Informatica

Informatica® Multidomain MDM
10.4

セキュリティガイド

Informatica Multidomain MDM セキュリティガイド
10.4
2020 年 3 月

発行日: 2020-06-05

目次

序文 7

Informatica のリソース 7

Informatica Network 7

Informatica ナレッジベース 7

Informatica マニュアル 8

Informatica 製品可用性マトリックス 8

Informatica Velocity 8

Informatica Marketplace 8

Informatica グローバルカスタマサポート 8

第 1 章 : MDM Hub のセキュリティの概要 9

MDM Hub のセキュリティの概要 9

MDM Hub コンソール 10

Dynamic Data Masking 10

セキュリティアクセスマネージャ 11

認証 11

認証 12

セキュアリソースと特権 12

ロール 13

セキュリティの実装シナリオ 13

内部ポリシー決定ポイント 14

外部ユーザーディレクトリ 14

ロールベースの集中管理型のポリシー決定 15

包括的な集中管理型のポリシー決定 15

セキュリティの設定タスクのシナリオ 16

第 2 章 : リソース 17

リソース概要 17

セキュアリソースと非公開リソース 18

リソースグループ 18

リソースグループ階層 19

セキュアリソース 19

セキュアリソースツール 19

セキュアリソースの設定 19

MDM Hub リソースのステータスの設定 20

リソースのフィルタリング 20

リソースグループの設定 20

リソースグループの追加 21

リソースグループの編集および削除 21

リソースリストの更新 22

その他のセキュリティ変更の更新. 22
Data Director ビジネスエンティティサービスのセキュリティの設定. 22
セキュアリソースとしてのビジネスエンティティサービスの設定. 22
ビジネスエンティティサービスへのロール特権の割り当て. 23

第 3 章 : ロール. 24
ロールの概要. 24
ロールの設定. 24
ロールの追加. 25
ロールの編集および削除. 25
特権. 25
内部ロールと外部ロール. 26
ロールへのリソース特権の割り当て. 26
他のロールへのロールの割り当て. 27
ロールのリソース特権レポートの生成. 27
生成されたレポートの HTML ファイルとしての保存. 27

第 4 章 : ユーザーとユーザーグループ. 29
ユーザーおよびユーザーグループの概要. 29
ユーザー設定. 29
MDM Hub のリソースへのユーザーアクセス. 30
ユーザーアカウントの追加. 30
ユーザーアカウントの編集および削除. 31
ユーザーの補足情報の編集. 31
ユーザーアカウントのパスワード設定の変更. 32
オペレーショナルリファレンスストアへのユーザーアクセスの設定. 32
パスワードポリシー設定. 32
パスワードポリシー設定. 33
グローバルパスワードポリシーの管理. 33
プライベートパスワードポリシーの管理. 34
JDBC データソースのセキュリティ設定. 34
保護された JDBC データソースのユーザー名とパスワード. 34
Oracle SID 接続タイプのデータベース ID. 34
Oracle サービス接続タイプのデータベース ID. 35
IBM DB2 接続タイプのデータベース ID. 35
Microsoft SQL Server 接続タイプのデータベース ID. 35
マスターデータベースのデータベース ID. 36
パスワードの暗号化. 36
ユーザーグループ設定. 36
ユーザーとグループツールの起動. 36
ユーザーグループの追加. 37
ユーザーグループの編集および削除. 37
ユーザーグループへのユーザーとユーザーグループの割り当て. 37

現在の ORS データベースへのユーザーの割り当て. 38
ロールとユーザーおよびユーザーグループの間の関連付け. 38
ロールへのユーザーとユーザーグループの割り当て. 38
ユーザーとユーザーグループへのロールの割り当て. 39

第 5 章 : セキュリティプロバイダ. 40
セキュリティプロバイダの概要. 40
セキュリティプロバイダ管理. 40
プロバイダファイル管理. 41
プロバイダファイルのアップロード. 41
プロバイダファイルの削除. 42
セキュリティプロバイダの設定. 42
セキュリティプロバイダの設定の変更. 42
セキュリティプロバイダの有効化および無効化. 43
セキュリティプロバイダの処理順の移動. 43
プロバイダのプロパティ. 43
プロバイダのプロパティの追加. 44
プロバイダプロパティの編集. 44
カスタムプロバイダ. 44
サンプルの providers.properties ファイル. 45
外部認証. 46
ログインモジュールの追加. 46
ログインモジュールの削除. 46

第 6 章 : アプリケーションレベルセキュリティ. 48
アプリケーションレベルセキュリティ概要. 48
Informatica Data Director. 49
プロビジョニングツール. 50
ActiveVOS. 50
Dynamic Data Masking. 51
Dynamic Data Masking と MDM Hub の統合. 51
MDM Hub 用の Dynamic Data Masking のベストプラクティス. 52
Dynamic Data Masking のオペレーショナルリファレンスストア用セットアップ. 52
Linux での WebLogic T3S チャネルのセットアップ. 53

第 7 章 : 証明書ベースの認証. 55
証明書ベースの認証概要. 55
証明書ベースの認証と外部クライアント. 55
信頼されたアプリケーション. 56
信頼されたアプリケーションとしての外部アプリケーションの追加. 56
証明書とキーの管理 56
セキュリティ設定ユーティリティ. 57

第 8 章 : パスワードのハッシュ化 58
パスワードのハッシュ化の概要 58
パスワードのハッシュ化オプション 59
カスタムハッシュアルゴリズム 59
パスワードリセットのプロセス 59
セキュリティ設定ユーティリティ 60
トラブルシューティング 60

付録 A : 用語集 61

索引 65

序文

Informatica (R) *Multidomain MDM のセキュリティガイド*を使用して、Multidomain MDM でセキュリティを有効にする方法を学習します。セキュリティアクセスマネージャを使用して MDM Hub リソースを保護し、Dynamic Data Masking を使用して機密データへのアクセスを防止する方法を理解します。ユーザーセキュリティを管理するために、ユーザーとグループの管理方法、権限、特権、ロールの使用方法を学習します。

このガイドでは、オペレーティングシステム、データベース環境、アプリケーションサーバーの知識があることを前提としています。

Informatica のリソース

Informatica は、Informatica Network やその他のオンラインポータルを通じてさまざまな製品リソースを提供しています。リソースを使用して Informatica 製品とソリューションを最大限に活用し、その他の Informatica ユーザーや各分野の専門家から知見を得ることができます。

Informatica Network

Informatica Network は、Informatica ナレッジベースや Informatica グローバルカスタマサポートなど、多くのリソースへの入口です。Informatica Network を利用するには、https://network.informatica.com にアクセスしてください。

Informatica Network メンバーは、次のオプションを利用できます。

- ナレッジベースで製品リソースを検索できます。
- 製品の提供情報を表示できます。
- サポートケースを作成して確認できます。
- 最寄りの Informatica ユーザーグループネットワークを検索して、他のユーザーと共同作業を行えます。

Informatica ナレッジベース

Informatica ナレッジベースを使用して、ハウツー記事、ベストプラクティス、よくある質問に対する回答など、製品リソースを見つけることができます。

ナレッジベースを検索するには、https://search.informatica.com にアクセスしてください。ナレッジベースに関する質問、コメント、ご意見の連絡先は、Informatica ナレッジベースチーム（KB_Feedback@informatica.com）です。

Informatica マニュアル

Informatica マニュアルポータルでは、最新および最近の製品リリースに関するドキュメントの膨大なライブラリを参照できます。マニュアルポータルを利用するには、https://docs.informatica.com にアクセスしてください。

製品マニュアルに関する質問、コメント、ご意見については、Informatica マニュアルチーム（infa_documentation@informatica.com）までご連絡ください。

Informatica 製品可用性マトリックス

製品可用性マトリックス（PAM）には、製品リリースでサポートされるオペレーティングシステム、データベースなどのデータソースおよびターゲットが示されています。Informatica PAM は、https://network.informatica.com/community/informatica-network/product-availability-matrices で参照できます。

Informatica Velocity

Informatica Velocity は、Informatica プロフェッショナルサービスが開発したヒントとベストプラクティスのコレクションで、多数のデータ管理プロジェクトから得た実体験に基づいています。Informatica Velocity には、世界中の組織と連携してデータ管理ソリューションを計画、開発、デプロイ、管理する Informatica コンサルタントによる集合知を表しています。

Informatica Velocity リソースには、http://velocity.informatica.com からアクセスしてください。Informatica Velocity についての質問、コメント、またはアイデアがある場合は、ips@informatica.com から Informatica プロフェッショナルサービスにお問い合わせください。

Informatica Marketplace

Informatica Marketplace は、お使いの Informatica 製品を拡張したり強化したりするソリューションを検索できるフォーラムです。Marketplace で、Informatica デベロッパーやパートナーからの多数のソリューションを活用すれば、生産性を向上したり、プロジェクトでの実装時間を短縮したりできます。Informatica Marketplace は、https://marketplace.informatica.com からアクセスしてください。

Informatica グローバルカスタマサポート

電話または Informatica Network からグローバルサポートセンターに連絡できます。

各地域の Informatica グローバルカスタマサポートの電話番号は、Informatica Web サイト（https://www.informatica.com/services-and-training/customer-success-services/contact-us.html）を参照してください。

Informatica Network でオンラインサポートリソースを見つけるには、https://network.informatica.com にアクセスし、eSupport オプションを選択します。

第 1 章

MDM Hub のセキュリティの概要

この章では、以下の項目について説明します。

- MDM Hub のセキュリティの概要 , 9 ページ
- MDM Hub コンソール, 10 ページ
- Dynamic Data Masking , 10 ページ
- セキュリティアクセスマネージャ , 11 ページ
- 認証, 11 ページ
- 認証, 12 ページ
- セキュアリソースと特権, 12 ページ
- ロール, 13 ページ
- セキュリティの実装シナリオ, 13 ページ

MDM Hub のセキュリティの概要

MDM Hub は、未承認のアクセスや改ざんからデータを保護し、情報のプライバシーおよびデータ整合性を保護します。

MDM Hub のリソースを保護するためには、Hub コンソールのセキュリティアクセスマネージャを使用することができます。このツールでは、ユーザーの認証および承認などのオペレーショナルセキュリティポリシーを適用することもできます。

一方、機密データへのアクセスを防止するためには、Dynamic Data Masking を使用することができます。例えば、Dynamic Data Masking を使用して、管理権のないあらゆるユーザーからクレジットカード番号を隠すことができます。

MDM Hub 実装のセキュリティは複数の方法で設定できます。組織のセキュリティの特定要素を処理するためにサードパーティのセキュリティプロバイダを使用することも、セキュリティの全要素を管理するように MDM Hub を設定することもできます。サービス統合フレームワーク（SIF）を使用したセキュリティの設定の詳細については、『*Multidomain MDM サービスの統合フレームワークガイド*』を参照してください。

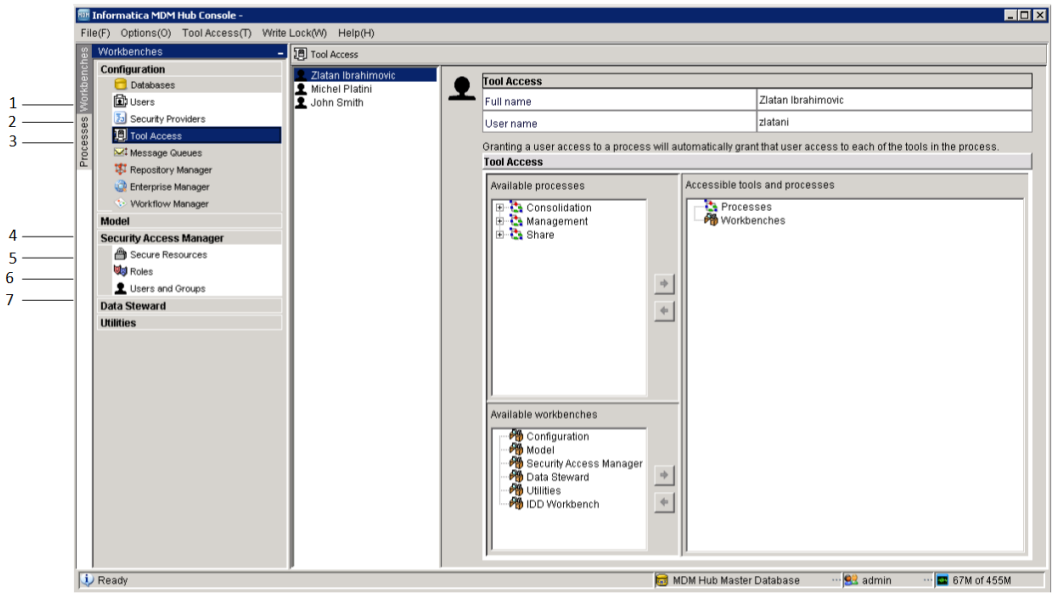
重要: Multidomain MDM の保護を開始する前に、アプリケーションサーバーおよびキャッシュデバイスが保護されていることを確認してください。

