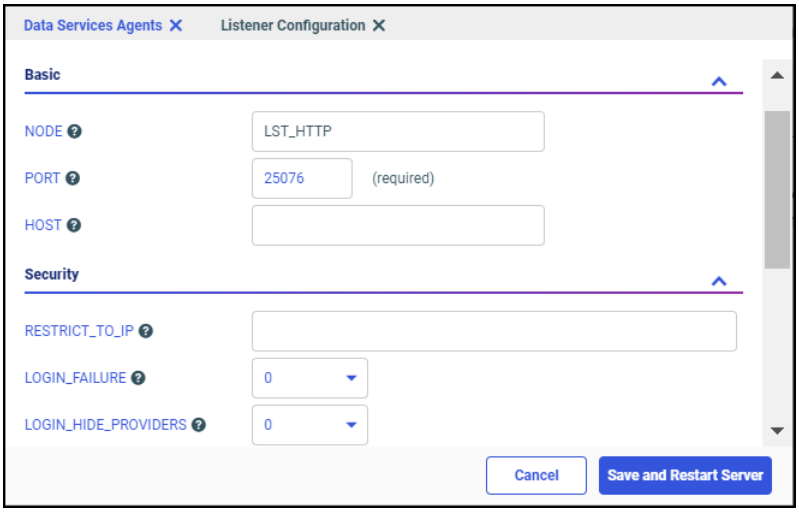
4. 下図のように、[セキュリティ] セクションを展開します。



5. WebFOCUS Reporting Server が WebFOCUS Client および Distribution Server と同一のホストマシンにインストールされている場合は、[RESTRICT_TO_IP] テキストボックスに「localhost」と入力します。

WebFOCUS Reporting Server が WebFOCUS Client および Distribution Server と異なるホストマシンにインストールされている場合は、この WebFOCUS Reporting Server にアクセスする WebFOCUS Client および Distribution Server すべての TCP/IP アドレスまたは名前を入力します。

6. 下図のように、[保存してリスナを再起動] をクリックします。



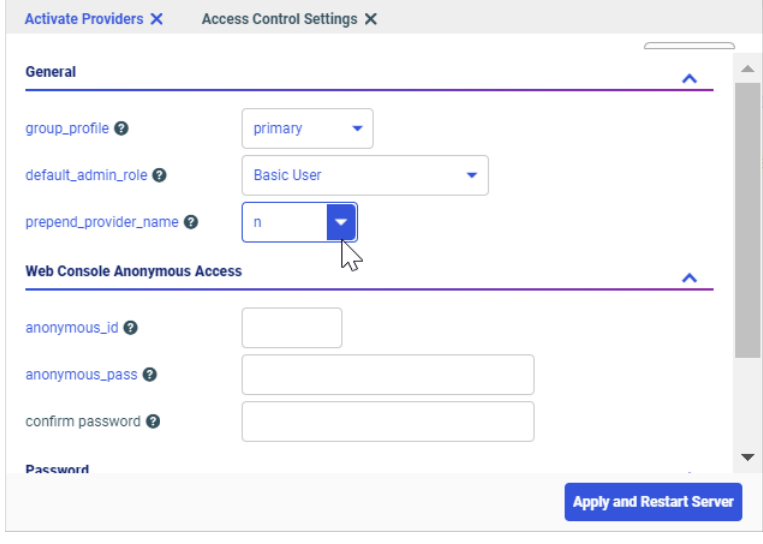
7. 「サーバの再起動によりセッションが失われました」というメッセージが表示され、ログインページが開いた場合は、インストールで使用されたサーバ ID およびパスワードを入力し (通常は両方とも「srvadmin」)、[ログイン] をクリックします。

   Reporting Server ブラウザインターフェースが再度開き、[アプリケーション] タブが表示されます。

手順　グループ名またはユーザ名へのプライマリセキュリティプロバイダ接頭語の追加を無効にするには

この設定を無効にすると、後から別のプライマリセキュリティプロバイダへの切り替えが可能になります。たとえば、これらのユーザやグループのロールを再登録せずに、内部認証から Active Directory によるユーザ認証に切り替えたい場合があります。

1. [アクセスコントロール] ページで、[設定]、[アクセスコントロール] を順に選択し、[アクセスコントロールの設定] タブを開きます。下図のように、[prepend_provider_name] ドロップダウンリストで [n] を選択します。



この設定により、プライマリプロバイダにグループやユーザを登録する際に、グループ名およびユーザ名の先頭にプロバイダ名が追加されなくなります。管理者は、この構成変更により、登録済みのユーザやグループの関係を失わずに、後から別のセキュリティプロバイダ (例、Active Directory、LDAP) に切り替えることができます。

2. [適用してサーバを再起動] をクリックします。

「ワークスペース再起動中です。しばらくお待ちください。」というメッセージが表示され、WebFOCUS Reporting Server が再起動すると、Reporting Server ブラウザインターフェースの [アプリケーション] タブに戻ります。

「サーバの再起動によりセッションが失われました」というメッセージが表示され、ログインページが開いた場合は、インストールで使用されたサーバ ID およびパスワードを入力し (通常は両方とも「srvadmin」)、[ログイン] をクリックします。

3. Reporting Server ブラウザインターフェースを閉じ、ログアウトします。

アクセスコントロールテンプレート作成方法の選択

要件の構成後、次の 2 つの方法のいずれかを使用してアクセスコントロールテンプレートを作成することができます。

このセクションに記載されているテキストをコピーして貼り付ける方法でテンプレートを作成する場合は、422 ページの 「 コピーと貼り付けによるアクセスコントロールテンプレートの作成 」 へ進みます。

テンプレートに含めるグループすべてを直接構成して登録する方法でテンプレートを作成する場合は、427 ページの 「 手動構成によるアクセスコントロールテンプレートの作成 」 へ進みます。

コピーと貼り付けによるアクセスコントロールテンプレートの作成

バージョン 8.2 SP01 以降、WebFOCUS Reporting Server をインストールすると、admin.cfg という管理構成ファイルが自動的に作成されます。次の admin.cfg ファイル (*drive*:¥ibi¥profiles) のサンプルテキストには、オペレーティングシステムのユーザ ID およびデフォルト PTH <内部> セキュリティプロバイダが定義されたデフォルト構成が含まれています。

サンプルデフォルト admin.cfg

```
admin_id = OPSYS¥DOMAIN¥operatingsystemuserid
BEGIN
  admin_level = SRV
END
admin_id = PTH¥srvadmin
BEGIN
  admin_password = {AES}encrytpedpassword
  admin_level = SRV
END
admin_level = APP
BEGIN
  admin_privilege = NODPT,NOSYS,METAP,DATMG,PRSAV,PRDFR,PRRPT,
                    PROUT,MONIT,CHGPW,MONUS,MONGR,KILT3,KILGR,
                    APATH,DBMSC,UPROF,APROF
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT);AREAD,ARWRT,PRRUN,ALIST
END
admin_level = USR
BEGIN
  admin_privilege = NODPT,NOSYS,PROUT,CHGPW,MONUS,KILT3,APATH,
                    DBMSC,UPROF
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT);AREAD,ARWRT,PRRUN,ALIST
END
admin_level = OPR
BEGIN
  admin_privilege = NODPT,NOSYS,MONIT,KILAL,STPSV,CHGPW,MONUS,
                    MONGR,KILT3,KILGR
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT);AREAD,ARWRT,ALIST
END
>>>Replace this line with all lines from the WebFOCUS
Access Control Template Text.<<<
[Access Control]
authenticate_all_pthuser = y
prepend_provider_name = n
```

説明

operatingsystemuserid

実際のオペレーティングシステムユーザ ID です。

encrytpedpassword

WebFOCUS Reporting Server で、cfgfile_cipher で指定されたキーを使用して暗号化される、上記ユーザ ID のパスワードです。

デフォルト設定では、このテンプレートにより、各ワークスペースの BasicUsers、AdvancedUsers、GroupAdmins グループに割り当てられるユーザすべてに USR ロールが割り当てられます。通常、これらのグループは、Workspace¥BasicUsers、Workspace¥AdvancedUsers、Workspace¥GroupAdmins と記述されます。ここで、「Workspace」は各ユーザの割り当て先ワークスペースの名前を表します。たとえば、「Finance¥BasicUsers」です。これらのグループのユーザが WebFOCUS Reporting Server に接続すると、そのユーザが属するワークスペースのアプリケーションフォルダ内のリソースに対して [読み取り]、[実行]、[リスト] 権限が付与されます。

また、このテンプレートにより、Workspace¥Developers グループに APP ロールが割り当てられます。このグループのユーザが WebFOCUS Reporting Server に接続すると、そのユーザが属するワークスペースのアプリケーションフォルダ内のリソースに対して [読み取り]、[書き込み]、[リスト]、[実行] 権限が付与されるとともに、開発者としての役割をサポートするための追加権限が付与されます。

この標準的な構成のアクセスコントロール設定をアクセスコントロールテンプレートで置き換えるには、以下の「アクセスコントロールテンプレートテキスト」セクションからテキストをコピーし、既存の admin.cfg ファイルに貼り付けます。この追加により、Administrators グループ、Managers グループ、および 415 ページの 「 WebFOCUS Client から WebFOCUs Reporting Server へのトラステッド接続を設定するには 」 で定義されたトラステッド接続で WebFOCUS Reporting Server に接続するすべてのワークスペースグループに、適切な認可を付与するアクセスコントロールテンプレートが作成されます。

アクセスコントロールテンプレートテキスト

このセクションに記載されているアクセスコントロールテンプレートは、このテンプレートが割り当てられた WebFOCUS Reporting Server に接続する、信頼されるユーザおよびグループのすべてに適用されます。このテンプレートでは、グループ ID パターンと正規表現を使用して、ほとんどの WebFOCUS 環境に適用可能な構成を効率的に作成します。このテンプレートは、すべてのユーザに ibisamp および baseapp ディレクトリへの [読み取り]、[リスト]、[実行] 権限を付与するアクセスモデルをベースにしています。

```
admin_group = Administrators
BEGIN
  admin_level = SRV
  admin_description = WebFOCUS Administrators
END
admin_group = Managers
BEGIN
  admin_level = SRV
  admin_description = WebFOCUS Managers
END
admin_group = modelgrp/Developers
BEGIN
  admin_level = APP
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
  admin_privilege = (APPROOT)/modelapp;AREAD,ARWRT,PRRUN,ALIST
  admin_privilege = (APPROOT);ANONE
  admin_privilege = ADPTP,NODPT,NOSYS,METAP,DATMG,PRSAV,PRDFR,
                    PRRPT,PROUT,MONIT,SRVLG,KILT3,APATH
  admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group = modelgrp
BEGIN
  admin_level = USR
  admin_privilege = NODPT,NOSYS,PRDFR,PRRPT,PROUT,KILT3,APATH
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
  admin_privilege = (APPROOT)/modelapp;AREAD,PRRUN,ALIST
  admin_privilege = (APPROOT);ANONE
  admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group_template = (.+)/Developers
BEGIN
  model_group = modelgrp/Developers
  file_replace_pattern = (modelapp)
END
admin_group_template = (.+)
BEGIN
  model_group = modelgrp
  file_replace_pattern = (modelapp)
  exclude_groups = (/)
END
```

手順　アクセスコントロールテンプレートをコピーして貼り付けるには

1. WebFOCUS Client で、*drive:*¥ibi¥profiles ディレクトリに移動します。
2. admin.cfg ファイルをテキストエディタで開きます。

3. 下方向へスクロールし、次の行を特定します。

```
[Access Control]
authenticate_all_pthuser = y
prepend_provider_name = n
```

4. 次のテキストをコピーし、[admin_level = OPR] セクションの最終ステートメントの後、[Access Control] タイトルの前に貼り付けます。

```
admin_group = Administrators
BEGIN
  admin_level = SRV
  admin_description = WebFOCUS Administrators
END
admin_group = Managers
BEGIN
  admin_level = SRV
  admin_description = WebFOCUS Managers
END
admin_group = modelgrp/Developers
BEGIN
  admin_level = APP
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
  admin_privilege = (APPROOT)/modelapp;AREAD,ARWRT,PRRUN,ALIST
  admin_privilege = (APPROOT);ANONE
  admin_privilege = ADPTP,NODPT,NOSYS,METAP,DATMG,PRSAV,PRDFR,
                    PRRPT,PROUT,MONIT,SRVLG,KILT3,APATH
  admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group = modelgrp
BEGIN
  admin_level = USR
  admin_privilege = NODPT,NOSYS,PRDFR,PRRPT,PROUT,KILT3,APATH
  admin_privilege = *;ANONE
  admin_privilege = (APPROOT)/baseapp;AREAD,PRRUN,ALIST
  admin_privilege = (APPROOT)/modelapp;AREAD,PRRUN,ALIST
  admin_privilege = (APPROOT);ANONE
  admin_privilege = (APPROOT)/ibisamp;AREAD,PRRUN,ALIST
END
admin_group_template = (.+)/Developers
BEGIN
  model_group = modelgrp/Developers
  file_replace_pattern = (modelapp)
END
admin_group_template = (.+)
BEGIN
  model_group = modelgrp
  file_replace_pattern = (modelapp)
  exclude_groups = (/)
END
```

5. (オプション) ユーザが ibisamp または baseapp アプリケーションディレクトリにアクセスする必要がない場合は、Application Control セクションテキストの [admin_group = modelgrp] および [admin_group = modelgrp/Developers] セクションから、各アプリケーションディレクトリに関連する行を削除します。
6. admin.cfg ファイルを保存して閉じます。

   必要に応じて構成作業を続行し、利用可能なリソースの範囲を制限します。構成の完了後、443 ページの 「 リソーステンプレートとアクセスコントロールテンプレートの統合ソリューションのテスト 」 の説明に従って、統合ソリューション全体をテストすることができます。

手動構成によるアクセスコントロールテンプレートの作成

アクセスコントロールテンプレートを手動で作成する方法では、管理者が Reporting Server ブラウザインターフェースを使用してテンプレートモデルを作成し、そのモデルに基づいてアクセスコントロールテンプレートを登録する必要があります。管理者は、テンプレートモデルを構成した後、そのモデルに基づいて各テンプレートをグループに登録します。この登録により、特定のグループに属するユーザがトラステッド接続で WebFOCUS Reporting Server にリクエストを送信する際に使用されるアクセスコントロールテンプレートが識別されます。

テンプレートモデルの作成

テンプレートモデルは、WebFOCUS Reporting Server に接続可能なグループ、およびこれらのグループに付与される権限を構成したものです。このテンプレートモデルに基づいて、アクセスコントロールポリシーが WebFOCUS Reporting Server 設定に直接組み込まれます。

以下は、テンプレートモデルを作成する手順の概要です。

1. Administrators グループを作成し、そのグループを WebFOCUS Reporting Server の [サーバ管理者] ロールに登録します。
2. Managers グループを作成し、そのグループを WebFOCUS Reporting Server の [サーバ管理者] ロールに登録します。
3. model アプリケーションを作成します。
4. model グループを作成し、[一般ユーザ] ロールに登録します。
5. model/developers グループを作成し、そのグループを [アプリケーション管理者] ロールに登録します。

上記のように Administrators および Managers グループを作成、登録すると、 Administrators グループおよび Managers グループに属するユーザすべてが、サーバ管理者として WebFOCUS Reporting Server および Reporting Server ブラウザインターフェースにシングルサインオンでアクセスできるようになります。

model グループおよび model/developers グループは、ワークスペースグループを表します。これらのグループを作成、登録すると、ワークスペースのサブグループに属するユーザが、一般ユーザまたは開発者として WebFOCUS Reporting Server にシングルサインオンで接続できるようになります。model アプリケーションは、トラステッド接続で WebFOCUS Reporting Server に接続したユーザが作成可能なアプリケーションフォルダを表します。前述のように、このテンプレートモデルは、標準的なアクセス権限のデフォルト構成を適用します。ただし、管理者は、Reporting Server ブラウザインターフェースの各種ツールを使用して、現在の WebFOCUS 環境のセキュリティ要件に適合する、あらゆる種類のアクセスコントロールテンプレートを作成することができます。

手順　WebFOCUS Reporting Server ブラウザインターフェースにログインするには

グループ権限を表示、確認、更新するために、アクセスコントロールテンプレートの構成を開始する前に WebFOCUS Reporting Server をセキュリティモード ON で開始しておく必要があります。

1. 管理者としてログインします。
2. WebFOCUS Hub で、サイドナビゲーションウィンドウから [管理センター] をクリックし、[アクセスコントロール] を選択します。

   または

   WebFOCUS ホームページで [設定] をクリックし、[WebFOCUS Server] を選択します。

   または

   プラス (+) メニューを開き、[データの準備と管理] を選択します。

   または

   ブラウザのアドレスバーに次の URL を入力します。

   ```
   http(s)://host:port/context/admin
   ```

   説明

   `host`
   WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

   `port`
   WebFOCUS Reporting Server または Application Server が受信待機するポートの番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

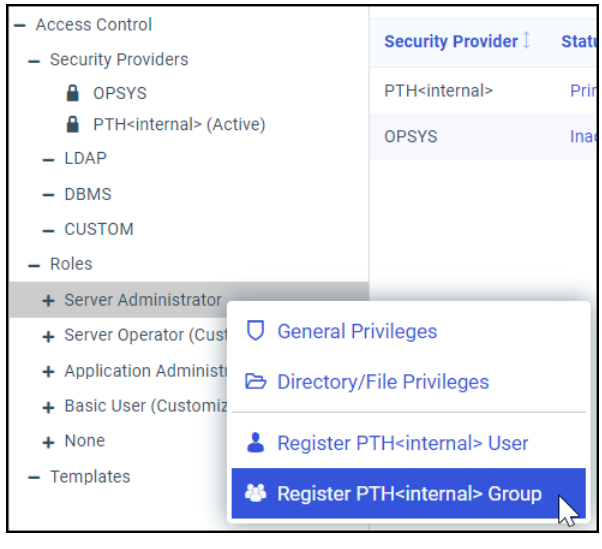
`context`

WebFOCUS で使用される特定のコンテキストです。たとえば、「ibi_apps」と入力します。

注意：ログインする際に、マシンの ID、ポート番号、コンテキストがアドレスバーにすでに表示されている場合は、コンテキストの後のパスの一部を「/admin」で上書きするだけです。

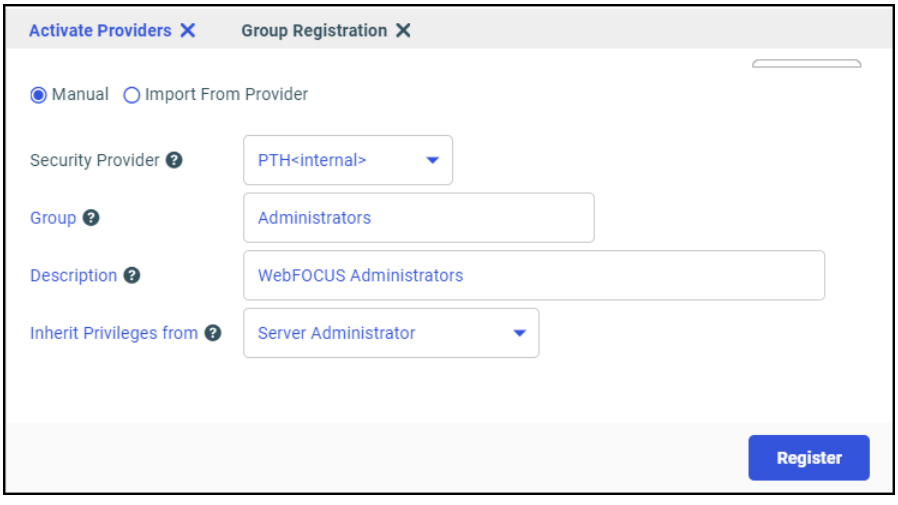
手順　WebFOCUS Administrators および Managers グループを作成してサーバ管理者ロールに登録するには

1. Reporting Server ブラウザインターフェースを開き、[設定]、[アクセスコントロール] を順に選択します。
2. 下図のように、[アクセスコントロール] ツリーの [ロール] フォルダ下で [サーバ管理者] ロールを右クリックし、[PTH <内部> グループの登録] を選択します。



3. [グループの登録] タブで、[手動] をクリックします。

4. [グループの登録] タブがリフレッシュされます。下図のように、[グループ] テキストボックスに「Administrators」と入力し、[説明] テキストボックスに「WebFOCUS Administrators」と入力した上で、[登録] をクリックします。

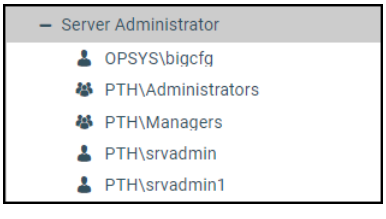


5. 確認メッセージのダイアログボックスで [OK] をクリックします。

   Reporting Server ブラウザインターフェースの画面がリフレッシュされます。

6. 手順 2 から 5 を繰り返して 2 つ目のグループを作成し、[サーバ管理者] ロールに登録します。この手順では、[グループ] テキストボックスに「Managers」と入力し、[説明] テキストボックスに「WebFOCUS Managers」と入力します。

7. [ロール] フォルダ下で 2 つ目のグループを作成、登録した後、下図のように [サーバ管理者] ロールを展開し、新しい 2 つのグループが表示されることを確認します。



   これら 2 つのグループが登録されたことで、WebFOCUS Administrators グループおよび Managers グループに属するユーザすべてが、サーバ管理者として WebFOCUS Reporting Server および Reporting Server ブラウザインターフェースへのアクセスにシングルサインオンを使用できるようになります。

注意：製品をインストールすると、OPSYS¥IBI¥username および PTH ¥srvadmin ユーザが自動的に追加され、これらのユーザが [サーバ管理者] ロール下に表示されます。

手順　Modelapp アプリケーションを作成して登録するには

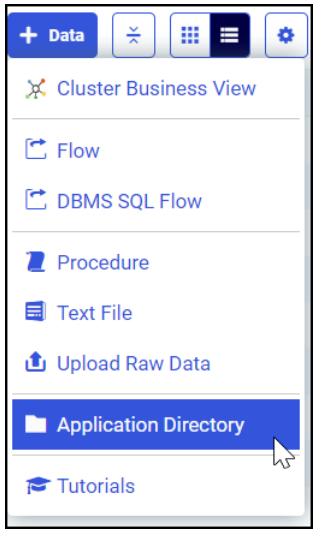
modelapp アプリケーションは、WebFOCUS Reporting Server 上のワークスペースに割り当てられたすべてのアプリケーションおよびアプリケーションディレクトリのプレースホルダです。

1. WebFOCUS Hub の左側のナビゲーションウィンドウで [アプリケーションディレクトリ] を選択し、アプリケーションディレクトリエリアを開きます。

   または

   Reporting Server ブラウザインターフェースを開きます。デフォルト設定では、アプリケーションエリアが表示されます。

2. 下図のように、[+データ] ボタン ([新規データ]) をクリックし、[アプリケーションディレクトリ] を選択します。

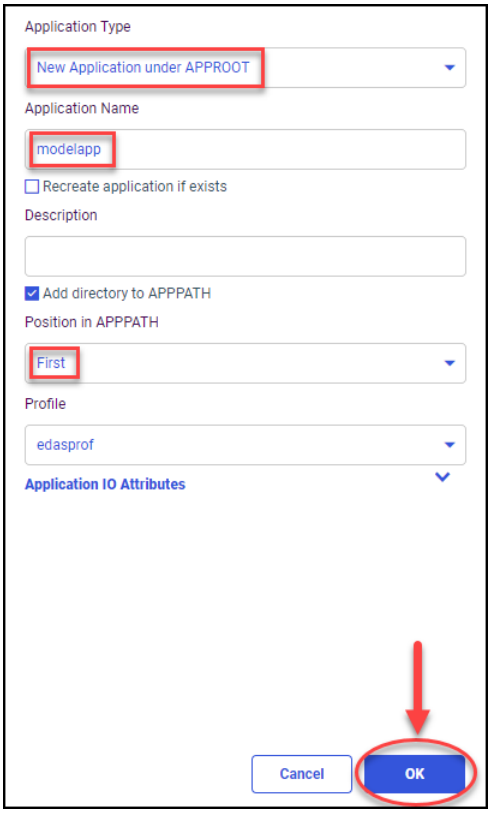


3. [新規アプリケーションの作成] タブで、次の手順を実行します。

   a. [アプリケーションタイプ] リストから [APPROOT 下の新規アプリケーション] が選択されていることを確認します。

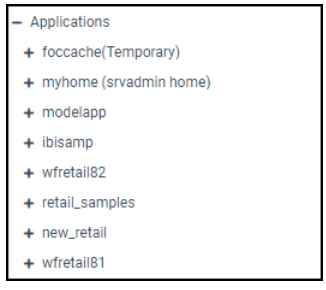
   b. [アプリケーション名] テキストボックスに「modelapp」と入力します。

c. 下図のように、[APPPATH 内の位置] リストから [最初] を選択し、[OK] をクリックします。



Reporting Server ブラウザインターフェースがリフレッシュされ、[ステータス] ページが表示されます。

下図のように、[アプリケーションディレクトリ] フォルダ下に新規アプリケーションのフォルダが表示されます。



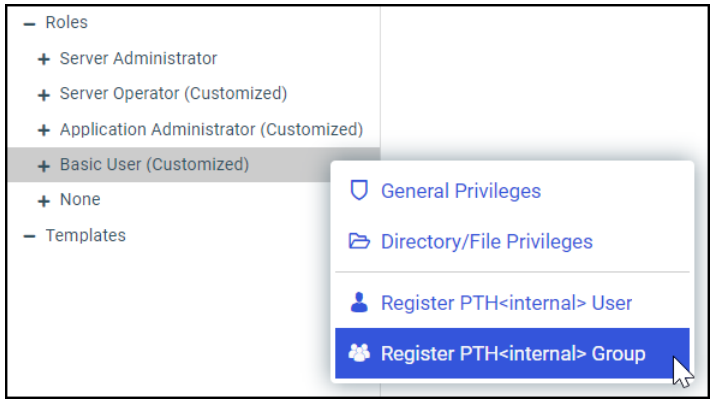
手順　新しい ModelGrp グループを登録するには

1. 次の手順のいずれかを実行し、[アクセスコントロール] ビューを表示します。

   WebFOCUS Hub の左側のナビゲーションウィンドウで [管理センター] をクリックし、[アクセスコントロール] を選択します。

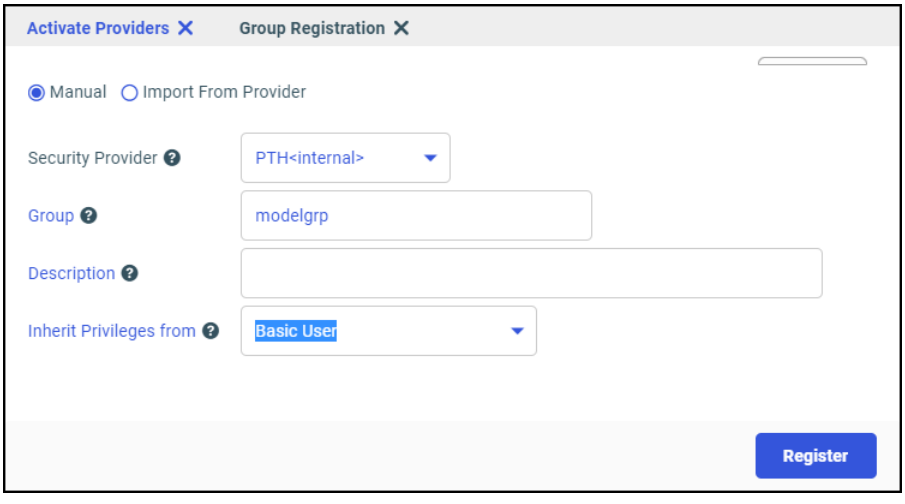
   Reporting Server ブラウザインターフェースに移動し、[ツール]、[アクセスコントロール] を順に選択します。

2. 下図のように、[アクセスコントロール] ツリーの [ロール] フォルダ下で [一般ユーザ] ロールを右クリックし、[PTH <内部> グループの登録] を選択します。

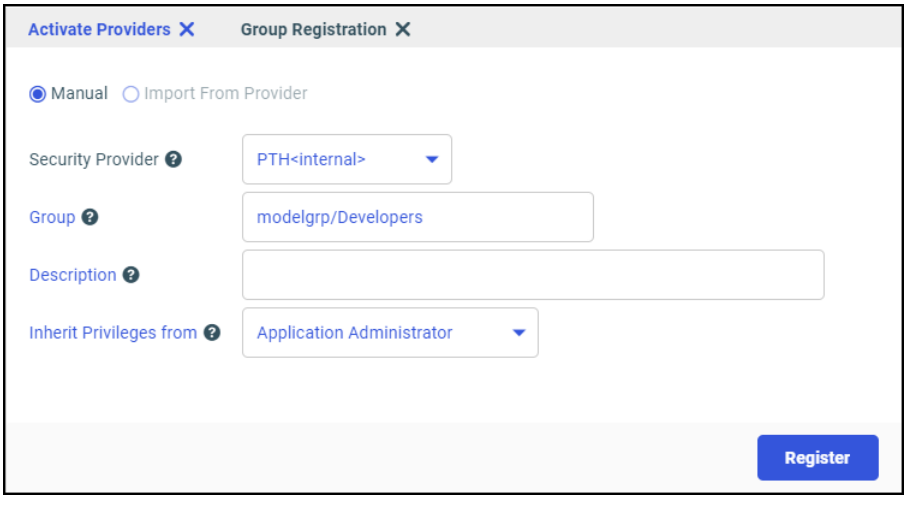


3. [グループの登録] タブで、[手動] をクリックします。

4. タブがリフレッシュされます。下図のように、[グループ] テキストボックスに「modelgrp」と入力し、[登録] をクリックします。



5. 新しいグループの登録を確認するメッセージで、[OK] をクリックします。
6. [アクセスコントロール] ツリーの [ロール] フォルダ下で [アプリケーション管理者] ロールを右クリックし、[グループの登録] を選択します。
7. [グループの登録] ページで、[手動] をクリックします。
8. ページがリフレッシュされた後、下図のように、[グループ] テキストボックスに「modelgrp/Developers」と入力し、[登録] をクリックします。

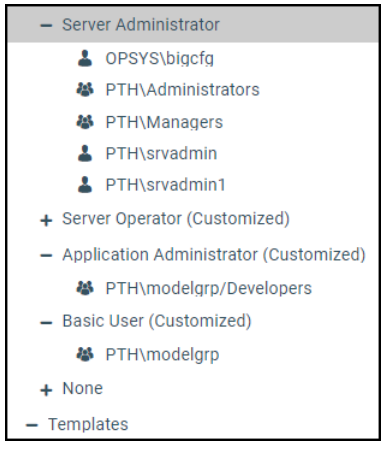


9. 新しいグループの登録を確認するメッセージで、[OK] をクリックします。

   Reporting Server ブラウザインターフェースにアクティブプロバイダのリストが表示されます。

10. [アクセスコントロール] ツリーの [ロール] フォルダ下で、[アプリケーション管理者] および [一般ユーザ] ロールを展開します。

    [サーバ管理者] ロール下に Administrators および Managers グループのアイコンが表示されます。[アプリケーション管理者] ロール下に modelgrp/Developers グループのアイコンが表示され、[一般ユーザ] ロール下に modelgrp グループのアイコンが表示されます (下図参照)。



重要：続行する前に、登録したユーザ名およびグループ名の綴りおよび大文字小文字の区別が正しいことを確認してください。WebFOCUS Reporting Server では、グループ名の大文字と小文字は区別されます。そのため、「modelgrp/Developers」の綴りおよび大文字小文字は、大文字の「D」を含めて上記に例示されたとおりに入力する必要があります。

手順　グループ権限の割り当てを構成するには

1. 次の手順のいずれかを実行し、[アプリケーションディレクトリ] ページに移動します。

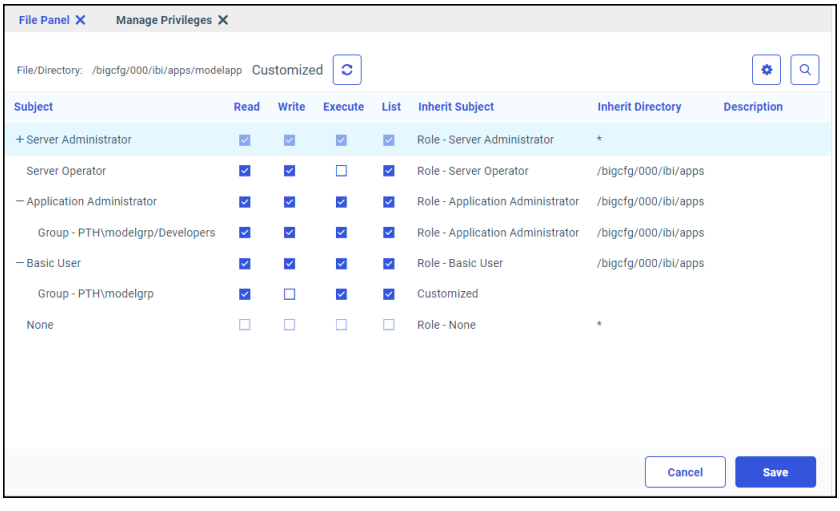
   WebFOCUS Hub の左側のナビゲーションウィンドウで、[アプリケーションディレクトリ] を選択します。

   または

   Reporting Server ブラウザインターフェースに移動します。デフォルト設定では、[アプリケーション] ページが開きます。

2. [modelapp] を右クリックし、[権限] を選択します。
3. [権限の管理] ページの [サブジェクト] 列のリストで、次のことを確認します。
   a. [アプリケーション管理者] 下の [グループ - modelgrp/Developers] エントリで、[読み取り]、[書き込み]、[実行]、[リスト] のチェックがオンになっていることを確認します。
   b. [一般ユーザ] 下の [グループ - modelgrp] エントリで、[読み取り]、[実行]、[リスト] のチェックがオンになっていることを確認します。デフォルト設定で [書き込み] のチェックがオフになっていない場合は、このチェックをオフにします。

下図のように、上記の 2 つのエントリ行で、チェックマークが 7 つ選択されていることを確認します。

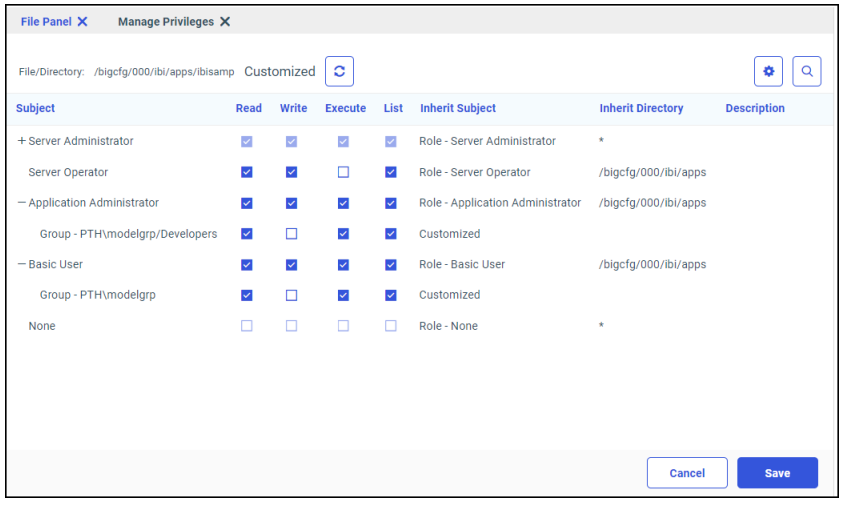


この構成は、411 ページの「 Reporting Server アクセスコントロールテンプレートのビジネス要件の定義 」 に記載されているビジネス要件に適合します。Developers グループのユーザは、ユーザ自身のアプリケーションへの [読み取り]、[書き込み] アクセス権限を所有しますが、BasicUsers および AdvancedUsers グループのユーザは [読み取り] アクセス権限のみを所有します。

注意：上記の構成に適合するようチェックボックスのいずれかをオンまたはオフにする必要があった場合は、[保存] をクリックして変更を保存します。

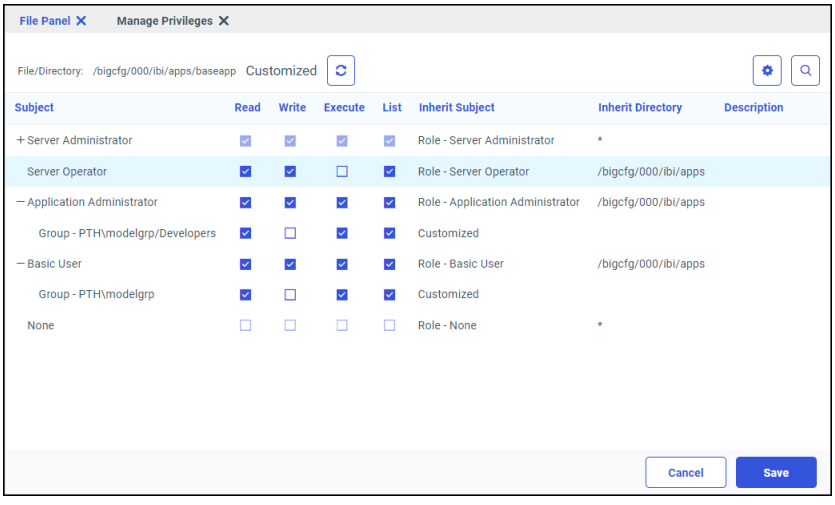
手順　ibisamp および baseapp アプリケーションに割り当てられたアクセス権限を確認するには

1. Reporting Server ブラウザインターフェースの [アプリケーション] タブで、[アプリケーションディレクトリ] フォルダ下の [ibisamp] フォルダを右クリックし、[権限] を選択します。
2. [権限の管理] ページの [サブジェクト] 列のリストで、次のことを確認します。
   a. [アプリケーション管理者] 下の [グループ - modelgrp/Developers] エントリで、[読み取り]、[実行]、[リスト] のチェックがオンになっていることを確認します。[書き込み] のチェックがオフになっていることを確認します。
   b. [一般ユーザ] 下の [グループ - modelgrp] エントリで、[読み取り]、[実行]、[リスト] のチェックがオンになっていることを確認します。下図のように、[書き込み] のチェックがオフになっていることを確認します。



3. アプリケーション] タブで、[アプリケーションディレクトリ] フォルダ下の [baseapp] フォルダを右クリックし、[権限] を選択します。
4. [権限の管理] ページの [サブジェクト] 列のリストで、次のことを確認します。
   a. [アプリケーション管理者] 下の [グループ - modelgrp/Developers] エントリで、[読み取り]、[実行]、[リスト] のチェックがオンになっていることを確認します。[書き込み] のチェックがオフになっていることを確認します。

b. [一般ユーザ] 下の [グループ - modelgrp] エントリで、[読み取り]、[実行]、[リスト] のチェックがオンになっていることを確認します。下図のように、[書き込み] のチェックがオフになっていることを確認します。



注意：これらの設定を要件に適合するよう更新するには、modelgrp/Developers および modelgrp ロールに割り当てる [読み取り]、[書き込み]、[実行]、[リスト] 権限のチェックをオフにすることもできます。

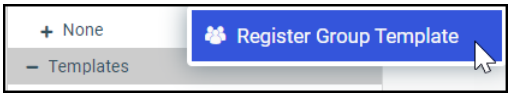
Reporting Server アクセスコントロールテンプレートの作成と登録

アクセスコントロールテンプレートを使用すると、modelapp アプリケーションで定義されたアクセスコントロールポリシーが、すべての接続に対して動的に適用されます。

Reporting Server アクセスコントロールテンプレートを作成するには、テンプレートを動的に適用するグループの範囲を指定します。

手順　modelgrp/developers アクセスコントロールテンプレートを作成して登録するには

1. Reporting Server ブラウザインターフェースを開き、[ツール]、[アクセスコントロール] を順に選択します。
2. 下図のように、[テンプレート] フォルダを右クリックし、[グループテンプレートの登録] を選択します。



3. [グループテンプレートの登録] ページで、[テンプレートグループ ID] テキストボックスに、「*(.+)/Developers*」と入力します。

   この値は、このテンプレートに関連付けられるパターン一致ロジックを定義するとともに、ツリーに表示されるテンプレート名として使用されます。このテンプレートの例では、「<Group>/Developers」という規則に準拠する名前のグループによるサーバ接続が定義されます。

   この値により、このアクセスコントロールテンプレートを有効にした後、作成されるワークスペースグループの Developers サブグループに自動的に割り当てられる権限が特定されます。

4. [モデルグループ] リストから [modelgrp/Developers] を選択します。

   このテンプレートに一致した接続には、このグループのアクセス権限が割り当てられます。

5. [除外するグループ ID] テキストボックスはブランクにします。

6. [置換パターン] テキストボックスに「(modelapp)」と入力します。

   この値により、modelapp グループに割り当てられているアクセス権限が、modelapp パターンに名前が一致する [Basic Users] グループすべてに割り当てられます。

   注意：WebFOCUS Reporting Server が Windows 上で実行されている場合、ディレクトリの区切り文字は円記号 (¥) です。そのため、円記号 (¥) は、別の円記号 (¥) でエスケープする必要があります。たとえば、「(¥¥)」と入力します。

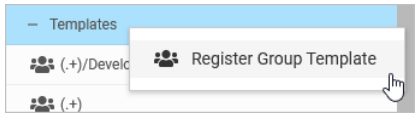
7. 入力した設定が正しいことを確認します。

8. [登録] をクリックします。

   [グループテンプレートの登録] ページがリフレッシュされ、そのテンプレートのエントリが [アクセスコントロール] ページの [テンプレート] ノード下に表示されます。

手順　modelgrp アクセスコントロールテンプレートを作成して登録するには

1. 下図のように、[アクセスコントロール] タブで [テンプレート] ノードを右クリックし、[グループテンプレートの登録] を選択します。



2. [テンプレートグループ ID] テキストボックスに「(.+)」と入力します。

この値により、このアクセスコントロールテンプレートを有効にした後、作成されるワークスペースグループの [Basic Users] および [Advanced Users] サブグループに自動的に割り当てられる権限が特定されます。

3. [モデルグループ] リストから [modelgrp] を選択します。

   このテンプレートに一致した接続には、このグループのアクセス権限が割り当てられます。

4. [除外するグループ ID] テキストボックスに「(/)」と入力します。

   この値により、anygroup/GroupName 形式を使用する名前のグループが (.+) テンプレートに割り当てられなくなります。

5. [置換パターン] テキストボックスに「(modelapp)」と入力します。

   この値は、動的に割り当てられるアクセス権限が、(modelapp) から既存の信頼されるグループ名に置き換えられることを示します。たとえば、sales¥advancedusers グループに属するユーザの場合、(modelapp) は「sales」に置き換えられます。

6. 入力した設定が正しいことを確認します。

7. [登録] をクリックします。

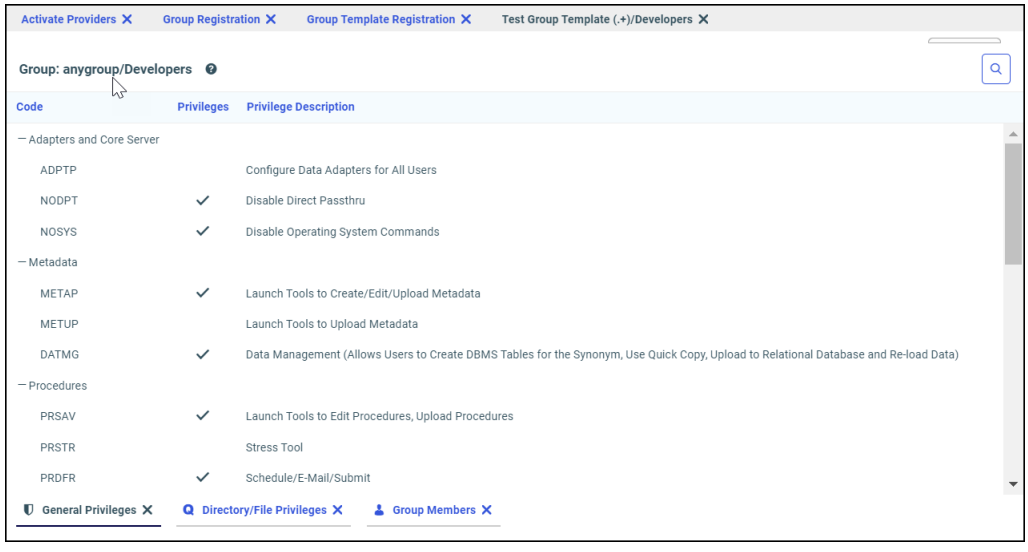
   両方のテンプレートのエントリが [アクセスコントロール] ページの [テンプレート] ノード下に表示されます。

手順　modelgrp および modelgrp/Developers アクセスコントロールテンプレートをテストするには

1. Reporting Server ブラウザインターフェースの [アクセスコントロール] タブの [テンプレート] フォルダ下で、[(.+)/Developers] テンプレートを右クリックし、[テスト] を選択します。

2. [グループ ID] テキストボックスに「anygroup/Developers」と入力し、[次へ] をクリックします。

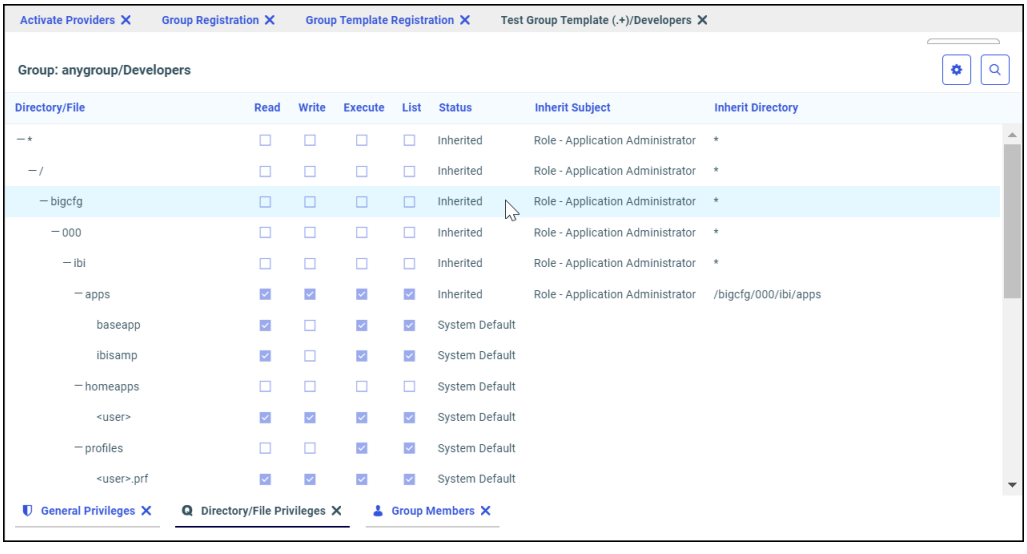
下図のように、テスト結果ウィンドウの [全般権限] ページが開き、[グループ ID] テキストボックスに入力されたグループの名前が表示されます。



この全般権限リストは、「anygroup/Developers」というパターンに名前が適合するグループのユーザすべてが、期待どおりに [modelgrp/Developers] サーバロールに関連付けられることを示しています。

3. [ディレクトリ/ファイル権限] タブをクリックします。

[ディレクトリ/ファイル権限] リストは、[anygroup/Developers] グループのメンバーに期待どおりのアクセス権限が定義されることを示しています。具体的には、anygroup アプリケーションフォルダに割り当てられている権限が、このユーザが属するワークスペースグループすべてに割り当てられることを意味します。



この時点では anygroup アプリケーションは存在しませんが、このアクセスコントロールテンプレートにより、この特定のテンプレートに一致する入力リクエストすべてに適用される権限とロールの割り当てが定義されます。

手順　WebFOCUS Reporting Server を再起動するには

アクセスコントロールテンプレートを追加または更新した後、WebFOCUS Reporting Server を再起動する必要があります。これにより、新しいテンプレートまたは更新されたテンプレートがその後の接続で使用可能になります。

1. Reporting Server ブラウザインターフェースで [ワークスペース] タブを開きます
2. [サーバアクション] アイコンの [再起動] をクリックします。
3. 確認メッセージのダイアログボックスで [OK] をクリックします。

   Reporting Server ブラウザインターフェースに、ワークスペースが再起動中であることを示すメッセージが表示されます。
4. Reporting Server ブラウザインターフェースがリフレッシュされ、[アプリケーション] タブに戻った後、Reporting Server ブラウザインターフェースを閉じます。

必要に応じて、Reporting Server ブラウザインターフェースでの構成作業を続行し、利用可能なリソースの範囲を制限します。構成の完了後、443 ページの 「 リソーステンプレートとアクセスコントロールテンプレートの統合ソリューションのテスト 」 の説明に従って、統合ソリューション全体をテストすることができます。

リソーステンプレートとアクセスコントロールテンプレートの統合ソリューションのテスト

リソーステンプレートとアクセスコントロールテンプレートの統合ソリューションをテストして、新しいワークスペースおよびグループに当初設計どおりのアクセスレベルが適用されていることを確認することができます。新しいワークスペースおよびユーザを作成し、これらをワークスペースグループに割り当てることで、ユーザに提供される機能の範囲をテストすることができます。その結果、新しいユーザおよびグループに割り当てられた権限が、期待される機能範囲に一致すること、および各グループのユーザの要件と役割に適合することが確認されます。

統合ソリューションをテストするには、次の手順を実行します。

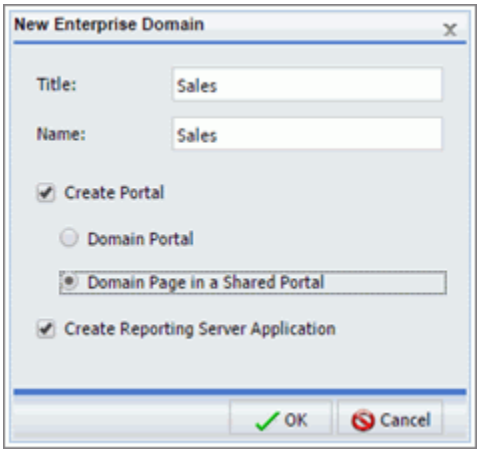
- ❑ [Administrator] グループのメンバーとしてログインし、[ワークスペースポータル] および [Reporting Server アプリケーションの作成] オプションを選択して 2 つのワークスペースを作成します。
- ❑ 各ワークスペースでユーザを作成し、そのユーザをそれぞれのワークスペースの [Advanced Users] グループに割り当てます。
- ❑ 各ワークスペースで 2 つ目のユーザを作成し、そのユーザをそれぞれのワークスペースの [Developers] グループに割り当てます。
- ❑ [Advanced Users] グループのユーザとしてログインし、割り当てられたワークスペースのコンテンツ、および [Advanced Users] グループのすべてのユーザにアクセス権限が付与された他のワークスペースのコンテンツを表示、実行できることを確認します。
- ❑ [Developers] グループのユーザとしてログインし、割り当てられたワークスペースのコンテンツ、および [Developers] グループのすべてのユーザにアクセス権限が付与された他のワークスペースのコンテンツを表示、実行、作成できることを確認します。

手順　アクセスコントロールテンプレートとリソーステンプレートの統合ソリューションテスト用のワークスペースを作成するには

この機能は、レガシーホームページからのみ使用できます。

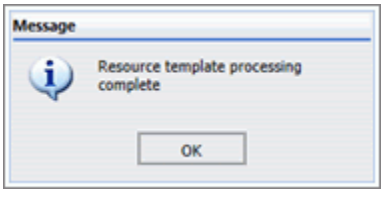
1. 管理者としてログインします。
2. レガシーホームページを開きます。

3. リソースツリーで [ワークスペース] ノードを右クリックし、[新規作成]、[エンタープライズワークスペース] を順に選択します。
4. [新規エンタープライズワークスペース] ダイアログボックスで、[ポータルの作成] のチェックをオンにして [共有ポータルのドメインページ] を選択し、[Reporting Server アプリケーションの作成] のチェックをオンにします。
5. [タイトル] テキストボックスに「Sales」と入力します。下図のように、[名前] テキストボックスにも同一の値が自動的に割り当てられます。

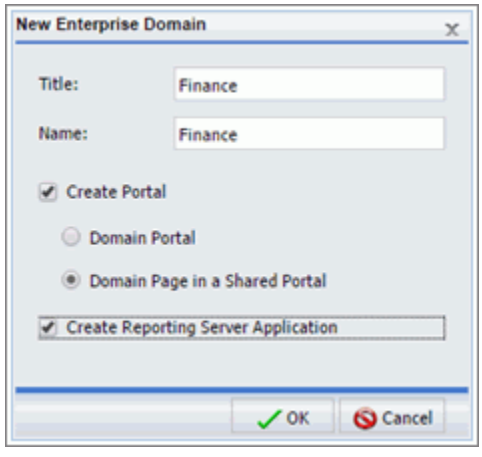


この例のリソーステンプレートは、WebFOCUS Client で定義された「EDASERVE」というノードからテナントアプリケーションを作成するよう構成されています。このノードは、作成したアクセスコントロールテンプレートが存在する WebFOCUS Reporting Server を参照するよう構成しておく必要があります。また、このテストの実行時に、参照先の WebFOCUS Reporting Server が実行されている必要があります。

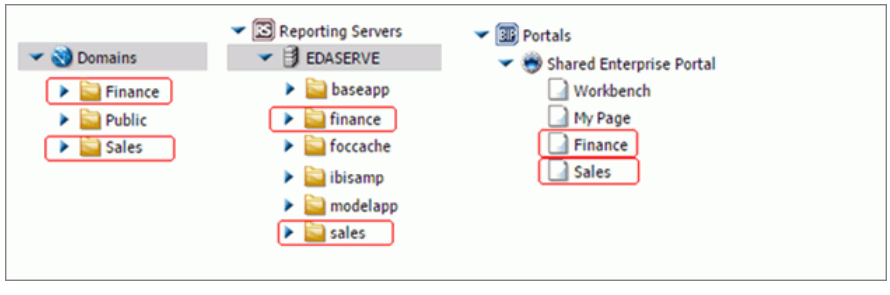
6. [OK] をクリックします。
7. 下図のように、リソーステンプレート処理が完了したことを示すメッセージで、[OK] をクリックします。



8. 手順 2 から 6 を繰り返して、別のワークスペースを作成します。この 2 つ目のワークスペースでは、下図のように [タイトル] テキストボックスに「Finance」と入力します。



9. 下図のように、リソースツリーの [ワークスペース] ノード、[Reporting Server] ノード、[ポータル] ノード下に、[Finance] および [Sales] ワークスペースの各フォルダが表示されていることを確認します。



手順　アクセスコントロールテンプレートとリソーステンプレートの統合ソリューションテスト用のユーザを作成するには

1. [セキュリティセンター] を開きます。
2. [ユーザ] ウィンドウで、[新規ユーザ] をクリックします。
3. [ユーザ ID] テキストボックスに「fdev」と入力します。
4. [作成先グループ] リストから [Finance/Developers] を選択します。
5. [OK] をクリックします。

6. 手順 2 から 5 を繰り返して、別のユーザを作成します。この 2 つ目のユーザでは、[ユーザ名] テキストボックスに「sdev」と入力し、[作成先グループ] リストから [Sales/Developers] を選択します。
7. 完了後、セキュリティセンターを終了し、ログアウトします。

手順　テストワークスペースにメタデータを追加するには

ここでは、ibisamp アプリケーションフォルダから car.foc ファイルをコピーし、新しいワークスペースのアプリケーションディレクトリに貼り付ける方法について説明します。ただし、car.foc ファイルの代わりに任意のメタデータファイルを使用してこのテストを実行することもできます。

この機能は、レガシーホームページからのみ使用できます。

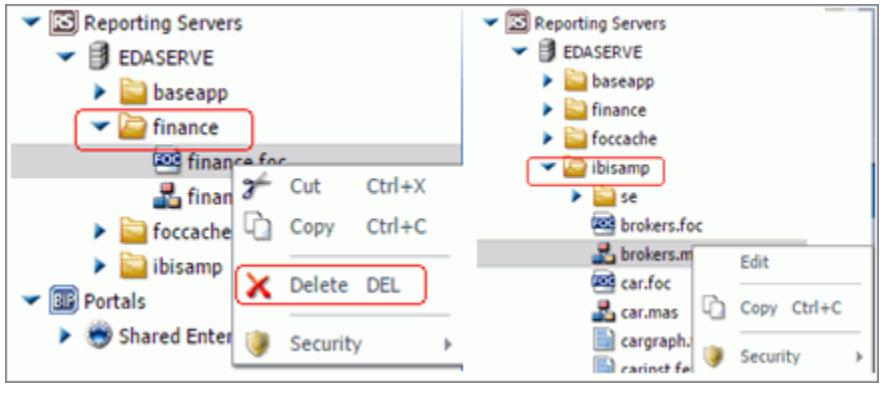
1. レガシーホームページを開きます。
2. リソースツリーで、[Reporting Server] ノード、[EDASERVE] ノードを順に展開します。
3. [ibisamp] フォルダを展開し、[car.foc] を右クリックして [コピー] を選択します。
4. [EDASERVE] ノード下で [finance] フォルダを右クリックし、[貼り付け] を選択します。
5. car.foc ファイルの名前を「finance.foc」に変更します。
6. [ibisamp] フォルダ下で [Legacy Metadata Sample: car.mas] を右クリックし、[コピー] を選択します。
7. [finance] フォルダを右クリックし、[貼り付け] を選択します。
8. 手順 2 から 6 を繰り返します。今回の操作では、[car.foc] および [Legacy Metadata Sample: Car.mas] ファイルをコピーし、これらのファイルを [EDASERVE] ノード下の [Sales] フォルダに貼り付けます。

手順　ワークスペース開発者グループメンバーの権限をテストするには

この機能は、レガシーホームページからのみ使用できます。

1. ログアウトし、ユーザ名「fdev」でログインします。
2. レガシーホームページを開きます。
3. リソースツリーで、[Reporting Server] ノードを展開します。
4. [EDASERVE] ノードを展開し、[finance] アプリケーションフォルダが表示されていることを確認します。
5. このワークスペース開発者グループに [ibisamp] および [baseapp] アプリケーションディレクトリへの [読み取り]、[実行]、[リスト] 権限を付与した場合は、[EDASERVE] ノード下にこれらの 2 つのフォルダも表示されていることを確認します。

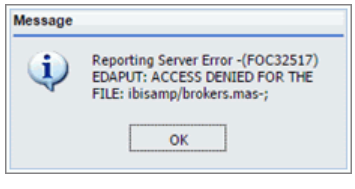
6. [finance] フォルダを右クリックし、コンテキストメニューを確認します。[削除] コマンドが表示されているかどうかを特定します。
7. [ibisamp] または [baseapp] アプリケーションフォルダを右クリックし、コンテキストメニューを確認します。下図のように、このコンテキストメニューに表示されるコマンドのリストと、[finance] フォルダのコンテキストメニューに表示されるコマンドのリストを比較します。



上図のように、fdev ユーザが [ibisamp] アプリケーションへの [書き込み] 権限を所有していないことが WebFOCUS に反映されているため、このフォルダ下でのコンテキストメニューに [削除] コマンドは表示されません。アクセスコントロールテンプレートは、そのテンプレートで定義された権限に基づいて、フォルダへのアクセス権限を動的に割り当てます。

一方、[ibisamp] フォルダ内の [Legacy Metadata Sample: brokers.mas] ファイルのコンテキストメニューには [編集] コマンドが表示されています。

8. [ibisamp] フォルダ下で [Legacy Metadata Sample: brokers.mas] ファイルを右クリックし、[編集] を選択します。
9. このファイルに変更を加え、[保存] をクリックします。
10. 下図のように、WebFOCUS Reporting Server からのメッセージが表示された場合は、[OK] をクリックします。



このメッセージは、WebFOCUS Reporting Server 上でファイルを編集するための十分なアクセス権限が fdev ユーザに付与されていないことを示しています。

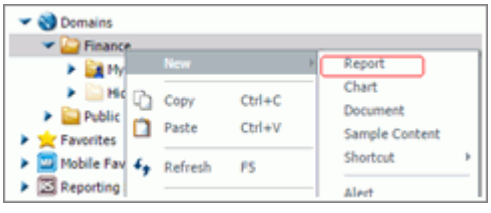
このフォルダのコンテキストメニューに [編集] コマンドが表示されるのは、リソースツリーでは [編集] コマンドが [開く] コマンドと同じ意味で使用されるためです。他のソフトウェアシステムのように、[編集] コマンドは表示と編集の両方に使用されます。

11. エディタを閉じます。
12. 変更を保存するかどうかの確認メッセージで、[いいえ] をクリックします。

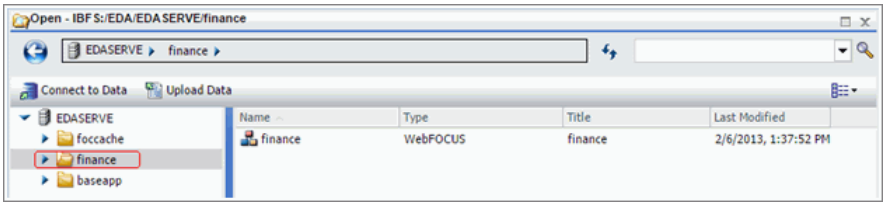
手順　ワークスペース開発者グループメンバーがアクセス可能なフォルダ範囲をテストするには

この機能は、レガシーホームページからのみ使用できます。

1. レガシーホームページを開きます。
2. 下図のように、リソースツリーの [ワークスペース] ノード下で [finance] フォルダを右クリックし、[新規作成]、[レポート] を順に選択します。



下図のように、[開く] ダイアログボックスが表示され、[finance] アプリケーションディレクトリがデフォルトアプリケーションとして選択されています。



特別なケースとして、[foccache] および [baseapp] アプリケーションディレクトリがあります。WebFOCUS に割り当てられたアクセスコントロールテンプレートで、これらのアプリケーションをユーザに表示するよう許可されている場合は、これらのアプリケーションディレクトリが常に [開く] ダイアログボックスに表示されます。Developers グループ内のこのユーザは [ibisamp] アプリケーションへのアクセス権限を所有していますが、InfoAssist には表示されません。これは、エンタープライズリソーステンプレートを使用してワークスペースが作成された際に、このアプリケーションがアプリケーションパスに含まれていないためです。

以下の finance マスターファイルの例のように、DESCRIPTION キーワードを使用してマスターファイルに説明を追加することができます。

```
FILENAME=WMDATA,DESCRIPTION='Finance Data',SUFFIX=FOC

SEGNAME=ORIGIN,SEGTYPE=S1
```

3. [キャンセル] をクリックして、 

レポートを作成せずに [開く] ダイアログボックスを閉じます。
4. InfoAssist ウィンドウを閉じます。

テスト結果の評価

上記テストのいずれかで期待どおりの結果が得られなかった場合は、アクセスコントロールテンプレート構成のトピックに戻り、問題を解決します。一方、これらのテストが期待どおりの動作結果になった場合、アクセスコントロールテンプレートとリソーステンプレートの統合ソリューションを実装する準備が整ったことを示しています。

メッセージテンプレートの使用

ユーザインターフェースの各オブジェクト (例、ディファードレポートインターフェースやそのインターフェースに表示されるメッセージ) を定義するメッセージテンプレートは、それぞれ個別の xml ファイルとして *drive*:¥ibi¥WebFOCUS¥client¥wfc¥etc¥prod ディレクトリに格納され、カスタマイズが可能になりました。

カスタムメッセージテンプレートは、標準メッセージテンプレートをベースに作成しますが、ローカルの製品環境の要件に合わせて特別なテキスト、イメージ、レイアウトを含めることができます。カスタムメッセージテンプレートを複数の言語で作成すると、各ユーザが日常作業で使用する言語に関係なく、すべてのユーザに同一のカスタム情報が提供されます。標準メッセージテンプレートの代わりにカスタムメッセージテンプレートを使用すると、ローカル WebFOCUS 環境で、ローカライズされたテキストと自社ブランドの表示が可能になります。

カスタムメッセージテンプレートの使用を有効にするには、管理者が標準テンプレートをコピーし、*drive*:¥ibi¥WebFOCUS¥client¥wfc¥etc¥custom ディレクトリに貼り付けた後、そのコピーを要件に適合するよう編集します。custom ディレクトリ内にカスタムメッセージテンプレートを作成すると、標準メッセージテンプレートの代わりにカスタムメッセージテンプレートが自動的に呼び出されます。custom ディレクトリにメッセージテンプレートが存在しない場合、prod ディレクトリ内の標準メッセージテンプレートが使用されます。

更新インストールを実行した場合でもカスタムメッセージテンプレートが保持されるため、カスタムメッセージテンプレートの作成に要した時間と労力が無駄になりません。管理者は、別のユーティリティを使用して、更新インストール後にカスタムメッセージテンプレートの内容が変更されていないことを確認することができます。

テンプレートから作成されるオブジェクト以外に、そのオブジェクトに表示されるテキストもカスタマイズすることができます。管理者は、*drive*:¥ibi¥WebFOCUS82¥webapps¥webfocus¥WEB-INF¥lib ディレクトリ内の com_ibi_intl.jar ファイルを使用して標準メッセージテキストのカスタムコピーを作成します。

また、管理者はカスタムメッセージテキストを複数の言語で作成することで、各ユーザが日常作業で使用する言語に関係なく、すべてのユーザに同一のカスタムテキストを提供することができます。

手順　カスタムメッセージテンプレートを作成するには

カスタムメッセージテンプレートは、prod ディレクトリ内の作成済みテンプレートをベースにして作成します。カスタムメッセージテンプレートを作成するには、ベースにする標準メッセージテンプレートを prod ディレクトリからコピーし、custom ディレクトリに貼り付けます。この操作には、管理コンソールや他のユーザインターフェースを使用する必要はありません。

1. WebFOCUS Client を実行しているマシンで、*drive*:¥ibi¥WebFOCUS¥client¥wfc¥etc¥prod ディレクトリを開きます。
2. カスタマイズするテンプレートを右クリックし、[コピー] を選択します。
3. *drive*:¥ibi¥WebFOCUS¥client¥wfc¥etc¥custom ディレクトリを開き、右クリックして [貼り付け] を選択します。

   注意：テンプレート名は変更しないでください。

メッセージテキストの理解

メッセージは、個別のファイルに格納されているテキストを、システムイベントまたはエラーの番号に対応するメッセージテンプレートに統合することで生成されます。たとえば、WebFOCUS Reporting Server がエラー 42 を生成すると、エラー 42 のメッセージテンプレートが呼び出され、下図のように、エラー 42 テンプレート内で識別されるテキストがメッセージテンプレートに挿入されます。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 1996-2015 Information Builders, Inc. All rights reserved. -->
<!--$Revision: 1.1 $:-->
<templates>
    <template name='error_42'>
        <![CDATA[
<HTML>
<HEAD>
<TITLE><inserttext err_42 /></TITLE>
</Head>
<Body>
<HR><H3>
<inserttext err_42_explain1 /><p>
<inserttext err_42_explain2 /><br>
<inserttext err_42_explain3 /><br>
<inserttext err_42_explain4 /><br>
<inserttext err_42_explain5 />
</H3><HR>
<PRE>
<H5>
<insertvariable html_no_output_msg />
</H5>
</PRE>
</Body>
</HTML>
        ]]>
    </template>
</templates>
```

この例では、inserttext タグ内の各リンクが、メッセージに表示するテキストが記述されたローカリゼーションファイルに接続されます。このテキストのカスタマイズが必要な場合は、技術サポートに問い合わせてください。

6

ユーザの管理

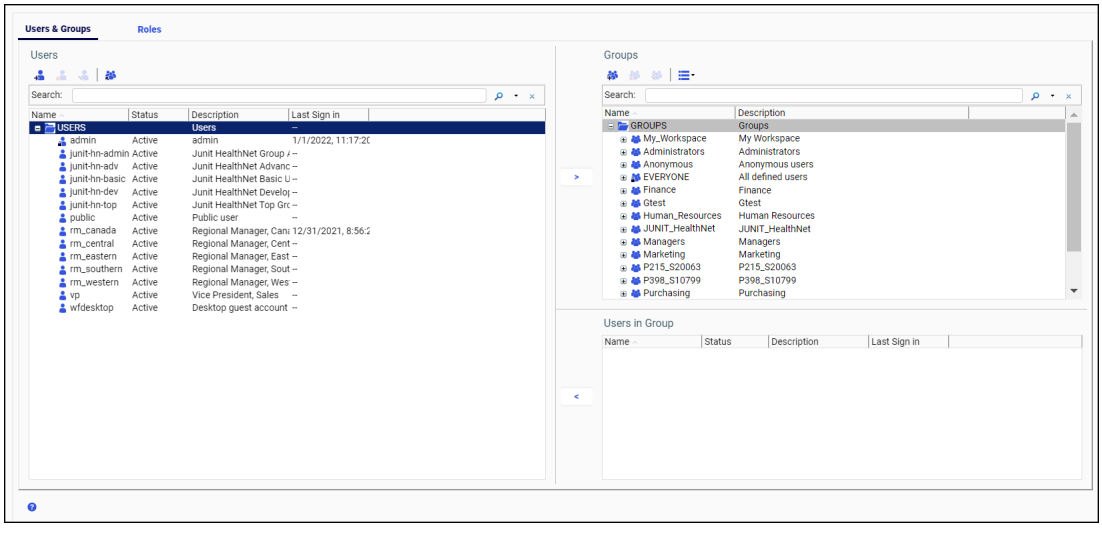
ここでは、ユーザ、グループ、ロール、ルールを管理する方法について説明します。完全な管理権限を所有するユーザは、これらの機能を実行することができますが、一部の管理権限をグループ管理者に委任することもできます。委任される機能の代表的なものは次のとおりです。

- グループおよびユーザを作成する。
- ユーザをグループに割り当てる。
- セキュリティルールを作成する。ただし、特別なグループのメンバーによるサブフォルダへのアクセスを拒否する、などの一部のセキュリティルールに限定されます。
- ユーザのプライベートコンテンツを管理する。
- スケジュールやレポートなどのリソースのオーナーシップの割り当てを変更する。

トピックス

セキュリティセンターの使用

セキュリティセンターを使用して、ユーザ、グループ、ロールを管理したり、これらの項目にルールを適用したりすることができます。WebFOCUS Hub のサイドナビゲーションウィンドウからセキュリティセンターを起動するには、[管理センター] をクリックし、[セキュリティセンター] を選択します。WebFOCUS ホームページでは、バナーから、[設定]、[セキュリティセンター] を順に選択します。下図のように、セキュリティセンターが表示されます。



ユーザの管理

セキュリティセンターの [ユーザとグループ] タブの [ユーザ] ウィンドウには、リポジトリ内のすべてのユーザが表示されます。このタブの [検索] テキストボックスを使用して、ユーザの名前および説明を検索することができます。また、単純なワイルドカード検索がサポートされます。ツールバーを使用して、次の操作を実行できます。

- ユーザを作成、編集、削除する。
- ユーザをインポートする。
- グループに適用されているアクセスルールを表示または編集する。
- ユーザが最後のログインした日時を表示する。

ユーザの理解

ユーザは、WebFOCUS へのアクセス権限を所有する利用者です。管理者およびグループ管理者は、類似した役割を担う複数のユーザを、ワークスペース内に自動的に作成されるユーザタイプグループのいずれかに割り当てることができます。この割り当てにより、ユーザが日常作業に必要な機能やコンテンツの利用が可能になる一方、ユーザの役割や権限の範囲を超える機能やコンテンツの利用が制限されます。管理者は、グループの構成および各グループで使用可能にする機能やコンテンツを、現在の環境に固有の要件に適合させることができます。ただし、通常は以下の 4 つのグループを使用し、各グループに割り当てられたユーザに次の権限を許可します。

- **Basic Users** ワークスペース内でアクセスが許可されているレポートやコンテンツを表示することができます。このユーザは、ディファードレポートをユーザ自身の [マイコンテンツ] フォルダに保存したり、作成済みレポートからパラメータをコピーしたりできます。ただし、フォルダおよびコンテンツの共有、公開、コピー、貼り付けを行うことはできません。
- **Advanced Users** Basic Users ユーザが実行可能なすべての機能を実行できる以外に、ユーザ自身の [マイコンテンツ] フォルダに新しいレポート、グラフ、他のコンテンツを作成することもできます。このユーザは、フォルダおよびそのフォルダ内のコンテンツをすべてのユーザと共有したり、選択したユーザやグループと共有したりできます。
- **Developers** Advanced Users ユーザが実行可能なすべての機能を実行できる以外に、ユーザ自身の [非表示のコンテンツ] フォルダ内のコンテンツを表示、公開することもできます。さらに、メンバー自身のワークスペースからフォルダまたはコンテンツをコピーし、別のワークスペースに貼り付けることができます。ただし、この操作のターゲットワークスペースで、コピー元コンテンツの作成時に使用されたメタデータと同一のメタデータが維持される必要があります。
- **Group Administrators** ユーザをグループに割り当てることができます。このユーザは、マネージャモードに切り替えたり、プライベートリソースを管理したりできます。

リポジトリ内の各ユーザは一意の名前で定義され、説明、Email アドレス、パスワードを割り当てることもできます。ユーザは、アカウント作成時にいずれかのグループに配置し、ステータスを割り当てる必要があります。デフォルト設定で、新規ユーザは EVERYONE グループに配置されます。これは、システム内のすべてのユーザが属するグループで、ユーザには ACTIVE ステータスが割り当てられます。

管理者は、一意のユーザ名を除いて、これらの特性を後から編集することができます。

ユーザ名に関する要件の理解

ユーザ名はリポジトリ内で定義されるため、作成するユーザ名は、リポジトリで要求されるフォーマット規則および文字制限に準拠する必要があります。インストールした WebFOCUS で外部認証 (例、Microsoft Active Directory) がサポートされている場合、ユーザ名は外部リポジトリにも存在し、その外部リポジトリで要求されるフォーマット規則に準拠する必要があります。

ユーザ名の作成に使用可能な文字セットは、Application Server で設定されている現在の文字エンコード、および NLS 設定に割り当てられた Client コードページに基づいて定義されます。たとえば、UTF-8 を使用するよう Application Server が構成され、さらに US Unicode (UTF) をサポートするよう NLS 設定が構成されている場合、ユーザ名を作成する際に 2 バイト文字セット (DBCS) の文字を使用することができます。

外部 LDAP または Active Directory 認証に依存する WebFOCUS 環境をサポートするには、WebFOCUS ユーザ名に、sAMAccountName 標準でサポートされる文字をすべて許可します。WebFOCUS のユーザ名で許可できる文字範囲は sAMAccountName 標準の範囲より広いため、管理者は、sAMAccountName 標準でサポートされていない文字を WebFOCUS ユーザ名に使用する文字として許可しないよう注意する必要があります。

ユーザ名を作成する際は、これらの要件を考慮した上で、次の規則に準拠する必要があります。

- ユーザ名には、文字、数字、ブランク、アンダースコア (_) を含めることができます。
- NLS 設定に割り当てられた Client コードページによっては、ユーザ名に 1 バイト文字または 2 バイト NLS 文字を含めることができます。

  注意：ログインの問題を回避し、sAMAccountName のベストプラクティスに準拠するには、ユーザ名に使用される文字の中で、アクセントなどの発音記号を含む文字を、発音記号が含まれない文字に置き換えます。たとえば、「Müller」を「Muller」に変換します。
- ユーザ名に「:"|;/*,?」の特殊文字を含めることはできません。

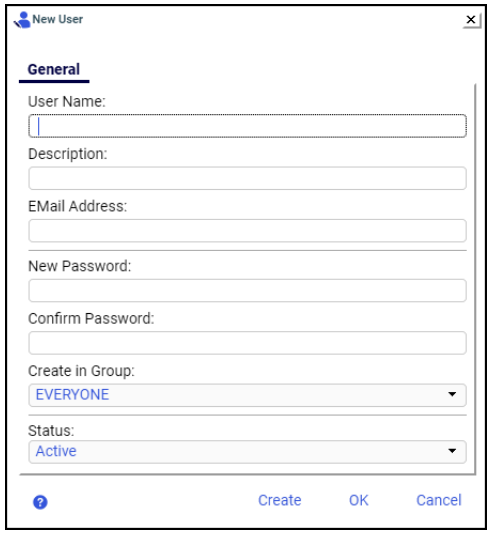
  注意：ユーザ名が sAMAccountName 標準に準拠する必要がある場合は、特殊文字の「[]:=+<>¥」もユーザ名から除外する必要があります。
- ユーザ名の最大長は、64 バイトに制限することをお勧めします。長いユーザ名を使用すると、マイグレート時に問題が発生する場合があります。
- エンドユーザ名にピリオド (.) は使用しないでください。

外部認証がサポートされている場合、外部認証リポジトリでサポートされない文字をユーザ名に使用しないようにします。サポートされない文字についての詳細は、技術サポートに問い合わせてください。

手順　ユーザを作成するには

1. [セキュリティセンター] の [ユーザとグループ] タブで、[新規ユーザ] ボタン をクリックします。

   下図のように、[新規ユーザ] ダイアログボックスが開きます。



   注意：組織内で外部セキュリティが有効化され、ユーザアカウントを開く際にパスワードの入力を必要としない WebFOCUS Reporting Server にユーザ認証が割り当てられている場合は、[新規ユーザ] ダイアログボックスに [新しいパスワード] および [パスワードの確認] テキストボックスが表示されません。

2. [ユーザ名] テキストボックスにユーザ名を入力します。また、オプションの [説明]、[Email アドレス]、[新しいパスワード]、[パスワードの確認] テキストボックスに値を入力し、必要に応じてユーザのグループおよびステータスを選択ます。
3. 入力の完了後、次の操作を実行します。
   a. [OK] をクリックしてユーザの作成を確定し、[新規ユーザ] ダイアログボックスを閉じます。
   b. [作成] をクリックしてユーザの作成を確定し、[新規ユーザ] ダイアログボックスを開いたままにします。

このボタンは、ダイアログボックスを閉じずに別のユーザを続けて作成する場合に使用します。このボタンをクリックすると、[新規ユーザ] ダイアログボックスの入力項目がクリアされ、作成したユーザのエントリがセキュリティセンターの [ユーザ] ウィンドウに表示されます。ここから上記の手順に戻り、別のユーザを作成することができます。

説明を入力しない場合、デフォルト設定で、説明にはユーザ名が使用されます。ユーザのグループおよびステータスを選択しない場合、デフォルト設定で、作成されたユーザは EVERYONE グループに配置され、ACTIVE ステータスが割り当てられます。

AD または LDAP を使用して外部認証するユーザを作成し、ユーザ情報を認証プロバイダと同期する場合は、[Email] および [説明] テキストボックスをブランクにします。

ユーザのインポート

[ユーザのインポート] コマンドを使用すると、カンマ区切り値 (.csv) テキストファイルからユーザ情報をインポートし、これらのレコードをリポジトリ内のユーザアカウントデータベースに転送することで、新しいユーザアカウントを自動的に作成することができます。この方法では、複数のユーザアカウントを作成する際に、新しいユーザアカウントごとに [新規ユーザ] ダイアログボックスを開き、詳細情報を入力して保存する必要がなくなるため、ユーザアカウントの作成が効率的になります。

このインポートで既存ユーザのレコードが上書きされることもなく、既存ユーザのレコードを削除することもできません。ユーザインポートファイル内のレコードが既存ユーザアカウントと一致する場合、下図のようにインポート時にメッセージが表示され、インポートできなかったレコードが示されます。

ユーザインポートファイルのレイアウトとフォーマット要件の理解

新しいユーザインポートファイルを作成するには、任意のテキストエディタにユーザ情報を入力し、そのファイルをカンマ区切り値 (.csv) ファイルとして保存します。外部ソースからユーザ情報をエクスポートする場合は、必要に応じてエクスポートしたユーザ情報のレイアウトとフォーマットを再編成し、そのユーザ情報を .csv ファイルに保存することで、ユーザインポートファイルを作成することができます。使用する方法に関係なく、作成するユーザインポートファイルはすべて、ここで説明するフォーマットおよびレイアウトの要件に適合するとともに、これらのユーザレコード内の情報が 460 ページの 「 ユーザレコードのフィールドフォーマット要件の理解 」 に記載されている要件に適合する必要があります。

ユーザインポートファイルに見出し行および列見出し行を含めることはできません。ファイルの先頭行には、最初のユーザレコードを含める必要があります。続いて、ユーザインポートファイルの各行に、新しい単一ユーザごとのレコードを記述します。複数のユーザレコードを同一行に記述することはできません。インポート時にブランク行が検知されると、その時点でインポートが終了するため、ユーザレコード間にブランク行を含めることはできません。

ユーザインポートファイルに英語 (米国)/西ヨーロッパ言語のコードページ 137 で使用される NLS 文字のみが含まれている場合、特別なエンコードは必要ありません。ただし、ユーザインポートファイルにその他のコードページで使用される NLS 文字が含まれている場合、バイトオーダーマーク (BOM) なしの UTF-8 エンコードを使用する必要があります。ユーザインポートファイルを UTF-8 エンコードに変更するには、他社製エディタでファイルを開き、そのファイルで UTF-8 エンコードを使用するよう設定を変更した上で、ファイルを保存します。

下図のように、各ユーザレコードには、ユーザ名、パスワード、説明、Email アドレス、ユーザステータス、グループの各フィールドが記述されている必要があります。