MDM Hub コンソール

Hub コンソールを使用して、MDM Hub のセキュリティを設定します。

Hub コンソールツールへのアクセス特権を制御するためには、設定ワークベンチのツールアクセスツールを使用することができます。 例えば、ツールアクセスツールを使用して、データマネージャツールとマージマネージャツールを除くすべての Hub コンソールツールへのアクセスをデータスチュワードに対して拒否することができます。

以下の図は、Hub コンソールインタフェースを示しています。



1. ユーザーツール
2. セキュリティプロバイダツール
3. ツールアクセスツール
4. セキュリティアクセスマネージャ
5. セキュアリソースツール
6. ロールツール
7. ユーザーとグループツール

Dynamic Data Masking

Informatica Dynamic Data Masking は、クライアントとデータベースの間で動作して、機密情報への不正アクセスを防止するデータセキュリティ製品です。 Dynamic Data Masking は、データベースに送信された要求をインターセプトし、その要求にデータマスキングルールを適用してから、要求に対する結果をクライアントに返送します。

Dynamic Data Masking を使用することで、MDM Hub によって管理されている運用データベースおよび非運用データベースに保存されている機密データへのアクセスをマスキング、つまり防止することができます。 データのマスキング方法を定義するには、着信要求を識別する接続ルールとセキュリティルールを設定します。 Dynamic Data Masking は、MDM Hub に着信するデータベース要求を監視し、変更したうえで、データベー

スに送信します。 データベースは変更された要求を処理し、マスキングした結果を Dynamic Data Masking に返します。 続いて、Dynamic Data Masking は結果を MDM Hub に送信します。

Dynamic Data Masking を使用して、特定タイプのデータベース要求に対してデータをマスキングしたり、組織内の特定グループに対してデータへのアクセスを制限したりすることができます。 例えば、データベース要求がサポートチームのメンバから着信した場合にクレジットカード番号にマスキング関数を適用するルールを作成することができます。 Dynamic Data Masking がデータを MDM Hub に返送すると、サポートチームのメンバにはクレジットカード番号自体でなくマスキングされた番号が表示されます。

注: MDM Hub で Dynamic Data Masking を使用するには、Dynamic Data Masking 9.6.0 と緊急バグフィックス 14590 をインストールしておく必要があります。 これより古いバージョンの Dynamic Data Masking には、MDM Hub との互換性がありません。

Dynamic Data Masking の詳細については、Dynamic Data Masking のマニュアルを参照してください。

セキュリティアクセスマネージャ

セキュリティアクセスマネージャーは MDM Hub のセキュリティモジュールです。 セキュリティアクセスマネージャーは、未承認のアクセスから MDM Hub リソースを保護します。

セキュリティアクセスマネージャーは、MDM Hub 実装において組織のセキュリティポリシーを適用します。 セキュリティアクセスマネージャーは、セキュリティ設定に従ってユーザーの認証および承認を管理します。

注: セキュリティアクセスマネージャーは、サードパーティアプリケーションからの MDM Hub リソースへのユーザーアクセスを設定するのに使用できます が、セキュリティアクセスマネージャーを使用しても、Hub コンソールツールおよびリソースのセキュリティを設定することはできません。 Hub コンソールは、別のセキュリティメカニズムを使用して、ユーザーを認証するとともに、Hub コンソールツールおよびリソースへのユーザーアクセスを承認します。

認証

認証はユーザーの ID を確認するプロセスです。

MDM Hub では、ユーザーが指定した資格情報（ユーザー名およびパスワードまたはセキュリティペイロードの RAW バイナリデータ）に基づいてユーザーが認証されます。

MDM Hub では、以下のタイプの認証が使用されます。

内部

ユーザーを MDM Hub 内で認証します。ユーザーにユーザー名とパスワードでログインさせます。

外部ディレクトリ

外部ユーザーディレクトリを使用してユーザーを認証します。LDAP 対応のディレクトリサーバー、Microsoft Active Directory、および Kerberos がネイティブでサポートされます。

外部認証プロバイダ

サードパーティの認証プロバイダを使用してユーザーを認証します。

MDM Hub 実装では、それぞれのタイプの認証を単独で使用することも、それらを組み合わせて使用することもできます。 使用する認証のタイプは、セキュリティの設定方法によって異なります。

認証

承認は、要求された MDM Hub のリソースにアクセスするために必要な特権をユーザーが持っているかどうかを決定するプロセスです。

MDM Hub では、内部承認と外部承認を使用できます。

内部

MDM Hub を使用して承認します。 MDM Hub は、ユーザーアカウントに割り当てられたロールに関連付けられた特権を調べることで、ユーザーがセキュアリソースにアクセスしてもよいかどうかを決定します。

外部

サードパーティの認証プロバイダを使用して承認します。

いずれかのタイプの承認を使用するようにも、両方のタイプを組み合わせて使用するようにも、MDM Hub を設定できます。

セキュアリソースと特権

複数の MDM Hub リソースをセキュアリソースとして設定できます。

以下のリソースが設定可能です。

- ベースオブジェクト
- マッピング
- パッケージ
- クレンジング関数
- 一致ルールセット
- メタデータ
- プロファイル
- ユーザーテーブル

MDM Hub リソースへのアクセスは、特権に応じて許可することができます。 MDM Hub では、以下の特権を割り当てることができます。

- 読み取り
- 作成
- 更新
- マージ
- 実行
- 削除

リソースは非公開またはセキュアのどちらかとして設定できます。 デフォルトではリソースはセキュアに設定されます。 MDM Hub では、セキュアリソースに対する特権のみを付与できます。

MDM Hub でセキュリティを設定する際は、次のファクトを考慮します。

- 特定のリソースがセキュアとなるように設定される。
- 特定のロールが、1 つ以上のセキュアリソースへのアクセス権を持つように設定される。

- 各セキュアリソースが、そのセキュアリソースに対するロールのアクセス権を定義する特定の特権（読み取り、書き込みなど）で設定できる。

サービス統合フレームワーク要求を実行するためには、要求に関係するリソースにアクセスするために必要な特権を持つロールをログインユーザーが持っている必要があります。

ロール

ロールは、MDM Hub のセキュアリソースにアクセスするための一連の特権を表します。 ユーザーに特権を付与するには、そのユーザーにロールを割り当てます。

ユーザーやユーザーグループにロールを割り当てるには、セキュリティアクセスマネージャーワークベンチのロールツールを使用します。 ユーザーやユーザーグループに割り当てられたロールにより、そのユーザーやユーザーグループのリソース特権が決まります。 ユーザーに直接特権を割り当てることはできません。

セキュリティアクセスマネージャーは、外部アプリケーションユーザーからの要求に対して、リソース認証を行います。 Hub コンソールを使用して MDM Hub リソースにアクセスする管理者およびデータスチュワードは、リソース特権の影響をそれほど受けません。

セキュリティの実装シナリオ

MDM Hub 実装のセキュリティは複数の方法で設定できます。

ポリシー決定ポイントは、実行時にユーザーの ID を確認する特定のセキュリティチェックポイントです。 これを認証と呼びます。 また、ポリシー決定ポイントでは、ユーザーがアクセスできる MDM Hub リソースも確認します。 これを承認と呼びます。 ポリシー決定ポイントがどの程度、MDM Hub によって内部で処理されるか、またはサードパーティのセキュリティプロバイダやその他のセキュリティサービスによって外部で処理されるかは、MDM Hub 実装によって決まります。

以下のシナリオは、MDM Hub 実装でセキュリティを設定できる高度な方法の例になっています。

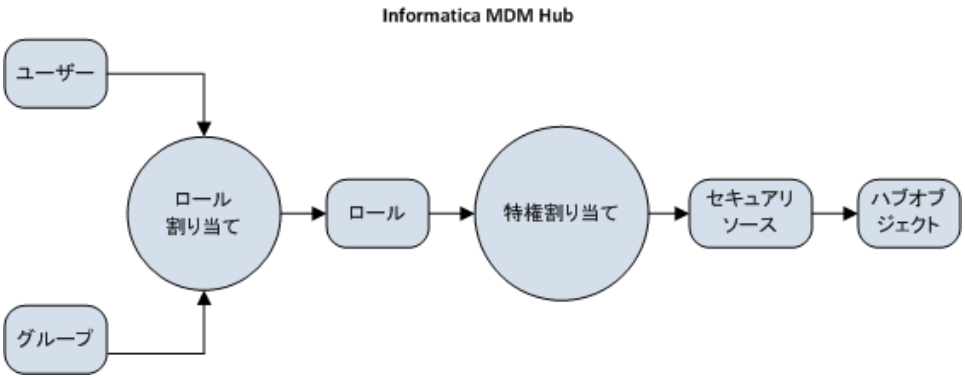
- 内部専用のポリシー決定ポイント
- 外部ユーザーディレクトリ
- ロールベースの集中管理型のポリシー決定ポイント
- 包括的な集中管理型のポリシー決定ポイント

注: 外部セキュリティプロバイダからのリソース特権への変更は、MDM Hub には反映されません。 外部セキュリティプロバイダを使用してリソース特権に変更を加える場合は、他の手段を使用して変更内容を MDM Hub と同期する必要があります。

内部ポリシー決定ポイント

MDM Hub はすべてのポリシー決定を内部処理できます。

以下の図は、すべてのポリシー決定が MDM Hub で内部処理されるセキュリティデプロイメントを示しています。



このシナリオでは、ユーザー、グループ、ロール、特権、およびリソースが Hub コンソールを使用してどのように設定されているかに基づいて、MDM Hub がすべてのポリシー決定を行います。

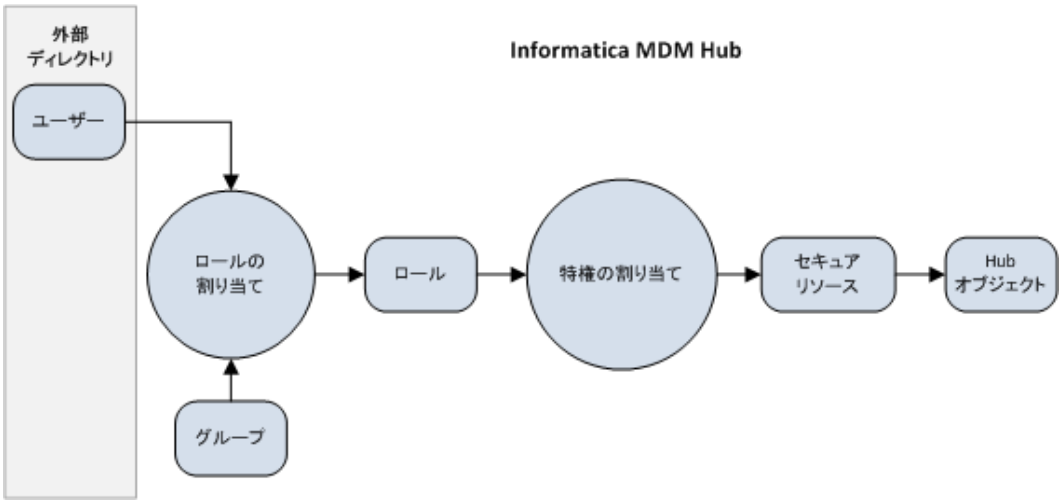
外部ユーザーディレクトリ

MDM Hub は外部ユーザーディレクトリと統合できます。

外部ユーザーディレクトリで管理されているユーザーやユーザーグループは、MDM Hub にも登録されている必要があります。 登録が必要なのは、MDM Hub がロールおよびロールに関連付けられた特権をこれらのユーザーやグループに割り当てられるようにするためです。

外部ディレクトリのユーザーを MDM Hub のグループに割り当てます。 Lightweight Directory Access Protocol を使用してリレーションを管理する場合でも、MDM Hub でユーザーとグループの間のリレーションを管理する必要があります。

次の図は、外部ディレクトリでユーザーを管理する一方で、MDM Hub でグループ、ロールの割り当て、特権の割り当てを管理するセキュリティデプロイメントを示しています。

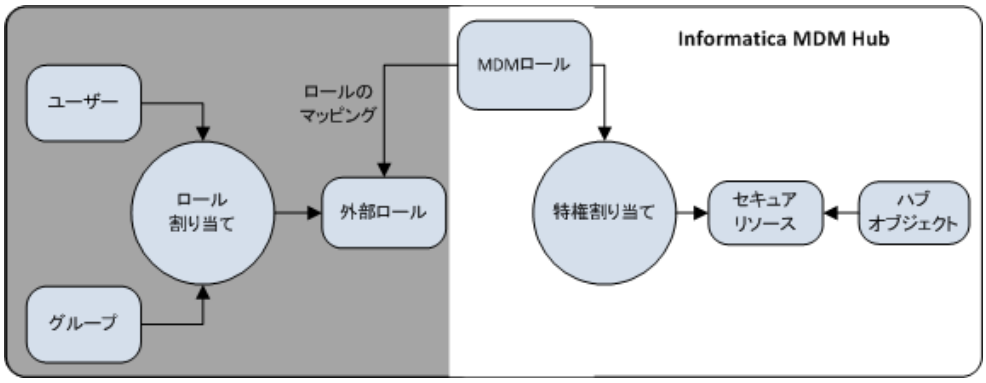


このシナリオでは、外部ユーザーディレクトリで、ユーザーアカウント、グループ、およびユーザープロファイルが管理されます。 外部ユーザーディレクトリは、ユーザーの認証を行い、グループメンバシップおよびユーザープロファイルの情報を MDM Hub に提供することができます。

ロールベースの集中管理型のポリシー決定

MDM Hub は一部のポリシー決定を内部処理するとともに、外部からのロールの割り当てを受信することができます。

以下の図は、ユーザーアカウント、グループ、およびユーザープロファイルに加えて、ロールの割り当てが MDM Hub の外部で行われる場合のセキュリティデプロイメントを示します。

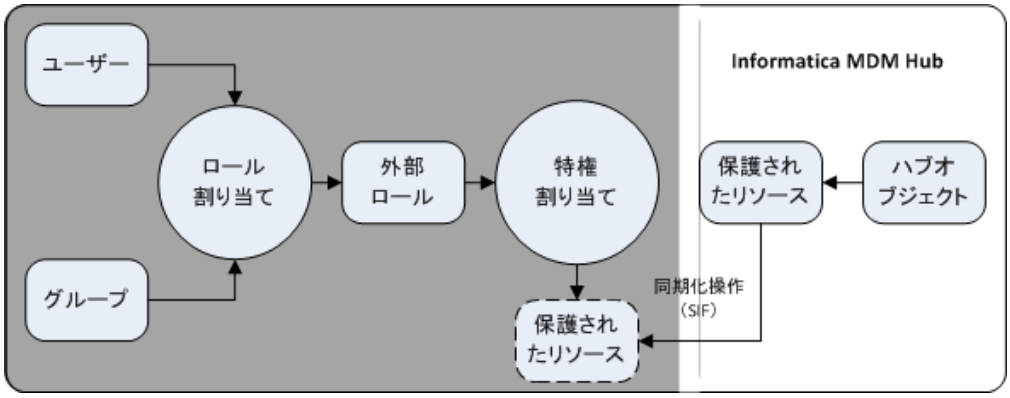


このシナリオでは、外部ロールが MDM Hub のロールに明示的にマッピングされています。

包括的な集中管理型のポリシー決定

MDM Hub は、内部的に保護されたリソースを管理できますが、外部ディレクトリから割り当てられたロールおよび特権も受け入れます。

以下の図は、ロールの定義と特権の割り当てが MDM Hub の外部で行われるセキュリティデプロイメントを示しています。 また、以下の図は、ユーザーアカウント、グループ、ユーザープロファイル、およびロールの割り当てが MDM Hub の外部で行われることを示しています。



このシナリオでは、MDM Hub 側で行うのは、保護されたリソースを外部プロキシを使用して公開することだけです。これらのリソースは、サービス統合フレームワーク要求を使用して、内部の保護されたリソースと同期されます。 ポリシー決定はすべて MDM Hub の外部で行われます。

セキュリティの設定タスクのシナリオ

次の表に、各セキュリティ実装シナリオに関連するセキュリティ設定タスクを示します。 "はい"が記入されている項目については、関連するタスクが MDM Hub の内部で実行されます。 "いいえ"が記入されている項目については、関連するタスクが MDM Hub の外部で実行されます。

サービス/タスク	内部ポリシー決定ポイント	外部ユーザーディレクトリ	ロールベースの集中管理型のポリシー決定ポイント	包括的な集中管理型のポリシー決定ポイント
MDM Hub ユーザーの設定	はい	はい	いいえ	いいえ
外部認証の使用	いいえ	はい	いいえ	いいえ
現在のオペレーショナル参照ストアデータベースへのユーザーの割り当て	はい	はい	いいえ	いいえ
グローバルパスワードポリシーの管理	はい	いいえ	いいえ	いいえ
ユーザーグループの設定	はい	はい	いいえ	いいえ
MDM Hub のセキュアリソース	はい	はい	はい	はい
MDM Hub リソースのステータスの設定	はい	はい	はい	はい
ロールの設定	はい	はい	はい	いいえ
内部ロールの外部ロールへのマッピング	いいえ	いいえ	はい	いいえ
ロールへのリソース特権の割り当て	はい	はい	はい	いいえ
セキュリティプロバイダの管理	いいえ	はい	はい	はい
ユーザーとユーザーグループへのロールの割り当て	はい	はい	いいえ	いいえ

注: MDM Hub 実装のセキュリティの一部をサードパーティのセキュリティプロバイダを使用して管理している場合は、そのセキュリティプロバイダの設定手順を参照してください。

第 2 章

リソース

この章では、以下の項目について説明します。

- リソース概要, 17 ページ
- セキュアリソースと非公開リソース , 18 ページ
- リソースグループ, 18 ページ
- セキュアリソースツール, 19 ページ
- セキュアリソースの設定, 19 ページ
- リソースグループの設定, 20 ページ
- Data Director ビジネスエンティティサービスのセキュリティの設定, 22 ページ

リソース概要

Hub コンソールでは、外部アプリケーションに対して、MDM Hub のリソースを公開したり非公開にしたりできます。

セキュアリソースは、ロールツールに公開される、保護された MDM Hub リソースです。ロールツールにより、リソースを、特定の特権を持つロールに追加できます。リソースグループは、セキュアリソースの集合で、特権の割り当てを簡単にします。セキュアリソースツールを使用して、リソースグループを定義し、リソースの階層を作成することができます。

以下の MDM Hub リソースをセキュアリソースとして設定できます。

ベースオブジェクト

ユーザーは、すべての安全なベースオブジェクト、カラム、およびコンテンツメタデータにアクセスできます。

クレンジング関数

ユーザーは、すべての安全なクレンジング関数を実行できます。

階層マネージャプロファイル

ユーザーは、すべての安全な階層マネージャプロファイルにアクセスできます。

ビジネスエンティティサービス

ユーザーはすべての安全なビジネスエンティティサービスにアクセスできます。

マッピング

ユーザーは、すべての安全なマッピングとそれらのカラムにアクセスできます。

パッケージ

ユーザーは、すべての安全なパッケージとそれらのカラムにアクセスできます。

リモートパッケージ

ユーザーは、すべての安全なリモートパッケージにアクセスできます。

バッチグループはデフォルトによりセキュアに設定されます。バッチグループのステータスをプライベートに変更することはできません。バッチグループには読み取りおよび実行の特権があります。

また、Hub コンソールでは、SIF 要求によってアクセスできるその他のリソース（メタデータ、一致ルールセット、監査テーブル、ユーザーテーブルなど）を保護できます。

注: Informatica Data Director を使用している場合、HTTP メソッドの GET または POST を使用して Hub サーバーにアクセスできます。DELETE や PUT など、他の HTTP メソッドを使用すると HTTP エラーが返されます。

セキュアリソースと非公開リソース

保護された MDM Hub リソースは、セキュアまたは非公開として設定できます。

セキュア

この MDM Hub リソースをロールツールに公開し、特定の特権を持つロールに追加することができます。ユーザーに特定のロールを割り当てると、そのユーザーは、そのロールに関連付けられている特権により、SIF 要求を使用してセキュアリソースにアクセスできるようになります。 デフォルトでは、MDM Hub により、ベースオブジェクトなどの新しいリソースがセキュアとして指定されます。

プライベート

MDM Hub リソースをロールツールに対して非公開にします。SIF 要求によるリソースへのアクセスを防止します。

MDM Hub リソースへの外部アプリケーションの SIF アクセス要求を許可する前に、リソースをセキュアにしておく必要があります。

特定の MDM Hub リソースを外部アプリケーションに非公開にする必要があるためです。 例えば、MDM Hub 実装に、SIF 要求においてではなくバッチジョブでのみ使用するマッピングまたはパッケージがある場合、これらは非公開のままにします。

注: MDM Hub では、パッケージカラムはセキュアリソースに設定されません。 パッケージカラムは、セキュアステータスおよび特権を、親のベースオブジェクトのカラムから継承します。 パッケージカラムは、システムテーブルカラムをベースにしている場合にはデフォルトでアクセス可能になっているため、パッケージカラムにセキュリティを設定する必要はありません。

リソースグループ

リソースグループは、セキュアリソースの論理的な集合です。

セキュアリソースツールを使用して、リソースグループを定義し、関連するリソースをそのグループに割り当てることができます。 リソースグループを使用すると、特権を複数のリソースに割り当て、リソースグループをロールに割り当てられるため、特権の割り当てが簡素化されます。

管理を簡素化するために、以下の種類のリソースグループの作成を検討してください。

- すべてのセキュアリソースを含んだ ALL_RESOURCES リソースグループ。最小限の特権をグローバルに設定することができます。
- リソースタイプ別のリソースグループ。この種類のリソースに対する最小限の特権を定義できるようになる。
- 機能領域別のリソースグループ。TRAINING_RESOURCES など。
- ほぼ同じ特権を持つさまざまなロールに割り当てることのできる包括的なリソースグループ。

リソースグループ階層

リソースグループには、それが属するリソースグループ以外のリソースグループを含めることもできます。 つまり、リソースグループの階層を構築し、大規模なリソース集合の管理を簡素化できるということです。

セキュアリソース

セキュアリソースのみがリソースグループに属することができます。 非公開リソースはリソースグループに属することができません。

リソースのステータスを非公開に変更すると、MDM Hub により、そのリソースが属するリソースグループから削除されます。 リソースのステータスをセキュアに設定すると、MDM Hub により、そのリソースが該当するリソースグループに追加されます。

セキュアリソースツール

Hub コンソールのセキュアリソースツールを使用して、MDM Hub リソースをきめ細かく管理します。たとえば、MDM Hub リソースのステータスをセキュアまたは非公開に設定します。 また、リソースグループはリソースの階層を設定するのにも使用できます。