```
testbas,password,Getting Started Basic User,testbas@domain.com,ACTIVE,Getting_Started/BasicUsers
testadv,password,Getting Started Advanced User,testadv@domain.com,ACTIVE,Getting_Started/AdvancedUsers
testdev,password,Getting Started Developer,testdev@domain.com,ACTIVE,Getting_Started/Developers
testgrp,password,Getting Started Group Admin,testgrp@domain.com,ACTIVE,Getting_Started/GroupAdmins
testdevgrp,password,Getting Started Dev-Grp Admin,testdevgrp@domain.com,ACTIVE,Getting_Started/Developers;Getting_Started/GroupAdmins
testbas2,password,Getting Started Basic User 2,testbas@domain.com,INACTIVE,Getting_Started/BasicUsers
testbas3,password,Getting Started Basic User 3,testbas@domain.com,MUSTCHANGE,Getting_Started/BasicUsers
```

ユーザレコードの各フィールドはカンマ (,) で区切ります。フィールドに割り当てられた値にカンマ (,) が含まれている場合は、そのフィールドの値を二重引用符 (") で囲む必要があります。たとえば、次の新規ユーザレコードの 3 つ目のフィールド (説明フィールド) にはカンマ (,) が含まれているため、そのフィールド全体が二重引用符 (") で囲まれています。

testadv,password,"Getting Started, Advanced User",testadv@workspace.com,ACTIVE,Getting_Started/AdvancedUsers

ユーザレコードのフィールドに情報が含まれていない場合でも、そのレコードの正しい位置に 2 つのカンマ (,) を連続して配置することで、ブランクフィールドのプレースホルダを定義する必要があります。たとえば、次の新規ユーザレコードでは、通常はユーザエントリの 2 つ目のフィールドに配置されているパスワードが省略されています。

testbas,,Getting Started Basic User,testbas@workspace.com,ACTIVE,Getting_Started/BasicUsers

ユーザレコードのフィールドフォーマット要件の理解

ユーザレコードを作成する際に各フィールドに割り当てる値は、次の要件に準拠する必要があります。

- **ユーザ名**　インポートするユーザの名前には、[新規ユーザ] ダイアログボックスでユーザ名を直接入力する場合と同一の有効文字の制限事項が適用されます。ユーザ名の詳細およびユーザ名に使用可能な文字範囲については、456 ページの 「 ユーザ名に関する要件の理解 」 を参照してください。

  注意：ネームスペースを使用する必要のあるテナントワークスペースにユーザをインポートする場合、[グループ管理者によるユーザの作成時にネームスペースを追加] (IBI_USER_NAMESPACE) 設定に [PREFIX] または [SUFFIX] 値を割り当て済みの場合は、このフィールドにネームスペースを入力する必要はありません。ユーザのインポートプロセスで新規ユーザレコードが作成される際に、関連するネームスペースが自動的に割り当てられ、その設定で指定されたフォーマットが使用されます。この機能は、グループ管理者がテナントワークスペースにインポートするユーザのみに関係します。詳細は、150 ページの 「 詳細設定の使用 」 に記載されている [グループ管理者によるユーザの作成時にネームスペースを追加] (IBI_USER_NAMESPACE) 設定に関する説明を参照してください。

- **パスワード**　パスワードフィールドには、一般的なワンタイムパスワードを割り当てることも、UOA_USERS テーブルのハッシュ形式のパスワードのいずれかを割り当てることもできます。

- **説明**　管理コンソールの [セキュリティ] タブの [外部] ページで [ユーザ情報の同期] 設定を有効にした場合、このフィールドはブランクにします。この設定を有効にしていない場合は、このフィールドにユーザのフルネームまたは簡単な説明を入力します。[ユーザ情報の同期] 設定を有効にすると、このフィールドの値が外部認証プロバイダまたは外部認可プロバイダから提供される値で自動的に更新されます。

- **Email アドレス**　管理コンソールの [セキュリティ] タブの [外部] ページで [ユーザ情報の同期] 設定を有効にした場合、このフィールドはブランクにします。この設定を有効にしていない場合は、このフィールドに新規ユーザの Email アドレスを入力します。[ユーザ情報の同期] 設定を有効にすると、このフィールドの値が外部認証プロバイダまたは外部認可プロバイダから提供される値で自動的に更新されます。

- **ユーザステータス**　このフィールドに [アクティブ]、[非アクティブ]、[パスワードの変更が必要] のいずれかを入力して、新規ユーザアカウントの作成時にユーザに割り当てる初期ステータスを指定します。これらの値は大文字で入力する必要があります。[アクティブ] を入力した場合、そのアカウントに割り当てられたユーザは、そのアカウントが作成された時点から操作を開始することができます。[非アクティブ] を入力した場合、そのアカウントに割り当てられたユーザは、管理者がそのユーザアカウントのステータスを [アクティブ] に変更した時点からのみ操作を開始することができます。[パスワードの変更が必要] を入力した場合、そのアカウントに割り当てられたユーザは、最初のログイン時にユーザのワンタイムパスワードを変更するよう要求されます。

- **グループ**　ユーザを割り当てる 1 つまたは複数のグループの名前を入力します。グループ名フィールドに値を含めない場合、そのユーザは EVERYONE グループに自動的に割り当てられます。グループ名を含める場合、既存のグループ名の綴りと大文字小文字に完全に一致する名前を入力する必要があります。

  グループ名は、ワークスペース名、スラッシュ (/)、グループ名の順序で記述したフォーマットで入力します。たとえば、次の新規ユーザレコードの場合、レコードの最終フィールドに示すように、ユーザは Getting_Started ワークスペースの AdvancedUsers グループに追加されます。

  testadv,password,Getting Started Advanced User,testadv@workspace.com,ACTIVE,Getting_Started/AdvancedUsers

  このフィールドには複数のグループ名を含めることができます。その場合は、各グループ名をセミコロン (;) で区切ります。たとえば、次の新規ユーザレコードの場合、レコードの最終フィールドに示すように、ユーザは Getting_Started ワークスペースの Developers グループと GroupAdmin グループに追加されます。

  testdevgrp,password,Getting Started Dev-Grp Admin,testdevgrp@workspace.com,ACTIVE,Getting_Started/Developers;Getting_Started/GroupAdmins

  ユーザレコードのインポートの失敗を回避するには、ユーザレコードで指定するグループを WebFOCUS で事前に定義しておく必要があります。ユーザインポート機能を使用して、新しいグループとユーザを同時にインポートすることはできません。

  注意：グループ管理者としてテナントワークスペースにユーザをインポートする場合、そのワークスペース内のグループに新規ユーザを割り当てることはできません。エラーの発生を回避するには、このフィールドにテナントワークスペースの名前のみを含め、スラッシュ (/) とグループ名は省略します。

手順　ユーザをインポートするには

次の手順を開始する前に、ユーザインポートファイルで指定されたグループのすべてがセキュリティセンターの [グループ] ウィンドウに表示されていることを確認し、表示されていないグループまたはワークスペースは事前に作成する必要があります。

1. [セキュリティセンター] の [ユーザとグループ] タブで、[ユーザのインポート]  をクリックします。
2. [ユーザのインポート] ダイアログボックスで、[参照] をクリックします。
3. [ファイルのアップロード] ダイアログボックスで、インポートするユーザが記述された .csv ファイルを特定し、ファイルをダブルクリックするか、ファイルを選択して [開く] をクリックします。
4. [ユーザのインポート] ダイアログボックスで、インポートするユーザレコードが記述されたファイルの名前が [インポートするファイル] テキストボックスに表示されていることを確認し、[インポート] をクリックします。

   インポート処理により、ファイルのレコードで指定された各ユーザの新規ユーザアカウントが作成され、これらの新規ユーザが各レコードで指定されたグループに割り当てられます。

   a. 「ファイルの処理で問題が発生しました」というメッセージが表示された場合は、[詳細の表示/非表示] をクリックして、[警告の詳細] ダイアログボックスに示された問題を確認し、インポートユーザファイルのテキストまたはレイアウトを更新して問題を解決します。

   b. 更新したユーザインポートファイルを保存し、[警告の詳細] ダイアログボックスを閉じた後、手順 2 に戻り、インポートを再実行します。
5. インポートの完了後、[ユーザのインポート] ダイアログボックスの [OK] をクリックします。
6. [ユーザ] ウィンドウおよび [グループのユーザ] ウィンドウで、一連の新規ユーザがインポートされたこと、およびこれらのユーザがすべてのグループに正しく割り当てられたことを確認します。

手順　ユーザ情報を編集するには

1. セキュリティセンターの [ユーザとグループ] タブで、ユーザをダブルクリックするか、ユーザを右クリックして [編集] を選択するか、ユーザを選択して [ユーザの編集] ボタン をクリックします。下図のように、[ユーザの編集] ダイアログボックスが開きます。

2. 必要に応じて、[ユーザ名]、[説明]、[Email アドレス] テキストボックスに新しい情報を入力します。
3. ユーザのステータスを変更するには、[ステータス] ドロップダウンリストから [アクティブ]、[非アクティブ]、[パスワードの変更が必要] のいずれかを選択します。

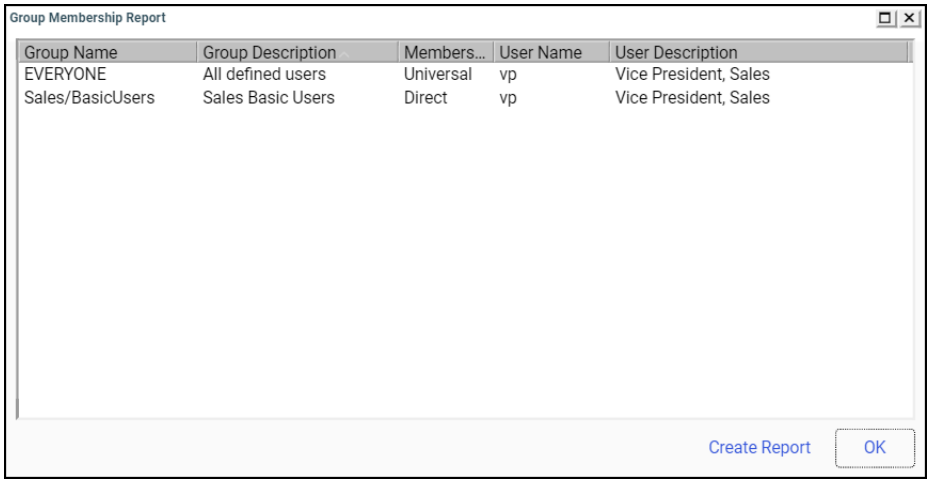
   注意：[パスワードの変更が必要] を選択した場合、ユーザがログインする際に、ユーザに対してパスワードの変更が要求されます。

手順　ユーザを削除するには

セキュリティセンターの [ユーザとグループ] タブで、ユーザを右クリックして [削除] を選択するか、ユーザを選択して [ユーザの削除] ボタン をクリックします。

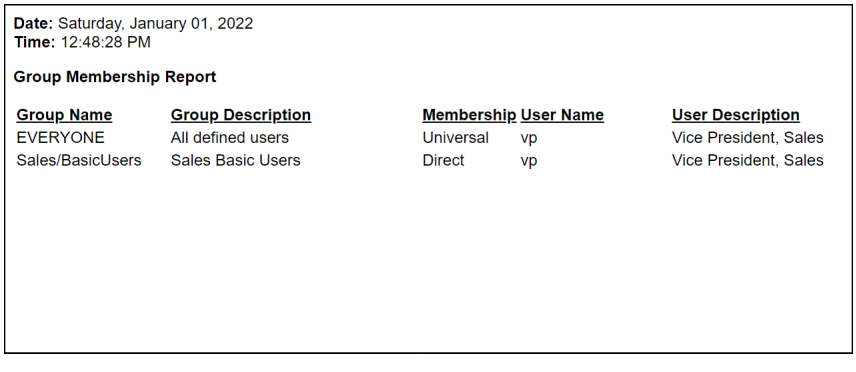
グループメンバーシップレポートの理解

グループメンバーシップレポートには、特定のユーザまたは選択した複数ユーザに現在割り当てられているグループのリストが表示されます。下図のように、各グループ割り当てのエントリリストで、グループ名、グループの説明、ユーザ名、ユーザの説明が識別されます。



デフォルト設定では、レポートのエントリリストはグループ名の昇順で表示されます。このデフォルト表示順序を変更するには、列見出しのいずれかをクリックして、その列の値を基準にレポートエントリを昇順または降順にソートします。

このダイアログボックスから、下図のような HTML 形式のレポートを作成することもできます。



ブラウザの各種コマンドを使用して、このレポートを保存したり、他のユーザに Email 送信したりできます。

HTML 形式のグループメンバーシップレポートに表示される日付時間には、WebFOCUS インストールでマシンに指定されたデフォルト設定のロケール依存の時間フォーマット (24 時間表記または 12 時間表記) が使用されます。そのため、ログイン時に別の言語を選択した場合も、日付時間は、選択した言語で必要なフォーマットではなく、マシンのデフォルト設定のロケールで使用されるフォーマットで表示されます。

たとえば、Windows オペレーティングシステムを使用するマシンにインストールされ、デフォルト言語として英語が使用されている場合、24 時間表記ではなくロケール依存の 12 時間表記 (午前/午後) の時間フォーマットが使用されます。この場合、すべての時間が 12 時間表記のフォーマットで表示されます。WebFOCUS 構成時に Unicode コードページを使用し、[言語の切り替え] 設定に日本語ロケールを追加した場合も、このレポートおよびユーザインターフェース全体で表示される時間には 12 時間表記のフォーマットが使用されます。WebFOCUS を実行するマシンの Windows 設定で [言語] に日本語を追加し、[日付と時刻] で 24 時間表記の時間フォーマットに変更しない限り、時間表示を 24 時間表記のフォーマットに変更することはできません。

手順　グループメンバーシップレポートを作成するには

グループメンバーシップレポートは、管理者と、セキュリティセンターの表示権限を所有するユーザのみが作成することができます。

1. セキュリティセンターで、次のいずれかを実行します。
   - ❏ 特定のユーザに関するレポートを作成するには、[ユーザ] ウィンドウでユーザを右クリックします。
   - ❏ 隣接する複数ユーザに関するレポートを作成するには、[ユーザ] ウィンドウで最初のユーザを選択し、Shift キーを押しながら最後のユーザを選択した後、選択した複数ユーザを右クリックします。
   - ❏ 隣接しない複数ユーザに関するレポートを作成するには、[ユーザ] ウィンドウで最初のユーザを選択し、Ctrl キーを押しながら他のユーザを順に選択した後、選択した複数ユーザを右クリックします。
2. コンテキストメニューから [グループ]、[グループメンバーシップレポート] を順に選択します。

   [グループメンバーシップレポート] ダイアログボックスが開き、選択したユーザのグループ割り当てがすべて表示されます。
3. レポートエントリの順序を変更するには、列見出しのいずれかをクリックして、その列の値に基づいてレポートエントリを昇順または降順でソートします。
4. レポートの HTML バージョンを作成するには、[レポートの作成] をクリックします。

ブラウザメニューの各種コマンドを使用して、レポートを印刷、保存、送信します。

5. このダイアログボックスを閉じるには、[OK] をクリックします。

グループの管理

セキュリティセンターの [ユーザとグループ] タブの [グループ] ウィンドウには、リポジトリ内のすべてのグループが階層順に表示されます。[グループ] ウィンドウでは、親グループの下にサブグループが表示されます。[グループのユーザ] ウィンドウには、選択したグループのすべてのメンバーが表示されます。グループが選択されていない場合、このウィンドウはブランクになります。このタブの [検索] テキストボックスを使用して、グループの名前および説明を検索することができます。単純なワイルドカード検索がサポートされます。ツールバーを使用して、次の操作を実行できます。

- グループを作成、編集、削除する。
- グループのメンバーを表示する。

グループの理解

グループは、類似した権限や、同一リソースへのアクセス許可を必要とする複数のユーザまたはサブグループの集合体です。ルールは個々のユーザロールに適用することもできますが、通常は、ユーザに許可されるアクティビティやリソースは、各ユーザが属するグループに適用されるルールに基づいています。そのため、グループの割り当ては、セキュリティポリシー実装の重要な要素になります。

すべてのユーザは、デフォルト設定で EVERYONE グループに自動的に割り当てられます。このグループには、システム内で定義されたすべてのユーザが属しています。管理者は、ユーザに必要なコンテンツリソースを含むワークスペース内の適切なグループ、また [マイワークスペース] および [開始] ワークスペース内の適切なグループにユーザを割り当てる必要があります。

デフォルト設定では、新規作成したワークスペースには、Basic Users、Advanced Users、Developers、Group Administrators の 4 つのグループが含まれます。これらの各グループには、それぞれのロールの一般的なユーザのアクティビティおよびリソースニーズをサポートする定義済みの権限範囲が設定されています。構成済みのインフラストラクチャグループ (例、マイワークスペース、開始ワークスペース) は、この基本構成とは異なります。

管理者は、独自のグループを作成することもできます。これらのグループは、各ワークスペース内の 4 つの初期設定グループを補完することができ、複数のワークスペースに割り当てられる特別なグループにすることもできます。

ユーザは複数のグループに属することができ、各グループには異なる権限セットが含まれます。さまざまなグループにユーザを割り当てる機能を使用して、管理者は、同一ユーザに異なるレベルのアクセス権限を付与することができます。

ワークスペースグループ

以下のグループは、新しいワークスペースに自動的に割り当てられます。これらは、一般的なタイプのユーザグループで、割り当てられた権限は、このようなワークスペースグループのメンバーによる実行が予想される一連のアクティビティをサポートします。

リソーステンプレートから作成されると、新しいワークスペースごとにこれらのグループが自動的に生成されます。デフォルト設定では、Basic Users、Advanced Users、Developers、Group Administrators の 4 つのグループが新しいワークスペースで使用できます。5 つ目のグループの Authors グループは、[マイワークスペース] および [開始] ワークスペースでのみ使用できます。

Basic Users

BasicUsers グループのメンバーは、所属するワークスペース内のコンテンツを表示することができます。これらのメンバーは、[マイコンテンツ] フォルダ内にフォルダを作成し、ディファードレポートを保存することができます。また、以前に作成されたレポートからオートリンクパラメータをコピーし、それらのパラメータをメンバー自身のフォルダに保存することができます。ただし、フォルダおよびコンテンツの共有、公開、コピー、貼り付けを行うことはできません。

Advanced Users

AdvancedUsers グループのメンバーは、所属するワークスペース内のコンテンツを表示することができます。これらのメンバーは、[マイコンテンツ] フォルダ内にフォルダを作成し、ディファードレポートを保存することができます。また、以前に作成されたレポートからオートリンクパラメータをコピーし、これらをメンバー自身のフォルダに保存することができます。また、独自コンテンツ項目やフォルダの作成および共有も行えます。

Authors

このグループは、[マイワークスペース] および [開始] というタイトルの構成済みワークスペースでのみ使用できます。Authors グループのメンバーは、コンテンツの表示、フォルダの作成、およびメンバー自身のフォルダへのディファードレポートの保存が行えます。また、以前に作成されたレポートからオートリンクパラメータをコピーし、これらをメンバー自身のフォルダに保存することができます。また、フォルダやコンテンツ項目の作成および共有も行えます。上記の権限のほか、これらのセルフサービス分析ユーザは、ユーザ自身の [マイワークスペース] または [開始] 表示を使用したデータへの接続、データファイルの表示、およびポータルの作成が行えます。

Developers

Developers グループのメンバーは、所属するワークスペース内のコンテンツを表示することができます。これらのメンバーは、[マイコンテンツ] フォルダ内にフォルダを作成し、ディファードレポートを保存することができます。また、以前に作成されたレポートからオートリンクパラメータをコピーし、これらをメンバー自身のフォルダに保存することができます。また、独自コンテンツ項目やフォルダの作成および共有も行えます。このグループのメンバーは、データのアップロードと接続、メタデータの編集、ワークスペースコンテンツの作成と編集が行えます。また、他のユーザが閲覧可能なコンテンツを管理することもできます。さらに、メンバー自身のワークスペースからフォルダまたはコンテンツをコピーし、別のワークスペースに貼り付けることができます。ただし、この操作のターゲットワークスペースで、コピー元コンテンツの作成時に使用されたメタデータと同一のメタデータへの接続が可能である必要があります。

Group Administrators

Group Administrators グループのメンバーは、5 つのタイプのユーザグループにユーザを追加したり、ユーザを削除したりすることで、ワークスペース内での各ユーザのロールを決定します。また、ワークスペースに割り当てられた全般アクセス権限を変更することもできます。このグループのメンバーは、レポート作成機能や開発機能にはアクセスできません。

ワークスペースで作業するユーザにとって必要な基本アクセス権限は、これら 5 つのユーザタイプにほぼすべて含まれています。そのため、管理者はこれらのユーザグループへのユーザ割り当てのみに集中することができ、ユーザごとにアクセスレベルのプロファイルを構成する必要はありません。

インフラストラクチャグループ

以下のグループは、製品のインストール時に自動的に作成されます。これらは、コンテンツ開発をサポートするために作成されたワークスペース以外で作業するユーザのロールを定義します。

My_Workspace グループ

My_Workspace グループには、[マイワークスペース] というタイトルの特別なワークスペースに割り当てられたユーザが含まれます。

マイワークスペースは、標準リソーステンプレートから作成され、すべてのテンプレートに割り当てられたルールと同一のセキュリティルールを使用します。ただし、ワークスペースには通常 4 つのグループが割り当てられるのに対し、このグループには Basic Users グループと Authors グループのみが含まれます。これら 2 つのグループに対して定義された権限は、ユーザが [マイワークスペース] の [マイコンテンツ] フォルダで作業する場合のみ適用されます。

他のワークスペースと同様に、管理者は、[マイワークスペース] 内の 2 つのグループへのユーザの割り当てを積極的に管理する必要があります。[マイワークスペース] のユーザに与えられる権限は、他のワークスペースのユーザに与えられる権限とは完全に独立したものです。

製品インストールによっては、WebFOCUS Hub および WebFOCUS ホームページから直接作成されるコンテンツ、または既存のワークスペース以外で作成されるコンテンツ用に、別のワークスペースがデフォルトワークスペースとして使用される場合があります。この場合は、管理コンソールの [BI Portal] ページの [デフォルトワークスペースリポジトリパス] (IBI_DEFAULT_WORKSPACE_PATH) 設定で別のワークスペースのパスを定義します。

この構成によって、マイワークスペースまたはこれに割り当てられたグループが削除されることはありません。[デフォルトワークスペースリポジトリパス] で別のワークスペースが指定されたとしても、マイワークスペースグループ内のサブグループに割り当てられたユーザは、マイワークスペースグループの割り当てによって許可されたように、WebFOCUS ホームページのコンテンツ表示から [マイワークスペース] を開いたり、新規コンテンツを実行したり作成したりできます。

Administrators グループ

Administrators グループのメンバーには、すべてのワークスペースおよび製品機能へのフルアクセス権限が与えられます。このグループのユーザは、デフォルト設定で、SystemFullControl ロールに割り当てられます。デフォルト設定の管理者 (ユーザ ID admin) は、このグループに割り当てられます。パスワードがインストール時に指定され、複数のユーザに知られる可能性があるこのデフォルト管理者は、独自のユニークパスワードを設定した他のユーザで補完することができます。

Anonymous グループ

Anonymous グループのメンバーは、このグループに割り当てられたルールによる制限内で、EVERYONE グループで使用可能なリソースにアクセスできます。Anonymous グループのメンバーは、デフォルト設定で BIDRunTimeAccess ロールに割り当てられます。このロールでは、コンテンツリソースに制限付きアクセスが与えられます。このグループのメンバーは、AnonymousRestrictions ロールにも割り当てられます。このロールではリソースの作成またはコピーができません。このグループのメンバーは、[マイワークスペース] およびパブリックユーザに使用可能な他のワークスペースのリソースのみ表示したり実行したりできます。

パブリックユーザは、デフォルト設定でこのグループに割り当てられます。WebFOCUS Client は、WFC/Repository/Public フォルダ内および管理者が表示と実行権限を与えたワークスペースフォルダ内のリソースにアクセスするすべての未承認リクエストに対してこのユーザ ID を自動的に割り当てます。匿名ユーザごとに個別のセッションが作成されます。

このデフォルト匿名ユーザに割り当てられたユーザ ID は、管理コンソールの [セキュリティ] タブの [詳細] ページの [匿名ユーザ ID] (IBI_ANONYMOUS_USER) 設定で定義されます。デフォルト設定では、「public」が割り当てられます。このように、ほとんどのインストールでは、デフォルト匿名ユーザはパブリックユーザとして指定されます。

EVERYONE グループ

EVERYONE グループ のメンバーには、すべてのワークスペースへの Basic User アクセス権限が与えられます。このグループのメンバーは、ワークスペース内のリソースを表示したり実行したりできますが、コンテンツを作成することも、自分以外のワークスペース内の既存コンテンツに変更を加えることもできません。デフォルト設定で、ユーザは、他のグループへの割り当てに加えて、EVERYONE グループのメンバーになります。

Managers グループ

Managers グループのメンバーには、すべてのワークスペースへのアクセスが与えられます。このグループのメンバーは、アプリケーション全体で WebFOCUSManager ロールに割り当てられます。このロールでは、WebFOCUS 操作の管理を可能にする幅広い権限が与えられます。

SelfServiceDevelopers グループ

Self Service Developers グループのメンバーには、すべてのシステム機能へのアクセスが与えられます。この特殊なユーザグループは、セルフサービスライセンスで WebFOCUS を使用するユーザにのみ適用されます。これらのユーザは、デフォルトユーザインターフェースを独自にデザイン、開発したユーザインターフェースで置換した WebFOCUS バージョンを使用します。

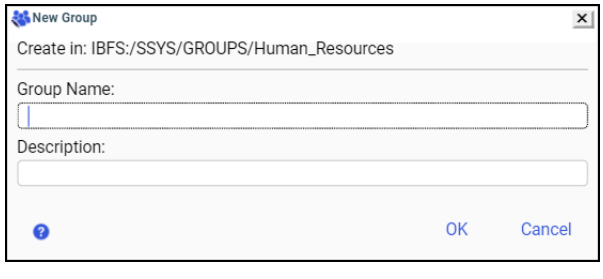
このグループには、デスクトップツールにアクセスするためのデフォルトユーザ ID「Wfdesktop」が含まれます。このグループのメンバーは、[データサーバ]、[Web アプリケーション] エリアでセルフサービス開発作業を行えます。リポジトリへのアクセス権限は、EVERYONE グループに与えられたアクセスに制限されます。

手順　グループを作成するには

1. セキュリティセンターの [ユーザとグループ] タブで、次の手順を実行します。

   - グループを作成するには、[新規グループ] ボタン  をクリックするか、階層の [GROUPS] レベルを右クリックして [新規作成] を選択します。
   - サブグループ (ネストされたグループ) を作成するには、[ユーザとグループ] タブで、サブグループを作成する親グループを選択し、[新規グループ] ボタンをクリックします。別の方法として、親グループを右クリックし、[新規作成] を選択します。

   下図のように、[新規グループ] ダイアログボックスが表示されます。



   外部グループが有効になっている場合、外部グループの名前を直接入力するか、[参照] ボタンをクリックして外部グループを選択することもできます。

[作成] に表示されるパスは、[新規グループ] ボタンのクリック時のカーソルの位置によって異なります。

2. グループ名およびオプションの説明を入力し、[OK] をクリックします。

   グループ名には文字、数字、アンダースコア (_) を含めることができますが、「* / | ; " , ?」の特殊文字およびブランクを使用することはできません。グループ名の最大長は 255 バイトです。説明には、システムで許可されている任意の文字を使用することができます。説明をブランクにした場合、説明には自動的にグループ名が使用されます。名前または説明はいつでも編集することができます。

手順　グループを編集するには

1. セキュリティセンターの [ユーザとグループ] タブで、グループを右クリックして [編集] を選択するか、グループを選択して [グループの編集] ボタン  をクリックします。

   [グループの編集] ダイアログボックスが開きます。

2. 必要に応じてグループ名または説明を編集し、[OK] をクリックします。

手順　グループを削除するには

1. セキュリティセンターの [ユーザとグループ] タブで、グループを右クリックして [削除] を選択するか、グループを選択して [グループの削除] ボタン  をクリックします。
2. 「選択した項目をすべて削除しますか?」というメッセージで、[はい] をクリックします。

手順　ユーザをグループに追加するには

1. [セキュリティセンター] を開きます。
2. [ユーザとグループ] タブで、次の操作のいずれかを実行します。
   a. グループに追加するユーザを [ユーザ] ウィンドウから [グループ] ウィンドウにドラッグし、グループまたはサブグループの [名前] にドロップします。
   b. [グループ] ウィンドウでグループまたはサブグループをクリックし、このグループに追加するユーザを [ユーザ] ウィンドウから [グループ] ウィンドウにドラッグします。
   c. [グループ] ウィンドウでグループまたはサブグループをクリックし、このグループに追加するユーザを [ユーザ] ウィンドウで選択して [選択したユーザをグループに追加] ボタン  をクリックします。

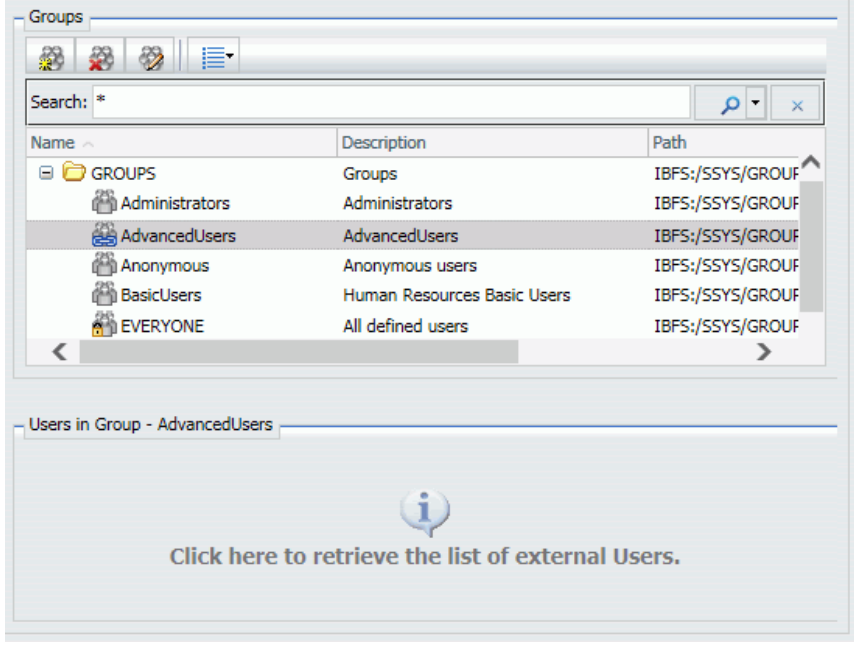
選択した操作の完了後、追加したユーザが [グループのユーザ] ウィンドウに表示されます。

注意

- [グループ] ウィンドウの任意のグループにユーザをドラッグすると、グループが自動的に展開され、このグループ内のサブグループの名前にこのユーザをドロップすることができます。
- 外部グループのマッピングが有効でない場合、任意のグループまたはサブグループをクリックすると、選択したグループのメンバーが [グループのユーザ] ウィンドウに表示されます。
- WebFOCUS グループが外部グループにマッピングされている場合、このグループにユーザを直接割り当てることはできません。

手順　グループ内の外部ユーザを表示するには

1. 下図のように、セキュリティセンターの [ユーザとグループ] タブの [グループ] ウィンドウで、マッピングされたグループを選択します。



2. [グループのユーザ] ウィンドウをクリックします。

外部ユーザのリストが表示されます。

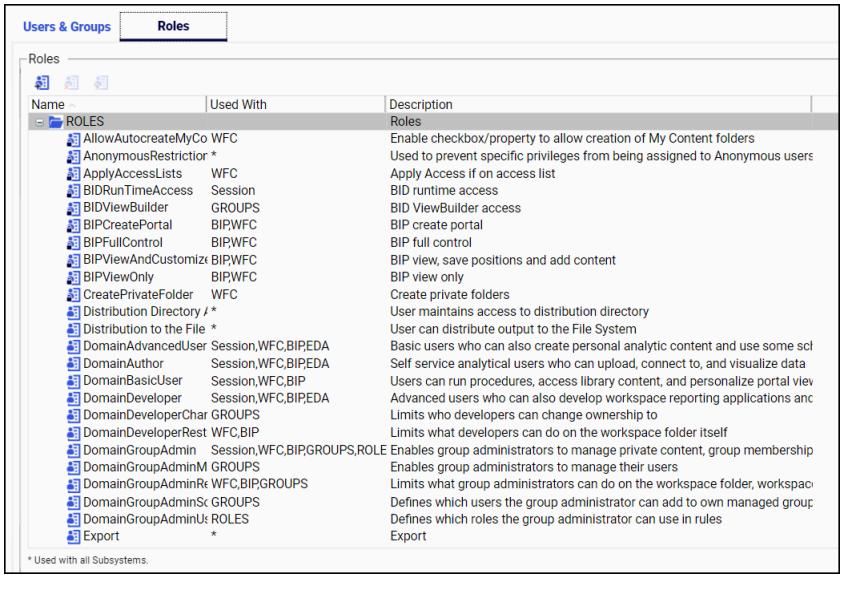
手順　ユーザをグループから削除するには

1. セキュリティセンターの [ユーザとグループ] タブの [グループ] ウィンドウで、グループを選択します。
2. [グループのユーザ] ウィンドウでユーザを選択し、[選択したユーザをグループから削除] ボタン < をクリックするか、選択したユーザを [ユーザ] ウィンドウにドラッグします。

   ユーザをグループから削除する別の方法として、ユーザを右クリックし、[削除] を選択することもできます。

ロールの管理

下図のように、[ロール] タブには、各ロールの名前、適用先サブシステム、具体的な説明が表示されます。



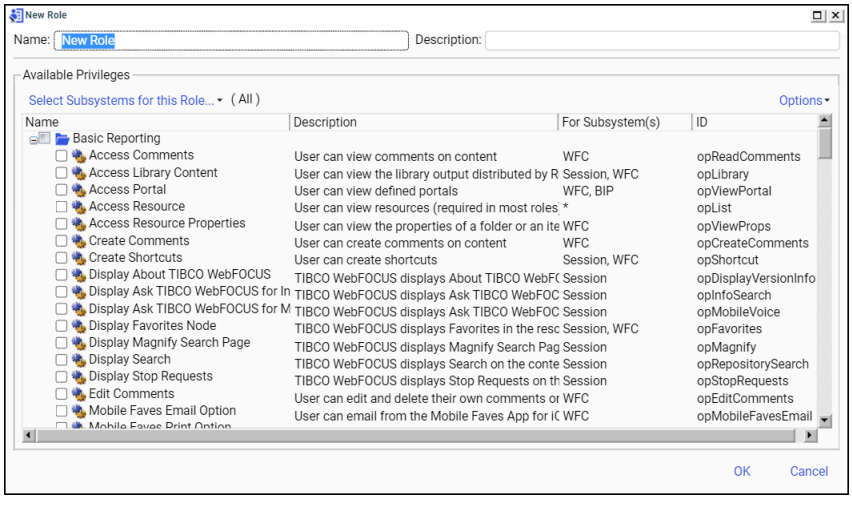
ロックアイコンが付いたロールは、そのロールが読み取り専用で、編集、削除できないことを示しています。事前にインストールされているロールはすべて読み取り専用です。カスタムリソーステンプレートをインストールする場合、ロックされたロールと事前インストール済みのロールは自動更新されません。 ただし、カスタムリソーステンプレートの構成の一部として、これらを変更することは可能です。 詳細は、405 ページの 「 カスタムリソーステンプレートへのカスタマイズの追加 」 を参照してください。

WebFOCUS Reporting Server アプリケーションへのアクセスは、事前定義済みのロックされたロールではなく、サーバのアクセスコントロールテンプレートに適合するグループに割り当てられたアクセス権限によって決まります。詳細は、410 ページの 「 アクセスコントロールテンプレートの理解 」 を参照してください。

[ロール] タブでは、次の操作を実行できます。

- ロールを作成、編集、削除、複製する。
- ロールに適用されたアクセスルールを表示、編集する。
- ユーザまたはグループのロールに適用された有効なポリシーを表示、編集する。
- 選択したロールを使用しているルールを表示する。

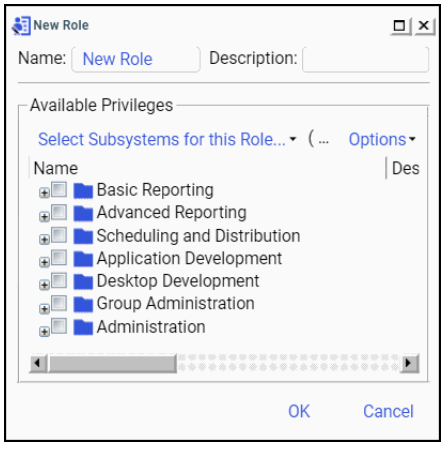
ロールを作成または表示する際に、利用可能な権限のリストが、権限の名前、説明、対象のサブシステム、権限 ID とともに表示されます。



長い説明の末尾が表示されない場合、説明の上にマウスポインタを置くと、ツールヒントに説明の全文が表示されます。権限 ID は、ツールヒントの最後に表示されます。また、スクロールバーを使用して [ID] 列まで移動することもできます。権限 ID は、一意の内部識別子です。ただし、技術サポート以外で使用されることはほとんどありません。

権限カテゴリ

新しいロールを作成する際に、ロールに権限を割り当てます。下図のように、権限はカテゴリ別に分類されているため、特定の権限を簡単に見つけられます。また、下表には、これらのカテゴリの説明が記載されています。



権限カテゴリ	説明
Basic Reporting	最小限のトレーニングを受けたユーザを含め、ほとんどのユーザに割り当て可能な権限です。他のカテゴリの権限はすべて、この Basic Reporting カテゴリの権限を補足する目的で割り当てます。
Advanced Reporting	ユーザ独自のレポートを作成、共有する必要のあるユーザに割り当て可能な権限です。一般に、これらの権限は、Basic Reporting カテゴリの権限の代わりに割り当てるのではなく、補足する目的で割り当てます。
Scheduling and Distribution	ReportCaster を使用してレポート配信のスケジュールを作成するユーザ、開発者、管理者に割り当て可能な権限です。

権限カテゴリ	説明
Application Development	開発者に割り当て可能な一連の権限です。これらの権限を所有する開発者は、Web ベースのツールのみを使用して完全な WebFOCUS アプリケーションを作成することができます。WebFOCUS アプリケーション開発のすべての機能へのアクセスを有効にするには、開発チームに Desktop Development カテゴリの権限も割り当てる必要があります。
Desktop Development	Windows ベースの WebFOCUS Desktop 製品を使用する開発者に割り当て可能な権限です。開発機能のすべてを有効にするには、これらの権限を Application Development、Advanced Reporting、Basic Reporting カテゴリの権限とともに割り当てる必要があります。
Group Administration	部門またはテナントのグループ管理者に割り当て可能な権限です。これにより、グループ管理者が、管轄するグループ内のユーザの管理や、これらのユーザが作成したコンテンツの管理を行えるようになります。
Administration	一般に WebFOCUS 管理者のみに割り当てられるシステム管理者権限です。
Legacy Privileges	WebFOCUS の以前のバージョンからバージョン 8 にマイグレートしたユーザ向けに、レガシー製品の動作を有効にする権限です。

各カテゴリ内で、権限は英語名のアルファベット順に表示されます。すべての言語で、ローカライズされた権限名は元の順序のまま表示され、表示言語に関わらず一貫した順序で権限が表示されます。一貫した場所に表示されることで、権限の検索と特定がしやすくなります。

権限は、隣接するチェックボックスを選択して個別に選択することも、カテゴリのフォルダに隣接するチェックボックスを選択して権限カテゴリ全体を選択することもできます。また、権限カテゴリ全体を選択した後、そのカテゴリ下で自動的に選択されている権限の中から、一部の権限の選択を解除することもできます。

カテゴリのタイトルエントリ横にあるチェックボックスの外観によって、カテゴリ内で選択された権限範囲が識別されます。 カテゴリ内の権限が選択されていない場合、このチェックボックスはブランクになります。 カテゴリ内で 1 つ以上の権限が選択されている場合、このチェックボックスにはブロックが表示されます。 カテゴリ内のすべての権限が選択されている場合、チェックボックスにチェックマークが表示されます。

各カテゴリの権限についての詳細は、643 ページの 「 権限 」 を参照してください。

参照 サブシステム

一部の権限は任意のサブシステムに適用することができますが、ほとんどの権限は特定の種類のサブシステムに限定されます。たとえば、[Access Portal] 権限は BIP (BI Portal) サブシステムのみに適用され、[Access Resource Properties] 権限は WFC (コンテンツ) サブシステムと EDA (WebFOCUS Reporting Server) サブシステムのみに適用されます。[Access Resource] 権限は、すべてのサブシステムに適用されます。その場合、[サブシステム] 列にアスタリスク (*) が表示されます。[サブシステム] 列の「Session」は、権限が特定のサブシステムに適用されるのではなく、ユーザセッション中に限り、その権限がキャッシュされることを示します。

ロールを作成する際に、使用可能な権限がすべて表示されます。リストに表示する権限をフィルタするには、[このロールのサブシステムを選択] リストから [すべてクリア] を選択した後、ロールの作成に使用するサブシステムのみを選択します。サブシステムを選択するたびにリストが閉じるため、複数のサブシステムを選択する場合は、リストを再度開いて別のサブシステムを選択する必要があります。

注意

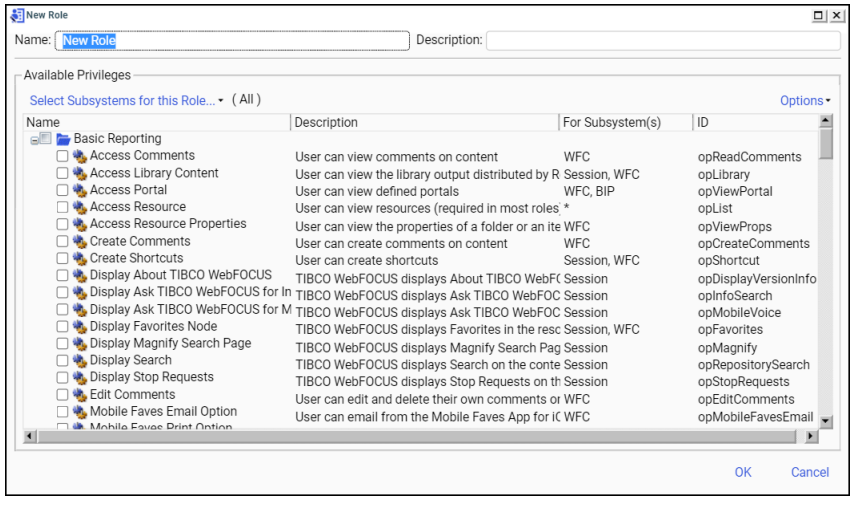
- ロールのサブシステムリストから特定のサブシステム設定をクリアすると、新しいサブシステム設定に該当しない構成済み権限がすべて除外されることを示す警告メッセージが表示されます。リストから [すべてクリア] を選択した場合、警告メッセージは表示されず、権限がすべて除外されます。[すべてクリア] を誤って選択した場合は、[キャンセル] をクリックして、変更を保存せずに [ロール] ダイアログボックスを閉じます。
- ユーザがルールを追加、削除、置換する際に、そのルールの影響を受けるリソースへのアクセス権限をユーザがその時点でも所有しているかどうかが確認されます。この確認は、そのリソースに対する [Access Resource (opList)] および [Manage Rules on Resources (opManageRulesOn)] 権限に基づいて実施されます。新しいルールによってそのリソースへのアクセスが拒否された場合、変更は保存されず、ERROR_RULE_WOULD_DROP_CONTROL エラーが返されます。

サブシステムおよびセッション権限についての詳細は、354 ページの 「 セッション権限 」 を参照してください。

手順　ロールを作成するには

1. [セキュリティセンター] で、[ロール] タブをクリックし、[新規ロール] ボタン をクリックします。

   下図のように、[新規ロール] ダイアログボックスが表示されます。



2. [名前] テキストボックスに名前を入力し、[説明] テキストボックスに説明を入力します。[説明] テキストボックスをブランクにした場合、入力した名前が使用されます。
3. この新しいロールからサブシステムを削除する場合、[このロールのサブシステムを選択] ドロップダウンリストを開き、削除するサブシステムのチェックをオフにします。デフォルト設定では、[(すべて)] が選択されています。

   注意：このロールは、フォルダリソースに対してルールを作成する際に、選択したサブシステムおよびその下位フォルダに適用されるルールでのみ使用できます。
4. このロールに権限を追加するには、次の手順のいずれかを実行します。
   a. 各権限横のチェックボックスを選択します。
   b. 権限カテゴリフォルダ横のチェックボックスを選択します。
   c. このロールから除外する個別権限または権限カテゴリのチェックをオフにします。
5. 必要に応じて、上記の手順を繰り返します。
6. [OK] をクリックします。

   新しいロールが、名前のアルファベット順に [ロール] タブのリストに表示されます。

手順　ロールの複製を作成するには

セキュリティセンターで [ロール] タブをクリックし、ロールを右クリックして [複製を作成] を選択します。

新しいロールが元のロールの下に表示され、新しいロールの末尾に「_copy」という語句が追加されます。

注意：ロールの複製を作成すると、複製されたロールから、元のロールに関連付けられていたルールが削除されます。

手順　ロールを編集するには

1. セキュリティセンターで [ロール] タブをクリックし、ロールを右クリックして [編集] を選択するか、ロールを選択して [ロールの編集] ボタン  をクリックし、[ロールの編集] ダイアログボックスを開きます。
2. 名前または説明を変更するには、それぞれのテキストボックスに新しい値を入力します。
3. サブシステムを変更するには、[このロールのサブシステムを選択] ドロップダウンリストから別のサブシステムを選択し、[OK] をクリックします。
4. 変更する権限が含まれた権限カテゴリのチェックをオンにします。必要に応じて、特定の権限のチェックをオフにします。
5. 更新する権限カテゴリごとに手順 4 を繰り返します。
6. [OK] をクリックします。

手順　ロールを削除するには

1. セキュリティセンターの [ロール] タブで、ロールを右クリックして [削除] を選択するか、ロールを選択して [ロールの削除] ボタン  をクリックします。
2. 「選択した項目をすべて削除しますか?」という確認メッセージで、[はい] をクリックします。
3. [はい] をクリックして削除を確定します。

   注意：事前にインストールされているデフォルトロールを削除することはできません。

マイグレート機能およびユーザデフォルトロール (UDR)

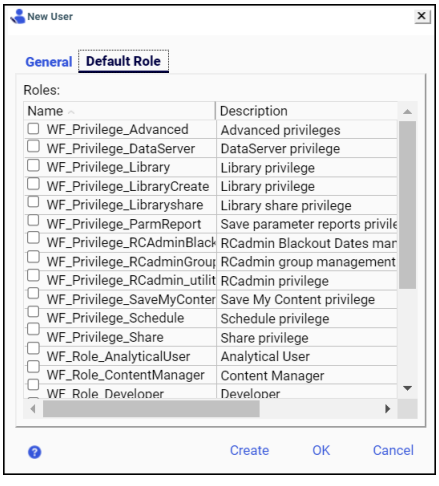
WebFOCUS バージョン 7 では、各ユーザに特定のロールが割り当てられ、それぞれのユーザは 1 つまたは複数のグループに配置されます。WebFOCUS バージョン 8 では、ユーザのアクセス権限は、ユーザロールではなく、グループに基づくルールによって決定されます。マイグレートプロセスでは、WebFOCUS バージョン 7 のユーザロールがバージョン 8 のユーザデフォルトロール (UDR) にマッピングされます。このマッピングは、ユーザが所属するグループおよびユーザがアクセス権限を持つワークスペースに関連付けられたルールに基づいて実装されます。

マイグレートされた環境で WebFOCUS バージョン 8 を使用する場合、セキュリティセンターの [ユーザデフォルトロール] タブの表示を有効にすることで、UDR 情報を確認することができます。詳細は、『TIBCO WebFOCUS マイグレーションガイド』を参照してください。

手順　セキュリティセンターにデフォルトロールタブを表示するには

1. 管理コンソールの [構成] タブで [その他] をクリックして、[その他] 設定のページを開きます。
2. [ユーザデフォルトロール (マイグレートで使用)] (IBI_ENABLE_UDR) のチェックをオンにし、[保存] をクリックします。
3. 「保存しました」というメッセージで [OK] をクリックします。
4. 現在のセッションからログアウトします。
5. 管理者として再度ログインし、セキュリティセンターに移動します。
6. セキュリティセンターで、[新規ユーザ] ボタンをクリックするか、既存のユーザを選択して [ユーザの編集] ボタンをクリックします。

下図のように、[新規ユーザ] または [ユーザの編集] ダイアログボックスが開きます。[デフォルトロール] タブをクリックします。



ルールの管理

ルールの作成は、常にリソースツリーまたはセキュリティセンターでリソースを選択することから開始します。ルールは、任意のリソースに配置することができます。これらのリソースには次のものがあります。

- フォルダ
- プロシジャ
- ReportLibrary 出力
- ポータルページ
- WebFOCUS Reporting Server
- グループ
- ユーザ
- ロール

手順　コンテンツリソースに対してルールを作成するには

1. リソースツリーまたはコンテンツエリアで、ノードまたはコンテンツリソースを右クリックし、[セキュリティ]、[ルール] を順に選択します。

2. 対象を選択します。

   - グループを選択するには、グループ名をクリックします。
   - ユーザを選択するには、最初に [ユーザ] タブを選択し、ユーザ名をクリックします。

   [グループを対象とするルール] または [ユーザを対象とするルール] ウィンドウに、利用可能なロールのリストが表示され、[このリソースで使用可能なすべてのロール] でフィルタされています。選択したリソースおよび対象のルールで使用済みのロールは、太字で表示されます。

3. ロールを選択します。

   デフォルト設定では、[グループを対象とするルール] または [ユーザを対象とするルール] リストに、コンテンツリソースで使用可能なロールがすべて表示されます。表示するロールを制限するには、[ロール] ドロップダウンリストから、次のフィルタのいずれかを選択します。

   - **カスタム** - ユーザ定義
   - **標準** - リソースタイプに適用する標準オプション
   - **ロール** - レガシーロールと権限
   - **詳細.** - リソースタイプに適用する詳細オプション

4. [アクセス] 列で、各ロールのアクセスを [許可する]、[拒否する]、[最上級の許可]、[継承のクリア] のいずれかに設定します。

   デフォルト値は [設定しない] ですが、別のアクセスタイプが親リソースから継承されていない限り、この設定を選択する必要はありません。継承されている場合、継承元の親リソースが [継承されたルール] 列に表示されます。

5. [適用先] 列で、ルールの適用先を [フォルダと下位]、[フォルダのみ]、[下位のみ] のいずれかに設定します。

   これらの設定は、グループとサブグループの関係、ポータルとポータルページの関係、または IBFS 内で階層関係を持つオブジェクト間の関係を示す場合もあります。

6. 選択したリソース上の選択した対象に対して別のルールを引き続き作成する場合は、[適用] をクリックします。現在のルールを保存し、セキュリティセンターに戻る場合は、[OK] をクリックして [セキュリティルール] ダイアログボックスを閉じます。

手順　グループ、ユーザ、ロールに対してルールを作成するには

1. セキュリティセンターの [ユーザとグループ] タブで、リソースを選択します。
   - ❏ ユーザを選択するには、ユーザ名を右クリックし、[セキュリティ]、[ルール] を順に選択します。
   - ❏ グループを選択するには、グループ名を右クリックし、[セキュリティ]、[ルール] を順に選択します。
   - ❏ ロールを選択するには、[ロール] タブでロール名を右クリックし、[セキュリティ]、[ルール] を順に選択します。
2. 対象を選択します。
   - ❏ グループを選択するには、グループ名をクリックします。
   - ❏ ユーザを選択するには、最初に [ユーザ] タブを選択し、ユーザ名をクリックします。

   [グループを対象とするルール] または [ユーザを対象とするルール] ウィンドウに、利用可能なロールのリストが表示され、[このリソースで使用可能なすべてのロール] でフィルタされています。選択したリソースおよび対象のルールで使用済みのロールは、太字で表示されます。
3. ロールを選択します。

   デフォルト設定では、[グループを対象とするルール] または [ユーザを対象とするルール] リストに、コンテンツリソースで使用可能なロールがすべて表示されます。表示するロールを制限するには、[ロール] ドロップダウンリストから、次のフィルタのいずれかを選択します。
   - ❏ カスタム - ユーザ定義
   - ❏ 標準 - リソースタイプに適用する標準オプション
   - ❏ ロール - レガシーロールと権限
   - ❏ 詳細 - リソースタイプに適用する詳細オプション
4. [アクセス] 列で、各ロールのアクセスを [許可する]、[拒否する]、[最上級の許可]、[継承のクリア] のいずれかに設定します。

   デフォルト値は [設定しない] ですが、別のアクセスタイプが親リソースから継承されていない限り、この設定を選択する必要はありません。継承されている場合、継承元の親リソースが [継承されたルール] 列に表示されます。
5. [適用先] 列で、ルールの適用先を [フォルダと下位]、[フォルダのみ]、[下位のみ] のいずれかに設定します。

これらの設定は、グループとサブグループの関係、ポータルとポータルページの関係、または IBFS 内で階層関係を持つオブジェクト間の関係を示す場合もあります。[適用先] 列は、[アクセス] 列でこのルールの値を選択した後にのみ選択可能になります。

6. 選択したリソース上の選択した対象に対して別のルールを引き続き作成する場合は、[適用] をクリックします。現在のルールを保存し、セキュリティセンターに戻る場合は、[OK] をクリックします。

手順　リソースからルールを削除するには

1. リソースツリーまたはコンテンツエリアで、ノードまたはコンテンツリソースを右クリックし、[セキュリティ]、[ルール] を順に選択します。
2. ルールの対象とするグループまたはユーザを選択します。
3. [ユーザを対象とするルール] または [グループを対象とするルール] リストの [アクセス] 列で、不要なロールごとにアクセスを [設定しない] に設定します。
4. さらに変更を加える場合は、[適用] をクリックます。変更を保存し、セキュリティセンターを閉じる場合は、[OK] をクリックします。

手順　リソースのルールを表示するには

特定のリソースにアクセスできるユーザを確認するには、リソースを右クリックし、[セキュリティ]、[このリソースのルール] を順に選択します。継承された有効なルールを表示するには、[継承されたルールを含める] のチェックをオンにします。列見出しをクリックして、その列を基準にソートします。ダイアログボックスに表示された情報をリッチテキスト形式のレポートで出力するには、[レポートの作成] をクリックします。

手順　グループまたはユーザのルールを表示するには

特定のグループまたはユーザがアクセスできるリソースを確認するには、グループまたはユーザを右クリックし、[セキュリティ] を選択した後、[このユーザを対象とするルール] または [このグループを対象とするルール] を選択します。列見出しをクリックして、その列を基準にソートします。ダイアログボックスに表示された情報をリッチテキスト形式のレポートで出力するには、[レポートの作成] をクリックします。

参照　このリソースのルールダイアログボックスの理解

[このリソースのルール] ダイアログボックスには、選択したリソースに割り当てられたルールがすべて表示されます。これらのルールには、親リソースから継承されたルールも含まれます。このダイアログボックスでは、選択したリソースに割り当てられたルールを確認できる以外に、この表示からレポートを生成して後から確認することもできます。

すべてのリソースには一連のルールが適用され、これらのルールに基づいて、さまざまなグループやユーザの各リソースへのアクセスが決定されます。[このリソースのルール] ダイアログボックスの各エントリには、リソースに割り当てられたルールが表示されます。そのルールを構成するコンポーネントにより、特定のユーザまたはグループと、事前に構成されたロールが関連付けられます。ユーザおよびグループはロールに関連付けられ、そのロールにルールに割り当てられることで、ユーザやグループの要求および役割に応じたリソースの使用権限が許可されます。リソースに複数のルールが割り当てられることで、広範囲のユーザの要求および役割に応じたリソースの使用が可能になります。

各ルールは、次のコンポーネントで構成されます。

対象

ルールが適用されるグループまたはユーザです。グループおよびユーザは、セキュリティセンターで定義されます。

アクセス

ユーザグループがリソースにアクセスできるかどうかを示します。有効な値は、[設定しない]、[許可する]、[拒否する]、[最上級の許可]、[継承のクリア] です。この値では、アクセス権限が親リソースから継承されたかどうかも示されます。

ロール

特定のアクションを実行する権限の集合体です。ロールは、セキュリティセンターで定義されます。

適用先

リソースの階層内でこのルールが適用されるリソースの範囲です。有効な値は、[フォルダと下位]、[フォルダのみ]、[下位のみ] です。これらの設定は、グループとサブグループの関係、ポータルとポータルページの関係、または IBFS 内で階層関係を持つオブジェクト間の関係を示す場合もあります。

設定先

リソースツリー内で特定のルールが設定されたフォルダまたはサブフォルダです。たとえば、「/WFC」に設定されている場合、ルールはツリー内のすべてのリソースに適用されます。「/WFC/Repository」に設定されている場合、ルールは [リポジトリ] ノード内のリソースにのみ適用されます。

このダイアログボックスのその他の機能を使用して、ルールの表示方法を調整したり、現在の表示からレポートを生成したりできます。

[継承されたルールを含める] チェックボックスを使用して、継承されたルールの表示と非表示を切り替えることができます。フォルダまたはオブジェクトから継承されたルールを表示に含めるには、このチェックをオンにします。

[レポートの作成] ボタンをクリックすると、ルールのリストをリッチテキスト形式のレポートとして保存または印刷することができます。このダイアログボックスから作成されたレポートには、リソース名とともに、レポートの作成日時も表示されます。このレポートは、特定の日時にそのリソースに割り当てられている一連のルールを記録する際に役立ちます。

手順　選択したロールを使用するルールを表示するには

ロールを削除する前に、そのロールの使用先を確認することをお勧めします。

1. セキュリティセンターで [ロール] タブをクリックします。
2. ロールを右クリックし、[セキュリティ]、[このロールを使用するルール] を順に選択します。
3. ダイアログボックスに表示された情報をリッチテキスト形式のレポートで出力するには、[レポートの作成] をクリックします。

プライベートリソースの管理

マネージャが他のユーザのプライベートリソースを表示または変更することが必要になる場合があります。たとえば、従業員が会社を退社し、そのステータスが非アクティブに設定されている場合、その従業員のプライベートリソースを削除したり、他のユーザに移動したりすることが必要になります。また、マネージャが管理するグループのプライベートリソースへのアクセス権限を所有することで、リソースの共有やプロシジャのトラブルシューティング時にも役立つ場合があります。ユーザまたはグループに [Manage Private Resources (opManagePrivateResources)] 権限を付与すると、指定されたユーザやグループが所有するプライベートコンテンツを管理することが可能になります。通常、この権限が [許可する] に設定されているのは、ワークスペースに関連付けられたグループの管理者や、特定のグループを管理するグループ管理者です。

他のユーザが所有する非出力リソース (例、プロシジャ、レポートオブジェクト、スケジュール) に対しては、ほとんどのアクションを実行することができます。出力リソースの場合 (例、PDF、ReportLibrary)、実行可能なアクションは、リソースの削除とリソースタイトルの変更のみに限定されます。

プライベートリソースの表示と管理は、ワークスペース別に実行することも、ユーザまたはグループ別に実行することもできます。

手順　ユーザまたはグループ別にプライベートリソースを管理するには

[プライベートリソース管理] 機能を使用することで、特定のユーザまたはグループが所有するプライベートリソースを識別、管理することができます。

1. 管理者としてログインします。

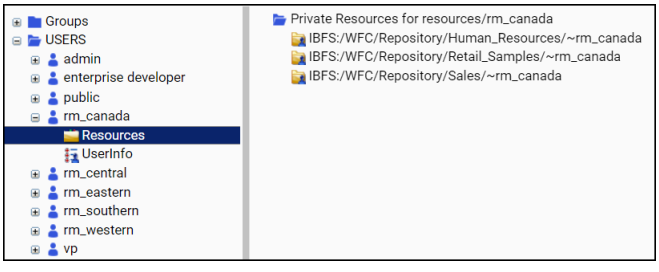
2. WebFOCUS Hub のサイドナビゲーションウィンドウから、[管理センター]、[プライベートリソース] を順に選択します。

   または

   WebFOCUS ホームページで、[設定]、[プライベートリソース管理] を順に選択し、[プライベートリソース管理] ダイアログボックスを開きます。

3. 表示または管理するリソースを所有するユーザまたはグループを展開します。

   グループを選択すると、そのグループが所有するリソースがすべて表示されます。下図のように、ユーザを選択すると、リソースとユーザ情報が表示されます。



   ユーザ情報には、プライベートポータルやホームディレクトリなどの、ユーザ固有のリソースのフルパスが表示されます。

4. 管理対象グループのメンバーに属するリソースを右クリックし、メニューからアクションを選択します。

   他のユーザが所有する非出力リソース (例、プロシジャ、レポートオブジェクト、スケジュール) に対しては、ほとんどのアクションを実行することができます。出力リソースの場合 (例、PDF、ReportLibrary)、実行可能なアクションは、リソースの削除とリソースタイトルの変更のみに限定されます。

7

TIBCO WebFOCUS 環境の保護

ここでは、WebFOCUS の情報セキュリティ保証のベストプラクティス、セキュリティ機能、暗号化機能について説明します。また、WebFOCUS コンポーネントに推奨されるファイルシステムアクセス許可、および WebFOCUS 変数を保護するための注意事項についても説明します。

トピックス

情報セキュリティ保証のベストプラクティス

情報セキュリティ保証 (Information Assurance*) とは、可用性、完全性、真正性、機密性、否認防止性を確保することによって、情報および情報システムを保護するための基準のことをいいます。これらの基準には、保護、検出、応答機能の統合によって、情報システムの復旧能力を提供することが含まれています。WebFOCUS には、戦略的リスク管理および悪意のあるハッカーの攻撃からの保護に重点を置いた、さまざまな新しいセキュリティ機能が追加されています。このレベルのセキュリティは、外部と接触する Web ベースの BI アプリケーションでは不可欠です。

WebFOCUS バージョン 8 は、OWASP ASVS を使用した検証でレベル 2a を達成し、OWASP によって業界で最も重要であると定義された脆弱性および脅威に対して、脆弱性が低いとの評価が得られました。情報セキュリティ保証および OWASP についての詳細は、http://www.owasp.org/index.php/Main_Page を参照してください。

*出典 - アメリカ合衆国政府発行情報セキュリティ保証用語集、セキュリティ統合上位文書 (US Government's Information Assurance Glossary Superset of Security Integration)

マニュアル

この章には、標準的な構成が参考情報として記載されています。この章に記載されている設定およびコントロールについての詳細は、以下のマニュアルを参照してください。

- 『TIBCO WebFOCUS インストールガイド』
- 『TIBCO WebFOCUS ReportCaster 利用ガイド』

Open Web Application Security Project (OWASP)

OWASP (Open Web Application Security Project) は、アプリケーションソフトウェアのセキュリティ向上に特化して活動するオープンコミュニティ組織です。OWASP の情報、ツール、文書、フォーラムはすべて、Web ベースのセキュリティおよびアプリケーションソフトウェア環境内のセキュリティ向上の学習に関心のある誰もが無料で利用することができます。

OWASP Top Ten Project には、Web 脆弱性のリスト、これらの脆弱性を解消するための対策が記載されています。

さらに、OWASP からは Application Security Verification Standard (ASVS) 文書が提供されています。この文書は、Web アプリケーションのセキュリティ脆弱性をテストするために実装可能な基準が要約されています。

Top Ten Project および ASVS 文書についての詳細は、OWASP の Web サイト (https://www.owasp.org/index.php/Main_Page) を参照してください。

ReportCaster の設定

通常、ReportCaster Distribution Server はセキュアなネットワーク環境内で実行され、これらの通信パラメータを暗号化する必要ありません。Distribution Server から BI Portal への通信の暗号化、Distribution Server と Reporting Server 間のデータの暗号化が必要な場合は、次の手順を実行します。

JSSE Caster

ReportCaster の構成で、このオプションを YES に設定します。この設定により、ReportCaster Distribution Server から BI Portal リポジトリに通信して MR プロシジャをスケジュールする際に SSL の使用が可能になります。

JSSE Servlet

ReportCaster の構成で、このオプションを YES に設定します。この設定により、アプレットスケジュールツールで MR プロシジャを取得する際に SSL の使用が可能になります。

3DES 暗号化接続を WFRS に設定し、WebFOCUS Reporting Server JDBC URL に次のパラメータを追加します。

```
jdbc:eda:¥¥hostname:port;server=;ENCRYPTION=1;
```

TIBCO WebFOCUS Reporting Server のセキュリティ

ここでは、TIBCO WebFOCUS Reporting Server のセキュリティについて説明します。詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。ガイドラインは次のとおりです。

- WebFOCUS Reporting Server を WebFOCUS Client とは異なる物理マシンにインストールする。
- RESTRICT_TO_IP 設定を使用して、外部からの通信を制限する。

  TCP/IP および HTTP 接続用ホストの制限リストで、外部からの接続要求を受容するよう WebFOCUS Reporting Server を構成します。この方法を使用するか、WebFOCUS Client と WebFOCUS Reporting Server 間にファイアウォールを設定する方法のいずれかまたは両方を使用します。
- SSL を使用して、ブラウザ、WebFOCUS Client、WebFOCUS Reporting Server の HTTP リスナ間のデータをすべて暗号化する。
- WebFOCUS Client から WebFOCUS Reporting Server への TCP/IP 通信に AES 暗号化を使用する。

- オペレーティングシステムコマンドを無効にする。

  アプリケーションでオペレーティングシステムコマンドを使用する必要がない場合は、WebFOCUS Reporting Server 上でロールベースのアクセスコントロールを使用することで、これらのコマンドを無効にします。セキュリティが設定されたサーバの Reporting Server ブラウザインターフェースで、[アクセスコントロール] タブをクリックし、[一般ユーザ] ロールをクリックします。[全般権限] ウィンドウで、[オペレーティングシステムのコマンドを無効にする] のチェックをオンにします。

- ダイレクトパススルーオプションを無効にする。

  アプリケーションでダイレクト SQL パススルーを使用する必要がない場合は、WebFOCUS Reporting Server 上でロールベースのアクセスコントロールを使用することで、ダイレクトパススルーを無効にします。セキュリティが設定されたサーバの Reporting Server ブラウザインターフェースで、[アクセスコントロール] タブをクリックし、[一般ユーザ] ロールをクリックします。[全般権限] ウィンドウで、[ダイレクトパススルーを無効にする] のチェックをオンにします。

- HTML 出力データをエンコードする。

  この設定により、HTML タグが実データ内に格納されている場合や DEFINE または COMPUTE コマンドを使用して作成された場合に、これらのタグのブラウザ内での表示が無効になります。セキュリティが設定された Reporting Server ブラウザインターフェースで、[ワークスペース] タブをクリックし、[ワークスペース] フォルダを右クリックして [その他の設定] を選択します。[htmlencode] リストで [y] を選択し、[保存] をクリックします。

- WebFOCUS Reporting Server でマスターファイルを暗号化する。

- WebFOCUS Reporting Server のプロシジャを暗号化する。

- SET DEFECHO=NONE を設定する。この設定により、エコー出力が無効になり、WebFOCUS コードに関する情報がブラウザに返されなくなります。

- アクセスを制限するマスターファイルに DBA セキュリティを使用する。

TIBCO WebFOCUS Reporting Server と IBFS セキュリティの分離

サーバの保護が必要な場合は、IBFS ルールを使用して WebFOCUS Reporting Server ノードの表示と非表示を切り替える方法をお勧めしますが、WebFOCUS Reporting Server 上の特定のリソースを保護する場合は、WebFOCUS Reporting Server のロールとアクセスコントロール機能を使用することをお勧めします。WebFOCUS Reporting Server ノードより下位のリソースに適用されたルールは、WebFOCUS ユーザインターフェースの他の部分に表示される項目には影響しません。このルールは、リソースツリーの表示にのみ適用されます。WebFOCUS Reporting Server アクセスコントロール機能によるセキュリティは、SQL パススルーやオペレーティングシステムコマンドなどのサーバエンジン設定へのアクセス制御や、メタデータおよびアップロード済みデータを格納するアプリケーションフォルダへのアクセス制御を行える点で、より優れています。

データセキュリティと IBFS セキュリティの分離

IBFS セキュリティは、リポジトリ内のリソースおよび一部の外部リソース (例、WebFOCUS Reporting Server ノード) を管理します。ただし、データベースのデータ行およびメタデータのフィールド名へのアクセスは、データセキュリティ (DBA) 機能によって管理されます。これらのデータセキュリティ機能を使用するには、認証済みのユーザ ID およびユーザグループを WebFOCUS Reporting Server に渡します。

WebFOCUS Client と WebFOCUS Reporting Server 間の情報通信についての詳細は、25 ページの 「 TIBCO WebFOCUS Reporting Server の構成 」 を参照してください。

TIBCO WebFOCUS 変数の保護

WebFOCUS スクリプトにより、変数処理制御のオプションを設定することができます。保護オプションはその 1 つで、次の構文を使用してブラウザから変数の設定を防止します。

```
<SET> variable_name (protect)
```

WebFOCUS スクリプトコマンドについての詳細は、717 ページの 「 TIBCO WebFOCUS スクリプトコマンド 」 を参照してください。

保護すべき変数には IBIF_adhocfex と IBIF_raw が含まれます。これらにより、WebFOCUS が FOCUS コマンドを URL 上の WebFOCUS Reporting Server に送信することができます。

TIBCO WebFOCUS の暗号化機能

WebFOCUS では、さまざまな方法で暗号化機能や暗号化サービスが使用されます。これらの暗号化機能には次のものがあります。

- WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続の暗号化機能
- サービスアカウント情報の暗号化機能
- WebFOCUS スクリプトファイルの暗号化機能
- WebFOCUS プロシジャおよびメタデータの暗号化機能

セキュリティを考慮する上で重要な要素の 1 つに機密性の問題があります。機密性とは、機密データを暗号化することによって情報のプライバシーを保護することです。暗号化されたファイルは、認証されていないユーザによる閲覧や使用から保護されます。暗号化されたファイルを復号化するには、キーファイルを使用します。暗号化には、データ、ネットワークセッション、ファイルをベースにした方法があります。管理コンソールの [Client 設定] および [出力先変更設定] の暗号化オプションを使用することで、さまざまな構成ファイルの中で、WebFOCUS スクリプトファイル (.wfs) を暗号化することができます。また、WebFOCUS Client と WebFOCUS Reporting Server 間の通信を暗号化することもできます。

WebFOCUS Client についての詳細は、560 ページの 「 暗号化の設定 」 を参照してください。出力先変更設定についての詳細は、130 ページの 「 出力先変更設定の理解 」 を参照してください。

WebFOCUS バージョン 8 には独自の暗号化アルゴリズムが付属していますが、業界標準の AES 暗号化を使用するよう構成することもできます。レガシーアプリケーションには、ネイティブ WebFOCUS 暗号化が必要になる場合があります。

デフォルト TIBCO WebFOCUS 暗号化と AES 暗号化

WebFOCUS ソフトウェアでは、次の形式の暗号化がサポートされます。

- デフォルト WebFOCUS 暗号化
- AES (高度暗号化標準) 暗号化

  代替 AES 暗号化プロバイダは、管理コンソールで有効にすることができます。キーの長さは、128 ビット、192 ビット、256 ビットのいずれかにすることができます。

ReportCaster で AES 暗号化を使用するよう構成する方法についての詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』の「ZIP 暗号化保護デフォルトプラグインの使用」を参照してください。

注意：WebFOCUS ソフトウェアの以前のバージョンでは、カスタムアルゴリズムに基づくカスタムセキュリティ暗号化プロバイダがサポートされていました。新しいバージョンでは AES 暗号化が優先的にサポートされるため、カスタムアルゴリズム機能は廃止されました。カスタムアルゴリズムを使用する必要のある場合は、技術サポートに問い合わせてください。

参照

キーファイルのフォーマット

暗号化のキー情報は、テキストファイルに格納され、16 進数表記の文字列で表されます。キーの 8 ビット (1 バイト) が、16 進数表記の 2 文字を表します。たとえば、64 ビット (8 バイト) のキーは、16 進数表記の 16 個の文字で表されます。各文字は、数字 (0 - 9) または英文字 (A - F) のいずれかです。

下表は、AES アルゴリズムの暗号化キーに必要な 16 進数の文字数を示しています。

キーの長さ (ビット)	16 進数文字数	サンプル文字列	アルゴリズム
128	32	5468658A6C617A795468658A6C617A79	AES128
192	48	5468658A6C617A7920646F67206A756D 7073206F7665723F	AES192
256	64	5468658A6C617A7920646F67206A756D 7073206F7665723F5468658A6C617A79	AES256

WebFOCUS Client での暗号化の構成

WebFOCUS 管理コンソールでは、代替暗号化プロバイダの有効化、外部セキュリティトークンの構成、WebFOCUS 構成ファイルの暗号化、WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続の暗号化を行えます。

注意：128 ビットを超える暗号化キーを使用する場合は、製品環境で使用する JVM で、暗号強度を無制限にするための Java Cryptography Extension (JCE) Jurisdiction Policy File を使用する必要があります。詳細は、Oracle のマニュアルを参照してください。

http://www.oracle.com/technetwork/java/javase/downloads/jce-6-download-429243.html

手順　代替 AES 暗号化プロバイダを有効にするには

管理コンソールを使用して、代替 AES 暗号化プロバイダを有効にし、内部キーまたは外部キーを指定することができます。

1. 管理者としてログインし、管理コンソールを起動します。
2. [アプリケーションの設定] フォルダ下で、[暗号化] をクリックします。
3. [プロバイダ] (IBI_ENCRYPTION_PROVIDER) 設定のリストから、下表に示す暗号化プロバイダのいずれかを選択します。「KeyFile」と記載されていない場合、内部キーファイルが使用されます。

暗号化アルゴリズム	オプション
内部キーによる AES 128 暗号化	ibi.webfoc.wfsecurity.encryption.wireaes WFWireAES128
外部キーによる AES 128 暗号化	ibi.webfoc.wfsecurity.encryption.wireaes WFWireAES128KeyFile
内部キーによる AES 192 暗号化	ibi.webfoc.wfsecurity.encryption.wireaes WFWireAES192
外部キーによる AES 192 暗号化	ibi.webfoc.wfsecurity.encryption.wireaes WFWireAES192KeyFile
内部キーによる AES 256 暗号化	ibi.webfoc.wfsecurity.encryption.wireaes WFWireAES256
外部キーによる AES 256 暗号化	ibi.webfoc.wfsecurity.encryption.wireaes WFWireAES256KeyFile

内部キーを使用する場合は、手順 7 へ進みます。外部キーを使用する場合は、手順 4 へ進みます。セキュリティトークンを使用する場合は、手順 6 へ進みます。

4. キーファイルを作成し、そのファイルをテキストファイルとして保存します。

   16 進数キーについての詳細は、495 ページの 「 キーファイルのフォーマット 」 を参照してください。

   セキュリティトークンを使用して WebFOCUS Client と他のソフトウェア間のトラステッド通信を有効にする場合は、手順 5 へ進みます。それ以外の場合は、手順 7 へ進みます。

5. セキュリティトークンを使用して WebFOCUS Client と他のアプリケーション間のトラステッド通信を有効にする場合は、[トークンキー] (IBI_WF_TOKEN_KEY) 設定にトークンの値を入力し、[保存] をクリックします。
6. 他のアプリケーションで、セキュリティトークンの値を指定します。

   セキュリティトークンの構成についての詳細は、使用する他のアプリケーションのマニュアルを参照してください。
7. 管理コンソールの [セキュリティ] タブをクリックし、[セキュリティの構成] フォルダ下の [詳細] をクリックします。
8. 次の 1 つまたは複数のサーバアカウント認証情報を入力します。

   - ❏ IBI_WFRS_Service_Pass
   - ❏ IBI_Anonymous_WFRS_Pass
   - ❏ IBI_Admin_Pass
   - ❏ IBI_Magnify_Repos_DB_Password
9. Application Server を再起動します。

   起動プロセス中に、構成ファイル内の新しいパスワードすべてが自動的に暗号化されます。

手順 WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続を暗号化するには

管理コンソールを使用して、WebFOCUS Client と WebFOCUS Reporting Server 間のトラステッド接続を暗号化することができます。トラステッド接続の構成についての詳細は、51 ページの 「 WebFOCUS Client と TIBCO WebFOCUS Reporting Server 間のトラステッド接続を構成するには 」 を参照してください。

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブで、[Reporting Server] フォルダ、[サーバ接続] フォルダを順に展開します。
3. 特定の Reporting Server ノードをクリックします。

   [Client の構成] ページが開きます。
4. [詳細] ノードを展開します。
5. [暗号化] リストから次のオプションのいずれかを選択し、[保存] をクリックします。

   - ❏ **0** オフ

- ***cipher*(*x*)[-*mode*]**

  説明

cipher

使用する暗号化アルゴリズムです (例、AES128、AES256)。

x

必要に応じて、RSA キー長の 1024 ビットを定義します。この値を指定しない場合、デフォルト値の 512 ビットが使用されます。

mode

必要に応じて、処理モードとして ECB (Electronic Code Book) または CBC (Cipher Block Chaining) を指定します。この値を指定しない場合、デフォルト値の ECB が使用されます。

6. [保存] をクリックします。
7. 「保存しました」というメッセージで [OK] をクリックします。
8. 他のアプリケーションで、セキュリティトークンの値を指定します。

   セキュリティトークンの構成についての詳細は、使用する他のアプリケーションのマニュアルを参照してください。
9. 構成ファイルに次のサーバアカウント認証情報の 1 つまたは複数を再入力します。
   - IBI_WFRS_Service_Pass
   - IBI_Anonymous_WFRS_Pass
   - IBI_Admin_Pass
   - IBI_Magnify_Repos_DB_Password
10. Application Server を再起動します。

    起動プロセス中に、構成ファイル内の新しいパスワードすべてが自動的に暗号化されます。

8

TIBCO WebFOCUS 変更管理

変更管理とは、同一リリースレベルの WebFOCUS 環境間でアプリケーションコンポーネントを移動するプロセスのことです。通常、WebFOCUS 環境間のアプリケーションコンポーネントの移動は、実稼動環境に展開する前に、アプリケーションをテスト環境で十分にテストした上で行われます。

WebFOCUS には、これらの重要な作業を簡単に行うための機能や手法が用意されています。

トピックス

変更管理プロセスの理解

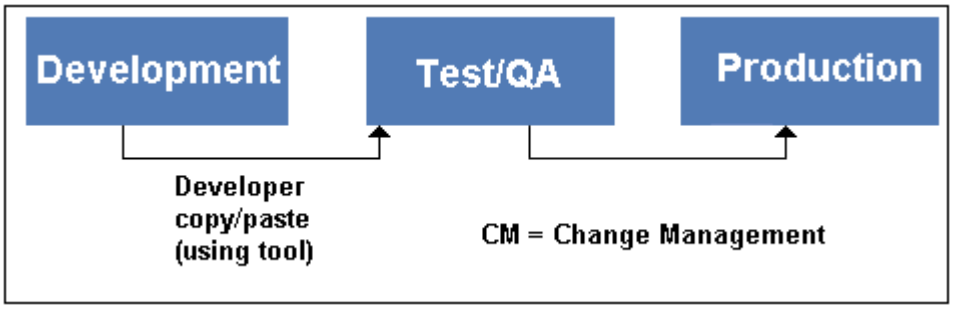
アプリケーションの開発は反復的なプロセスです。開発者は、アプリケーションコードを修正し、コンポーネントを定期的にテスト環境に移動して、ユーザのフィードバックや承認を受け取ります。アプリケーション開発サイクルのある時点でアプリケーションが安定すると、それを実稼動環境に移動します。アプリケーションを一般公開した後は、問題の解決、修正版のテスト、実稼動環境への組み込みが必要になります。これが、工程管理とも呼ばれる、変更管理プロセスの重要な点です。

変更管理に対する組織の取り組み方はさまざまです。多くの業務を開発者に委ねる組織もあれば、より高度な管理レベルを維持するための代替プロセスを構築している組織もあります。通常、開発者は開発ツールを使用してこれらの業務を遂行しますが、変更管理の担当者は環境間でアプリケーションコンポーネントを移動するバッチ指向の方法を好みます。アプリケーションを実稼動環境に移動した後の変更作業のため、開発者には、変更管理パッケージを作成するという作業が必要になる場合があります。大規模な企業では、多くの場合、これらの方式を組み合わせて使用します。

次の例では、2 つの異なる変更管理プロセスについて紹介します。ここでは、各組織の変更管理プロセスの目的を達成するための機能や手法について説明します。

例　アプリケーションファイルの移動 - 単純な変更管理プロセス

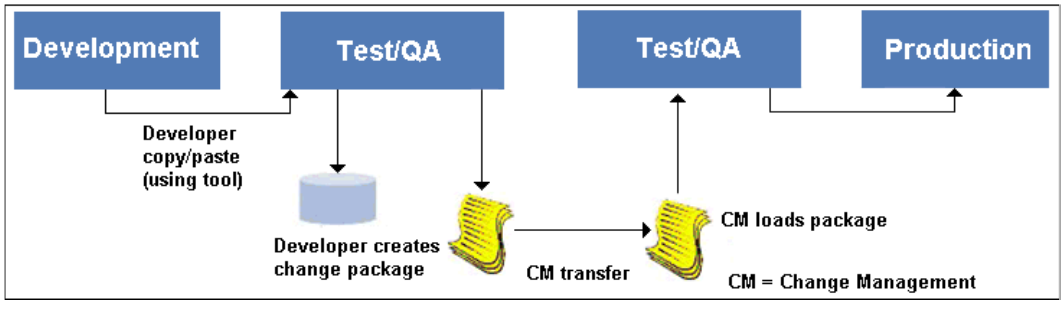
下図のように、開発者は開発ツールを使用して、開発環境とテスト環境の間でアプリケーションファイルを移動します。アプリケーションが完成した段階で、オペレーティングシステムのユーティリティを使用して、アプリケーションをテスト環境から実稼動環境にコピーします。この例では、テスト環境は 1 つだけです。



例　アプリケーションファイルの移動 - 包括的な変更管理プロセス

この例では、4 つの 環境が構築され、アプリケーションコードを実稼動環境に移動する管理レベルが強化されています。開発者は、リソースツリーを使用して、 アプリケーションファイルを開発環境からテスト環境に移動します。その後、ユーザテスト環境に変更を移動する準備ができた段階で、開発者は変更管理エクスポート機能を使用します。

開発者は、変更管理エクスポート機能を使用して、移動するリソースを選択し、変更管理パッケージを作成できます。続いて、管理者は、変更管理インポート機能を使用して、変更管理パッケージをユーザテスト環境に移動できます。各組織のビジネスプロセスとの統合を図るために、コンテンツを自動的にインポートするプロセスを採用している組織もあります。下図のように、アプリケーションのリリース準備ができた段階で、工程管理担当者は、アプリケーションのファイルシステムコピーを実稼動環境に移動します。ユーザがアプリケーションの使用を開始すると、変更管理プロセスは、アプリケーションの保守サポートの段階に移ります。これ以降、管理者は変更管理インポート機能を使用することで、実稼動環境への段階的な更新を簡単に行うことができます。



変更管理パッケージの作成

多くの組織では、ユーザテスト環境および実稼動環境への書き込みアクセス権限を開発者に与えていません。これらの環境へのアクセスは厳しく管理され、アクセス権限は、管理者、工程管理担当者、または変更管理の自動プロセスのみに許可されています。

ただし、変更をテスト環境に移動する準備ができているかどうかを判断できるのは開発者だけです。開発者は、変更管理エクスポート機能を使用することで、グラフィカルな外観で表示された管理対象のリソースから、変更管理パッケージを作成することができます。作成されたパッケージは、工程管理担当者または自動プロセスによって別の環境へロードされます。

ユーザには、変更管理パッケージを作成する権限が必要です。この権限は、[Resource Export (opExport)] というハイブリッド権限で、[Application Development] 権限カテゴリ下にあります。この権限は、デフォルト設定で Administrators グループのメンバーに割り当てられます。

変更管理パッケージの作成に必要な手順は次のとおりです。

1. **シナリオの作成**　変更管理エクスポート機能を使用して、エクスポートするリソースを選択するという方法でシナリオを作成します。シナリオは、変更管理エクスポートパッケージに含めるリソースがすべて記述された説明です。

2. **シナリオのエクスポート**　シナリオの作成後、変更管理パッケージとしてそのシナリオを変更管理エクスポートディレクトリにエクスポートします。エクスポートプロセスでは、フォルダおよび変更管理 ZIP ファイルの 2 つのフォーマットでパッケージが生成されます。フォルダには、変更管理パッケージの展開済みコンテンツが格納されます。変更管理 ZIP ファイルには、このパッケージの圧縮されたコンテンツが、ターゲット環境にダウンロードおよび転送可能なフォーマットで格納されます。

   変更管理エクスポートディレクトリは、WebFOCUS のホストマシンのファイルシステム内に格納されます。実際のパスは、ユーザの WebFOCUS インスタンスで使用されたインストールタイプによって異なります。通常、このパスは *drive*:¥ibi¥*context*¥cm¥export です。この場合の *context* は、ibi ルートディレクトリと cm ディレクトリ間にあるフォルダを表します。

3. **シナリオのダウンロード**　変更管理 ZIP ファイルは、Web ブラウザを使用して、エクスポートディレクトリから変更管理ディレクトリ外部の場所にダウンロードすることができます。この外部の場所から、変更管理 ZIP ファイルをターゲットの WebFOCUS 環境のインポートディレクトリに転送し、そのコンテンツをインポートしたり、コンテンツにアクセスしたりできます。

変更管理 ZIP ファイルの使用

ZIP ファイル形式では、変更管理パッケージに含まれるリソースが単一ファイルに圧縮され、変更管理パッケージを処理する際の速度とセキュリティが向上します。この形式は、変更管理パッケージを物理ディレクトリ間で移動する場合に特に役立ちます。この形式では変更管理パッケージに含まれるファイルのすべてが単一ファイルに圧縮、統合されるため、この単一ファイルをネットワークのソースフォルダから Email 送信することも、他のネットワークのターゲットフォルダにコピーまたは移動することもできます。

デフォルト設定では、変更管理パッケージが圧縮され、変更管理 ZIP ファイルが作成されます。この機能を無効にするには、管理コンソールの [構成] タブの [変更管理] ページで、[変更管理パッケージを圧縮する] (IBI_CM_ZIP) のチェックをオフにします。この機能を無効にした場合、変更管理パッケージに、圧縮されていない変更管理ファイル形式が使用されます。

変更管理 ZIP ファイル名のデフォルトフォーマットは、NAME_DATE_TIME_USERID です。このファイル名は、変更管理パッケージの名前、パッケージが作成された日付と時間、パッケージ作成者のユーザ ID で構成されます。

たとえば、「retail_samples_20160504_161133_administrator.zip」です。

変更管理 ZIP ファイル名に別のフォーマットを指定するには、管理コンソールの [構成] タブの [変更管理] ページで、[ZIP エクスポートファイル名のフォーマット] (IBI_CM_ZIP_FILE_FORMAT) 設定のドロップダウンリストからテンプレートを選択します。

変更管理パッケージへのコラボレーションポータルの追加

使用する WebFOCUS のバージョンでコラボレーションポータルがサポートされ、[コラボレーションポータル] オプションが有効の場合、変更管理プロセス (最初のシナリオ作成から最後のインポートまで) は、コラボレーションポータルにも対応しています。変更管理パッケージの作成、エクスポート、ダウンロード、アップロード、インポートの操作手順が記載されたトピックはすべて、ベーシックポータルだけでなく、コラボレーションポータルが含まれた変更管理パッケージも対象にしています。ただし、コラボレーションポータルを含める場合は、いくつかの注意点があります。

コラボレーションポータルを選択する際は、次の点に注意します。

- コラボレーションポータルで参照されているページすべてを変更管理シナリオに含めるには、そのポータルで参照されているページが格納されたフォルダを右クリックし、[サブツリーを含めて選択] コマンドを選択します。
- コラボレーションポータルおよびそのページで参照されているコンテンツのすべてを変更管理パッケージに含める必要があります。
- 同一環境内の各ポータルは一意のエイリアスを保持する必要があるため、インポートするために選択したポータルのいずれにも、ターゲット環境内の既存ポータルと同じエイリアスが含まれていないことを確認してください。インポートパッケージ内のポータルのいずれかに、既存ポータルと同じエイリアスが含まれる場合は、インポートプロセスにより既存ポータル内のエイリアスが削除され、新しいポータルのエイリアスに置き換えられます。このプロセスでは、既存ポータル内のエイリアスが削除されたことを通知するメッセージは送信されません。
- コラボレーションポータルが含まれた変更管理パッケージを作成する際は、[ハンドルの保持] のチェックをオンにする必要はありません。このチェックをオンにするのは、コラボレーションポータルで参照されているコンテンツがバージョン 7.7 からマイグレートされた場合のみです。

コラボレーションポータルをインポートする際は、次の点に注意します。

- コラボレーションポータルに加えたカスタマイズは、インポート後のターゲット環境でそのまま保持されます。
- ベーシックポータルに加えたカスタマイズは、インポート後のターゲット環境で再構成する必要があります。

プライベートおよび公開済みのポータルとプロシジャファイルをインポートパッケージに含めることができます。

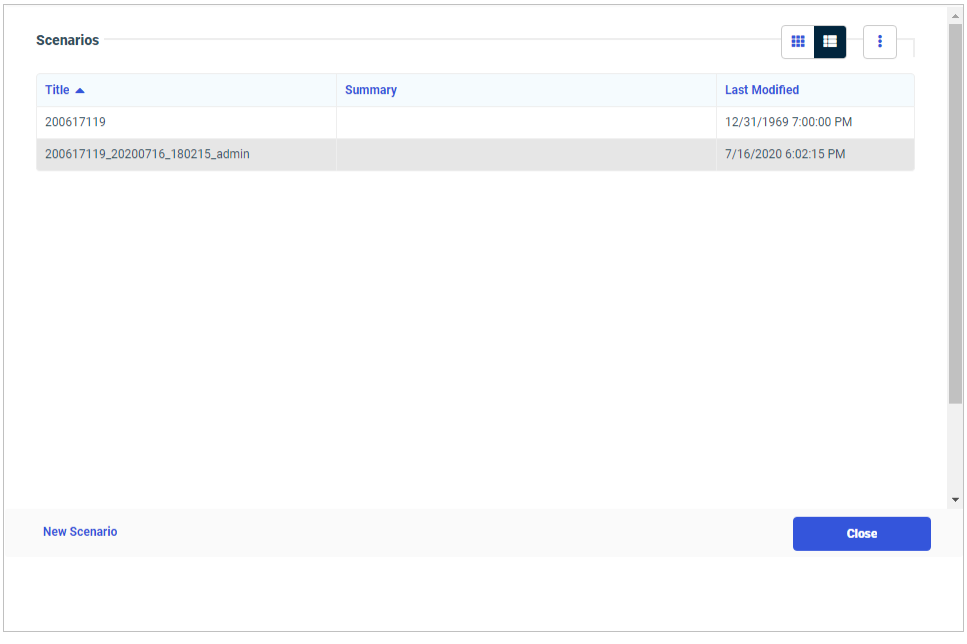
手順　変更管理機能を使用してシナリオを作成するには

使用中のブラウザでポップアップウィンドウがブロックされる場合は、その機能を無効にした上で変更管理機能を使用する必要があります。これにより、以下の手順に記載されている各ダイアログボックスが表示されます。

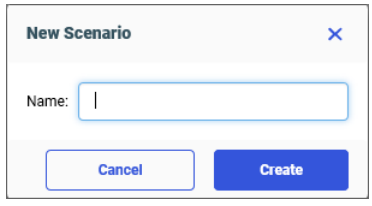
1. WebFOCUS Hub のサイドナビゲーションウィンドウから、[管理センター]、[パッケージのエクスポート] を順に選択します。

   または

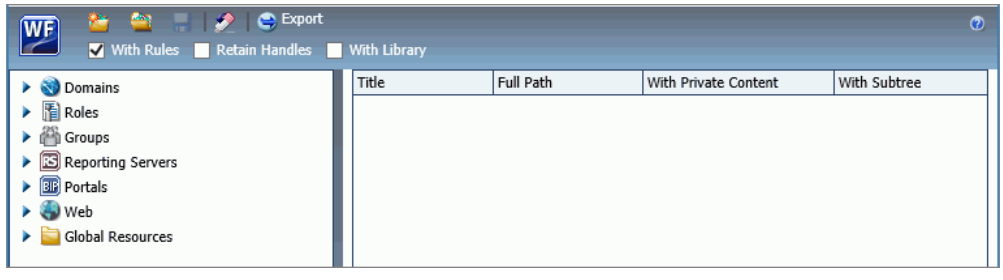
   下図のように、WebFOCUS ホームページのバナーで [ユーティリティ] メニューを開き、[変更管理]、[エクスポート] を順に選択して [シナリオ] ダイアログボックスを開きます。



2. 下図のように、[新規シナリオ] を選択して [新規シナリオ] ダイアログボックスを開きます。



3. 下図のように、[新規シナリオ] ダイアログボックスにシナリオの名前を入力し、[作成] を選択して [シナリオ] ダイアログボックスを開きます。



デフォルト設定では、[ルールを含める] のチェックはオンになっています。選択したリソースに関連付けられたルールを変更管理パッケージに含めない場合にのみ、このチェックをオフにします。

注意：ブラウザでポップアップウィンドウがブロックされたことを示す警告が表示された場合は、この Web サイトからのポップアップウィンドウをすべて許可するようブラウザ設定を変更した上で再実行します。

4. WebFOCUS バージョン 7.7 からバージョン 8 にマイグレートされたコンテンツまたは WebFOCUS バージョン 7.7 で作成された ReportCaster スケジュールが内部ハンドルを使用してプロシジャを参照している場合、これらのコンテンツやスケジュールを変更管理パッケージに含めるには、[ハンドルの保持] のチェックをオンにします。

5. シナリオに追加するフォルダに ReportCaster ReportLibrary を含めるには、[ReportLibrary を含める] のチェックをオンにします。

これらの 3 つのチェックボックスについての詳細は、511 ページの 「 変更管理オプションの理解 」 を参照してください。

6. 利用可能なリソースのリストで、追加するリソースが格納されたノードを展開します。

7. 追加するリソースを右クリックし、次の操作を実行します。

   a. [サブツリーを含めて選択] を選択すると、フォルダおよびすべてのサブフォルダとそのコンテンツ、またはグループおよび選択したすべてのサブグループが追加されます。

      外部ページを参照するコラボレーションポータルを選択する際は、そのポータルで参照されているページが格納されたフォルダも選択し、[サブツリーを含めて選択] コマンドを選択した上で、これらのページをシナリオに移動する必要があります。

   b. [フォルダのみ選択] を選択すると、指定したフォルダは追加されますが、コンテンツは含まれません。通常、このオプションは、フォルダに適用されたルールを移動する場合に使用します。

   c. [選択] をクリックすると、ロール、ポータル、またはフォルダ内の個別リソースが追加されます。

   d. [ルールのみ選択] をクリックすると、[グループ] または [WebFOCUS Reporting Server] ノードからルールが追加されます。

   e. リソースを選択する別の方法として、リソースツリーからリソースをドラッグし、右側ウィンドウにドロップすることもできます。この方法でリソースを選択した場合、デフォルト設定で [サブツリーを含める] のチェックがオンになっているため、選択したリソースからサブフォルダおよびコンテンツを除外するには、チェックをオフにする必要があります。

   リソースの選択が完了すると、そのリソースのエントリが右側ウィンドウに表示されると同時に、リソースツリーのエントリ上に取り消し線が表示されます。

   - プライベートリソースを選択した場合、[プライベートコンテンツを含める] のチェックが自動的にオンになり、これを手動でオフにすることはできません。
   - プライベートコンテンツを選択した場合、そのプライベートコンテンツのオーナーがターゲット環境に存在する場合にのみインポートされます。
   - 公開済みリソースを選択した場合、そのリソースの [プライベートコンテンツを含める] のチェックをオンにすることで、そのフォルダ内にプライベートコンテンツを含めることができます。これにより、ユーザがそのプライベートコンテンツの表示権限を所有していない場合でも、そのフォルダおよびサブフォルダ (ユーザに割り当てられている [マイコンテンツ] フォルダも含む) のプライベートコンテンツがすべてエクスポートされます。
   - 親フォルダを含めずにサブフォルダのみを選択した場合、インポートプロセスでターゲット環境に親フォルダが再作成されます。ターゲット環境には、ソース環境と同一のメタデータへの接続が存在する必要があります。

- 外部コンテンツを参照するコラボレーションポータルやページを選択する際は、その外部コンテンツも変更管理パッケージに含める必要があります。
- ソース環境とターゲット環境で適用されるルールが異なる場合、ユーザがソース環境でプライベートコンテンツへのアクセス権限を所有している場合でも、ターゲット環境でアクセスが拒否される場合があります。この問題は、ユーザがソース環境でプライベートコンテンツが格納された公開済みフォルダへのアクセス権限は所有するが、ターゲット環境でそのアクセス権限を所有していない場合に発生します。
- [ReportLibrary を含める] のチェックがオフの場合でも、上記の手順に従って個別に選択することで、シナリオに ReportLibrary を含めることができます。
- 利用可能なロールのリストには、ロックされたロールは含まれません。変更管理シナリオでは、ロックされていないロールのみエクスポートできます。

8. 変更管理シナリオに含めるリソースをさらに追加する場合は、上記の手順を繰り返します。
9. [シナリオ] ダイアログボックスで未保存の選択項目をクリアするには、ツールバーの [シナリオのリセット] をクリックします。
10. すべてのリソースの選択が完了した後、[保存] をクリックします。

    新しいシナリオのエントリが [エクスポート] ノード下に表示されます。

    新しいシナリオが表示されない場合は、[エクスポート] ノードを右クリックし、[リフレッシュ] を選択します。

    コマンドラインからスクリプトを実行して変更管理シナリオをエクスポートするには、次のディレクトリに移動し、いずれかのコマンドをダブルクリックします。

    ```
    WebFOCUS82/utilities/cm/cm_export.bat
    ```

    ```
    WebFOCUS82/utilities/cm/cm_export.sh
    ```

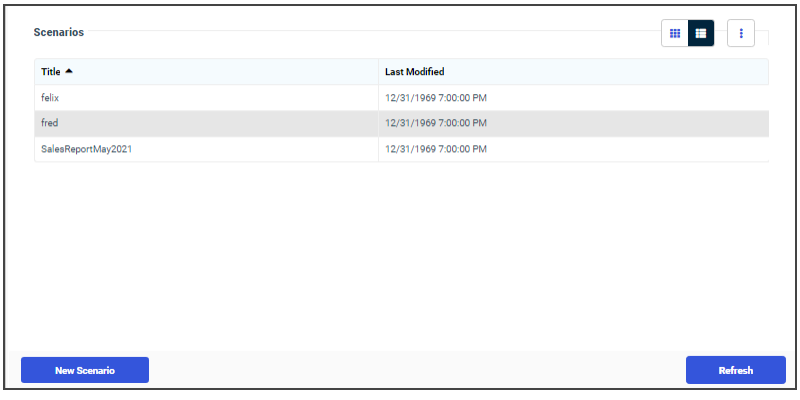
手順　変更管理インターフェースで特定のコラボレーションポータルページを移動するには

使用する WebFOCUS のバージョンでコラボレーションポータルがサポートされ、[コラボレーションポータル] オプションが有効の場合、変更管理インターフェースを使用して、特定の環境でコラボレーションポータル用に作成されたページを、同一のコラボレーションポータルが存在する別の環境に移動することができます。この手順は、コラボレーションポータル用に作成されたページにのみ適用されます。ベーシックポータル用に作成されたページには適用されません。

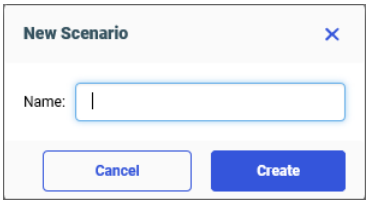
1. WebFOCUS Hub のサイドナビゲーションウィンドウから、[管理センター]、[パッケージのエクスポート] を順に選択します。

または

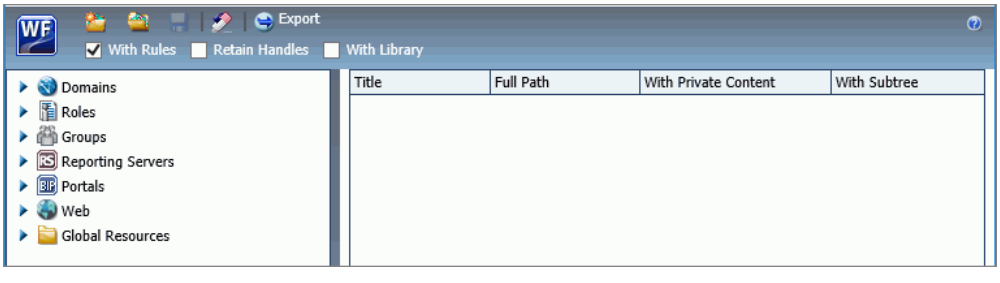
下図のように、WebFOCUS ホームページのバナーで [ユーティリティ] メニューを開き、[変更管理]、[エクスポート] を順に選択して [シナリオ] ダイアログボックスを開きます。



2. 下図のように、[新規シナリオ] を選択して [新規シナリオ] ダイアログボックスを開きます。



3. 下図のように、[新規シナリオ] ダイアログボックスにシナリオの名前を入力し、[作成] を選択して [シナリオ] ダイアログボックスを開きます。



デフォルト設定では、[ルールを含める] のチェックはオンになっています。選択したリソースに関連付けられたルールを変更管理パッケージに含めない場合にのみ、このチェックをオフにします。

注意：ブラウザでポップアップウィンドウがブロックされたことを示す警告が表示された場合は、この Web サイトからのポップアップウィンドウをすべて許可するようブラウザ設定を変更した上で再実行します。

4. 別の環境に移動するコラボレーションポータルページを右クリックし、[サブツリーを含めて選択] を選択します。
5. [保存] をクリックします。

   新しいシナリオのエントリが [エクスポート] ノード下に表示されます。

   新しいシナリオが表示されない場合は、[エクスポート] ノードを右クリックし、[リフレッシュ] を選択します。
6. 以降のトピックに記載されている手順に従って、変更管理パッケージの移動を完了します。

手順　変更管理シナリオダイアログボックスから新規変更管理シナリオを開くには

1. [変更管理 - シナリオ] ダイアログボックスのツールバーで、[新規シナリオの作成] をクリックします。
2. これまでに加えた変更を保存するかどうかを確認するメッセージが表示された場合は、[はい] をクリックします。
3. 新しいシナリオの名前を入力し、[OK] をクリックします。

   新しい [変更管理 - シナリオ] ダイアログボックスが開きます。現在の [変更管理 - シナリオ] ダイアログボックスは開いた状態で保持されます。
4. 新しいシナリオを作成します。詳細は、504 ページの 「 変更管理機能を使用してシナリオを作成するには 」 を参照してください。

手順　変更管理シナリオダイアログボックスから既存の変更管理シナリオを開くには

1. [変更管理 - シナリオ] ダイアログボックスのツールバーで、[既存のシナリオを開く] をクリックします。
2. これまでに加えた変更を保存するかどうかを確認するメッセージが表示された場合は、[はい] をクリックします。
3. [シナリオを開く] ダイアログボックスで、既存のシナリオをダブルクリックするか、既存のシナリオを選択して [OK] をクリックします。

   選択したシナリオの [変更管理 - シナリオ] ダイアログボックスが開き、これまで表示されていた [変更管理 - シナリオ] ダイアログボックスが置き換えられます。

手順　変更管理機能を使用して保存済みシナリオをエクスポートするには

変更管理シナリオをエクスポートするには、そのシナリオを保存しておく必要があります。保存されていない変更管理シナリオをエクスポートすることはできません。

1. [変更管理 - シナリオ] ダイアログボックスのクイックアクセスツールバーで、[エクスポート] をクリックします。
2. 確認メッセージのダイアログボックスで [OK] をクリックします。

   リソースツリーの [変更管理] ノード下の [エクスポート] フォルダに新しいシナリオが表示されます。

   新しいシナリオが表示されない場合は、[エクスポート] ノードを右クリックし、[リフレッシュ] を選択します。

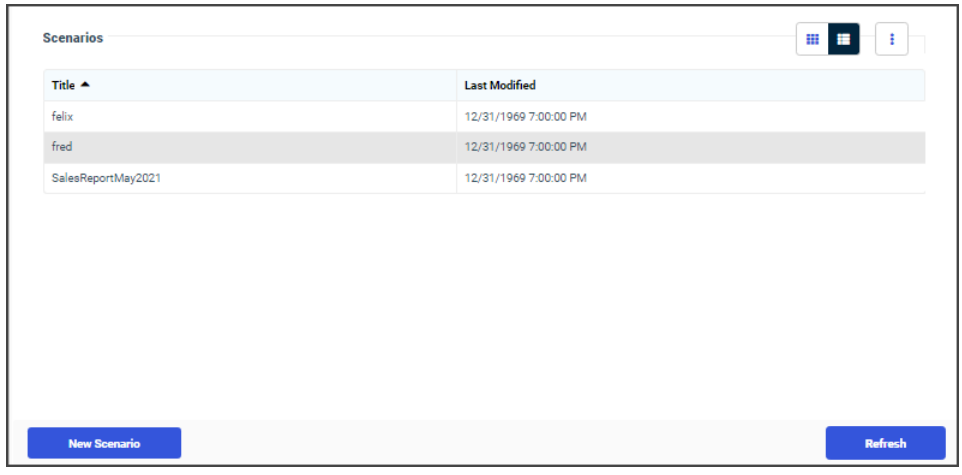
手順　変更管理パッケージ ZIP ファイルをダウンロードするには

エクスポートプロセスでは、変更管理 ZIP ファイルが変更管理エクスポートディレクトリ (*drive*:¥ibi¥*context*¥cm¥export) に保存されます。この場合の *context* は、ibi ルートディレクトリと変更管理ディレクトリの間にあるフォルダを表します。ダウンロードプロセスでは、その変更管理 ZIP ファイルが取得され、ユーザのローカルマシンにダウンロードされます。ダウンロードした変更管理パッケージ ZIP ファイルのコピーを別の WebFOCUS 環境に移動して、変更管理インポートパッケージとして使用することができます。

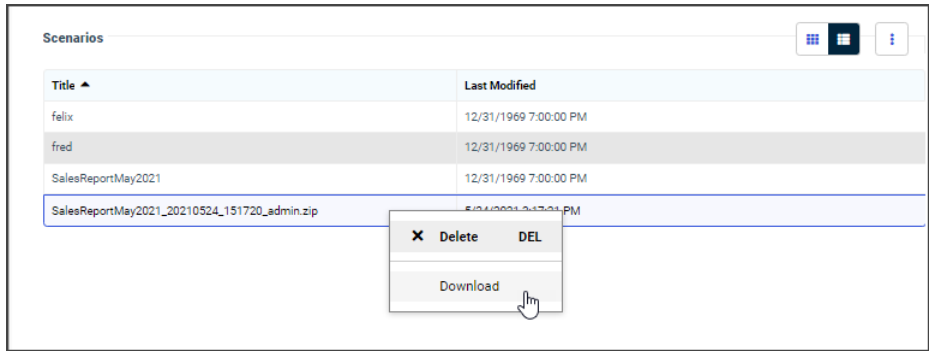
1. WebFOCUS Hub のサイドナビゲーションウィンドウから、[管理センター]、[パッケージのエクスポート] を順に選択します。

   または

   下図のように、WebFOCUS ホームページのバナーで [ユーティリティ] メニューを開き、[変更管理]、[エクスポート] を順に選択して [シナリオ] ダイアログボックスを開きます。



2. 下図のように、ダウンロードする変更管理 ZIP ファイルを右クリックし、[ダウンロード] を選択します。



注意：同一名を含む 2 つのリストエントリ間で選択する場合、完全な変更管理パッケージと ZIP ファイルバージョンを区別する際は、ZIP ファイルに割り当てられた名前には取得元の変更管理パッケージの名前、パッケージの作成日時、作成者のユーザ ID が含まれることを覚えておきます。完全な変更管理パッケージに割り当てられた名前には、このような詳細は含まれません。

3. ブラウザの指示に従って、ZIP ファイルを外部の場所に保存します。
4. [シナリオ] ダイアログボックスを閉じます。

参照　変更管理オプションの理解

[シナリオの作成] ダイアログボックスには、次のエクスポートオプションが表示されます。

ルールを含める　このオプションは、デフォルト設定で選択されています。このオプションを選択すると、オプションがシナリオ全体に適用され、選択したリソースすべてに関連付けられたルールがすべてエクスポートされます。これには、これらのルールのセキュリティコンポーネントがすべて含まれます。セキュリティコンポーネントは、グループ、ロール、およびユーザ (ルールの対象がユーザの場合) です。たとえば、[Sales] という公開済みフォルダを選択し、Sales/Dev グループにそのフォルダに対するルールが適用されている場合、[Sales] フォルダがエクスポートされるだけでなく、そのフォルダおよびサブフォルダに対して適用されているルールのコンポーネントもすべてエクスポートされます。

ハンドルの保持　このオプションは、変更管理機能を使用してコンテンツを移動する場合 (例、WebFOCUS バージョン 7.7 からマイグレートされたコンテンツ)、および ReportCaster スケジュールを移動する場合に必要です。このオプションを選択すると、変更管理パッケージでバージョン 7.7 の href がバージョン 8 のハンドルとして使用されます。また、WebFOCUS バージョン 7.7 で作成された ReportCaster スケジュールは内部ハンドルを使用してプロシジャを参照しますが、この内部ハンドルも継続して機能します。これにより、-INCLUDE およびドリルダウンの以前のコードが、バージョン 7.7 のスタイル構文で引き続き機能するようになります。WebFOCUS バージョン 8 で作成された ReportCaster スケジュールは、ハンドルを使用する代わりにスケジュールオブジェクトの IBFS を使用するため、[ハンドルの保持] 機能は必要ありません。

[ハンドルの保持] のデフォルト値は、管理コンソールの [ハンドルを保持する] (IBI_CM_Retain_Handles) 設定で指定します。

移動可能なリソースには次のタイプがあります。

- /WFC/Repository に格納されている任意のフォルダまたは項目。つまり、ユーザインターフェースに [コンテンツ] として表示される、プロシジャ、スタイルシート、イメージ、HTML ファイル、スケジュール、アクセスリスト、配信リストのすべてが含まれます。
- 任意のグループまたはサブグループ。グループを移動しても、ユーザ/グループメンバーシップは移動されません。また、親グループを移動せずに、サブグループのみを移動することができます。
- ツリー上の WebFOCUS Reporting Server ノードの任意のアプリケーションまたは特定のファイル。ツリー上に表示され、エクスポートの対象として選択可能なサーバコンテンツは、[エクスポートパッケージに含めるファイルタイプ] (IBI_CM_Export_WFRS_File_Extensions) 設定で指定します。この値を更新して、デフォルトリストに含まれていないファイル拡張子を追加することができます。この設定は、パフォーマンスの観点から、大規模データファイルではなく、アプリケーションコンテンツのみを対象にしています。大規模データファイルの移動が必要な場合は、それらのファイルをソース環境からターゲット環境へコピーすることをお勧めします。

❑ BI Portal

ReportLibrary を含める このチェックをオンにすると、変更管理エクスポートシナリオの対象として選択したすべてのフォルダ内の ReportLibrary コンテンツがエクスポートシナリオに追加されます。このチェックをオフにすると、選択したフォルダ内の ReportLibrary コンテンツがエクスポートシナリオに追加されません。このチェックがオフの場合でも、ReportLibrary を個別に選択してシナリオに追加することができます。デフォルト設定では、このチェックはオフになっています。

ReportLibrary は、ReportCaster で配信されるレポートを格納するセキュアな機能です。ReportLibrary についての詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』を参照してください。

手順 コマンドラインで変更管理エクスポートシナリオを実行するには

シナリオの作成が完了すると、そのシナリオをエクスポートすることができます。シナリオのエクスポートは、変更管理ユーザインターフェースを使用しても、cm_export スクリプトのいずれかを実行する自動プロセスでも行えます。このスクリプトは、drive:¥ibi¥context¥utilities¥cm ディレクトリに格納されています。この場合の context は、ibi ルートディレクトリと変更管理ディレクトリの間のフォルダを表します。

事前に、cm_export スクリプトの ENCODING パラメータの値で指定されたコードページと、Application Server に割り当てられたエンコード値が一致していることを確認する必要があります。一致しない場合、16 進数値が x7F より大きい文字がエクスポート時に破損する可能性があります。

[シナリオの作成] ダイアログボックスからシナリオをエクスポートするには、リソースツリーで保存済みシナリオを選択し、[エクスポート] をクリックします。

cm_export スクリプトによる自動プロセスでシナリオをエクスポートするには、次の手順を実行します。

1. 変更管理エクスポートユーティリティを格納するディレクトリ (通常は、*drive*:¥ibi¥*context*¥utilities¥cm。この場合の *context* は、ibi ルートディレクトリと変更管理ディレクトリの間のフォルダ) に移動し、cm_export.bat (Windows) または cm_export.sh (UNIX) をダブルクリックします。
2. 最初のプロンプトでシナリオのエクスポート権限を所有する管理者のユーザ ID を入力し、次のプロンプトでその管理者 ID のパスワードを入力します。
3. プロンプトに従って、エクスポートする変更管理パッケージの名前を入力します。

   ユーティティにこのジョブの関連するパラメータが表示され、エクスポートが実行されます。

4. プロンプトに従って任意のキーを押します。

   [コマンドプロンプト] ウィンドウが閉じ、エクスポートプロセスが完了します。

エクスポートを実行する別の方法として、次のパラメータ名の値が格納されたコマンドファイルを作成することもできます。

USERNAME WebFOCUS 管理者 ID です。

PASSWORD WebFOCUS 管理者 ID のパスワードです。トラステッド認証方法を使用する場合、パスワードはブランクにします。

EXPORTTO エクスポートフォルダの名前、またはエクスポートパッケージの名前です。デフォルト名は export です。

LOGLEVEL オプションです。エクスポートのログレベルです。利用可能な値には、次のものがあります。

- **info** 情報メッセージのみを記録します。 デフォルトのログレベルは info です。
- **debug** 最大トレース情報を記録します。

ENCODING オプションです。Java ベースの文字エンコーディングをサポートする変更管理エクスポートシナリオで使用されるコードページを示す値です。16 進数値が x7F より大きい文字がエクスポート時に破損されることを回避するため、この値を Application Server に割り当てられたエンコード値と一致させる必要があります。このパラメータのデフォルト値は UTF-8 です。Application Server が別のエンコード値を使用する場合は、サーバで使用される値でこの値を置換する必要があります。Client コードページのリストおよび対応するエンコード値の名前については、cm_export.bat ファイルの REMARKS 属性を参照してください。

たとえば、次の変更管理エクスポートシナリオは、Windows オペレーティングシステム用に記述されたものです。シナリオ名は ACWorkspace で、USERNAME、PASSWORD、EXPORTTO パラメータおよび関連する値が含まれます。

```
C:¥ibi¥WebFOCUS82¥utilities¥cm>type cmbatch.bat
cm_export USERNAME=admin PASSWORD=admin EXPORTTO=ACWorkspace
C:¥ibi¥WebFOCUS82¥utilities¥cm>
```

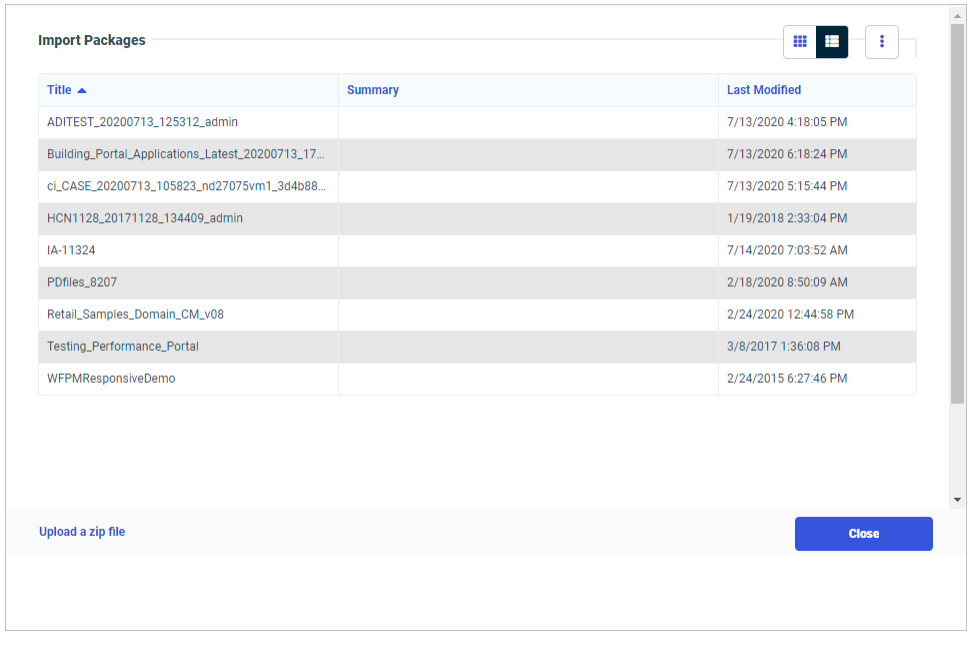
手順　変更管理パッケージ ZIP ファイルをアップロードするには

ZIP ファイルのアップロードプロセスでは、ローカルマシンに格納されている変更管理 ZIP ファイルのコピーが、サーバ上の変更管理インポートディレクトリ (*drive*:¥ibi¥*context*¥cm¥import) に保存されます。この場合の *context* は、ibi ルートディレクトリと変更管理ディレクトリ間のフォルダを表します。この変更管理 ZIP ファイルのコピーを WebFOCUS にインポートすることができます。

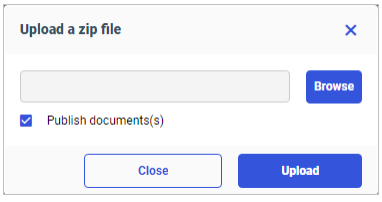
1. WebFOCUS Hub のサイドナビゲーションウィンドウから、[管理センター]、[パッケージのインポート] を順に選択します。

   または

   下図のように、WebFOCUS ホームページのバナーで [ユーティリティ] メニューを開き、[変更管理]、[インポート] を順に選択して [インポートパッケージ] ダイアログボックスを開きます。



2. 下図のように、[ZIP ファイルのアップロード] を選択して、[ZIP ファイルのアップロード] ダイアログボックスを開きます。



3. [ZIP ファイルのアップロード] ダイアログボックスで、[参照] ボタンをクリックし、変更管理パッケージの保存先ディレクトリに移動します。アップロードする変更管理 ZIP ファイルを選択し、[開く] をクリックします。
4. [アップロードするファイル] テキストボックスに変更管理 ZIP ファイルが正しく表示されていることを確認し、パッケージからインポートするファイルを公開するか、非公開にするかを指定します。
   - ❑ アップロード完了後に変更管理 ZIP ファイルのコンテンツを公開するには、[ドキュメントを公開] のチェックをオンにします。この設定がデフォルト値です。
   - ❑ アップロード完了後に変更管理 ZIP ファイルのコンテンツを公開しない場合は、[ドキュメントを公開] のチェックをオフにします。
5. [アップロード] をクリックします。

   確認ダイアログボックスが表示されます。[OK] をクリックしてアップロードを完了します。
6. ZIP ファイルが正常にアップロードされたことを確認するメッセージで [OK] をクリックし、アップロードを完了します。
7. [ZIP ファイルのアップロード] ダイアログボックスの [閉じる] をクリックします。

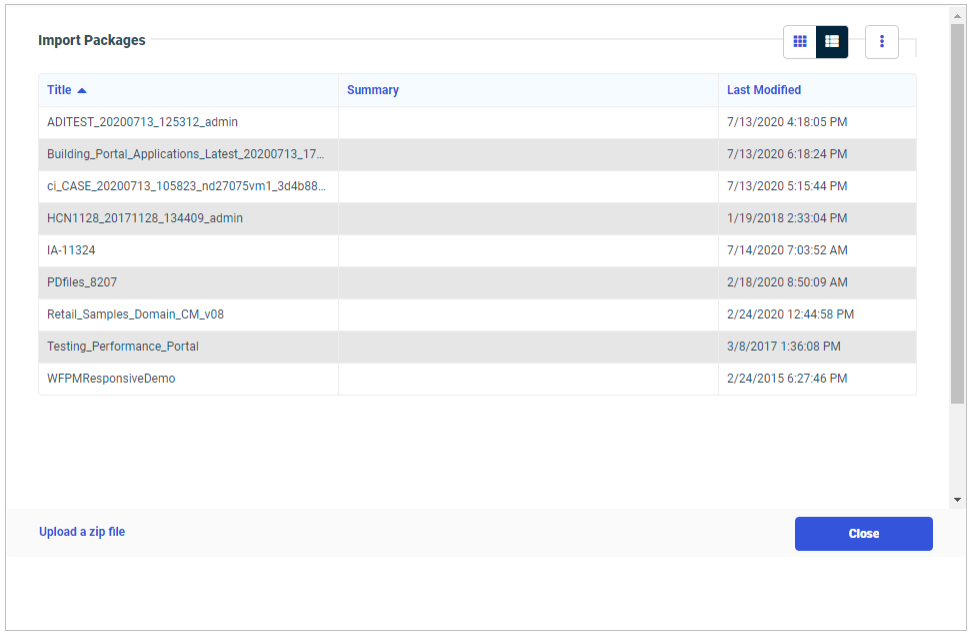
   変更管理 ZIP ファイルのエントリが [インポートパッケージ] ダイアログボックスのリストに表示されます。

手順　変更管理インポート機能を使用して変更管理パッケージをインポートするには

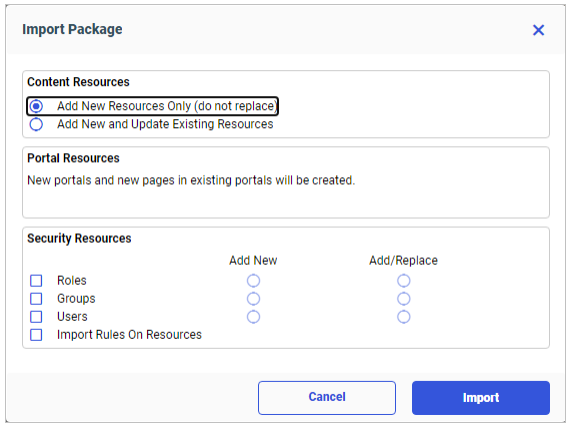
1. WebFOCUS Hub のサイドナビゲーションウィンドウから、[管理センター]、[パッケージのインポート] を順に選択します。

   または

下図のように、WebFOCUS ホームページのバナーで [ユーティリティ] メニューを開き、[変更管理]、[インポート] を順に選択して [インポートパッケージ] ダイアログボックスを開きます。



2. 下図のように、インポートする変更管理 ZIP ファイルを右クリックして [インポート] を選択し、[インポートパッケージ] ダイアログボックスを開きます。



3. [コンテンツリソース] グループで、変更管理インポートを新しいコンテンツリソースのみに制限するには、デフォルト値の [新規リソースの追加のみ (置換しない)] を受容します。

または

変更管理インポートに新しいコンテンツリソースとともに、既存コンテンツリソースの更新を含めるには、[新規リソースを追加して既存のリソースを更新] を選択します。

4. [セキュリティリソース] グループで、次のように選択します。
   a. [ロール] のチェックをオンにして、変更管理インポートパッケージにロールを含めます。
   b. [グループ] のチェックをオンにして、変更管理インポートパッケージにグループを含めます。
   c. [ユーザ] のチェックをオンにして、変更管理インポートパッケージにユーザを含めます。

      各セキュリティリソースで、変更管理インポートを新規セキュリティリソースのみに制限するには、デフォルト値の [追加] を受容します。

      または

      変更管理インポートに新しいセキュリティリソースとともに、既存セキュリティリソースの更新を含めるには、[追加/更新] を選択ます。

   d. [リソースのルールをインポート] のチェックをオンにして、変更管理インポートパッケージに追加するセキュリティリソースに割り当て済みのルールを含めます。
5. 構成の完了後、[インポート] をクリックします。

   インポートプロセスで変更管理パッケージからコンテンツがロードされ、古い環境で使用されていたフォルダの名前に正確に一致するフォルダに格納されます。変更管理パッケージに含めたリソースが古い環境と同一のフォルダに割り当てられている限り、インポートされたリソースが古い環境と同様に表示されます。

   ただし、予期した変更が確認されない場合は、リソースツリーの [ワークスペース] エントリを右クリックして [リフレッシュ] を選択します。

変更管理インポートオプションの理解

[インポートパッケージ] ダイアログボックスには、次のオプションが表示されます。

コンテンツリソース

このグループの各オプションを使用して、変更管理インポートに含めるコンテンツリソースの範囲を定義します。コンテンツリソースとして、リソースツリーの [ワークスペース] ノードおよび [ポータル] ノード下に存在するワークスペース、ポータル、レポート、グラフ、その他の機能があります。

新規リソースの追加のみ (置換しない) このオプションを選択すると、変更管理パッケージに含めたコンテンツリソースの中で、ターゲット環境に存在しないコンテンツリソースのみがインポートされます。インポートプロセスでは、インポートの結果として作成された新しいコンテンツリソースすべての [作成日] および [最終更新日] テキストボックスにインポート日時が割り当てられます。[作成日] および [最終更新日] テキストボックスの値を確認するには、項目を右クリックし、[プロパティ] を選択します。

変更管理パッケージに含めたリソースの中で、ターゲット環境にすでに存在するリソースはインポートから除外されます。その結果、ターゲット環境に存在するリソースはインポートの影響を受けず、[最終更新日] テキストボックスに割り当てられている値も更新されません。

新規リソースを追加して既存のリソースを更新 このオプションを選択すると、ターゲット環境に新しいリソースが追加されるとともに、既存のリソースが更新されます。インポートプロセスでは、インポートの結果として作成された新しいコンテンツリソースすべての [作成日] および [最終更新日] テキストボックスにインポート日時が割り当てられます。インポートによって更新された既存リソースすべての [最終更新日] テキストボックスにはインポート日時が割り当てられますが、[作成日] テキストボックスには元の値が保持されます。

セキュリティリソース

このグループの各オプションを使用して、変更管理パッケージにセキュリティリソース (ロール、グループ、ユーザ) が含まれている場合に実行するアクションを指定します。セキュリティリソースが変更管理パッケージに含まれる場合として、セキュリティリソース自体を明示的に選択した場合、または別のタイプのリソースで [ルールを含める] のチェックをオンにした場合があります。

ロール ユーザグループの権限です。変更管理インポートパッケージにロールを含めた場合、リポジトリで管理されているロールのリストにそのロールが追加 (または更新) され、そのロールがセキュリティセンターの [ロール] タブに表示されます。

グループ 類似した権限や同一リソースへのアクセスを必要とする複数のユーザまたはサブグループで構成された集合体です。変更管理インポートパッケージにグループを含めた場合、リポジトリで管理されている既存グループのリストにそのグループが追加 (または更新) され、そのグループがセキュリティセンターの [ユーザとグループ] タブに表示されます。

ユーザ WebFOCUS へのアクセス権限を所有する利用者です。変更管理インポートパッケージにユーザを含めた場合、リポジトリで管理されている既存ユーザのリストにそのユーザが追加 (または更新) され、そのユーザがセキュリティセンターの [ユーザとグループ] タブに表示されます。

セキュリティリソースのカテゴリごとに、インポートの範囲を定義するオプションが 2 つ表示されます。

- **追加** このオプションを選択すると、変更管理パッケージに含めたセキュリティリソースの中で、ターゲット環境に存在しないセキュリティリソースのみがインポートされます。
- **追加/置換** このオプションを選択すると、ターゲット環境に新しいセキュリティリソースが追加されるとともに、既存のセキュリティリソースが更新されます。

リソースのルールをインポート このオプションを使用して、現在の変更管理パッケージからルールをインポートするかどうかを指定します。このオプションは、変更管理パッケージにエクスポート済みルールが含まれている場合にのみ必要です。

セキュリティリソースのいずれのオプションも選択しない場合、ルールは、ターゲット環境に存在するルールのコンポーネントに基づいてインポートされます。

たとえば、[新規リソースの追加のみ (置換しない)] を選択し、[リソースのルールをインポート] のチェックをオンにした場合、インポートされるルールは、すべてのコンポーネント (グループ、ロール、ユーザ) がターゲット環境に存在するルールのみです。

別の例として、[新規リソースの追加のみ (置換しない)] を選択し、[リソースのルールをインポート] のチェックをオンにした上で [ロール (追加)] を選択すると、選択したリソースと、そのリソースに適用されているルールがインポートされます。この場合、ロールが追加されるのは、ロールがターゲット環境に存在せず、かつルールの他のコンポーネントがターゲット環境に存在する場合のみです。

手順　コマンドラインで変更管理インポートシナリオを実行するには

シナリオのインポートは、変更管理ユーザインターフェースを使用しても、cm_import スクリプトのいずれかを実行する自動プロセスでも行えます。このスクリプトは、drive:¥ibi¥context ¥utilities¥cm ディレクトリに格納されています。この場合の context は、ibi ルートディレクトリと変更管理ディレクトリの間のフォルダを表します。

事前に、cm_import スクリプトの ENCODING パラメータの値で指定されたコードページと、Application Server に割り当てられたエンコード値が一致していることを確認する必要があります。一致しない場合、16 進数値が x7F より大きい文字がインポート時に破損する可能性があります。

1. 変更管理インポートユーティリティを格納するディレクトリ (通常は、*drive*:¥ibi¥*context* ¥utilities¥cm。この場合の *context* は、ibi ルートディレクトリと変更管理ディレクトリの間のフォルダ) に移動し、cm_import.bat (Windows) または cm_import.sh (UNIX) をダブルクリックします。

2. 最初のプロンプトでシナリオのインポート権限を所有する管理者のユーザ ID を入力し、次のプロンプトでその管理者 ID のパスワードを入力します。
3. 次のプロンプトで、インポートパッケージの名前を入力します。
4. 次のプロンプトで、インポートするコンテンツリソースのタイプを選択します。次のオプションがあります。
   - **1 - 新規リソースの追加のみ (置換しない)。**これがデフォルト値です。
   - **2 - 新規リソースを追加して既存のリソースを更新**
   - **q - インポートプロセスを終了**
5. 次のプロンプトで、ロールをインポートする方法を選択します。次のオプションがあります。
   - **1 - ロールのインポートを省略**
   - **2 - ロールを追加**
   - **3 - ロールを追加/置換**
   - **q - インポートプロセスを終了**
6. 次のプロンプトでグループをインポートする方法を選択します。次のオプションがあります。
   - **1 - グループのインポートを省略**
   - **2 - グループを追加**
   - **3 - グループを追加/置換**
   - **q - インポートプロセスを終了**
7. 次のプロンプトで、ユーザをインポートする方法を選択します。次のオプションがあります。
   - **1 - ユーザのインポートを省略**
   - **2 - ユーザを追加**
   - **3 - ユーザを追加/置換**
   - **q - インポートプロセスを終了**
8. 次のプロンプトで、「このリソースのルール」をインポートするかどうかを選択します。次のオプションがあります。
   - **1 - いいえ**

- **2 - はい**
- **q - インポートプロセスを終了**

ユーティティにこのジョブの関連するパラメータが表示され、インポートが実行されます。

9. プロンプトに従って任意のキーを押します。

[コマンドプロンプト] ウィンドウが閉じ、インポートプロセスが完了します。

インポートを実行する別の方法として、次のパラメータ名の値が格納されたコマンドファイルを作成することもできます。

USERNAME WebFOCUS 管理者 ID です。

PASSWORD WebFOCUS 管理者 ID のパスワードです。

IMPORTFROM オプションです。インポートフォルダの名前、またはインポートパッケージの名前です。デフォルト名は export です。

LOGLEVEL オプションです。インポートのログレベルです。利用可能な値には、次のものがあります。

- **info** 情報メッセージのみを記録します。 デフォルトのログレベルは info です。
- **debug** 最大トレース情報を記録します。

ENCODING オプションです。Java ベースの文字エンコーディングをサポートする変更管理インポートシナリオで使用されるコードページを示す値です。16 進数値が x7F より大きい文字がインポート時に破損されることを回避するため、この値を Application Server に割り当てられたエンコード値と一致させる必要があります。このパラメータのデフォルト値は UTF-8 です。Application Server が別のエンコード値を使用する場合は、サーバで使用される値でこの値を置換する必要があります。Client コードページのリストおよび対応するエンコード値の名前については、cm_import.bat ファイルの REMARKS 属性を参照してください。

resOverwrite オプションです。コンテンツリソースをインポートするかどうかを指定します。デフォルト設定では、コンテンツリソースはインポートされません。

importRoles オプションです。ロールをインポートするかどうかを指定します。デフォルト設定では、ロールはインポートされません。

importGroups オプションです。グループをインポートするかどうかを指定します。デフォルト設定では、グループはインポートされません。

importUsers オプションです。ユーザをインポートするかどうかを指定します。デフォルト設定では、ユーザはインポートされません。

importRules オプションです。リソースに適用されているルールをインポートするかどうかを指定します。デフォルト設定では、ルールはインポートされません。

たとえば、次の変更管理インポートシナリオは、Windows オペレーティングシステム用に記述されたものです。シナリオ名は ACWorkspace で、USERNAME、PASSWORD、IMPORTFROM パラメータおよび関連する値が含まれます。

```
C:¥ibi¥WebFOCUS82¥utilities¥cm>type cmbatch.bat
cm_import USERNAME=admin PASSWORD=admin IMPORTFROM=ACWorkspace
C:¥ibi¥WebFOCUS82¥utilities¥cm>
```

A

構成設定

ここには、WebFOCUS Client の構成に使用されるファイルのリスト、および WebFOCUS 管理コンソールに表示される構成設定のリストが記載されています。

[構成] タブの各オプションを使用して、Web アプリケーションおよび WebFOCUS Client のさまざまなコンポーネントの構成を表示、編集することができます。

トピックス

TIBCO WebFOCUS Client 構成ファイル

WebFOCUS Client のインストール時に複数の構成ファイルが作成されます。そのうち、設定情報を含んだ構成ファイルを変更して、ユーザの環境に対応するよう WebFOCUS をカスタマイズすることができます。これらのファイルの多くは手動でカスタマイズすることができますが、設定を変更する場合は、管理コンソールを使用することをお勧めします。

注意：構成設定を更新する際は、ファイルを直接編集するのではなく、可能な限り管理コンソールを使用して更新することを強くお勧めします。管理コンソールを使用すると、パラメータ値が自動的に検証され、パスワードが暗号化されます。ただし、変更が推奨されない設定は、管理コンソールでは読み取り専用として表示されます。これらの設定は、ファイルを直接編集する必要があります。

下表は、管理コンソールでカスタマイズできる構成ファイルについての説明です。

インストールディレクトリパス	ファイル名	説明
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	install.cfg	WebFOCUS 構成設定ファイルです。このファイルには、初回の製品インストール時に選択された構成パラメータが記述されます。

インストールディレクトリパス	ファイル名	説明
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	securitysettings.xml	WebFOCUS の認証方法を指定します。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	securitysettings-mobile.xml	TIBCO WebFOCUS Mobile App などの WebFOCUS モバイル製品の認証方法を指定します。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	securitysettings-portlet.xml	SharePoint などの WebFOCUS Open Portal Services 製品の認証方法を指定します。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	securitysettings-zone.xml	必要に応じて、複数認証方法のゾーンを指定します。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	webfocus.cfg	WebFOCUS 構成設定ファイルです。このファイルには、デフォルトの構成設定に加えられたセキュリティ変更が記述されます。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	odin.cfg	WebFOCUS 通信ファイルです。このファイルは、WebFOCUS Client が接続可能な WebFOCUS Reporting Server を指定します。 詳細は、89 ページの 「 TIBCO WebFOCUS Reporting Server の設定 」を参照してください。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	mime.wfs	利用可能な MIME タイプの情報を格納します。
drive:¥ibi¥WebFOCUS82¥client¥wfc¥etc *install_directory*/ibi/WebFOCUS82/client/wfc/etc	site.wfs	WebFOCUS スクリプト処理に対してサイト固有の動作を定義します。

インストールディレクトリパス	ファイル名	説明
drive:¥ibi¥WebFOCUS82¥client¥wfc¥etc *install_directory*/ibi/WebFOCUS82/client/wfc/etc	nlscfg.err	国際言語サポート (NLS) の設定を格納します。 nlscfg.err ファイルについての詳細は、126 ページの 「 国際言語サポートを構成するには 」 を参照してください。
drive:¥ibi¥WebFOCUS82¥config *install_directory*/ibi/WebFOCUS82/config	languages.xml	言語の切り替え設定をカスタマイズします。 詳細は、128 ページの 「 言語の切り替えのカスタマイズ 」 を参照してください。

アプリケーションの設定

[アプリケーションの設定] では、WebFOCUS Web アプリケーションの構成および動作を設定します。

手順　アプリケーション設定を表示または編集するには

1. 管理コンソールの [構成] タブで [アプリケーションの設定] フォルダを展開し、表示または編集する設定のカテゴリを選択します。

   右側の構成ウィンドウに各種設定が表示されます。

2. 変更後、[保存] をクリックします。

参照　アプリケーションキャッシュの設定

[アプリケーションキャッシュ] ページの設定では、Application Server のデータ値キャッシュのサイズおよびコンテンツを構成します。これらのキャッシュは、オートプロンプトレポート、埋め込み BI アプリケーションで使用するパラメータ、または FIND パラメータ構文を含むプロシジャに割り当てられます。FIND パラメータ構文は、使用可能な検索パラメータ値の範囲を制限するために使用されます。

これらの設定では、ユーザ環境のデータ値キャッシュ操作のデフォルト構成を定義します。管理者およびセッションビューアの使用権限を所有するユーザは、[キャッシュ] リストのオプションを使用してこれらのデフォルト設定を一時的に上書きすることができます。

[アプリケーションキャッシュ] ページには、[レポート出力キャッシュ] の設定も含まれます。この設定では、レポート出力に別のキャッシュの使用を定義します。

データ値最大キャッシュメモリ (MB) (IBI_DATAVALUES_CACHE_MAXMEG)

データ値キャッシュに割り当てる最大メモリを定義します。このキャッシュには、プロシジャで発行されたクエリから WebFOCUS Reporting Server が取得したデータソース値が保持されます。プロシジャは、FIND パラメータ構文の 2 部構成名でマスターファイルのソースを識別します。これらの値は通常、オートプロンプトレポート、埋め込み BI アプリケーションで使用するパラメータ、または FIND パラメータ構文を含むプロシジャに割り当てられます。FIND パラメータ構文は、使用可能な検索パラメータ値の範囲を制限するために使用されます。また、マスターファイルへの IBFS パスおよびプロシジャを実行したユーザ ID もこのキャッシュに含まれます。データ値キャッシュは、WebFOCUS Application Server をホストするマシンのメモリを使用します。

この設定にはデフォルト値 0 (ゼロ) が割り当てられます。これは、データ値キャッシュに割り当てられるメモリがないこと、およびデータ値がキャッシュされていないことを示します。

データ値キャッシュの使用を有効にするには、管理者はこの設定に 1 から 500 までの数値を割り当てる必要があります。ほとんどの場合、組織のキャッシュ要件には 10 メガバイトで対応できます。

データ値ユーザキャッシュパス (IBI_DATAVALUES_CACHE_INCLUDEPATHS)

データを取得したユーザのみデータソース値の使用が可能なリソースへの IBFS パスを指定します。

この設定で定義するパスには、DBA または行レベルセキュリティの制限が適用されるデータを含むリソースのみを指定します。これらの制限が適用されないキャッシュリソースの呼び出しについては、[データ値グローバルキャッシュパス] (IBI_DATAVALUES_CACHE_GLOBALPATHS) 設定で定義されたパスが使用されます。

この設定で IBFS パスが定義されていない場合、データソース値はキャッシュされません。これがデフォルト値です。

この設定で 1 つまたは複数の IBFS パスが定義されている場合、これらのパスで定義されたすべてのリソースから取得されたデータ値が、各ユーザのデータ値ユーザキャッシュに含まれます。この設定に複数のパスを含める必要がある場合は、ブランクを使用せずセミコロン (;) で区切ります (例、/EDA/EDASERVE/retail_samples;/EDA/EDASERVE/ibisamp)。

この設定で定義するパスには、IBFS パスフォーマットを使用します。このフォーマットには、少なくとも IBFS サブシステムコンポーネント (/EDA) と WebFOCUS Reporting Server ノード名をこの順序で含める必要があります。比較的短い、上位のパスを使用した場合、幅広いフォルダおよびフォルダ内のマスターファイルが定義されます。下位レベルに及ぶ比較的長いパスを使用した場合、より狭い範囲のアプリケーションフォルダおよびマスターファイルが定義されます。パスは、個別のアプリケーションフォルダレベルまたは単一のマスターファイルレベルまで指定することができます。

この設定で複数のフォルダまたはマスターファイルを指定するには、幅広いフォルダを含む比較的短い、上位レベルのパスを使用することも、フォルダおよびマスターファイルの非常に特定されたグループを指定する一連のより長く、詳細なパスを指定することもできます。この設定に複数のパスを含める必要がある場合は、ブランクを使用せずセミコロン (;) で区切ります (例、/EDA/EDASERVE/retail_samples;/EDA/EDASERVE/ibisamp)。

この設定の IBFS パスには、次の構造を使用します。パスの先頭の 2 つのコンポーネントのみが必須です。残りのパスコンポーネントは、絞り込むパスの範囲に応じていくつでも追加することができます。

```
/EDA/Node/ApplicationFolder/SubFolder1 ... SubFolderN/Resource
```

説明

`EDA`
: EDA IBFS サブシステムです。このコンポーネントはすべてのパスで必須です。このコンポーネントには、先頭にスラッシュ (/) が必要です。

`Node`
: WebFOCUS Reporting Server ノードの名前です。このコンポーネントはすべてのパスで必須です。

`ApplicationFolder`
: データをデータ値キャッシュに追加するリソースが格納されたアプリケーションフォルダの名前です。

`SubFolder1 ... SubFolderN`
: アプリケーションフォルダ下のパスのフォルダ名です。パスのエンドポイントに接続します。必要な数のフォルダを追加します。

`Resource`
: パスのエンドポイントです。これが、1 つまたは複数のマスターファイルを格納するフォルダ名の場合、このフォルダのすべてのマスターファイルのデータがキャッシュに含まれます。ここで指定するマスターファイルの名前に拡張子.mas が付かない場合、この特定のマスターファイルのデータのみがキャッシュに含まれます。

注意：[データ値ユーザキャッシュパス] 設定で定義したフォルダまたはマスターファイルへのパスは、[データ値グローバルキャッシュパス] 設定で定義したパスに優先します。つまり、[データ値グローバルキャッシュパス] 設定と [データ値ユーザキャッシュパス] 設定で同一のパスが表示される場合は、このパスのマスターファイルから取得されたデータは、グローバルキャッシュではなくユーザセッションキャッシュに移動されます。

データ値グローバルユーザキャッシュパス (IBI_DATAVALUES_CACHE_GLOBALPATHS)
データソース値が、データ値グローバルキャッシュで制限なくすべてのユーザに使用可能なリソースへの IBFS パスを定義します。

この設定で定義するパスには、DBA または行レベルセキュリティの制限が適用されないデータを含むリソースのみを指定します。これらの制限が適用されるキャッシュリソースの呼び出しについては、[データ値ユーザキャッシュパス] (IBI_DATAVALUES_CACHE_INCLUDEPATHS) 設定で定義されたパスが使用されます。

この設定で IBFS パスが定義されていない場合、データソース値はデータ値グローバルキャッシュに含まれません。これがデフォルト値です。

この設定で 1 つまたは複数の IBFS パスが定義されている場合、これらのパスで定義されたリソースから取得されたデータ値が、データ値グローバルキャッシュに含まれます。

この設定で定義するパスには、IBFS パスフォーマットを使用します。このフォーマットには、少なくとも IBFS サブシステムコンポーネント (/EDA) と WebFOCUS Reporting Server ノード名をこの順序で含める必要があります。比較的短い、上位のパスを使用した場合、幅広いフォルダおよびフォルダ内のマスターファイルが定義されます。下位レベルに及ぶ比較的長いパスを使用した場合、より狭い範囲のアプリケーションフォルダおよびマスターファイルが定義されます。パスは、個別のアプリケーションフォルダレベルまたは単一のマスターファイルレベルまで指定することができます。

この設定で複数のフォルダまたはマスターファイルを指定するには、幅広いフォルダを含む比較的短い、上位レベルのパスを使用することも、フォルダおよびマスターファイルの非常に特定されたグループを指定する一連のより長く、詳細なパスを指定することもできます。この設定に複数のパスを含める必要がある場合は、ブランクを使用せずセミコロン (;) で区切ります (例、/EDA/EDASERVE/retail_samples;/EDA/EDASERVE/ibisamp)。

この設定の IBFS パスには、次の構造を使用します。パスの先頭の 2 つのコンポーネントのみが必須です。残りのパスコンポーネントは、絞り込むパスの範囲に応じていくつでも追加することができます。

```
/EDA/Node/ApplicationFolder/SubFolder1 ... SubFolderN/Resource
```

説明

`EDA`
EDA IBFS サブシステムです。このコンポーネントはすべてのパスで必須です。このコンポーネントには、先頭にスラッシュ (/) が必要です。

`Node`
WebFOCUS Reporting Server ノードの名前です。このコンポーネントはすべてのパスで必須です。

`ApplicationFolder`
データをデータ値キャッシュに追加するリソースが格納されたアプリケーションフォルダの名前です。

`SubFolder1 ... SubFolderN`
アプリケーションフォルダ下のパスのフォルダ名です。パスのエンドポイントに接続します。必要な数のフォルダを追加します。

`Resource`
パスのエンドポイントです。これが、1 つまたは複数のマスターファイルを格納するフォルダ名の場合、このフォルダのすべてのマスターファイルのデータがキャッシュに含まれます。ここで指定するマスターファイルの名前に拡張子.mas が付かない場合、この特定のマスターファイルのデータのみがキャッシュに含まれます。

データ値除外キャッシュパス (IBI_DATAVALUES_CACHE_EXCLUDEPATHS)

[データ値グローバルキャッシュパス] 設定または [データ値ユーザキャッシュパス] 設定で定義されたパスのうち、データ値をこれらのキャッシュから除外する必要のあるフォルダまたはマスターファイルへの IBFS パスを指定します。

この設定で IBFS パスが定義されていない場合、[データ値グローバルキャッシュパス] (IBI_DATAVALUES_CACHE_GLOBALPATHS) 設定または [データ値ユーザキャッシュパス] (IBI_DATAVALUES_CACHE_INCLUDEPATHS) 設定のパスで定義された各リソースまたはフォルダからデータ値が除外されません。これがデフォルト値です。

この設定で 1 つまたは複数の IBFS パスが定義されている場合、これらのパスで定義された各リソースまたはフォルダのデータ値が、グローバルデータ値キャッシュおよび各ユーザのセッションキャッシュから除外されます。この場合、データ値は、格納するフォルダまたはディレクトリがキャッシュの対象であっても除外されます。

この設定で定義するパスには、IBFS パスフォーマットを使用します。このフォーマットには、少なくとも IBFS サブシステムコンポーネント (/EDA) と WebFOCUS Reporting Server ノード名をこの順序で含める必要があります。比較的短い、上位のパスを使用した場合、幅広いフォルダおよびフォルダ内のマスターファイルが定義されます。下位レベルに及ぶ比較的長いパスを使用した場合、より狭い範囲のアプリケーションフォルダおよびマスターファイルが定義されます。パスは、個別のアプリケーションフォルダレベルまたは単一のマスターファイルレベルまで指定することができます。通常、この設定では、他のデータキャッシュ設定で定義されたパスから除外する個別のフォルダまたはマスターファイルを特定するため、比較的長い、より詳細なパスが必要です。

この設定に複数のパスを含める必要がある場合は、ブランクを使用せずセミコロン (;) で区切ります (例、/EDA/EDASERVE/retail_samples;/EDA/EDASERVE/ibisamp)。

この設定の IBFS パスには、次の構造を使用します。パスの先頭の 2 つのコンポーネントのみが必須です。残りのコンポーネントを使用して、パスを絞り込むことができます。

```
/EDA/Node/ApplicationFolder/SubFolder1 ... SubFolderN/ResourceFolder/
Resource
```

説明

`EDA`
: EDA IBFS サブシステムです。このコンポーネントはすべてのパスで必須です。このコンポーネントには、先頭にスラッシュ (/) が必要です。

`Node`
: WebFOCUS Reporting Server ノードの名前です。このコンポーネントはすべてのパスで必須です。

`ApplicationFolder`
: データをデータ値キャッシュから除外するリソースを格納するアプリケーションフォルダの名前です。

`SubFolder1 ... SubFolderN`
: アプリケーションフォルダ下のフォルダの名前です。パスのエンドポイントに接続します。必要な数のフォルダを追加します。

`Resource`
: パスのエンドポイントです。これが、1 つまたは複数のマスターファイルを格納するフォルダ名の場合、このフォルダのすべてのマスターファイルのデータがキャッシュから除外されます。ここで指定するマスターファイルの名前に拡張子.mas が付かない場合、この特定のマスターファイルのデータのみがキャッシュから除外されます。

レポート出力キャッシュ (IBI_REPORT_CACHE_ENABLE)

レポート出力をキャッシュするかどうかを指定します。次の値が使用できます。

- **オフ** レポート出力はキャッシュされません。これがデフォルト値です。
- **オン** レポート出力がキャッシュされます。
- **HIDDEN** レポート出力がキャッシュされます。

レポート出力は、レポートまたはグラフのプロシジャに対して WebFOCUS Reporting Server から取得される情報で、データ値、列タイトル、フォーマット設定が含まれます。

注意：[レポート出力キャッシュのルール名] テキストボックスには、レポート出力のキャッシュ方法を制御するルールを指定する文字列が表示されます。これらのルールは、キャッシュがすべてのユーザに適用されるか、データをリクエストしたユーザにのみ適用されるか、ユーザが割り当てられたグループのメンバーで共有されるかどうかを決定します。

手順 データ値キャッシュを構成するには

1. 管理者としてログインし、管理コンソールを起動します。
2. [構成] タブの [アプリケーションの設定] フォルダ下で、[アプリケーションキャッシュ] をクリックして [アプリケーションキャッシュ] ページを開きます。
3. [データ値最大キャッシュメモリ (MB)] (IBI_DATAVALUES_CACHE_MAXMEG) 設定で、データ値キャッシュに割り当てる Application Server メモリをメガバイト数で入力します。0 から 500 の値を指定する必要があります。
4. [データ値ユーザキャッシュパス] (IBI_DATAVALUES_CACHE_INCLUDEPATHS) 設定で、リクエストしたユーザに割り当てられた個別キャッシュにのみ含めることができ、他のユーザに使用不可能なデータが格納されたすべてのリソースへのパスを入力します。

   注意：この設定または次の設定に複数のパスを入力する必要がある場合、パスの末尾にはセミコロン (;) を使用し、パスとパスの間にブランクは使用しません。
5. [データ値グローバルキャッシュパス] (IBI_DATAVALUES_CACHE_GLOBALPATHS) 設定で、グローバルキャッシュに含めることができ、すべてのユーザに使用可能なデータが格納されたすべてのリソースへのパスを入力します。
6. [データ値グローバルキャッシュパス] 設定または [データ値ユーザキャッシュパス] 設定のいずれかで指定したパス内に、データ値キャッシュから除外する必要があるフォルダまたはマスターファイルが存在する場合は、これらのパスを [データ値除外キャッシュパス] (IBI_DATAVALUES_CACHE_EXCLUDEPATHS) 設定に入力します。

   この手順はオプションです。通常は、データ値キャッシュの構成手順に含まれません。
7. [保存] をクリックします。

変更が即時有効になります。[キャッシュのクリア] はクリックしないでください。

参照　アプリケーションコンテキストの設定

[アプリケーションコンテキスト] 設定では、さまざまな WebFOCUS コンポーネントのコンテキストルートパスを定義します。

ヘルプ (IBI_HELP_CONTEXT)

ローカルオンラインヘルプ Web アプリケーションのコンテキストルートを指定します。

デフォルト値は /ibi_help です。この値は、製品インストール中に設定され、デフォルト設定でローカルオンラインヘルプ Web アプリケーションに割り当てられたコンテキストルートが指定されています。

ローカルオンラインヘルプ Web アプリケーションを WebFOCUS コンテキストルートに割り当てるには、デフォルト値を新しい値 (WebFOCUS コンテキストで始まり、次にヘルプコンテキストが続く値) に置き換えます。たとえば、「/ibi_apps/ibi_help」と指定します。

オンラインヘルプ Web アプリケーションを別のコンテキストルートに割り当てるには、デフォルト値を新しい値 (社内で使用中のコンテキストルートを識別する値) に置き換えます。

この設定で定義したコンテキストルートは、ローカルホストにのみ適用されます。[ヘルププロキシホストとポート] (IBI_HELP_PROXY_HOST) 設定で外部サーバ名とポートを指定した場合は、その外部サーバのコンテキストルートを [ヘルププロキシコンテキスト] (IBI_HELP_PROXY_CONTEXT) 設定で指定する必要があります。

ヘルププロキシホストとポート (IBI_HELP_PROXY_HOST)

リモートオンラインヘルプ Web アプリケーションがインストールされている外部サーバの名前とポート番号を指定します。

この設定がブランクの場合、リモートオンラインヘルプ Web アプリケーションは使用できません。これがデフォルト値です。

この設定にサーバ名とポート番号を入力した場合、指定されたサーバ名とポート番号のサーバ上でリモートオンラインヘルプ Web アプリケーションが使用可能になります。リモートアプリケーションは、WebFOCUS Web アプリケーションと同一のサーバに存在する必要はありません。

この設定で値を指定した場合は、[ヘルププロキシコンテキスト] (IBI_HELP_PROXY_CONTEXT) 設定でも値を指定する必要があります。この設定をブランクにすることはできません。

これらの 2 つの設定に値を割り当てることでリモートオンラインヘルプ Web アプリケーションを指定した場合、Help Servlet がプロキシとして機能し、この設定で指定されたホストにヘルプシステムコールを転送します。設定の名前に「ヘルププロキシ」という語句が使用されている場合、その設定値がリモートオンラインヘルプ Web アプリケーションに適用されることを示しています。

ヘルププロキシコンテキスト (IBI_HELP_PROXY_CONTEXT)

[ヘルププロキシホストとポート] (IBI_HELP_PROXY_HOST) 設定で指定されたターゲット環境に存在するリモートオンラインヘルプ Web アプリケーションのコンテキストルートを指定します。

[ヘルププロキシホストとポート] (IBI_HELP_PROXY_HOST) 設定でリモートオンラインヘルプ Web アプリケーションが指定されていない場合、この設定はブランクにする必要があります。この設定がブランクの場合、リモートオンラインヘルプ Web アプリケーションのコンテキストルートは識別されません。これがデフォルト値です。

[ヘルププロキシホストとポート] (IBI_HELP_PROXY_HOST) 設定でリモートオンラインヘルプ Web アプリケーションが指定されている場合、この設定でコンテキストルートを指定する必要があります。

ヘルププロキシセキュア (IBI_HELP_PROXY_SECURE)

このチェックをオンにすると、WebFOCUS Client からリモートオンラインヘルプ Web アプリケーション ([ヘルププロキシホストとポート] (IBI_HELP_PROXY_HOST) 設定で指定) に転送されたコールすべてに SSL セキュリティが使用されます。

このチェックをオフにすると、リモートオンラインヘルプ Web アプリケーションの呼び出しに SSL セキュリティおよび暗号化は使用されません。これがデフォルト値です。

注意 : この設定は、WebFOCUS または他のアプリケーションからローカルサーバ上のヘルプシステムを呼び出す際には影響しません。顧客向けアプリケーションはすべて、セキュリティポリシーに従ってデフォルト設定で SSL が有効になっています。ただし、WebFOCUS Client がローカルイントラネットサーバ上のヘルプシステムにアクセスするよう構成され、そのイントラネットサーバ上のヘルプシステムが SSL を使用するよう構成されている場合は、この設定を選択する必要があります。

ReportCaster アプリケーション (IBI_REPORTCASTER_CONTEXT)

ReportCaster のコンテキストルートを指定します。以前のバージョンのデフォルト値は「/raster」です。現在のバージョンのデフォルト値は「/ibi_apps」です。

TIBCO WebFOCUS Servlet (IBI_WEBFOCUS_CONTEXT)
WebFOCUS Servlet のコンテキストルートを指定します。以前のバージョンのデフォルト値は「/ibi_apps」です。現在のバージョンのデフォルト値は「/ibi_apps/WFServlet.ibfs」です。

TIBCO WebFOCUS アプリケーション (IBI_WEBAPP_CONTEXT_DEFAULT)
WebFOCUS Web アプリケーションのコンテキストルートを指定します。デフォルト値は /ibi_apps です。

製品機能のデフォルトホストとポート (IBI_WEBAPP_DEFAULT_URL)
WebFOCUS インストールのデフォルト URL を指定します。

この値には次のフォーマットを使用します。