セキュアリソースツールには以下のタブがあります。

リソース

個々の MDM Hub リソースのステータスをセキュアまたは非公開に設定するために使用します。 MDM Hub により、リソースはリソースのリレーションを反映した階層で表示されます。 グローバルリソースは階層のトップに表示されます。

リソースグループ

リソースグループの設定に使用します。

セキュアリソースツールでは、ロールツールや SIF の要求に対して、リソースを公開したり非公開にしたりできます。 このツールを使用する前に、オペレーショナル参照ストアに接続しておく必要があります。

セキュアリソースの設定

MDM Hub のリソースを参照および設定するには、セキュアリソースツールの［リソース］タブを使用します。

MDM Hub リソースのステータスの設定

MDM Hub リソースのリソースステータスはセキュアまたは非公開に設定することができます。

注: このステータス設定は、セキュアリソースのみを含むリソースグループや、グローバルリソースには適用されません。

1. セキュアリソースツールを起動します。
2. 書き込みロックを取得します。
3. ［リソース］タブで、リソースツリーを移動して、設定するリソースを見つけます。
4. リソース名をダブルクリックして、セキュアと非公開の間で切り替えます。 複数のリソースのステータスを同時に変更するには、手順 5 と 6 を実行します。
5. ステータスの変更が必要なリソースを選択します。 必要に応じて複数のリソースを選択できます。
6. 選択したリソースのステータスを更新します。
   - 選択したリソースのステータスをセキュアに変更する場合は、**［セキュア］**ボタンをクリックします。
   - 選択したリソースのステータスを非公開に変更する場合は、**［非公開］**ボタンをクリックします。
7. **［保存］**ボタンをクリックして変更を保存します。

リソースのフィルタリング

MDM Hub リソースの集合のステータスを簡単に変更できるようにするには、変更するリソースのみを表示するフィルタを指定します。

1. セキュアリソースツールを起動します。
2. 書き込みロックを取得します。
3. **［リソースのフィルタリング］**ボタンをクリックします。

   セキュアリソースツールにより［リソースフィルタ］ダイアログボックスが表示されます。
4. リソースタイプを選択します。
   - フィルタに含めるリソースタイプを選択する。
   - フィルタで除外するリソースタイプを選択解除する。
5. **［OK］**をクリックします。

   フィルタリングされたリソースツリーが表示されます。

リソースグループの設定

セキュアリソースツールを使用して、リソースグループを定義し、リソースの階層を作成することができます。その後、ロールツールを使用して、複数のリソースに 1 回の操作で特権を割り当てることができます。

セキュアリソースツールでは、現在のリソースグループに直接属しているリソースと間接的に属しているリソースが、視覚的に区別されます。 リソースグループに明示的に追加されたリソースは、直接的なメンバシップを持っています。 リソースグループに追加されたリソースグループに属するリソースは、間接的なメンバシップを持っています。

例えば、次の 2 つのリソースグループを作成するとします。

- リソースグループ A には、Consumer ベースオブジェクトが含まれています。つまり、Consumer ベースオブジェクトはリソースグループ A の直接メンバです。

- リソースグループ B には、Address ベースオブジェクトが含まれています。
- リソースグループ A にはリソースグループ B が含まれています。つまり、Address ベースオブジェクトはリソースグループ A の間接メンバです。

この例では、リソースグループ A を編集するときには、Address ベースオブジェクトは使用できません。Address ベースオブジェクトを編集するには、リソースグループ B を編集する必要があります。

リソースグループの追加

リソースグループをリソースリストに追加するには、セキュアリソースツールを使用します。

1. セキュアリソースツールを起動します。
2. 書き込みロックを取得します。
3. **［リソースグループ］**タブをクリックします。

   ［リソースグループ］タブが表示されます。
4. **［追加］**ボタンをクリックします。

   セキュアリソースにより［リソースグループへのリソースの追加］ダイアログボックスが表示されます。
5. リソースグループの一意のわかりやすい名前を入力します。
6. 必要に応じて、プラス記号（+）をクリックしてリソースの階層を展開します。

   リソースごとに、リソースグループにおけるメンバシップを示すチェックボックスがあります。 親を選択した場合は、子もすべて選択されます。 例えば、ツリーの［ベースオブジェクト］項目を選択すると、すべてのベースオブジェクトとその子リソースが選択されます。
7. このリソースグループに割り当てるリソースを選択します。
8. **［OK］**をクリックします。

   ［リソースグループ］ノードに新しいリソースが追加されます。

リソースグループの編集および削除

リソースグループを編集または削除するには、セキュアリソースツールを使用します。

1. セキュアリソースツールを起動します。
2. 書き込みロックを取得します。
3. **［リソースグループ］**タブをクリックします。
4. プロパティを編集または削除するリソースグループを選択します。
   - リソースグループを編集する場合は、**［編集］**ボタンをクリックします。
   - リソースグループを削除する場合は、**［削除］**ボタンをクリックします。

   セキュアリソースツールにより、［リソースグループへのリソースの割り当て］ダイアログボックスが表示されます。 または、セキュアリソースツールにより、削除したリソースが［リソースグループ］ノードから削除されます。
5. リソースグループ名を編集します。
6. プラス記号（+）をクリックしてリソースの階層を展開します。
7. **［このリソースグループに選択されているリソースのみを表示する］**チェックボックスをオンにします。
8. このリソースグループに割り当てるリソースを選択します。
9. このリソースグループから削除するリソースをオフにします。
10. **［OK］**をクリックします。

リソースリストの更新

リソースの追加後に、リソースリストの内容を更新して、リソースリストの表示も更新できます。

リソースリストを更新するには、［セキュアリソース］メニューで **［更新］** を選択します。

セキュアリソースツールによりリソースリストが更新されます。

その他のセキュリティ変更の更新

その他のすべてのセキュリティ変更に対する更新間隔を変更することもできます。

セキュリティ変更の更新レートを設定するには、cmxserver.properties ファイルで次のパラメータを設定します。

cmx.server.sam.cache.resources.refresh_interval

注: デフォルトの更新間隔は、1 クロックティックで 60,000 ミリ秒のレートで、5 クロックティック、すなわち 5 分です。

Data Director ビジネスエンティティサービスのセキュリティの設定

ビジネスエンティティサービスは保護されたリソースであり、特権を持つユーザーロールのみが Data Director のビジネスエンティティサービスにアクセスできます。

MDM Hub コンソールで次のビジネスエンティティサービスリソースを設定できます。

- 検索-置換
- ファイルのインポート
- アドホック照合

セキュアリソースツールを使用して、ビジネスエンティティサービスをセキュアリソースとして設定する必要があります。次に、ロールツールを使用して、ユーザーロールに特権を割り当てます。

セキュアリソースとしてのビジネスエンティティサービスの設定

セキュリティアクセスマネージャワークベンチのセキュアリソースツールを使用して、必要なリソースをセキュアリソースとして設定します。

1. セキュアリソースツールを起動します。
2. 書き込みロックを取得します。
3. **［リソース］** タブをクリックします。
4. リソースツリーに移動し、**［ビジネスエンティティサービス］** を展開します。
5. リソース名をダブルクリックして、セキュアと非公開の間で切り替えます。
   a. 選択したリソースのステータスをセキュアに変更する場合は、**［セキュア］** ボタンをクリックします。
   b. 選択したリソースのステータスを非公開に変更する場合は、**［非公開］** ボタンをクリックします。
6. **［保存］** をクリックします。

ビジネスエンティティサービスへのロール特権の割り当て

セキュリティアクセスマネージャワークベンチのロールツールを使用して、ビジネスエンティティサービス特権をユーザーロールに割り当てます。

1. ロールツールを起動します。
2. 書き込みロックを取得します。
3. ロールのリストをスクロールして、必要なロールを選択します。
4. **［リソース特権］**タブをクリックします。
5. リソースツリーに移動し、**［ビジネスエンティティサービス］**を展開します。
6. 各ビジネスエンティティサービスリソースの**［実行］**特権を選択します。
7. **［保存］**をクリックします。

第 3 章

ロール

この章では、以下の項目について説明します。

- ロールの概要, 24 ページ
- ロールの設定, 24 ページ
- 特権, 25 ページ
- 内部ロールと外部ロール, 26 ページ

ロールの概要

ロールとは、ユーザーまたはグループに割り当てる特権の集合です。ロールは、MDM Hub のセキュアリソースにアクセスするための一連の特権を表します。

ユーザーが MDM Hub のセキュアリソースを表示したり操作したりするには、そのリソースにアクセスするために必要な特権を付与するロールが割り当てられていなければなりません。 ユーザーが MDM Hub でアクセスできるオブジェクトと実行できるタスクは、ロールによって決まります。

MDM Hub のロールは、非常に細かく柔軟に設定できるため、管理者は組織のセキュリティポリシーに従って複合的なセキュリティ対策を実装することができます。 管理者など一部のユーザーには、すべてのオブジェクトへのアクセス権を付与した単一のロールを割り当てることもできます。 データスチュワードなど他のユーザーには、明示的に制限した特権を付与したロールを割り当てることができます。

また、ロールに他のロールを割り当てて、後者のロールに設定されているアクセス特権を継承することもできます。特権は追加される仕組みになっているので、ロールを組み合わせれば、そのロールの特権も組み合わされます。 例えば、ロール A に Address ベースオブジェクトに対する読み取り特権があり、ロール B にそのオブジェクトに対する作成特権と更新特権があるとします。 ユーザーカウントにロール A とロール B を割り当てると、そのユーザーアカウントは、Address ベースオブジェクトに対する読み取り、作成、および更新の特権を持つことになります。 ユーザーアカウントは、割り当てられたすべてのロールに設定されている特権を継承します。

ロールの設定

MDM Hub では、ロールの作成、編集、および削除を行うことができます。

注: ユーザーが外部で承認される、包括的な集中管理型のセキュリティデプロイメントを使用する場合には、ロールを設定する必要はありません。

リソース特権は、ユーザーがジョブを実行するために必要なアクセスの範囲によって異なります。 管理者にとってのベストプラクティスは、特権を最小限にする原則に従うことです。 作業を実行するのに必要最小限度の特権をユーザーに割り当てます。

ロールの追加

ロールを設定し、MDM Hub のリソースへのアクセス特権を割り当てるには、セキュリティアクセスマネージャワークベンチのロールツールを使用します。

ヒント: ロール名にスペースを使用しないでください。スペースは、MDM Hub が ActiveVOS と通信するときにエラーを引き起こす可能性があります。

1. ロールツールを起動します。
2. 書き込みロックを取得します。
3. ナビゲーションペインの任意の場所をポイントして右クリックし、**[ロールの追加]** を選択します。

   ロールツールにより［ロールの追加］ダイアログが表示されます。
4. ロールの名前を入力します。
5. ロールの説明（オプション）を入力します。
6. ロールの外部名またはエイリアスを入力します。
7. **[OK]** をクリックします。

   ロールリストに新しいロールが表示されます。

ロールの編集および削除

既存のロールを編集または削除するには、セキュリティアクセスマネージャワークベンチのロールツールを使用します。

1. ロールツールを起動します。
2. 書き込みロックを取得します。
3. ロールリストをスクロールし、編集するロールを選択します。
   - 編集するプロパティごとに、その横にある **[編集]** ボタンをクリックし、新しい値を指定します。
   - ナビゲーションペインの任意の場所をポイントして右クリックし、**[ロールの削除]** を選択して、確認を求められたら、**[はい]**をクリックします。
4. **[保存]** ボタンをクリックして変更を保存します。

特権

MDM Hub 内部承認を使用して、ロールに特権を割り当てることができます。

ロールには以下の特権を割り当てることができます。

読み取り

ユーザーはデータを表示することはできますが、データを変更することはできません。

作成

ユーザーは、Hub ストア内にデータレコードを作成できます。

更新

ユーザーは、Hub ストア内のデータレコードを更新できます。

削除

ユーザーは、Hub ストアからデータレコードを削除できます。

マージ

ユーザーは、データのマージとアンマージを行うことができます。

実行

ユーザーは、クレンジング関数とバッチグループを実行できます。

外部アプリケーションユーザーが MDM Hub リソースに対して持つアクセス権は、特権によって決まります。例えば、特定のパッケージに対する読み取り、作成、更新、およびマージ特権を持つロールを設定することができます。