```
http(s)://host:port
```

説明

`host`
WebFOCUS へのアクセスに使用されるホストの名前または IP アドレスです。

`port`
Web サーバまたは Application Server が受信待機するポートの番号です。

この値は必要に応じて指定します。URL のポートが、そのスキームで使用されるプロトコルのデフォルトポートの場合、ポートを含める必要はありません。HTTP プロトコルを使用する URL の場合、デフォルトポートは 80、HTTPS プロトコルを使用する URL の場合、デフォルトポートは 443 です。

ホスト名およびポート番号は、製品インストール時に自動的にこの値に割り当てられ、ユーザの所属する組織で使用されるホスト名または IP アドレス、ポート番号が指定されます。製品コンポーネントは、この設定で定義された URL を使用して WebFOCUS にアクセスします。

参照　アプリケーションディレクトリの設定

[アプリケーションディレクトリ] 設定では、さまざまなファイルを格納するディレクトリを定義します。

APPROOT (IBI_APPROOT_DIRECTORY)
WebFOCUS で使用するアプリケーションネームスペースのルートディレクトリパスを指定します。デフォルトパスは、*drive* :¥ibi¥apps です (インストール時に別のディレクトリを指定しなかった場合)。

変更管理インポート (IBI_IMPORT_DIRECTORY)

変更管理インポートパッケージのインポート先ディレクトリのパスを指定します。デフォルトパスは、*drive*:¥ibi¥WebFOCUS82¥cm¥import です (インストール時に別のディレクトリを指定しなかった場合)。

変更管理エクスポート (IBI_EXPORT_DIRECTORY)

変更管理エクスポートパッケージの格納先ディレクトリのパスを指定します。デフォルトパスは、*drive*:¥ibi¥WebFOCUS82¥cm¥export です (インストール時に別のディレクトリを指定しなかった場合)。

ソースコードステージング領域ディレクトリ (IBI_SCM_STAGING_DIRECTORY)

ソース管理の操作時にファイルが移動されるディレクトリのパスを指定します。これらの操作には、ソース管理へのファイルの追加、ソース管理リポジトリへのファイルのチェックイン、リポジトリからのファイルのチェックアウトなどがあります。デフォルトパスは、*drive*:¥ibi¥webfocus82¥scm です。

このパスはカスタマイズすることができます。ディレクトリパスは、WebFOCUS がインストールされているマシンと同一のマシン上に存在する必要があります。現在、UNC パスはサポートされません。

一時ファイル (IBI_TEMPORARY_DIRECTORY)

リクエストを実行する際の一時ファイルのパスを指定します。たとえば、リダイレクトされたリクエストは、このパスに書き込まれます。デフォルトパスは、*drive*:¥ibi¥WebFOCUS82¥temp です (インストール時に別のディレクトリを指定しなかった場合)。

ログ削除までの日数 (IBI_LOG_RETAIN_DAYS)

logs ディレクトリ内にファイルを保持する日数を指定します。デフォルト値は、10 日間です。

トレース (IBI_TRACE_DIRECTORY)

セッションモニタおよびセッションビューアに表示される WebFOCUS Client トレースの格納先ディレクトリのパスを指定します。デフォルトパスは、*drive*:¥ibi¥WebFOCUS82¥traces です (インストール時に別のディレクトリを指定しなかった場合)。

機能診断のすべての出力は logs ディレクトリに格納されます。デフォルトパスは、*drive*:¥ibi¥WebFOCUS82¥logs です (インストール時に log4j2.xml file で指定)。

トレース削除までの日数 (IBI_TRACE_RETAIN_DAYS)

traces ディレクトリ内にファイルを保持する日数を指定します。デフォルト値は、10 日間です。

参照　BI Portal の設定

[BI Portal] 設定では、ポータルの表示および動作を構成します。

リダイレクト /ibi_apps 先

デフォルトホームページを指定します。

この設定の「/ibi_apps」は、主要エイリアスまたはコンテキストを表し、すべての WebFOCUS Web ページのパスがこの後に続きます。ほとんどの環境ではこれが一般的なコンテキストですが、ローカル WebFOCUS 環境によっては別のコンテキストが使用される場合があります。その場合、インストールで使用する名前がこの設定のラベルに表示されます。

注意：主要エイリアスまたはコンテキストとして「/bi」という用語を使用しないでください。これは予約語であり、エイリアスまたはコンテキストとして使用すると、管理コンソールおよびセキュリティセンターの正しい表示ができなくなります。

この設定では、次のいずれかのオプションを選択して、デフォルト設定のユーザのリダイレクト先を指定します。

- **新しい開始ページ**　このオプションを選択すると、ナビゲーションバーおよび関連メニューから WebFOCUS Client および WebFOCUS Reporting Server の表示に直接接続する WebFOCUS Hub が、デフォルトエントリページになります。これは、バージョン 8.2.07.28 以降のデフォルト設定です。
- **WebFOCUS ホームページ**　このオプションを選択すると、WebFOCUS バージョン 8.2.02 以降で実装された WebFOCUS ホームページがデフォルトホームページになります。
  - **バナーリンクにレガシーホームページオプションを表示**　[ユーザ] メニューに [レガシーホームページ] コマンドを表示するかどうかを制御します。このメニューは、WebFOCUS ホームページのユーザ名をクリックした際に開きます。このレガシーホームページは、WebFOCUS バージョン 8.2 SP 01 以降で実装されたホームページです。管理者が引き続き [リソーステンプレート] 機能を使用するには、レガシーホームページにアクセスする必要があります。
    - このチェックをオンにすると、[ユーザ] メニューに [レガシーホームページ] コマンドが表示されます。この設定がデフォルト値です。
    - このチェックをオフにすると、[ユーザ] メニューに [レガシーホームページ] コマンドは表示されません。このチェックをオフにした場合でも、ブラウザのアドレスバーに「/ibi_apps/legacyhome」と入力することでレガシーホームページを開くことができます。

- **レガシーホームページ**　このオプションを選択すると、バージョン 8.2 SP 01 で実装されたレガシーホームページがデフォルトホームページになります。このページを開くと、WebFOCUS ホームページに表示されない [グローバルリソース]、[リソーステンプレート]、[変更管理] 機能にアクセスすることができます。
- **カスタムようこそページ**　このオプションを選択すると、このオプション下側の [/ibi_apps/] テキストボックスで指定されたページがデフォルトホームページになります。一般にカスタムようこそページとしてポータルが使用されますが、この設定には、URL、レポート、またはプロシジャから生成される HTML ページを指定することもできます。

  このオプションを選択すると、カスタムようこそページを開いた際に、ブラウザのアドレスバーに基本コンテキストのみが表示されます。カスタムようこそページ URL のフルパスは表示されません。

  - **/ibi_apps/**　主要コンテキストまたはエイリアス下で、カスタムようこそページとして使用するコンテンツの URL を指定します。

    このテキストボックスには、カスタムようこそページ URL の、主要コンテキストまたはエイリアスに続く部分のみを入力します。このテキストボックスで指定したカスタムようこそページにユーザをリダイレクトする際に、このテキストボックスの値に主要コンテキストが自動的に追加され、URL のフルパスが生成されます。

    たとえば、カスタムようこそページにベーシックポータルを使用する場合、URL のフルパスは次のとおりです。

    ```
    Server01.ibi.com:8080/ibi_apps/bip/portal/Sales_Performance.
    ```

    [/ibi_apps/] テキストボックスには、次のように値を入力します。

    ```
    bip/portal/Sales_Performance.
    ```

    注意：ベーシックポータルは、製品のバージョンでサポートされ、[ベーシックポータル] オプションが有効な場合のみ使用できます。

    カスタムようこそページにコラボレーションポータルを使用する場合、URL のフルパスは次のとおりです。

    ```
    Server01.ibi.com:8080/ibi_apps/portal/sales_october/sales_october.
    ```

    [/ibi_apps/] テキストボックスには、次のように値を入力します。

    ```
    portal/sales_october/sales_october.
    ```

注意：コラボレーションポータルは、製品のバージョンでサポートされ、[コラボレーションポータル] オプションが有効な場合のみ使用できます。

カスタムようこそページとしてポータルホームページを使用する場合、[/ibi_apps/] テキストボックスには次のように値を入力します。

```
portals.
```

注意：ポータルホームページには、製品のバージョンで [ベーシックポータル] および [コラボレーションポータル] のポータルタイプがサポートされ、有効化されている場合のみ、ベーシックポータルまたはコラボレーションポータルが追加されます。

この設定の割り当て値に関係なく、ブラウザのアドレスバーに次の値のいずれかを入力することで、任意のホームページを開くことができます。

- この設定で定義されているデフォルトホームページを開くには、「/ibi_apps」と入力します。
- 新しい開始ページを開くには、「/ibia_apps/start」と入力します。
- WebFOCUS ホームページを開くには、「/ibi_apps/home」と入力します。
- レガシーホームページを開くには、「/ibi_apps/legacyhome」と入力します。
- ポータルホームページを開くには、「/ibi_apps/portals」と入力します。
- カスタムようこそページを開くには、「/ibi_apps/」に続いて、カスタムようこそページの残りのパスを入力します。

webfocus.cfg ファイルでは、[リダイレクト /ibi_apps 先] 設定は IBI_HOME_PAGE_CONFIGURATION 設定にマッピングされます。

- [WebFOCUS ホームページ] オプションを選択した場合、IBI_HOME_PAGE_CONFIGURATION=HOME に設定されます。
- [レガシーホームページ] オプションを選択した場合、IBI_HOME_PAGE_CONFIGURATION=LEGACY に設定されます。
- [カスタムようこそページ] オプションを選択した場合、IBI_HOME_PAGE_CONFIGURATION=CUSTOM に設定されます。
- [新しい開始ページ] オプションを選択した場合は IBI_HOME_PAGE_CONFIGURATION=DEFAULT に設定されますが、これがデフォルト値のため、webfocus.cfg ファイルには IBI_HOME_PAGE_CONFIGURATION 設定は表示されません。

webfocus.cfg ファイルでは、[バナーリンクにレガシーホームページを表示] チェックボックスは IBI_HOME_PAGE_LEGACY_LINKS 設定にマッピングされます。

- [バナーリンクにレガシーホームページを表示] のチェックをオンにした場合、IBI_HOME_PAGE_LEGACY_LINKS=TRUE に設定されます。
- このチェックをオフにした場合、IBI_HOME_PAGE_LEGACY_LINKS=FALSE に設定されます。

webfocus.cfg ファイルでは、[/ibi_apps/] テキストボックスは IBI_DEFAULT_WELCOME_PAGE 設定にマッピングされます。

デフォルトリストリポジトリパス (IBI_DYNAMIC_LIST_PATH)

WebFOCUS ホームページのホーム表示上部に配置されるカルーセルにタイトルおよびコンテンツが表示されるワークスペースの IBFS パスを定義します。

パス内の最後のフォルダと名前が一致するワークスペースが、IBFS ファイスシステムに存在する必要があります。対応するワークスペースが存在しない場合、またはワークスペースの名前がこのパス内の最後のフォルダの名前と一致しない場合は、接続が確立できず、カルーセルが表示されません。

IBFS:/WFC/Repository/Getting_Started パスは、この設定のデフォルト値です。このパスは、[開始] ワークスペースを指定し、カルーセルに [開始] のタイトルを割り当てます。このデフォルト値により、新規ユーザがアプリケーションを起動するとすぐにオリエンテーションリソースが表示されます。

統合インストールでは、[開始] ワークスペースが自動的にロードされます。また、クラウドインスタンスでもデフォルト設定で表示されます。WebFOCUS の他のインストールおよびインスタンスでは、この設定にデフォルトパスを割り当てても、このワークスペースはロードされません。これらのインストールには Getting_Started ワークスペースが存在しないため、この設定にパスが表示されていても、[開始] カルーセルは表示されません。

この設定のテキストボックスに 1 バイトのブランクが表示される場合、パスは定義されておらず、Getting_Started ワークスペースが使用可能な場合でも、[開始] カルーセルはホーム表示に表示されません。

そのため、デフォルト値を削除し、このテキストボックスに 1 バイトのブランクを入力して変更を保存すると、[開始] カルーセルを非表示にすることができます。変更後にログアウトし、再度ログインすると、[開始] カルーセルの代わりに [最近の更新] カルーセルが表示されます。WebFOCUS ホームページから管理コンソールを開いた場合、ブランクを入力することで、変更を保存後に管理コンソールを閉じる際に、管理コンソールによるデフォルトパスでの空のテキストボックスの上書きが回避されます。

この設定でテキストボックスに別のワークスペースのパスが表示される場合、カルーセルにはこの別のワークスペースのタイトルおよびこのワークスペースの最上位フォルダに格納されるリソースが表示されます。

このテキストボックスに別のワークスペースの IBFS パスを入力して変更を保存することで、[開始] ワークスペースの代わりに別のワークスペースを表示することができます。ログアウト後に再度ログインすると、[開始] カルーセルの代わりに別のワークスペースのタイトルとリソースを含むカルーセルが表示されます。

IBFS パスは、「IBFS:/WFC/Repository」で開始する必要があります。この後にスラッシュ (/) を入力し、続けて [開始] カルーセルに表示するリソースを格納する新しいワークスペースの名前を入力することができます。パス内のワークスペースおよびフォルダの区切り文字には、スラッシュ (/) を使用します (円記号 (¥) は使用しません)。別のワークスペースの [名前] に関連付けられた [タイトル] が、このカルーセルの新しいタイトルとして表示されます。IBFS パス内の最終フォルダ名は、大文字小文字の区別や綴りを含め、このワークスペースに割り当てられた [名前] ([タイトル] ではなく) と一致する必要があります。IBFS のフォーマット規則に準拠するためには、ワークスペースの [名前] に自動的に追加されたアンダースコア (_) やその他特殊文字はすべて最終フォルダの名前に含める必要があります。

このテキストボックスからすべての文字およびブランクを削除してページを保存することで、この設定のデフォルト値をいつでも復元することができます。ログアウト後に再度ログインすると、[開始] ワークスペースのデフォルトパスが、この設定に自動的に再度割り当てられます。

デフォルトワークスペースリポジトリパス (IBI_DEFAULT_WORKSPACE_PATH)

ホームページ、マイワークスペース表示、[開始] カルーセル、または定義済みワークスペース以外の場所から各ユーザが作成したデータ、ビジュアライゼーション、その他リソースへの接続のデフォルトパスとして使用するワークスペースの IBFS パスを定義します。

定義済みワークスペース以外で操作するユーザが [データの取得] ボタン、[ビジュアライゼーション] ボタン、またはプラス (+) ボタンのメニューオプションを選択すると、この設定で指定したワークスペースが、リポジトリ内の選択した操作の開始場所として機能し、新規コンテンツの最初の格納先として、デフォルト設定で [保存] ダイアログボックスに表示されます。

デフォルト設定で、この設定の値はブランクに設定され、マイワークスペース (IBFS:/WFC/Repository/MyWorkspace/) がデフォルトワークスペースリポジトリパスとして使用されます。このパスは、操作を開始する URL に自動的に割り当てられ、定義済みワークスペース以外の場所で作成された新規コンテンツの保存先フォルダパスとして、Workspaces > My Workspace > My Content パスが [保存] ダイアログボックスに表示されます。

このデフォルトパスは、別のワークスペースまたはリポジトリ内の最上位フォルダの IBFS パスで置換することができます。このパスは、操作を開始する URL に自動的に割り当てられ、定義済みワークスペース以外の場所で作成された新規コンテンツの保存先フォルダパスとして、Workspaces > My Workspace > My Content パスが [保存] ダイアログボックスに表示されます。ただし、コンテンツが定義済みワークスペースに割り当てられたデータ接続で作成される場合は除きます。

無効な IBFS パスまたは存在しないワークスペースのパスを入力すると、エラーメッセージが表示されます。パスは、ワークスペースまたは最上位フォルダにのみ指定できます。これより下位のパスには指定できません。

この設定の構成方法についての詳細は、550 ページの 「 デフォルトワークスペースリポジトリパスを構成するには 」 を参照してください。

注意

- 定義済みのフォルダまたはワークスペースで操作するユーザが、[データの取得] ボタン、[ビジュアライゼーション] ボタン、またはプラス (+) ボタンのメニューオプションを選択すると、これらの保存先のワークスペースまたはフォルダのパスがデフォルトワークスペースリポジトリパスになります。
- [データの取得] ボタン、[ビジュアライゼーション] ボタン、またはプラス (+) ボタンのメニューオプション選択時にユーザが操作する場所に関係なく、定義済みのワークスペースからデータソースを選択すると、選択したデータソースを格納するワークスペースのパスが、自動的にデフォルトワークスペースリポジトリパスになり、デフォルト設定で、このデータソースを格納するワークスペースに新規リソースを保存するよう要求されます。

ベーシックポータル (IBI_V3_PORTAL)

ベーシックポータルをサポートするかどうかを指定します。

ベーシックポータルは、[ポータル] ノード下で管理され、レポートやグラフなどのすべての機能が提供されるポータルです。

このチェックをオフ (False) にすると、リソースツリーに [ポータル] ノードは表示されず、ユーザはベーシックポータルを作成、編集、実行することはできません。ただし、以前に作成されたベーシックポータルのデータはリポジトリ内に残っているため、ユーザはブラウザのアドレスバーに URL を直接入力することで、以前に作成されたポータルを実行することができます。また、ユーザはベーシックポータルが含まれた変更管理パッケージのインポートも引き続き実行することができます。この設定がデフォルト値です。

このチェックをオン (True) にすると、リソースツリーに [ポータル] ノードが表示され、ユーザはベーシックポータルを作成、編集、実行することができます。

ベーシックポータルのデフォルトページレイアウト (IBI_V3_DEFAULT_LAYOUT)
ポータルで作成する新しいページのデフォルトレイアウトを設定します。

この設定は、製品のバージョンでコラボレーションポータルがサポートされ、[コラボレーションポータル] オプションが有効化されている場合のみ関係します。

この設定で定義されたデフォルト設定のレイアウトは、レポートやグラフなどの項目をページに配置する方法を指定します。[可変キャンバス] (デフォルト値) に設定すると、ページ上のコンテンツが自動的に均等配分され、項目を追加するたびに領域が再配分されます。[単一エリア] に設定すると、ページ上にグリッドは定義されず、ユーザは項目を任意の位置に配置することができます。

この設定は、ベーシックポータルにのみ関係します。コラボレーションポータルには関係しません。

コラボレーションポータル (IBI_V4_PORTAL)
コラボレーションポータルをサポートするかどうかを指定します。コラボレーションポータルは、V4 ポータルとも呼ばれます。

コラボレーションポータルは、レポートやグラフなど、ベーシックポータルで提供される機能をすべて備えています。また、コラボレーションポータルには、レスポンシブデザインのページテンプレートが付属しているほか、各ページを独立して作成、管理したり、ポータルやページに割り当て可能なブログ (インタラクティブメッセージコンポーネント) を作成、管理したりすることもできます。

この設定のチェックは、デフォルトでオフ (False) に設定されています。

このチェックがオフ (False) の場合、WebFOCUS ホームページでは、[ワークスペース] エリアのアクションバーの [その他] タブの [コラボレーションポータル]、[ポータルページ]、[ブログ] アクションボタン、およびレガシーホームページでは、[ワークスペース] フォルダのコンテキストメニューの [コラボレーションポータル]、[ポータルページ]、[ブログ] コマンドが、いずれのユーザタイプにも表示されません。

このチェックをオンにして作成したコラボレーションポータルは、Administrators、ワークスペースの Developers、およびこれらのコラボレーションポータルを格納するワークスペースのロールに [Delete Resource (opDelete)] 権限が含まれるその他のユーザが引き続き表示、使用することができます。作成済みのコラボレーションポータルを表示、実行、編集、削除する権限は、この設定のチェックをオフにした後に作成済みのコラボレーションポータルに基づいて DESIGNER ポータル (V5 ポータルとも呼ばれる) を作成する Administrators および Developers の作業をサポートします。

このチェックがオフの場合、ユーザは割り当てられたグループに従って次の権限が与えられます。

- **Basic Users** および **Advanced Users** のユーザは、コラボレーションポータルの表示または実行ができません。
- **Developers** はコラボレーションポータルの作成ができません。ただし、[WorkspaceDeveloper] ロールには [Delete Resources (opDelete)] 権限が含まれるため、割り当てられたワークスペース内の作成済みのコラボレーションポータルの表示、実行、編集、削除が行えます。この場合、コンテキストメニューのコマンドをクリックするか、これらの機能の URL をブラウザのアドレスバーに直接入力します。
- **Administrators** はコラボレーションポータルの作成ができません。ただし、[SystemFullControl] ロールには [Delete Resources (opDelete)] 権限が含まれるため、Administrators は、すべてのワークスペースの作成済みのコラボレーションポータル、ポータルページ、ブログの表示、実行、編集、削除が行えます。この場合、コンテキストメニューのコマンドをクリックするか、これらの機能の URL をブラウザのアドレスバーに直接入力します。また、作成済みのコラボレーションポータル、ポータルページ、ブログを含む変更管理パッケージのインポートおよびエクスポートを実行することができ、インポート後にこれらを表示、実行、編集、削除することもできます。
- **注意：**作成済みのコラボレーションポータルページおよびブログは引き続き表示することができますが、[Delete Resources (opDelete)] 権限を所有するユーザによる実行または編集はできなくなります。

このチェックがオン (True) の場合、WebFOCUS ホームページでは、[ワークスペース] エリアのアクションバーの [その他] タブの [コラボレーションポータル]、[ポータルページ]、[ブログ] アクションボタン、およびレガシーホームページでは、[ワークスペース] フォルダのコンテキストメニューの [コラボレーションポータル]、[ポータルページ]、[ブログ] コマンドが、任意のワークスペースを使用する管理者および割り当てられたワークスペースを使用する開発者に表示されます。

このチェックがオンの場合、ユーザは割り当てられたグループに従って次の権限が与えられます。

- **Basic Users** および **Advanced Users** のユーザは、使用が許可されたコラボレーションポータルを表示、実行することができます。
- **Developers** ユーザは、割り当てられたワークスペースのコラボレーションポータルを表示、実行することができます。また、割り当てられたワークスペースの既存のコラボレーションポータルの作成、編集、削除も可能です。

- **Administrators** ユーザは、すべてのワークスペースのコラボレーションポータルの表示、実行、作成、編集、削除が行えます。また、変更管理パッケージに含まれたコラボレーションポータルのエクスポート、インポートを実行することができ、インポート後にこれらを表示、実行、編集、削除することもできます。

最初のワークスペースを開く (IBI_BIP_OPEN_FIRST_DOMAIN)

BI Portal を起動した際に、リソースツリーに表示されたワークスペースリストの中で最初のワークスペースを自動的に展開された状態にするかどうかを指定します。このチェックをオン (True) にすると、BI Portal を起動した際に、最初のワークスペースが自動的に展開された状態で表示されます。このチェックをオフ (False) にすると、BI Portal を起動した際に、最初のワークスペースが閉じた状態で表示されます。デフォルト設定では、このチェックはオフになっています。

アップロード可能ファイルの拡張子 (IBI_UPLOAD_EXTENSIONS)

BI Portal にアップロード可能なファイルのタイプを指定します。この設定で指定されていない拡張子のファイルは BI Portal にアップロードできません。デフォルト設定では、次のファイル拡張子が指定されています。

.acx、.bmp、.css、.doc、.docx、.fex、.gif、.htm、.html、.ico、.jpe、.jpeg、.jpg、.js、.mas、.pdf、
.png、.ppt、.pptx、.sty、.svg、.txt、.xls、.xlsx、.xml、.zip、.ely

移動確認メッセージ (IBI_MOVE_CONFIRMATION_MESSAGE)

ユーザがドラッグアンドドロップ操作でフォルダを移動する際に確認を要求するかどうかを指定します。このチェックは、デフォルトでオン (True) に設定されています。

メッセージ詳細 (IBI_MESSAGE_DETAIL)

ユーザが簡易メッセージを受け取るレベルを指定します。簡易エラーメッセージでは、エラーの詳細を省略することで、機密情報や技術情報がエンドユーザに公開されることを回避することができます。簡易エラーメッセージがユーザに送信された際は、管理者のトラブルシューティング用として詳細なエラーメッセージが event.log ファイルに記録されます。event.log ファイルの各エラーメッセージには、IBFS-YYMMDD_hhmmss-n 形式の ID が先頭に付けられます。ここで、n は同一時刻 (秒) に生成された複数のメッセージに付けられる連続番号を表します。

ユーザに表示される簡易エラーメッセージには、event.log エントリ ID が含まれます。

[メッセージ詳細] リストの各オプションを選択して、エンドユーザが詳細メッセージを受け取る最上位のエラーレベルを指定します。次のオプションがあります。

- **重大** ユーザは、[重大] レベル以下のエラーで詳細メッセージを受け取ります。[重大] レベルは、最上位のエラーレベルです。この設定では、ユーザが簡易メッセージを受け取ることはありません。これがデフォルト値です。

- **エラー** ユーザは、[重大] レベルのエラーでは簡易メッセージ、[エラー] レベル以下のエラーでは詳細メッセージを受け取ります。
- **期待値** ユーザは、[重大] および [エラー] レベルのエラーでは簡易メッセージ、[期待値] レベル以下のエラーでは詳細メッセージを受け取ります。
- **なし** ユーザは、常に簡易エラーメッセージを受け取ります。

管理者は、簡易エラーメッセージのベースとなるカスタムテンプレートを作成、編集することで、メッセージのスタイルをカスタマイズすることができます。カスタムエラーメッセージテンプレートを作成するには、webfocus_ibfs_error.xml ファイルを prod ディレクトリから custom ディレクトリにコピーします。prod ディレクトリおよび custom ディレクトリは、*drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc ディレクトリ下にあります。custom ディレクトリにコピーした webfocus_ibfs_error.xml ファイルに変更を加えます。

注意: [Display Administration Console] (opWFAdminConsole) 権限または [Desktop Connect] (opDTConnect) 権限を所有するユーザは、常に詳細エラーメッセージを受け取ります。

ログインメッセージ (IBI_SIGNIN_MESSAGE)
ユーザがログインした際に [メッセージ] ダイアログボックスに表示されるカスタムメッセージを指定します。このテキストボックスには、テキストのみを入力することも、テキスト、リンク、イメージの HTML タグを入力することもできます。このテキストボックスをブランクのままにした場合 (これがデフォルト値)、[メッセージ] ダイアログボックスは表示されません。

ログインメッセージに使用可能な HTML タグには、次のものがあります。

<l>、
、<b>、<u>、<a href>、、<img>

ログインページのリンク (IBI_SIGNIN_PAGE_LINKS)
(現在、この項目の説明はありません)

カスタムログインページ (IBI_CUSTOMIZED_SIGNIN_PAGE)
ユーザへのカスタムログインページの表示を有効にします。デフォルト値は False です。

Mobile Favorites プロキシ URL (IBI_MOBILE_FAVORITES_PROXY_URL)
Mobile Favorites へのアクセスに使用する URL を指定します。ブランクにした場合、デフォルトの Mobile Favorites が使用されます。

セッション権限検索の深さ (IBI_SESSION_PRIVILEGE_SEARCH_DEPTH)

ユーザのログインプロセス中に行われる IBFS:/WFC/Repository サブシステム内のセッション権限検索の深さを定義します。確認するセッション権限をワークスペースフォルダのみに限定するには (例、IBFS:¥WFC¥Repository¥Sales)、検索の深さをデフォルト値の 1 に設定します。セッション権限をワークスペースフォルダ直下のサブフォルダまで検索するには、検索の深さを 2 に設定します。

注意：理論的には検索の深さを任意のレベルに設定できますが、実際には、検索の深さを大きくすると、パフォーマンスの問題が発生する場合があります。検索の深さは、可能な限り小さくすることを強く推奨します。

セッション権限についての詳細は、354 ページの「 セッション権限 」 を参照してください。

セッションタイムアウト (分) (IBI_SESSION_TIMEOUT)

有効な認証情報でログインしたユーザがアイドル状態を保持できる期間のセッションタイムアウト値を制御します。この制限時間を超えると、セッションタイムアウトになります。

この設定は分単位で定義され、デフォルト値として 120 (分) が割り当てられます。

この設定は、パブリックユーザ以外のすべてのユーザに適用されます。すべてのパブリックユーザのタイムアウト制限は、[パブリックセッションタイムアウト (分)] 設定で定義されます。

パブリックセッションタイムアウト (分) (IBI_PUBLIC_SESSION_TIMEOUT)

パブリックユーザがアイドル状態を保持できる期間のパブリックセッションタイムアウト値を制御します。この制限時間を超えると、セッションタイムアウトになります。

この設定は分単位で定義され、デフォルト値として 120 (分) が割り当てられます。

この設定は、パブリックユーザのみに適用されます。その他すべてのユーザのタイムアウト制限は、[セッションタイムアウト (分)] 設定で定義されます。パブリックユーザは、認証情報を提示せずにセッションを開始し、Anonymous グループで定義されたアクセス権限が与えられます。

最大同時パブリックセッション数 (IBI_CONCURRENT_PUBLIC_SESSION_LIMIT)

セッションを同時に開くことのできるパブリックユーザの最大数を定義します。パブリックユーザは、認証情報を提示せずにセッションを開始し、Anonymous グループで定義されたアクセス権限が与えられます。

この設定の値が 0 (ゼロ) の場合、パブリックユーザ数に上限は設定されません。この設定では、デフォルト値 0 (ゼロ) が割り当てられています。

この設定で値が定義された場合、制限に達した後に セッションの開始を試行したパブリックユーザには、警告メッセージが表示され、リクエストを完了することができません。

IBI_CONCURRENT_VISUALIZATION_LIMIT (IBI_CONCURRENT_VISUALIZATION_LIMIT)

単一ユーザが同時に開くことのできる、プロシジャまたはオートドリルダウン、Drill Anywhere、InfoMini、インサイトのリクエストから作成される WebFOCUS DESIGNER または InfoAssist ビジュアライゼーションの最大数を定義します。開いているビジュアライゼーションの数がこの最大数に達すると、新しいビジュアライゼーションを開く次のリクエストが完了せず、エラーメッセージが記録されます。

この設定の値は、デフォルトで 0 (ゼロ) に設定されています。これは、単一ユーザが同時に開くことのできるビジュアライゼーションの数に制限がないことを示します。この制限を設定するには、管理者は、同時に開くことのできるビジュアライゼーションの最大数を定義する値を入力する必要があります。

自動ログアウトを有効にする (IBI_AUTO_SIGNOFF)

アイドル状態が継続したためにセッションが期限切れとなり、保存されていない作業が失われることをユーザに知らせる警告メッセージの表示を有効にします。このチェックがオンの場合、ホームページ、セキュリティセンター、およびポータルに警告メッセージが表示されます。このチェックがオフの場合、警告メッセージは表示されません。デフォルト設定で、このチェックはオンになっています。

アイドルタイムアウトメッセージまでの期間 (分) (IBI_AUTO_SIGNOFF_MESSAGE_DURATION)

タイムアウト警告メッセージを表示する時間を分数で指定します。この値は、[自動ログアウトを有効にする] (IBI_AUTO_SIGNOFF) 設定のチェックをオンにした場合のみ関係します。デフォルト設定で、この値には 2 分が割り当てられています。

ホームページまたはセキュリティセンターに表示された場合、警告メッセージにはセッション期限切れまでの残り時間も表示されます。ポータルに表示された場合、警告メッセージには残り時間は表示されません。

埋め込みリソースバンドルを有効にする (IBI_ENABLE_INLINED_RESOURCE_BUNDLES)

この機能はオプションです。このチェックがオン (True) の場合、WebFOCUS ホームページおよび WebFOCUS DESIGNER ツールに必要な JavaScript とカスケードスタイルシートのリソースファイルのデータが、XML 埋め込みリソースバンドルファイルに統合されます。これにより、ネットワークが遅いシステムのパフォーマンスを改善することができます。このチェックがオフ (False) の場合、この機能は有効化されません。デフォルト設定では、このチェックはオフになっています。

Ajax タイムアウト (IBI_AJAX_TIMEOUT)

(現在、この項目の説明はありません)

手順　デフォルトワークスペースリポジトリパスを構成するには

デフォルトワークスペースリポジトリパスがブランクの場合、定義済みワークスペース以外で作成されたコンテンツはすべて、[マイワークスペース] (IBFS Path IBFS:/WFC/Repository/MyWorkspace/) に割り当てられます。以下の手順を使用して、定義済みワークスペース以外で作成された新規コンテンツのデフォルト保存先として使用する別のフォルダまたはワークスペースを割り当てます。

1. 管理者としてログインし、管理コンソールを開きます。
2. [構成] タブの [アプリケーションの設定] フォルダ下で、[BI Portal] をクリックして [BI Portal] ページを開きます。
3. [デフォルトワークスペースリポジトリパス] (IBI_DEFAULT_RESOURCE_PATH) 設定に、定義済みワークスペース以外で作成されたすべてのリソースのデフォルト保存先として使用するワークスペースまたは最上位フォルダのパスを入力します。

   入力した IBFS パスが無効または存在しないことを示すエラーメッセージが表示された場合、アドレスを再入力し、これが既存のワークスペースまたは最上位フォルダを指していることを確認します。
4. [保存] をクリックします。

   変更が即時有効になります。[キャッシュのクリア] をクリックする必要はありません。

参照　変更管理の設定

[変更管理] 設定では、変更管理プロセスでエクスポート可能なファイルタイプ、エクスポートファイル名のフォーマット、一部のレガシー機能を保持するかどうかを指定します。

注意：変更管理のエクスポートパッケージおよびインポートパッケージの格納先は、[アプリケーションディレクトリ] 設定で指定します。詳細は、536 ページの 「 アプリケーションディレクトリの設定 」 を参照してください。

エクスポートパッケージに含めるファイルタイプ (IBI_CM_EXPORT_WFRS_FILE_EXTENSIONS)

変更管理のエクスポート機能を使用する際に、WebFOCUS Reporting Server からエクスポートするファイルの拡張子を指定します。デフォルト設定で指定されているファイル拡張子は、acx、bmp、css、fex、gif、htm、html、ico、jpe、jpeg、jpg、js、mas、mnt、png、sty、svg です。

ハンドルを保持する (IBI_CM_RETAIN_HANDLES)

このオプションを選択すると (True)、エクスポートパッケージに元の href が含まれます。元の href は、変更管理を使用して、WebFOCUS バージョン 7 からマイグレートされたコンテンツを移動する場合、および WebFOCUS バージョン 8 の特定の環境からバージョン 8 の別の環境に ReportCaster スケジュールを移動する場合に必要になります。この設定により、WebFOCUS バージョン 7 からマイグレートされたコードの -INCLUDE およびドリルダウンが引き続き機能するようになります。また、ハンドルを使用してプロシジャを参照する ReportCaster スケジュールも引き続き機能します。デフォルト設定では、このチェックはオフ (False) になっています。

変更管理パッケージを圧縮 (IBI_CM_ZIP)

このチェックをオン (True) にすると、エクスポートパッケージが圧縮され、ZIP ファイルで保存されます。

ZIP エクスポートファイル名のフォーマット (IBI_CM_ZIP_FILE_FORMAT)

ドロップダウンリストからオプションを選択して、ZIP ファイルの名前フォーマットを指定します。

作成、更新、最終アクセス情報の保存 (IBI_CM_PRESERVE_SOURCE_INFO)

このチェックがオン (True) の場合 (デフォルト設定)、変更管理ユーティリティを使用して WebFOCUS インストールにインポートされたすべての項目について、次の情報が保存されます。

- **作成日時** 項目が最初に作成された日時、および作成したユーザ ID。
- **更新日時** 項目が変更管理エクスポートファイルに追加される前に最後に変更された日時、および変更したユーザ ID。
- **アクセス日時** コンテンツ項目が変更管理エクスポートファイルに追加される前に最後に使用された日時、および使用したユーザ ID。

これらの値は、[プロパティ] ダイアログボックスの [全般] タブに表示されます。

このチェックがオフ (False) の場合、変更管理インポートの日時およびこれを実行したユーザ ID でこれら元の値が上書きされ、変更管理ユーティリティを使用してインポートされた項目のこれら 3 つのプロパティすべてに割り当てられます。

参照

Client 設定

[Client 設定] では、さまざまな WebFOCUS Client オプションを構成します。

サイトプロファイル (IBI_SITE_PROFILE)

次の構文を使用して、WebFOCUS Client リクエストによって WebFOCUS Reporting Server 上で実行されるコードを含めることができます。

```
_site_profile=command
```

説明

`command`
任意の有効な WebFOCUS Reporting Server 構文です。サイトプロファイルは、WebFOCUS Reporting Server ログイン時、および ReportCaster でスケジュールされたプロシジャの実行時には処理されません。WebFOCUS Reporting Server でのプロシジャの実行時のみ処理されます。

サイトプロファイルは、*drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc¥site.wfs ファイルに直接追加することもできます。

ユニバーサルプロファイル (IBI_UNIVERSAL_PROFILE)

次の構文を使用して、WebFOCUS Client と ReportCaster Distribution Server の両方で実行されるコードを追加することができます。この点が _site_profile と異なります。_site_profile は、WebFOCUS Client リクエストによってのみ実行されます。

```
_universal_profile=command
```

説明

`command`
任意の有効な WebFOCUS Reporting Server 構文です。

_universal_profile には、WebFOCUS Client でのみ実行されるロジックやコンストラクトを含めないようにする必要があります。たとえば、HTTP ヘッダ変数は、WebFOCUS Client では使用できますが、ReportCaster Distribution Server では使用できないため、HTTP ヘッダ変数をユニバーサルプロファイルに追加することはできません。

ユニバーサルプロファイルは、*drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc¥site.wfs ファイルに直接追加することもできます。

一時ファイルのタイムアウト (IBI_TEMPFILETIMEOUT)

一時ディレクトリからファイルを削除します。指定した時間 (秒数) が経過した場合、それより前のファイルは削除されます。デフォルト値は 900 秒です。

TIBCO 言語 (IBI_LANG)

この設定は、UNIX のみに適用されます。サーバサイドグラフとともにレポート上に NLS 文字を表示するには、このパラメータに対して適切な UNIX ロケールエンコード (例、ja_JP) を設定しておく必要があります。

永続変数 (IBIF_PERSISTENTAMP)

&& 変数の永続機能をオンにします。デフォルト設定では、このチェックはオンになっています (True)。 この機能を無効にするには、このチェックをオフにします (False)。 && 変数の永続機能を使用すると、ブラウザセッションが終了するまで && 変数を永続化することができます。

デフォルト言語 (IBIWF_LANGUAGE)

言語の切り替え機能では、各セッションのデフォルトユーザインターフェース言語は、ブラウザの言語、または URL の IBIWF_language=*nn* パラメータで設定した言語で決定されます。ここで、*nn* は ISO の言語略名を表します。

ユーザのブラウザの言語が、ログイン時に選択する [言語の選択] ドロップダウンリストに表示される言語以外のものである場合、または URL 呼び出しにパラメータが設定されていない場合、WebFOCUS Client はこのデフォルト設定で表示言語を制御します。

リダイレクト (IBIWF_REDIRECT)

リダイレクトのオンとオフをグローバルに設定します。利用可能な値には、次のものがあります。

- **MIME** MIME テーブル内で設定された値を使用します。これがデフォルト値です。
- **なし** リダイレクトしません。出力レポートは、リクエストの実行直後にブラウザに表示されます。レポートコンテンツは、コンテンツのサイズが IBIWF_sendbufsize に指定された値を超過すると、レポートキャッシュに書き込まずに、ブラウザに送られます。
- **常時** 常にリダイレクトします。レポートコンテンツは、一時レポートキャッシュディレクトリに保存されます。レポートコンテンツのサイズが IBIWF_sendbufsize で指定した値を超えると、コンテンツはメモリからレポートキャッシュへ移動されます。次に、ブラウザから 2 つ目の HTTP コールが実行されて、表示するレポートコンテンツを取得します。
- **長さ** リダイレクトしません。レポートコンテンツのサイズが IBIWF_sendbufsize で指定した値を超えると、出力レポートはメモリからレポートキャッシュへ移動されます。出力レポートでレポートキャッシュが一杯になると、追加の HTTP コールは実行されずに、そのままブラウザに送信されます。

リダイレクトレポート名にタイムスタンプを追加しない (IBIWF_AS_NAME_REPORT)

Microsoft Excel を使用してリダイレクトされたすべてのレポートのファイル名の末尾から、日付と時間を自動的に削除するかどうかを定義します。この設定は、関連する [リダイレクト] 設定および [保存レポート] 設定の値に関係なく定義されます。

このチェックがオフ (False) の場合、リダイレクトされた Excel レポートのファイル名に日付と時間が自動的に追加されます。この設定がデフォルト値です。

このチェックがオン (True) の場合、リダイレクトされた Excel レポートのファイル名に日付と時間が追加されません。デフォルト設定のシステム動作を上書きし、Excel レポートファイル名に一意の日付時間を追加しない場合は、このオプションを選択します。

他のレポート出力リダイレクト設定で使用するこの設定の役割についての詳細は、130 ページの 「 ファイル出力のリダイレクトおよび保存 」 を参照してください。

最大メッセージ数 (IBIWF_MAX_MESSAGES)

WFServlet がリクエストの処理を停止し、エラーメッセージ 32100 を表示するまでに蓄積する WebFOCUS Reporting Server メッセージ行数を制御します。

```
Reporting Server messages exceeded IBIF_max_messages, report retrieval
aborted.
```

メッセージには、–TYPE コマンド、&ECHO=ALL 変数、およびデータアダプタからのエラーまたは警告が含まれます。この設定は、Java VM が WFServlet を実行するときにメモリ不足になることを防ぎます。デフォルト値は 20000 行です。IBIF_max_messages 設定は、リクエストとともに送信することができます。その場合、コンソールで設定した値を上書きします。App Studio でデバッグモードが有効な場合、各リクエストとともに値 50000 が送信されます。値 0 (ゼロ) は無制限であることを示します。

最大レスポンスウィンドウサイズ (IBIWF_REDIRNEWWINDOWSIZE)

Internet Explorer の使用時に、元のウィンドウに表示するレスポンスの最大許容サイズをバイト数で定義します。

この設定で指定したサイズを超えるレスポンスは新しいウィンドウに表示されます。これにより、エラーを発生させずにウィンドウが開きます。この設定がブランクの場合、最大制限は適用されません。デフォルト値は 400,000 バイトです。

Excel Server URL (IBIF_EXCELSERVURL)

Excel 2007 ファイル (.xlsx) フォーマットで出力を表示するために使用されるリソースの場所を指定します。

[Excel Server URL] ドロップダウンリストには、次の 2 つのオプションが表示されます。

- **デフォルト** 出力をミッドティアの IBIExcel Servlet に転送し、この Servlet が出力を Excel ファイルフォーマットで表示します。この設定で使用される URL は、WebFOCUS ミッドティアのデフォルト URL です。SSL のサポートやデフォルト内部セキュリティ以外の認証タイプのサポートが必要ない場合は、このオプションを使用します。これが、デフォルト設定のオプションです。
- **Reporting Server JSCOM** 出力を WebFOCUS Reporting Server の JSCOM3 リスナに転送し、このリスナが出力を Excel ファイルフォーマットで表示します。この設定で使用される URL は、JSCOM3 リスナの URL です。SSL のサポートやデフォルト内部セキュリティ以外の認証タイプのサポートを必要とする場合は、このオプションを使用します。

Active テクノロジ外部 JavaScript (IBIF_ACTIVE_EXTJS)

実行時のパフォーマンスを向上させるために、HTML 出力に JavaScript を埋め込む代わりに、外部 JavaScript ファイルの使用を可能にします。NO に設定した場合、ブラウザの [名前を付けて保存] オプションをサポートする Active Report または Active Dashboard (AHTML フォーマット) をオフラインで使用することができます。デフォルト値は [NO] です。

注意：HTML 出力での外部 JavaScript ファイルの使用についての詳細は、『WebFOCUS Active Technologies 利用ガイド』を参照してください。

Google マップ API バージョン (IBI_GOOGLE_MAPS_API_VERSION)

Google マップ API のバージョン番号を特定します。整数値、小数値をとることができます。整数値は安定版を示しています。現在、Google マップ API v3 のみがサポートされます。

Google マップ API キー (IBI_GOOGLE_MAPS_API_KEY)

Google API v3 には API キーは必要がありません。そのため、このテキストボックスはブランクにします。

グラフサーバ URL (IBIF_GRAPHSERVURL)

グラフイメージファイルフォーマットで出力を表示するために使用されるリソースの場所を指定します。

[グラフサーバ URL] ドロップダウンリストには、次の 2 つのオプションが表示されます。

- **デフォルト** 出力をミッドティアの IBIGraph Servlet に転送し、この Servlet が出力をグラフイメージファイルフォーマットで表示します。この設定で使用される URL は、WebFOCUS ミッドティアのデフォルト URL です。SSL のサポートやデフォルト内部セキュリティ以外の認証タイプのサポートが必要ない場合は、このオプションを使用します。これが、デフォルト設定のオプションです。

  構成オプションとして JSCOM3 をお勧めします。

- **Reporting Server JSCOM** 出力を WebFOCUS Reporting Server の JSCOM3 リスナに転送し、このリスナが出力をグラフイメージファイルフォーマットで表示します。この設定で使用される URL は、JSCOM3 リスナの URL です。SSL のサポートやデフォルト内部セキュリティ以外の認証タイプのサポートを必要とする場合は、このオプションを使用します。

注意：現在の構成で別のリソースを使用する必要がある場合は、技術サポートに問い合わせてください。

グラフエージェント (IBIF_GRAPHAGENTS)

グラフ処理に使用できる事前開始エージェントの数を指定します。エージェント数のデフォルト値は 10 です。

DBA ソース (IBIF_DBAPASS_SRC)

リクエストごとに WebFOCUS Reporting Server に DBA パスワードを送信するかを制御します。

次の値が使用可能です。

- **オフ** このオプションを選択すると、[DBA ソース] (IBF_DBAPASS_SRC) 設定の値がブランクに設定され、リクエストごとに DBA パスワードは転送されません。これが、デフォルト設定のオプションです。
- **IBIMR_user** このオプションを選択すると、[DBA ソース] (IBF_DBAPASS_SRC) 設定の値が BI Portal ユーザ ID に設定されます。

詳細は、217 ページの 「 DBA パスワードの設定 」 を参照してください。

TransIn/TransOut (IBI_WFTRANSINOUT)

transin/transout 処理 (WebFOCUS Reporting Server にリクエストを送信する処理、WebFOCUS Reporting Server から出力を返す処理) を行う完全修飾 Java クラスです。このクラスは、WebFOCUS Client の Servlet 実装用のプラグインで使用されます。このクラスは、WFTransInOutInterface Java クラスを実装する必要があります。たとえば、このクラスを使用することにより、WebFOCUS Reporting Server と Servlet 間で送受信されたデータを、双方向 (左から右の文字列、右から左の文字列) で解析できるようになります。デフォルト設定では、この値はブランクです。

プラグインクラス (IBI_WFEXT)

WebFOCUS Servlet が呼び出すプラグインクラスの修飾名を指定します。デフォルトの状態では、この変数は ibi.webfoc.WFEXTDefault に設定されています。これは、WebFOCUS が提供するデフォルトのプラグインであり、役立つ関数が格納されています。

マスターファイル完全情報 (IBI_MAS_FULLINFO)

WebFOCUS Reporting Server から取得されたマスターファイルにマスターファイルタイトルおよび接尾語を含めるかどうかを指定します。ドロップダウンメニューから以下のいずれかを選択します。

- **デフォルト** WebFOCUS Reporting Server のグローバルプロファイル (edasprof.prf) で指定された設定に準拠します。これが、デフォルト設定のオプションです。
- **はい** 取得されたマスターファイルにタイトルと接尾語を含めます。マスターファイル数が多いと、この取得に時間を要する場合があります。
- **いいえ** 取得されたマスターファイルにタイトルと接尾語を含めません。

共有の継承先 (IBI_CASCADE_SHARING)

(現在、この項目の説明はありません)

参照 ディファードレポート設定

[ディファードレポート] 設定では、ディファードレポートの処理方法を指定します。

カスタムディファードレポート名称のプロンプト (IBI_DEFERRED_CUSTOM_DESCRIPTION)

このチェックをオンにすると (デフォルト設定)、ディファードレポートの名称をカスタマイズするかどうかを選択するプロンプトが表示されます。この名称のデフォルト値は、ディファード実行されたレポートのタイトルです。このプロンプトは、パラメータ (IBIMR_defer_description) で定義された名称が、ディファード実行されたレポートリクエストとともに送信されていない場合に常に表示されます。

このチェックをオフにすると、ディファード実行用に送信されたレポートのタイトルが、ディファードレポート名称に自動的に割り当てられ、プロンプトは表示されません。

ディファードリクエスト送信済み通知の表示 (IBI_DEFERRED_NOTIFY_SUBMITTED)

このチェックをオンにすると (デフォルト設定)、[ディファードリクエスト送信済み] ウィンドウに、ディファードリクエストの実行に成功したことを示す確認メッセージが表示されます。ユーザは [OK] をクリックしてウィンドウを閉じます。

このチェックをオフにすると、[ディファードリクエスト送信済み] ウィンドウは表示されません。

ディファードチケット削除確認の表示 (IBI_DEFERRED_TICKET_DELETE_CONFIRM)

ユーザにディファードレポートの削除の確認を要求する自動メッセージを有効にします。このチェックをオンにすると (デフォルト設定)、削除の確認をユーザに要求するメッセージが表示されます。そのため、削除を確定するには 2 回のクリックが必要です。このチェックをオフにすると、削除の確認をユーザに要求するメッセージは表示されず、1 回のクリックで削除が確定されます。確認メッセージを省略すると、削除数が多い場合に時間を短縮できます。

参照　機能診断/トレース設定

機能診断/トレース設定は、現在の製品環境のシステムトレースおよびシステムログ収集について、特定の機能を定義します。

テストページ (IBI_ENABLE_TEST_PAGE)

HTTP リクエストのテストおよび RESTful Web サービスのテストに使用するページを有効にします。デフォルト設定で、このチェックはオンになっています。実稼動環境では、このページを無効にすることができます。

HTTP リクエストのテストページの URL は次のとおりです。

```
http://host:port/context_root/WFServlet?IBFS1_action=TEST
```

および

```
http://host:port/context_root/WFServlet?IBFS1_action=TEST1
```

自動セッショントレースレベル (IBI_AUTO_TRACE)

WebFOCUS セッションのデフォルトトレースレベルを設定します。この設定に割り当てたセッショントレースレベルは、セッションビューアメインページの [トレースレベル] 列のデフォルト値として表示されます。トレースファイルに収集されるイベントのレベルは、トレースレベルで識別されます。トレースレベルの範囲は、概要レベルのトレースのみを収集する [基本] から、すべてのイベントのトレースを収集する [サーバ] までがあります。管理者は、このデフォルト値をセッションごとに変更することができます。デフォルト値は [オフ] に設定されています。この設定では、トレースは収集されません。詳細は、191 ページの 「 セッションビューアメインページの表示 」 を参照してください。

プロシジャトレースのデフォルトオプション (IBI_AUTO_FEXOPTIONS)

プロシジャファイルのコマンド実行から取得される ECHO トレースおよび SQL トレースのデフォルトレベルを設定します。プロシジャファイルでは、&ECHO 変数により、コマンドが実行されるたびにコマンドラインが表示されるため、プロシジャのテストやデバッグに役立ちます。すべての SQL リクエストおよびレスポンスイベントから取得されるトレースのレベルです。デフォルト値は [ECHO ON、SQL ON] に設定されています。この設定では、プロシジャファイルの ECHO トレースと SQL トレースの両方が有効になります。管理者は、リストから別の組み合わせを選択してデフォルト値を変更することができます。

JavaScript エラーレポートを有効にする (IBI_JS_TRACE)

event.log ファイルおよびセッションビューアの JavaScript エラーメッセージの表示を有効にします。この設定の値は次のとおりです。

- **オン** JavaScript エラーを記録するエントリを event.log ファイルに追加し、これらをセッションビューアおよびセッションモニタに収集します。この設定がデフォルト値です。
- **オフ** このログ収集機能を無効にします。ただし、セッションビューアを使用する場合は、JavaScript エラーは、セッションビューアのトレースにも、event.log ファイルのエントリとしても追加されます。
- **なし** この機能を完全に無効にします。

ベストプラクティスとして、JavaScript エラーを event.log ファイルおよびセッションビューアのトレースに追加することをお勧めします。

完了時にすべての URL ログを取得 (IBI_REQUEST_LOGGING)

すべてのセッションに適用される URL リクエストメッセージログのデフォルトレベルを設定します。URL リクエストログのすべてのエントリは、リクエストログファイルに書き込まれます。このファイルは、管理コンソールの [機能診断] タブの [ログファイル] ページに表示されます。管理者は、[ログファイル] ページのリクエストエントリで別のログレベルを選択することで、特定のセッションに対してこのデフォルト値を上書きすることもできます。この設定の値は次のとおりです。

- **オフ** URL リクエストイベントのログを収集しません。
- **オン** すべての URL リクエストイベントのログを収集します。HTTP POST メッセージのログエントリにはデータは含まれません。
- **完全** すべての URL リクエストイベントのログを収集します。HTTP POST メッセージのログエントリには、POST リクエストで送信されたデータが含まれます。この設定がデフォルト値です。

Web サービス SOAP 詳細 (IBI_SOAP_DETAIL)

SOAP XML レスポンスに詳細なエラーメッセージを表示します。デフォルト設定で、このチェックはオンになっています。このチェックをオフにすると、管理者用の詳細情報がエンドユーザに表示されなくなります。

参照　暗号化の設定

[暗号化] 設定では、暗号化プロバイダ、暗号化手法、トークンキーの場所を指定します。

プロバイダ (IBI_ENCRYPTION_PROVIDER)

WebFOCUS のファイルに格納されたパスワードを暗号化するために使用する暗号化プロバイダを指定します。すべてのオプションが AES (Advanced Encryption Standard) 規格に基づいています。

次のオプションがサポートされます。

- 内部キーによる AES 128 暗号化

  これがデフォルト値です。
- 内部キーによる AES 192 暗号化
- 内部キーによる AES 256 暗号化
- 外部キーによる AES 128 暗号化
- 外部キーによる AES 192 暗号化
- 外部キーによる AES 256 暗号化

内部キーを指定するオプションを選択した場合、WebFOCUS 内部に埋め込まれたキーに基づいて暗号化されます。

外部キーを指定するオプションを選択した場合、このキーを作成し、key.cfg という名前のファイルにこれを割り当て、このファイルを次のディレクトリに保存する必要があります。

```
drive:¥ibi¥WebFOCUS82¥config
```

外部暗号化キーの作成についての詳細は、494 ページの 「 デフォルト TIBCO WebFOCUS 暗号化と AES 暗号化 」 を参照してください。

参照

ESRI 設定

[ESRI] 設定では、ESRI ベースのマップをサポートするローカルアプリケーションへの接続を定義します。

ESRI On Premise (IBI_ESRI_ON_PREMISE)

ESRI ベースのマップを作成するために使用する内部 ArcGIS JavaScript API ソースのパスを指定します。デフォルト設定では、この値はブランクです。この設定では、内部ソースの使用は有効になっていません。ESRI マップを作成するための内部 ArcGIS JavaScript API の使用を有効にするには、その API のパスをこの設定に入力します。通常は、「/web_resource/arcgis_api」と入力します。

この設定では、デフォルト API として JavaScript ArcGIS API バージョン 3.28 を参照する必要があります。この API には、「https://js.arcgis.com/3.28/」からアクセスすることができます。ArcGIS JavaScript API zip ファイルは、「https://developers.arcgis.com/downloads/#javascript」からダウンロードすることができます。このファイルにアクセスするには、ArcGIS で確立する有効なユーザ ID とパスワードが必要です。

ESRI ArcGIS JavaScript API についての詳細は、「https://developers.arcgis.com」を参照してください。

InfoAssist 用に ESRI On Premise を構成する方法についての詳細は、『TIBCO WebFOCUS InfoAssist 利用ガイド』の「ESRI On Premise 環境の構成」を参照してください。

App Studio 用に ESRI On Premise を構成する方法についての詳細は、『TIBCO WebFOCUS App Studio 利用ガイド』の「ESRI On Premise のインストールと構成」を参照してください。

参照

フィルタの設定

[フィルタ] 設定では、一般的な Web セキュリティ脆弱性に対する危険を防御する手法を設定します。

クロスサイトリクエストフォージェリ保護 (IBI_CSRF_ENFORCE)

すべての POST リクエストで、有効性を検証するクロスサイトリクエストフォージェリ (CSRF) セキュリティトークンを提供する必要があります。ただし、IBI_CSRF_Allow_Legacy 設定で例外が許可されている場合のレガシーリクエストは除きます。このチェックは、デフォルトでオン (True) に設定されています。

クロスサイトリクエストフォージェリセキュリティトークン (IBI_CSRF_TOKEN_NAME)

クロスサイトリクエストフォージェリ (CSRF) セキュリティトークンの名前を指定します。デフォルト値は IBIWF_SES_AUTH_TOKEN です。

CSRF トークンなしの WFServlet リクエストを許可する (IBI_CSRF_ALLOW_LEGACY)
このチェックをオン (True) にすると (デフォルト設定)、クロスサイトリクエストフォージェリ (CSRF) セキュリティトークンを必要とせずに (使用せずに) レガシー WFServlet リクエストを実行することができます。

RESTful Web サービスメソッドの実行 (IBI_REST_METHOD_ENFORCE)
このチェックをオン (True) にすると、作成、更新、削除を実行する RESTful Web サービス関数が HTTP POST メソッドでのみ実行可能になります。

デフォルト設定で、このチェックはオンになっています。

注意：[クロスサイトリクエストフォージェリ保護] (IBI_CSRF_ENFORCE) 設定を True に設定した場合、RESTful Web サービスでも CSRF トークンが必要になります。トークン名は、[クロスサイトリクエストフォージェリトークン] (IBI_CSRF_Token_Name) 設定で指定します。

静的コンテンツヘッダ (IBI_HTTP_RESPONSE_HEADER_ENABLED)
このチェックをオン (True) にすると (デフォルト設定)、Cache-Control レスポンスヘッダおよび expires レスポンスヘッダが、*.htm、*.html、bindowsBundle.jsp、*.css、*.gif、*.png、*.jpeg、*.jpg、*.txt、*.htc、CombineImageServlet フォーマットを使用する静的ファイルに追加されます。

Cache-Control レスポンスヘッダは、[キャッシュコントロールヘッダ] (IBI_HTTP_Response_Header_Cache_Control) 設定で変更することができます。expires レスポンスヘッダは、[ヘッダ有効期限] (IBI_HTTP_Response_Header_Expires) 設定で変更することができます。ただし、これらの設定のいずれかまたは両方を変更する場合は、事前に技術サポートに問い合わせてください。

キャッシュコントロールレスポンスヘッダ (IBI_HTTP_HEADER_CACHE_CONTROL)
Web アプリケーションがアクセスする静的コンテンツのデフォルトのキャッシュコントロールレスポンスヘッダを指定します。デフォルト値は「public, max-age=2592000」(30 日) です。この設定を変更する前に、技術サポートに問い合わせてください。

レスポンスヘッダ有効期限 (IBI_HTTP_HEADER_EXPIRES)
Web アプリケーションが提供する静的コンテンツのデフォルトの有効期限レスポンスヘッダを指定します。 デフォルト値は 2592000 (30 日) です。この設定を変更する前に、技術サポートに問い合わせてください。

クロスサイトスクリプト保護 (IBI_XSS_PROTECTION)

Microsoft Internet Explorer クロスサイトスクリプト (XSS) フィルタを有効にするか、無効にするかを指定します。有効なオプションには、次のものがあります。

- **True**

  次の HTTP レスポンスヘッダを返すことでブラウザの XSS フィルタを有効にします。

  ```
  X-XSS-Protection: 1
  ```

- **False**

  次の HTTP レスポンスヘッダを返すことでブラウザの XSS フィルタを無効にします。

  ```
  X-XSS-Protection: 0
  ```

  これがデフォルト値です。

- **オフ**

  HTTP レスポンスヘッダをブラウザに返しません。ブラウザは、ブラウザセキュリティゾーンのデフォルト XSS フィルタ設定に依存します。

[クロスサイトスクリプト保護] (IBI_XSS_PROTECTION) 設定は、[クロスサイトスクリプト保護ブロックモード] (IBI_XSS_MODE_BLOCK) 設定と連動して機能します。

注意：開発環境では、このフィルタを無効にする必要があります。これは、アプリケーション開発では、クロスサイトスクリプト攻撃と誤解される可能性のある文字を HTTP リクエストに使用する必要があるためです。[クロスサイトスクリプト保護] (IBI_XSS_PROTECTION) は、[False] (デフォルト値) または [オフ] に設定することができます。[クロスサイトスクリプト保護] (IBI_XSS_PROTECTION) を [オフ] に設定した場合、Internet Explorer がクロスサイトスクリプト保護を呼び出すかどうかは、ブラウザのセキュリティ設定に基づいて決定されます。この設定は、開発目的にのみ使用します。実稼動環境を個別に構築している場合は、その環境で [クロスサイトスクリプト保護] (IBI_XSS_PROTECTION) を [True] に設定することができます。

クロスサイトスクリプト保護ブロックモード (IBI_XSS_MODE_BLOCK)

[クロスサイトスクリプト保護] (IBI_XSS_PROTECTION) 設定で Microsoft Internet Explorer クロスサイトスクリプトフィルタを有効にした場合、このチェックボックスに割り当てた値でクロスサイトスクリプト攻撃に対するブラウザのレスポンスを指定します。次の値が使用可能です。

- **False**

  [クロスサイトスクリプト保護ブロックモード] (IBI_XSS_MODE_BLOCK) 設定のチェックをオフ (False) にした場合、次の値が返されます。

```
X-XSS-Protection: 1
```

クロスサイトスクリプト攻撃が検知された場合、Internet Explorer が Web ページに対して最小限の修正を試みます。これがデフォルト値です。

- **True**

  [クロスサイトスクリプト保護ブロックモード] (IBI_XSS_MODE_BLOCK) 設定のチェックをオン (True) にした場合、次の値が返されます。

  ```
  X-XSS-Protection: 1; mode=block
  ```

  Internet Explorer がクロスサイトスクリプト攻撃を検知した場合、Web ページを表示しません。

X-Content-Type-Options ヘッダ (IBI_XCONTENT_TYPE_OPTIONS)

このチェックをオンにすると、WebFOCUS から発行される HTTP レスポンスメッセージに XCONTENT TYPE ヘッダが含まれます。Reporting Server これがデフォルト値です。

XCONTENT TYPE ヘッダを含めると、サーバは HTTP レスポンスメッセージを受信するブラウザに対して、メッセージ内のデータを解釈して割り当て済みコンテンツタイプを上書きする MIME スニッフィングの代わりに、そのメッセージに割り当てられたコンテンツタイプを受容するよう指示します。サーバは、メッセージに割り当てられたコンテンツタイプが信頼できること、および割り当て済みコンテンツタイプを使用してメッセージ内のデータを表示できることをアサートします。

また、XCONTENT TYPE ヘッダを含めることで、メッセージを受信するブラウザがクロスサイトスクリプト攻撃から保護されます。クロスサイトスクリプト攻撃では、HTTP レスポンスメッセージの MIME スニッフィングにより、メッセージのデータ内に潜む実行可能コードに基づいて意図しないプログラムがブラウザで実行される可能性があります。

このチェックをオフにすると、WebFOCUS Server から発行される HTTP レスポンスメッセージに XCONTENT TYPE ヘッダは含まれず、このメッセージを受信するブラウザがクロスサイトスクリプトなどの攻撃に対して脆弱になります。この設定に割り当てられたデフォルト値を変更すると、ユーザがこの脆弱性の影響を受けやすくなるため、デフォルト値を変更する場合は、技術サポートに問い合わせてください。

マルチパートリクエストの最大コンテンツサイズ (IBI_MAX_CONTENT_SIZE)

リポジトリまたは EDA サーバにアップロードされるデータファイルの最大サイズを定義します。この設定値を超えるデータファイルをアップロードすることはできません。デフォルト値は 2048 メガバイトです。最大許容値は 10240 メガバイトです。-1 を指定すると、この設定が無効になります。

キャッシュ前のアップロードの最大メモリサイズ (IBI_UPLOAD_MAX_MEMORY)
リポジトリまたは EDA サーバにアップロードされたファイルのデータが占有可能なメモリの最大サイズを定義します。アップロードプロセス中にメモリに移動されるデータは、この設定で定義された最大サイズに制限されます。最大サイズを超えた残りのデータは、一時的にディスクにキャッシュされます。デフォルト値は 256 メガバイトです。-1 を指定すると、キャッシュが無効になります。

参照　複数レポートの設定

[複数レポート] 設定では、複数フレームレポートのオプションを構成します。

フレーム名 (IBIWF_MFRAMENAME)
複数フレームのレポートがある場合に各フレームに名前を付けます。各フレームの名前は、ここで設定した値と、その値の末尾に付けられるインデックス番号とで構成されます。たとえば、IBWIF_mframename に「MYFRAME」という値が設定された 2 つのフレームがある場合、これらのフレームの名前はそれぞれ MYFRAME1 と MYFRAME2 になります。デフォルト値は MREPORT です。

最大列数 (IBIWF_MRCOLUMNS)
複数フレームのレポートで、1 ページあたりの最大列数を指定します。列数のデフォルト値は 1 です。

レポートの順序 (IBIWF_MORDER)
複数フレームレポートの各フレームを表示させる方法として、リクエストで指定したフィールドの順序で表示させるか、その逆の順序で表示させるかを指定します。有効な値には、FORWARD と REVERSE があります。デフォルト値は FORWARD です。

タイプ (IBIWF_MREPORTS)
インデックスレポート、複数フレームレポート、標準レポートの中からどのレポートを作成するかを指定します。有効な値には、オフ、INDEX、FRAME があります。デフォルト値は [オフ] です。

接頭語 (IBIWF_MPREFIX)
最大 50 バイトの説明テキストを指定します。このテキストの末尾には連続番号が付けられて、目次でそのレポートを特定できるようになります。インデックスレポートにハイパーリンク名を追加します。たとえば、この値が MyReport の場合、ハイパーリンク名は「MyReport」という名前とインデックス番号とで構成されます。インデックス番号は 1 から始まります。デフォルト値は Report です。

注意：IBIWF_mreports が FRAME に設定されている場合、この設定は使用しないでください。

最大行数 (IBIWF_MRROWS)

IBIWF_mreports が FRAME に設定されている場合、縦方向に重ねるレポート数を指定します。デフォルト設定では、この値はブランクです。

インデックス (IBIWF_INDEX)

IBIWF_mreports=INDEX に設定されている場合に、目次上でレポート名の末尾に追加する連続番号を制御します。[オン] に設定すると、最初に生成したレポートには連続番号 1 が追加されます。[オフ] に設定すると、連続番号は省略されます。IBIWF_mprefix で指定したテキストのみが適用されます。デフォルト値は [オン] です。

参照 Web ビューアの設定

[Web ビューア] 設定では、Web ビューアのオプションを構成します。

Web ビューアを有効にする (IBIF_ODPENABLE)

Web ビューアレポートの表示を制御します。

このチェックがオン (YES) の場合、Web ビューアレポートが表示されます。デフォルト設定で、このチェックはオンになっています。

このチェックがオフ (NO) の場合、Web ビューアレポートは表示されません。その代わりに、メッセージが記述されたページが表示されます。このメッセージの内容は、IBIODP_disable_msg 変数で設定します。設定しない場合は、ブランク行が表示されます。

無効メッセージ (IBIODP_DISABLE_MSG)

この変数にはメッセージが格納されます。このメッセージは、IBIF_odpenable が NO に設定されている場合に Web ビューアレポートの代わりに表示されます。デフォルト値は、ブランク行 (¥n) です。

ターゲット (IBI_ODP_TARGET)

Web ビューアの [戻る] ボタンのアクションを制御します。

- このチェックがオン (ON) の場合、ブラウザの [戻る] ボタンで、Web ビューアの先頭ページを再表示します。デフォルト設定で、このチェックはオン (ON) になっています。
- このチェックがオフ (OFF) の場合、ブラウザの [戻る] ボタンで、ブラウザの表示が Web ビューアレポートの呼び出しページに戻ります。

ハイライト HTML タグ値の検索 (IBI_ODP_SEARCH_HIGHLIGHT)

Web ビューアレポートで検索結果として検出されたテキストを強調表示するための HTML タグです。デフォルト値は、テキストに下線を付ける <u> です。

参照 OLAP の設定

[OLAP] 設定では、OLAP オプションを構成します。

これらの設定は、[OLAP を有効にする] のチェックをオンにした場合にのみ表示されます。[OLAP を有効にする] チェックボックスは、管理コンソールの [構成] タブの [その他] ページに表示されます。

ドッキング (IBI_OLAP_DOCKED)
このチェックをオンにすると、OLAP レポートの実行中に OLAP コントロールパネルが常時表示されます。デフォルト設定では、このチェックはオフになっています。

Excel 形式で保存 (IBI_OLAP_SAVEEXCEL)
OLAP レポートに [Excel 形式で表示] オプションを表示するかどうかを指定します。デフォルト設定で、このチェックはオンになっています。

Excel 2000 形式で保存 (IBI_OLAP_SAVEEXCEL2000)
OLAP レポートに [Excel 2000 形式で表示] オプションを表示するかどうかを指定します。デフォルト設定で、このチェックはオンになっています。

Excel 2000 Formula 形式で保存 (IBI_OLAP_SAVEEXCEL2000WITHFORMULAS)
OLAP レポートに [Excel Formula 形式で表示] オプションを表示するかどうかを指定します。デフォルト設定で、このチェックはオンになっています。

位置 (IBIF_OLAPPOS)
OLAP パネルの位置です (TOP または BOTTOM)。有効な値は、[TOP] または [BOTTOM] です。デフォルト値は [BOTTOM] です。

スキン名 (IBIF_OLAPSKINNAME)
管理者は、OLAP コントロールパネルなどの OLAP コンポーネントの配色に名前を付けたり、配色を変更したりできます。デフォルト値は [NEUTRAL] です。

スキン色 (IBIF_OLAPSKINCOLOR)
管理者は、OLAP コントロールパネルなどの OLAP コンポーネントの配色をプレビュー表示したり、配色を変更したりできます。デフォルト値は、[BLACK] です。

参照　その他の設定

[その他] 設定では、さまざまな構成設定を指定します。

メールサーバ (IBI_EMAIL_SERVER)
WebFOCUS Mobile のリンクを Email 送信するためのメールサーバを指定します。

メールサーバポート (IBI_EMAIL_SERVER_PORT)
(現在、この項目の説明はありません)

メールサーバユーザ名 (IBI_EMAIL_SMTP_USER)
(現在、この項目の説明はありません)

メールサーバパスワード (IBI_EMAIL_SMTP_PASS)
(現在、この項目の説明はありません)

ユーザデフォルトロール (マイグレートで使用) (IBI_ENABLE_UDR)
マイグレート済みの環境で、セキュリティセンターの [デフォルトロール] タブを有効にします。デフォルト設定では、このチェックはオフになっています。

OLAP を有効にする (IBI_ENABLE_OLAP)
OLAP 設定および機能を有効にします。このチェックをオンにすると、OLAP 機能が次の場所に表示されます。

- **WebFOCUS**
  - セキュリティセンターの [Basic Reporting] セクション下の [Run Procedures with OLAP] 権限
  - 管理コンソールの [構成] タブ下の [OLAP] 設定ページ
  - [プロパティ] ダイアログボックスの [OLAP 実行] チェックボックス

    注意：ポータルおよびワークスペースの [プロパティ] ダイアログボックスでは、このチェックボックスは灰色 (選択不可) で表示されます。レポート、グラフ、ビジュアライゼーションの [プロパティ] ダイアログボックスでは、このチェックボックスは選択可能です。
- **InfoAssist および InfoAssist Basic** [オートドリルダウン] および [OLAP 分析] メニューに表示される OLAP 関連機能のすべて ([OLAP オプション] パネル、[OLAP] パネル、リボンの [OLAP] ボタン、OLAP レポートを含む)。

この設定では、App Studio での OLAP の使用は有効になりません。App Studio で OLAP の使用を有効にするには、App Studio を起動し、[App Studio オプション] ダイアログボックスの [レポート] タブで [OLAP の有効化] のチェックをオンにします。詳細は、『TIBCO WebFOCUS App Studio 利用ガイド』の「オプションダイアログボックスでのユーザ設定の指定」を参照してください。

デフォルト設定では、このチェックはオフになっています。

FOCUS エラーを警告に変換 (IBI_FOCUS_WARNING_NUMBERS)

1 つまたは複数の FOCUS エラーメッセージ番号をカンマ (,) 区切りで指定します。WebFOCUS および ReportCaster は、この設定に番号が表示される FOCUS エラーメッセージを、エラーメッセージではなく警告と見なします。

WebFOCUS でこれらの FOCUS エラーメッセージ番号のいずれかが検出された場合、エラーメッセージではなく警告メッセージが生成され、FOCUS エラーメッセージをエラーとして収集するトレースが、セッションビューアでハイライト表示されません。

レポートスケジュール実行時に、ReportCaster でこれらの FOCUS エラーメッセージ番号のいずれかが検出された場合、FOCUS エラーメッセージとは関係なくレポートが配信されます。この場合、レポートスケジュールの [通知タイプ] が [エラー時] に設定されていても、エラー通知が送信されることはありません。

ReportLibrary 項目のデフォルトアクション (IBI_LIBRARY_ITEM_DEFAULT_ACTION)

ReportLibrary 項目をダブルクリックした際にレポートの最新バージョンを開くか ([最新] を選択)、レポートバージョンのリストを表示するかを指定します ([バージョン] を選択)。デフォルト値は [最新] です。ここで指定した値は、ReportLibrary 項目を右クリックし、[表示] を選択した際のコンテキストメニューの先頭に表示されます。

レポート埋め込みイメージのアップロード (IBI_PUSH_IMAGE)

レポートおよび HTML ページにイメージを埋め込むために、リポジトリイメージを WebFOCUS Reporting Server にアップロードします。デフォルト設定で、このチェックはオンになっています。

ユーザログイン時の実行パス (IBI_SIGNIN_PATHS)

ユーザがポータルまたは Web サービスにログインした際に実行するプロシジャすべてのリストを指定します。デフォルト設定では、この値はブランクです。この設定では、ユーザのログインに応答して実行されるプロシジャはありません。下図のように、プロシジャのリストを構成するには、各プロシジャのパス名を入力し、それぞれのパス名をカンマ (,) で区切ります。

```
IBFS:/WFC/Repository/Public/motd.fex,
```

この設定には、さまざまな用途に使用されるプロシジャを含めることができます。たとえば、この設定を使用して、ログイン時に「今日のメッセージ」をユーザに送信するプロシジャを実行することができます。以下の例は、「今日のメッセージ」を送信する motd.fex ファイルのコードを示しています。

```
-IF &FOCSECUSER EQ admin GOTO ADMINMSG;
-TYPE <UserMsg>Hello normal user</UserMsg>
-GOTO DONE;
-ADMINMSG
-TYPE <UserMsg>Hello admin</UserMsg>
-DONE
```

また、次の例のように、この設定でプロシジャを実行して環境を初期化し、単一 foccache チケットを作成するプロシジャをリポジトリ内に構築することで、そのチケットを後続のリクエストすべてで使用可能にすることもできます。