注: 各特権は個別に存在するものであり、それぞれ明示的に割り当てる必要があります。 特権は他の特権を集約しません。 例えば、リソースへの更新アクセス権があるからといって、読み取りアクセス権もあるわけではありません。 いずれの特権も個別に割り当てる必要があります。

Hub コンソールを使用する場合、特権は適用されません。それでも、設定は Hub コンソールの使用に影響します。 例えば、データスチュワードは、読み取り特権を持つパッケージのみをマージマネージャおよびデータマネージャで表示できます。 データスチュワードが特定パッケージのデータを編集して変更を保存するには、そのパッケージの更新特権と作成特権が必要です。

更新特権と作成特権がない場合は、データマネージャでデータを変更できません。 同様に、マージマネージャを使用してレコードをマージまたはアンマージするには、マージ特権が必要です。 マージマネージャツールおよびデータマネージャツールの詳細については、『*Multidomain MDM のデータスチュワードガイド*』を参照してください。

内部ロールと外部ロール

ロールベースの集中型セキュリティ実装では、MDM Hub の内部ロールと、MDM Hub と切り離して管理されている外部ロールの間のマッピングを作成する必要があります。

外部ロール名は、MDM Hub 環境で使用されている内部ロール名とは異なっている場合もあります。

設定の詳細は、セキュリティプロバイダのロールマッピングの実装によって異なります。 ロールのマップ作成は設定ファイルで行います。 1 つの外部ロールを複数の内部ロールにマップすることができます。

注: マッピングは通常 XML 内に作成されますが、定義済みの設定ファイルフォーマットはありません。 XML ファイルでなくてもかまいません。また、ファイルである必要もありません。 マッピングはカスタムユーザープロファイルまたは認証プロバイダ実装の一部です。 マッピングの目的は、ユーザープロファイルのオブジェクトロールリストに内部ロール ID を取り込むことです。

ロールへのリソース特権の割り当て

リソース特権のロールへの割り当てと編集を行うには、セキュリティアクセスマネージャワークベンチのロールツールを使用します。

1. ロールツールを起動します。
2. 書き込みロックを取得します。
3. ロールのリストをスクロールして、リソース特権を割り当てるロールを選択します。

4. **［リソース特権］**タブをクリックします。
5. リソースの階層を展開して、このロールに対して設定するセキュアリソースを表示します。
6. 設定する各リソースについて、次の操作を行います。
   - このロールに付与する特権を選択する。
   - このロールから削除する特権を選択解除する。
7. **［保存］**ボタンをクリックして変更を保存します。

他のロールへのロールの割り当て

ロールは、自らが属するロール以外のロールを継承することもできます。 例えば、ロール B をロール A に割り当てると、ロール A はロール B のアクセス特権を継承します。

1. ロールツールを起動します。
2. 書き込みロックを取得します。
3. ロールのリストをスクロールして、他のロールを割り当てるロールを選択します。
4. **［ロール］**タブをクリックします。

   ロールツールにより、選択したロールに割り当てることができるロールが表示されます。
5. 選択したロールに割り当てるロールを選択します。
6. このロールから削除するロールを選択解除します。
7. **［保存］**ボタンをクリックして変更を保存します。

ロールのリソース特権レポートの生成

特定のロールに付与されたリソース特権を示すレポートを生成することができます。

1. ロールツールを起動します。
2. 書き込みロックを取得します。
3. ロールのリストをスクロールして、レポートを生成するロールを選択します。
4. **［レポート］**タブをクリックします。
5. **［生成］**をクリックします。

   ロールツールによってレポートが生成され、［レポート］タブに表示されます。

生成されたレポートの HTML ファイルとしての保存

1. **［保存］**をクリックします。

   レポートの保存場所を指定するように求められます。
2. 保存場所に移動します。
3. **［保存］**をクリックします。

   セキュリティアクセスマネージャにより、以下の命名規則に従ったレポートが保存されます。

   <*ORS_Name*>-<*Role_Name*>-RolePrivilegeReport.html

   ここで、
   - *ORS_Name* はターゲットデータベースの名前である。
   - *Role_Name* は、生成されるレポートに関連付けられるロールである。

現在のレポートが HTML ファイルとして保存場所に保存されます。 このレポートは、後でブラウザを使用して表示できます。

第 4 章

ユーザーとユーザーグループ

この章では、以下の項目について説明します。

- ユーザーおよびユーザーグループの概要, 29 ページ
- ユーザー設定, 29 ページ
- パスワードポリシー設定, 32 ページ
- JDBC データソースのセキュリティ設定, 34 ページ
- ユーザーグループ設定, 36 ページ
- ロールとユーザーおよびユーザーグループの間の関連付け, 38 ページ

ユーザーおよびユーザーグループの概要

MDM Hub ユーザーとは、MDM Hub リソースにアクセスできる個人のことです。

ユーザーアカウントは、Hub ストアのマスターデータベースに定義されます。 MDM Hub ユーザーの概要については、『*Multidomain MDM の概要ガイド*』を参照してください。

ユーザーアカウントは、割り当てられているロールを使用し、ロールごとに設定されている特権を継承して、MDM Hub リソースにアクセスします。

設定ワークベンチのユーザーツールを使用して、MDM Hub ユーザーのユーザーアカウントを設定したり、パスワードの変更や外部認証の有効化を行ったりすることができます。 また、外部アプリケーションであっても、SIF 要求を使用してユーザーアカウントを登録できるだけの承認が付与されていれば、そのようにすることができます（『*Multidomain MDM サービスの統合フレームワークガイド*』を参照）。

ユーザー設定

MDM Hub では、ユーザーの作成、編集、削除を行うことができます。

セキュリティのデプロイ方法に応じて、MDM Hub の実装でマスターデータベースにユーザーを追加する必要があるかどうかが決まります。

以下のシナリオでは、マスターデータベースにユーザーを設定する必要があります。

- MDM Hub の内部承認を使用する。
- MDM Hub の外部承認を使用する。
- 複数のユーザーがさまざまなアカウントを使用して Hub コンソールにアクセスする。

1 人のユーザーは、マスターデータベースに関連付けられている複数のオペレーショナル参照ストアにアクセスする場合でも、一度しか定義してはなりません。

MDM Hub のリソースへのユーザーアクセス

管理者およびデータスチュワードを含むユーザーは、次の方法で MDM Hub リソースにアクセスできます。

MDM **アプリケーション**

Hub コンソールにログインし、アクセス権を持つツールを使用して MDM Hub と対話できます。 ユーザーは、IDD またはプロビジョニングツールを使用して、ベースオブジェクトおよびビジネスエンティティのデータにアクセスすることもできます。

サードパーティアプリケーション

SIF クラスを使用するサードパーティアプリケーションを使用して間接的に MDM Hub データを操作することができます。 このユーザーは Hub コンソールにログインしません。 代わりに、SIF クラスを呼び出すことができるアプリケーションから MDM Hub にログインします。 このようなユーザーは外部アプリケーションユーザーと呼ばれます。 開発者が呼び出すことのできる SIF 要求の種類については、『*Multidomain MDM サービスの統合フレームワークガイド*』を参照してください。

ユーザーアカウントの追加

ユーザーアカウントを MDM Hub に追加するには、セキュリティアクセスマネージャワークベンチのユーザーツールを使用します。

1. ユーザーツールを起動します。
2. 書き込みロックを取得します。
3. **[ユーザー]** タブをクリックします。
4. **[ユーザーの追加]** ボタンをクリックします。

   ユーザーツールにより、**[ユーザーの追加]** ダイアログボックスが表示されます。
5. ユーザーの名（ファーストネーム）、ミドルネーム、および姓を入力します。
6. ユーザーのユーザー名を入力します。

   注: ユーザー名では、大文字と小文字は区別されず、小文字で保存されます。
7. ユーザーの有効な電子メールアドレスを入力します。この電子メールアドレスに、MDM Hub から、このユーザーアカウントのパスワードが送信されます。
8. ユーザーのデフォルトのデータベースを入力します。これは、ユーザーが Hub コンソールにログインするときにデフォルトで選択されるデータベースです。
9. ユーザーアカウントがアプリケーション用である場合、**[アプリケーションユーザー]** チェックボックスを選択します。

   注: アプリケーションユーザーは、ユーザーに代わって信頼されたアプリケーションで生成された要求の、証明書ベースの認証に使用されます。
10. ユーザーのパスワードを入力および再入力します。
11. 認証のタイプを選択します。
    - MDM Hub の実装でサードパーティのセキュリティプロバイダを介した認証を使用する場合は、**[外部認証の使用]** チェックボックスをオンにする。
    - MDM Hub で内部認証を使用する場合は、**[外部認証の使用]** チェックボックスをオフにする。
12. ユーザーの公開証明書を参照します。MDM Hub は、この証明書をユーザー要求の認証に使用できます。

    注: ユーザーアカウントがアプリケーションユーザー用である場合、証明書を選択する必要があります。

13. **[OK]** をクリックします。

    [ユーザー] タブのユーザーのリストに新しいユーザーが追加されます。

ユーザーアカウントの編集および削除

ユーザーアカウントを編集したり削除したりするには、セキュリティアクセスマネージャワークベンチのユーザーツールを使用します。

1. ユーザーツールを起動します。
2. 書き込みロックを取得します。
3. **[ユーザー]** タブをクリックします。
4. ユーザーを削除する場合は、削除するユーザーアカウントを選択します。
5. **[削除]** ボタンをクリックします。

   ユーザーツールにより、削除を確認するように求められます。
6. **[はい]** をクリックして削除を確定します。

   ユーザーツールにより、削除したユーザーアカウントがユーザーリストから削除されます。
7. ユーザーを編集する場合は、設定するユーザーアカウントを選択します。
8. 名前を変更するには、セルをダブルクリックし、別の名前を入力します。
9. 必要に応じて、別のログインデータベースおよびサーバーを選択します。
10. このユーザーに管理用のアクセス権を付与してすべての Hub コンソールツールとデータベースにアクセスできるようにするには、**[管理者]** チェックボックスをオンにします。
11. このユーザーアカウントを有効にして、このユーザーにログインを許可する場合は、**[有効化]** チェックボックスをオンにします。

    注: ユーザーに外部認証を使用する場合、Hub コンソールを使用してユーザーアカウントを無効にすることはできません。
12. **[保存]** ボタンをクリックします。

    ユーザーツールにより、ユーザーアカウントへの変更が保存されます。

ユーザーの補足情報の編集

MDM Hub を使用して各ユーザーの補足情報（電子メールアドレスや電話番号など）を管理できます。 ユーザーが MDM Hub にこの情報を提供する必要はありません。また、この情報が MDM Hub によって特別な方法で使用されることもありません。

注: Hub コンソールの管理者ユーザーの電子メールアドレスは変更できません。管理者ユーザーの電子メールアドレスを変更するには、CMX_SYSTEM スキーマの C_REPOS_USER テーブルを

1. ユーザーツールを起動します。
2. 書き込みロックを取得します。
3. **[ユーザー]** タブをクリックします。
4. プロパティを編集するユーザーを選択します。
5. **[編集]** ボタンをクリックします。

   ユーザーツールにより、**[ユーザーの編集]** ダイアログボックスが表示されます。
6. 役職や電子メールアドレス、ログインメッセージなど、ユーザーのプロパティを指定します。 ログインメッセージは、このユーザーがログインした後に Hub コンソールに表示されるメッセージです。
7. **[OK]** をクリックします。

8. **[保存]** ボタンをクリックして変更を保存します。

ユーザーアカウントのパスワード設定の変更

ユーザーのパスワード設定を変更することができます。

1. ユーザーツールを起動します。
2. 書き込みロックを取得します。
3. **[ユーザー]** タブをクリックします。
4. パスワードを変更するユーザーを選択します。
5. **[パスワードの変更]** ボタンをクリックします。