```
TABLE FILE IBISAMP/CAR PRINT COUNTRY
IF RECORDLIMIT EQ 1
ON TABLE HOLD AS FOCCACHE/LATCH
END
```

このプロシジャからレポート出力を生成することはできません。

カスタム文字列 (IBI_RESOURCEBUNDLE_ALTERNATE_PREFIXES)

グローバル項目 (例、メニューバーオプション、エラーメッセージ、その他の機能) のラベルのカスタマイズに使用されるテキスト文字列が格納されたファイルの名前です。このテキストボックスは、デフォルト設定でブランクになっています。

注意：この設定を変更する場合は、技術サポートに問い合わせてください。

レガシー Cookie (IBI_ALLOWED_COOKIES)

このテキストボックスに「WF_USER」と入力すると、この Cookie がブラウザに返されます。これにより、WebFOCUS Reporting Server での認証時に WFSIGNON アクションが可能になります。

除外する Reporting Server ファイル拡張子 (IBI_EXCLUDE_WFRS_FILE_EXTENSIONS)

WebFOCUS Reporting Server へのアップロードを禁止するファイルタイプを指定します。ファイルタイプは、ファイルの拡張子で識別します。たとえば、この設定で指定された拡張子のいずれかを使用する PDF ファイルはアップロードできません。デフォルト値はブランクです。この設定では、任意のタイプのファイルをアップロードすることができます。

ツールのテーマを上書き (IBI_TOOL_THEME)

InfoAssist およびポータルデザイナに割り当てるテーマの名前を指定します。デフォルト設定では、この値はブランクです。この設定では、これらのツールにデフォルトテーマ動作が適用されます。別の値として [BIPNeutral] を選択すると、これらのツールに斬新でニュートラルな外観のデフォルトテーマが設定されます。

レガシー機能を有効にする (IBI_ENABLE_LEGACY_FEATURES)

レガシー機能の使用を有効にします。

このチェックがオフ (FALSE) の場合、レガシー機能権限は使用不可となり、グループに割り当てることもできません。クラウドベースのフリートライアルのインストールでは、これがデフォルト設定です。

このチェックがオン (TRUE) の場合、レガシー機能権限は使用可能となり、グループに割り当てることができます。クラウドベースのフリートライアル以外のインストールではすべて、これがデフォルト設定です。

この設定が適用されるのは、次のレガシー機能権限です。

- Advanced Reporting 権限カテゴリ
  - Create Alerts (opAlertAssistant)
  - Data Visualization From Metadata (opVisualization)
  - Display Easel.ly Link (opEaselly)
  - Express Analytics (opExpressAnalytics)
  - InfoAssist From Metadata (opInfoAssist)
  - InfoAssist From Reporting Object (opInfoAssistviaReportingObject)
- Application Development 権限カテゴリ
  - Create Reporting Objects (opReportingObject)

これらのレガシー権限が有効の場合、InfoAssist、レポートオブジェクトツール、およびその他のレガシーツールが、管理者および Advanced Users、Developers グループ、またこれらの権限が与えられたロールのグループで使用可能になります。

テクニカルプレビュー機能 (IBI_TECHPREVIEW_FEATURES)

テクニカルプレビューモードを有効にします。このモードを有効にすると、今後のリリースで導入が計画されている特定の機能をユーザが表示して評価することができます。

この設定は、プレビュー機能が組み込まれた製品バージョンにのみ関係します。一連の新機能はバージョンごとに異なるため、特定のバージョンに組み込まれたプレビュー機能のコード名が別のバージョンに関係しない場合があります。そのため、インストール済み製品バージョンのテクニカルプレビューモードに組み込まれている機能のいずれかのコード名がリストに含まれていない場合、テクニカルプレビューモードを有効にすることはできません。

この設定がブランクの場合、テクニカルプレビューモードは無効です。ユーザは新機能をプレビューすることはできません。これがデフォルト値です。

この設定のテキストボックスに、インストール済み製品バージョンのテクニカルプレビューモードに組み込まれている 1 つまたは複数の機能のコード名をセミコロン区切りリストとして入力すると、WebFOCUS でそのテクニカルプレビューモードが有効になり、ユーザはそのリストに含まれている新機能を表示してテストすることができます。

テクニカルプレビューモードを有効にすると、管理者がログインした直後に、現在有効なテクニカルプレビュー機能を識別するメッセージが表示されます。このメッセージも、管理者のログインイベントに関する他のレコードとともにイベントログに書き込まれます。管理者以外のユーザがログインした場合、このメッセージは表示されません。

接続情報プロンプトオプション (IBI_PROMPT_FOR_CONNECTION_CREDENTIALS)

このチェックがオン (TRUE) の場合、[Run Procedures with Different Connection Credentials] (opRunAs)権限が、[ロール] ダイアログボックスの [Basic Reporting] 権限カテゴリで使用可能になります。

この権限が与えられたユーザは、コンテキストメニューから [別の接続認証情報で実行] オプションを選択することができます。このメニューオプションを使用することで、ユーザは、高度なデータセットにアクセスするために内部認証に対して別の認証情報が要求されるデータベースでプロシジャを実行する際に、認証情報を提供することができます。これにより、レポート作成機能が、実行時に別のユーザ ID とパスワードを認証できなければ使用不可能な情報にまで拡張されます。

このチェックがオフ (FALSE) の場合、これらの権限およびメニューオプションが使用できません。これが、この設定のデフォルト値です。

この設定は、WebFOCUS Client 内の [別の接続認証情報で実行] メニューオプションの構成にのみ影響します。この機能の構成を完了するには、WebFOCUS Reporting Server および各データベース接続でも別の認証情報を受容するよう構成する必要があります。WebFOCUS Reporting Server の構成についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

WebFOCUS Client の構成についての詳細は、573 ページの 「 別の接続認証情報で実行設定の構成 」 を参照してください。

拡張コピーを有効にする (IBI_ENABLE_COPY_SPECIAL)

[Application Development] 権限カテゴリ下の [Copy and Update Paths] (opCopySpecial) 権限が割り当てられたユーザの [コピーとパスの更新] メニューオプションの使用を有効にします。

このチェックをオン (TRUE) にすると、ユーザのロールに [Copy and Update Paths] (opCopySpecial) 権限が含まれる場合、[コピーとパスの更新] メニューオプションが使用可能になります。

このチェックをオフ (FALSE) にすると、[コピーとパスの更新] メニューオプションはすべてのユーザに表示されません。これがデフォルト値です。

パスワード変更の Email 通知を有効にする (IBI_EMAIL_CHANGE_PSWD_NOTIFY)

(現在、この項目の説明はありません)

パスワードリセットリクエストを有効にする (IBI_REQUEST_PSWD_RESET)
(現在、この項目の説明はありません)

CACHECOMS を有効にする (IBI_ENABLE_CACHECOMS)
バックグラウンド処理で UOA_CACHECOMS テーブルの使用を有効にします。

UOA_CACHECOMS テーブルは、WebFOCUS リポジトリデータベースに格納され、WebFOCUS のいずれかのインスタンスでエントリ記録が変更された場合に、これらの変更が内部ポーリング処理で取得され、他のインスタンスに配信されるまで保持することで、分散環境内の WebFOCUS の複数インスタンスを同期します。別のデータベース処理で UOA_CACHECOMS をポーリングし、配信済みの変更を含むエントリのテーブルを 1 分ごとにクリアします。

このチェックがオン (True) の場合、UOA_CACHECOMS テーブルおよび関連するデータベース処理が有効になります。これがデフォルト値です。

このチェックがオフ (False) の場合、UOA_CACHECOMS テーブルおよび関連するデータベース処理が無効になります。

このチェックをオフにして、このテーブルの使用および関連するデータベース処理を中断することができます。

別の接続認証情報で実行設定の構成

[別の接続認証情報で実行] メニューオプションは、プロシジャのターゲットデータベース内で保持される別の認証情報の認証をサポートするデータベースへの接続を開きます。通常、別の認証情報の使用をサポートするデータベースには、実行時にこれらに対する認証情報の提示が可能なユーザのみ利用できる情報が含まれます。これらの別の認証情報は、データ接続の認証に使用するデフォルト設定のサービスアカウントの認証情報によって提供される一般に利用可能な情報へのアクセスを補完するものです。

WebFOCUS Reporting Server ブラウザインターフェースおよび WebFOCUS Client 内の構成機能を使用して、管理者は、このメニューオプションおよび機能の利用を、組織の要件を満たした規模でユーザに許可することができます。

WebFOCUS Reporting Server では、別の接続認証情報の使用権限は、これを要求するデータベース接続にのみ割り当てることができます。

WebFOCUS Client では、別の接続認証情報を要求するプロシジャの実行権限は、独自の認証情報を保持するデータベースへのアクセスが必要なコンテンツリソース、およびこれらのデータベースで別の認証情報の使用が許可されたユーザにのみ割り当てることができます。

[Run Procedures with Different Connection Credentials] 権限を、別の接続認証情報の使用をサポートするリソースの利用時にこれを必要とするユーザにのみ利用可能にするには、WebFOCUS Client で次の構成を確立する必要があります。

1. WebFOCUS Reporting Server が、データベース接続で要求される別の接続認証情報をサポートするよう構成します。

   WebFOCUS Reporting Server の構成についての詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

2. [Run Procedures with Different Connection Credentials] (opRunAs) 権限をロールで使用可能にするには、管理コンソールの [構成] タブの [その他] 設定ページで、[認証情報プロンプトオプション] のチェックをオンにします。

   詳細は、574 ページの 「 認証情報プロンプトオプション設定を有効にするには 」 を参照してください。

3. セキュリティセンターの [ロール] タブの [Basic Reporting] 権限カテゴリで、[Run Procedures with Different Connection Credentials (opRunAs)] 権限を、このメニューオプションの使用が必要なグループのロールに割り当てます。

   詳細は、480 ページの 「 ロールを編集するには 」 を参照してください。この権限を含む新しいロールを作成する場合は、479 ページの 「 ロールを作成するには 」 を参照してください。

4. このメニューオプションの使用が必要なユーザが、この権限を含むグループに割り当てられていることを確認します。

   この権限を使用するグループにユーザを割り当てる必要がある場合は、472 ページの「 ユーザをグループに追加するには 」 を参照してください。

5. 別の認証情報の使用をサポートするすべてのコンテンツ項目に対してルールを作成します。この場合、[Run Procedures with Different Connection Credentials (opRunAs)] 権限を含むロールを、これらの項目の実行時に強化されたユーザアクセス権がメンバーに与えられたグループに割り当てます。

   詳細は、482 ページの 「 コンテンツリソースに対してルールを作成するには 」 を参照してください。

手順　認証情報プロンプトオプション設定を有効にするには

1. 管理者としてログインし、管理コンソールを開きます。
2. [構成] タブの [アプリケーションの設定] フォルダ下で [その他] を選択し、[その他] 設定ページを表示します。

3. [認証情報プロンプトオプション] のチェックをオンにします。
4. [保存] をクリックします。
5. 「変更は正常に保存されました」というメッセージで、[OK] をクリックします。
6. 管理コンソールのメニューバーで、[キャッシュのクリア] をクリックします。
7. キャッシュがクリアされたことを示すメッセージで [OK] をクリックします。
8. 現在のセッションからログアウトします。
9. 再度ログインし、構成を続行します。

参照　パラメータプロンプトの設定

[パラメータのプロンプト] 設定では、WebFOCUS Client でのパラメータプロンプトの動作を指定します。

Managed Reporting (IBIMR_PROMPTING)

WebFOCUS の BI Portal 内のリクエストを対象に、パラメータのプロンプトを有効にするかどうかを指定します。利用可能な値には、次のものがあります。

- **オフ**　サイトレベルでのパラメータのプロンプトをオフにします。
- **デフォルト値で実行 (XMLRUN)**　-DEFAULT コマンドが設定されていない場合、オートプロンプト画面を表示します。変数の初期値がすべて設定されていれば、その値でプロシジャを実行します。
- **常にプロンプトを表示 (XMLPROMPT)**　-DEFAULT コマンドが設定されている場合でも、オートプロンプト画面を表示します。すべての変数が -DEFAULT で指定されている場合も、オートプロンプト画面を表示します。-DEFAULT コマンドで指定された変数は、オートプロンプト画面を表示しません。これがデフォルト値です。

[パラメータのプロンプト] オフ時の動作 (IBIMR_PROMPTINGUNSET)

[Managed Reporting] (IBIMR_PROMPTING) が [常にプロンプトを表示] (XMLPROMPT) または [デフォルト値で実行] (XMLRUN) に設定されている場合、およびプロシジャの [プロパティ] ダイアログボックスで [パラメータのプロンプト] のチェックがオフの場合に、BI Portal 内のプロシジャ (FEX) のパラメータプロンプトを有効または無効にします。利用可能な値には、次のものがあります。

- **オフ**　パラメータのプロンプトを無効にします。
- **デフォルト値で実行 (XMLRUN)**　-DEFAULT コマンドが設定されていない場合、オートプロンプト画面を表示します。変数の初期値がすべて設定されていれば、その値でプロシジャを実行します。これがデフォルト値です。

- **常にプロンプトを表示 (XMLPROMPT)** -DEFAULT コマンドが設定されている場合でも、オートプロンプト画面を表示します。すべての変数が -DEFAULT で指定されている場合も、オートプロンプト画面を表示します。-DEFAULT コマンドで指定された変数は、オートプロンプト画面を表示しません。

セルフサービス (IBI_WFDESCRIBE_DEFAULT)

セルフサービスレポートのオートプロンプトを有効または無効にします。利用可能な値には、次のものがあります。

- **オフ** オートプロンプトを無効にします。これがデフォルト値です。
- **デフォルト値で実行 (XMLRUN)** -DEFAULT コマンドが設定されていない場合、オートプロンプト画面を表示します。変数の初期値がすべて設定されていれば、その値でプロシジャを実行します。
- **常にプロンプトを表示 (XMLPROMPT)** -DEFAULT コマンドが設定されている場合でも、オートプロンプト画面を表示します。すべての変数が -DEFAULT で指定されている場合も、オートプロンプト画面を表示します。-DEFAULT コマンドで指定された変数は、オートプロンプト画面を表示しません。
- **XML の表示 (構文エラー確認付きデバッグ) (XML)** 変数が記述された XML ドキュメントをブラウザに表示します。この設定は内部的に使用され、デバッグおよび構文エラー確認用としてのみ使用することをお勧めします。
- **XML の表示 (デバッグ) (XMLCHECK)** 変数が記述された XML ドキュメントをブラウザに表示します。この設定は内部的に使用され、デバッグ用としてのみ使用することをお勧めします。

注意： BI Portal では、IBIMR_prompting という別の変数設定が使用されます。

静的リストコントロールですべての値を事前選択 (IBI_FOCALL_DEFAULT)

実行時のレスポンシブオートプロンプトの複数選択静的リストパラメータで、すべての値の自動選択をデフォルト設定で有効にします。

このチェックがオン (TRUE) の場合、複数選択静的リストを含むレスポンシブオートプロンプトの選択リストパラメータには、デフォルト設定で、初期選択値として FOC_ALL が自動的に割り当てられます。これにより、これらのリストには、実行時の選択値としてすべての値が自動的に表示されます。ただし、複数選択静的リストに表示するデフォルト値が指定されている場合は、初期選択値としての FOC_ALL の自動割り当てがこの値で上書きされ、デフォルト値が初期選択値として表示されます。

このチェックがオフ (FALSE) の場合、複数選択静的リストを含むパラメータには、デフォルト設定で、初期選択値として FOC_ALL が自動的に割り当てられません。この場合、リスト内のすべての項目は、実行時に自動的に選択されません。複数選択静的リストに指定されたデフォルト値が含まれる場合、この値がデフォルト設定で表示されます。静的選択リストのすべての値をクエリに含めるには、ユーザは手動で [すべての値] オプションを選択するか、リスト内のすべての値を個別に選択する必要があります。

デフォルト設定では、このチェックはオフ (FALSE) になっています。

デフォルトオートプロンプトテンプレート (IBI_DESCRIBE_TEMPLATES)

オートプロンプトインターフェースのレイアウトを定義するテンプレートを指定します。

- **デザイナ** デザイナオートプロンプト実装およびデザイナオートプロンプトテンプレートの使用を指定します。このテンプレートでは、オートテンプレートのインターフェースに DESIGNER のページフォーマットが使用されます。これがデフォルト値です。
- **レスポンシブ** レスポンシブ実装および autoprompt_jqm.jsp テンプレートを使用します。
- **HTML_TOP** HTML ベースの実装および autoprompt_top.html テンプレートを使用します。このテンプレートでは、パラメータがページ上部に横方向に表示されます。
- **HTML_TOP_CHECKED** HTML ベースの実装および autoprompt_top_checked.html テンプレートを使用します。このテンプレートでは、新規ウィンドウのチェックボックスで [Run] が事前に選択され、デフォルト設定ですべてのレポートが新規ウィンドウで開きます。

aptemplates.xml ファイルにカスタムテンプレート名タグを入力することで、このリストにカスタマイズされた HTML およびレスポンシブオートプロンプトインターフェーステンプレートを追加することができます。ただし、デザイナオートプロンプトインターフェーステンプレートは、カスタマイズすることができません。詳細は、578 ページの 「カスタムオートプロンプトテンプレートを追加するには」 および579 ページの 「カスタムオートプロンプトテンプレートをテストするには」 を参照してください。

[選択なし] の動作 (IBIF_DESCRIBE_NULL)

動的複数選択リストで [選択なし] の値が選択された場合に、WebFOCUS Client が -SET コマンドで変数に割り当てる値 (_FOC_NULL または FOC_NONE) を指定します。デフォルト値は _FOC_NULL です。

自動記述 (IBI_AUTODESCRIBE)

レポートおよびグラフのパラメータの自動インデックス機能を有効にします。このチェックをオン (TRUE) にすると、ユーザがレポートまたはグラフを保存した際に、そのレポートまたはグラフの作成時に指定したパラメータに自動的にインデックスが付けられます。これにより、これらのパラメータに関する情報が即座に検索可能になり、より速やかに広範囲の検索結果が得られます。

このチェックは、デフォルトでオン (TRUE) に設定されています。

手順　カスタムオートプロンプトテンプレートを追加するには

この手順では、カスタムオートプロンプトインターフェーステンプレートのエントリをAPTemplates.xml ファイルに直接追加する方法について説明します。追加したカスタムテンプレートは、デフォルト設定でロードされる 3 つのテンプレートとともに、[デフォルトオートプロンプトテンプレート] (IBI_DESCRIBE_TEMPLATES) 設定リストに表示されます。テンプレート名タグおよび属性についての詳細は、APTemplates.xml ファイルの最上部に表示されるコメントセクションを参照してください。

1. WebFOCUS がインストールされたマシンで、*drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc¥prod に移動します。
2. APTemplates.xml ファイルを ¥etc ディレクトリの ¥prod フォルダから ¥custom フォルダにコピーします。
3. ¥custom フォルダで、APTemplates.xml ファイルをテキストエディタで開き、ファイルの末尾までスクロールします。
4. カーソルを <APTemplates> タグの後に置きます。
5. 次の属性を含む <template> タグを入力して、カスタムテンプレートを追加します。

```
<template name="templatename" src="templatepath" type="{HTML|REDIR}" />
```

説明

templatename
カスタムテンプレートの名前です。この名前が [デフォルトオートプロンプトテンプレート] 設定リストに表示されます。たとえば、「template name="RedirectTemplate"」と入力します。

templatepath
カスタムテンプレートのパス名およびファイル名です。カスタムオートプロンプトテンプレートファイルは、次のいずれかの WebFOCUS フォルダにのみ追加できます。

- **レスポンシブオートプロンプトテンプレート**　*drive*:¥ibi¥WebFOCUS82¥webapps¥webfocus¥tools¥autoprompt_jqm

- **HTML ベースオートプロンプトテンプレート** *drive*:¥ibi¥WebFOCUS82¥ibi_html¥javaassist¥ibi¥html¥describe

  注意 : ただし、デザイナオートプロンプトテンプレートは、カスタマイズすることができません。

`type`
オートプロンプトの実装タイプです。

`HTML`
このテンプレートが HTML 実装に使用されることを指定します。

`REDIR`
このテンプレートがレスポンシブ実装に使用されることを指定します。

以下はその例です。

```
<template name="HTMLhorizontal" src="C:/ibi/WebFOCUS82/ibi_html/
javaassist/ibi/html/describe/autoprompt_top.html" type="HTML" />
```

6. APTemplates.xml ファイルに追加するカスタムオートプロンプトインターフェーステンプレートごとに上記の手順を繰り返します。
7. すべてのカスタムオートプロンプトインターフェーステンプレートのタグを追加した後、ファイルを保存します。
8. 管理者としてログインし、管理コンソールを起動します。
9. 管理コンソールのメニューバーで [キャッシュのクリア] をクリックします。
10. 個々のキャッシュがクリアされたことを示すメッセージで、[OK] をクリックします。
11. 更新後の結果をテストします。詳細は、579 ページの 「 カスタムオートプロンプトテンプレートをテストするには 」 を参照してください。

手順　カスタムオートプロンプトテンプレートをテストするには

1. [構成] タブの [アプリケーションの設定] フォルダ下で、[パラメータのプロンプト] をクリックします。
2. [パラメータのプロンプト] ページで、[デフォルトオートプロンプトテンプレート] リストをクリックします。
3. APTemplates.xml ファイルに追加したカスタムテンプレートがリストに表示されていることを確認します。
4. 一部のカスタムテンプレートがリストに表示されない場合は、APTemplates.xml ファイルを開き、<template name> タグで属性および値がそれぞれ正確に指定されていることを確認して編集します。詳細は、「カスタムオートプロンプトテンプレートを追加するには」の手順 5 から 7 を参照してください。

5. カスタムテンプレートのエントリがすべてリストに表示されている場合、いずれかを選択し、[保存] をクリックします。
6. 変更が保存されたことを示すメッセージで [OK] をクリックします。
7. 値が割り当てられておらず、[パラメータのプロンプト] プロパティのチェックボックスが選択されたフィルタパラメータを含むレポートリクエストを選択または作成します。
8. 選択したレポートリクエストを実行し、手順 5 で選択したカスタムオートプロンプトページが表示されるかを確認します。
9. 手順 5 で選択したカスタムオートプロンプトインターフェースが開かない場合は、エラーの可能性があります。ブラウザのトレースおよび WebFOCUS Client のセッショントレースを確認してエラーを特定します。
10. 手順 5 で選択したカスタムオートプロンプトインターフェースが開いた場合は、リクエストを終了します。

参照 Quick Data 設定

[Quick Data] 設定では、Quick Data が認証を実行する方法を指定します。

セキュリティ (IBI_QUICK_DATA_SECURITY)

WebFOCUS Quick Data で使用するログインのタイプを指定します。選択可能な値は、[Reporting Server] および [Managed Reporting] です。デフォルト値は [Reporting Server] です。追加の構成は必要ありません。

フォームのみ (IBI_QUICK_DATA_FORM_ONLY)

IBI_Quick_Data_Security で MR 認証が選択された場合に適用されます。次の値が使用可能です。

- **はい** ユーザは、各自のレポートの作成に、InfoAssist は使用できず、定義済みの adhoc フォームのみを使用できます。
- **いいえ** ユーザは、定義済みの adhoc フォームまたは InfoAssist を使用して、各自のレポートを作成することができます。デフォルト値は [いいえ] (チェックオフ) です。

参照 リポジトリの設定

[リポジトリ] 設定では、JDBC ドライバが リポジトリへのアクセスに使用する認証情報を指定します。

データベースドライバ (IBI_REPOS_DB_DRIVER)

リポジトリへのアクセスに使用する JDBC ドライバを指定します。

この設定の値を更新することはできません。この設定に割り当てられたデフォルト値の変更が必要な場合は、技術サポートに問い合わせてください。

データベース URL (IBI_REPOS_DB_URL)
JDBC ドライバがリポジトリへのアクセスに使用する URL を指定します。

この設定の値を更新することはできません。この設定に割り当てられたデフォルト値の変更が必要な場合は、技術サポートに問い合わせてください。

データベースユーザ ID (IBI_REPOS_DB_USER)
JDBC ドライバがリポジトリへのアクセスに使用するユーザ ID を指定します。

この設定の値を更新することはできません。この設定に割り当てられたデフォルト値の変更が必要な場合は、技術サポートに問い合わせてください。

データベースパスワード (IBI_REPOS_DB_PASSWORD)
JDBC ドライバがリポジトリへのアクセスに使用するパスワードを指定します。

同期間隔 (IBI_REPOSITORY_SYNC_INTERVAL)
複数の JVM が同一の リポジトリを使用している場合に、他の JVM が リポジトリのセキュリティ情報を同期する時間間隔を分単位で指定します。たとえば、この時間間隔が経過するまで、クラスタ内の別の Application Server や、ReportCaster Distribution Server でセキュリティ情報は更新されません。デフォルト値は 1 分 です。

ユーザ名のキャッシュ制限 (IBI_CACHE_USERNAMES_LIMIT)
(現在、この項目の説明はありません)

外部グループキャッシュ制限 (IBI_CACHE_USERS_GROUPS_LIMIT)
グループメンバーシップのリストに保持するユーザ数を指定します。ユーザ数のデフォルト値は 500 で、最大値は 1000 です。

外部グループキャッシュ期間 (IBI_CACHE_USERS_EXTERNAL_GROUPS_DURATION)
各ユーザの外部グループのリストを保持する期間を分単位で指定します。デフォルト値は 180 分で、最大値は 720 分です。

ユーザプロファイルキャッシュ期間 (IBI_CACHE_USER_AFTER_SIGNOFF_DURATION)
ユーザのログアウト後にユーザセキュリティ情報を保持する期間を分単位で指定します。デフォルト値は 30 です。

注意：この設定は、ログイン、補助的なタスクの実行、ログアウトを処理する Web サービスアプリケーションを実行するようなアプリケーションで使用すると便利です。

有効なポリシーキャッシュ制限 (IBI_CACHE_EFFECTIVE_POLICIES_PER_SESSION_LIMIT)
1 回のセッションで保持するセキュリティポリシーの最大数を指定します。ポリシー数のデフォルト値は 50 で、最大値は 500 です。

有効なポリシーキャッシュ期間 (IBI_CACHE_EFFECTIVE_POLICY_DURATION)
キャッシュされたセキュリティポリシーを有効であると見なす期間を分単位で指定します。デフォルト値は 180 分で、最大値は 720 分です。

プロシジャキャッシュ制限 (IBI_CACHE_WFC_FEX_LIMIT)
レスポンス時間を向上するためにメモリにキャッシュするプロシジャ数を指定します。プロシジャ数のデフォルト値は 100 です。

最新のアクセス時間を更新 (IBI_UPDATE_LAST_ACCESS)
リソースへのアクセスが発生した際に、[プロパティ] ダイアログボックスの [最終アクセス日] プロパティを更新するかどうかを指定します。デフォルト値は [オン] です。この設定では、プロパティは更新されます。

参照　ソース管理の設定

[ソース管理] 設定では、WebFOCUS または App Studio での他社製ソース管理プロバイダの使用を有効にします。また、ソース管理プロバイダのリポジトリが格納されているサーバのパスおよびルートプロジェクトのパスを指定します。

ソース管理を有効にする (IBI_SCM_ENABLE)
このチェックをオンにすると、ソース管理プロバイダの統合により、WebFOCUS または App Studio でのアプリケーションコードの開発を管理することができます。

WebFOCUS で Git ソース管理の使用を有効にするには、このチェックおよび [プライベート作業領域] (IBI_SCM_PWA_ENABLE) のチェックをオンにする必要があります。

プライベート作業領域 (IBI_SCM_PWA_ENABLE)
このチェックをオンにすると、WebFOCUS または App Studio のソース管理でプライベート作業領域の使用が有効になります。

WebFOCUS で Git ソース管理の使用を有効にするには、このチェックおよび [ソース管理を有効にする] (IBI_SCM_ENABLE) のチェックをオンにする必要があります。

プロバイダ (IBI_SCM_PROVIDER_TYPE)
WebFOCUS または App Studio 使用時に利用可能なソース管理プロバイダを指定します。

この設定に表示される利用可能なプロバイダリストから、使用するソース管理プロバイダを選択することができます。

- **Git**　WebFOCUS からソース管理の各操作が実行できます。
- **Team Foundation Server**　App Studio からソース管理の各操作が実行できます。

通常、これらのプロバイダで作成されたアプリケーションは、WebFOCUS または App Studio のホストサーバと同一マシンにインストールされます。

バージョン (IBI_SCM_PROVIDER_VERSION)

[プロバイダ] (IBI_SCM_PROVIDER_TYPE) 設定で指定したソース管理プロバイダのバージョン番号を指定します。

たとえば、Team Foundation Server 2013 を使用する場合は「2013」と入力します。

この設定は、Git には関係しません。ソース管理プロバイダとして Git を使用する場合は、ブランクのままにします。

ソース管理の構成パス (IBI_SCM_REPOSITORY_LOCATION)

Team Foundation Server のホストサーバの URL を指定します (プロジェクトのホストとして使用されるコレクション名を含む)。

たとえば、Team Foundation Server 2013 を使用する場合、「http://TFS_*hostname*:*portcollection_name*」のフォーマットを使用して値を入力します。

この設定は、Git には関係しません。ソース管理プロバイダとして Git を使用する場合は、ブランクのままにします。

ルートプロジェクトパス (IBI_SCM_ROOT_PROJECT_LOCATION)

ルートソース管理プロジェクトがインストールされているフォルダの名前およびパスを指定します。

たとえば、Team Foundation Server 2013 を使用する場合は「$/TeamProject1」と入力します。

この設定は、Git には関係しません。ソース管理プロバイダとして Git を使用する場合は、ブランクのままにします。

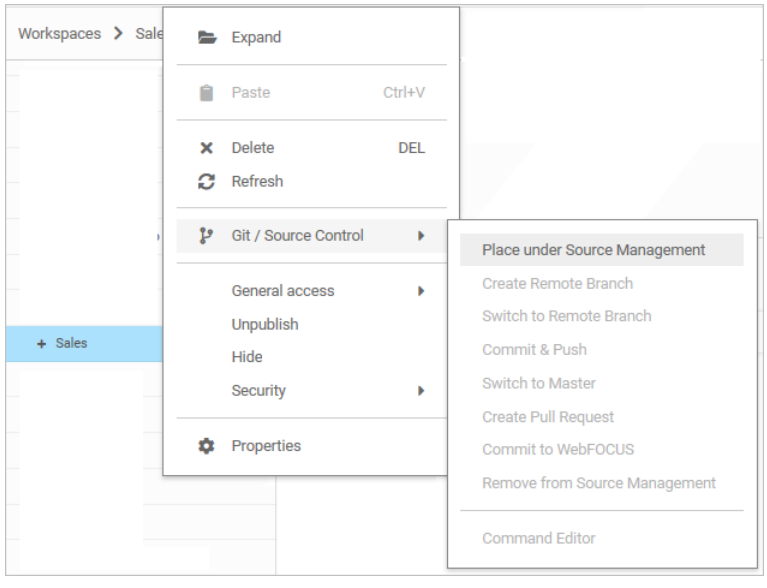
手順　WebFOCUS ホームページでソース管理プロバイダを構成するには

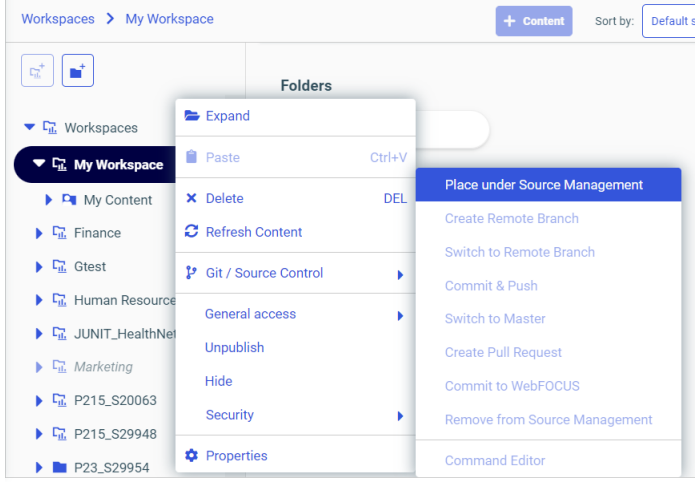
ソース管理プロバイダの構成を試行する前に、[プロバイダ] (IBI_SCM_PROVIDER_TYPE) 設定リストの WebFOCUS ユーザが使用可能なすべてのプロバイダが、WebFOCUS で利用可能なネットワーク上のディレクトリに構成済みであることを確認します。

1. 管理者としてログインし、管理コンソールを開きます。
2. [構成] タブの [アプリケーションの設定] フォルダ下で [ソース管理] を選択し、[ソース管理] ページを表示します。
3. [ソース管理を有効にする] (IBI_SCM_ENABLE) 設定のチェックをオンにします。
4. [プライベート作業領域] (IBI_SCM_PWA_ENABLE) 設定のチェックをオンにします。
5. [プロバイダ] (IBI_SCM_PROVIDER_TYPE) 設定のリストから [Git] を選択します。

6. [ソース管理] セクションの残りの設定はブランクのままにします。以下はこれらのリストです。
   - バージョン (IBI_SCM_PROVIDER_VERSION)
   - ソース管理の構成パス (IBI_SCM_REPOSITORY_LOCATION)
   - ルートプロジェクトパス (IBI_SCM_ROOT_PROJECT_LOCATION)
7. [保存] をクリックします。
8. 「変更は正常に保存されました」というメッセージで、[OK] をクリックします。
9. 管理コンソールのメニューバーで、[キャッシュのクリア] をクリックします。
10. キャッシュがクリアされたことを示すメッセージで [OK] をクリックします。
11. 現在のセッションからログアウトします。
12. 再度ログインし、ワークスペース表示を開きます。

13. 下図のように、コンテンツエリアのリソースツリーで、任意のワークスペースを右クリックし、コンテキストメニューに [Git/ソース管理] オプションが表示されることを確認します。





手順　TIBCO WebFOCUS App Studio でソース管理プロバイダを構成するには

ソース管理プロバイダの構成を試行する前に、[プロバイダ] (IBI_SCM_PROVIDER_TYPE) 設定リストの App Studio ユーザが使用可能なすべてのプロバイダが、WebFOCUS で利用可能なネットワーク上のディレクトリに構成済みであることを確認します。

1. 管理者としてログインし、管理コンソールを開きます。
2. [構成] タブの [アプリケーションの設定] フォルダ下で [ソース管理] を選択し、[ソース管理] ページを表示します。
3. [ソース管理を有効にする] (IBI_SCM_ENABLE) 設定のチェックをオンにします。
4. [プロバイダ] (IBI_SCM_PROVIDER_TYPE) 設定のリストで、WebFOCUS のソース管理を実行するアプリケーションを選択します。

   たとえば、[Team Foundation Server] を選択します。
5. [バージョン] (IBI_SCM_PROVIDER_VERSION) 設定テキストボックスに、[プロバイダ] (IBI_SCM_PROVIDER_TYPE) テキストボックスで指定したソース管理プロバイダのバージョン番号を入力します。

   たとえば、Team Foundation Server 2013 を使用する場合は「2013」と入力します。
6. [ソース管理の構成パス] (IBI_SCM_REPOSITORY_LOCATION) 設定テキストボックスに、ソース管理プロバイダのホストサーバの URL を入力します。この場合、プロジェクトのホストに使用されるコレクション名も含めます。

   たとえば、「http://TFS_*hostname*:*port*/tfs/*collection_name*」と入力します。
7. [ルートプロジェクトパス] (IBI_SCM_ROOT_PROJECT_LOCATION) 設定テキストボックスに、ルートソース管理プロジェクトがインストールされたフォルダの名前とパスを入力します。

   たとえば、「$/TeamProject1」と入力します。
8. [保存] をクリックします。
9. 「変更は正常に保存されました」というメッセージで、[OK] をクリックします。
10. 管理コンソールのメニューバーで、[キャッシュのクリア] をクリックします。
11. キャッシュがクリアされたことを示すメッセージで [OK] をクリックします。
12. 構成をテストします。

参照　テキスト生成サーバ設定

[テキスト生成サーバ] 設定では、グラフの見出し、脚注、ツールヒントのナレーションを提供する、独立したサーバへの接続を定義します。

テキスト生成サーバ URL (IBI_TEXT_GENERATION_SERVER_URL)

グラフの見出し、脚注、ツールヒントのナレーションを提供する外部自然言語生成 (NLG) サーバの URL を指定します。インストールした製品でグラフの自然言語生成がサポートされる場合、この設定にテキスト生成サーバの URL を入力します。デフォルト設定では、この値はブランクです。

外部自然言語生成 (NLG) サーバの使用を有効にした場合、この設定には一般に次の値を入力します。

```
http://machine_name:20000/yseop-manager/direct/savvy-kb/dialog.do
```

説明

machine_name
外部自然言語ジェネレータのホストサーバの名前です。

参照　検証の設定

[検証] 設定では、検証テストが失敗した際の WebFOCUS の動作を指定します。

注意： IBI、IBIFS、PG_ の文字パターンは、内部の製品変数に予約されています。変数名の先頭にこれらの文字パターンを使用しないでください。

検証 (IBI_VALIDATE_ACTION)

URI パラメータ検証のテストに失敗した場合に実行するアクションを指定します。この検証テストは、SQL インジェクション攻撃およびクロスサイトスクリプティング攻撃に対する予防措置として実行します。次の値が使用可能です。

- **ログのみ**　WebFOCUS はリクエストを許可しますが、失敗を *drive*:¥ibi¥WebFOCUS82¥logs¥websecurity.log ファイルに記録します。
- **カスタム実行とログ(ENFORCE)**　WebFOCUS がリクエストをブロックし、失敗を *drive*:¥ibi¥WebFOCUS82¥logs¥websecurity.log ファイルに記録した上で、IBI_Validate.Error_Response で指定されたアクションを実行します。
- **デフォルト実行とログ(XMLENFORCE)**　WebFOCUS がリクエストをブロックし、失敗を *drive*:¥ibi¥WebFOCUS82¥logs¥websecurity.log ファイルに記録した上で、XML レスポンスとともに HTTP ステータスコード 200 (成功) を返します。これがデフォルト値です (推奨値)。

カスタムレスポンス (IBI_VALIDATE_ERROR_RESPONSE)

URI パラメータ検証に失敗し、IBI_Validate.Action が ENFORCE に設定されている場合にブラウザに返す HTTP レスポンスコードを指定します。指定可能な値は、有効な任意の HTTP ステータスコード (例、400、403)、URI、完全修飾 URL のいずれかです。HTTP ステータスコードを入力した場合、WebFOCUS はレスポンスヘッダとともにそのステータスコードを返します。URL または URI を入力した場合、WebFOCUS は 200 (成功) を返し、ブラウザをそのアドレスにリダイレクトします。デフォルト値は 400 です。

レスポンスヘッダ (IBI_VALIDATE_RESPONSE_HEADER)

診断用としてのみ使用します。True に設定した場合、検証に失敗した URL、およびその失敗の理由が指定された HTTP レスポンスヘッダをブラウザに返します。デフォルト値は False です。

InfoAssist のプロパティ

InfoAssist の機能の表示および使用は、管理コンソールの [InfoAssist のプロパティ] ページの設定に基づいて決定されます。InfoAssist は、コンテンツを作成または更新する際に使用するツールです。

[InfoAssist のプロパティ] ページを開くには、管理コンソールで [構成] タブをクリックし、下方向へスクロールして [InfoAssist のプロパティ] をクリックします。このページで、InfoAssist の各オプションを有効または無効にすることができます。

参照 InfoAssist ホームタブプロパティの理解

InfoAssist の [ホーム] タブでよく使用するプロパティおよびオプションを有効にするかどうかを制御します。次のプロパティがあります。

ライブプレビューモードを使用する

デフォルト設定で InfoAssist をライブプレビューモードで起動するか、クエリデザインモードで起動するかを指定します。[はい] を選択した場合、デフォルト設定で InfoAssist がライブプレビューモードで起動します。[はい] を選択しない場合、InfoAssist はクエリデザインモードで起動します。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

最大レコード数

[ホーム] タブの [最大レコード数] メニューを有効にします。[表示] を選択しない場合、[最大レコード数] メニューは、InfoAssist インターフェースに表示されません。

テーマ

InfoAssist ユーザは、さまざまな配色のスタイルシートテーマを適用して、レポートやグラフにスタイルを設定することができます。ユーザは、標準の InfoAssist テーマを選択することも、社内で作成されたカスタムカスケードスタイルシートテーマを選択することもできます。

ページ見出し

[ホーム] タブの [ページ見出し] メニューを有効にします。このメニューを使用して、レポート出力の各ページに見出しまたは脚注を追加することができます。

レポート見出し

[ホーム] タブの [レポート見出し] メニューを有効にします。このメニューを使用して、レポート出力の先頭ページに見出しまたは脚注を追加することができます。

参照 InfoAssist フォーマットタブプロパティの理解

レポートまたはグラフの場合、InfoAssist の [ホーム] タブの [フォーマット] グループに出力ファイルフォーマットオプションのリストが表示されます (例、HTML、PDF、Excel)。 これらのオプション以外に、レポートまたはグラフの作成時に使用可能なレイアウト機能および表示機能を [フォーマット] タブに表示するオプションもあります。このセクションの各種設定を使用して、これらの両方のタイプのオプションを表示するかどうかを制御することができます。

注意：このセクションの設定は、ビジュアライゼーションの [フォーマット] タブの機能には影響しません。

Analytic PDF

InfoAssist での Analytic PDF フォーマットの使用を有効にします。Analytic PDF は、PDF レポートに Analytic Document のポータビリティとインタラクティブ機能が追加されたフォーマットです。出力結果はオフライン分析のために設計され、フィルタ、ソート、グラフなど自己完結型レポートの分析処理をサポートするために必要なデータおよび JavaScript ツールがすべて含まれています。

このチェックをオンにした場合、[出力ファイルフォーマット] ドロップダウンリストのオプションとしてこのフォーマットが使用可能になります。[出力ファイルフォーマット] ドロップダウンリストは、InfoAssist ホームページのリボンの [フォーマット] グループから開きます。また、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの、[レポート出力フォーマット]、[グラフ出力フォーマット]、[ドキュメント出力フォーマット] の各ドロップダウンリストからデフォルト出力フォーマットとして選択することもできます。

デフォルト設定では、このチェックはオフになっています。

Analytic Document

InfoAssist での Analytic Document フォーマットの使用を有効にします。Analytic Document は、HTML レポートに Analytic Document のポータビリティとインタラクティブ機能が追加されたフォーマットです。出力結果はオフライン分析のために設計され、フィルタ、ソート、グラフなど自己完結型レポートの分析処理をサポートするために必要なデータおよび JavaScript ツールがすべて含まれています。

このチェックをオンにした場合、[出力ファイルフォーマット] ドロップダウンリストのオプションとしてこのフォーマットが使用可能になります。[出力ファイルフォーマット] ドロップダウンリストは、InfoAssist ホームページのリボンの [フォーマット] グループから開きます。また、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの、[レポート出力フォーマット]、[グラフ出力フォーマット]、[ドキュメント出力フォーマット] の各ドロップダウンリストからデフォルト出力フォーマットとして選択することもできます。

デフォルト設定で、このチェックはオンになっています。

その他の HTML (グラフ)

PNG、JPEG、GIF、SVG 出力フォーマットの使用を有効にします。デフォルト値は [PNG] です。[PNG] は、グラフ出力のフォーマットとして選択する値ではありません。

その他の PDF (グラフ)

PDF/SVG および PDF/GIF 出力フォーマットの使用を有効にします。デフォルト値は [PDF/SVG] です。

Excel (EXL2K)

Excel 2000 出力フォーマットの使用を有効にします。Excel では、ほとんどのスタイルシートの属性がサポートされるため、完全なレポートのフォーマット設定が可能です。レポートを表示するコンピュータには、Microsoft Excel 2000 がインストールされている必要があります。

このチェックをオンにすると、この出力フォーマットオプションが、[ツールオプションダイアログのデフォルト] セクションの [出力フォーマット] ドロップダウンリストから選択可能になります。

デフォルト設定で、このチェックはオンになっています。

Excel Formula (EXL2K FORMULA)

[Excel (EXL2K)] オプションが選択されている場合に、[Excel Formula (EXL2K FORMULA)] の使用を有効にします。

デフォルト設定で、このチェックはオンになっています。

Excel (XLSX)
Excel 2007 出力フォーマットの使用を有効にします。レポートを表示するコンピュータには、Microsoft Excel 2007 がインストールされている必要があります。

このチェックをオンにすると、この出力フォーマットオプションが、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの各出力フォーマットドロップダウンリストから選択可能になります。

デフォルト設定で、このチェックはオンになっています。

Excel Formula (XLSX FORMULA)
[Excel (XLSX)] オプションが選択されている場合に、[Excel Formula (XLSX FORMULA)] の使用を有効にします。

デフォルト設定で、このチェックはオンになっています。

Excel Pivot (EXL2K PIVOT)
Excel 2000 PivotTable 出力フォーマットの使用を有効にします。PivotTable は、複雑なデータを分析するための Excel ツールです。

デフォルト設定で、このチェックはオフになっています。

Excel CSV
カンマ区切り値 (CSV) ファイルフォーマットの使用を有効にします。

このチェックをオンにすると、InfoAssist で [Excel CSV] フォーマットオプションの使用が可能になり、[ホーム] タブの [フォーマット] グループオプションリストの [Excel] フォーマットオプション下に表示されます。このチェックをオフにすると、このオプションは使用できなくなり、[フォーマット] グループオプションリストに表示されません。

デフォルト設定で、このチェックはオンになっています。

HTML
HTML ページレポートフォーマットの使用を有効にします。

このチェックをオンにすると、この出力フォーマットオプションが、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの各出力フォーマットドロップダウンリストから選択可能になります。

InfoMini の即時実行
InfoMini の即時実行オプションの使用を有効にします。デフォルト設定で、このチェックはオンになっています。

その他のグラフタイプ
ブロック地図、メータグラフ、パレートなど、より複雑なグラフの作成を可能にします。

Web ビューア
レポート出力を一度に 1 ページずつ表示することを可能にします。ユーザは、出力画面の下部に表示されるナビゲーションメニューを使用して各ページに移動することができます。このオプションは、HTML または Active Report 出力フォーマットが選択されている場合にのみ有効になります。

PDF
PDF フォーマットの使用を有効にします。

このチェックをオンにすると、この出力フォーマットオプションが、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの各出力フォーマットドロップダウンリストから選択可能になります。

PowerPoint (PPT)
PowerPoint 2000 出力フォーマットの使用を有効にします。レポートを表示するコンピュータには、Microsoft PowerPoint 2000 以降がインストールされている必要があります。

このチェックをオンにすると、この出力フォーマットオプションが、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの各出力フォーマットドロップダウンリストから選択可能になります。

PowerPoint (PPTX)
PowerPoint 2007 出力フォーマットの使用を有効にします。レポートを表示するコンピュータには、Microsoft PowerPoint 2007 以降がインストールされている必要があります。

このチェックをオンにすると、この出力フォーマットオプションが、[InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションの各出力フォーマットドロップダウンリストから選択可能になります。

積み重ねメジャー
レポートの最初の列にすべての数値フィールド名と値が表示されます。[積み重ねメジャー] 機能は HTML、Excel、PowerPoint 出力フォーマットが選択されている場合にのみ有効になります。

ユーザ選択
レポートの実行時に、ユーザによる出力フォーマットの変更を可能にします。

参照

InfoAssist 表示タブプロパティの理解

デザインモード、出力場所、データ表示など、InfoAssist のさまざまなレポートコンポーネントの表示をカスタマイズできます。InfoAssist の [表示] タブに表示される次のプロパティを構成することができます。

表示タブの表示

[表示] タブおよびそのメニューオプションをすべて有効にします。このチェックをオフにした場合、InfoAssist インターフェースに [表示] タブは表示されません。

データパネル

データパネルの設定をカスタマイズできます。有効値は、[論理] (デフォルト)、[リスト]、[構造] です。

クエリ

レポート作成時の [フィルタ]、[BY] および [ACROSS]、[SUM] などのクエリコンポーネントの表示方法をカスタマイズできます。有効値は、[ツリー] (デフォルト)、[縦横表示]、[縦表示] です。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

参照

InfoAssist ツールオプションダイアログのデフォルトプロパティの理解

管理者は、[ツールオプションダイアログのデフォルト] セクションの設定で、デフォルトツール設定を指定することができます。各オプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。ただし、管理者は、別のグループのいずれかで無効にされているデフォルト値を指定することはできません。たとえば、[フォーマットタブ] セクションで [Analytic PDF] フォーマットを無効にした場合、[ツールオプションダイアログのデフォルト] セクションで、[レポート出力フォーマット]、[グラフ出力フォーマット]、[ドキュメント出力フォーマット] のデフォルトとしてこのフォーマットを設定しようとすると、エラーメッセージが表示されます。

レポート出力フォーマット

レポートのデフォルトフォーマットを設定します。有効値は、[HTML]、[Analytic Document]、[PDF]、[Analytic PDF]、[EXL07]、[EXL2K]、[PowerPoint (PPT)]、[PowerPoint (PPTX)] です。このリストの各フォーマットオプションは、[InfoAssist のプロパティ] ページ の [フォーマットタブ] セクションで各フォーマットのチェックがオンに設定されている場合にのみ選択できます。特定のフォーマットのチェックがオフに設定されている場合、このリストからそのフォーマットを選択すると、フォーマットオプションが無効であることを示す警告メッセージが表示されます。デフォルト値は [HTML] です。

グラフ出力フォーマット

グラフのデフォルトフォーマットを設定します。有効値は、[HTML]、[HTML5]、[Analytic Document]、[PDF]、[Analytic PDF]、[EXL07]、[EXL2K]、[PowerPoint (PPT)]、[PowerPoint (PPTX)] です。このリストの各フォーマットオプションは、[InfoAssist のプロパティ] ページ の [フォーマットタブ] セクションで各フォーマットのチェックがオンに設定されている場合にのみ選択できます。特定のフォーマットのチェックがオフに設定されている場合、このリストからそのフォーマットを選択すると、フォーマットオプションが無効であることを示す警告メッセージが表示されます。デフォルト値は [HTML5] です。

レイアウト出力フォーマット

InfoAssist で生成されるレイアウトのデフォルトフォーマットを設定します。有効値は、[HTML]、[Analytic Document]、[PDF]、[Analytic PDF]、[EXL07]、[EXL2K]、[PowerPoint (PPT)]、[PowerPoint (PPTX)] です。このリストの各フォーマットオプションは、[InfoAssist のプロパティ] ページ の [フォーマットタブ] セクションで各フォーマットのチェックがオンに設定されている場合にのみ選択できます。特定のフォーマットのチェックがオフに設定されている場合、このリストからそのフォーマットを選択すると、フォーマットオプションが無効であることを示す警告メッセージが表示されます。デフォルト値は [Analytic Document] です。

ページの向き

レポートおよびグラフのデフォルトページ方向を設定します。有効値は [縦] と [横] です。デフォルト値は [横] です。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

ページサイズ

レポートおよびグラフのデフォルトページサイズを設定します。有効値は、[A3]、[A4]、[A5]、[Letter]、[Tabloid]、[Legal]、[PPT-SLIDE]、[E] です。デフォルト値は [Letter] です。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

データプレビュー方法

レポートのデフォルトプレビュー方法を、サンプルデータ、データソースの実際のデータのいずれかに設定します。有効値は、[ライブ] および [サンプル] です。デフォルト値は [ライブ] です。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

最大レコード数

[インタラクティブ] デザインビューが選択されている場合に、データソースから取得するデフォルト設定の行数を設定します。これは、ユーザが大規模なデータを扱う際のレスポンス時間の短縮に役立ちます。この設定は、レポート作成時にのみ適用されます。レコード数の制限の設定は、実行時のレポート出力には影響を与えません。有効値は、[すべて]、[1]、[10]、[50]、[100]、[500]、[1000]、[2000]、[5000]、[10000] です。デフォルト値は 500 行です。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

出力ターゲット

レポートおよびグラフのデフォルト位置を設定します。有効値は、[単一タブ]、[新規タブ]、[単一ウィンドウ]、[新規ウィンドウ] です。デフォルト値は [単一タブ] です。このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

Analytic Document

InfoAssist のクイックアクセスツールバーから開く [プロシジャの設定] ダイアログボックスの [Analytic Document] 設定のデフォルト値を指定します。有効な値は、[DESIGNER スタイル] と [レガシー] です。[InfoAssist のプロパティ] ページでは、[DESIGNER スタイル] がデフォルト設定で選択されています。

この設定の値は、InfoAssist で Analytic Document フォーマットを使用したレポート、グラフ、レイアウトの実行時に使用するデフォルト設定のインターフェースを指定します。ユーザが InfoAssist で Analytic Document フォーマットのレポート、グラフ、レイアウトを新規作成する場合、[プロシジャの設定] ダイアログボックスに表示される [Analytic Document] 設定から別のオプションを選択すると、[InfoAssist のプロパティ] ページの設定で指定したデフォルト値が上書きされます。

InfoAssist/BI Portal スタイルシート

InfoAssist およびポータルで使用するスタイルシートを設定します。[スタイルシートの変更] をクリックすると、[テンプレート - 定義済みスタイルシートを参照] ウィンドウが開きます。デフォルト設定で表示される値は [Warm.sty] です。

このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

Visualization スタイルシート

ビジュアライゼーションの作成時に使用するスタイルシートを設定します。[スタイルシートの変更] をクリックすると、[テンプレート - 定義済みスタイルシートを参照] ウィンドウが開きます。デフォルト設定で表示される値は [Warm.sty] です。

このオプションの [ユーザの上書きを許可] のチェックをオンにすると、ユーザは、管理者が指定したデフォルト設定を変更することができます。

HTML のエンコード

データ内のスクリプトタグをエンコードします。これにより、スクリプトタグが置き換えられ、ブラウザで実行されなくなります。デフォルト値は [はい] です。この設定は、プロシジャに ON TABLE SET HTMLENCODE ON コマンドを追加します。

Web ビューアを有効にする

InfoAssist ユーザがレポートを一度に 1 ページずつ表示できるようにします。出力画面の下部に表示されるナビゲーションメニューを使用して、各ページを表示できます。このオプションは、HTML または Active Report 出力フォーマットが選択されている場合にのみ有効になります。

キャッシュから取得する行数

バイナリファイルに格納されたキャッシュデータから、出力ウィンドウに表示する 1 回あたりの行数を指定します。デフォルト値は 100 行です。

HTML の高さを固定

InfoAssist で、リボンの [フォーマット] タブの [ナビ] グループから、[固定] オプションでレポートエリアの高さを自動的に固定する方法を指定します。

この設定で [自動調整] を指定した場合、[固定] オプションを選択して生成したレポートで、表示されるウィンドウの高さが自動的に調整されます。これがデフォルト値です。

この設定で [固定] を指定した場合、[固定] オプションを選択して生成したレポートで、表示されるウィンドウのサイズに関わらず、固定高さが 4 インチに自動的に設定されます。

HTML アコーディオン

InfoAssist で、リボンの [フォーマット] タブの [ナビ] グループから、[アコーディオン] オプションで、表示されるコンテナに合わせてデータのサイズを自動的に変更するアコーディオンレポートを表示するかどうかを指定します。

この設定で [自動調整] を指定した場合、[アコーディオン] オプションを選択して生成したレポートで、表示されるコンテナのサイズに合わせてデータ表示のサイズが自動的に変更され、最大データ値または列タイトルのサイズに基づいて列幅が自動的に調整されます。これがデフォルト値です。

この設定で [レガシー] を指定した場合、[アコーディオン] オプションを選択して生成したレポートで、表示されるコンテナのサイズに合わせてデータ表示のサイズが自動的に変更されず、列幅も自動的に調整されません。

グローバル設定でのキャッシュの有効化

InfoAssist でキャッシュオプションを使用すると、Analytic Document フォーマットを使用したレポート出力の先頭ページのみをブラウザに送信し、後続のページを WebFOCUS Reporting Server の一時キャッシュから取得することが可能になります。キャッシュは、ローカルで InfoAssist の [Analytic Document オプション] ダイアログボックスの [詳細] タブから有効にすることができます。WebFOCUS 管理コンソールで関連する [InfoAssist のプロパティ] の設定を構成することで、キャッシュオプションをグローバルに有効化することができます。InfoAssist でのこれらの設定の影響についての詳細は、『TIBCO WebFOCUS InfoAssist 利用ガイド』の「キャッシュオプションの使用」を参照してください。

手順　InfoAssist のプロパティでキャッシュを有効化するには

管理コンソールの設定を使用して InfoAssist のキャッシュをグローバルに有効化するには、次の手順を実行します。

1. 管理コンソールを開きます。
2. [構成] タブで [InfoAssist のプロパティ] をクリックします。
3. [InfoAssist のプロパティ] ページの [ツールオプションダイアログのデフォルト] セクションで、次の手順を実行します。
   a. [Web ビューアを有効にする] 設定で、[はい] のチェックをオンにします。
   b. [キャッシュから取得する行数] 設定で、デフォルト値の 100 を受容するか、ユーザ要件に適合する別の値を入力します。
4. ページ下部の [保存] をクリックします。
5. 変更が保存されたことを示すメッセージで [OK] をクリックします。

手順　キャッシュ構成を検証するには

InfoAssist が、管理コンソールで構成したグローバル設定を使用することを確認するためには、次の手順を実行します。

1. InfoAssist を起動して、レポートを新規作成するか、既存のレポートを編集します。
2. [ホーム] タブの [フォーマット] グループで、[出力ファイルフォーマット] リストをクリックし、[Analytic Document] または [Analytic PDF] を選択します。
3. [フォーマット] タブをクリックします。
4. [ナビ] グループで、[Web ビューア] オプションがハイライト表示されていることを確認します。

5. [機能] グループで、[Analytic Document オプション] を選択します。
6. [Analytic Document オプション] ダイアログボックスで、[詳細] をクリックします。
7. [取得行数] テキストボックスの値と、管理コンソールの [キャッシュから取得する行数] 設定で受容した値または入力した値を比較します。

   これら 2 つの値が一致する場合、管理コンソールの構成が正常に更新されています。一致しない場合は、管理コンソールの設定の構成を確認してください。

参照 InfoAssist ファイルオプションの理解

InfoAssist ユーザが HOLD ファイルを作成して保存する際に選択可能なファイルタイプを設定します。

バイナリ
レポートまたはグラフのデータをバイナリ値として数値フィールドに格納します。バイナリファイルには、.ftm 拡張子が使用されます。

FOCUS
レポートまたはグラフのデータを、FOCUS データベースの要件に適合するセグメント構造にテキストとして格納します。FOCUS ファイルには、.foc 拡張子が使用されます。

フィールド名付きカンマ区切りテキストファイル
レポートまたはグラフのデータをフィールド順にテキストとして格納します。文字フィールドは引用符で囲まれます。各フィールドはカンマ (,) で区切られ、フィールド名が先頭行に挿入されます。フィールド名付きカンマ区切りテキストファイルには、.csv 拡張子が使用されます。

テキスト
レポートまたはグラフのデータをフィールド順にテキストとして格納しますが、区切り文字およびフィールド名は挿入されません。テキストファイルには、.ftm 拡張子が使用されます。

タブ区切り
レポートまたはグラフのデータをフィールド順にテキストとして格納します。各フィールドは、タブ文字で区切られます。タブ区切りテキストファイルには、.tab 拡張子が使用されます。

フィールド名付きタブ区切りテキストファイル
レポートまたはグラフのデータをフィールド順にテキストとして格納します。各フィールドはタブ文字で区切られ、フィールド名が先頭行に挿入されます。フィールド名付きタブ区切りテキストファイルには、.tab 拡張子が使用されます。

データベーステーブル

レポートまたはグラフのデータを、SQL データベースフォーマットに適合するフィールド構造にテキストとして格納します。データベーステーブルファイルには、.sql 拡張子が使用されます。

データベーステーブル出力は、SQL データベースに対して実行する場合にのみ使用できます。

HYPERSTAGE

レポートまたはグラフのデータを、Hyperstage データベーステーブルフォーマットに適合するフィールド構造にテキストとして格納します。Hyperstage ファイルには、.bht 拡張子が使用されます。

Hyperstage 出力は、WebFOCUS Reporting Server で Hyperstage アダプタが構成されている場合にのみ使用できます。

SQL スクリプト

レポートまたはグラフのデータを、SQL データベースフォーマットに適合するデータベーステーブルにインポート可能なシーケンシャルフィールド構造にテキストとして格納します。SQL スクリプトファイルには、.sql 拡張子が使用されます。

SQL スクリプト出力は、SQL データベースに対して実行する場合にのみ使用できます。

XML

レポートまたはグラフのデータを、XML (Extensible Markup Language) の規則に適合するフィールド構造にテキストとして格納します。各フィールドは、コンテンツを識別するタグで区切られます。XML ファイルには、.xml 拡張子が使用されます。

JSON

レポートまたはグラフのデータを、JSON (JavaScript Object Notations) の規則に適合する構造にテキストとして格納します。JSON ファイルは拡張子 .json を使用します。

参照　InfoAssist グラフタイプオプションの理解

Leaflet マップ

InfoAssist のグラフモードおよびビジュアライゼーションモードで Leaflet マップを使用する際に必要なアイコンを有効にします。2 つの Leaflet マップアイコンを有効にすると、モバイル対応インタラクティブマップ用の Leaflet オープンソース JavaScript ライブラリに基づいて、コロプレスマップまたはプロポーショナルシンボル (バブル) マップが選択可能になります。

グラフモードでは、これらのアイコンは [グラフの選択] ダイアログボックスに表示されます。このダイアログボックスを開くには、[フォーマット] タブの [グラフタイプ] グループで [その他] をクリックします。[グラフの選択] ダイアログボックスで、[マップ] をクリックします。

ビジュアライゼーションモードでは、これらのアイコンは [ビジュアルの選択] ダイアログボックスに表示されます。このダイアログボックスを開くには、[ホーム] タブの [ビジュアル] グループで [変更] をクリックします。

この設定が選択されていない場合、Leaflet マップのアイコンは上記のいずれにも表示されません。デフォルト値はオンです。

参照 InfoAssist オートドリルダウンプロパティの理解

このセクションの各種設定を使用して、オートドリルダウン機能の一部であるドリルダウンナビゲーションの各オプションを有効にします。

シングルクリックナビゲート

シングルクリックナビゲートの使用を有効にします。シングルクリックナビゲートを有効にした場合、レポートまたはグラフの最上位のエントリまたは機能を 1 回クリックした際に、ディメンションの次のレベルに自動的にドリルダウンします。

デフォルト設定では、このチェックはオフです。この設定では、シングルクリックナビゲートが無効になり、最上位オートドリルダウンのエントリまたは機能を 1 回クリックした際に、ドリルダウンメニューが表示されます。このチェックをオンにすると、シングルクリックナビゲートが有効になり、最上位オートドリルダウンのエントリまたは機能を 1 回クリックした際に、ドリルダウンメニューが表示されずにレポートまたはグラフが自動的にリフレッシュされ、選択したディメンションの次のレベルに基づいて結果が表示されます。

階層リンク

オートドリルダウンを有効にしたレポートまたはグラフの最上部に階層リンクを表示します。

デフォルト設定では、このチェックはオンです。この設定では、オートドリルダウンを有効にしたレポートまたはグラフに階層リンクが表示されます。このチェックをオフにすると、オートドリルダウンを有効にしたレポートまたはグラフに階層リンクは表示されません。

オートドリルダウンを有効にしたレポートまたはグラフでは、ディメンションのレベル間をドリルダウンした際に、現在レベルに到達するまでに通過した各レベルが一連のリンクとして階層リンクに表示されます。

[元に戻す] オプション

ドリルダウンメニューの [元に戻す] オプションの表示を有効にします。

デフォルト設定では、このチェックはオンです。この設定では、ドリルダウンメニューに [元に戻す] オプションが表示されます。このチェックをオフにすると、ドリルダウンメニューに [元に戻す] オプションは表示されません。

オートドリルダウンを有効にしたレポートまたはグラフで [元に戻す] オプションを選択すると、元のレポートに直接戻ることができます。

ドリルアップ

ドリルダウンメニューの [ドリルアップ] オプションの表示を有効にします。

デフォルト設定では、このチェックはオンです。この設定では、ドリルダウンメニューに [ドリルアップ] オプションが表示されます。このチェックをオフにすると、ドリルダウンメニューに [ドリルアップ] オプションは表示されません。

オートドリルダウンを有効にしたレポートまたはグラフで [ドリルアップ] オプションを選択すると、選択したディメンションの現在レベルから 1 つ上のレベルに基づく結果で表示が更新されます。

ドリルダウン

ドリルダウンメニューの [ドリルダウン] オプションの表示を有効にします。

デフォルト設定では、このチェックはオンです。この設定では、ドリルダウンメニューに [ドリルダウン] オプションが表示されます。このチェックをオフにすると、ドリルダウンメニューに [ドリルダウン] オプションは表示されません。

オートドリルダウンを有効にしたレポートまたはグラフで [ドリルダウン] オプションを選択すると、選択したディメンションの現在レベルから 1 つ下のレベルに基づいて出力結果が更新されます。

注意：この設定のチェックをオフにすると、[ドリルダウン] オプションが無効になるとともに、レポートおよびグラフの最上位エントリからのハイパーリンク、および階層リンクも表示されなくなります。また、[シングルクリックナビゲート] 設定のチェックがオフの場合に、[ドリルダウン] 設定のチェックもオフにすると、オートドリルナビゲートツールが実質的に無効になり、最上位ディメンション値のみが表示されたレポートまたはグラフが生成されます。[シングルクリックナビゲート] 設定のチェックをオンにし、レポートまたはグラフの最上位から下のレベルにエントリが含まれている場合、[ドリルダウン] 設定のチェックをオフにした場合でも、シングルクリックナビゲート機能により、これらの下位エントリに移動します。ただし、この設定によりドリルダウンメニューが表示されなくなるため、ユーザがレポートまたはグラフを元のレベルに戻すことも、上位にドリルアップすることもできなくなります。

参照 **InfoAssist その他オプションの理解**

2 部構成ファイル名の使用
: このオプションを選択した場合、マスターファイルディレクトリへのパスを含めた 2 部構成ファイル名を使用する必要があります。このオプションを選択しない場合、1 部構成ファイル名を使用する必要があります。デフォルト値はオンです。

データソースツリーを展開する
: データソースツリーを初期表示で展開するか、折りたたむかを指定します。このチェックをオンにした場合、ツリーは展開されて表示されます。このチェックをオフにした場合、ツリーは折りたたまれて表示されます。デフォルト値はオンです。

JOIN ツール
: InfoAssist の [データ] タブに、[JOIN] メニューオプションを表示します。このチェックをオフにした場合、[データ] タブに [JOIN] メニューオプションは表示されません。デフォルト値はオンです。

レイアウトタブ
: InfoAssist リボンの [レイアウト] タブを有効にします。このチェックをオフにした場合、InfoAssist リボンに [レイアウト] タブは表示されません。デフォルト値はオンです。

シリーズタブ
: InfoAssist リボンの [シリーズ] タブを有効にします。[シリーズ] タブは、グラフおよびビジュアライゼーションを作成する場合に表示されます。[プロパティ]、[折れ線]、[円] の各メニューのグラフ作成プロパティおよびオプションにアクセスできます。このチェックをオフにした場合、InfoAssist リボンに [シリーズ] タブは表示されません。デフォルト値はオンです。

パスの適用を有効にする

: [パスの適用] コンテナ  のデフォルト条件を設定します。[パスの適用] コンテナは、InfoAssist アプリケーションウィンドウの [リソース] パネルの [データ] ウィンドウ上部に表示されます。

  [データ] ウィンドウのフィールドを [クエリ] ウィンドウのフィールドコンテナに移動すると、パスの適用によって、データソースツリーで使用可能なフィールドの表示が、フィールドコンテナに移動したフィールドへのマルチパスリレーションシップに基いて、有効な論理接続が設定されたフィールドに自動的に制限されます。

  このチェックをオフにすると、この設定のデフォルト値 [パスの適用] コンテナがデフォルト設定で無効になります。この条件では、ユーザがフィールドを [クエリ] ウィンドウのフィールドコンテナに移動した場合も、データソースツリーの使用可能なフィールドの表示が変更されません。InfoAssist のセッションでは、ユーザは [パスの適用] コンテナをクリックすることでパスの適用を有効にすることができます。

このチェックをオンにすると、[パスの適用] コンテナがデフォルト設定で有効になります。この条件では、[クエリ] ウィンドウのフィールドコンテナに移動したフィールドに論理接続されていないデータソースツリーのフィールドは、淡色表示になり、使用できなくなります。InfoAssist のセッションでは、ユーザは [パスの適用] コンテナをクリックすることでパスの適用を無効にすることができます。

注意：新しいプロシジャを保存すると、[パスの適用] コンテナに設定された条件がこのプロシジャに保存されます。このプロシジャを InfoAssist アプリケーションウィンドウで再度開くと、[パスの適用] コンテナの条件が、[パスの適用を有効にする] 設定で指定した値ではなく、プロシジャに保存された値で設定されます。

InfoAssist Basic のプロパティ

インストールに InfoAssist Basic ライセンスのみが付与されている場合、InfoAssist のプロパティは次の設定に限定されます。

[フォーマット] タブ

- その他の HTML (グラフ)
- その他の PDF (グラフ)
- Excel (EXL2K)
- Excel Formula (EXL2K FORMULA)
- Excel (XLSX)
- Excel Formula (XLSX FORMULA)
- Excel Pivot (EXL2K PIVOT)

オートドリルダウン

- シングルクリックナビゲート
- 階層リンク
- [元に戻す] オプション
- ドリルアップ
- ドリルダウン

その他

- 2 部構成ファイル名の使用

B

ログの収集

ここでは、セキュリティイベントの監査ログへのアクセス方法および監査ログの意味について説明します。

トピックス

ログファイルおよびトレースファイルの日単位の保守

ログファイルおよびトレースファイルには、短期間で大量のデータが蓄積される場合があります。これらのファイルが増加すると、ストレージやオペレーショナルリソースの必要量が増大し、検索や調査に長時間を要します。そのため、ほとんどのクライアントは、一定期間のログファイルおよびトレースファイルのみを保持します。

このバックログを最小にするために、一定期間が経過した後にログファイルおよびトレースファイルが自動的に削除されます。これらの期間は、[ログ削除までの日数] (IBI_LOG_RETAIN_DAYS) および [トレース削除までの日数] (IBI_TRACE_RETAIN_DAYS) で定義されます。両方の設定のデフォルト保持期間は 10 日ですが、1 から 3650 までの任意の値を割り当てることで、保持期間を変更することができます。これらの設定は、管理コンソールの [構成] タブの [アプリケーションディレクトリ] ページに表示されます。

特定のログファイルまたはトレースファイルの保持期間を計測するために、ファイルに最後に記録された日時を識別するためのタイムスタンプが割り当てられます。

毎日午前零時に、タイムスタンプの日付と現在の日付が自動的に比較されます。これらの日付の日数差が上記の設定で定義された日数を超えた場合、期限切れになったログファイルが自動的に削除されます。

たとえば、[ログ削除までの日数] (IBI_LOG_RETAIN_DAYS) 設定に割り当てられた値が 10 日の場合、10 日前の日付より前に作成された audit.log ファイルが自動的に削除されます。この自動確認は、早い場合には午前零時の 1 分前、遅い場合でも午前零時の 1 分後に実行されます。

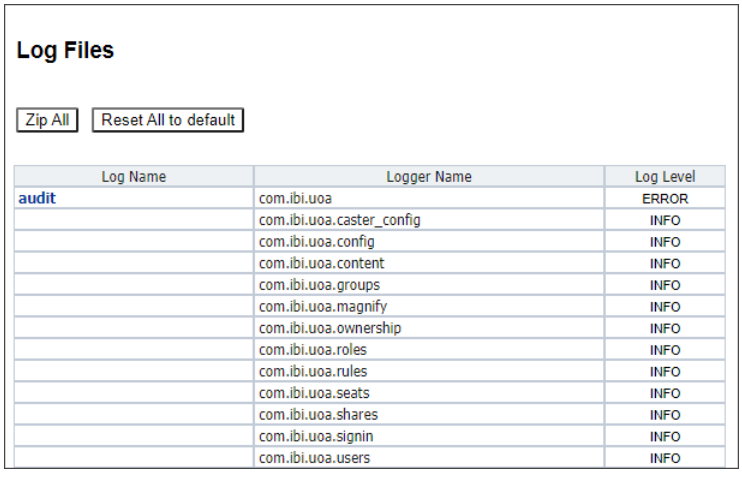
ログファイルおよびトレースファイルの日単位の保守を設定することにより、ログファイルおよびトレースファイルのバックログが大量に蓄積されなくなるとともに、発生した問題や予期しないイベントが記録されたファイルが永続的に保存されなくなります。ログファイルまたはトレースファイルを分析に必要な期間だけ残すには、これらのファイルのコピーを作成し、安全な場所に格納する必要があります。

監査ログの理解

監査ログは、システム管理アクティビティのレコードを収集します。これには、システム構成イベント、ロール、ルール、コンテンツオーナーシップの変更、ユーザ管理アクティビティ、ログインおよびログアウトイベントの記録が含まれます。セキュリティ上の理由から、監査ログは常に有効になっています。

監査ログファイルは、*drive*:¥ibi¥WebFOCUS82¥logs ディレクトリに格納され、割り当てられたロガーで収集されたイベントはすべてこの単一ファイルに記録されます。

監査ファイルへのイベント記録に関与するロガーのリストは、下図のように、管理コンソールの [機能診断] タブの [ログファイル] ページ上部の監査ログ名エントリ横に表示されます。このログのイベント記録に関与する特定のロガー (例、com.ibi.uoa.roles) は、情報 (INFO) レベルのルーチンイベントを収集します。主要ロガーの com.ibi.uoa は、エラー (ERROR) レベルのその他非特殊イベントを収集します。



log4j2.xml ファイル (*drive*:¥ibi¥WebFOCUS_WFI¥WebFOCUS¥webapps¥webfocus¥WEB-INF¥classes) には、各ログで収集されるログ記録のフォーマットと範囲を定義するロガーおよびアペンダのデフォルト構成が含まれます。[ログファイル] ページのログ名およびロガーの表示は、このファイルの構成に基づきます。

監査ログは、管理コンソールの構成タブの [アプリケーションディレクトリ] ページの [ログ削除までの日数] (IBI_LOG_RETAIN_DAYS) 設定で定義された日数だけ保持されます。デフォルト設定で、監査ログは 10 日間保持されます。この設定で定義された日数を変更することで、ログの保存期間をカスタマイズすることができます。ただし、この設定への変更は、監査ログだけでなくすべてのログの保持日数に影響することに注意してください。

手順　監査ログにアクセスするには

監査ログを表示するには、管理コンソールへのアクセス権限を所有する管理ユーザとしてログインする必要があります。

1. 管理コンソールで [機能診断] タブをクリックします。
2. [機能診断] フォルダ下の [ログファイル] をクリックします。
3. [ログファイル] ページの [ログ名] 列で、[audit] リンクをクリックします。

   [audit.log] ページが開きます。

   各エントリは、ログイベントが発生した日時の古い順から新しい順に表示されます。

   - ログイベントの発生日時の新しいエントリを確認するには、下方向へスクロールします。
   - 最新のエントリに直接移動するには、[最下行へ] をクリックします。
   - このログファイルを開いた時点より後に発生したシステムログイベントのエントリを表示するには、[新規トレース行] をクリックします。
4. 以前の日付の監査ログを確認するには、ページ上部の最新監査ログファイルのドロップダウンリストから、その日付のログを選択します。

   デフォルト設定で、ログは 10 日間保持されます。この保持期間は、[構成] タブの [アプリケーションディレクトリ] ページの [ログ削除までの日数] (IBI_Log_Retain_Days) 設定で定義された値に基づいて決定されます。

監査ログ構成のカスタマイズ

log4j2.xml ファイルで定義されたログファイルのデフォルト構成は、ほとんどの製品インストールをサポートするよう設定されています。管理者は、この構成を変更して、1 つまたは複数の監査ファイルロガーが収集したイベントを、組織の要件に準拠するよう、デフォルト構成で定義されていない別のログファイルまたはデータベーステーブルにリダイレクトすることができます。

たとえば、ログインイベントとセキュリティイベントを別のデータベーステーブルにリダイレクトする場合は、次の情報を収集します。

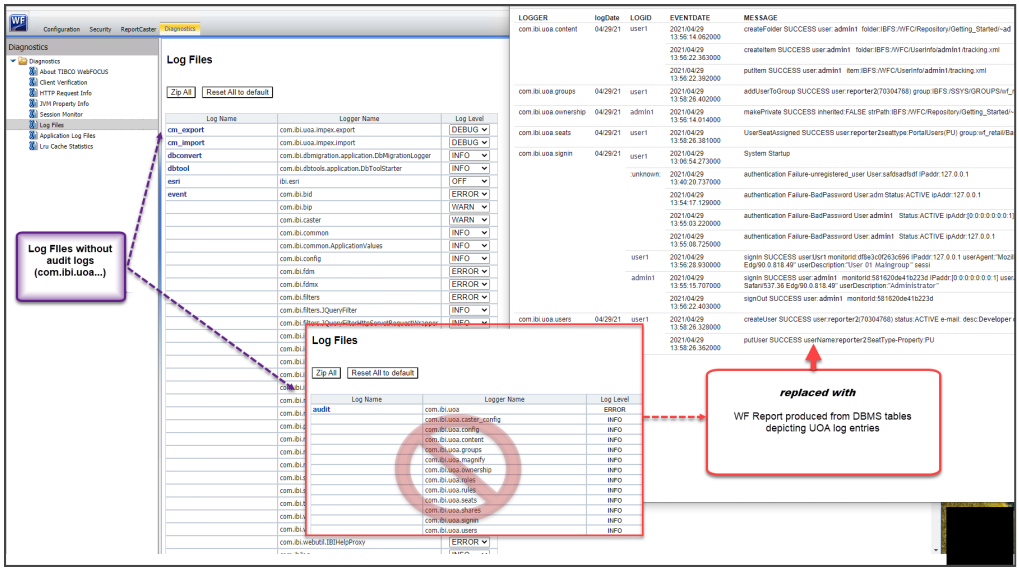
- ログインおよびログアウトの試行
- ユーザの作成、変更、削除
- グループへのユーザの割り当てまたはグループからのユーザの削除

log4j2.xml ファイル自体に加えた変更により、管理コンソールの [ログファイル] ページに表示されるログファイル名および関連するロガーの構成がクリアされます。そのため、必要に応じてこの表示を復元できるよう、log4j2.xml ファイルに変更を加える前にこのファイルのバックアップコピーを作成することをお勧めします。詳細は、609 ページの 「 log4j2.xml ファイルのコピーを作成するには 」 を参照してください。

バックアップコピーを作成後、log4j2.xml 構成ファイルのコピー専用のアペンダおよびロガーを追加することで、ログインイベントの記録を別のログファイルにリダイレクトすることができます。詳細は、610 ページの 「 監査ログイベントを別のログファイルにリダイレクトするには 」 を参照してください。

データベーステーブルのレコードをリダイレクトする場合は、log4j2.xml ファイルのコピー専用のアペンダとロガーを追加する以外に、ターゲットデータベース内にレコードを収集するための専用テーブルを作成する必要があります。詳細は、611 ページの 「 監査ログイベントを別のデータベーステーブルにリダイレクトするには 」 を参照してください。

[ログファイル] ページのロガー表示の代わりに、下図のように、データベースレポートを作成し、*drive*:¥ibi¥WebFOCUS_WFI¥WebFOCUS¥logs ディレクトリに保存されたログファイルに直接接続することができます。



手順　log4j2.xml ファイルのコピーを作成するには

ログファイル構成への変更が必要な場合、この手順の説明に従って、log4j2.xml ファイルのバックアップコピーを最初に作成しておくことをお勧めします。

1. 現在のファイルシステムで、*drive*:¥ibi¥WebFOCUS¥webapps¥webfocus¥WEB-INF¥classes に移動します。
2. log4j2.xml ファイルをコピーし、これを同一ディレクトリに貼り付けます。

   注意

   - 作成したコピーに拡張子 xml を保持するように注意します。
   - 製品のインストール時にも、log4j2.xml.backup ファイルがフェイルセーフとしてこのディレクトリに追加されます。このファイルを変更または削除しないでください。
3. log4j2.xml ファイルのコピーに新しい名前を割り当てます。

手順　別のログファイルに含める監査ログイベントを特定するには

617 ページの 「 セキュリティイベントの理解 」 の表に示されたロガーを確認し、別のファイルに転送する必要があるログメッセージを収集するロガーを特定します。

たとえば、com.ibi.uoa.signin というロガーは、ログイン、ログアウト、セッションタイムアウトイベントのレコードを収集します。ログインイベントを別のログファイルまたはデータベーステーブルに保存する場合は、このロガーの更新が必要です。

注意：複数のロガーから同一ファイルにイベントをリダイレクトする必要がある場合は、これらをすべて選択します。たとえば、ログインイベントとユーザの保守イベントのログレコードを同一ファイルにリダイレクトするには、com.ibi.uoa.signin ロガーと com.ibi.uoa.users ロガーを選択する必要があります。

手順　監査ログイベントを別のログファイルにリダイレクトするには

1. *drive*:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/ に移動します。
2. log4j2.xml ファイルを開き、<Appenders> セクションの <RollingFile name="LOGuoa"> ブロックに移動します。
3. LOGuoa ブロックの終了タグの下に、次のサンプルコードに基づいて新しい RollingFile アペンダを挿入します。これは、アペンダで指定した別のファイルにリダイレクトする監査ログイベントを保存します。

```
<RollingFile name="appendername">
  <FileName>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/logfilename.log</FileName>
  <FilePattern>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/messagepattern-%d{yyyy-
MM-dd}-%i.log</FilePattern>
    <PatternLayout>
      <Pattern>[%d] %-5p %-16.16c{1} %-16.16X{monitorID} %X{userId} %m
%n</Pattern>
    </PatternLayout>
    <Policies>
      <TimeBasedTriggeringPolicy />
      <SizeBasedTriggeringPolicy size="20 MB" />
    </Policies>
</RollingFile>
```

説明

`appendername`
新しいアペンダの名前です。新しいファイルにリダイレクトされるログメッセージのタイプを識別する名前を使用します。たとえば、ログインロガーで収集されたメッセージには、signinout.log を使用します。

`logfilename`
リダイレクトされたログメッセージを格納する新しいログファイルの名前です。

`messagepattern`
このアペンダを使用するロガーが収集するログメッセージのパターンです。

次のサンプルコードでは、com.ibi.uoa.signin ロガーで収集されたイベントが、signinout.log という名前の別のログファイルにリダイレクトされます。

```
<RollingFile name="LOGuoaSignInOut">
  <FileName>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout.log</FileName>
  <FilePattern>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout-%d{yyyy-MM-
dd}-%i.log</FilePattern>
    <PatternLayout>
      <Pattern>[%d] %-5p %-16.16c{1} %-16.16X{monitorID} %X{userId} %m
%n</Pattern>
    </PatternLayout>
    <Policies>
      <TimeBasedTriggeringPolicy />
      <SizeBasedTriggeringPolicy size="20 MB" />
    </Policies>
</RollingFile>
```

4. リダイレクトするログメッセージを収集する各ロガーの名前を検索します。
5. AppenderRef タグの ref 属性の値を、新しいアペンダの名前で置換し、アペンダ参照のターゲットとして作成した新しいアペンダブロックを指定します。以下はその例です。

```
<logger name="logger" level value="info" additivity="false">
  <AppenderRef ref="appender"/>
</logger>
```

説明

`logger`
通常監査ログに割り当てられるメッセージを収集するロガーの名前です (例、com.ibi.uoa.signin)。

`appender`
選択したロガーから新しいログファイルにメッセージをリダイレクトする新しいアペンダの名前です。

次の例では、name="com.ibi.uoa.signin" ロガーにより、アペンダ参照のターゲットとして新しい LOGuoaSignInOut アペンダブロックが指定されます。

```
<logger name="com.ibi.uoa.signin" level value="info" additivity="false">
  <AppenderRef ref="LOGuoaSignInOut"/>
</logger>
```

6. ファイルを保存します。

ログイベントが、新しいアペンダで指定したログファイルに記録されます。たとえば、ログインイベントが signinout.log ファイルに記録されます。

手順　監査ログイベントを別のデータベーステーブルにリダイレクトするには

1. 監査ログ情報の格納に使用するデータベーステーブルを作成します。テーブルには、ログで収集する情報に適切なフィールドを含める必要があります。

たとえば、ユーザ ID、日付時間スタンプ、ロガー名、ログイン監査イベント、ログアウト監査イベント、セッション終了イベントを収集するテーブルを、PostgreSQL データベース用に準備された次のコードで作成することができます。

```
CREATE TABLE public.wf_log
(
    eventdate timestamp with time zone,
    logger character varying(128) COLLATE pg_catalog."default",
    level character varying(12) COLLATE pg_catalog."default",
    logid character varying(128) COLLATE pg_catalog."default",
    message character varying(255) COLLATE pg_catalog."default",
    exception text COLLATE pg_catalog."default"

GRANT UPDATE, INSERT, SELECT ON TABLE public.wf_log TO webfocus;
```

2. *drive*:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/ に移動します。
3. log4j2.xml ファイルを開き、<Appenders> セクションの <RollingFile name="LOGuoa"> ブロックに移動します。
4. 次の部分コードのいずれかを使用して、log4j2.xml ファイルに JDBC アペンダを追加します。

   a. 接続のコントロールを外部のデータベースに移行する場合は、以下の例の 2 行目に示すように、ConnectionFactory クラスの記述を追加します。

   ```
   <JDBC name="LOGevent" tableName="public.wf_log">
     <ConnectionFactory
       class="com.ibi.log4j2.ConnectionFactory"
       method="getConnection" />
     <Column name="eventdate" isEventTimestamp="true" />
     <Column name="logger" pattern="%logger" isUnicode="false" />
     <Column name="level" pattern="%level" isUnicode="false" />
     <Column name="logid" pattern="%X{userId}" isUnicode="false" />
     <Column name="message" pattern="%message" isUnicode="false" />
     <Column name="exception" pattern="%ex{full}" isUnicode="false" />
   </JDBC>
   ```

   説明

   `LOGevent`
   このロガーで収集したイベントを外部のデータベーステーブルにリダイレクトする JDBC アペンダの名前です (例、LOGuoa)。

   `logger`
   通常監査ログに割り当てられるメッセージを収集する既存ロガーの名前です (例、com.ibi.uoa.signin)。

   b. 接続のコントロールを WebFOCUS 内に保持する場合は、以下の例の 2 行目に示すように、DriverManager タグを追加します。

```
<JDBC name="LOGevent" tableName="public.wf_log">
  <DriverManager
    connectionString="jdbc:postgresql://localhost:5432/WebFOCUS82"
    driverClassName="org.postgresql.Driver"
    username="webfocus"
    password="webfocus" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>
```

説明

LOGevent
: このロガーで収集したイベントを外部のデータベーステーブルにリダイレクトする JDBC アペンダの名前です (例、LOGuoa)。

logger
: 通常監査ログに割り当てられるメッセージを収集する既存ロガーの名前です (例、com.ibi.uoa.signin)。

5. 情報の記録先を指定し、追加する各既存ロガーの名前にアペンダ参照を追加します。

- ログ情報を外部データベースのみに格納するには、次のコードを使用します。

```
<Logger name="logger" level="info" additivity="false">
   <AppenderRef ref="LOGevent"/>
</Logger>
```

説明

logger
: 通常監査ログに割り当てられるメッセージを収集する既存ロガーの名前です (例、com.ibi.uoa.signin)。

LOGevent
: このロガーで収集したイベントを外部のデータベーステーブルにリダイレクトする JDBC アペンダの名前です (例、LOGuoa)。

- ログ情報を WebFOCUS と外部データベースの両方に格納するには、次のコードを使用します。

```
<Logger name="logger" level="info" additivity="false">
  <AppenderRef ref="LOGevent"/>
  <AppenderRef ref="LOGdb"/>
</Logger>
```

説明

`logger`
通常監査ログに割り当てられるメッセージを収集する既存ロガーの名前です (例、com.ibi.uoa.signin)。

`LOGevent`
このロガーで収集したイベントを外部のデータベーステーブルにリダイレクトする JDBC アペンダの名前です (例、LOGuoa)。

`LOGdb`
このロガーで収集したイベントを外部のデータベーステーブルにリダイレクトする JDBC アペンダの名前です。

6. Application Server で *drive*:/ibi/WebFOCUS82/webapps/webfocus/webfocus.war ファイルが展開されている場合は、webfocus.war ファイルを更新し、再展開します。
7. *drive*:/ibi/ WebFOCUS82/webapps/webfocus 拡張ディレクトリが展開されている場合は、WebFOCUS Application Server を再起動します。

   下図のように、セキュリティイベントがデータベーステーブルの各行に収集されます。

	USERID	DATETIME	LOGGER	MESSAGE
1	admin	2012-01-11 22:09:53,115	com.ibi.uoa.signin	signIn SUCCESS user:admin monitorId:666c011363cd9...
2	admin	2012-01-11 22:12:37,727	com.ibi.uoa.signin	signIn SUCCESS user:admin monitorId:6987fff8443e8d...
3	admin	2012-01-11 22:13:14,743	com.ibi.uoa.users	createUser SUCCESS user:shawshank (2065653048) s...
4	admin	2012-01-11 22:13:34,415	com.ibi.uoa.users	deleteUser SUCCESS user:abcdefghi (2065532905) sta...
5	admin	2012-01-11 22:16:31,058	com.ibi.uoa.signin	signIn SUCCESS user:admin monitorId:6f9fcb1e85c6f3...

手順　ログインイベントを別のログファイルに保存するには

1. *drive*:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/ に移動します。
2. log4j2.xml ファイルを開き、<Appenders> セクションの <RollingFile name="LOGuoa"> ブロックに移動します。
3. LOGuao ブロックの終了タグの下に、次の新しい RollingFile タグを挿入します。これは、ログインイベントを、signinout.log という名前のファイルに保存します。以下はこのサンプルコードを示しています。

```
<RollingFile name="LOGuoaSignInOut">
  <FileName>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout.log</FileName>
  <FilePattern>C:/ibi/WebFOCUS_WFI/WebFOCUS/logs/signinout-%d{yyyy-MM-
dd}-%i.log</FilePattern>
    <PatternLayout>
      <Pattern>[%d] %-5p %-16.16c{1} %-16.16X{monitorID} %X{userId} %m
%n</Pattern>
    </PatternLayout>
    <Policies>
      <TimeBasedTriggeringPolicy />
      <SizeBasedTriggeringPolicy size="20 MB" />
    </Policies>
</RollingFile>
```

4. このファイル内で logger name="com.ibi.uoa.signin" を検索し、アペンダ参照のターゲットとして新しい LOGuoaSignInOut アペンダブロックを指定するようエントリを更新します。以下はその例です。

```
<logger name="com.ibi.uoa.signin" level value="info" additivity="false">
  <AppenderRef ref="LOGuoaSignInOut"/>
</logger>
```

5. ファイルを保存します。

   これで、ログインイベントが signinout.log ファイルに記録されます。

手順　ログインイベントを別のデータベーステーブルに保存するには

1. 使用するデータベースに、ログインイベントレコードを収集するための新しいテーブルを作成します。以下は、PostgreSQL データベースの例を示しています。

```
CREATE TABLE public.wf_log
(
    eventdate timestamp with time zone,
    logger character varying(128) COLLATE pg_catalog."default",
    level character varying(12) COLLATE pg_catalog."default",
    logid character varying(128) COLLATE pg_catalog."default",
    message character varying(255) COLLATE pg_catalog."default",
    exception text COLLATE pg_catalog."default"

GRANT UPDATE, INSERT, SELECT ON TABLE public.wf_log TO webfocus;
```

2. *drive*:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/ に移動します。
3. テキストエディタで、*drive*:/ibi/WebFOCUS82/webapps/webfocus/WEB-INF/classes/log4j2.xml ファイルのコピーを開きます。
4. <Appenders> セクションの <RollingFile name="LOGuoa"> ブロックに移動します。
5. LOGuoa ブロックの終了タグの下に、新しい JDBC タグを挿入します。これは、次の例のいずれかを使用して、データベーステーブルにログインイベントを保存します。

接続のコントロールを外部のデータベースに移行するには、以下の例の 2 行目に示すように、ConnectionFactory クラスの記述を含めます。

```
<JDBC name="LOGuoaSignInOut" tableName="public.wf_log">
  <ConnectionFactory
     class="com.ibi.log4j2.ConnectionFactory"
     method="getConnection" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>
```

または

接続のコントロールを WebFOCUS 内に保持するには、以下の例に示すように、DriverManager タグを含めます。

```
<JDBC name="LOGuoaSignInOut" tableName="public.wf_log">
  <DriverManager
    connectionString="jdbc:postgresql://localhost:5432/WebFOCUS82"
    driverClassName="org.postgresql.Driver"
    username="webfocus"
    password="webfocus" />
  <Column name="eventdate" isEventTimestamp="true" />
  <Column name="logger" pattern="%logger" isUnicode="false" />
  <Column name="level" pattern="%level" isUnicode="false" />
  <Column name="logid" pattern="%X{userId}" isUnicode="false" />
  <Column name="message" pattern="%message" isUnicode="false" />
  <Column name="exception" pattern="%ex{full}" isUnicode="false" />
</JDBC>
```

注意：上記の例の「LOGuaoSignInOut」という名前は、任意で別の説明的な名前で置き換えることができます。イベントをこの新しいアペンダにリダイレクトするロガーの AppenderRef タグにもこれと同じ名前を使用する必要があります。

6. name="com.ibi.uoa.signin" タグを含むロガーを検索し、アペンダ参照のターゲットとして新しい LOGevent JDBC クラスを指定するようエントリを更新します。以下はその例です。

```
<Logger name="com.ibi.uoa.signin" level="info" additivity="false">
 <AppenderRef ref="LOGuoaSignInOut"/>
```

注意：上記の例の「LOGuaoSignInOut」という名前は、任意で別の説明的な名前に置き換えることができます。このロガーからイベントを受信するアペンダの名前タグにもこれと同じ名前を使用する必要があります。

7. ファイルを保存します。

ログインイベントが、public.wf_log データベーステーブルに記録されます。

セキュリティイベントの理解

下表は、WebFOCUS で監査用に記録されるセキュリティイベントのタイプを示しています。

イベントの対象	イベントの説明	記録される変更タイプ	log4j.xml 内のロガー名
config	構成	webfocus.cfg ファイルに追加された変更、ライセンスの変更	com.ibi.uoa.config
content	コンテンツ	作成、更新、削除	com.ibi.uoa.content
groups	グループ	作成、更新、削除	com.ibi.uoa.groups
ownership	オーナーシップ	リソースオーナーの変更	com.ibi.uoa.ownership
roles	ロール	作成、更新、削除	com.ibi.uoa.roles
rules	ルール	作成、更新、削除	com.ibi.uoa.rules
shares	共有	共有、共有先	com.ibi.uoa.shares
signin	ログイン	ログイン、ログアウト、期限切れセッション	com.ibi.uoa.signin
users	ユーザ	作成、更新、削除、グループへの追加、グループからの削除	com.ibi.uoa.users

構成イベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「config」で示された構成イベント。
- アクションを実行したユーザのモニタ ID。

- 記録された特定のイベント。この場合は「configUpdate」で示された構成の更新。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- 影響を受けたファイル名 (通常は webfocus.cfg)。
- アクションを実行したユーザの名前。
- 変更されたプロパティの新しい値。
- 変更されたプロパティの古い値。

イベント	ログエントリ
webfocus.cfg の変更	`[YYYY-MM-DD hh:mm:ss,sss] INFO config monitor_ID user_ID updateConfig {SUCCESS|FAILURE} file:file_name user:user_ID parameterName:parameter_name newValue:new_value oldValue:old_value`
ライセンスキーの変更	`[YYYY-MM-DD hh:mm:ss,sss] INFO config monitor_ID user_ID updateConfig {SUCCESS|FAILURE} file:license_key_file user:user_ID parameterName:parameter_name newKey:new_value newSite:site_code`

コンテンツイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「content」で示されたコンテンツイベント。
- アクションを実行したユーザのモニタ ID。
- 特定のイベント (例、createFolder、putItem)。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- アクションを実行したユーザの名前。
- アクションの影響を受けたコンテンツの場所。
- アクションによって変更されたフィールド。

イベント	ログエントリ
フォルダの作成	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID createFolder {SUCCESS|FAILURE} user:user_ID folder:IBFS_address
フォルダ詳細の変更	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID putFolderProperties {SUCCESS|FAILURE} user:user_ID folder:IBFS_address
フォルダの削除	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID delete {SUCCESS|FAILURE} user:user_ID folder:IBFS_address
フォルダの複製作成、フォルダのコピーと貼り付け	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID copyFolder {SUCCESS|FAILURE} user:user_ID srcitem: IBFS_address dstitem:IBFS_address_copy [YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_IDuser_ID putFolderProperties {SUCCESS|FAILURE} user:user_ID folder:IBFS_address
フォルダの移動	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID moveFolder {SUCCESS|FAILURE} user:user_ID srcitem:old_IBFS_address dstitem:new_IBFS_address
フォルダの名前変更	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID putFolderProperties {SUCCESS|FAILURE} user:user_ID folder:new_IBFS_address
項目の作成	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID createItem {SUCCESS|FAILURE} user:user_ID folder:IBFS_address
項目詳細の変更	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID putItem {SUCCESS|FAILURE} user:user_ID item:IBFS_address
項目の削除	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID delete {SUCCESS|FAILURE} user:user_ID item:IBFS_address

イベント	ログエントリ
項目の複製作成、項目のコピーと貼り付け	[YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID copyItem {SUCCESS|FAILURE} user:user_ID srcitem:old_IBFS_address dstitem:new_IBFS_address [YYYY-MM-DD hh:mm:ss,sss] INFO content monitor_ID user_ID putItemProperties {SUCCESS|FAILURE} user:user_ID folder:IBFS_address

グループイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「groups」で示されたグループイベント。
- アクションを実行したユーザのモニタ ID。
- アクションの説明 (例、createGroup、putGroup)
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- アクションの影響を受けたグループの名前および一意の数値 ID。
- アクションによって変更されたフィールド。

各ユーザおよびグループは、それぞれの名前以外に、一意の数値 ID で識別されます。

イベント	ログエントリ
グループの作成	[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID createGroup {SUCCESS|FAILURE} name:group_name (group_ID) parent:group_parent (parent_group_ID) desc:group_description extGrp:external_group_mappings
グループの削除	[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID deleteGroup {SUCCESS|FAILURE} group:IBFS_address (group_ID) users-autoremoved:number_of_group_members

イベント	ログエントリ
グループ説明の変更	[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID putGroup {SUCCESS|FAILURE} groupPath:IBFS_address (group_ID) newdesc:new_description olddesc:old_description externalGroups:external_group_mappings
グループの名前変更	[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID renameGroup {SUCCESS|FAILURE} name:group_name (group_ID) parent:parent_group oldName:old_group_name
グループへのユーザの追加	[[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID addUserToGroup {SUCCESS|FAILURE} user:user_IDgroup:group_name (group_ID)
グループからのユーザの削除	[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID removeUserFromGroup {SUCCESS|FAILURE} user:user_ID group:group_name (group_ID)

ReportLibrary アクセスイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- ReportLibrary レポートにアクセスした日時のタイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- スレッド識別子 (http-connector-port_number-exec-ID_number:libaccess 形式)。
- ReportLibrary レポートにアクセスしたユーザ ID。
- ReportLibrary レポートの IBFS フルパス。
- ReportLibrary レポートのタイトル。
- ReportLibrary レポートのバージョン番号。

イベント	ログエントリ
ReportLibrary レポートの表示	[YYYY-MM-DD hh:mm:ss,sss] INFO [Thread Identifier] User_ID – FullPath: IBFS_address ; Description: Library_Report_Title; Version Number: Library_Report_Version_Number

オーナーシップイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「ownership」で示されたログインイベント。
- 実行されたアクション。たとえば、「changeOwner」で示されたオーナーシップの変更や「makePublic」で示された項目の公開。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- 上位リソースからの [プライベート] ステータスの継承の有無。
- リソースの IBFS フルパス。
- 新しいリソースオーナーのユーザ ID。
- オーナーのタイプ。グループは「G」、ユーザは「U」で示されます。

イベント	ログエントリ
グループへのオーナー変更	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership monitor_ID user_ID makeManaged {SUCCESS|FAILURE} inherited:{TRUE|FALSE} strPath:IBFS_address ownerName:owner_group_name ownerType:G
ユーザへのオーナー変更	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership monitor_ID user_ID changeOwner {SUCCESS|FAILURE} inherited:{TRUE|FALSE} strPath:IBFS_address ownerName:owner_user_ID ownerType:U

イベント	ログエントリ
フォルダまたは項目のプライベート化	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership monitor_ID user_ID makePrivate {SUCCESS|FAILURE} strPath:IBFS_address ownerName:new_owner ownerType:U
フォルダまたは項目の公開	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership monitor_ID user_ID makePrivate {SUCCESS|FAILURE} strPath:IBFS_address ownerName:new_owner ownerType:U
フォルダまたは項目の公開の失敗	[YYYY-MM-DD hh:mm:ss,sss] INFO ownership monitor_ID user_ID isPublishable {SUCCESS|FAILURE} inherited:{TRUE|FALSE} ownerName:parent_folder

ReportCaster 構成イベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「caster_config」で示された ReportCaster 構成イベント。
- アクションを実行したユーザのモニタ ID。
- アクションを実行したユーザの名前。
- 影響されるファイルの名前。通常は、古い CasterConfig ファイル。

イベント	ログエントリ
ReportCaster 構成設定の編集および保存	[YYYY-MM-DD hh:mm:ss,sss] INFO caster_config monitor_ID user_ID updated ReportCaster configuration, old CasterConfig file: dserver_file_ID.xml

注意：ReportCaster 構成設定の変更が保存される前に、ReportCaster 構成ツールの以前の設定がタイムスタンプ形式の dserver.xml ファイルに記録されます。このファイルは、...ibi ¥WebFOCUSnn ディレクトリに保存されます。この場合、*nn* は WebFOCUS のバージョン番号です。

ReportCaster グローバル更新イベントの理解

グローバル更新コマンドを使用し、ReportCaster スケジュールおよび特定のスケジュールツールに保存された値のグローバル変更は、globalUpdates ログに記録されます。詳細は、『TIBCO WebFOCUS ReportCaster 利用ガイド』を参照してください。.

下表に記載された各ログエントリは、次の要素で構成されています。

- グローバル更新イベントを開始したユーザ ID。
- グローバル更新でターゲット設定されたデータベーステーブルの名前。
- 更新された変数の名前。
- グローバルに削除された古い値。
- グローバルに追加された新しい値。
- スレッド識別子 (ID_number 形式)。

イベント	ログエントリ
値のグローバル更新	`User_ID database table name variable name old value new value Thread Identifier`

ロールイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「roles」で示されたロールイベント。
- アクションを実行したユーザのモニタ ID。
- アクションを実行したユーザのユーザ ID。
- 特定のイベント (例、createRole)。

- アクションの成功または失敗 (SUCCESS または FAILURE)。
- アクションの影響を受けたロールの名前。
- ロールのポリシー。

イベント	ログエントリ
ロールの作成	`[YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID createRole {SUCCESS|FAILURE} role:role_name (role_ID) desc:description policy:privilege_name:OPERATION;`
ロール詳細の変更	`[YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID putRole {SUCCESS|FAILURE} role:role_name (role_ID) desc:description policy:privilege_name:OPERATION;`
ロールの削除	`[YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID deleteRole {SUCCESS|FAILURE} role:role_name (role_ID) rules-autoremoved:number_rules_using_this_role policy:privilege_name:OPERATION;`
ロールの複製	`[YYYY-MM-DD hh:mm:ss,sss] INFO roles monitor_ID user_ID createRole {SUCCESS|FAILURE} role:role_name_copy (role_ID) desc:description_copy policy:privilege_name:OPERATION;`

ルールイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「rules」で示されたルールイベント。
- アクションを実行したユーザのモニタ ID。
- アクションを実行したユーザのユーザ ID。
- 特定のイベント (例、addGroupRule、addUserRule)。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- ルールの適用先リソースの場所。
- ルールのアクセスポリシー。

- ルールの適用先 (このフォルダのみ、このフォルダの下位のみ、このフォルダとその下位)。

イベント	ログエントリ
グループに対するルールの作成	`[YYYY-MM-DD hh:mm:ss,sss] INFO rules monitor_ID user_IDaddGroupRule {SUCCESS|FAILURE} group_name (group_ID)role:IBFS_address (role_ID) resource:resource_location (resource_ID) verb:operation applyTo:scope`
ユーザに対するルールの作成	`[YYYY-MM-DD hh:mm:ss,sss] INFO rules monitor_ID user_ID addUserRule {SUCCESS|FAILURE} user_ID (numeric_user_ID) role:IBFS_address (role_ID) resource:resource_location (resource_ID) verb:operation applyTo:scope`

共有イベントの理解

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「shares」で示された構成イベント。
- アクションを実行したユーザのモニタ ID。
- アクションを実行したユーザのユーザ ID。
- 特定のイベント (例、clearShares)。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- リソースオーナーの識別。グループの場合は G、ユーザの場合は U。
- オーナー ID。

イベント	ログエントリ
リソースの共有または共有先	`[YYYY-MM-DD hh:mm:ss,sss] INFO shares monitor_ID user_ID {SUCCESS|FAILURE} setShares resource:IBFS_address count:number_of_parties_shared_with ownerType:{G|U} ownerID:owner_ID`

イベント	ログエントリ
リソースの共有解除	`[YYYY-MM-DD hh:mm:ss,sss] INFO shares monitor_ID user_ID clearShares {SUCCESS|FAILURE} resource:IBFS_address count:number_of_parties_shared_with ownerType:{G|U} ownerID:owner_ID`

ログインイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「signin」で示されたログインイベント。
- アクションを実行したユーザのモニタ ID。
- アクションを実行したユーザのユーザ ID。
- アクションの説明 (例、sign-in)。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- ログインしたユーザの名前およびモニタ ID。
- IP アドレス、ユーザエージェントまたはブラウザタイプ (該当する場合)。

各ユーザは、ユーザ名以外に、一意の数値 ID で識別されます。

イベント	ログエントリ
ユーザによるログイン	`[YYYY-MM-DD hh:mm:ss,sss] INFO signin monitor_ID user_ID signIn {SUCCESS|FAILURE} user:user_ID monitorId:monitor_ID IPaddr:IP_address userAgent:user_agent userDescription:user_description sessionType:session_type`
ユーザによるログアウト	`[YYYY-MM-DD hh:mm:ss,sss] INFO signin monitor_ID user_ID signOut {SUCCESS|FAILURE} user:user_ID monitorId:monitor_ID`
ユーザセッションの期限切れ	`[YYYY-MM-DD hh:mm:ss,sss] INFO signin monitor_ID user_ID signOut {SUCCESS|FAILURE} user:user_ID monitorId:monitor_ID`

参照 WebFOCUS Reporting Server 認証失敗時メッセージの理解

[外部セキュリティタイプ] (IBI_AUTHENTICATION_TYPE) 設定が [Reporting Server] の場合に WebFOCUS Reporting Server 認証が失敗すると、エンドユーザには常に通常の失敗メッセージが表示されます。ただし、監査ログには、下表に示す詳細エラーが記録されます。

説明	リターンコード
無効なユーザ ID またはパスワードです。	ERROR_AUTHENTICATION_FAILURE(5003)
認証情報は有効ですが、ユーザ ID が非アクティブです。	ERROR_AUTHENTICATION_FAILURE_ID_INACTIVE(5006)
認証情報は有効ですが、ユーザがパスワードを変更する必要があります。	ERROR_AUTHENTICATION_MUST_CHANGE_PASSWORD(5007)
認証情報は有効ですが、パスワードが期限切れです。	ERROR_AUTHENTICATION_PASSWORD_EXPIRED(5008)
認証情報は有効ですが、ユーザのログイン試行回数が、IBI_Max_Bad_Attempts 設定で指定された許容値を超えました。	ERROR_AUTHENTICATION_USER_LOCKED(5009)
認証情報は有効ですが、ユーザが前回のセッションでログインしている状態です。	ERROR_AUTHENTICATION_USER_ALREADY_LOGGED_IN(5020)

参照 ユーザログインエラーメッセージの理解

下表は、ログイン試行またはパスワード変更が失敗した場合のエラーメッセージのリストを示しています。

イベント	失敗時のメッセージ
ユーザがリポジトリに存在しません。	signIn Failure-unregistered_user User:xyzabc
ユーザはリポジトリに存在しますが、Reporting Server には存在しません。	signIn Failure-EDA-RC User:admin RC:32033 EDANODE:EDASERVE
ユーザはリポジトリおよび Reporting Server に存在しますが、無効なパスワードが入力されました。	signIn Failure-EDA-RC User:bn01618 RC:32034 EDANODE:EDASERVE

イベント	失敗時のメッセージ
ユーザはリポジトリおよび Reporting Server には存在しますが、アカウントが無効になっています。	`signIn Failure-Unknown User:cssadmin RC:32063 EDANODE:EDASERVE`
ユーザはリポジトリおよび Reporting Server には存在しますが、パスワードを変更する必要があります。	`signIn Failure-EDA-RC User:cssadmin RC:32034 EDANODE:EDASERVE`

手順　データベース接続の失敗をトラブルシューティングするには

1. データベースが稼動していることを確認します。

   Derby をインストールした場合は、リスナポート番号がデフォルトの 1527 であることを確認し、そのネットワークインターフェースを特定します。netstat –an コマンドを使用することができます。次のような結果が得られます。

ローカルアドレス	説明
0.0.0.0	リスナポートは、すべてのネットワークインターフェースで使用されています。
127.0.0.1	リスナポートは、ユーザのコンピュータからの接続のみに使用されています。
ユーザの IP アドレス	リスナポートは、そのインターフェース上の接続のみに使用されています。

2. audit.log ファイルを開いてエラーを確認します。
3. 管理ユーザが未登録であることが audit.log ファイルに記録されているが、これがデフォルト管理ユーザを使用した新規インストールの場合は、イベントログを開いてこのユーザの登録に関するエラーを確認してください。

   イベントログには、特定のデータベース接続エラーが記録されています。このログには、次の関連情報が表示されます。

   - ❏ BI Portal がデータベースに接続できるかどうか。
   - ❏ データベーステーブルが作成されているかどうか。
   - ❏ データベーステーブルにデータが挿入されているかどうか。

ユーザイベントの理解

下表に記載された各ログエントリは、次の要素で構成されています。

- タイムスタンプ (YYYY-MM-DD hh:mm:ss,sss 形式)。
- ログレベル (例、INFO)。
- 記録されたイベントタイプ。この場合は「users」で示されたユーザイベント。
- アクションを実行したユーザのモニタ ID。
- アクションの説明 (例、createUser、putUser)。
- アクションの成功または失敗 (SUCCESS または FAILURE)。
- アクションの影響を受けたユーザのユーザ名および一意の数値 ID。
- アクションによって変更されたフィールド。

各ユーザおよびグループは、それぞれの名前以外に、一意の数値 ID で識別されます。

イベント	ログエントリ
ユーザの作成	`[YYYY-MM-DD hh:mm:ss,sss] INFO users monitor_ID user_ID createUser {SUCCESS|FAILURE} user:user_ID (user_number) status:{ACTIVE|INACTIVE} email:email_address desc:description`
ユーザ詳細の変更	`[YYYY-MM-DD hh:mm:ss,sss] INFO users monitor_ID user_ID putUser {SUCCESS|FAILURE} userName:user_name Seat-Type-Property:property`
ユーザアカウントの無効	`[YYYY-MM-DD hh:mm:ss,sss] INFO users monitor_ID user_ID putUser {SUCCESS|FAILURE} user:user_ID (user_number) status:INACTIVE email:email_address desc:description`
ユーザアカウントの削除	`[YYYY-MM-DD hh:mm:ss,sss] INFO groups monitor_ID user_ID removeUserFromGroup {SUCCESS|FAILURE} user:user_ID (user_number) group:group_name (group_ID) [YYYY-MM-DD hh:mm:ss,sss] INFO deleteUser monitor_ID user_ID status:{ACTIVE|INACTIVE} email:email_address desc:description`
パスワードの変更	`[YYYY-MM-DD hh:mm:ss,sss] INFO users changePassword {SUCCESS|FAILURE} user:user_whose_password_is_changed (user_number) status:{ACTIVE|INACTIVE} email:email_address desc:description`

モニタログの理解

モニタログは、分単位でシステムパフォーマンスの記録を収集します。

セキュリティ上の理由から、モニタログは常に有効になっています。デフォルト設定では、モニタログは WebFOCUS Client 上に 10 日間保存されます。ログの保存期間は、カスタマイズすることができます。また、ログインイベントを別のログに保存したり、ログをデータベースに保存したりすることも可能です。

モニタログイベントの理解

モニタログイベントは、特定日時のシステムパフォーマンス統計を記録します。このようなイベントで作成されたモニタログのエントリには、記録が収集された日時、およびイベント発生時に記録された統計と値が表示されます。

下表とその説明では、時間がすべてミリ秒単位で示され、ファイルサイズはすべてキロバイト (KB) 単位で示されています (別途の指定がない限り)。

モニタログの記録には次のフォーマットを使用します。

イベント	ログエントリ
モニタログの収集	`[YYYY-MM-DD HH:MM:SS,sss] INFO ActLog Sessions= n ActRecentSes= n SrvReq= n SrvTime= ms maxSrvRsp= ms SrvDbmsReq= n SrvDbmsTime= ms maxSrvDbmsRsp= ms maxConcur= n UrlReq= n UrlTime= ms maxUrlRsp= ms ClientCPU= ms maxClientCPU= ms dummy= n dummy= n dummy= n numSRVLogs= n numURLLogs= n minHeapAvail= kb minNonHeapAvail= kb maxPendFinalization= n CpuLoad= n JavaCpuLoad= n ActUrlSes= n ActUrls= n ActLongRunUrls= n ActSrvReqSes= n ActSrvReq= n ActLongRunSrvReq= n`

説明

`[YYYY-MM-DD HH:MM:SS,sss]`

モニタイベント記録の日時です。イベントによって収集された統計はすべて、この日時に基づきます。

`INFO`

ログレベル (例、INFO)。詳細は、206 ページの 「 ログファイルの使用 」 を参照してください。

`ActLog`

ログが収集されたイベントのタイプです。この場合、ログレコードが収集するアクティビティは、ActLog で識別されます。

`Sessions= n`

前の 1 分間にアクティブ状態にあったすべてのセッション数です。この数字には、アクティブと非アクティブのセッションが含まれます。

`ActRecentSes= n`

前の 1 分間に開いていてアクティブ状態にあったすべてのセッション数です。この値は、Sessions 値のサブセットです。

`SrvReq= n`

前の 1 分間に発生した Reporting Server リクエストの総数です。

`SrvTime= ms`

前の 1 分間に発生したすべての Reporting Server リクエストの合計時間をミリ秒単位で示した数です。

`maxSrvRsp= ms`

前の 1 分間に発生した Reporting Server レスポンスの最大時間をミリ秒単位で示した数です。

`SrvDbmsReq= n`

前の 1 分間に発生した外部 RDBMS アクセスのリクエスト数です。この値は、Reporting Server へのリクエスト総数を示す SrvReq 値のサブセットです。

`SrvDbmsTime= ms`

前の 1 分間に、外部 RDBMS へのリクエスト実行に要した合計時間をミリ秒単位で示した数です。

`maxSrvDbmsRsp= ms`

前の 1 分間に実行された RDBMS リクエストの最長時間をミリ秒単位で示した数です。この値は、外部 RDBMS へのリクエスト実行に要した合計時間を示す SrvDbmsTime 値のサブセットです。

`maxConcur= n`

前の 1 分間に開いていた Reporting Server 同時接続数です。

`UrlReq= n`

前の 1 分間の URL リクエストの数です。

`UrlTime= ms`

前の 1 分間に、すべての URL リクエストの実行に要した合計時間をミリ秒単位で示した数です。

`maxUrlRsp= ms`

前の 1 分間で最長 URL レスポンスメッセージの実行に要した時間です。

`ClientCPU= ms`

前の 1 分間に、すべての URL リクエストの実行に要した CPU 時間の合計をミリ秒単位で示した数です。

`maxClientCPU= ms`

前の 1 分間で最長 URL リクエストの実行に要した最大 Client CPU 時間です。

`dummy= n`

プレースホルダパラメータです。このパラメータとその値は使用する必要がありません。

`dummy= n`

プレースホルダパラメータです。このパラメータとその値は使用する必要がありません。

`dummy= n`

プレースホルダパラメータです。このパラメータとその値は使用する必要がありません。

`numSRVLogs= n`

前の 1 分間に開いていたサーバリクエストおよびサーバレスポンスのログの総数です。

`numURLLogs= n`

前の 1 分間に開いていた URL リクエストおよび URL レスポンスのログの総数です。

`minHeapAvail= kb`

Java 仮想マシンヒープで使用可能な最小メモリ量をキロバイト単位で示した数です。

`minNonHeapAvail= kb`

Java 仮想マシンの追加メモリの最小メモリ量をキロバイト単位で示した数です。

`maxPendFinalization= n`

前の 1 分間に完了しなかったプロセスの最大数です。

`CpuLoad= n`

前の 1 分間のシステム全体の CPU 使用量を表す指数です。値には、CPU がすべてアイドル状態だったことを示す 0.0 から、CPU がすべて 1 分間連続でアクティブ状態だったことを示す 1.0 までの値を使用します。最新の CPU 使用量が取得できない場合、このパラメータには負の値が使用されます。

`JavaCpuLoad= n`
前の 1 分間の Java 仮想マシン (JVM) の CPU 使用量を表す指数です。値には、いずれの CPU も JVM プロセスからのスレッドを実行していなかったことを示す 0.0 から、すべての CPU が 1 分間連続で JVM からのスレッドを実行していたことを示す 1.0 までの値を使用します。JVM プロセスの最新の CPU 使用量が取得できない場合、このパラメータには負の値が使用されます。

`ActUrlSes= n`
現在アクティブな URL を含むセッション数です。

`ActUrls= n`
現在アクティブな URL の数です。

`ActLongRunUrls= n`
現在の長時間アクティブ URL の数です。

`ActSrvReqSes= n`

現在アクティブな Reporting Server 接続を含むセッション数です。

`ActSrvReq= n`
現在アクティブなサーバリクエストの数です。

`ActLongRunSrvReq= n`
現在の長時間アクティブ Reporting Server 接続の数です。

モニタ ID の理解

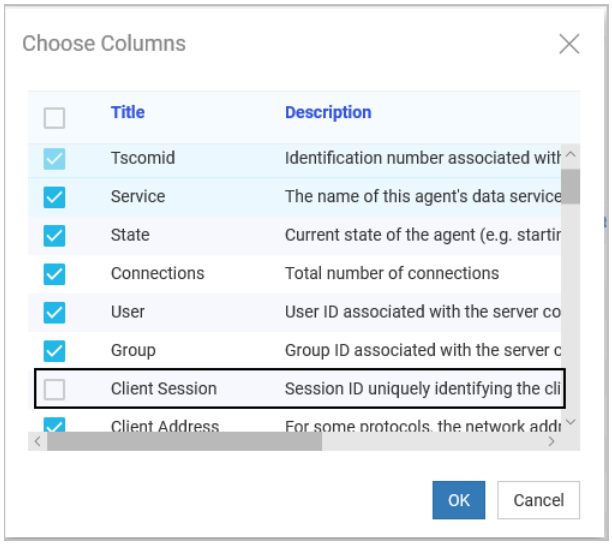
モニタ ID は、クライアントセッションごとにランダムに生成される一意の識別子です。管理者は、モニタ ID を使用して、各ユーザの Application Server セッション ID を表示せずに、WebFOCUS セッションを参照することができます。モニタ ID は、特定の場所からログインした特定のユーザを識別する一意の ID として機能するため、複数のユーザが同一ユーザ名 (例、public、admin) でログインした場合でも、各ユーザを識別することができます。デフォルト設定では、モニタ ID は Reporting Server に送信されますが、Reporting Server コンソールには表示されません。

WebFOCUS への独立したログインごとに、64 バイトの一意の内部 IBFS セッション ID で識別されます。モニタ ID (IBFS セッション ID の最初の 15 バイト) は、Reporting Server に送信され、現在のセッションで Reporting Server 上に存在する各ユーザの一時ファイル foccache の場所の識別に使用されます。

モニタ ID は、セッションモニタログ、トレースログ、セキュリティログなど、多くの WebFOCUS ログに表示されます。これらのログは、管理コンソールの [機能診断] タブの [ログファイル] ページから表示することができます。

管理コンソールの [機能診断] タブの [セッションモニタ] ページでは、現在セッションを個別に表示できるほか、特定のセッションのトレースログ、リクエストログ、プロシジャログを有効にすることができます。

Reporting Server コンソールでモニタ ID を表示するには、セッションのカラムを有効にする必要があります。これを行うには、Reporting Server コンソールを開き、[ツール]、[ワークスペース] を順に選択します。[ワークスペース] タブの [モニタ] グループで、[データサービスエージェント] をクリックします。[データサービスエージェント] ページで、ショートカットメニューから [カラムの選択] を選択します。下図のように、[カラムの選択] ダイアログボックスで [クライアントセッション] のチェックをオンにし、[OK] をクリックします。



変更管理のインポートおよびエクスポートログの理解

変更管理のインポートおよびエクスポートログは、変更管理のエクスポートおよびインポート操作で発生するイベントを収集します。 システムイベントおよびメッセージの記録により、変更管理アクティビティの確認や変更管理で発生した問題のトラブルシューティングがサポートされます。

cm_export ログおよび cm_import ログのリンクは、管理コンソールの [機能診断] タブからアクセス可能な [ログファイル] ページの [ログ名] 列に表示されます。

どちらのログでも、エントリは発生時間の早い順に上から表示され、各ログには 1 日のアクティビティが記録されます。 デフォルト設定では、これらのログは [デバッグ] トレースレベルに設定されますが、管理者はこのトレースレベルを調整して、ログで収集される詳細レベルを加減できます。

ログエントリは、次の要素で構成されます。

- タイムスタンプ (yyyy-MM-dd HH:mm:ss,SSS 形式)
- ログレベル (例、デバッグ)
- インポートまたはエクスポートのリクエスト URL ([http-host-port-directory-file:operation] 形式)。 たとえば、[http-nio-8080-exec-5:import] と記録されます。
- ユーザ ID
- システムイベントまたはメッセージ

以下はその例です。

```
[2018-08-17 08:33:32,987] DEBUG [http-nio-8080-exec-4:export] admin  -
ExportData - addResource: "IBFS:/WFC/Repository/HealthcareNet"
```

エントリで作成されたエクスポートパッケージ

cm_import ログでは、ユーザログエントリで生成されたエクスポートパッケージにより、インポートパッケージを作成したユーザ ID が収集されます。以下はその例です。

```
[2018-08-17 09:08:50,614] INFO  [http-nio-8080-exec-2:import] admin  -
Export package generated by user: admin
```

このエントリは、START IMPORT Process エントリに続くインポート処理のパラメータリストの後に表示されます。 ただし、このエントリを収集するには、cm_import ログのトレースレベルを [情報] に設定しておく必要があります。

高度な Web ツール、BI Portal、イベント、EclipseLink JPA、ReportCaster ログの理解

InfoAssist、BI Portal、ReportCaster のアクティビティはすべてトラッキングされ、*drive*:¥ibi¥WebFOCUS82¥logs ディレクトリ内の event.log ファイルに追加されます。 次のログレベルがあります。

- **オフ**　アクティビティはログファイルに書き込まれません。
- **重大**　最小トレース情報を記録します。
- **エラー**　エラーが発生した場合にのみ情報を記録します。

- **警告** 警告メッセージのみを記録します。
- **情報** 情報メッセージのみを記録します。
- **デバッグ** 最大トレース情報を記録します。
- **トレース** トレースを有効にします。

注意：org.eclipse.persistence のログレベルを [デバッグ] または [トレース] に設定すると、SQL クエリのバインド済みパラメータのリストが含まれたトレース情報が event.log ファイルに記録されます。

C

機能診断

ここでは、WebFOCUS Client で使用可能な機能診断トレースを有効にする方法について説明します。

管理コンソールを使用して、WebFOCUS Client の Servlet 実装のトレースを作成、表示することができます。これらの各トレースは、対応する [トレース] のページでオンとオフを切り替えることができます。トレースを有効にできるのは管理者のみです。 内部パスワード変数は、トレースファイルまたはログに記録される際にマスクされます。

トレースの実行はパフォーマンスに影響するため、トラブルシューティング目的以外では使用しないことをお勧めします。WebFOCUS の構成が正しいことを確認した後、トレースをオフにし、Web アプリケーションを再ロードします。

トレースファイルにアクセスするには、セッションビューアを開きます。特定のセッションのトレースを画面上に表示することも、セッショントレースの ZIP コピーをトレースファイルフォーマットで保存し、後から確認することもできます。詳細は、190 ページの 「 セッションの表示 」 を参照してください。

トピックス

すべての Client トレースの理解

特定のトレースファイルではなく [すべての Client] メニューを選択すると、有効なトレースのすべてのファイルが表示されます。

モニタログトレースの理解

モニタログトレースは、1 つまたは複数のアクティブセッションに関する情報を提供します。ログを有効にするには、管理コンソールの [機能診断] タブの [セッションモニタ] ページまたは [セッションビューア] のトレース機能を使用します。すべてのセッション、または個々のセッションのトレースを有効にすることができます。モニタログでは、次のレベルの診断情報が書き込まれます。

- **オフ** monitor.log ファイルに情報は何も書き込まれません。
- **重大** 最小トレース情報を記録します。
- **エラー** エラーが発生した場合にのみ情報を記録します。
- **警告** 警告メッセージのみを記録します。
- **情報** 情報メッセージのみを記録します。
- **デバッグ** 最大トレース情報を記録します。
- **トレース** トレースを有効にします。

ログファイルには、設定されているログレベルに基づいて情報が書き込まれます。たとえば、[情報] ログレベルの場合、次の情報がログに書き込まれます。

```
[YYYY-MM-DD hh:mm:ss,sss] INFO ReqEnd MonID=monitor_ID
ClientUser=user_ID ReqID=16.29.03.987-1 Node=node ServerUser=
Completed=completion_time
TimeUsed=time_to_run_request ReqInfo=request_information
```

説明

`MonID`

セッションごとの一意の識別子です。

`ClientUser`

リクエストを実行している ユーザ ID です。

`ReqID`

Reporting Server の一意のリクエスト識別子です。

`Node`

リクエストを実行している Reporting Server です。

`ServerUser`

Reporting Server ユーザ ID です。

`Completed`

リクエストが完了した時刻 (ミリ秒) です。

`TimeUsed`

リクエストの実行に要した時間 (ミリ秒) です。

`ReqInfo`

アプリケーション名やレポートプロシジャ名などの、リクエストに関する情報です。

ログレベルは通常、[情報] に設定されています。トラブルシューティングには、[デバッグ] レベルの使用をお勧めします。

Web セキュリティのトレースの理解

Web セキュリティのトレースは、検証設定の影響を受ける検証リクエストをトラッキングします。ログレベルのオプションは次のとおりです。

- **オフ**　monitor.log ファイルに情報は何も書き込まれません。
- **重大**　最小トレース情報を記録します。
- **エラー**　エラーが発生した場合にのみ情報を記録します。
- **警告**　警告メッセージのみを記録します。
- **情報**　情報メッセージのみを記録します。
- **デバッグ**　最大トレース情報を記録します。
- **トレース**　トレースを有効にします。

Web サービストレースの理解

Web サービスを使用すると、.NET または Java 環境でのアプリケーション開発、およびこれらの環境での WebFOCUS 機能の実行が可能になります。

トレースファイルはそれぞれ別の Web Service 関数コールで、SOAP メッセージをトレースします。このトレースは、WebFOCUS Web サービス関数の呼び出し中に、開発者が .NET または Java プログラムをデバッグする必要がある場合に重要です。

注意：Web サービストレースは、セッションビューアまたはセッションモニタで確認することができます。

WFServlet トレースの理解

WFServlet のトレースは、WebFOCUS Client の Servlet 実装で処理されたリクエストをトラッキングします。トレースファイルの名前のフォーマットは次のとおりです。

*sequencenumber*_WFServlet_WFAPI_*date_time*.trace

各トレースファイルには作成時に連続番号が付けられます。date および time は、ファイルが作成された日時を示します。

WFServlet トレースを有効にするには、セッションモニタの [トレースの制御] リストから [詳細] オプションを選択するか、セッションビューアの [トレースレベル] リストから [詳細] オプションを選択します。

D

権限

ここでは、ユーザロールを編集または作成する際に使用可能な各権限について説明します。権限の適用先フォルダは、[サブシステム] 列に記載されています。ここに記載されている権限の一部は、ライセンスおよび構成設定に関連付けられています。これらの権限は、関連するライセンスまたは構成設定が使用されていない限り、セキュリティセンターの [ロール] ダイアログボックスには表示されません。

トピックス

Basic Reporting

次の権限は、最小限のトレーニングを受けたユーザを含め、ほとんどのユーザに割り当てることができます。他のカテゴリの権限はすべて、この Basic Reporting カテゴリの権限を補足する目的で割り当てます。

権限	説明	サブシステム	権限 ID
Access Comments	コンテンツに関するコメントを表示できます。	WFC	opReadComments
Access Library Content	ReportCaster から配信された ReportLibrary 出力を表示できます。	Session, WFC	opLibrary

権限	説明	サブシステム	権限 ID
Access Portal	定義済みポータルを表示できます。	WFC, BIP	opViewPortal
Access Resource	リソースを表示できます (ほとんどのロールで必要)。	*	opList
Access Resource Properties	フォルダまたは項目のプロパティを表示できます。	WFC	opViewProps
Create Comments	コンテンツに関するコメントを作成できます。	WFC	opCreateComments
Create Shortcuts	ショートカットを作成できます。	Session, WFC	opShortcut
Display About TIBCO WebFOCUS	[ヘルプ] メニューに [TIBCO WebFOCUS について] および [ライセンス] オプションを表示します。ユーザは、このオプションを使用して、バージョンおよび環境情報を確認できます。	Session	opDisplayVersionInfo
Display Ask TIBCO WebFOCUS for InfoSearch	サイドバーに [TIBCO WebFOCUS に質問] オプションを表示します。この機能を使用して、コンテンツの検索ができます。	Session	opInfoSearch
Display Ask TIBCO WebFOCUS for Mobile Voice	サイドバーに [TIBCO WebFOCUS に質問] オプションを表示します。この機能を使用して、音声対応コンテンツにアクセスできます。	Session	opMobileVoice
Display Favorites Node	リソースツリーに [お気に入り] ノードを表示します。	Session, WFC	opFavorites

権限	説明	サブシステム	権限 ID
Display Magnify Search Page	[ツール] メニューに [Magnify 検索ページ] オプションを表示します。このページを使用して、WebFOCUS コンテンツを検索できます。	Session	opMagnify
Display Search	最上位フォルダのコンテキストメニューに [検索] オプションを表示します。この機能を使用して、TIBCO WebFOCUS リソースを検索できます。	Session	opRepositorySearch
Display Stop Requests	[ツール] メニューに [リクエストの停止] オプションを表示します。この機能を使用して、送信済みレポートリクエストをキャンセルできます。	Session	opStopRequests
Edit Comments	コンテンツに関するユーザ自身のコメントを編集、削除できます。	WFC	opEditComments
Mobile Faves Email Option	iOS または Android 用の Mobile Faves アプリケーションから Email 送信できます。	WFC	opMobileFavesEmail
Mobile Faves Print Option	iOS または Android 用の Mobile Faves アプリケーションから印刷できます。	WFC	opMobileFavesPrint
Mobile Faves Save Option	iOS または Android 用の Mobile Faves アプリケーションからユーザ独自のデバイスにコンテンツを保存できます。	WFC	opMobileFavesSave

権限	説明	サブシステム	権限 ID
My Content Folder	フォルダのプロパティで [[マイコンテツ] フォルダの自動作成] オプションが選択されている場合に、そのフォルダにユーザの [マイコンテンツ] フォルダが作成されます。	WFC	opCreateMyFolder
Run Resources	レポート、グラフ、ページ、スケジュールなどのリソースの実行、および静的コンテンツへのアクセスを行えます。	WFC, EDA	opRun
Run Procedures Deferred	レポートやグラフをディファード処理に送信できます。	Session, WFC	opRunDef
Run Procedures with Different Connection Credentials	[接続情報プロンプトオプション] で構成されたデータ接続に異なる資格情報を指定することができます。 **注意：**この権限は、管理コンソールの [その他] 設定の [認証情報プロンプトオプション] のチェックがオンの場合のみ表示されます。	WFC, EDA	opRunAs
Run Procedures with Insight	adhoc クエリの実行が可能なインタラクティブキャンバスモードでグラフを実行できます。	WFC	opRunEnhanced
Save Deferred Output	ディファード出力をユーザ自身の [マイコンテンツ] フォルダまたは任意の書き込み可能な場所に保存できます。	Session	opSaveDef
Save Portal Customization	ユーザ自身がカスタマイズしたポータルビューを保存できます。	WIF, BIP	opCustomizePortal

権限	説明	サブシステム	権限 ID
Save Procedure Parameters	プロシジャのパラメータ選択値を保存できます。	WFC	opParmrpt

Advanced Reporting

次の権限は、ユーザ独自のレポートを作成、共有する必要のあるユーザに割り当てることができます。一般に、これらの権限は、Basic Reporting カテゴリの権限の代わりに割り当てるのではなく、補足する目的で割り当てます。

権限	説明	サブシステム	権限 ID
Create Alerts	条件付きでレポートを実行するアラートを作成できます(アラートアシストが利用できます)。	WFC	opAlertAssistant
Create URL Reports	Web の URL を参照するレポートを作成できます。	Session, WFC	opURL
Data Visualization from Metadata	ビジュアライゼーションツールおよびメタデータ選択ダイアログボックスを使用できます。	WFC	opVisualization
Designer Workbook	WebFOCUS DESIGNER で、埋め込みコンテンツを使用したブックを作成できます。	Session, WFC	opWorkbookDesigner
Designer Content from Metadata	WebFOCUS DESIGNER で、メタデータからコンテンツを作成できます。	Session, WFC	opDesignerMetadata
Designer Content from Business View	WebFOCUS DESIGNER で、ビジネスビューからコンテンツを作成できます。	Session, WFC	opDesignerBV

権限	説明	サブシステム	権限 ID
Designer Content from Reporting Object	WebFOCUS DESIGNER で、レポートオブジェクトからコンテンツを作成できます。	Session, WFC	opDesignerReportingObject
Designer Page	WebFOCUS DESIGNER を使用してページを作成できます (ダッシュボード、InfoApps)。	Session, WFC	opAppDesigner
Display Easel.ly Link	WebFOCUS の [ツール] メニューに Easel.ly Infographic を表示します。	Session, WFC	opEaselly
Express Analytics	Express Analytics Engine を使用してレポート、グラフ、ダッシュボードを作成できます。	WFC	opExpressAnalytics
InfoAssist from Metadata	InfoAssist レポートツールおよびメタデータ選択ダイアログボックスを使用できます。	WFC	opInfoAssist
InfoAssist from Reporting Object	InfoAssist およびレポートオブジェクトツールを使用できます。	WFC	opInfoAssistviaReportingObject
Open Items	項目を開くことができます (項目の作成に使用されたツールの権限も必要)。	WFC, EDA, WEB	opOpen
Save OPS Portlet Customization	Open Portal Service ポートレットのユーザカスタムビューを保存できます。	Session	opCustomizeOPS
Share Private Library Content	ReportLibrary コンテンツおよびウォッチリストレポートを、割り当てられたユーザと共有できます。	WFC	opShareLibraryReport

権限	説明	サブシステム	権限 ID
Share Private Resources	プライベートリソースを、割り当てられたユーザと共有できます。	WFC	opShareBasic
Share Private Resources with Specific Users	プライベートリソースを、割り当てられたユーザの一部と共有できます。	WFC	opShareAdvanced
Upload Data	サポート対象のデータファイルタイプを Reporting Server にアップロードできます。	Session, WFC, EDA	opUploadDataFile
Upload Documents	サポート対象のドキュメントファイルタイプをリポジトリにアップロードできます。	Session, WFC, FILE	opUploadDocument
Upload Images	サポート対象のイメージファイルタイプをリポジトリにアップロードできます。	Session, WFC, EDA	opUploadImage
Web Services	TIBCO WebFOCUS Web サービスを使用できます。	Session	opWebServices

Scheduling and Distribution

次の権限は、ReportCaster を使用してレポート配信のスケジュールを作成するユーザ、開発者、管理者に割り当てることができます。

権限	説明	サブシステム	権限 ID
Access Blackout Periods	レポートのスケジュール禁止日を表示できます。	Session	opRCBlackoutDatesTool
Access Job Logs	権限が与えられた ReportCaster ジョブに関連するログを表示できます。	Session	opRCJobLogsTool

権限	説明	サブシステム	権限 ID
Access Job Status	権限が与えられた ReportCaster ジョブのステータスを表示できます。	Session	opRCJobStatusTool
Assign Credentials for Schedules	Reporting Server、FTP サーバ、Web サーバへの接続時にスケジュールで使用される認証情報を管理できます。	Session	opRCExecutionId
Create Access List	ReportLibrary 出力を表示できるユーザを制限するためのアクセスリストを作成できます。	Session, WFC	opSchedAccessList
Create Distribution List	スケジュールに割り当てる配信リストを作成、表示できます。	Session, WFC	opSchedDistributionList
Create Library Item	ReportLibrary 項目を作成できます。	WFC	opCreateLibraryItem
Display ReportCaster Explorer	[ツール] メニューに [ReportCaster エクスプローラ] オプションを表示します。	Session, WFC	opRCExplorer
Distribute to Email	出力を Email 配信するジョブをスケジュールできます。	Session, WFC	opDistributeEmail
Distribute to File System	出力をファイルシステムに配信するジョブをスケジュールできます。	Session, WFC	opDistributeFileSystem
Distribute to FTP	出力を FTP サーバに配信するジョブをスケジュールできます。	Session, WFC	opDistributeFTP
Distribute to Library	出力を ReportLibrary に配信するジョブをスケジュールできます。	Session, WFC	opDistributeLibrary

権限	説明	サブシステム	権限 ID
Distribute to Printer	出力をプリンタに配信するジョブをスケジュールできます。	Session, WFC	opDistributePrinter
Distribute to Repository	出力をリポジトリに配信できます。	Session, WFC	opDistributeMR
ReportCaster Advanced UI	フォルダのコンテキストメニューに [スケジュール] オプションを表示します。このオプションを使用して、複数タスクのスケジュールを作成できます。	Session, WFC, EDA	opScheduleAdvancedTool
Schedule Files	スケジュールの [タスク] から ReportCaster Distribution Server のオペレーティングシステムからのファイル配信をスケジュールできます。	Session, WFC	opScheduleTaskFile
Schedule FTP Resources	スケジュールの [タスク] から FTP サーバからのファイル配信をスケジュールできます。	Session, WFC	opScheduleTaskFTP
Schedule HTTP Requests	スケジュールの [タスク] から Web サーバから取得された HTTP 応答の配信 (URL 配信) をスケジュールできます。	Session, WFC	opScheduleTaskURL
Schedule Other Schedules	スケジュールの [タスク] から他の WebFOCUS スケジュールをスケジュールできます。	Session, WFC	opScheduleTaskSchedule
Schedule MR Procedures	スケジュールの [タスク] から WebFOCUS レポート をスケジュールできます。	Session, WFC	opScheduleTaskMR

権限	説明	サブシステム	権限 ID
Schedule Reporting Server Procedures	スケジュールの [タスク] から Reporting Sever のアプリケーションフォルダに格納されたプロシジャをスケジュールできます。	Session, WFC	opScheduleTaskWFRS

Application Development

次の権限は、Web ベースのツールのみを使用して完全な WebFOCUS アプリケーションを作成する開発者に割り当てることができます。WebFOCUS アプリケーション開発のすべての機能へのアクセスを有効にするには、開発チームに Desktop Development カテゴリの権限も割り当てる必要があります。

権限	説明	サブシステム	権限 ID
Copy and Update Paths	コピーした項目のパス参照が調整されます。 **注意：**この権限は、WebFOCUS バージョン 8.2.06.06 ではテクニカルプレビュー機能として使用できます。	WFC	opCopySpecial
Create Folders	フォルダを作成できます。	WFC, EDA, WEB	opCreateFL
Create Items	項目を作成できます。	WFC, BIP, EDA, WEB	opCreateItem
Create Metadata	フォルダの [メタデータ] メニューから Reporting Server コンソールのメタデータウィザードにアクセスできます。	Session, WFC, EDA	opMetadata
Create Portal	ポータルを作成できます。	Session, WFC, BIP	opCreatePortal

権限	説明	サブシステム	権限 ID
Create Reporting Objects	フォルダ内でレポートオブジェクトを作成できます。	WFC	opReportingObject
Delete Resources	リソースを削除できます。	*	opDelete
Edit Items	リソースコンテンツを編集できます。	*	opWrite
Edit OPS Portlets	OPS (Open Portal Services) ポートレットに表示される内容を変更できます。	Session	opEditOPS
Edit Resource Names	リソースのタイトル名 (IBFS 名) を変更できます。	WFC, BIP, EDA	opRename
Edit Resource Properties	フォルダおよび項目のプロパティを変更できます。	WFC, BIP	opUpdProps
Portal Designer	ポータルデザイナを使用できます。	Session, WFC, BIP	opEditPortal
Portal Page Designer	ポータルページデザイナを使用してポータルページを作成、編集できます。	Session, WFC, BIP	opPageDesigner
Reporting Server Console	Reporting Server コンソール、および Reporting Server ロールで許可された機能にアクセスできます。	EDA	opServerConsole
Resource Export	リソースおよび変更パッケージをエクスポートできます。	*	opExport
Resource Export Download	変更管理 ZIP ファイルをダウンロードできます。	*	opDownloadCM
Resource Publish	プライベートリソースを公開できます。公開後のリソースへのアクセスは、セキュリティポリシーで管理されます。	WFC, BIP	opPublish

権限	説明	サブシステム	権限 ID
Resource Unpublish	公開済みリソースをプライベートリソースに変更できます。	WFC, BIP	opMakePrivate
Resource Text Editor	項目のコンテンツをテキストエディタで変更できます。	Session	opEditor
Run with SQL Traces	SQL トレースを取得するプロシジャを実行できます。	WFC	opRunSQLTrace
Session Traces	ユーザ自身のセッショントレースを有効にして表示できます。	Session	opDevTraces
Validate Portal	ポータルのコンテンツが他のユーザにも表示されることを確認できます。	WFC, BIP	opValidatePortal
View Rules on a Resource	リソースに適用されているルールを表示できます。	*	opViewRulesOn

Desktop Development

次の権限は、Developer Studio を使用してコンテンツ (リポジトリ配下) にアプリケーションを開発するユーザに割り当てることができます。開発機能のすべてを有効にするには、これらの権限を Application Development、Advanced Reporting、Basic Reporting カテゴリの権限とともに割り当てる必要があります。

権限	説明	サブシステム	権限 ID
Desktop Alert	条件付きでプロシジャを実行するアラートを作成できます(アラートウィザードを利用できます)。	WFC	opDTAlert
Desktop Allocation	物理ファイルに論理名を割り当てることができます。	WFC	opDTAllocation

権限	説明	サブシステム	権限 ID
Desktop Chart	グラフを作成することができます。	WFC	opDTChart
Desktop Connect	TIBCO WebFOCUS に接続できます。	Session	opDTConnect
Desktop Define	一時項目 (DEFINE) を作成できます。	WFC	opDTDefine
Desktop Define Function	DEFINE 関数を作成できます。	WFC	opDTDefineFunction
Desktop Dialog Manager	スクリプトを使用してプロシジャのフローを制御できます。	WFC	opDTDialogManager
Desktop Document	複数のレポート、グラフ、イメージで構成されたレイアウトを作成できます。	WFC	opDTDocumentCanvas
Desktop Editor	レポートやグラフなどのオブジェクトをデスクトップのテキストエディタで編集できます。	WFC	opDTEditor
Desktop Engine Facility	データソースにアクセスする接続コマンドを作成できます。	WFC	opDTEngine
Desktop Execute	プロシジャ内から別のプロシジャを呼び出すことができます(EX コマンドが利用できます)。	WFC	opDTExecute
Desktop File View Panel	App Studio で [プロシジャビュー] パネルを使用できます。	WFC	opDTFileViewPanel

権限	説明	サブシステム	権限 ID
Desktop HTML	フォーム、レポート、グラフ、マップなどのオブジェクトが統合された HTML ページを作成できます。	WFC	opDTHTMLCanvas
Desktop HTMLFORM	プロシジャ内で -HTMLFORM コマンドを作成できます。	WFC	opDTHTMLForm
Desktop Impact Analysis	アプリケーション全体でのメタデータの使用状況を分析できます。	WFC	opDTImpactAnalysis
Desktop Include	他のプロシジャの再利用可能コードの一部を参照できます。(-INCLUDE コマンドが利用できます。)	WFC	opDTInclude
Desktop Join	JOIN を使用してデータソースを結合できます。	WFC	opDTJoin
Desktop Match	MATCH を使用してデータソースを統合できます。	WFC	opDTMatch
Desktop Procedure Viewer	プロシジャビューアでプロシジャを表示できます。	WFC	opDTProcedureViewer
Desktop Report	レポートを作成できます。	WFC	opDTReport
Desktop RSTAT Facility	予測およびスコアリングアプリケーションを作成できます。	WFC	opDTRstat
Desktop Set	環境設定を使用して製品の動作をカスタマイズできます。	WFC	opDTSet
Desktop Source Control	サポート対象のソース管理システムを統合できます。	Session, WFC	opDTSourceControl

権限	説明	サブシステム	権限 ID
Desktop SQL Editor	プロシジャ内に SQL コードを埋め込むことができます。	WFC	opDTSQLEditor
Desktop SQL Report Wizard	SQL レポートウィザードを使用してプロシジャを作成できます。	WFC	opDTSQLReport
Desktop Use	FOCUS データソースの名前とパスを指定できます。	WFC	opDTUse

Group Administration

次の権限は、部門またはテナントのグループ管理者に割り当てることができます。これらの権限により、グループ管理者が、管理対象のグループ内のユーザの管理や、これらのユーザが作成したコンテンツの管理を行えるようになります。

権限	説明	サブシステム	権限 ID
Access Roles	管理対象のグループのロールを [セキュリティルール] ダイアログボックスで表示できます。	ROLES	opViewPermSet
Access Users	管理対象のグループ内のユーザをリスト表示できます。	GROUPS	opListUser
Assign Ownership	リソースのオーナーシップを、割り当てられたユーザやグループに変更できます。	WFC, BIP	opUpdateOwnership
Assign Ownership to Groups	管理対象のグループにリソースのオーナーシップを割り当てることができます。	GROUPS	opSetGroupOwner

権限	説明	サブシステム	権限 ID
Assign Ownership to Users	管理対象のグループ内のユーザにリソースのオーナーシップを割り当てることができます。	GROUPS	opSetUserOwner
Content Sharing Scope	管理対象のグループ内のユーザとリソースを共有できます。	GROUPS	opShareWith
Group Creation	管理対象のグループ内にグループを作成できます。	GROUPS	opCreateGroup
Group Deletion	管理対象のグループ内のグループを削除できます。	GROUPS	opDeleteGroup
Group Property Access	管理対象のグループのプロパティを表示できます。	GROUPS	opViewGroup
Group Property Management	管理対象のグループのプロパティを更新できます。	GROUPS	opUpdateGroup
Group Rename	管理対象のグループ内のグループ名を変更できます。	GROUPS	opRenameGroup
Manage Comments	コンテンツに関するコメントを管理できます。	Session, WFC	opManageComments
Manage General Access	管理対象のリソースへの基本アクセス権限を EVERYONE ユーザに付与できます。	Session	opGeneralAccess
Manage Group Membership	管理対象のグループのメンバーシップを管理できます。	GROUPS	opAssignUsersTo

権限	説明	サブシステム	権限 ID
Manage Private Resources	管理するグループ内のユーザのプライベートリソースを管理できます。[管理] メニューに [プライベートリソース管理] を表示できます。	GROUPS	opManagePrivateResources
Manage ReportCaster Blackout Periods	管理対象のグループの ReportCaster スケジュール禁止日を管理できます。	GROUPS	opSetBlackoutDates
Manage Rules for a Group	管理対象のグループのセキュリティルールを作成できます。	GROUPS	opUseGroupInRules
Manage Rules for a User	管理対象のユーザのセキュリティルールを作成できます。	GROUPS	opUseUserInRules
Manage Rules on Resources	管理対象のリソースのルールを管理できます。	*	opManageRulesOn
ReportCaster Administration Scope	管理対象のグループ内のユーザが所有する ReportCaster リソースを管理できます。	GROUPS	opRCGroupAdmin
Security Center	[管理] メニューに [セキュリティセンター] オプションを表示します。この機能を使用して、割り当てられたユーザ、グループ、ロールを管理できます。	Session	opManageSecurity
Security Center Scope	管理対象のユーザを、割り当てられたグループに追加できます。	GROUPS	opAssignUsersFrom

権限	説明	サブシステム	権限 ID
Use Roles in a Rule	管理対象のグループのロールに対してセキュリティルールを作成できます。	ROLES	opUsePermSetInRules
User Account Creation	管理対象のグループ内でユーザを作成できます。	USERS, GROUPS	opCreateUser
User Account Deletion	管理対象のグループ内のユーザを削除できます。	USERS, GROUPS	opDeleteUser
User Account Password Management	管理対象のユーザのパスワードを再設定できます。	USERS, GROUPS	opSetPassword
User Account Property Access	管理対象のユーザのアカウントプロパティを表示できます。	USERS, GROUPS	opViewUser
User Account Property Management	管理対象のユーザのアカウントプロパティを更新できます。	USERS, GROUPS	opUpdateUser

Administration

次の権限は、一般に WebFOCUS 管理者にのみ割り当てられます。

権限	説明	サブシステム	権限 ID
Allow My Content Folders	フォルダのプロパティに [[マイコンテンツ] フォルダの自動作成] オプションを表示します。	WFC	opAutocreateMyFolders
Create Roles	ロールを作成できます。	ROLES	opCreatePermSet
Delete Roles	ロールを削除できます。	ROLES	opDeletePermSet
Display Administration Console	[ツール] メニューに [管理コンソール] オプションを表示します。	Session	opWFAdminConsole

権限	説明	サブシステム	権限 ID
Display Magnify Console	[管理] メニューに [Magnify コンソール] オプションを表示します。このコンソールを使用して、検索システムを構成できます。	Session	opMagnifyConsole
Group Mapping	WebFOCUS グループを外部認可ソースにマッピングできます。	GROUPS	opExternalGroupMapping
Manage ReportCaster Configuration	[ツール] メニューに [ReportCaster ステータス] オプションを表示します。	Session	opRCConfiguration
Manage ReportCaster Global Settings	ReportCaster コンテンツに対してグローバル更新を実行できます。	Session	opRCGlobalUpdate
Manage ReportCaster Library Report Deletion	ReportLibrary 削除ユーティリティを実行できます。	Session	opRCExpLibraryDelete
Manage ReportCaster Log Purge	ReportCaster ログ削除ユーティリティを実行できます。	Session	opRCPurgeJobLogs
Manage ReportCaster Schedule Deletion	ReportCaster スケジュール削除ユーティリティを実行できます。	Session	opRCSchedDelete
Manage ReportCaster Watch List Subscription	他のユーザの ReportLibrary レポートの登録を解除できます。	Session	opRCUnsubscribe
Manage Reporting Server Properties	リソースの Reporting Server プロパティを更新できます。	WFC	opRepSrvProps
ReportCaster Server Administration	ReportCaster Distribution Server を管理できます。	Session	opRCServerManagement

権限	説明	サブシステム	権限 ID
Resource Import	リソースおよび変更パッケージをインポートできます。	*	opImport
Resource Import Upload	変更管理 ZIP ファイルをアップロードできます。	*	opUploadCM
Resource Templates	最上位フォルダのコンテキストメニューからリソーステンプレートを使用できます。	Session,WFC, FILE	opUseTemplate
Update Roles	ロールを変更できます。	ROLES	opUpdatePermSet
System Configuration	WebFOCUS システム構成を変更できます。	Session	opWFAdminConfiguration
System Tracing	WebFOCUS システムトレースを作成、表示できます。	Session	opWFAdminTraces
Toggle Repository View	リソースツリーの [表示] メニューから表示をリポジトリ表示から完全表示 (IBFS) に切り替えることができます。	Session	opToggleTree

E

データソースのセキュリティ設定 - DBA

データベース管理者は、DBA セキュリティ機能を使用して FOCUS データソースにセキュリティを設定することができます。このセキュリティ機能を使用すると、ユーザが 1 つのレポートでリクエスト可能なレコード数または読み取り数を制限することができます。

DBA セキュリティ機能は、FOCUS 以外のデータソースにセキュリティを設定する場合にも使用することができます。なお、DBA セキュリティ機能では、WebFOCUS 以外からアクセスするデータソースを保護することはできません。

注意：FOCUS データソースに関するすべての説明は、XFOCUS データソースにも適用されます。

トピックス

データソースセキュリティの概要

DBA 機能には、次のようなセキュリティオプションが用意されています。

- USER 属性 - 特定のデータソースにアクセス可能なユーザを限定します。この属性についての詳細は、668 ページの 「 アクセス権限によるユーザの識別 - USER 属性 」 を参照してください。
- ACCESS 属性 - ユーザのアクセス権限を、読み取り、書き込み、更新のいずれかに制限します。この属性についての詳細は、674 ページの 「 アクセス権限タイプの指定 - ACCESS 属性 」 を参照してください。
- RESTRICT 属性 - ユーザアクセスを特定のフィールドまたはセグメントに制限します。この属性についての詳細は、677 ページの 「 データソースのアクセス制限 - RESTRICT 属性 」 を参照してください。
- RESTRICT 属性 - 取得するレコードを、確認テストにパスしたレコードのみに制限します。この属性についての詳細は、677 ページの 「 データソースのアクセス制限 - RESTRICT 属性 」 を参照してください。
- RESTRICT 属性 - ユーザがデータソースにアクセスして読み取り、書き込み、または変更できる値を制限します。この属性についての詳細は、677 ページの 「 データソースのアクセス制限 - RESTRICT 属性 」 を参照してください。
- SET DBASOURCE コマンド - マルチファイル構造でのアクセス制限のソースを制御することができます。このコマンドについての詳細は、684 ページの 「 マルチファイル構造でのアクセス制限のソース制御 」 を参照してください。
- DBAFILE 属性 - 別のマスターファイルに格納されているパスワードおよび制限を参照するように指定します。この属性についての詳細は、688 ページの 「 主マスターファイルへのセキュリティ情報の追加 」 を参照してください。
- WebFOCUS DBA イグジットルーチン - 外部セキュリティシステムで WebFOCUS パスワードを設定することができます。詳細は、『TIBCO WebFOCUS セキュリティ管理ガイド』を参照してください。
- プロシジャにセキュリティを設定することができます。この方法について詳細は、698 ページの 「 プロシジャのセキュリティ 」 WebFOCUS を参照してください。

データソースセキュリティの実装

WebFOCUS セキュリティは、ファイル単位で実装します。次の項目を指定して、DBA セキュリティ機能を簡単に実装することができます。

- データソースへのアクセス権限を与える WebFOCUS ユーザの名前またはパスワード。
- ユーザに与えるアクセス権限のタイプ。
- ユーザのアクセスを制限するセグメント、フィールド、データ値の範囲。

マスターファイルの END コマンドの後に宣言 (セキュリティ宣言と呼ばれる) を記述して、指定したデータソースにセキュリティが必要であること、および必要になるセキュリティタイプに関する情報を WebFOCUS に指示します。セキュリティ宣言は、次の 1 つまたは複数の属性で構成されます。

- DBA 属性 - データソースのデータベース管理者の名前またはパスワードを指定します。データベース管理者には、指定したデータソースおよびそのマスターファイルに無制限のアクセスが与えられます。
- USER 属性 - データソースの正規ユーザとなるユーザを識別します。セキュリティが設定された FOCUS データソースのマスターファイルでユーザ名またはパスワードが指定されている場合は、そのユーザのみがデータソースにアクセスすることができます。
- ACCESS 属性 - アクセス権限が与えられたユーザのアクセスタイプを定義します。次の 4 つのアクセスタイプを使用することができます。

  RW - データソースの読み取りと書き込み

  R - データソースの読み取り専用

  W - 新しいセグメントインスタンスのデータソースへの書き込み専用

  U - データソースのレコードの更新専用

- RESTRICT 属性 - ユーザにアクセス権限を与えないセグメントまたはフィールドを指定します。この属性は、ユーザが表示またはトランザクションを実行できるデータ値を制限する場合にも使用することができます。
- NAME 属性および VALUE 属性 - RESTRICT 宣言の一部として使用します。

データソースにセキュリティを設定するには、マスターファイルでこれらの属性値をカンマ (,) 区切りのフォーマットで指定します。これは、マスターファイルで他の属性を指定する場合と同様です。

マスターファイルで END のみが 1 行に配置されている場合、これはセグメントおよびフィールドの属性がそこで終了し、アクセス制限がその後に続くことを示しています。マスターファイルに END を配置する場合、少なくとも 1 つの DBA 属性をその後に続ける必要があります。

例　マスターファイルへのデータソースセキュリティの実装

次の例は、WebFOCUS DBA の記述例です。