   ユーザーツールにより、選択したユーザーの **[パスワードの変更]** ダイアログボックスが表示されます。
6. 新しいパスワードを指定および再入力します。
7. 認証のタイプを選択します。
   - MDM Hub の実装でサードパーティのセキュリティプロバイダを介した認証を使用する場合は、**[外部認証の使用]** チェックボックスをオンにする。
   - MDM Hub で内部認証を使用する場合は、**[外部認証の使用]** チェックボックスをオフにする。
8. **[OK]** をクリックします。

オペレーショナルリファレンスストアへのユーザーアクセスの設定

オペレーショナル参照ストアデータベースに対するユーザーアクセスを設定することができます。

1. ユーザーツールを起動します。
2. 書き込みロックを取得します。
3. **[ターゲットデータベース]** タブをクリックします。

   [ターゲットデータベース] タブが表示されます。
4. 各データベースのノードを展開して、そのデータベースにアクセスできるユーザーを確認します。
5. データベースへのユーザーの割り当てを変更するには、データベース名を右クリックし、**[ユーザーの割り当て]** を選択します。

   ユーザーツールにより、**[データベースへのユーザーの割り当て]** ダイアログボックスが表示されます。
6. 選択したデータベースに割り当てるユーザーの名前を選択します。
7. 選択したデータベースへの割り当てを解除するユーザーの名前を選択解除します。
8. **[OK]** をクリックします。

パスワードポリシー設定

すべてのユーザーに対するグローバルパスワードポリシーを定義することができます。個別ユーザーには、グローバルパスワードポリシーをオーバーライドするプライベートパスワードポリシーを設定します。すべてのパスワードでは、大文字と小文字を区別します。

注: セキュリティが有効な JBoss アプリケーションサーバーで MDM Hub をデプロイする場合は、設定するパスワードが JBoss パスワードポリシーに従っていることを確認します。 また、パスワードは MDM Hub グロー

バルパスワードポリシーに従っている必要もあります。 これは重要です。Hub コンソールのパスワードが JBoss のパスワードと一致している必要があるためです。

パスワードポリシー設定

MDM Hub ユーザーに対するパスワードポリシー設定を指定することができます。

MDM Hub では、ユーザーに対して以下のプライベートパスワードポリシーを設定できます。

パスワードの長さ

パスワードの最小長と最大長（単位: 文字）

パスワードの有効期限

パスワードが期限切れになるかどうか、およびパスワードが有効な日数を指定します。

［パスワードの有効期限］チェックボックスをオンにして、パスワードに有効期限を設定します。 **［パスワードの有効期限］**チェックボックスをオフにして、期限切れしないパスワードを設定します。

［パスワードの有効期限］チェックボックスをオンにして、パスワードの期限が切れるまでの日数を指定します。 設定できるパスワード有効期限までの最小期間は、10 です。

ログイン設定

猶予ログインの回数、およびログインで許可される上限の失敗回数。

パスワード履歴

パスワードを再利用できる回数。

パスワードの要件

［パスワードパターンの検証の有効化］チェックボックスをオンにして、パスワードパターンを適用します。パスワードパターンには、次の条件を指定できます。

- 最低限必要な一意の文字数
- パスワードは次で始まっている必要があります:
- パスワードには次を含める必要があります:
- パスワードは次で終わっている必要があります:

グローバルパスワードポリシーの管理

グローバルパスワードポリシーは、プライベートパスワードポリシーが指定されていないユーザーに適用されます。

1. **［ユーザー］**ツールを起動します。
2. 書き込みロックを取得します。
3. **［グローバルパスワードポリシー］**タブをクリックします。

   ［グローバルパスワードポリシー］ウィンドウが表示されます。
4. パスワードポリシーの設定を指定します。
5. **［OK］**をクリックします。
6. **［保存］**ボタンをクリックして、グローバル設定を保存します。

プライベートパスワードポリシーの管理

すべてのユーザーが対象のグローバルパスワードポリシーよりも優先されるプライベートパスワードポリシーを指定することができます。

注: パスワードポリシー管理のベストプラクティスは、ユーザーパスワードの大部分を多数のプライベートポリシーによってでなくグローバルポリシーによって管理するようにすることです。

1. ユーザーツールを起動します。
2. 書き込みロックを取得します。
3. **[ユーザー]** タブをクリックします。
4. プライベートパスワードポリシーの設定対象にするユーザーを選択します。
5. **[パスワードポリシーの管理]** ボタンをクリックします。

   選択されたユーザーに関する **[プライベートパスワードポリシー]** ウィンドウが表示されます。
6. **[プライベートパスワードポリシーを有効にする]** オプションを有効にします。
7. そのユーザーに対してパスワードポリシーの設定を指定します。
8. **[OK]** をクリックします。
9. **[保存]** ボタンをクリックして変更を保存します。

JDBC データソースのセキュリティ設定

MDM Hub の実装では、JDBC データソースでアプリケーションサーバーのセキュリティが使用される場合には、cmxserver.properties ファイルの設定を行う必要があります。

JDBC データソースに対するアプリケーションサーバーのユーザー名およびパスワードを cmxserver.properties ファイルに保存する必要があります。 パスワードをクリアテキストとして表示することはできません。 パスワードは cmxserver.properties ファイルに保存する前に暗号化しておく必要があります。

保護された JDBC データソースの詳細については、アプリケーションサーバーのドキュメントを参照してください。

保護された JDBC データソースのユーザー名とパスワード

保護された JDBC データソースに対するユーザー名とパスワードを設定するには、cmxserver.properties ファイルで以下のパラメータを使用します。

```
databaseId.username=username
databaseId.password=encryptedPassword
```

databaseId は、JDBC データソースの一意の識別子です。

Oracle SID 接続タイプのデータベース ID

Oracle SID 接続タイプの場合、データベース ID は以下の文字列で構成されます。

<database hostname: データベースホスト名>-<Oracle SID>-<schema name: スキーマ名>

例えば、以下の設定があるとします。

- <database hostname: データベースホスト名> = localhost

- <Oracle SID> = MDMHUB
- <schema name: スキーマ名> = Test_ORS

ユーザー名プロパティとパスワードプロパティは以下のようになります。

```
localhost-MDMHUB-Test_ORS.username=weblogic
localhost-MDMHUB-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Oracle サービス接続タイプのデータベース ID

Oracle サービス接続タイプの場合、データベース ID は以下の文字列で構成されます。

<service name: サービス名>-<schema name: スキーマ名>

例えば、以下の設定があるとします。

- <service name: サービス名> = MDM_Service
- <schema name: スキーマ名> = Test_ORS

ユーザー名プロパティとパスワードプロパティは以下のようになります。

```
MDM_Service-Test_ORS.username=weblogic
MDM_Service-Test_ORS.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

IBM DB2 接続タイプのデータベース ID

IBM DB2 接続タイプの場合、データベース ID は次の文字列で構成されています。

<database hostname: データベースホスト名>-<database name: データベース名>-<schema name: スキーマ名>

例えば、以下の設定があるとします。

- <database hostname: データベースホスト名> = localhost
- <database name: データベース名> = dsui2
- <schema name: スキーマ名> = DS_UI2

ユーザー名プロパティとパスワードプロパティは以下のようになります。

```
localhost-dsui2-DS_UI2.username=weblogic
localhost-dsui2-DS_UI2.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

Microsoft SQL Server 接続タイプのデータベース ID

Microsoft SQL Server 接続タイプの場合、データベース ID は次の文字列で構成されます。

<database hostname: データベースホスト名>-<database name: データベース名>

例えば、以下の設定があるとします。

- <database hostname: データベースホスト名> = localhost
- <database name: データベース名> = ds_ui1

ユーザー名プロパティとパスワードプロパティは以下のようになります。

```
localhost-ds_ui1.username=weblogic
localhost-ds_ui1.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

マスターデータベースのデータベース ID

マスターデータベースにアクセスする JDBC データソースをセキュリティで保護する場合は、databaseId が CMX_SYSTEM となります。 この場合、プロパティは以下のようになります。

```
CMX_SYSTEM.username=weblogic
CMX_SYSTEM.password=9C03B113CD8E4BBFD236C56D5FEA56EB
```

パスワードの暗号化

データベーススキーマの暗号化パスワード生成するには、次のコマンドを使用します。

```
C:\>java -cp siperian-common.jar com.siperian.common.security.Blowfish password
Plaintext Password: password
Encrypted Password: 9C03B113CD8E4BBFD236C56D5FEA56EB
```

ユーザーグループ設定

ユーザーグループは、ユーザーアカウントの論理的な集まりです。

ユーザーグループを使用すると、セキュリティの管理が簡単になります。 例えば、外部アプリケーションユーザーを 1 つのユーザーグループにまとめれば、ユーザーごとではなくユーザーグループ単位でセキュリティロールを付与することができます。 ユーザーグループには、ユーザーだけでなく、他のユーザーグループを含めることもできます。

ユーザーグループを設定するには、セキュリティアクセスマネージャワークベンチのユーザーとグループツールにある［グループ］タブを使用します。

ユーザーとグループツールの起動

Hub コンソールでユーザーとグループツールを開始します。

1. Hub コンソールでオペレーショナル参照ストアに接続します（接続していない場合）。
2. Security Access Manager ワークベンチを展開し、**［ユーザーとグループ］**をクリックします。

   Hub コンソールにユーザーとグループツールが表示されます。

   ユーザーとグループツールには以下のタブが含まれます。

   グループ

   ユーザーグループの定義およびユーザーグループへのユーザーの割り当てに使用します。

   データベースに割り当てられているユーザー

   ユーザーアカウントとデータベースの関連付けに使用します。

   ロールへのユーザー/グループの割り当て

   ユーザーおよびユーザーグループにロールを関連付けるために使用します。

   ユーザー/グループへのロールの割り当て

   ロールをユーザーおよびユーザーグループに関連付けるために使用します。

ユーザーグループの追加

ユーザーグループを追加するには、セキュリティアクセスマネージャワークベンチのユーザーとグループツールを使用します。

1. ユーザーとグループツールを起動します。
2. 書き込みロックを取得します。
3. **[グループ]** タブをクリックします。
4. **[追加]** ボタンをクリックします。

   ユーザーとグループツールにより、**[ユーザーグループの追加]** ダイアログが表示されます。
5. ユーザーグループのわかりやすい名前を入力します。
6. 必要に応じて、ユーザーグループの説明を入力します。
7. **[OK]** をクリックします。

   リストに新しいユーザーグループが追加されます。

ユーザーグループの編集および削除

ユーザーとグループツールを使用して、ユーザーグループを編集したり削除したりすることもできます。

1. ユーザーとグループツールを起動します。
2. 書き込みロックを取得します。
3. **[グループ]** タブをクリックします。
4. ユーザーグループのリストをスクロールし、編集するユーザーグループを選択します。
5. ユーザーグループを削除する場合は、**[削除]** ボタンをクリックします。

   ユーザーとグループツールから、削除を確認するように求められます。
6. **[はい]** をクリックします。

   ユーザーとグループツールにより、削除したユーザーグループがリストから削除されます。
7. ユーザーグループを編集する場合は、編集する各プロパティの横にある **[編集]** ボタンをクリックし、新しい値を指定します。
8. **[保存]** ボタンをクリックして変更を保存します。

ユーザーグループへのユーザーとユーザーグループの割り当て

ユーザーグループにメンバを割り当てる手順

1. ユーザーとグループツールを起動します。
2. 書き込みロックを取得します。
3. **[グループ]** タブをクリックします。
4. ユーザーグループのリストをスクロールし、編集するユーザーグループを選択します。
5. 作成したユーザーグループを右クリックし、**[ユーザーおよびグループの割り当て]** を選択します。