```
FILENAME = PERS, SUFFIX = FOC,$
SEGMENT = IDSEG, SEGTYPE = S1,$
 FIELD = SSN          ,ALIAS = SSN    ,FORMAT = A9   ,$
 FIELD = FULLNAME     ,ALIAS = FNAME  ,FORMAT = A40  ,$
 FIELD = DIVISION     ,ALIAS = DIV    ,FORMAT = A8   ,$
SEGMENT=COMPSEG, PARENT=IDSEG, SEGTYPE=S1,$
 FIELD = SALARY       ,ALIAS = SAL    ,FORMAT = D8   ,$
 FIELD = DATE         ,ALIAS = DATE   ,FORMAT = YMD  ,$
 FIELD = INCREASE     ,ALIAS = INC    ,FORMAT = D6   ,$
END
DBA=JONES76,$
USER=TOM    ,ACCESS=RW, $
USER=BILL   ,ACCESS=R  ,RESTRICT=SEGMENT  ,NAME=COMPSEG    ,$
USER=JOHN   ,ACCESS=R  ,RESTRICT=FIELD    ,NAME=SALARY     ,$
                                           NAME=INCREASE   ,$
USER=LARRY  ,ACCESS=U  ,RESTRICT=FIELD    ,NAME=SALARY     ,$
USER=TONY   ,ACCESS=R  ,RESTRICT=VALUE    ,NAME=IDSEG,
   VALUE=DIVISION EQ 'WEST' ,$
USER=MARY   ,ACCESS=W  ,RESTRICT=VALUE    ,NAME=SALTEST,
   VALUE=INCREASE+SALARY GE SALARY,$
                                           NAME=HISTTEST,
   VALUE=DIV NE ' ' AND DATE GT 0,$
```

参照　データソースセキュリティを実装する際の特別な注意

- JOIN コマンドを使用する場合、データソースの DBA 情報が無視される可能性があります。JOIN 構造では、DBA 情報がホストマスターファイルから読み取られるため、このようなセキュリティ障害が発生します。この問題を解決するには、DBAFILE 機能を使用します。この方法についての詳細は、688 ページの 「 主マスターファイルへのセキュリティ情報の追加 」 を参照してください。JOIN 構造のすべてのデータソースは、DBAFILE でコーディングされたセキュリティ情報を取得します。
- マスターファイルの DBA セクションにコメントを使用することはできません。

データベース管理者の識別 - DBA 属性

セキュリティ属性として最初に指定するのは、データベース管理者を識別するパスワードです。このパスワードの最大長は 64 バイトで、大文字と小文字の区別はありません。このパスワードには、特殊文字を使用することができます。DBA パスワードにブランクを含める場合は、そのパスワードを一重引用符 (') で囲む必要があります。この行を終了するには、単に通常の区切り文字 (,$) を配置します。

注意

- データソースにアクセス制限が設定されている場合、そのデータソースには DBA 属性を指定する必要があります。
- 複数のクロスリファレンスデータソースが存在する場合、そのすべてのデータソースに同一の DBA 属性値を指定する必要があります。
- 分割データソースを USE コマンドで一括読み取りする場合、これらのデータソースには同一の DBA 属性値を指定する必要があります。
- データベース管理者には、データソースとクロスリファレンスデータソースすべてに無制限のアクセスが与えられます。そのため、DBA 属性を使用して、フィールド、セグメント、値の制限を指定することはできません。
- マスターファイルの暗号化および復号化や既存のデータソースの制限を行うには、DBA パスワードが必要です。
- データソースを使用する前に、すべてのセキュリティ属性を十分にテストしておく必要があります。特に、値の制限をテストして、エラーが発生しないことを確認しておくことが重要です。値をテストするには、仮の選別条件を追加したり、各リクエスト文の後に VALIDATE ステートメントを記述したりします。ユーザは値の制限について認識していないため、値の制限によってエラーが発生した場合、ユーザはその原因を理解できない場合があります。

例　DBA 属性によるデータベース管理者の識別

```
DBA=JONES76,$
```

手順　DBA パスワードを変更するには

データベース管理者は、すべてのセキュリティ属性を自由に変更することができます。既存の FOCUS データソースのマスターファイルで DBA パスワードを変更する場合は、RESTRICT コマンドを使用して、この変更で影響を受けるすべての FOCUS データソースにも変更後の DBA パスワードを格納する必要があります。この操作を怠ると、WebFOCUS はこの新しい記述が制限規則を無視していると見なします。影響を受けるすべてのデータソースに対して次の手順を実行します。

1. マスターファイルを編集して、DBA の古い値を新しい値に変更します。
2. 次のコマンドを発行します。

   ```
   SET PASS=old_DBA_password
   ```

3. 次のコマンドを発行します。

   ```
   RESTRICT
   mastername
   END
   ```

4. 次のコマンドを発行します。

   ```
   SET PASS=new_DBA_password
   ```

HOLD ファイルへの DBA 属性の追加

SET HOLDSTAT コマンドを使用して、DBA 情報およびコメントが格納されたデータソースを識別し、その情報を HOLD マスターファイルおよび PCHOLD マスターファイルに自動的に追加することができます。SET HOLDSTAT コマンドについての詳細は、『WebFOCUS アプリケーション作成ガイド』を参照してください。

アクセス権限によるユーザの識別 - USER 属性

USER 属性は、データソースに正規アクセスを与えるユーザを識別するためのパスワードです。USER 属性は、この属性単独で使用することはできません。この属性の後に 1 つ以上の ACCESS 制限を追加して、ユーザに与えるアクセスタイプを指定する必要があります。詳細は、674 ページの 「 アクセス権限タイプの指定 - ACCESS 属性 」 を参照してください。

セキュリティが設定されたデータソースを使用する前に、ユーザは SET PASS または SET USER コマンドを使用してパスワードを入力する必要があります。ユーザが入力したパスワードがマスターファイルに存在しない場合、データソースへのアクセスは拒否されます。ユーザにパスワードが与えられていない場合、またはパスワードは与えられているがリクエストしたアクセスタイプに適合しない場合、次のメッセージが表示されます。

```
(FOC047) ユーザに十分なアクセス権限がありません。ファイル：
filename
```

構文　USER 属性の設定

マスターファイルでユーザ名またはパスワードが宣言されていないユーザは、データソースへのアクセスが拒否されます。USER 属性の構文は次のとおりです。

```
USER = name
```

説明

`name`
: ユーザのパスワードです。パスワードの最大長は 64 バイトです。パスワードには特殊文字を使用することができ、大文字と小文字の区別はありません。パスワードにブランクを含める場合は、パスワードを一重引用符 (') で囲む必要があります。

ブランクのパスワードを指定することができます。変更しない限り、これがデフォルト値です。ブランクのパスワードを指定すると、ユーザは SET PASS= コマンドを発行する必要はありません。ブランクのパスワードを指定した場合でもアクセス制限を設定できるため、多数のユーザに同一のアクセス権限を与える場合にこのパスワードが役立ちます。

例　USER 属性の設定

```
USER=TOM,...
```

次の例では、ユーザのパスワードをブランクに指定し、アクセス権限を読み取り専用に設定しています。

```
USER= , ACCESS=R,$
```

上書き禁止のユーザパスワード (SET PERMPASS)

PERMPASS パラメータを使用して、セッション中または接続中は継続して有効となるユーザパスワードを設定します。この設定は、サポートされているすべてのプロファイルで発行できますが、特にユーザプロファイルで発行すると、特定のユーザに限定してパスワードを作成できるため便利です。このパラメータは、ON TABLE 句で設定することはできません。このパラメータがすべてのユーザに適用されることを回避するため、EDASPROF では設定しないことをお勧めします。

PERMPASS が有効な場合は、既存のマスターファイルの DBA セクションで設定したすべてのセキュリティルールが適用されます。ユーザは、SET PASS または SET USER コマンドを発行して、別のセキュリティルールに従うユーザパスワードに変更を加えることはできません。この変更を加えようとすると、次のメッセージが表示されます。

```
(FOC32409) 恒久 PASS が有効化されています。これ以外は無視されます。
値は変更されていません。
```

注意: 1 回のセッションで設定できる永続パスワードは 1 つです。パスワードを一度設定すると、そのセッション内で変更することはできません。

構文　上書き禁止のユーザパスワードの設定

```
SET PERMPASS=userpass
```

説明

`userpass`
データソースに関連付けられたマスターファイルで DBA セキュリティルールが確立されている場合に、そのデータソースへのアクセスに使用するユーザパラメータです。

例　上書き禁止のユーザパスワードの設定

次の例は、DBA ルールを有効にした MOVIES マスターファイルを示しています。

```
DBA=USER1,$
USER = USERR,  ACCESS = R ,$
USER = USERU,  ACCESS = U ,$
USER = USERW,  ACCESS = W ,$
USER = USERRW, ACCESS = RW,$
```

次のプロシジャで永続パスワードが設定されます。

```
SET PERMPASS = USERU
TABLE FILE MOVIES
PRINT TITLE BY DIRECTOR
END
```

このユーザのアクセス権限は ACCESS=U に設定されているため、ファイルに対して TABLE リクエストを発行することはできません。

```
(FOC047) ユーザに十分なアクセス権限がありません。ファイル：
MOVIES
コマンドの終わりまで処理をバイパスします
```

永続パスワードを変更することはできません。

```
SET PERMPASS = USERRW

(FOC32409) 恒久 PASS が有効化されています。これ以外は無視されます。
値は変更されていません
```

ユーザパスワードを変更することはできません。

```
SET PASS = USERRW

(FOC32409) 恒久 PASS が有効化されています。これ以外は無視されます。
値は変更されていません
```

パスワードの大文字小文字の区別

データベース管理者またはユーザが SET USER、SET PERMPASS、SET PASS コマンドのいずれかを発行すると、DBA 属性を含むマスターファイルすべてのデータソースへのアクセスを許可する前に、このユーザ ID の認証情報が確認されます。このパスワードは、プロシジャを暗号化または復号化する際にも確認されます。

SET DBACSENSITIV コマンドは、確認の前にパスワードを大文字に変換するかどうかを指定します。

構文　パスワードの大文字小文字の切り替え

```
SET DBACSENSITIV = {ON|OFF}
```

説明

ON
: パスワードを大文字に変換しません。ユーザ定義のパスワードと、マスターファイルまたはプロシジャのパスワードを比較する際は、常に大文字と小文字が区別されます。

OFF
: 確認前にパスワードを大文字に変換します。ユーザ定義のパスワードと、マスターファイルまたはプロシジャのパスワードを比較する際は、大文字と小文字は区別されません。デフォルト値は OFF です。

例 パスワードの大文字小文字の切り替え

ここでは、EMPLOYEE マスターファイルに次の DBA 宣言を追加する場合について考察します。

```
USER = User2, ACCESS = RW,$
```

User2 は EMPLOYEE データソースからレポートを作成する必要があるため、次のコマンドを発行します。

```
SET USER = USER2
```

DBACSENSITIV を OFF に設定しているため、入力したパスワードの大文字と小文字がマスターファイルと一致しなくても、User2 はリクエストを実行することができます。

DBACSENSITIV を ON に設定すると、User2 は次のメッセージを受信します。

```
(FOC047) ユーザに十分なアクセス権限がありません。ファイル：filename
```

DBACSENSITIV を ON に設定する場合、ユーザは次のコマンドを発行する必要があります。

```
SET USER = User2
```

ユーザ ID の設定

セキュリティが設定された FOCUS データソースを使用する場合、ユーザはパスワードを入力する必要があります。1 名のユーザが、複数のファイルでそれぞれ異なるパスワードを入力する場合もあります。たとえば、ファイル ONE ではパスワード BILL の権限、ファイル TWO ではパスワード LARRY の権限をそれぞれ適用するような場合です。パスワードを設定するには、SET PASS コマンドを使用します。

構文 ユーザ ID の設定

```
SET {PASS|USER} = name [[IN {file|* [NOCLEAR]}], name [IN file] ...]
```

説明

`name`
ユーザ名またはパスワードです。 パスワードに使用する文字がオペレーティングシステム環境で特別な意味を持つ場合 (例、エスケープ文字)、プロシジャ内で SET USER コマンドを発行し、そのプロシジャを実行してパスワードを設定することができます。SET USER コマンドを発行する場合は、パスワードにブランクが含まれている場合でもパスワードを一重引用符 (') で囲む必要はありません。

`file`
パスワードを適用するマスターファイルの名前です。

*
すべてのファイルのパスワードを name の値で置換します。

NOCLEAR
特定のパスワードリストは変更せずに、有効なパスワードリストのパスワードをすべて置換します。

例 ユーザ ID の設定

次の例では、「TOM」というパスワードが、特定のパスワードが設定されていないすべてのデータソースで有効になります。

```
SET PASS=TOM
```

次の例では、ファイル ONE には「BILL」というパスワード、ファイル TWO には「LARRY」というパスワードが有効になります。その他のファイルにはパスワードは設定されていません。

```
SET PASS=BILL IN ONE, LARRY IN TWO
```

次の例では、ファイル SIX および SEVEN には「DAVE」というパスワード、それ以外のすべてのファイルには「SALLY」というパスワードが有効になります。

```
SET PASS=SALLY, DAVE IN SIX
SET PASS=DAVE IN SEVEN
```

次の例では、ファイル FIVE には「MARY」というパスワード、それ以外のすべてファイルには「FRANK」というパスワードが有効になります。

```
SET PASS=MARY IN FIVE,FRANK
```

特定のファイルに固有のパスワードを設定した場合、それらのファイルのリストは保持されます。このファイルリストを表示するには次のコマンドを発行します。

```
? PASS
```

パスワードを IN * (すべてのファイル) に設定すると、有効なパスワードテーブルはファイル名が関連付けられていない 1 つの値に集約されます。ファイル名のリストを保持するには、NOCLEAR オプションを使用します。

次の例では、すべてのファイルで有効なすべてのパスワードが「KEN」というパスワードに変更され、有効なパスワードテーブルが 1 つの値に集約されます。

```
SET PASS=KEN IN *
```

次の例では、ファイル NINE および TEN の現在有効なパスワードテーブルのすべてのパスワードが「MARY」というパスワードに変更され、その他のすべてのファイルでは「FRANK」というパスワードが有効になります。NOCLEAR オプションを使用すると、指定したファイルリストのすべてのパスワードをすばやく変更することができます。

```
SET PASS=BILL IN NINE,TOM IN TEN
SET PASS=MARY IN * NOCLEAR,FRANK
```

注意：COMBINE コマンドで結合されたデータソースが別のパスワードでセキュリティ設定されている場合は、FIND 関数を使用することはできません。

セキュリティ設定されたデータソースを使用する場合、ユーザはセッションごとに SET PASS コマンドでパスワードを発行する必要があります。ユーザはいつでもパスワードを発行して特定のデータソースにアクセスし、その後、別のパスワードを発行して他のデータソースにアクセスすることができます。

アクセス権限タイプの指定 - ACCESS 属性

ACCESS 属性を使用して、ユーザに与えるアクセス権限のタイプを指定します。DBA 宣言以外のすべてのセキュリティ宣言では、USER 属性および ACCESS 属性を必ず指定します。

次の例は、USER 属性および ACCESS 属性を含むセキュリティ宣言全体を示しています。

```
USER=TOM, ACCESS=RW,$
```

この宣言では、ユーザ Tom に対してデータソースの読み取りおよび書き込み (新しいセグメントインスタンスの追加) のアクセス権限が与えられます。

ACCESS 属性には 4 つの値のいずれかを割り当てることができます。その値は次のとおりです。

`ACCESS=R`	読み取り専用
`ACCESS=W`	書き込み専用
`ACCESS=RW`	データソースの読み取り、新しいセグメントの書き込み
`ACCESS=U`	更新専用

ユーザが発行できるコマンドの種類は、各ユーザに与えられたアクセスレベルにより異なります。ユーザに割り当てるアクセスレベルを決定する前に、各ユーザに必要なコマンドを検討する必要があります。ユーザがコマンドを使用するのに十分なアクセス権限が与えられていない場合、次のメッセージが表示されます。

```
(FOC047) ユーザに十分なアクセス権限がありません。ファイル：filename
```

ACCESS 属性で指定したアクセスレベルにより、ユーザがデータソースに対して実行できる操作が異なります。ユーザがアクセスできるフィールド、値、セグメントを制限するには、RESTRICT 属性を使用します。詳細は、677 ページの 「 データソースのアクセス制限 - RESTRICT 属性 」 を参照してください。すべての USER 属性に対して ACCESS 属性を割り当てる必要があります。RESTRICT 属性はオプションとして設定します。この属性を設定していないと、ユーザはデータソース内のフィールドおよびセグメントに無制限にアクセスすることができます。

アクセス権限のタイプ

下表のように、アクセス権限のタイプに応じて使用可能な WebFOCUS コマンドの種類が異なります。複数のアクセス権限のタイプに印が付いている場合、それは部分的にでもそのコマンドを使用できることを表しています。ただし、同一のコマンドでもユーザに与えられたアクセス権限のタイプにより使用方法が異なる場合がよくあります。

コマンド	R	W	RW	U	DBA
CHECK	X	X	X	X	X
CREATE			X		X
DECRYPT					X
DEFINE	X		X		X
ENCRYPT					X
MATCH	X		X		X
REBUILD			X		X
RESTRICT					X
TABLE	X		X		X

CHECK コマンド　DBA パスワードを持っていないユーザ、または読み取りと書き込み (RW) のアクセス権限が与えられていないユーザは、CHECK コマンドを制限付きで使用することができます。ただし、HOLD オプションが指定されている場合は、「パスワードによりアクセスが制限されました (ACCESS LIMITED BY PASSWORD)」という警告が表示され、DBA RESTRICT 属性に基づいて制限付きのフィールドが HOLD ファイルに継承されます。RESTRICT 属性についての詳細は、677 ページの 「 データソースのアクセス制限 - RESTRICT 属性 」 を参照してください。

CREATE コマンド　DBA パスワードを持っているユーザ、または読み取りと書き込み (RW) の権限が与えられたユーザのみが CREATE コマンドを発行することができます。

DECRYPT コマンド　DBA パスワードを持っているユーザのみが DECRYPT コマンドを発行することができます。

DEFINE コマンド　すべてのレポートコマンドと同様に、読み取り専用 (R) のアクセス権限が与えられたユーザは DEFINE コマンドを使用することができます。読み取り専用 (R) のアクセス権限が与えられた場合、ユーザはデータソースからレコードを読み取り、レポートの作成準備を行うことができます。書き込み専用 (W) または更新専用 (U) のアクセス権限が与えられた場合、ユーザは DEFINE コマンドを使用することはできません。

ENCRYPT コマンド　DBA パスワードを持っているユーザのみが ENCRYPT コマンドを使用することができます。

REBUILD コマンド　DBA パスワードを持っているユーザ、または読み取りと書き込み (RW) のアクセス権限が与えられているユーザのみが REBUILD コマンドを発行することができます。このコマンドは、FOCUS データソース専用です。

RESTRICT コマンド　DBA パスワードを持っているユーザのみが RESTRICT コマンドを使用することができます。

TABLE または MATCH コマンド　読み取り専用 (R) または読み取りと書き込み (RW) のアクセス権限が与えられたユーザは TABLE コマンドを使用することができます。書き込み専用 (W) または更新専用 (U) のアクセス権限が与えられたユーザはこのコマンドを使用することはできません。

参照 RESTRICT 属性のキーワード

RESTRICT 属性のキーワードは、CHECK コマンドで作成される HOLD ファイルに次のような影響を与えます。

FIELD
: NAME パラメータで指定されたフィールドは HOLD ファイルに含まれません。

SEGMENT
: NAME パラメータで指定されたセグメントは HOLD ファイルに含まれますが、そのセグメント内のフィールドは含まれません。

SAME
: NAME パラメータで指定されたユーザと同一の動作特性になります。

NOPRINT
: NAME または SEGNAME パラメータで指定されたフィールドは、ユーザがこれらのフィールドを参照できるため、HOLD ファイルに含まれます。

VALUE
: VALUE パラメータで指定されたフィールドは、ユーザがこれらのフィールドを参照できるため、HOLD ファイルに含まれます。

CHECK コマンドを PICTURE オプションとともに発行すると、RESTRICT 属性のキーワードは結果の図に次のような影響を与えます。

FIELD
: NAME パラメータで指定されたフィールドは図には含まれません。

SEGMENT
: NAME パラメータで指定されたセグメントにはボックスが表示されますが、セグメント内のフィールドには表示されません。

SAME
: NAME パラメータで指定されたユーザと同一の動作特性になります。

NOPRINT
: このオプションは図に影響しません。

VALUE
: このオプションは図に影響しません。

データソースのアクセス制限 - RESTRICT 属性

ACCESS 属性を使用して、ユーザがデータソースに対して実行可能な操作を制御します。

また、オプションの RESTRICT 属性を指定して、特定のフィールド、値、セグメントへのユーザアクセスを制限します。

RESTRICT=VALUE 属性は、IF 句でサポートされている条件で使用することができます。RESTRICT=VALUE_WHERE 属性は、WHERE 句でサポートされているすべての条件で使用することができます (例、フィールド間での比較、関数の使用)。WHERE 式は、可能な場合に構成済みのアダプタに渡されます。

構文　データソースのアクセス制限

```
...RESTRICT=level, NAME={name|SYSTEM} [,VALUE=test],$
```

または

```
...RESTRICT=VALUE_WHERE, NAME=name,  VALUE=expression; ,$
```

説明

`level`
次のいずれかの値です。

- **FIELD**　ユーザは NAME パラメータで指定されたフィールドにアクセスすることはできません。
- **SEGMENT**　ユーザは NAME パラメータで指定されたセグメントにアクセスすることはできません。
- **PROGRAM**　ユーザがデータソースを使用するたびに NAME パラメータで指定されたプログラムが呼び出されます。
- **SAME**　ユーザには NAME パラメータで指定されたユーザと同一の制限が適用されます。ネストされた SAME ユーザは 4 名まで有効です。
- **NOPRINT**　NAME または SEGMENT パラメータで指定されたフィールドをリクエストステートメントに記述することはできますが、そのフィールドは表示されません。VALUE テストを使用して、制限の対象を式の条件を満たす値のみに限定することができます。たとえば、次のように RESTRICT=NOPRINT 宣言を記述した場合、ユーザ MARY が表示できるのは、給与が 10000 未満の従業員の ID のみです。

  ```
  USER=MARY    ,ACCESS=R   ,RESTRICT=NOPRINT   ,NAME=EMP_ID ,
     VALUE=CURR_SAL LT 10000;,$
  ```

  注意：RESTRICT=NOPRINT が設定されたフィールドは、表示コマンド (動詞) で参照することはできますが、すべての種類のフィルタコマンド (例、IF、WHERE、FIND、LOOKUP、VALIDATE) で参照することはできません。

name
制限の対象とするフィールドまたはセグメントの名前です。これを NOPRINT の後に使用すると、フィールドの名前のみが対象になります。値のテストでのみ使用可能な NAME=SYSTEM は、下位のセグメントを含めてデータソース内のすべてのセグメントが制限の対象になります。制限の対象として複数のフィールドまたはセグメントを指定するには、1 名のユーザに対して RESTRICT 属性を複数回発行します。

注意：値の制限を使用する場合、NAME=segment を指定すると、代替ファイルビューにより検索ビューが変更されるかどうかに関係なく、指定されたセグメントと、階層内でそのセグメントの下位にあるセグメントすべてが制限の対象になります。つまり、親セグメントに値の制限があり、JOIN または代替ファイルビューにより子セグメントが新しいルートになった場合でも、元の親セグメントに対する値の制限が新しいルートにそのまま適用されます。

VALUE
ユーザは test パラメータで指定されたテスト条件を満たす値にのみアクセスすることができます。

test
データがこの値のテスト条件を満たす場合に限り、ユーザはこの値にアクセスすることができます。このテスト条件は、IF 句でサポートされる式です。

VALUE_WHERE
ユーザは expression パラメータで指定されたテスト条件を満たす値にのみアクセスすることができます。

expression;
データがこの値のテスト条件を満たす場合に限り、ユーザはこの値にアクセスすることができます。このテスト条件は、WHERE 句でサポートされる式です。

注意：セミコロン (;) が必要です。

例　VALUE_WHERE による値へのアクセス制限

次の DBA 宣言を GGSALES マスターファイルの末尾に追加します。これらの宣言により、USER1 に West 地域および「C」という文字で始まる製品へのアクセス権限が与えられます。

```
END
DBA = USERD,$
USER = USER1, ACCESS = R, NAME = SALES01, RESTRICT = VALUE_WHERE,
       VALUE = REGION EQ 'West' AND PRODUCT LIKE 'C%'; ,$
```

次のリクエストは、USER1 にパスワードを設定し、REGION、CATEGORY、PRODUCT 別に売上および個数の合計を計算します。

```
SET USER = USER1
TABLE FILE GGSALES
SUM DOLLARS UNITS
BY REGION
BY CATEGORY
BY PRODUCT
END
```

出力結果には、マスターファイル内の WHERE 式を満たす地域および製品のみが表示されます。

```
Region       Category     Product           Dollar Sales  Unit Sales
------       --------     -------           ------------  ----------
West         Coffee       Capuccino              915461       72831
             Food         Croissant             2425601      197022
             Gifts        Coffee Grinder         603436       48081
                          Coffee Pot             613624       47432
```

RESTRICT=VALUE_WHERE 属性を RESTRICT=VALUE 属性に変更した場合、この式は無効になります。次のメッセージが表示され、リクエストは実行されません。

```
(FOC002) 無効な語句です。
```

例　データソースのアクセス制限

```
USER=BILL ,ACCESS=R ,RESTRICT=SEGMENT ,NAME=COMPSEG,$
```

フィールドまたはセグメントのアクセス制限

RESTRICT 属性を使用して、ユーザのアクセスを制限するフィールドまたはセグメントを識別します。RESTRICT 属性で指定されていないフィールドまたはセグメントはすべてアクセス可能になります。

RESTRICT 属性を使用しない場合、ユーザはデータソース全体にアクセスすることができます。ユーザのアクセス権限を新しいレコードの読み取り、書き込み、更新のいずれかに限定することはできますが、データソースのすべてのレコードは処理に使用することができます。

構文　フィールドまたはセグメントのアクセス制限

```
...RESTRICT=level,  NAME=name,$
```

説明

`level`

次のいずれかの値です。

`FIELD` - ユーザは NAME パラメータで指定されたフィールドにアクセスすることはできません。

`SEGMENT` - ユーザは NAME パラメータで指定されたセグメントにアクセスすることはできません。

`SAME` - ユーザには NAME パラメータで指定されたユーザと同一の制限が適用されます。

`NOPRINT` - NAME または SEGMENT パラメータで指定されたフィールドをリクエストステートメントに記述することはできますが、そのフィールドは表示されません。これを NOPRINT の後に使用すると、フィールドの名前のみが対象になります。
RESTRICT=NOPRINT が設定されたフィールドは、表示コマンド (動詞) で参照することはできますが、すべての種類のフィルタコマンド (例、IF、WHERE、FIND、LOOKUP、VALIDATE) で参照することはできません。

`name`

制限の対象とするフィールドまたはセグメントの名前です。これを NOPRINT の後に使用すると、フィールドの名前のみが対象になります。

値のテストでのみ使用可能な NAME=SYSTEM は、下位のセグメントを含めてデータソース内のすべてのセグメントが制限の対象になります。制限の対象として複数のフィールドまたはセグメントを指定するには、1 名のユーザに対して RESTRICT 属性を複数回発行します。

注意

- NAME 属性にフィールドまたはセグメントが記述されている場合、ユーザがそのフィールドまたはセグメントを取得することはできません。リクエストステートメントでこのようなフィールドまたはセグメントが記述されている場合、そのリクエストはユーザのアクセス権限を超えているとして拒否されます。NOPRINT を使用した場合、フィールドまたはセグメントを記述することはできますが、データは表示されません。このデータは、文字フォーマットのフィールドではブランク、数値フォーマットのフィールドでは 0 (ゼロ) として表示されます。RESTRICT=NOPRINT が設定されたフィールドは、表示コマンド (動詞) で参照することはできますが、すべての種類のフィルタコマンド (例、IF、WHERE、FIND、LOOKUP、VALIDATE) で参照することはできません。

- 複数のフィールドまたはセグメントを制限するには、RESTRICT ステートメントを複数回記述します。たとえば、Harry に対してフィールド A とセグメント B の使用を制限するには、次のアクセス制限を発行します。

```
USER=HARRY, ACCESS=R, RESTRICT=FIELD,   NAME=A,$
   RESTRICT=SEGMENT, NAME=B,$
```

- フィールドとセグメントのアクセス制限は、必要に応じていくつでも追加することができます。
- RESTRICT=SAME は、複数のパスワードに共通した一連の制限を繰り返し使用する場合に役立ちます。新しいユーザに RESTRICT=SAME を指定し、USER 属性の NAME 値で指定されたユーザ名またはパスワードを使用すると、このユーザにはこの NAME 属性で指定されたユーザと同一の制限が適用されます。必要に応じて、他の制限を後から追加することができます。

例　セグメントのアクセス制限

次の例では、「Bill」というユーザに、データソースの COMPSEG セグメントを除くすべてのデータへの読み取り専用のアクセス権限が与えられています。

```
USER=BILL ,ACCESS=R ,RESTRICT=SEGMENT ,NAME=COMPSEG,$
```

例　共通のアクセス制限の再利用

次の例では、Sally および Harry に Bill と同一のアクセス権限が与えられています。また、Sally は SALARY フィールドの読み取りが制限されています。

```
USER=BILL, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
     VALUE=DIVISION EQ 'WEST',$
USER=SALLY, ACCESS=R, RESTRICT=SAME, NAME=BILL,$
                      RESTRICT=FIELD, NAME=SALARY,$
USER=HARRY, ACCESS=R, RESTRICT=SAME, NAME=BILL,$
```

注意：特定のセグメントへのアクセス制限は、その下位にも影響します。

値のアクセス制限

RESTRICT 属性にテスト条件を設定して、ユーザアクセスを特定の値のみに制限することができます。ユーザが使用できる値は、テスト条件に一致する値に限定されます。

値を制限する方法は 2 つあります。ユーザがデータソースから読み取れる値を制限する方法と、ユーザがデータソースに書き込める値を制限する方法です。これらの 2 つの制限は、互いに独立して機能します。ACCESS 属性を使用して、ユーザが読み取れる値と書き込める値のどちらを制限するかを指定します。

ユーザが読み取れる値を制限するには、ACCESS=R および RESTRICT=VALUE を設定します。このタイプの制限を設定すると、ユーザが参照できるデータは RESTRICT 属性で指定されたテスト条件に一致する値に限定され、その他すべての値は参照できなくなります。RESTRICT 属性に ACCESS=R を使用すると、レポートリクエストで指定する強制 IF ステートメントのように機能します。そのため、ACCESS=R で値を制限する構文は、レポートリクエストの IF テストの規則に従う必要があります。

構文　ユーザが読み取り可能な値の制限

```
...ACCESS=R, RESTRICT=VALUE, NAME=name, VALUE=test,$
```

説明

`name`
テスト条件を有効にするセグメントの名前です (テスト条件として参照されている場合)。データソースのすべてのセグメントを指定するには、NAME=SYSTEM を使用します。

`test`
実行するテストです。

例　ユーザが読み取り可能な値の制限

```
USER=TONY, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
     VALUE=DIVISION EQ 'WEST',$
```

この制限では、Tony は WEST 地区からのレコードのみを読み取ることができます。

テスト条件の式は VALUE= の後に入力します。テスト条件の構文は、レコードの選別時に TABLE コマンドで使用する構文と同一です。ただし、この句の前に「IF」という語句は使用しません。TABLE コマンドで使用する選別条件についての詳細は、『TIBCO WebFOCUS Language リファレンス』を参照してください。複数のフィールドでテストを実行する場合は、VALUE 属性をさらに追加する必要があります。各テストには、テストを適用するセグメント名をそれぞれ指定する必要があります。以下はその例です。

```
USER=DICK, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
     VALUE=DIVISION EQ 'EAST' OR 'WEST',$
     NAME=IDSEG,
     VALUE=SALARY LE 10000,$
```

1 つのテスト条件が行の許容する長さを超える場合は、複数のセクションに分割して記述することができます。各セクションは VALUE= 属性で開始し、終了文字 (,$) で終了する必要があります。以下はその例です。

```
USER=SAM, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
     VALUE=DIVISION EQ 'EAST' OR 'WEST',$
     VALUE=OR 'NORTH' OR 'SOUTH',$
```

注意：値の制限を指定した 2 行目以降は、キーワードの OR で開始する必要があります。

テスト条件は、テストを適用するデータセグメントの親セグメントに対して適用することができます。ここでは、次の例について考察します。

```
USER=DICK, ACCESS=R, RESTRICT=VALUE, NAME=IDSEG,
     VALUE=DIVISION EQ 'EAST' OR 'WEST',$
     NAME=IDSEG,
     VALUE=SALARY LE 10000,$
```

「SALARY」というフィールドは、実際には COMPSEG というセグメントの一部です。NAME=IDSEG でテストを指定しているため、このテストは親セグメントの IDSEG に対するリクエストで有効になります。この場合、「PRINT FULLNAME」というリクエストでは、このテストが下位セグメント IDSEG の一部となるフィールドで実行されたにも関わらず、このテスト条件に一致する従業員、つまり給与が $10,000 以下の従業員の氏名のみが表示されます。ただし、このテストが COMPSEG 上 (つまり NAME=COMPSEG) で有効になった場合、データソースの全員の氏名が取得されますが、このテスト条件に一致する給与情報のみが取得されます。

値の読み取りと書き込みの制限

ユーザに適用する値の制限として、ACCESS=W (データ更新用) と ACCESS=R (データ検索用) の両方を発行すると便利な場合が多くあります。これにより、ユーザがデータソースに書き込める値とユーザが実際に閲覧できる値の両方が制限されます。この制限を適用するには、RESTRICT=VALUE 属性の発行時に ACCESS=R を追加します。これにより、ユーザはテスト条件で指定された値以外の値を参照できなくなります。さらに、RESTRICT=VALUE 属性の発行時に ACCESS=W を使用すると、このユーザに書き込み制限が追加されます。ACCESS=RW を使用してこの設定を行うことはできません。

注意：このマニュアルに説明はありませんが、書き込み制限はデータ管理機能に適用されます。

マルチファイル構造でのアクセス制限のソース制御

DBASOURCE パラメータにより、マルチファイル構造へのアクセスを許可するセキュリティ属性が指定されます。デフォルト設定では、アクセス制限は JOIN 構造のホストファイル、または COMBINE 構造の最後のファイルに基づいて決定されます。DBASOURCE パラメータを「ALL」に設定した場合、JOIN または COMBINE 構造のファイルすべてのアクセス制限が適用されます。

注意：JOIN 構造および COMBINE 構造のファイルすべてのアクセス制限を格納して適用するには、DBAFILE を作成して実行することもできます。主マスターファイルにアクセス制限を含める方法についての詳細は、688 ページの 「 主マスターファイルへのセキュリティ情報の追加 」 を参照してください。

SET DBASOURCE コマンドは 1 回のセッションまたは接続につき、一度だけ発行することができます。それ以上コマンドを発行しようとしても、2 回目以降は無視されます。値がプロファイルで設定されている場合、セッション中にユーザが変更することはできません。

DBASOURCE=ALL の場合は、次のようになります。

- JOIN 構造に対する TABLE リクエストでは、ユーザが構造内の各ファイルに最低読み取り権限を所有している場合に限り、クロスリファレンスファイルおよびクロスリファレンスセグメントへのアクセスが許可されます。

DBASOURCE=HOST の場合は、次のようになります。

- TABLE リクエストでは、ユーザは JOIN 構造のホストファイルの読み取り権限が必要です。セキュリティ制限は、すべてホストファイルから適用されます。構造内のファイルのセキュリティ制限を適用するには、DBAFILE を作成して有効にすることもできます。

構文　JOIN または COMBINE 構造のアクセス制限適用制御

```
SET DBASOURCE = {HOST|ALL}
```

説明

HOST
: DBAFILE を使用して、構造内の別ファイルのアクセス制限を適用する場合を除き、JOIN 構造のホストファイル、または COMBINE 構造の最後のファイルに、アクセス制限を限定します。デフォルト値は HOST です。

ALL
: ユーザには、JOIN 構造および COMBINE 構造のファイルすべてに読み取り権限が必要です。このファイルに INCLUDE、DELETE、または UPDATE コマンドを発行する場合、ユーザに WRITE、UPDATE、または READ/WRITE アクセス権限が必要です。

参照　SET DBASOURCE 使用時の注意

- JOIN 構造および COMBINE 構造のファイルには、すべて同一の DBA パスワードが設定されている必要があります。DBA 属性が同一でない場合、構造にアクセスする方法はありません。

- SET DBASOURCE コマンドがセッション中に複数回発行された場合は、次のメッセージが表示され、値は変更されません。

```
(FOC32575) DBASOURCE を再設定できません。
値は、変更されていません
```

例 JOIN 内のアクセス制限制御

次のリクエストにより、TRAINING データソースが EMPDATA データソースと COURSE データソースに結合され、JOIN 構造に対してリクエストが発行されます。

```
JOIN CLEAR *
JOIN COURSECODE IN TRAINING TO COURSECODE IN COURSE AS J1
JOIN PIN IN TRAINING TO PIN IN EMPDATA AS J2
TABLE FILE TRAINING
PRINT COURSECODE AS 'CODE' CTITLE
   LOCATION AS 'LOC'
BY LASTNAME
WHERE COURSECODE NE '    '
WHERE LOCATION EQ 'CA' OR LOCATION LIKE 'N%'
END
```

マスターファイルに DBA 属性が存在しない場合、出力は次のようになります。

```
LASTNAME         CODE     CTITLE                                LOC
--------         ----     ------                                ---
ADAMS            EDP750   STRATEGIC MARKETING PLANNING          NJ
CASTALANETTA     EDP130   STRUCTURED SYS ANALYSIS WKSHP         NY
                 AMA130   HOW TO WRITE USERS MANUAL             CA
CHISOLM          EDP690   APPLIED METHODS IN MKTG RESEARCH      NJ
FERNSTEIN        MC90     MANAGING DISTRIBUTOR SALE NETWORK     NY
GORDON           SFC280   FUND OF ACCTG FOR SECRETARIES         NY
LASTRA           MC90     MANAGING DISTRIBUTOR SALE NETWORK     NY
MARTIN           EDP130   STRUCTURED SYS ANALYSIS WKSHP         CA
MEDINA           EDP690   APPLIED METHODS IN MKTG RESEARCH      NJ
OLSON            PU168    FUNDAMNETALS OF MKTG COMMUNICATIONS   NY
RUSSO            PU168    FUNDAMNETALS OF MKTG COMMUNICATIONS   NY
SO               BIT420   EXECUTIVE COMMUNICATION               CA
WANG             PU440    GAINING COMPETITIVE ADVANTAGE         NY
WHITE            BIT420   EXECUTIVE COMMUNICATION               CA
```

さらに、次の DBA 属性を TRAINING マスターファイルの最後に追加します。

```
END
DBA = DBA1,$
USER = TUSER, ACCESS =R,$
```

同一のリクエストを実行すると、次のメッセージが生成されます。

```
(FOC047) ユーザに十分なアクセス権限がありません。ファイル：
TRAINING
コマンドの終わりまで処理をバイパスします
```

さらに、次の SET PASS コマンドを発行します。

```
SET PASS = TUSER
```

次の DBA 属性を COURSE マスターファイルの最後に追加します。

```
END
DBA = DBA1,$
USER = CUSER, ACCESS = R,$
```

次の DBA 属性を EMPDATA マスターファイルの最後に追加します。

```
END
DBA = DBA1,$
USER = EUSER, ACCESS = R,$
```

DBA 属性の値は、すべてのマスターファイルで共通です。

リクエストを再度実行します。セキュリティ違反は発生せずに、レポート出力が生成されます。DBASOURCE パラメータは、デフォルト設定で「HOST」に設定されているため、ホストファイル内のみで有効なパスワードを使用して、リクエストを実行することができます。

さらに、DBASOURCE パラメータを「ALL」に設定します。

```
SET DBASOURCE = ALL
SET PASS = TUSER
```

TUSER は COURSE データソースで有効なユーザではないため、リクエストを実行すると、次のようなメッセージが生成されます。

```
(FOC052) フィールドに対するパスワードが無効です
```

さらに、次の SET PASS コマンドを発行して、各ファイルに有効なパスワードを設定します。

```
SET PASS = TUSER IN TRAINING, CUSER IN COURSE, EUSER IN EMPDATA
```

ここで、リクエストを実行し、レポート出力を生成することができます。

SET DBASOURCE コマンドの発行後、値を変更することはできません。次の SET コマンドは、値の「HOST」への変更を試みますが、クエリコマンド出力は、変更が実行されなかったことを示しています。

```
>  > set dbasource = host
(FOC32575) DBA SOURCE を再設定できません。
値は、変更されていません
```

JOIN 条件への DBA 制限の追加

複数セグメント構造のリクエストに DBA 制限を適用すると、デフォルト設定で、その制限がリクエストの WHERE 条件として追加されます。DBAJOIN パラメータを ON に設定すると、DBA 制限が、それらが指定されているファイルまたはセグメントに対して内部的な制限として処理され、JOIN 構文に追加されます。

制限の対象とするファイルまたはセグメントに構造上の親が含まれ、その JOIN が OUTER JOIN または UNIQUE JOIN の場合、この違いが重要になります。

制限がレポートフィルタとして処理される場合、そのフィルタに一致しない下位セグメントインスタンスは、ホストセグメントとともにレポート出力から省略されます。ホストセグメントが省略されるため、出力には OUTER JOIN または UNIQUE JOIN が正しく反映されません。

制限が JOIN 条件として処理される場合、その JOIN 条件に一致しない下位セグメントインスタンスはミッシング値として表示され、レポート出力にはホスト行がすべて表示されます。

詳細は、『TIBCO WebFOCUS Language リファレンス』を参照してください。

主マスターファイルへのセキュリティ情報の追加

DBAFILE 属性を使用して、複数のマスターファイルのすべてのパスワードおよびセキュリティ制限を 1 つのファイルに集約することができます。個々のマスターファイルは、この主マスターファイルを参照します。複数のマスターファイルで同一の DBA パスワードを使用する場合は、共通の DBAFILE でこの DBA パスワードを共有することができます。

この方法には次のような利点があります。

- パスワードを複数のデータソースに適用する場合でもパスワードを別々に格納する必要がないため、パスワードの管理が簡略化されます。
- JOIN または COMBINE コマンドを使用して、異なるユーザパスワードを使用するデータソースを結合することができます。また、JOIN または COMBINE で結合された各データソースでそれぞれの DBA 情報は保持されます。

主 DBAFILE は標準的なマスターファイルです。DBAFILE 属性で主マスターファイルの名前を指定することにより、他のマスターファイルでも主マスターファイルのパスワードおよびセキュリティ制限を使用することができます。

注意

- 同一の DBAFILE を指定したすべてのマスターファイルは、共通の DBA パスワードを持ちます。
- 管理用の DBAFILE では、通常のマスターファイルのように END ステートメントの前に 1 つ以上のセキュリティ宣言と 1 つのフィールド宣言を記述して、DBA 情報が含まれていることを示す必要があります。必須の属性に特定の値を割り当てない場合でも、そのことをカンマ (,) で明示する必要があります。DBAFILE の DBA パスワードは、このファイルを参照する他のすべてのマスターファイルのパスワードと共通です。これにより、個人が各自のセキュリティを変更することを防止します。すべてのマスターファイルは暗号化する必要があります。
- DBAFILE には、DBA パスワードの後にパスワードおよび制限を列記することができます。これらのパスワードは、この DBAFILE を参照するすべてのデータソースに適用されます。
- DBAFILE では、共通パスワードの後にデータソース固有のパスワードおよび一般パスワードの追加分を指定することができます。この機能を実装するには、DBAFILE の DBA セクションに FILENAME 属性を追加します (例、FILENAME=TWO)。FILENAME 属性についての詳細は、693 ページの 「 DBAFILE ファイル名の規則 」 を参照してください。
- データソースに固有の制限は、指定したデータソースに適用された一般の制限を上書きします。これらの制限が競合する場合は、FILENAME セクションのパスワードが優先されます。たとえば、DBAFILE の共通セクションに ACCESS=RW が指定されている場合でも、特定のデータソースに対して FILENAME セクションを追加し、同一のパスワードに ACCESS=R を指定することができます。
- 追加した値の制限はすべて累積されるため、データを取得する場合はすべての値の制限を満足させなければなりません。以降の例では、PASS=JOE を 2 回使用しています。JOE はすべてのデータソースに適用された共通パスワードですが、FILENAME=THREE では「RESTRICT=...」というデータソース THREE にのみ適用される別の制限が追加されています。

構文　主マスターファイルへのセキュリティ属性の追加

```
END
DBA=dbaname, DBAFILE=filename ,$
```

説明

`dbaname`
　主マスターファイルの dbaname と同一の名前です。

filename
　主マスターファイル名です。

DBAFILE でパスワードと制限を指定し、その DBAFILE を参照するすべてのマスターファイルにそのパスワードと制限を適用することができます。また、DBAFILE に FILENAME 属性を追加して、特定のマスターファイルにのみ適用するパスワードと制限を指定することもできます。

例　主マスターファイルへのセキュリティ属性の追加

次の例は、複数のマスターファイルで「FOUR」という共通の DBAFILE を共有する方法を示しています。

```
ONE MASTER
FILENAME=ONE
  .
  .
END
DBA=ABC, DBAFILE=FOUR,$


TWO MASTER
FILENAME=TWO
  .
  .
END
DBA=ABC, DBAFILE=FOUR,$


THREE MASTER
FILENAME=THREE
  .
  .
END
DBA=ABC,
DBAFILE=FOUR,$


FOUR MASTER
FILENAME=FOUR,$
SEGNAME=mmmmm,$
FIELDNAME=fffff,$
END
DBA=ABC,$
   PASS=BILL,ACCESS=R,$
   PASS=JOE,ACCESS=R,$
FILENAME=TWO,$
   PASS=HARRY,ACCESS=RW,$
FILENAME=THREE,$
   PASS=JOE,ACCESS=R,RESTRICT=...,$
   PASS=TOM,ACCESS=R,$
```

例　JOIN 構造での DBAFILE の使用

次のリクエストにより、TRAINING データソースが EMPDATA データソースと COURSE データソースに結合され、JOIN 構造に対してリクエストが発行されます。

```
JOIN CLEAR *
JOIN COURSECODE IN TRAINING TO COURSECODE IN COURSE AS J1
JOIN PIN IN TRAINING TO PIN IN EMPDATA AS J2
TABLE FILE TRAINING
PRINT COURSECODE AS 'CODE' CTITLE
   LOCATION AS 'LOC'
BY LASTNAME
WHERE COURSECODE NE '    '
WHERE LOCATION EQ 'CA' OR LOCATION LIKE 'N%'
END
```

マスターファイルに DBA 属性が存在しない場合、出力は次のようになります。

```
LASTNAME         CODE     CTITLE                                LOC
--------         ----     ------                                ---
ADAMS            EDP750   STRATEGIC MARKETING PLANNING          NJ
CASTALANETTA     EDP130   STRUCTURED SYS ANALYSIS WKSHP         NY
                 AMA130   HOW TO WRITE USERS MANUAL             CA
CHISOLM          EDP690   APPLIED METHODS IN MKTG RESEARCH      NJ
FERNSTEIN        MC90     MANAGING DISTRIBUTOR SALE NETWORK     NY
GORDON           SFC280   FUND OF ACCTG FOR SECRETARIES         NY
LASTRA           MC90     MANAGING DISTRIBUTOR SALE NETWORK     NY
MARTIN           EDP130   STRUCTURED SYS ANALYSIS WKSHP         CA
MEDINA           EDP690   APPLIED METHODS IN MKTG RESEARCH      NJ
OLSON            PU168    FUNDAMNETALS OF MKTG COMMUNICATIONS   NY
RUSSO            PU168    FUNDAMNETALS OF MKTG COMMUNICATIONS   NY
SO               BIT420   EXECUTIVE COMMUNICATION               CA
WANG             PU440    GAINING COMPETITIVE ADVANTAGE         NY
WHITE            BIT420   EXECUTIVE COMMUNICATION               CA
```

EMPDATA マスターファイルがリクエストの主 DBAFILE になります。次の DBA 属性を EMPDATA マスターファイルの最後に追加します。

```
END
DBA=DBA1,$
USER = EUSER, ACCESS = R,$
FILENAME = COURSE
USER = CUSER2, ACCESS=RW,$
```

これらの属性により、EUSER ユーザには、DBAFILE として EMPDATA を使用するすべてのファイルへの読み取りアクセス権限が与えられます。CUSER2 ユーザには、COURSE データソースへの読み取りと書き込みのアクセス権限が与えられます。

次のセキュリティ属性を COURSE マスターファイルの最後に追加します。これらの属性により、EMPDATA マスターファイルが主ファイルになり、このファイル内のセキュリティ情報が COURSE データソースへのアクセスに使用されます。これにより、DBA 属性の値が、EMPDATA マスターファイルの DBA 属性の値と同一になります。

```
END
DBA = DBA1, DBAFILE=EMPDATA,$
```

次のセキュリティ属性を TRAINING マスターファイルの最後に追加します。これらの属性により、EMPDATA マスターファイルが主ファイルになり、このファイル内のセキュリティ情報が TRAINING データソースへのアクセスに使用されます。これにより、DBA 属性の値が、EMPDATA マスターファイルの DBA 属性の値と同一になります。

```
END
DBA = DBA1, DBAFILE=EMPDATA,$
```

これで、この JOIN 構造に対してリクエストを実行するには、JOIN 構造の各ファイルへの読み取りアクセス権限を持つ現在のユーザパスワードが必要になります。次の SET PASS コマンドを発行してリクエストを実行します。

```
SET PASS = EUSER
```

または

```
SET PASS = EUSER IN *
```

EUSER ユーザは JOIN 構造の各ファイルで有効なユーザであるため、リクエストが実行され、出力結果が生成されます。

EMPDATA マスターファイルは CUSER2 ユーザを COURSE マスターファイルの有効なユーザとして識別するため、次の SET PASS コマンドを発行してリクエストを実行することもできます。

```
SET USER = EUSER IN EMPDATA, EUSER IN TRAINING, CUSER2 IN COURSE
```

JOIN 構造の各ファイルに無効なパスワードを指定して SET PASS コマンドを発行すると、次のいずれかのメッセージが生成され、リクエストは実行されません。

```
(FOC052) フィールドに対するパスワードが無効です：フィールド名
```

```
(FOC047) ユーザに十分なアクセス権限がありません。ファイル：filename
```

DBAFILE ファイル名の規則

DBAFILE に FILENAME 属性を追加して特定のマスターファイルを指定する場合、参照する側のマスターファイルの FILENAME 属性と、DBAFILE の DBA セクションで指定する FILENAME 属性は一致させる必要があります。これにより、ユーザがマスターファイルの名前を変更して、DBAFILE が理解できない名前になることが回避されます。

例　DBAFILE 名の規則

```
ONE MASTER
FILENAME=XONE
   .
   .
   .
END
DBA=ABC, DBAFILE=FOUR,$


FOUR MASTER
FILENAME=XFOUR
   .
   .
   .
END
DBA=ABC,$
   .
   .
   .
FILENAME=XONE,$
   .
   .
   .
```

ONE MASTER は、リクエストでは「TABLE FILE ONE」として参照されます。ただし、ONE MASTER および DBAFILE である FOUR MASTER の DBA セクションの両方で FILENAME=XONE を指定します。

セキュリティ上の理由から、DBAFILE 情報を含むマスターファイルの FILENAME 属性には、マスターファイル名とは異なる名前を指定することをお勧めします。なお、FOUR MASTER では FILENAME 属性に「XFOUR」という名前を指定しています。

DBAFILE による既存 DBA システムへの接続

既存のシステムでは、新しい属性である DBAFILE を使用しない場合、システムの特性に変更はありません。現在のシステムでは、複数のデータソースを JOIN コマンドで結合した場合、リスト内の最初のデータソースがコントロールデータソースになります。そのデータソースのパスワードのみが検証の対象になります。複数のデータソースを COMBINE コマンドで結合した場合は、最後のデータソースのパスワードのみが有効になります。この場合、すべてのデータソースで DBA パスワードを一致させる必要があります。

新しいシステムでは、JOIN または COMBINE で結合したすべてのデータソースの DBA セクションが検証の対象になります。マスターファイルに DBAFILE が含まれている場合は、そのパスワードおよびセキュリティ制限が読み込まれます。JOIN または COMBINE のリストでデータソースの DBA セクションを有効にするには、そのデータソースの DBAFILE を指定します。

新しいシステムの使用を開始した段階で、すべてのマスターファイルを変換します。データベース管理者が既存のシステムを変換する際に別の物理 DBAFILE を作成したくない場合は、DBAFILE 属性でデータソース自体を指定することもできます。

例　DBAFILE による既存の DBA システムへの接続

```
FILENAME=SEVEN,
  SEGNAME=..
    FIELDNAME=...
      .
      .
      .
END
DBA=ABC,DBAFILE=SEVEN,$    (OR DBAFILE= ,$)
 PASS=...
 PASS=...
```

DBAFILE によるアプリケーションの結合

各データソースにはそれぞれ独自の制限が設定されているため、異なるアプリケーションのデータソースや異なるユーザパスワードを持つデータソースを取り扱う場合でも、これらのデータソースを JOIN コマンドおよび COMBINE コマンドで結合することができます。ここでの要件は、各データソースで有効なパスワードのみです。ここで、現在のシステムのパスワードを割り当てることにより、異なるデータベース管理者の管理下のアプリケーションに別のアプリケーションのアクセス権限を与えることができます。

データソースに選別条件を割り当て、データソースにアクセスするすべてのレポートリクエストにその選別条件を自動的に適用することができます。詳細は、『TIBCO WebFOCUS Language リファレンス』を参照してください。

セキュリティ属性の概要

下表は、WebFOCUS で使用するセキュリティ属性の一覧です。

属性	エイリアス	最大長	説明
DBA	DBA	8	割り当てる値は、データソースに無制限でアクセス可能なデータベース管理者 (DBA) のコード名です。
USER	PASS	8	割り当てる値は、セキュリティ制限を設定するユーザを識別するための任意のコード名です。
ACCESS	ACCESS	8	このユーザのアクセスレベルです。次の値があります。 R - 読み取り専用 W - 新しいセグメントの書き込み専用 RW - 読み取りと書き込み U - 値の更新専用
RESTRICT	RESTRICT	8	このアクセスレベルに適用する制限のタイプです。次の値があります。 SEGMENT FIELD VALUE SAME NOPRINT
NAME	NAME	66	制限の対象となるセグメントまたはフィールドの名前、あるいは呼び出すプログラムの名前です。
VALUE	VALUE	80	制限のタイプとして RESTRICT=VALUE を指定した場合に、結果が TRUE となるテスト条件の式です。

属性	エイリアス	最大長	説明
DBAFILE	DBAFILE	8	使用するパスワードおよび制限が格納されたマスターファイルの名前です。

制限規則の非表示 - ENCRYPT コマンド

FOCUS データソースの制限情報はマスターファイルに保存されるため、ユーザがその制限規則を検査できないようにマスターファイルを暗号化する必要があります。記述した内容を暗号化できるのはデータベース管理者のみです。ENCRYPT コマンドを発行する前に、PASS=DBAname を設定しておく必要があります。なお、ENCRYPT コマンドの構文は、オペレーティングシステムの種類により異なります。

注意：暗号化するマスターファイルの 1 行目は、68 バイト以下にする必要があります。68 バイトを超える場合、複数行に分割する必要があります。

構文　制限規則の非表示 - ENCRYPT コマンド

```
ENCRYPT FILE filename
```

説明

`filename`
　暗号化するファイルの名前です。

例　マスターファイルの暗号化と復号化

次の例は、プロシジャ全体を示しています。

```
SET PASS=JONES76
ENCRYPT FILE PERS
```

制限を変更する場合は、上記の逆の手順を実行します。その場合は、DECRYPT コマンドを使用して、記述内容を読み取り可能な形式で保存します。

ファイルを復号化する前に、SET コマンドで DBA パスワードを発行しておく必要があります。以下はその例です。

```
SET PASS=JONES76
DECRYPT FILE PERS
```

データの暗号化

マスターファイルに ENCRYPT パラメータを使用して、すべてのセグメントまたはその一部を暗号化することもできます。暗号化したファイルを外部メディア (ディスクまたはテープ) に保存した場合でも、各ファイルは許可されていないアクセスに対してセキュリティが確保されます。

暗号化はセグメントレベルで実行されます。つまり、セグメント全体が暗号化されます。暗号化をリクエストするには、マスターファイルで ENCRYPT 属性を ON に設定します。

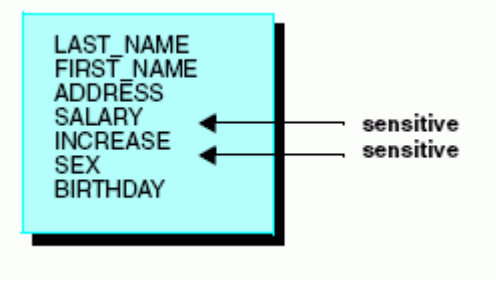
例　データの暗号化

```
SEGMENT=COMPSEG, PARENT=IDSEG, SEGTYPE=S1, ENCRYPT=ON,$
```

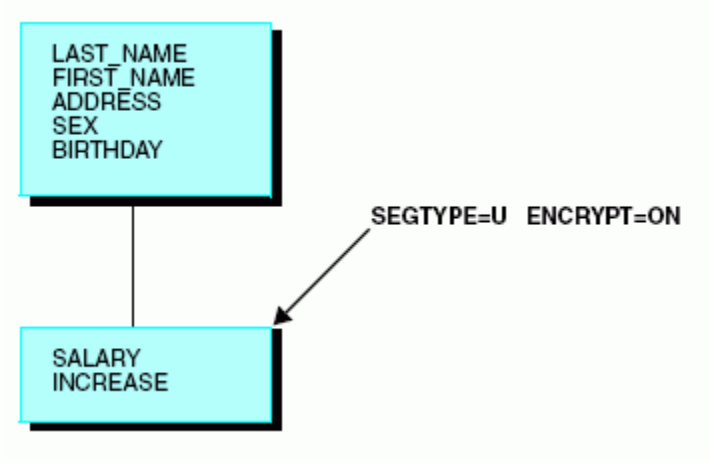
データソースにデータを入力する前に、ENCRYPT パラメータを指定する必要があります。暗号化をはじめてリクエストする場合、「NEW FILE...」というメッセージが表示されます。マスターファイルに変更を加えて暗号化を後からリクエストすることはできません。また、リクエスト後またはデータソースに何らかのデータを入力した後では暗号化を解除することはできません。

暗号化したデータのパフォーマンスに関する注意

データを暗号化すると処理効率がわずかに低下します。処理効率の低下を最小限に抑えるには、セグメント上で暗号化の必要なデータフィールドのみをグループ化し、それを独立したユニークセグメント (SEGTYPE=U) として元のセグメントの下に配置します。たとえば、セグメント上に次のようなデータ項目があることを想定します。



次のようにグループ化します。



注意：DBA パスワードを変更するには、RESTRICT コマンドを発行する必要があります。詳細は、668 ページの 「 DBA パスワードを変更するには 」 を参照してください。

プロシジャのセキュリティ

データセキュリティに関する問題の大部分は、WebFOCUS DBA イグジットルーチンを使用して解決するのが最善の方法です。WebFOCUS DBA イグジットルーチンについての詳細は、『TIBCO WebFOCUS セキュリティ管理ガイド』を参照してください。また、プロシジャを暗号化および復号化することもできます。

プロシジャの暗号化と復号化

プロシジャの実行をユーザに許可した場合でも、プロシジャ内のテキストデータを機密扱いにする必要があります。それは、プロシジャに機密情報が含まれていたり、権限のないユーザによるプロシジャの変更を回避するためです。保存したプロシジャを権限のないユーザから保護するには、ENCRYPT コマンドを使用します。

暗号化したプロシジャは、すべてのユーザが実行できますが、その内容を参照するにはプロシジャを復号化する必要があります。プロシジャを復号化できるのは、暗号化パスワードを持っているユーザのみです。

プロシジャを暗号化または復号化するためにユーザが選択したパスワードはエディタには表示されず、使用するファイルの DBA パスワードとは関連性はありません。

構文　プロシジャの暗号化と復号化

次のプロシジャを使用して「SALERPT」という名前のプロシジャを暗号化します。

```
SET PASS = DOHIDE
ENCRYPT FILE SALERPT FOCEXEC
```

次のプロシジャを使用して「SALERPT」という名前のプロシジャを復号化します。

```
SET PASS = DOHIDE
DECRYPT FILE SALERPT FOCEXEC
```

F

App Studio カスタムログインテンプレート

WebFOCUS をカスタムセキュリティで保護している場合、カスタムログインテンプレートを使用することで、App Studio から WebFOCUS にアクセスすることができます。ログインテンプレートは、カスタムセキュリティソリューションに固有の動作を定義するもので、管理者が作成します。

このテンプレートでは、XML タグを使用して次のことを記述します。

- ログインリソースの検索方法。これらのリソースには Servlet、JSP、ASP、CGI のいずれかが含まれ、セキュリティシステムへのユーザのログインに使用されます。
- ログイン結果。正常ログインの後、セキュリティシステムは Cookie を返す必要があります。App Studio ソフトウェアは、この Cookie をサイトに継続的に転送することで、セッションが終了するまで WebFOCUS 環境を保護します。

セキュリティシステム技術の知識を持つ管理者は、テンプレートを作成し、それを各開発者に配信、またはネットワーク上の共有ロケーションから参照することができます。開発者は [環境のプロパティ] ダイアログボックスでカスタムログインテンプレートを選択し、このテンプレートを使用して、保護された WebFOCUS 環境にアクセスします。

トピックス

ログインテンプレートの動作

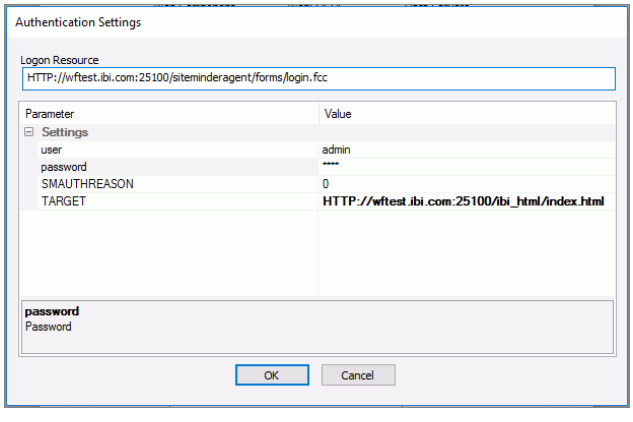
カスタムログインテンプレートは、「dssso.xml」というファイルに格納されます。このファイルは、App Studio ソフトウェアとともに drive:¥ibi¥AppStudio82¥bin ディレクトリにインストールされ、次の Windows レジストリキーで格納先が指定されています。

```
HKEY_CURRENT_USER¥Software¥Information Builders¥
AppStudio¥82¥FOCSHELL¥WFSCOM
```

デフォルト設定では、このキーは drive:¥ibi¥AppStudio82¥bin¥dssso.xml ファイルを指定しています。このファイルには、次のセキュリティプロバイダのテンプレートが格納されています。

- SiteMinder.
- RSA Access Manager
- WebSEAL
- Oracle Access Manager
- Basic、IWA、Kerberos ではテンプレートは使用されません。

UNC (Universal Naming Convention。例、¥¥wftest¥sharedfiles¥dssso.xml) を使用して、ファイルのネットワーク上の共有コピーファイルを指定することができます。



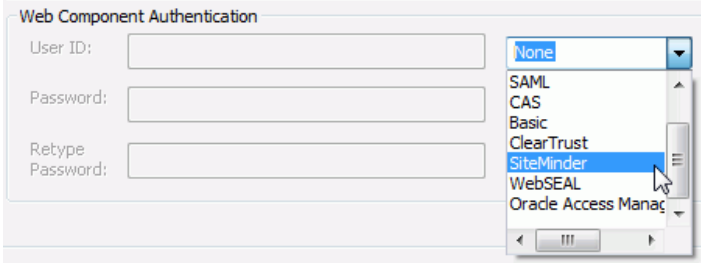
手順　ログインテンプレートを選択するには

1. WebFOCUS App Studio を起動します。
2. [ホーム] タブの [ユーティリティ] グループで、[環境] をクリックします。

   [環境リスト] ダイアログボックスが開きます。
3. 環境を選択し、[プロパティ] をクリックします。

   [WebFOCUS 環境のプロパティ] ダイアログボックスが開きます。

4. 下図のように、[Web コンポーネント認証情報] セクションで、ドロップダウンリストから利用可能なテンプレートを選択します。



5. [ユーザ ID] および [パスワード] テキストボックスに、ユーザ ID とパスワードを入力します。

   App Studio は、このダイアログボックスを開いた際にログインテンプレートファイルの検索を試みます。ファイルが検索されない場合は、[None] と [Basic] のみがリストに表示されます。ファイルが検索された場合、ファイル内のログインテンプレートに基づいて、リストに追加されるコンポーネントが決定されます。

   テンプレートの設定が開発者によって表示および編集可能な場合は、テンプレートの選択時に [設定] ボタンが有効になります。このボタンをクリックすると、[認証情報の設定] ダイアログボックスが開きます。

6. [WebFOCUS 環境のプロパティ] ダイアログボックスで、[WebFOCUS] ボタンをクリックして接続をテストします。

   [WebFOCUS ログイン] ダイアログボックスが表示されます。

7. 手順 5 で指定したユーザ ID とパスワードを入力し、[ログイン] をクリックします。

   ログインに失敗した場合、プロンプトダイアログボックスが開き、[認証情報] テキストボックスにログインテンプレート名が表示された状態で認証情報の入力が要求されます。これは、パスワードの入力を間違えた場合、セキュリティシステムに問題がある場合、またはログインテンプレートの設計が間違っている場合に表示される可能性があります。

   [OK] をクリックして環境を保存すると、このテンプレートに関連した情報が、次のようにローカルマシンの App Studio パーソナライズファイルに書き込まれます。

   ```
   drive:¥Users¥user_id¥AppData¥Roaming¥Information Builders¥wfscom.xml
   ```

   説明
   user_id

   Windows のユーザ ID です。

カスタムテンプレートの作成

テンプレートファイルは、drive:¥ibi¥AppStudio82¥bin ディレクトリ内の「dssso.xml」という名前の xml ファイルです。

このファイルには、すべてのカスタムログインテンプレートが含まれています。

- テンプレートはすべて、<authentications> (開始 XML タグ) と</authentications> (終了 XML タグ) の間に含まれます。
- 各テンプレートは、独自の <authentication> タグおよび </authentication> タグの間に含まれています。これらのタグ内には、各テンプレートの名前と説明も含まれます。この説明は、[WebFOCUS 環境のプロパティ] ダイアログボックスの [Web コンポーネント認証情報] セクションに表示されます。

次に、テンプレートファイルに必要なすべてのタグについて説明します。属性値が指定されていない場合にも、すべての必須タグが必要です。属性値が指定されていない場合は、デフォルト値が使用されます。デフォルト値を変更しない場合でも、すべての属性を指定します。

構文　ログインテンプレートファイルの開始

次のタグは必須です。

```
<?xml version="1.0" encoding="utf-8"?>
<authentications>
```

構文　個別のテンプレート定義の開始

このタグは必須です。

```
<authentication name="form1" desc="Description of Form 1">
```

説明

`form1`

テンプレートの名前です。

`Description of Form 1`

Web コンポーネント認証リストに表示される名前です。この属性値を省略すると、name 属性の値が表示されます。

構文　ログインリソースへのアクセスのための属性指定

次のタグは必須です。

```
<sso_logon_resource desc="Logon Resource" read_only="true"
visible="true">
  <protocol default="%%environment%%" />
  <host default="%%environment%%" />
  <port default="%%environment%%" />
  <path desc="Description of path" default="resource_uri" />
</sso_logon_resource>
```

説明

`sso_logon_resource`

SSO 製品へのユーザのログインに使用されるプログラムの URL です。このプログラムには、JSP、Servlet、有効なサーバページ、CGI があります。

`Logon Resource`

[WebFOCUS 環境のプロパティ] ダイアログボックスの [Web コンポーネント認証情報] リストに表示される説明です。

`read_only="true"`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を変更可能にするには true、値を変更不可にするには false を指定します。デフォルト値は true です。

`visible="true"`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を表示可能にするには true、値を表示不可にするには false を指定します。デフォルト値は true です。

`protocol`

ログインリソースへのアクセスに使用されるプロトコル (http または https) です。

`hostname`

ログインリソースのホスト名です。

`port_number`

ログインリソースのポート番号です。デフォルト属性が指定されない場合は、接続には明示的なポート値は使用されません。この場合、有効なポート番号はプロトコル値によって異なります。プロトコルが http の場合、ポート番号は 80 です。プロトコルが https の場合、ポート番号は 443 です。スラッシュ (/) がデフォルトキーワード値の先頭にない場合は、追加されます。

`%%environment%%`

実行時に、[WebFOCUS コンポーネント環境] ダイアログボックスで指定された値が代入されるテンプレート変数です。

`resource_uri`

ポートの後に記述される URL の一部で、ログインリソースへのパスを指定します。

構文　ログイン結果の指定

次のタグは必須です。

ログインに成功した場合、そのログイン結果が Cookie になります。ログインに失敗した場合、セキュリティシステムから Cookie は返されません。これにより、ログインに失敗したことが App Studio に示されます。この場合、ログインダイアログボックスが表示され、ユーザは ID およびパスワードを再入力することができます。

Cookie が返された場合、ログインが成功したと見なされ、リクエストごとに Cookie が WebFOCUS に転送されます。認証に必要な Cookie を記述するには、次のタグをテンプレートに追加します。

```
<logon_result name="cookie_name" type="cookie"  visible="false" />
```

説明

`cookie_name`

ログインリソースから返される Cookie の名前です。この名前には、大文字と小文字の区別があります。

`type=cookie`

ログインに成功した結果として App Studio ソフトウェアに返される値を指定します。この値を省略すると、デフォルト値の「cookie」が使用されます。

`visible="false"`

[WebFOCUS 環境のプロパティ] ダイアログボックスで値を表示可能にするには true、値を表示不可にするには false を指定します。デフォルト値は false です。

構文　必須ログインパラメータの指定

次のタグは必須です。

```
<user name="user" desc="user Id" default="%%environment%%"
read_only="true" visible="true" />
<password name="password" desc="Password" default="%%environment%%"
read_only="true" visible="true" />
```

説明

`user`

認証されたユーザ ID です。この値は読み取り専用に設定されており、デフォルト値は [WebFOCUS 環境のプロパティ] ウィンドウから読み取られます。

`user Id`

[WebFOCUS 環境のプロパティ] ダイアログボックスの [Web コンポーネント認証情報] リストに表示される名前です。この属性値を省略すると、user name 属性の値が表示されます。

`%%environment%%`

実行時に、[WebFOCUS コンポーネント環境] ダイアログボックスで指定された値が代入されるテンプレート変数です。

`read_only="true"`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を変更可能にするには true、値を変更不可にするには false を指定します。デフォルト値は true です。

`visible="true"`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を表示可能にするには true、値を表示不可にするには false を指定します。デフォルト値は true です。

`password`

認証されたパスワードです。この値は読み取り専用に設定されており、デフォルト値は [WebFOCUS 環境のプロパティ] ウィンドウから読み取られます。この値は、visible プロパティが指定されている場合でも表示されません。

パスワード

[WebFOCUS 環境のプロパティ] ダイアログボックスの [Web コンポーネント認証情報] リストに表示される名前です。この属性値を省略すると、password name 属性の値が表示されます。

構文　オプションのログインパラメータの指定

その他の変数 (ユーザ ID とパスワード以外) が必要かどうかは、ログインの処理方法により異なります。

```
<variable name="var1" default="initial_value" read_only="false"
visible="true"/>
<variable name="var2" read_only="false" visible="true">
  <protocol default="%%environment%%" />
  <host default="%%environment%%" />
  <port default="%%environment%%" />
  <path default="resource_uri"/>
</variable>
```

説明

`var1`

セキュリティシステムで必要なその他の変数名です。

`initial_value`

変数のデフォルト値です。

`read_only="false"`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を変更可能にするには true、値を変更不可にするには false を指定します。デフォルト値は false です。

`visible="true"`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を表示可能にするには true、値を表示不可にするには false を指定します。変数名タグのデフォルト値は true です。プロトコル、ホスト、ポート、パスのタグのデフォルト値は false です。

`protocol`

その他の変数に対する環境情報が SSO 製品で必要な場合に、プロトコルの指定に使用されます。コンテキストについての詳細は、sso_logon_resource タグの説明を参照してください。

`hostname`

その他の変数に対する環境情報が SSO 製品で必要な場合に、ホスト名の指定に使用されます。コンテキストについての詳細は、sso_logon_resource タグの説明を参照してください。

`port_number`

その他の変数に対する環境情報が SSO 製品で必要な場合に、ポート番号の指定に使用されます。コンテキストについての詳細は、sso_logon_resource タグの説明を参照してください。

`%%environment%%`

実行時に、[WebFOCUS コンポーネント環境] ダイアログボックスで指定された値が代入されるテンプレート変数です。

`resource_uri`

その他の変数に対する環境情報が SSO 製品で必要な場合に、リソースの URL の指定に使用されます。コンテキストについての詳細は、sso_logon_resource タグの説明を参照してください。

構文　ユーザ定義 Cookie の追加

デフォルト設定では、ユーザが App Studio ソフトウェアを終了した際、またはユーザがログアウトした際に Cookie 情報が削除されます。ユーザ定義の Cookie を保持するには、テンプレートファイルの Cookie 例外リストを使用して、Cookie の名前を指定する必要があります。このリストは、既存のテンプレートに追加することができますが、この Cookie リストの格納のみの目的で、新しいテンプレートを作成することもできます。指定可能な Cookie の数に、制限はありません。

```
<cookie_exclude_list>
  <variable name="var1" default="cookie_name" visible="true"/>
</cookie_exclude_list>
```

`var1`

Cookie のパラメータです。

`cookie_name`

Cookie の名前です。この値をブランクにする場合や表示の目的でサンプル名を格納する場合、開発者は、[認証情報の設定] ダイアログボックスで、必要な Cookie 名を指定する必要があります。

`visible="true”`

値は true または false です。[WebFOCUS 環境のプロパティ] ダイアログボックスで値を表示可能にするには true、値を表示不可にするには false を指定します。デフォルト値は true です。

構文　個別のテンプレート定義の終了

このタグは必須です。

```
</authentication>
```

構文　テンプレート定義ファイルの終了

このタグは必須です。

```
</authentications>
```

例　サンプルテンプレートファイル

TIBCO App Studio 製品に付属のテンプレートファイルには、複数のサンプルテンプレートが含まれています。次の例は、SiteMinder ログインテンプレートのサンプルです。次の点に注意してください。

- ログインリソースの名前は ibi_sm です。[Web コンポーネント認証] ダイアログボックスに表示される記述は SiteMinder です。
- URL 情報は [Web コンポーネント] ダイアログボックスから読み取られ、URL は / siteminderagent/forms/login.fcc です。
- ログイン結果は、「SMSESSION」という名前の Cookie です。SMAUTHREASON と TARGET の 2 つの変数が必要です。TARGET 変数は、WebFOCUS ホームページの URL 情報を指定します。

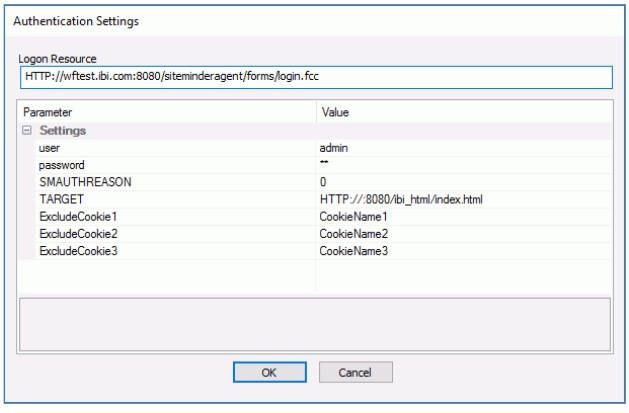
```
<authentication name="ibi_sm" desc="SiteMinder">
  <sso_logon_resource desc="Logon Resource" read_only="false"
visible="false">
    <protocol default="%%environment%%" />
    <host default="%%environment%%" />
    <port default="%%environment%%" />
    <path desc="" default="/siteminderagent/forms/login.fcc" />
  </sso_logon_resource>
  <user name="user" desc="User Id" default="%%environment%%"
     read_only="true" visible="true" />
  <password name="password" desc="Password" default="%%environment%%"
     read_only="true" visible="true" />
  <logon_result name="SMSESSION" type="cookie" />
  <variable name="SMAUTHREASON" default="0" read_only="true"
     visible="true" />
  <variable name="TARGET" read_only="false" visible="true">
   <protocol default="%%environment%%" />
   <host default="%%environment%%" />
   <port default="%%environment%%" />
   <path default="/ibi_html/index.html" />
  </variable>
 </authentication>
```

例　Cookie 除外リストを含むサンプルテンプレート

次の例は、Cookie 除外リストを含む SiteMinder テンプレートを示しています。

```
<authentication name="ibi_sm" desc="SiteMinder">
   <sso_logon_resource desc="Logon Resource" read_only="false" visible="false">
     <protocol default="%%environment%%"/>
     <host default="%%environment%%"/>
     <port default="%%environment%%"/>
     <path desc=""default="/siteminderagent/forms/login.fcc"/>
   </sso_logon_resource>
   <user name="user" desc="User Id" default="%%environment%%"
    read_only="true" visible="true"/>
   <password name="password" desc="Password" default="%%environment%%"
    read_only="true" visible="true"/>
   <logon_result name="SMSESSION" type="cookie"/>
   <variable name="SMAUTHREASON" default="0" read_only="true" visible="true"/>
   <variable name="TARGET" read_only="false" visible="true">
     <protocol default="%%environment%%"/>
     <host default="%%environment%%"/>
     <port default="%%environment%%"/>
     <path default="/ibi_html/index.html"/>
   </variable>
   <cookie_exclude_list>
     <variable name="ExcludeCookie1" visible="true">CookieName1</variable>
     <variable name="ExcludeCookie2" visible="true">CookieName2</variable>
     <variable name="ExcludeCookie3" visible="true">CookieName3</variable>
   </cookie_exclude_list>
</authentication>
```

[WebFOCUS 環境のプロパティ] ダイアログボックスで Web 認証コンポーネントとして [SiteMinder] を選択した場合、[設定] ボタンをクリックすると、下図のような [認証情報の設定] ダイアログボックスが表示されます。



例　Cookie 除外リストを含み、ログインリクエストを含まないサンプルテンプレート

次の例は、「Cookie_save_list」という名前のテンプレートを示しています。sso_logon_resource パラメータを NONE に設定することで、ログインリクエストを無効にしています。

```
<authentication name="ibi_Preserve_Cookies_Template"
      desc="Cookie_save_list">
  <sso_logon_resource desc="Logon Resource" read_only="false"
      visible="false">NONE  </sso_logon_resource>
  <user name="user" desc="User's Name" default="%%environment%%"
      read_only="true" visible="true"/>
  <password name="password" desc="User's Password"
      default="%%environment%%" read_only="true" visible="true" />

<cookie_exclude_list>
   <variable name="ExcludeCookie1" default="CookieName1"
       visible="true"/>
   <variable name="ExcludeCookie2" default="CookieName2"
       visible="true"/>
   <variable name="ExcludeCookie3" default="CookieName3"
       visible="true"/>
   <variable name="ExcludeCookie4" default="CookieName4"
       visible="true"/>
  </cookie_exclude_list>
</authentication>
```

G

TIBCO WebFOCUS 変数の操作

WebFOCUS 変数は、WebFOCUS 処理を制御します。管理コンソールでは、さまざまな WebFOCUS 変数を表示、変更することができます。WebFOCUS には、これらの変数をさらに操作するための次の機能が備わっています。

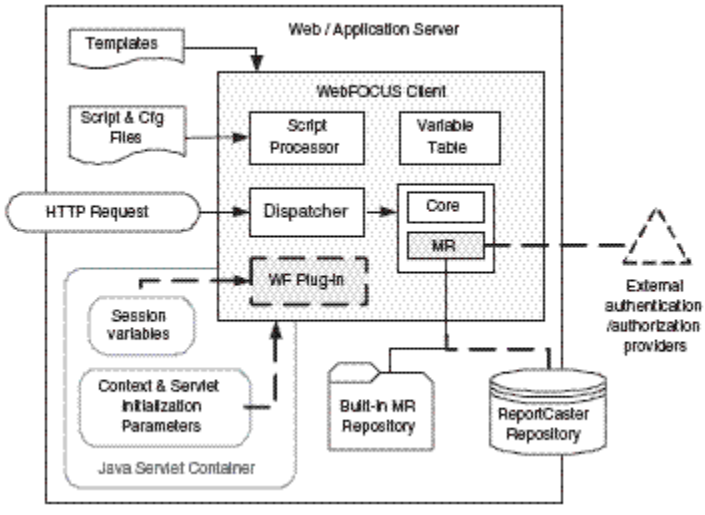
- 条件に基づいて変数の値を設定したり、これらの変数の処理オプションを制御したりするためのスクリプト言語。
- WebFOCUS Client の Servlet 実装用のプラグイン。このプラグインから提供されるメソッドを使用して、WebFOCUS 変数テーブルと HTTP ヘッダ (またはアプリケーションのセッション) 間で変数をコピーすることができます。

トピックス

TIBCO WebFOCUS リクエスト処理のカスタマイズ

WebFOCUS アプリケーションを構成、拡張して、さまざまな他社製品またはカスタムソリューションと連携させることができます。

下図は、WebFOCUS Client 処理でカスタマイズが実装できるポイントを示しています。



WebFOCUS Client には、カスタマイズしたプログラムを使用してデフォルト処理を拡張できるポイントが 2 つ用意されています。

- 個々の HTTP リクエストが WebFOCUS アプリケーションに送信される前に、Java Servlet フィルタを呼び出すことができます。HTTP クライアント (例、Web ブラウザ) からリクエストが Web サーバに送信され、そこから Application Server へ送信されます。Java Servlet フィルタは、Application Server から WebFOCUS アプリケーションへの呼び出しを代行受信することができます。また、WebFOCUS アプリケーションが呼び出しを受信する前に、リクエストの変更、返信、実行の一時停止を行うこともできます。たとえば、Java Servlet フィルタを使用してカスタム認証を実行することができます。
- WebFOCUS プラグインは、リクエストがセルフサービスリクエストであるか BI Portal リクエストであるかに関係なく、リクエストが WebFOCUS Reporting Server に送信される前に呼び出すことができます。また、プラグインコードは、WebFOCUS Reporting Server から WebFOCUS Client へ結果が送信される前に呼び出すことができます。これにより、ブラウザに結果を返信する前に、ブラウザからのリクエストを前処理し、そのレスポンスを後処理することが可能になります。

WebFOCUS プラグインを使用するには、ユーザのサイトで WebFOCUS 変数値の設定やプロパティの編集など、いくつかの構成手順を実行する必要があります。このプラグインを使用すると、WebFOCUS 変数、Application Server セッション変数、HTTP ヘッダ変数などの各種変数を、WebFOCUS 変数テーブル、Application Server セッション、HTTP ヘッダの間でコピーすることが可能になります。このプラグインの使用方法についての詳細は、721 ページの 「 TIBCO WebFOCUS Servlet プラグイン 」 を参照してください。

前処理または後処理メソッドを必要としているが、提供されたプラグインにそのメソッドが実装されていない場合、ユーザが独自のプラグインを開発することができます。既存のプラグインのクラスを拡張すると、同メソッドをそのまま使用することができます。WebFOCUS Client の Servlet 実装用プラグインは、Java 言語で記述する必要があります。

WebFOCUS Reporting Server において、WebFOCUS Client プラグインによく似たカスタムプログラムのことを「イグジット」と呼びます。WebFOCUS Reporting Server には、WebFOCUS で使用可能なイグジットが 2 つ用意されています。

- **事前確認ユーザ ID イグジット (PVUIDXT)** このイグジットは、WebFOCUS Reporting Server 認証のカスタマイズに使用します。このイグジットを使用して、次のことを行えます。
  - WebFOCUS Reporting Server が他社製ディレクトリに対して認証を行うよう構成する。
  - WebFOCUS Reporting Server や HUB Server が認証情報を確認せずに、他の WebFOCUS Reporting Server や WebFOCUS Client からセキュアな接続を確立する。この場合、認証情報は以前のポイントですでに確認されています。
  - 確認済みのユーザ ID を後続のサーバで有効な別のユーザ ID に置換することで、WebFOCUS Reporting Server や HUB Server が他の WebFOCUS Reporting Server とのセキュアな接続を確立する。
- **WebFOCUS DBA イグジット** このイグジットにより、WebFOCUS のメタデータが、データソースセキュリティ用に置換可能なパラメータを使用できるようになります。通常はこのイグジットを使用して、データソース内でユーザがアクセスできる値を制限します。

TIBCO WebFOCUS スクリプトファイルと構成ファイル

WebFOCUS は、リクエストを処理する際にスクリプトファイルと構成ファイルを使用します。WebFOCUS Client は、これらのファイルで設定された変数値を使用してローカル処理とリクエスト処理を行います。

リクエストのタイプごとに、これらのファイルが所定の順序で処理されます。それぞれのファイルは、WebFOCUS 変数テーブルの変数値を変更することができます。

WebFOCUS Client の構成ファイルについての詳細は、525 ページの「 TIBCO WebFOCUS Client 構成ファイル 」 を参照してください。

TIBCO WebFOCUS 変数

WebFOCUS Client の処理動作は、内部変数により制御されます。この内部変数は、複数のソースから読み出されてメモリ常駐テーブルにロードされます。これらのソースには次のものがあります。

- **WebFOCUS スクリプトファイルと構成ファイル** WebFOCUS Client には、スクリプトファイルと構成ファイル (*.wfs、*.prf、*.cfg) が一式用意されています。これらのファイルには、処理方法を定義する情報が含まれています。たとえば、ユーザ ID、ホスト名、ホストポート、ディレクトリパスなどの情報は変数によって識別されます。

  初期化パラメータは構成ファイル (*.cfg) から収集され、各リクエストの環境を定義します。初期化パラメータは、*name=value* の組み合わせで構成されます。

  スクリプトファイル (*wfs、*.prf) は、処理中に使用される WebFOCUS 変数を定義します。WebFOCUS スクリプト言語を使用して、条件に基づいて変数値を変更することができます。

- **テンプレートファイルと HTML ページ** テンプレートファイルは、中核処理および一部の BI Portal 処理のステータスを表示するページ (例、ディファードステータスページ) のページレイアウトを記述したものです。

- **HTTP ヘッダ** HTTP 変数は、HTTP リクエストヘッダおよびレスポンスヘッダに組み込まれて Web サーバと Web ブラウザ間で送受信されます。HTTP 変数は通常、Web ブラウザの環境を定義します。たとえば、「HTTP_USER_AGENT」という変数は、ブラウザの開発会社とバージョンを定義します。WebFOCUS Client では、Web サーバおよび Web ブラウザで作成され、値が挿入される任意の標準 HTTP 変数を使用することができます。

TIBCO WebFOCUS 変数テーブル

変数は、メモリ常駐の WebFOCUS 変数テーブルに格納されます。これにより、これらの変数をローカル処理に使用したり、WebFOCUS の各種コンポーネント間の通信に使用したりすることが可能になります。

管理コンソールを使用して、ほとんどの WebFOCUS 変数の値を変更することができます。管理コンソールについての詳細は、63 ページの 「 WebFOCUS Client の構成 」 を参照してください。

TIBCO WebFOCUS スクリプトコマンド

WebFOCUS スクリプト (WFS) コマンドを WebFOCUS Client 設定および HTTP ヘッダ変数 (731 ページの 「 スクリプト処理で使用可能な HTTP ヘッダ変数 」 を参照) とともに使用して、WebFOCUS Client の処理および制御をさらにカスタマイズすることができます。

WFS コマンドを使用して次のことを行えます。

- WebFOCUS Client 変数の定義、確認、制御
- WebFOCUS プラグインの呼び出し
- WebFOCUS Reporting Server への情報の送信 (例、プロシジャの名前や説明)

ヒント：WebFOCUS スクリプトコマンドには、次の変数を使用することも可能です。

- **フォーム変数** HTML ページから設定します。変数名が「IBI」または「WF」で始まる場合を除いて、フォーム変数は WebFOCUS Reporting Server に自動的に送信されます。
- **出力変数** WebFOCUS Reporting Server により設定され、WebFOCUS Client に返されます。

参照 WFS コマンド構文

次の WFS コマンドを site.wfs ファイルに追加することができます。このファイルは、*drive*:¥ibi¥WebFOCUS82¥client¥wfc¥etc ディレクトリに格納されています。

コマンドの構文	説明
`<EXIT>`	WebFOCUS Client の処理を停止し、即時終了します。
`<INCLUDE> filename`	外部ファイルから WFS ロジックを標準の WFS 処理に組み込みます。処理を続けるためには、このファイルが存在する必要があります。詳細は、721 ページの 「 WFS 処理での外部ファイルの組み込み 」 を参照してください。
`<CONDITIONAL_INCLUDE> filename`	<INCLUDE> *filename* と同様に動作します。ただし、このファイルが存在する必要はありません。詳細は、721 ページの 「 WFS 処理での外部ファイルの組み込み 」 を参照してください。

コマンドの構文	説明
`<SET> variable (option)`	サーバプロシジャで使用するために、変数を WebFOCUS Reporting Server へ送信します。これは、Reporting Server に自動的に送信されない変数に使用します。詳細は、729 ページの 「TIBCO WebFOCUS Reporting Server への変数の送信」を参照してください。
`<CALL> function(parm1,...)`	WebFOCUS プラグインを呼び出します。各 WebFOCUS プラグインは、最大 10 個の入力パラメータを保有することができます。詳細は、722 ページの 「TIBCO WebFOCUS Servlet プラグインの起動」 を参照してください。

`<IF> variable operator value`
`<ELSE>`
`<ENDIF>`
	WebFOCUS Client 変数を条件付きで確認します。詳細は、727 ページの 「変数の条件付き確認」 を参照してください。

`<IFDEF> variable`
`<ELSE>`
`<ENDIF>`
	WebFOCUS Client 変数が存在することを確認します。詳細は、728 ページの 「変数が存在することの確認」 を参照してください。

`<IFNDEF> variable`
`<ELSE>`
`<ENDIF>`
	WebFOCUS Client 変数が存在しないことを確認します。詳細は、728 ページの 「変数が存在しないことの確認」 を参照してください。

`<SENDVAR> name={constant|&value}` `<ENDSENDVAR>`	サーバプロシジャで使用するために、変数を WebFOCUS Reporting Server へ送信します。これは、Reporting Server に自動的に送信されない変数に使用します。詳細は、729 ページの 「TIBCO WebFOCUS Reporting Server への変数の送信」を参照してください。 **注意:** この構文は廃止される予定です。<SENDVAR> を使用する代わりに、<SET> *variable_name* (pass) を使用することをお勧めします。

参照

WFS 言語の構文

WFS コマンドのコーディングには、次の構文を使用することができます。

コマンドの構文	説明
<! > #	コメント文字です。現在の行がコメント行であることを WebFOCUS Client に通知します。行の先頭文字には、不等号 (<) と感嘆符 (!) の組み合わせ (<!) を使用するか、シャープ記号 (#) を使用する必要があります。以下はその例です。 <! This is a comment.> # This is also a comment.
¥¥=	連続文字です。任意の行の末尾に追加することができます。現在の行が次の行に続くことを WebFOCUS Client に通知します。
¥n	改行文字です。複数のコマンドを単一行に入力することができます。

コマンドの構文	説明

`value = {constant|&variable}`	WFS ファイル内の変数に値 (定数または変数) を入力します。
	`constant`
	リテラル値です。二重引用符 (") で囲まれた部分は、変数の一部として転送されます。
	注意：この定数値にアンパサンド (&) や円記号 (¥) などの特殊文字が含まれている場合は、円記号 (¥) をエスケープ文字として使用することで、その特殊文字を値の一部として確実に転送することができます。
	`&variable`
	値のプレースホルダです。
	変数に値が割り当てられると、変数名の先頭にアンパサンド (&) を追加して、その値の代わりに変数を使用することができます。この方法で、複数のリテラル値を連結することができます。以下はその例です。
	`long_string = this is a`
	`long_string = &long_string very long string`
	`long_string = &long_string that requires multiple lines`

参照

円記号エスケープ文字

円記号 (¥) をエスケープ文字として使用すると、次のことが可能になります。

- 文字列内の値の一部として一重引用符 (') などの区切り文字を含めることができます。区切り文字の前に円記号 (¥) を配置すると、その文字は文字列の終わりを示す区切り文字ではなく、データとして認識されます。
- 文字列内の値の一部として円記号 (¥) を含めることができます。その円記号 (¥) の前に 2 つ目の円記号 (¥) をエスケープ文字として追加することができます。

円記号 (¥) をエスケープ文字として使用する場合、その文字は文字列の長さとしてカウントされません。5 つの文字と 1 つのエスケープ文字で構成される文字列は、5 バイトの変数に正しく格納されます。

構文　WFS 処理での外部ファイルの組み込み

標準の WFS 処理に外部ファイルを組み込むことができます。次の <INCLUDE> コマンドを使用して、標準の WFS ファイルから別の WFS ファイルを呼び出すことができます。処理を続行するには、このカスタムファイルが存在する必要があります。<CONDITIONAL_INCLUDE> filename コマンドは、<INCLUDE> filename コマンドと同様に動作しますが、指定したファイルが存在している必要はありません。

```
<INCLUDE> filename
```

```
<CONDITIONAL_INCLUDE> filename
```

説明

`filename`

WFS 処理に追加されるファイルのファイル名です。

例　標準 WFS 処理への外部ファイルの組み込み

次のコマンドは、&CGI_BASE_DIR 変数で指定された、client/wfc/etc ディレクトリ内の custom.wfs ファイルを組み込みます。処理を継続するには、このファイルが存在している必要があります。

```
_exit=custom.wfs
```

```
-<INCLUDE> &CGI_BASE_DIR&_exit
```

次の条件付き <INCLUDE> コマンドは、&CGI_BASE_DIR 変数で指定された、client/wfc/etc ディレクトリに custom.wfs ファイルが存在することを確認します。

```
_exit=custom.wfs
```

```
-<CONDITIONAL_INCLUDE> &CGI_BASE_DIR&_exit
```

TIBCO WebFOCUS Servlet プラグイン

TIBCO WebFOCUS Servlet のプラグインには、WebFOCUS 変数を操作するためのメソッドが用意されています。これらの各メソッドに転送されるパラメータにはリテラル値は使用できないため、最初に変数に値を入力する必要があります。これらの変数はメソッドの呼び出しに使用されます。

WebFOCUS 変数テーブルに配置される HTTP ヘッダ変数のリストについての詳細は、731 ページの 「 スクリプト処理で使用可能な HTTP ヘッダ変数 」 を参照してください。

手順　TIBCO WebFOCUS Servlet プラグインを有効にするには

TIBCO WebFOCUS Servlet プラグインを有効にするには、webfocus.cfg ファイル内の WFEXT 変数を「ibi.webfoc.WFEXTDefault」というクラス名に設定します。

1. 管理コンソールの [構成] タブで、[アプリケーションの設定] フォルダ下の [Client 設定] をクリックします。
2. [プラグインクラス] (IBI_WFEXT) の値としてクラス名の「ibi.webfoc.WFEXTDefault」が表示されていない場合は、「ibi.webfoc.WFEXTDefault」と入力し、[保存] をクリックします。

注意：一度にアクティブにすることができるプラグインは 1 つだけです。別の機能を追加する必要がある場合は、このクラスを拡張することで新しい機能を追加します。これにより、このクラスで提供されるメソッドへのアクセスを失うことはありません。

構文　TIBCO WebFOCUS Servlet プラグインの起動

次の <CALL> コマンドを使用して、WebFOCUS プラグインを呼び出します。

```
<CALL> routine(parm1,parm2)
<IF> RETCODE NE "returncodevalue"
# insert your code here
<ENDIF>
```

説明

`<CALL>`

WebFOCUS Servlet プラグインを呼び出すコマンドです。

`routine`

呼び出される関数の名前を定義します (例、security、CopyHTTPCookieToWFVar)。

`(parm1,parm2)`

WebFOCUS プラグインの入力パラメータです。各 WebFOCUS プラグインは、最大 10 個の入力パラメータを保有することができます。出力バッファは転送されますが、入力パラメータの最大数にはカウントされません。

`RETCODE`

メソッド呼び出しのステータスです。

`returncodevalue`

プラグインからの戻り値 (例、0) と比較する値です。

CopyHTTPHeaderToWFVar メソッド

CopyHTTPHeaderToWFVar メソッドは、HTTP ヘッダ変数の値を WebFOCUS Servlet 変数にコピーします。

例　CopyHTTPHeaderToWFVar メソッドの使用

1. 管理コンソールの [構成] タブで [カスタム設定] をクリックし、次のコードを [カスタム設定] ウィンドウに入力します。

```
HTTP_HEADER_NAME = hostWFS_VAR_NAME = WFV
<CALL> CopyHTTPHeaderToWFVar (HTTP_HEADER_NAME,WFS_VAR_NAME)
<SET> WFV (pass)
```

   説明

   `HTTP_HEADER_NAME`

   値を抽出する HTTP ヘッダエントリの名前です。

   `host`

   抽出する値です。

   `WFS_VAR_NAME`

   値を受け取る WebFOCUS Servlet 変数名です。

   `WFV`

   WebFOCUS Servlet 変数に割り当てる値です。

   リターンコードの 0 (ゼロ) は成功、999 は失敗を示します。

2. BI Portal から次のプロシジャを実行します。

```
-TYPE &WFV
```

HTTP ヘッダ内の HTTP_HOST (Web サーバ名) が、WebFOCUS Servlet 変数にコピーされます。

CopyWFVarToSessionVar メソッド

CopyWFVarToSessionVar メソッドは、WebFOCUS Servlet 変数値を Web アプリケーションセッション変数にコピーします。

例　CopyWFVarToSessionVar メソッドの使用

1. *drive:*¥ibi¥WebFOCUS82¥webapps¥webfocus フォルダに移動します。テキストエディタを開き、次のコードをコピーして貼り付けます。

```
<HTML>
<BODY>
Session variable value is <%= session.getAttribute("sampleVariable")%>
</BODY>
</HTML>
```

   注意：この sample.jsp ファイルは、session.getAttribute メソッドを使用して Web アプリケーションセッション変数の値を取得します。

2. このファイルを sample.jsp として保存し、テキストエディタを閉じます。
3. 管理者としてログインします。
4. 管理コンソールの [構成] タブで [カスタム設定] をクリックし、次のコードを入力します。

```
<IFDEF> IBIMR_user
SESSION_VAR_NAME = sampleVariable
WFS_VAR_NAME = &IBIMR_user
<CALL> CopyWFVarToSessionVar (WFS_VAR_NAME, SESSION_VAR_NAME)
<ENDIF>
```

   説明

   `WFS_VAR_NAME`

   WebFOCUS Servlet 変数名です。この変数値は、Web アプリケーションセッション変数に値がコピーされる、実際の WebFOCUS 変数名です。

   `SESSION_VAR_NAME`

   Web アプリケーションセッション変数名です。

   この関数は常に 0 (ゼロ) を返します。

5. [保存] をクリックします。
6. ファイルが保存されたことを示すメッセージで [OK] をクリックします。
7. BI Portal にログインします。
8. 同じブラウザウィンドウのアドレスバーに、http://*hostname*:*port*/ibi_apps/sample.jsp と入力し、Enter キーを押します。

sample.jsp ファイルを実行すると、セッション変数に、ログインページで入力したユーザ ID が表示されます。

CopySessionVarToWFVar メソッド

CopySessionVarToWFVar メソッドは、Web アプリケーションセッション変数値を WebFOCUS Servlet 変数にコピーします。

例　CopySession VarToWFVar メソッドの使用

1. *drive:*¥ibi¥WebFOCUS82¥webapps¥webfocus フォルダに移動します。テキストエディタを開き、次のコードをコピーして貼り付けます。

   ```
   <%@ page language="java" contentType="text/html"%>
   <%  session.setAttribute("sampleVariable","sampleValue"); %>
   ```

   注意：この sample.jsp ファイルは、session.setAttribute メソッドを使用して Web アプリケーションセッション変数を初期化します。

2. このファイルを sample.jsp として保存し、テキストエディタを閉じます。
3. 管理者としてログインします。
4. 管理コンソールの [構成] タブで [カスタム設定] をクリックし、次のコードを入力します。

   ```
   SESSION_VAR_NAME = sampleVariable
   WFS_VAR_NAME = WFV
   <CALL> CopySessionVarToWFVar (SESSION_VAR_NAME,WFS_VAR_NAME)
   <SET> WFV (pass)
   ```

   説明

   `SESSION_VAR_NAME`

   Web アプリケーションセッション変数名です。

   `WFS_VAR_NAME`

   値を受け取る WebFOCUS Servlet 変数名です。

   リターンコードの 0 (ゼロ) は成功、999 は失敗を示します。

5. BI Portal から次のプロシジャを実行します。

   ```
   -TYPE &WFV
   ```

   Application Server セッション変数および関連付けられた値が WebFOCUS Servlet 変数にコピーされた上で表示されます。

CopyHTTPMethodToWFVar メソッド

CopyHTTPMethodToWFVar メソッドは、HTTP リクエストタイプを表す値を WebFOCUS Servlet 変数にコピーします。通常、リクエストタイプは GET または POST です。

例　CopyHTTPMethodToWFVar メソッドの使用

1. 管理者としてログインします。
2. 管理コンソールの [構成] タブで [カスタム設定] をクリックし、次のコードを入力します。

```
WFS_VAR_NAME = WFV
<CALL> CopyHTTPMethodToWFVar (WFS_VAR_NAME)
<SET> WFV (pass)
```

説明

`WFS_VAR_NAME`

値を受け取る WebFOCUS Servlet 変数名です。

リターンコードの 0 (ゼロ) は成功、999 は失敗を示します。

3. BI Portal から次のプロシジャを実行します。

```
-TYPE &WFV
```

WebFOCUS Servlet の呼び出し方法に応じて、GET または POST 演算子が表示されます。

CopyHTTPCookieToWFVar メソッド

CopyHTTPCookieToWFVar メソッドは、HTTP Cookie の内容を WebFOCUS Servlet 変数にコピーします。

例　CopyHTTPCookieToWFVar メソッドの使用

1. 管理者としてログインします。
2. 管理コンソールの [構成] タブで [カスタム設定] をクリックし、次のコードを入力します。

```
COOKIE_NAME = WF_SESSIONID
WFS_VAR_NAME = WFV
<CALL> CopyHTTPCookieToWFVar (COOKIE_NAME,WFS_VAR_NAME)
<SET> WFV (pass)
```

説明

`COOKIE_NAME`

値を抽出する HTTP Cookie の名前です。

`WFS_VAR_NAME`

値を受け取る WebFOCUS Servlet 変数名です。

リターンコードの 0 (ゼロ) は成功、999 は失敗を示します。

3. BI Portal から次のプロシジャを実行します。

```
-TYPE &WFV
```

HTTP Cookie の内容が表示されます。この場合、HTTP Cookie は WF_SESSIONID Cookie です。

構文　変数の条件付き確認

次の <IF> ステートメントは、条件付きで WebFOCUS Client 変数を確認します。

```
<IF> variable operator value
<ELSE>
<ENDIF>
```

説明

`variable`

任意の WebFOCUS Client 変数です。

`operator`

EQ、NE、CONTAINS、OR、AND のいずれかに設定可能です。

`value`

任意の WebFOCUS Client 変数または定数に適用されます。

例　変数の大文字での条件付き確認

次の <IF> ステートメントを使用することにより、ログインページが呼び出されたことを確認することができます。

WFS 変数に upper を追加すると、その変数値がすべて大文字と見なされた上で値が確認されます。これにより、大文字と小文字を区別することなく、ユーザが入力した値の確認が可能になります。

次のように <IF> ステートメントを記述すると、入力された値すべてが大文字として扱われます。

```
<IF> ABC.upper EQ "Y" OR ABC.upper EQ "YES"
DEF = &GHI
<ENDIF>
```

次のように <IF> ステートメントを記述すると、入力されたサーバ値の大文字と小文字が区別されなくなります。

```
<IF> IBIC_server.upper EQ "EDASERV"
# INSERT YOUR CODE HERE....
<ENDIF>
```

次の <IF> ステートメントは、WebFOCUS Client 変数の HTTP_HOST 内に「.ibi.com」という定数が含まれているかどうかを確認します。

```
<IF> HTTP_HOST contains ".ibi.com"
# INSERT YOUR CODE HERE....
<ENDIF>
```

構文　変数が存在することの確認

<IFDEF> ステートメントは、WebFOCUS Client 変数が存在することを確認します。

```
<IFDEF> variable
<ELSE>
<ENDIF>
```

説明

`variable`

任意の WebFOCUS Client 変数です。

例　変数の確認と定義

次の例では、*_ON_NT* 変数が存在する場合、PATH_SEP はセミコロン (;) に設定されます。*_ON_NT* 変数が存在しない場合、PATH_SEP はコロン (:) に設定されます。

```
<IFDEF> _ON_NT
PATH_SEP=;
<ELSE> PATH_SEP=:
<ENDIF>
```

構文　変数が存在しないことの確認

次の <IFNDEF> ステートメントは、WebFOCUS Client 変数が存在しないことを確認します。

```
<IFNDEF> variable
<ELSE>
<ENDIF>
```

説明

`variable`

任意の WebFOCUS Client 変数です。

構文　TIBCO WebFOCUS Reporting Server への変数の送信

次の <SET> コマンドは、サーバプロシジャで使用するために、変数を WebFOCUS Reporting Server へ送信します。カスタム変数には、WebFOCUS Reporting Server に自動的に送信されるものがあります。この構文は、WebFOCUS Reporting Server に自動的に送信されない変数に使用します。

```
<SET> name = {constant|&variable} (pass)
```

説明

`name`

WebFOCUS Reporting Server で使用されるダイアログマネージャ変数です。

`constant`

リテラル値です。二重引用符 (") で囲まれた部分は、変数の一部として転送されます。任意の WebFOCUS Client 変数に適用されます。

`&variable`

値のプレースホルダです。 任意の WebFOCUS Client 変数に適用されます。

Managed Reporting 内部変数

Managed Reporting 処理に関連する一部の変数を Reporting Server に転送することができます。この方法は、プロセスフローの制御やレポート出力の表示に利用できます。この変数を使用するには、管理コンソールで <SET> *variablename* (pass) コマンドを構成します。変数には、次のものがあります。

- **IBIMR_folder**　処理済みのレポートを格納するフォルダです。
- **IBIMR_fullpath**　ファイル名と拡張子を含めた、プロシジャのフルパスです。
- **IBIMR_user**　レポートリクエストを処理するユーザ ID です。
- **IBIMR_domain**　処理中のレポートを格納するドメイン HREF です。
- **MR_FULL_FEXNAME**　開発者が指定するレポートの説明です。この説明は、ユーザに表示されます。レポートがテキストエディタまたは InfoAssist から実行された場、この変数に値は挿入されません。

- **MR_ITEM_HANDLE** レポートを作成した際に、そのレポートに割り当てられるファイル名です (「IBFS 名」とも呼ばれる)。レポートが App Studio のテキストエディタまたはレポートキャンバスから実行された場合、この変数は ADHOCRQ に設定されます。

例 Managed Reporting 内部変数の使用

1. 管理者としてログインします。
2. 管理コンソールの [構成] タブで [カスタム設定] をクリックし、次のコードをファイルの末尾に入力します。

```
<SET> IBIMR_folder (pass)
<SET> IBIMR_fullpath (pass)
<SET> IBIMR_user (pass)
<SET> IBIMR_domain (pass)
<SET> MR_FULL_FEXNAME (pass)
<SET> MR_ITEM_HANDLE (pass)
```

   注意：[カスタム設定] ウィンドウの既存の行を上書きしないでください。ファイルの先頭は <VER> 行で始める必要があります。

3. [保存] をクリックします。
4. BI Portal にログインし、テキストエディタを使用してデフォルトワークスペース内に「test2」という標準レポートを作成します。
5. 次のコードを追加し、レポートを保存します。

```
-TYPE IBIMR_folder is &IBIMR_folder
-TYPE IBIMR_fullpath is &IBIMR_fullpath
-TYPE IBIMR_user is &IBIMR_user
-TYPE IBIMR_domain is &IBIMR_domain
-TYPE MR_FULL_FEXNAME is &MR_FULL_FEXNAME
-TYPE MR_ITEM_HANDLE is &MR_ITEM_HANDLE
```

6. 保存したレポートを右クリックしてコンテキストメニューから [プロパティ] を選択し、[パラメータのプロンプト] のチェックをオフにします。
7. [概要] を「Test 2 Description」に変更します。
8. 変更を保存し、レポートを実行します。

次の出力が表示されます。

```
IBIMR_folder is Sales
IBIMR_fullpath is IBFS:/WFC/Repository/Retail/Sales/variables.fex
IBIMR_user is admin
IBIMR_domain is Retail/
MR_FULL_FEXNAME is variablesTitle
MR_ITEM_HANDLE is variables
```

このレポートをテキストエディタから実行すると、次の出力が表示されます。

```
IBIMR_folder is Sales
IBIMR_fullpath is IBFS:/WFC/Repository/Retail/Sales/*
IBIMR_user is admin
IBIMR_domain is Retail/
MR_FULL_FEXNAME is
MR_ITEM_HANDLE is ADHOCRQ
```

スクリプト処理で使用可能な HTTP ヘッダ変数

標準の HTTP ヘッダ変数を使用して、WebFOCUS Client の処理および制御をカスタマイズすることができます。WebFOCUS Servlet がこれらの変数を WebFOCUS 変数テーブルに配置した後、これらの変数を site.wfs ファイルで使用することができます。

HTTP ヘッダ変数	説明
AUTH_TYPE	認可ヘッダが指定された場合に、認証スキーマを指定します。
CONTENT_LENGTH	送信データのバイト数を格納します。POST リクエストにのみ適用されます。
CONTENT_TYPE	添付データの MIME タイプを指定します。
DOCUMENT_ROOT	ホストディレクトリのパスを指定します。
HTTP_ACCEPT	WebFOCUS Client に受け入れが優先されるメディア (MIME) タイプをカンマ区切りで指定します。
HTTP_ACCEPT_ENCODING	レスポンス内で受け入れ可能なコンテキストコーディングを制限します。
HTTP_ACCEPT_LANGUAGE	ユーザ定義の言語を表示します。
HTTP_USER_AGENT	リクエストしているブラウザ (またはクライアント) を識別します。他のブラウザにコンテンツを返信する場合にも使用します。
HTTP_REFERER	参照している Web ページの URL を指定します。

HTTP ヘッダ変数	説明
PATH_INFO	URL に添付されたパス情報を、サーバアドレスとクエリ文字列の間に配置します。
PATH_TRANSLATED	PATH_INFO 値です。ディレクトリに展開する任意の仮想パス名を使用することができます。
QUERY_STRING	URL 内で、疑問符 (?) に続く情報です。
REMOTE_ADDR	リクエストしたクライアントの IP アドレスです。
REMOTE_HOST	リクエストしたクライアントの完全修飾ドメイン名です。
REQUEST_METHOD	HTTP リクエストメソッドです。
SCRIPT_NAME	実行中のスクリプトプログラムの名前です。
SERVER_NAME	サーバのホスト名または IP アドレスです。
SERVER_PORT	リクエストを受信した TCP/IP ポートです。
SERVER_PROTOCOL	リクエストに関連した情報検索プロトコルの名前とバージョンです。
SERVER_SOFTWARE	Web サーバの名前とバージョンです。
URL_PROTOCOL	デフォルトの URL プロトコル (HTTP または HTTPS) です。

ヒント：HTTP ヘッダ変数にスクリプト (WFS) コマンド (717 ページの「 TIBCO WebFOCUS スクリプトコマンド 」 を参照) を使用することで、WebFOCUS Client の処理と制御をカスタマイズすることができます。

H PCI セキュリティ基準に準拠する TIBCO WebFOCUS バージョン 8 実装

ここでは、PCI (Payment Card Industry) データセキュリティ基準に準拠する WebFOCUS バージョン 8 の推奨事項、情報、構成方法について説明します。PCI データセキュリティ基準の概要は、次の Web サイトの PCI DSS v 3.0 文書に記載されています。

https://www.pcisecuritystandards.org

以下の情報を使用して、PCI 準拠に必要な手順を実行することができます。

トピックス

PCI セキュリティ基準の概要

PCI DSS (Payment Card Industry Data Security Standard) は、カード会員データのセキュリティを促進、強化し、世界的に統一されたデータセキュリティ手法を広く導入していく目的で策定されました。PCI DSS には、カード会員データを保護するための技術的および運用上の要件の指針が規定されています。PCI DSS は、カード支払処理に関連する事業体すべてに適用されます。これらの事業体には、加盟店、決済代行会社、加盟店契約会社、カード発行会社、サービスプロバイダのほか、カード会員データを格納、処理、送信するその他の事業体すべてが含まれます。PCI DSS は、カード会員データを保護するための最低限の要件で構成されているため、リスクをさらに軽減するための追加の調整や対策が必要になる場合もあります。PCI DSS 準拠の 12 要件とそれに付随する要件項目は、テクノロジやセキュリティに関係するすべてのシステムコンポーネントに適用され、特にカード会員データの保護に重点が置かれています。

WebFOCUS は、情報セキュリティ会社による独立したアセスメントと、QSA (Qualified Security Assessor) による広範な審査プロセスに基づいて、ビジネスインテリジェンス機能に適用される PCI DSS 構成ベストプラクティスに関して審査されました。

安全なネットワークとシステムの構築と維持

要件 1 - カード会員データを保護するために、ファイアウォールをインストールして構成を維持する

要件 1 に関する推奨事項および情報

- WebFOCUS Client および WebFOCUS Reporting Server を、インターネット DMZ (Demilitarized Zone) から隔離された内部 (トラステッド) ネットワーク領域にインストールします。
- 特定の WebFOCUS 機能には、TCP/IP リスナポートが必要です。WebFOCUS は、TCP/IP 経由で WebFOCUS サーバ以外のサーバとも通信し、その場合にこれらのポートが必要になります。

WebFOCUS TCP/IP リスナポート

デフォルト TCP/IP ポート	用途	備考
WebFOCUS Reporting Server リスナポート		
8120	TCP/IP リスナ	WebFOCUS Client および ReportCaster Distribution Server からのアクセスのみに限定する必要があります。
8121	HTTP または HTTPS リスナ	内部 (トラステッド) ネットワークからのアクセスのみに限定する必要があります。
8122	FOCUS リスナ	複数ユーザ FOCUS データソースにアクセスしない場合は、無効にすることができます。

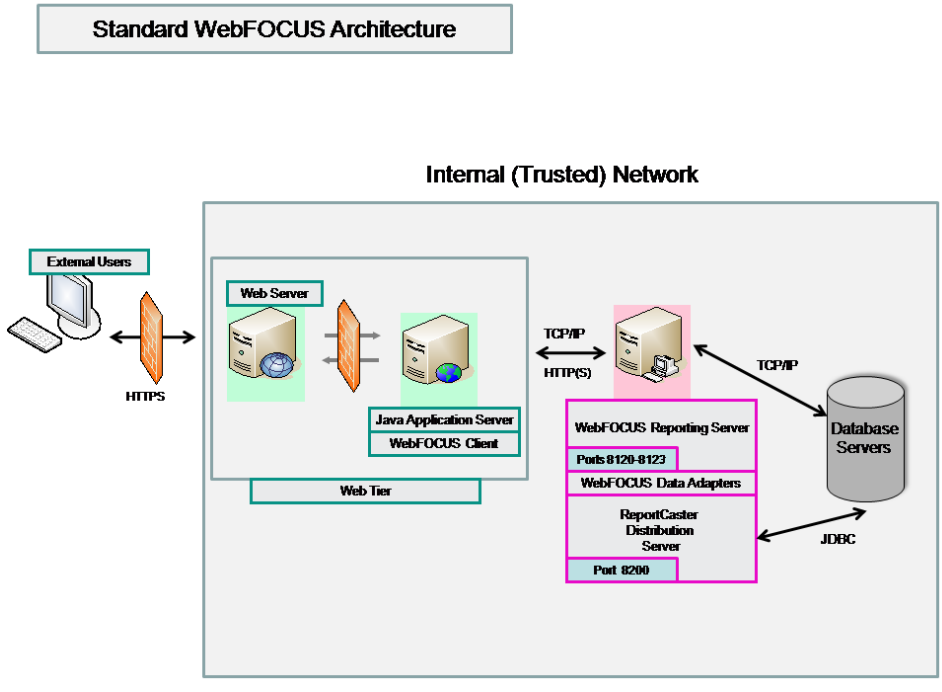
デフォルト TCP/IP ポート	用途	備考
8123	Java サービス (JSCOM3) リスナ	追加の JSCOM3 リスナには、値が 1 ずつ増加するポート番号が必要です (8124 - nnnn)。
WebFOCUS Client		
1527	リレーショナルデータベース	デフォルト設定では Apache Derby を使用しますが、他のリレーショナルデータベースを使用することもできます。
ReportCaster TCP/IP ポート		
8200	メインリスナ	WebFOCUS Client からアクセスできる必要があります。

WebFOCUS TCP/IP および HTTP ポート以外に必要なアクセス

デフォルト TCP/IP ポート	用途	備考
TCP/IP ポートへの WebFOCUS Reporting Server アクセス		
サイト依存	データアダプタ	データベースサーバへのネイティブ接続および JDBC 接続に使用します。
サイト依存	Web Services 対応アダプタ	HTTP ポートへのアクセスに必要な場合があります。
サイト依存	WebFOCUS グラフ、XLSX、および Maginfy と Solr でのリクエストのインデックス化	HTTP ポートへのアクセスに必要です。SSL を使用する場合、またはシングルサインオンのすべてのタイプで、JSCOM3 を使用する必要があります。

デフォルト TCP/IP ポート	用途	備考
389	LDAP サーバ	LDAP 通信に使用します。
636	LDAP サーバ	TLS/SSL 経由での LDAP 通信に使用します。
TCP/IP ポートへの ReportCaster アクセス		
25	メールサーバ	SMTP 接続に使用します。
サイト依存	データベースサーバへの JDBC アクセス	リポジトリへのアクセスに使用します。
389	LDAP サーバ	LDAP 通信に使用します。
636	LDAP サーバ	TLS/SSL 経由での LDAP 通信に使用します。

下図は、標準の WebFOCUS アーキテクチャモデルおよび TCP/IP リスナポートの使用形態を示しています。



要件 2 - システムパスワードおよび他のセキュリティパラメータにベンダー提供のデフォルト値を使用しない

要件項目 2.1 に関する推奨事項および情報

- ❑ WebFOCUS BI Portal 管理者のデフォルト認証情報を変更します。

  注意：通常、実稼動環境では、構成設定は変更されないため、管理コンソールへのアクセスは無効になっています。

- ❑ WebFOCUS メディアから Apache Tomcat をインストールした場合は、Tomcat 管理者の認証情報を変更します。

要件項目 2.2.1 に関する推奨事項および情報

- WebFOCUS を少なくとも 3 階層のアーキテクチャでインストールします。このアーキテクチャでは、WebFOCUS Client が 1 台目のマシンにインストールされ、ReportCaster Distribution Server および WebFOCUS Reporting Server が 2 台目のマシンにインストールされ、データベースサーバがさらに別のマシンにインストールされます。
- 要件 1 の情報に基づいて、ファイアウォールルールを構築することができます。WebFOCUS Reporting Server 構成パラメータの RESTRICT_TO_IP を使用して、TCP/IP リスナおよび HTTP リスナへのアクセスを制限することもできます。

要件項目 2.2.2 および 2.2.3 に関する推奨事項および情報

- SSL プロトコルを使用して WebFOCUS Client および WebFOCUS Reporting Server を構成し、セキュアな HTTPS 通信を提供します。詳細は、このマニュアルの関連するトピック、および『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。

要件項目 2.2.4 に関する推奨事項および情報

WebFOCUS が必要としない追加のソフトウェアや機能はインストールしないでください。

- WebFOCUS Client の最低要件は次のとおりです。
  - Java Application Server および Java 仮想マシン
  - リレーショナルデータベース管理システム
- WebFOCUS Reporting Server の要件は次のとおりです。
  - データベースアクセスに必要なデータベースアダプタ
  - Java 仮想マシン
- ReportCaster の要件は次のとおりです。
  - Java 仮想マシン

要件項目 2.3 に関する推奨事項および情報

- HTTPS でアクセスするよう WebFOCUS Reporting Server ブラウザインターフェースを構成します。詳細は、『TIBCO WebFOCUS サーバ管理者ガイド』を参照してください。
- WebFOCUS Client への通信に SSL を使用して Web サーバや Application Server インフラストラクチャにアクセスします。

カード会員データの保護

要件 3 - 保存されたカード会員データを保護する

要件項目 3.3 に関する推奨事項および情報

- WebFOCUS 開発者は、TIBCO FOCUS 言語で記述されたレポートで機密データが正しくマスクされるようレポートを作成する必要があります。
- マスターファイル属性の ACCESS=INTERNAL を追加して、機密データを含むフィールドを非表示にする必要があります。

要件項目 3.4 に関する推奨事項および情報

- 機密データが含まれた WebFOCUS 抽出ファイルの作成を制限します。
- トレースは、トラブルシューティングや機能診断情報の収集を目的とする場合にのみ有効にします。可能な場合は、WebFOCUS の実稼動環境以外で有効にします。トレースファイルの使用後は、即座に廃棄する必要があります。
- Excel や PDF 出力などのレポート出力タイプでは、WebFOCUS リダイレクトを無効にします。

要件 4 - オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する

要件 4 に関する推奨事項および情報

- 公共ネットワーク経由でコンテンツを FTP 配信する場合、SFTP を使用するよう ReportCaster を構成する必要があります。
- RSA PKI によりネゴシエートされる共通鍵を使用することで、WebFOCUS Reporting Server との通信に AES128 または AES256 暗号化を使用します。WebFOCUS Reporting Server への暗号化通信の構成および実装についての詳細は、494 ページの 「 TIBCO WebFOCUS の暗号化機能 」 を参照してください。

脆弱性管理プログラムの整備

要件 5 - すべてのシステムをマルウェアから保護し、ウィルス対策ソフトウェアまたはプログラムを定期的に更新する

要件 5 に関する推奨事項および情報

WebFOCUS に適用される要件はありません。

要件 6 - 安全性の高いシステムとアプリケーションを開発し、保守する

要件 6 に関する推奨事項および情報

- ❑ 最新の WebFOCUS サービスパックおよび Hotfix を適用します。最新のサービスパックおよびパッチについての詳細は、http://techsupport.ibi.com を参照してください。
- ❑ 製品に同梱されている他社製ソフトウェア (例、Tomcat、 Java) を、それぞれのベンダーで推奨されているバージョンに更新します。

要件項目 6.3 に関する推奨事項および情報

- ❑ アプリケーション開発に関する内部のソフトウェア開発ライフサイクル (SDLC) の推奨事項を順守することで、カスタマイズにより新たな脆弱性が発生しないようにします。
- ❑ 実稼動環境への展開前に、開発時に作成されたテストアカウントを削除します。

要件項目 6.4 に関する推奨事項および情報

- ❑ 開発用、テスト用、実稼動用にそれぞれ異なる WebFOCUS 環境を作成します。
- ❑ WebFOCUS アプリケーションを実稼動環境で直接開発することは避けてください。
- ❑ インストールした WebFOCUS Client および WebFOCUS Reporting Server のサービスパックは、ロールバックすることができます。アンインストール方法についての詳細は、使用するプラットフォームの『TIBCO WebFOCUS インストールガイド』を参照してください。
- ❑ 変更管理機能を使用することで、コンテンツを現在の環境から別の環境へ移動することができます。

要件項目 6.5 および 6.6 に関する推奨事項および情報

- ❑ WebFOCUS 情報保証ベストプラクティスおよびコーディング手法を使用することで、アプリケーションの脆弱性を排除します。
- ❑ 一般ユーザに公開されている WebFOCUS のアプリケーションの場合、顧客側で通常の Web アプリケーション脆弱性評価や外部ファイアウォールのインストールを行う必要があります。

強固なアクセス制御手法の導入

要件 7 - カード会員データへのアクセスを、業務上必要な範囲内に制限する

要件 7 に関する推奨事項および情報

- BI Portal では、ロールベースのセキュリティとオプションの権限が提供されています。アクセス制御には、このセキュリティを使用する必要があります。
- BI Portal のロールベースのセキュリティを使用したユーザアクセス制御は、共有認証スキームを使用して WebFOCUS Reporting Server と統合することができます。詳細は、221 ページの 「 認証と認可 」 を参照してください。
- 必要に応じて、WebFOCUS で行レベルおよび列レベルのセキュリティを追加することができます。

要件 8 - システムコンポーネントへのアクセスを識別、認証する

要件 8 に関する推奨事項および情報

- 同一ユーザによる複数ログインを制限するよう WebFOCUS を構成する必要があります。この制限を構成するには、管理コンソールの [セキュリティ] タブで、[同一ユーザによる多重ログイン] をオフ (False) に設定します。
- WebFOCUS BI Portal ユーザのパスワードは、Sha-512 Salt ハッシュ形式で格納されます。
- WebFOCUS サービスアカウントのパスワードは、内部キーまたは外部キーを使用して、AES128 から AES256 までの暗号化のいずれかの手法で暗号化されます。
- WebFOCUS Reporting Server のサービスアカウントのパスワードは、AES128 から AES256 までの暗号化手法で暗号化されます。
- デフォルトの暗号化手法でも不十分な場合は、カスタム暗号化に WebFOCUS イグジットを使用する方法もあります。詳細は、494 ページの 「 TIBCO WebFOCUS の暗号化機能 」 を参照してください。
- PCI DSS のパスワードポリシーは、次の方法で実装することができます。
  - 管理コンソールでアカウントポリシーを有効にする。
  - セキュリティを他社製の認証プロバイダ (例、Microsoft Active Directory、LDAP、Tivoli Access Manager、CA SiteMinder) に委任するよう WebFOCUS を構成する。
- カード会員データへのパブリックユーザアクセスは制限する必要があります。

- WebFOCUS を構成して、セッションタイムアウトを制御することができます。これにより、ユーザが次のコンポーネントを使用する際に、アクティブ状態を保持する時間が制限されます。
  - グローバル設定
    - *drive*:¥ibi¥WebFOCUS82¥webapps¥webfocus¥WEB-INF¥web.xml ファイルを次のように更新します。

      ```
      <session-config>
      <session-timeout>15</session-timeout>
      </session-config>
      ```

- WebFOCUS アプリケーションは、次のメカニズムを使用してデータベースへのすべてのアクセスを認証します。
  - Password Passthru
  - Explicit
  - Trusted
- adhoc レポートおよび共有レポートの場合は、顧客側で適切な制御および承認を実施する必要があります。

要件 9 - カード会員データへの物理アクセスを制限する

WebFOCUS に適用される要件はありません。

ネットワークの定期的な監視およびテスト

要件 10 - ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する

要件 10 に関する推奨事項および情報

- WebFOCUS Resource Analyzer を使用して、アプリケーションの次の使用状況を監査、モニタすることができます。
  - プロシジャ名、開始日時、実行時間、CPU 使用時間、待機時間
  - 入出力処理、レコード数、トランザクション数、行数
  - BI Portal ワークスペース、BI Portal ユーザ、接続ユーザ ID、APP PATH、ネットワーク接続

- 選択条件、データソース、フィールド

- Resource Analyzer リポジトリへのアクセスは、適切な認可情報を持つユーザ ID に制限する必要があります。詳細は、『TIBCO WebFOCUS Resource Analyzer 利用ガイド』を参照してください。
- WebFOCUS ログは、アプリケーションの開始時に初期設定され、アプリケーションが実行されている間はアクティブ状態が保持されます。
- ユーザおよび管理者が実行したアクションを監査する補助的な制御機能が備わっています。
- ユーザアクセスおよび管理操作の監査が製品に同梱されています。

TIBCO WebFOCUS ログ

ログファイル	USAGE	備考
WebFOCUS BI Portal		
audit.log	すべてのログイン変更、およびセキュリティに関連する変更をトラッキングします。	詳細は、605 ページの 「 ログの収集 」 を参照してください。
WebFOCUS Reporting Server		
edaprint.log	ユーザ接続をトラッキングします。	WebFOCUS Client および ReportCaster から WebFOCUS Reporting Server への接続です。

要件 11 - セキュリティシステムおよびプロセスを定期的にテストする

要件項目 11.3 に関する推奨事項および情報

WebFOCUS ソフトウェアには、戦略的リスク管理および悪意のあるハッカーの攻撃からの保護に重点を置いた、さまざまな新しいセキュリティ機能が追加されています。このレベルのセキュリティは、外部と接触する Web ベースの BI アプリケーションでは不可欠です。
WebFOCUS バージョン 8 ソフトウェアは、OWASP (Open Web Application Security Project) により定義されたアプリケーションセキュリティ検証標準 (Application Security Verification Standards) で、最も重要なセキュリティの脆弱性および脅威に対して、低リスクセキュリティであるレベル 3 を達成しています。

製品に含まれているセキュリティ対策には次のものがあります。

- XSS 脆弱性に対する攻撃から保護するための クロスサイトスクリプティング (XSS) 防御
- セッション固定の脆弱性に対する攻撃から保護するためのセッション固定防御
- クロスサイトリクエストフォージェリ (CSRF) 脆弱性に対する攻撃から保護するための CSRF フィルタ
- NULL タイプインジェクション攻撃から保護するための NULL インジェクションフィルタ
- フレームインジェクション脆弱性に対する攻撃から保護するためのクラックジャッキングフィルタ

情報保証および OWASP についての詳細は、「http://www.owasp.org」を参照してください。

要件項目 11.5 に関する推奨事項および情報

下表は、重要な WebFOCUS 構成が格納されているディレクトリをコンポーネントごとに示しています。ここで、drive は WebFOCUS インストールディレクトリを表しています。

TIBCO WebFOCUS 構成ディレクトリ

ディレクトリ	用途	備考
WebFOCUS Reporting Server		
drive:¥ibi¥srv82¥wfs¥etc	TCP/IP 通信とプロファイル	TCP/IP ポートの定義に使用します。 ホストグローバルプロファイルです。
drive:¥ibi¥profiles	プロファイル情報	ホストプロファイルおよびユーザプロファイルです。
drive:¥ibi¥srv82¥wfs¥bin	edaserve.cfg	主要な Reporting Server 構成ファイルです。
ReportCaster		

ディレクトリ	用途	備考
drive:¥ibi¥WebFOCUS82¥ReportCaster¥cfg	構成情報	Reporting Server の構成に使用します。 このフォルダ内のファイルは、リポジトリに格納されている ReportCaster 構成ファイル (dserver.xml) を補足するものです。
WebFOCUS Client		
drive:¥ibi¥WebFOCUS82¥client¥wfc¥web¥cgi	トレース情報	トレースレベルの定義に使用します。
drive:¥ibi¥WebFOCUS82¥client¥wfc¥etc	構成情報	セキュリティ、タイムアウト、およびその他の構成パラメータの構成に使用します。
drive:¥ibi¥WebFOCUS82¥config	構成情報	セキュリティ、タイムアウト、およびその他の構成パラメータの構成に使用します。
drive:¥ibi¥WebFOCUS82¥webapps	Web アプリケーション	WebFOCUS に同梱されている Web アプリケーションのホストとして使用します。

情報セキュリティポリシーの整備

要件 12 - すべての担当者の情報セキュリティポリシーを整備する

WebFOCUS に適用される要件はありません。

I

TIBCO WebFOCUS リポジトリデータベースの複製

リポジトリデータベースレプリケーションユーティリティは、ソースデータベースからターゲットデータベースに WebFOCUS リポジトリのコピーを転送します。このユーティリティを使用することで、転送中のリポジトリデータベースの構造およびコンテンツの完全性が保持されるため、WebFOCUS リポジトリの複製を Derby から Oracle、Db2、PostgreSQL、MySQL AB、Microsoft SQL Server に転送することができます。

トピックス

概要

リポジトリデータベースを複製するには、次の手順を実行します。

1. ターゲットリレーショナルデータベースを作成します。
2. ソースおよびターゲットのデータベース接続情報と認証情報を特定します。
3. ソースおよびターゲットのデータベース認証情報と接続情報を、データベースレプリケーション設定ファイルのそれぞれの設定に割り当てます。
4. データベースレプリケーションユーティリティを実行します。
5. レプリケーションユーティリティの実行結果を確認します。
6. install.cfg ファイルのデフォルト WebFOCUS リポジトリデータベースの設定を、複製された WebFOCUS リポジトリデータベースの設定で置き換えます。
7. 複製済み WebFOCUS リポジトリデータベースへの接続をテストします。

このユーティリティを正しく実行するために必要な認証情報およびソースとターゲットのデータベース接続情報についての詳細は、754 ページの 「 データベースレプリケーション設定の理解 」 を参照してください。

概要に示したように、このユーティリティを使用して、リポジトリデータベースの複製を Derby から Oracle、Db2、PostgreSQL、MySQL AB、Microsoft SQL Server に転送することができます。また、このユーティリティを使用して、これらのリレーショナルデータベース管理システム (RDBMS) からリポジトリデータベースの複製を Derby に転送することもできます。

リポジトリをその他のデータベースプラットフォームに複製する必要がある場合は、技術サポートに問い合わせてください。データベースレプリケーションユーティリティでは、非リレーショナルデータベースまたは JDBC ドライバを使用しないデータベースプラットフォームにリポジトリを複製することはできません。

手順　ソースおよびターゲットのデータベース接続情報と認証情報を特定するには

ソースデータベースの接続情報および認証情報を特定するには、次の手順に従って、utiluservars.bat ファイルおよび install.cfg ソースファイルを開きます。

1. 次のように、utiluservars.bat ファイルを開きます。

   - Windows の場合 - *drive*:¥ibi¥WebFOCUS82¥utilities¥setenv に移動し、utiluservars.bat ファイルをテキストエディタで開きます。
   - UNIX または Linux の場合 - *install_directory*/ibi/WebFOCUS82/utilities/setenv に移動し、utiluservars.sh ファイルをテキストエディタで開きます。

   このファイルの JDBC_PATH パラメータ値は、db_replication_settings ファイルの SOURCE_JDBC_PATH パラメータの値として使用されます。

2. 次のように、install.cfg ファイルを開きます。

   - Windows の場合 - *drive*:¥ibi¥WebFOCUS82¥config に移動し、install.cfg ファイルをテキストエディタで開きます。
   - UNIX または Linux の場合 - *install_directory*/ibi/WebFOCUS82/config に移動し、install.cfg ファイルをテキストエディタで開きます。

   このファイルの IBI_REPOS_DB_URL、IBI_REPOS_DB_DRIVER、IBI_REPOS_DB_USER パラメータの値は、db_replication_settings ファイルの SOURCE_REPOS_DB_URL、SOURCE_REPOS_DB_DRIVER、SOURCE_USER_NAME パラメータの値として使用されます。

3. データベースレプリケーション設定ファイルの構成が完了するまで、両方のファイルを開いておきます。
4. ターゲットデータベースの接続情報および認証情報を特定するには、ブランクのターゲットデータベースを作成したデータベース管理者に問い合わせてください。

   または

   ベンダーが提供するターゲットデータベースの構成およびマニュアルを参照してください。

ターゲットデータベースの特定の値の場所および構成は、ベンダーによって異なるため、このマニュアルでは説明を省略します。

手順　データベースレプリケーション設定ファイルを準備するには

準備を開始する前に、ターゲットデータベースとして使用するブランクのリレーショナルデータベースが作成済みであること、ソースデータベースとターゲットデータベースの両方で、最新のデータベース認証情報および接続情報が使用可能であることを確認します。

1. 次のように、db_replicate_settings ファイルを開きます。
   - Windows の場合 - *drive*:¥ibi¥WebFOCUS82¥utilities¥dbupdate に移動し、db_replicate_settings.bat ファイルをテキストエディタで開きます。
   - UNIX または Linux の場合 - *install_directory*/ibi/WebFOCUS82/utilities/dbupdate に移動し、db_replicate_settings.sh ファイルをテキストエディタで開きます。
   - **注意：**元の db_replicate_settings ファイルのバックアップコピーを保存する必要がある場合は、変更する前にこのファイルのコピーを作成します。
2. このファイルのソースセクションまで下方向へスクロールします。
3. SOURCE_CLASS_PATH パラメータで、表示されているデフォルト設定のパス名を受容します。変更はしません。
4. SOURCE_JDBC_PATH パラメータで、サンプル値を、utiluservars.bat ファイルの JDBC_PATH パラメータで指定されたソースデータベースの JDBC ドライバへのパス名で置換します。

   この値は、二重引用符 (") で囲む必要があります。
5. SOURCE_REPOS_DB_URL パラメータで、サンプル値を、install.cfg ファイルの IBI_REPOS_DB_URL パラメータの URL で置換します。
6. SOURCE_REPOS_DB_DRIVER パラメータで、サンプル値を、install.cfg ファイルの IBI_REPOS_DB_DRIVER パラメータの JDBC ドライバクラス名で置換します。
7. SOURCE_USER_NAME パラメータの値を、install.cfg ファイルの IBI_REPOS_DB_USER パラメータの値 (ユーザ ID) で置換します。

   ユーザ ID の文字およびフォーマットが、ソースデータベースで表示されるユーザ ID と正確に一致していること、およびユーザ ID の前後に余分なブランクが含まれていないことを確認します。

   このパラメータに有効なユーザ ID が割り当てられなかった場合、データベースレプリケーションユーティリティで実行時に有効なユーザ ID の入力が要求されます。

8. db_replicate_settings ファイルの SOURCE_PASSWORD パラメータで、製品インストール時にリポジトリのユーザ名に割り当てられたパスワードを入力します。

   この値は、install.cfg ファイルの IBI_REPOS_DB_PASSWORD パラメータでは暗号化されているため、install.cfg ファイルから貼り付けることはできません。

   パスワードの文字およびフォーマットが、ソースデータベースで表示されるパスワードと正確に一致していること、およびパスワードの前後に余分なブランクが含まれていないことを確認します。

   このパラメータに有効なパスワードが割り当てられなかった場合、データベースレプリケーションユーティリティで実行時に有効なパスワードの入力が要求されます。
9. このファイルのターゲットセクションまで下方向へスクロールします。
10. TARGET_JDBC_PATH パラメータで、サンプル値を、ターゲットデータベースの JDBC ドライバパス名で上書きします。

    JDBC ドライバが複数の jar ファイルで構成されている場合は、それぞれの jar ファイルのパスをセミコロン (;) で区切ります。
11. TARGET_REPOS_DB_URL パラメータで、サンプル値を、ターゲットデータベース接続の URL で上書きします。
12. TARGET_REPOS_DB_DRIVER パラメータで、サンプル値を、ターゲットデータベースの JDBC ドライバのクラス名で上書きします。
13. Å_NAME パラメータで、作成時に新しいデータベースに割り当てられたユーザ ID を入力します。

    ユーザ ID の文字およびフォーマットが、ターゲットデータベースで表示されるユーザ ID と正確に一致していること、およびユーザ ID の前後に余分なブランクが含まれていないことを確認します。

    このパラメータに有効なユーザ ID が割り当てられなかった場合、データベースレプリケーションユーティリティで実行時に有効なユーザ ID の入力が要求されます。
14. TARGET_PASSWORD パラメータで、新しいデータベースのユーザ ID に割り当てられたパスワードを入力します。

    パスワードの文字およびフォーマットが、ターゲットデータベースで表示されるパスワードと正確に一致していること、およびパスワードの前後に余分なブランクが含まれていないことを確認します。

    このパラメータに有効なパスワードが割り当てられなかった場合、データベースレプリケーションユーティリティで実行時に有効なパスワードの入力が要求されます。
15. 変更を保存し、db_replicate_settings ファイルを閉じます。

手順　データベースレプリケーションユーティリティを実行するには

開始前に、ターゲットデータベースがアクセス可能な場所にあること、およびソースデータベースとターゲットデータベースのユーザ認証情報および接続情報が db_replicate_settings ファイルに割り当て済みであることを確認します。

1. 次のように、データベースレプリケーションユーティリティを開始します。
   - Windows の場合 - *drive*:¥ibi¥WebFOCUS82¥utilities¥dbupdate に移動し、db_replicate.bat をダブルクリックします。
   - UNIX または Linux の場合 - *install_directory*/ibi/WebFOCUS82/utilities/dbupdate に移動し、db_replicate.sh をダブルクリックします。
2. 次のいずれかのプロンプトが表示された場合、次のように回答し、回答するたびに Enter キーを押します。
   a. Enter Source Database Repository Username - 製品インストール時に作成された WebFOCUS リポジトリに割り当てられたユーザ ID を入力します。
   b. Enter Source Database Repository Password - リポジトリユーザ名に割り当てられたパスワードを入力します。

      注意：パスワードの入力時は、カーソルが動かず、入力した文字は表示されません。
   c. Enter Target Database Repository Username - 作成時に新しいデータベースに割り当てられたユーザ ID を入力します。
   d. Enter Target Database Repository Password - 新しいデータベースのユーザ ID に割り当てられたパスワードを入力します。

      注意：パスワードの入力時は、カーソルが動かず、入力した文字は表示されません。
3. [コマンドプロンプト] ウィンドウをモニタします。ウィンドウには、このユーティリティの実行で指定したパラメータおよび値のリストが表示されます。
4. 「DB update process is starging」というメッセージが表示された場合、ユーティリティがデータベースのレプリケーションプロセスを完了するまで待機します。この処理には数秒かかることがあります。
5. ユーティリティを停止するエラーメッセージが表示された場合 (例、「jdbc driver not found」、「credentials invalid」、「credentials don’t have ability to access source or target」)、次の手順を実行します。
   a. [コマンドプロンプト] ウィンドウを閉じます。
   b. db_replicate_settings ファイルに割り当てられた値を、749 ページの「 データベースレプリケーション設定ファイルを準備するには 」 の手順に従って修正します。

これらのエラーは、ユーティリティ実行時に作成された db_replicate_install ログファイルでも確認できます。ログファイルの開き方および確認方法についての詳細は、752 ページの 「 レプリケーションの結果を確認するには 」 を参照してください。

6. データベースの更新が成功したことを示すメッセージが表示された場合、任意のキーを押して [コマンドプロンプト] ウィンドウを閉じます。

手順　レプリケーションの結果を確認するには

データベースレプリケーションユーティリティのログを使用して、レプリケーションプロセスで発生したエラーの特定とその対応ができます。ユーティリティで生成されたログは、WebFOCUS バージョン 8.2.05 以降では、application_logs ディレクトリに格納されます。

1. 管理者としてログインし、管理コンソールを起動します。
2. [機能診断] タブをクリックし、[アプリケーションログファイル] を選択します。
3. [アプリケーションログファイル] ページで、db_replicate_install_2_YYYY-MM-DD_HH-MM-SS.txt をクリックします。ここでは、YYYY-MM-DD_HH-MM-SS は、データベースレプリケーションユーティリティのログファイルが作成された日付と時間を示します。
4. ログファイルページのレコードで、レプリケーションが正常に完了したこと、および完了できなかったことを示すエラーメッセージが表示されていないことを確認できます。

   最終エントリに「Update process SUCCEEDED」と表示された場合、レプリケーションは正常に完了しています。
5. ログファイルページを閉じ、ログアウトします。

手順　古いソースデータベースから新しいターゲットデータベースにリポジトリデータベースをリダイレクトするには

ソースデータベースが、レプリケーション後もプリンシパルリポジトリデータベースとして維持される場合、これをさらに確認したり更新したりする必要はありません。ただし、ターゲットデータベースが新しいプリンシパルリポジトリデータベースになる場合、新しく複製されたリポジトリデータベースの有効化を完了する必要があります。この場合、install.cfg ファイルを開き、ソースデータベースのユーザ名、パスワード、データベースドライバ、データベース URL をターゲットデータベースのものと置換します。

1. Application Server が実行中であれば、これを停止します。
2. config ディレクトリに移動します。
   - *drive*:¥ibi¥WebFOCUS82¥config (Windows)
   - *install_directory*/ibi/WebFOCUS82/config (UNIX または Linux)

3. install.cfg ファイルのバックアップコピーを作成して保存します。
4. install.cfg ファイルをテキストエディタで開きます。
5. IBI_REPOS_DB_USER パラメータで、ソースデータベースの既存の値を、ターゲットデータベースに割り当てられたユーザ名で上書きします。

   ユーザ ID の文字およびフォーマットが、ソースデータベースで表示されるユーザ ID と正確に一致していること、およびユーザ ID の前後に余分なブランクが含まれていないことを確認します。
6. IBI_REPOS_DB_PASSWORD パラメータで、ソースデータベースの暗号化されたパスワードを、ターゲットデータベースのデータベースユーザに割り当てられた新しいプレーンテキストパスワードで上書きします。

   パスワードの文字およびフォーマットが、ソースデータベースで表示されるパスワードと正確に一致していること、およびパスワードの前後に余分なブランクが含まれていないことを確認します。

   プレーンテキストパスワードは、Application Server を再起動すると自動的に暗号化されます。
7. IBI_REPOS_DB_DRIVER パラメータで、ソースデータベースのデータベースドライバのクラス名を、ターゲットデータベースのデータベースドライバのクラス名で上書きします。
8. IBI_REPOS_DB_URL パラメータで、ソースデータベース接続の URL を、ターゲットデータベース接続の URL で上書きします。
9. 新しく入力した値が正しいことを確認し、install.cfg ファイルを保存して閉じます。
10. Application Server を再起動すると、install.cfg ファイルのリポジトリデータベースユーザのプレーンテキストパスワードが暗号化されます。

    注意：再起動時に、Application Server が新しい RDBMS の使用を試みます。

手順　新しいリポジトリデータベース接続をテストするには

1. Application Server が停止されず、install.cfg ファイルの更新後に再起動されなかった場合は、次の手順を始める前に Application Server を起動または再起動します。
2. 管理者としてログインし、管理コンソールを起動します。
3. 752 ページの 「 レプリケーションの結果を確認するには 」 の手順に従って、データベースレプリケーションユーティリティのログファイルを開きます。
4. ログファイルでエラーメッセージがないか確認します。
5. Application Server が新しい RDBMS への接続を試みた際に発生したエラーがあれば、これに対応します。

6. データベースレプリケーションユーティリティのログファイルのエラーに対応後、管理者として再度ログインします。
7. ログイン時にエラーが発生した場合、install.cfg ファイルの IBI_REPOS_DB 設定に割り当てられた値に、新しいターゲットデータベースの適切な接続値が含まれていることを確認します。
8. エラーが発生することなくレポートを実行できた場合は、ターゲットデータベースへの接続が正常に確立されています。

データベースレプリケーション設定の理解

データベースレプリケーションユーティリティで必要な設定の値は、db_replicate_settings ファイルに格納されます。このファイルには、[Prompt if Needed]、[Samples]、[Source]、[Target] の 4 つの主要セクションがあります。

[Prompt if Needed] セクションでは、データベースレプリケーションユーティリティのインタラクティブモードを有効または無効にすることができます。デフォルト設定でこのモードは有効になっており、データベースレプリケーションユーティリティを実行する際は必ずプロンプトが表示され、欠落しているデータベース接続情報の入力が要求されます。

[Samples] セクションには、サンプルのデータベースドライバのパスと URL、およびさまざまな RDBMS プロバイダ (例、MS SQL Server、PostgresSQL、MySQL、Db2、Oracle、Derby) のサンプル JDBC パスが含まれます。詳細は、最新バージョンの db_replicate_settings ファイルを参照してください。

[Source] セクションには、製品インストール時に作成されたリポジトリデータベースの接続情報を定義する次の設定が含まれます。このデータベースは、レプリケーションのソースとして使用されます。

SOURCE_CLASS_PATH の値を除き、[Source] セクションのサンプル値は、WebFOCUS のローカルインストールで使用した値に適合する値で置き換える必要があります (ローカルインストール構成の値と [SOURCE] セクションの設定に割り当てられたサンプル値が一致しない場合)。これらの値をクリアして、実行時にデータベースレプリケーションユーティリティがこれらの情報を要求するようにすることもできます。

- **SOURCE_CLASS_PATH**　複製元のデータベースと一致するエンティティクラスのパスを定義します。CLASSPATH は、WebFOCUS リポジトリの IBFSCommands.jar ファイルのパスです。この設定の値は、更新する必要がありません。

  データベースレプリケーションユーティリティでは、ターゲットデータベースのクラスパスは定義されません。

db_replicate_settings ファイルのこの設定に割り当てられた値には、Windows の場合は %WFROOT%、UNIX の場合は ${WFROOT} という変数が含まれます。この変数は、WebFOCUS インストールのルートディレクトリを取得します。このルートディレクトリ内では、IBFSCommands.jar ファイルのパスは変わりません。

- ¥utilities¥lib¥ (Windows)
- /utilities/lib/ (UNIX または Linux)

- **SOURCE_JDBC_PATH**　ソースデータベースの JDBC ドライバを構成する jar ファイルのフルパスを定義します。JDBC ドライバが複数の jar ファイルで構成されている場合は、それぞれの jar ファイルのパスをセミコロン (;) で区切ります。

  このフィールドに割り当てられたサンプル値は、データベースレプリケーションユーティリティの実行前に、組織で使用するパス名で置き換える必要があります。

  WebFOCUS インストールで使用されるソースデータベースの JDBC ドライバパスは、utiluservars.bat ファイルの JDBC_PATH パラメータで特定することができます。このファイルは、Windows の場合は *drive*:¥ ibi¥WebFOCUS82¥utilities¥setenv、UNIX または Linux の場合は *install_directory*/ibi/WebFOCUS82/utilities/setenv に格納されています。

  - 通常の Windows ベースの WebFOCUS インストールでは、JDBC ドライバの jar ファイルは、*drive*:¥ibi¥derby¥lib¥derbyclient.jar に格納されています。
  - 通常の UNIX または Linux ベースの WebFOCUS インストールでは、JDBC ドライバの jar ファイルは、*install_directory*/ibi/Drivers/derbyclient-10.8.1.2.jar に格納されています。

- **SOURCE_REPOS_DB_URL**　ソースデータベースへの接続文字列を特定する URL を定義します。この場合、URL のフォーマットは次のとおりです。

  ```
  jdbc:subprotocol:node/databaseName
  ```

  説明

  `jdbc`
  Java データベースのクラスプロトコルです。

  `subprotocol`
  データベースをホストする RDBMS のプロトコルです。 (例、derby//localhost)。

  注意：データベースが Java プログラムと同一マシンのノードに格納されている場合、JDBC のホスト名の部分と対応するダブルスラッシュ (//) は省略できます (例、jdbc:odbc:wham)。

`node`
データベースをホストするマシンのポート番号です。たとえば、データベースが同一マシン上にある場合は 8080 です。

`databaseName`
リポジトリデータベースまたはそのコピーの名前です (例、WebFOCUS82)。

このフィールドに割り当てられたサンプル値は、データベースレプリケーションユーティリティの実行前に、組織で使用するデータベース接続文字列で置き換える必要があります。

WebFOCUS インストールで使用されるソースデータベースの URL は、install.cfg ファイルの IBI_REPOS_DB_URL パラメータで特定することができます。このファイルは、Windows の場合は *drive*:¥ibi¥WebFOCUS82¥config、UNIX または Linux の場合 *install_directory*/ibi/WebFOCUS82/config に格納されています。

通常の Windows ベースおよび UNIX または Linux ベースの WebFOCUS インストールでは、データベース接続文字列は次のとおりです。

```
jdbc:derby://localhost:1527/WebFOCUS82;
```

- **SOURCE_REPOS_DB_DRIVER** リポジトリ (ソースデータベース) の JDBC (Java Database Connectivity) ドライバを含む jar ファイルのパスを定義します。JDBC ドライバクラスは、このデータベースのネットワークサーバへのネットワーク接続を提供します。

  製品インストールで使用される URL は、install.cfg ファイルの IBI_REPOS_DB_DRIVER パラメータで特定することができます。このファイルは、Windows の場合は drive:¥ibi¥WebFOCUS82¥config、UNIX または Linux の場合は install_directory/ibi/WebFOCUS82/config に格納されています。

  通常の製品インストールでは、JDBC ドライバを含む jar ファイルのパスは次のとおりです。

  ```
  org.apache.derby.jdbc.ClientDriver
  ```

- **SOURCE_USER_NAME** ソースデータベースユーザの ID を定義します。ユーティリティを実行する場合、この設定には製品インストール時にリポジトリに割り当てられたユーザ名を指定する必要があります。

  製品インストールで使用されるソースデータベースのユーザ ID は、install.cfg ファイルの IBI_REPOS_DB_USER パラメータで特定することができます。このファイルは、Windows の場合は drive:¥ibi¥WebFOCUS82¥config、UNIX または Linux の場合は install_directory/ibi/WebFOCUS82/config に格納されています。

デフォルト設定で、この設定にはサンプル値の username が指定されています。このフィールドにソースデータベースのユーザ ID を指定しないでデータベースレプリケーションユーティリティを実行すると、プロンプトが表示され、ソースデータベースのユーザ名の入力が要求されます。

データベースのユーザ ID は、割り当てられたユーザおよびアプリケーションに、データベースの情報およびリソースへのアクセス権限を与えます。ソースデータベースのユーザ ID には、データベースオブジェクトの読み取り権限が必要です。

- **SOURCE_PASSWORD** ソースデータベースのユーザに割り当てられたパスワードを定義します。ユーティリティを実行する場合、この設定には製品インストール時にリポジトリに割り当てられたパスワードを指定する必要があります。

  製品インストールで使用されるソースデータベースのユーザに割り当てられたパスワードの暗号化バージョンは、install.cfg ファイルの IBI_REPOS_DB_PASSWORD パラメータで特定することができます。このファイルは、Windows の場合は drive:¥ibi¥WebFOCUS82¥config、UNIX または Linux の場合は install_directory/ibi/WebFOCUS82/config に格納されています。

  デフォルト設定で、この設定にはサンプル値の password が指定されています。このフィールドにソースデータベースのパスワードを指定しないでデータベースレプリケーションユーティリティを実行すると、プロンプトが表示され、ソースデータベースユーザのパスワードの入力が要求されます。

  このソースデータベースのパスワードは、ソースデータベースのユーザ ID を認証します。

データベースレプリケーション設定ファイルの [TARGET] セクションには、レプリケーションのターゲットデータベースへの接続を定義する次の設定が含まれます。

[TARGET] セクションのサンプル値は、作成するターゲットデータベースに適合する値で常に置換するか、サンプル値をクリアして、実行時にデータベースレプリケーションユーティリティがこれらの情報の入力を要求するようにします。

- **TARGET_JDBC_PATH** ターゲットデータベースの JDBC (Java Database Connectivity) ドライバを含む jar ファイルのパスを指定します。JDBC ドライバクラスは、ターゲットデータベースのネットワークサーバへのネットワーク接続を提供します。

  サンプル値は、データベースレプリケーションユーティリティの実行前に、ターゲットデータベースの JDBC パスで置換する必要があります。

- **TARGET_REPOS_DB_URL** ターゲットデータベースへの接続文字列を特定する URL です。この場合の URL のフォーマットは次のとおりです。

  ```
  jdbc:subprotocol:node/databaseName
  ```

説明

`jdbc`
Java データベースのクラスプロトコルです。

`subprotocol`
データベースをホストする RDBMS のプロトコルです。 (例、derby//localhost)。

注意：データベースが Java プログラムと同一マシンのノードに格納されている場合、JDBC のホスト名の部分と対応するダブルスラッシュ (//) は省略できます (例、jdbc:odbc:wham)。

`node`
データベースをホストするマシンのポート番号です。たとえば、データベースが同一マシン上にある場合は 8080 です。

`databaseName`
ターゲットデータベースの名前です。

サンプル値は、データベースレプリケーションユーティリティの実行前に、ターゲットデータベースの URL で置換する必要があります。

- **TARGET_REPOS_DB_DRIVER** ターゲットデータベースの JDBC (Java Database Connectivity) ドライバを含む jar ファイルのパスを定義します。JDBC ドライバクラスは、ターゲットデータベースのネットワークサーバへのネットワーク接続を提供します。

  サンプル値は、データベースレプリケーションユーティリティの実行前に、ターゲットデータベースの JDBC ドライバパスで置換する必要があります。

- **TARGET_USER_NAME** ターゲットデータベースのユーザ ID を定義します。ユーティリティを実行する場合、この設定には作成時にターゲットデータベースに割り当てられたユーザ名を指定する必要があります。

  ただし、デフォルト設定ではサンプル値の username が表示されます。このフィールドにターゲットデータベースのユーザ ID を指定しないでデータベースレプリケーションユーティリティを実行すると、プロンプトが表示され、ターゲットデータベースのユーザ名の入力が要求されます。

  データベースのユーザ ID は、割り当てられたユーザおよびアプリケーションに、ソースデータベースの情報およびリソースへのアクセス権限を与えます。ターゲットデータベースのユーザ ID には、データベースオブジェクトの作成および変更権限が必要です。

- **TARGET_PASSWORD**　ターゲットデータベースのユーザに割り当てられたパスワードを定義します。ユーティリティを実行する場合、この設定にはターゲットデータベースの作成時にターゲットデータベースのユーザ名に割り当てられたパスワードを指定する必要があります。

  ただし、デフォルト設定ではサンプル値の password が指定されます。このフィールドにターゲットデータベースのパスワードを指定しないでデータベースレプリケーションユーティリティを実行すると、プロンプトが表示され、ターゲットデータベースユーザのパスワードの入力が要求されます。

  このパスワードは、ターゲットデータベースのデータベースユーザ ID を認証します。

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE "LICENSE" FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the readme file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.