   ユーザーとグループツールにより、**[ユーザーグループへの割り当て]** ダイアログボックスが表示されます。
6. 選択したユーザーグループに割り当てるユーザーおよびユーザーグループの名前を選択します。
7. 選択したユーザーグループへの割り当てを解除するユーザーおよびユーザーグループの名前を選択解除します。
8. **[OK]** をクリックします。

現在の ORS データベースへのユーザーの割り当て

現在のオペレーショナル参照ストアデータベースにユーザーを割り当てる手順

1. ユーザーとグループツールを起動します。
2. 書き込みロックを取得します。
3. **[データベースに割り当てられているユーザー]** タブをクリックします。
4. **[データベースへのユーザーの割り当て]** ボタンをクリックして、オペレーショナル参照ストアデータベースにユーザーを割り当てます。

   ユーザーとグループツールにより、**[データベースへのユーザーの割り当て]** ダイアログボックスが表示されます。
5. 選択したオペレーショナル参照ストアデータベースに割り当てるユーザーの名前を選択します。
6. 選択したオペレーショナル参照ストアデータベースへの割り当てを解除するユーザーの名前を選択解除します。
7. **[OK]** をクリックします。

ロールとユーザーおよびユーザーグループの間の関連付け

ロールをユーザーおよびユーザーグループに関連付けることができます。**ユーザーとグループ**ツールを使用し、以下の方法でロールをユーザーに関連付けることができます。

- ロールにユーザーとユーザーグループを割り当てます。
- ユーザーとユーザーグループにロールを割り当てます。

実装に最適な方法を選択します。

ロールへのユーザーとユーザーグループの割り当て

ロールにユーザーとユーザーグループを割り当てる手順

1. ユーザーとグループツールを起動します。
2. 書き込みロックを取得します。
3. **[ロールへのユーザー/グループの割り当て]** タブをクリックします。
4. ユーザーとユーザーグループを割り当てるロールを選択します。
5. **[編集]** ボタンをクリックします。

   ユーザーとグループツールにより、**[ロールへのユーザーの割り当て]** ダイアログボックスが表示されます。
6. 選択したロールに割り当てるユーザーおよびユーザーグループの名前を選択します。
7. 選択したロールへの割り当てを解除するユーザーおよびユーザーグループの名前を選択解除します。
8. **[OK]** をクリックします。

ユーザーとユーザーグループへのロールの割り当て

ユーザーとユーザーグループにロールを割り当てる手順

1. ユーザーとグループツールを起動します。
2. 書き込みロックを取得します。
3. **［ユーザー/グループへのロールの割り当て］**タブをクリックします。
4. ロールを割り当てるユーザーまたはユーザーグループを選択します。
5. **［編集］**ボタンをクリックします。

   ユーザーとグループツールにより、**［ユーザーへのロールの割り当て］**ダイアログボックスが表示されます。
6. 選択したユーザーまたはユーザーグループに割り当てるロールを選択します。
7. 選択したユーザーまたはユーザーグループへの割り当てを解除するロールを選択解除します。
8. **［OK］**をクリックします。

第 5 章

セキュリティプロバイダ

この章では、以下の項目について説明します。

- セキュリティプロバイダの概要, 40 ページ
- セキュリティプロバイダ管理, 40 ページ
- プロバイダファイル管理, 41 ページ
- セキュリティプロバイダの設定, 42 ページ
- プロバイダのプロパティ, 43 ページ
- カスタムプロバイダ, 44 ページ
- 外部認証, 46 ページ

セキュリティプロバイダの概要

セキュリティプロバイダは、MDM Hub にアクセスするユーザーに認証や承認などのセキュリティサービスを提供するサードパーティ製アプリケーションです。 セキュリティプロバイダは、MDM Hub のセキュリティデプロイメントシナリオの一部で使用されています。

プロバイダファイルには、セキュリティプロバイダのプロファイル情報が格納されています。 サードパーティのセキュリティプロバイダを使用するには、セキュリティプロバイダツールを使用してプロバイダファイルを MDM Hub にアップロードします。 また、プロバイダリスト内のセキュリティプロバイダを変更、削除、有効化、無効化するのにも、セキュリティプロバイダを使用することができます。

MDM Hub には、デフォルトの内部セキュリティプロバイダのセットが付属しています。 サードパーティのセキュリティプロバイダを追加することもできます。 内部セキュリティプロバイダは削除できません。

セキュリティプロバイダ管理

MDM Hub 実装のセキュリティプロバイダを管理するには、Hub コンソールの設定ワークベンチのセキュリティプロバイダツールを使用します。

セキュリティプロバイダの追加は、MDM Hub 内のデフォルトの選択肢か、またはカスタムで追加した独自のプロバイダ選択肢から行うことができます。 内部セキュリティプロバイダは削除できません。

MDM Hub では、以下のタイプのセキュリティプロバイダをサポートしています。

認証プロバイダ

ID を検証してユーザーを認証します。 ユーザーが申し立てているとおりの人物であることを MDM Hub に通知します。 このタイプのセキュリティプロバイダは、ユーザーが特定の MDM Hub リソースにアクセスするために必要な特権を持っているかどうかを検証しません。

承認プロバイダ

MDM Hub に、ユーザーが特定の MDM Hub リソースにアクセスするために必要な特権を持っているかどうかを通知します。

ユーザープロファイルプロバイダ

MDM Hub に、ユーザー固有の属性やユーザーが属しているロールなどの個々のユーザーに関する情報を通知します。

内部プロバイダは、認証、承認、およびユーザープロファイルサービス用の MDM Hub の内部実装を表します。

MDM Hub のデフォルトのプロバイダの一部は、スーパープロバイダです。 スーパープロバイダは、常に認証要求および承認要求に対して肯定応答を返します。 ユーザー、ロール、および特権を設定する必要がない開発環境では、スーパープロバイダを使用します。 スーパープロバイダは、セキュリティが SIF 要求の最上位層で提供されるプロダクション環境でもパフォーマンス向上のために使用できます。

プロバイダファイル管理

プロバイダファイルには、セキュリティプロバイダのプロファイル情報が格納されています。

サードパーティのセキュリティプロバイダを独自に使用する場合は、セキュリティプロバイダツールを使用して明示的に登録する必要があります。 セキュリティプロバイダを登録するには、登録に必要なプロファイル情報が入ったプロバイダファイルをアップロードします。

プロバイダファイルは、以下のデータが格納された JAR ファイルです。

- 1 つ以上の外部セキュリティプロバイダについて記述したマニフェスト。 各セキュリティプロバイダについて、以下の設定が記述されています。
  - プロバイダの名前
  - プロバイダの説明
  - プロバイダタイプ
  - プロバイダファクトリクラスの名前
  - プロバイダの設定詳細を指定するプロパティ。 これはプロパティ名とデフォルト値のペアのリストです。
- プロバイダ実装と必要なサードパーティライブラリ。

Informatica リソースキットは Hub サーバーにプロバイダファイルのサンプル実装をコピーします。 サンプルのプロバイダファイルの詳細については、『*Multidomain MDM のリソースキットガイド*』を参照してください。

プロバイダファイルのアップロード

プロバイダ情報を追加または更新するには、プロバイダファイルをアップロードします。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。

3. 左側のナビゲーションペインで、［プロバイダファイル］を右クリックして**［プロバイダファイルのアップロード］**を選択します。

   セキュリティプロバイダツールで、このプロバイダの JAR ファイルを選択するように求められます。

4. 必要に応じてファイルシステム内を移動し、アップロードする JAR ファイルを選択して、JAR ファイルを指定します。
5. **［開く］**をクリックします。

   セキュリティプロバイダツールによって選択したファイルがチェックされ、有効なプロバイダファイルかどうかが確認されます。

6. アップロードするプロバイダファイルの名前が既存のプロバイダファイルと同じ名前の場合は、セキュリティプロバイダツールに、既存のプロバイダファイルを上書きするかどうかを尋ねるメッセージが表示されます。 **［はい］**をクリックして確定します。

   セキュリティプロバイダツールにより、プロバイダリストに追加のプロバイダ情報が読み込まれます。 プロバイダファイルがアップロードされたら、元のファイルをファイルシステムから削除できます。

プロバイダファイルの削除

セキュリティプロバイダが不要になったら、対応するプロバイダファイルを削除してもかまいません。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。
3. 左のナビゲーションペインで、削除するプロバイダファイルを右クリックし、**［プロバイダファイルの削除］**を選択します。

   セキュリティプロバイダツールから、削除を確認するように求められます。

4. **［はい］**をクリックします。

   セキュリティプロバイダツールで、削除したプロバイダファイルがリストから削除されます。

   注: MDM Hub に付属している内部プロバイダファイルを削除することはできません。

セキュリティプロバイダの設定

セキュリティプロバイダツールでは、登録されているプロバイダのリストが表示されます。

登録されているプロバイダのリストはプロバイダタイプ別にソートされています。 プロバイダリスト上のプロバイダの順序は、呼び出される順序も表します。 ユーザーはプロバイダリスト内の少なくとも 1 つのプロバイダによって承認される必要があります。

例えば、ログイン時にユーザー名とパスワードを入力すると、MDM Hub により、ログイン資格情報が認証リスト上の各認証プロバイダに送信されます。 この場合、MDM Hub により、リスト上の各認証プロバイダに、順番に送信が行われます。 リスト上のいずれか 1 つのプロバイダで認証が成功すると、そのユーザーは MDM Hub により認証されます。 利用可能な認証プロバイダすべてに対して認証が失敗した場合は認証されません。

セキュリティプロバイダの設定の変更

セキュリティプロバイダの設定を変更するには、以下の手順を実行します。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。

3. 変更するセキュリティプロバイダを選択します。
4. ［プロパティ］パネルで、編集する設定の横にある**［編集］**ボタンをクリックします。
5. **［保存］**ボタンをクリックして変更を保存します。

セキュリティプロバイダの有効化および無効化

1. 書き込みロックを取得します。
2. 有効または無効にするセキュリティプロバイダを選択します。
   - 無効になっているセキュリティプロバイダを有効にするには、**［有効］**チェックボックスをオンにする。
   - セキュリティプロバイダを無効にするには、**［有効］**チェックボックスをオフにする。

   無効になったプロバイダは、名前が使用不可になり、プロバイダリストの末尾に移動します。 無効にしたプロバイダをプロバイダリスト内で再配置することはできません。
3. **［保存］**ボタンをクリックして変更を保存します。

セキュリティプロバイダの処理順の移動

MDM Hub は、プロバイダリスト上の順番に従ってセキュリティプロバイダを処理します。セキュリティプロバイダの順序は再配置できます。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。
3. プロバイダを上に移動するには、移動するプロバイダを右クリックし、**［プロバイダを上に移動］**を選択します。

   選択したプロバイダがプロバイダリストの直前のプロバイダの上に移動されて、ナビゲーションペインが更新されます。
4. プロバイダを下に移動するには、移動するプロバイダを右クリックし、**［プロバイダを下に移動］**を選択します。

   選択したプロバイダがプロバイダリストの直前のプロバイダの下に移動されて、ナビゲーションペインが更新されます。

プロバイダのプロパティ

プロバイダパネルには以下のフィールドがあります。

名前

このセキュリティプロバイダの名前。

説明

このセキュリティプロバイダの説明。

プロバイダタイプ

セキュリティプロバイダのタイプ。 タイプは、次の値のいずれかになります。

- 認証
- 認証

- ユーザープロファイル

プロバイダファイル

このセキュリティプロバイダに関連付けられているプロバイダファイルの名前。または、内部プロバイダの場合は**内部プロバイダ**の名前。

有効

このセキュリティプロバイダが有効か無効かを示します。 有効になっているセキュリティプロバイダにはチェックマークが付いています。 無効になっているセキュリティプロバイダにはチェックマークが付いていません。 内部プロバイダは無効にできません。

プロパティ

このセキュリティプロバイダの追加のプロパティ（このセキュリティプロバイダで定義されている場合）。各プロパティは、名前と値のペアです。 セキュリティプロバイダでは、ここに指定できる固有のプロパティを要求または許可することができます。

プロバイダのプロパティの追加

プロバイダのプロパティを追加するには、以下の手順を実行します。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。
3. ナビゲーションペインで、プロパティを追加する認証プロバイダを選択します。
4. **［追加］**ボタンをクリックします。

   ［プロバイダのプロパティの追加］ダイアログボックスが表示されます。
5. プロパティの名前を指定します。
6. このプロパティに割り当てる値を指定します。
7. **［OK］**をクリックします。

プロバイダプロパティの編集

既存のプロバイダプロパティを編集するには、以下の手順を実行します。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。
3. ナビゲーションペインで、プロパティを編集する認証プロバイダを選択します。
4. 編集するプロパティごとに、その横にある**［編集］**ボタンをクリックし、新しい値を指定します。
5. **［保存］**ボタンをクリックして変更を保存します。

カスタムプロバイダ

カスタムプロバイダクラスは、プロバイダファイルを含む JAR または ZIP ファイルにパッケージ化できます。

`providers.properties` ファイルで、カスタムプロバイダの設定を指定します。続いて、このファイルを META-INF ディレクトリにある JAR ファイル内に配置します。 これにより、設定がローダーで変換されて、Hub コンソールに表示されます。

provider.properties ファイルには以下の要素があります。

ProviderList

含まれているプロバイダ名をカンマで区切ったリスト。

File-Description

パッケージの説明。

XXX-Provider-Name

プロバイダ *XXX* の表示名。

XXX-Provider-Description

プロバイダ *XXX* の説明。

XXX-Provider-Type

プロバイダ *XXX* のタイプ。 指定可能な値は、USER_PROFILE_PROVIDER、JAAS_LOGIN_MODULE、AUTHORIZATION_PROVIDER です。

XXX-Provider-Factory-Class-Name

プロバイダの実装クラス（同じ JAR または ZIP ファイルに含まれています）。

XXX-Provider-Properties

プロバイダプロパティを定義する名前/値のペアをカンマで区切ったリスト。

注: プロバイダアーカイブファイルには、カスタムプロバイダが機能するために必要なすべてのクラス、および必要なリソースが含まれている必要があります。 これらのリソースは、各実装に固有です。

サンプルの providers.properties ファイル

注: 以下の設定は、*XXX*-Provider-Properties を除いてすべて必要です。

```
ProviderList=ProviderOne,ProviderTwo,ProviderThree,ProviderFour
ProviderOne-Provider-Name: Sample Role Based User Profile Provider
ProviderOne-Provider-Description: Sample User Profile Provider for roled-based management
ProviderOne-Provider-Type: USER_PROFILE_PROVIDER
ProviderOne-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleRoleBasedUserProfileProviderFactory
ProviderOne-Provider-Properties: name1=value1,name2=value2
ProviderTwo-Provider-Name: Sample Login Module
ProviderTwo-Provider-Description: Sample Login Module
ProviderTwo-Provider-Type: JAAS_LOGIN_MODULE
ProviderTwo-Provider-Factory-Class-Name: com.siperian.sam.sample.authn.SampleLoginModule
ProviderTwo-Provider-Properties:
ProviderThree-Provider-Name: Sample Role Based Authorization Provider
ProviderThree-Provider-Description: Sample Role Based Authorization Provider
ProviderThree-Provider-Type: AUTHORIZATION_PROVIDER
ProviderThree-Provider-Factory-Class-Name: com.siperian.sam.sample.authz.SampleAuthorizationProviderFactory
ProviderThree-Provider-Properties:
ProviderFour-Provider-Name: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Description: Sample Comprehensive User Profile Provider
ProviderFour-Provider-Type: USER_PROFILE_PROVIDER
ProviderFour-Provider-Factory-Class-Name:
com.siperian.sam.sample.userprofile.SampleComprehensiveUserProfileProviderFactory
ProviderFour-Provider-Properties:
File-Description=The sample provider files
```

外部認証

MDM Hub では、Java Authentication and Authorization Service（JAAS）によるユーザーの外部認証を使用できます。

MDM Hub には、以下のタイプの認証規格のテンプレートが用意されています。

- Lightweight Directory Access Protocol（LDAP）
- Microsoft Active Directory
- Kerberos プロトコルを使用したネットワーク認証

これらのテンプレートには、それぞれの認証規格に必要な設定（プロトコル、サーバー名、ポートなど）が備わっています。 これらのテンプレートを使用して、新しいログインモジュールを追加し、必要な設定を指定することができます。 これらの認証規格の詳細については、該当するベンダのドキュメントを参照してください。

ログインモジュールの追加

MDM Hub で外部認証を使用するには、ログインモジュールを作成する必要があります。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。
3. ［認証プロバイダ（ログインモジュール）］を右クリックし、**［ログインモジュールの追加］**を選択します。

   ［ログインモジュールの追加］ダイアログボックスが表示されます。
4. 下矢印をクリックし、ログインモジュールのテンプレートを選択します。

   OpenLDAP **テンプレート**

   LDAP 認証のプロパティに基づきます。

   MicrosoftActiveDirectory-template

   Active Directory 認証のプロパティに基づきます。

   Kerberos **テンプレート**

   Kerberos 認証のプロパティに基づきます。
5. **［OK］**をクリックします。

   新しいログインモジュールがリストに追加されます。
6. ［プロパティ］パネルで、編集するプロパティの横にある**［編集］**ボタンをクリックします。作成するログインモジュールのタイプの設定を指定します。
7. **［保存］**ボタンをクリックして変更を保存します。

ログインモジュールの削除

必要に応じて、ログインモジュールを削除できます。

1. セキュリティプロバイダツールを起動します。
2. 書き込みロックを取得します。
3. ナビゲーションペインで、［認証プロバイダ（ログインモジュール）］の下のログインモジュールを右クリックし、**［ログインモジュールの削除］**を選択します。

   セキュリティプロバイダツールから、削除を確認するように求められます。

4. **［はい］**をクリックします。

   セキュリティプロバイダツールにより、削除したログインモジュールがリストから削除され、左側のナビゲーションペインが更新されます。

第 6 章

アプリケーションレベルセキュリティ

この章では、以下の項目について説明します。

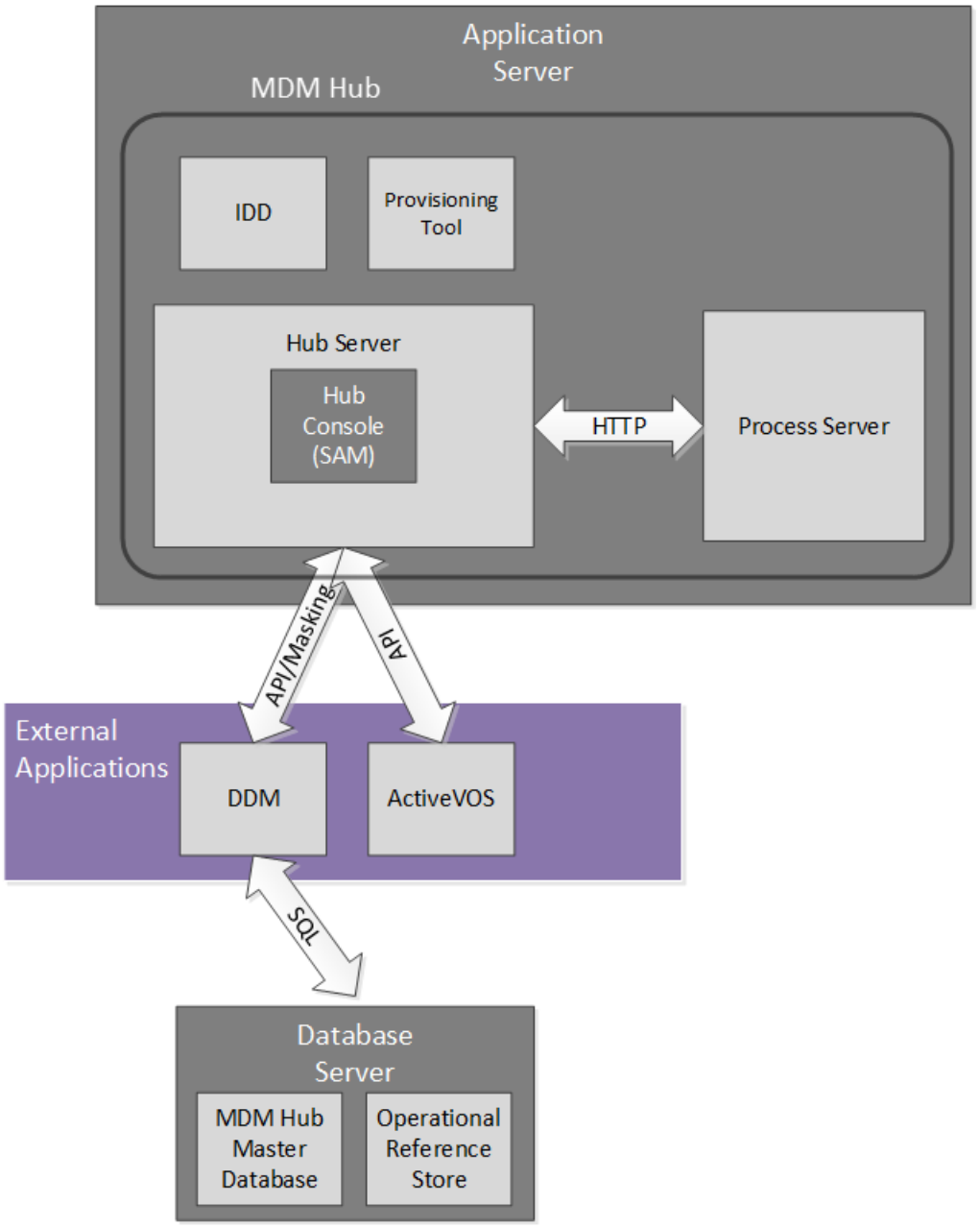
- アプリケーションレベルセキュリティ概要, 48 ページ
- Informatica Data Director, 49 ページ
- プロビジョニングツール, 50 ページ
- ActiveVOS, 50 ページ
- Dynamic Data Masking, 51 ページ
- Linux での WebLogic T3S チャネルのセットアップ, 53 ページ

アプリケーションレベルセキュリティ概要

セキュリティアクセスマネージャ（SAM）は、ユーザーの資格情報とロールを管理する MDM Hub 用のセキュリティモジュールです。MDM Hub 実装内の他のアプリケーションとコンポーネントにも、MDM Hub との通信を保護するためのセキュリティ設定があります。例えば、Informatica Data Director にはデータレベルのセキュリティを設定できます。

Informatica は、Informatica 製品に対してセキュリティテストを実施します。例えば、業界標準のスキャンアプリケーションを使用して、SQL インジェクション攻撃などのセキュリティ脆弱性について製品をテストします。 Informatica の他のセキュリティアプリケーションを SAM と連携して使用することで、MDM Hub 実装のセキュリティをさらに強化できます。Informatica Dynamic Data Masking（DDM）は、データにマスクを適用して機密情報への不正アクセスを防止します。Informatica MDM プロビジョニングツールと Informatica ActiveVOS はセキュリティアプリケーションではありませんが、MDM Hub との通信は保護されています。

次の図は MDM Hub の実装例で、コンポーネントどうしの接続方法を示しています。



Informatica Data Director

Informatica Data Director は、MDM Hub 用の Web ベースのデータガバナンスアプリケーションです。Data Director アプリケーションを構成すると、ビジネスユーザーはマスタデータを作成、管理、使用、および監視できます。

Informatica Data Director は、Open Web Application Security Project（OWASP）の上位 10 件のセキュリティ推奨事項に準拠しています。Informatica では、IBM Security AppScan を使用して、SQL インジェクション攻撃といったセキュリティ脆弱性をテストしています。HTTP メソッドの GET または POST は IDD から情報を取得できますが、DELETE や PUT などの他の HTTP メソッドは HTTP エラーを返します。

Data Director アプリケーションを構成すると、オペレーショナル参照ストアのテーブルをビジネスエンティティまたはサブジェクト領域別に分類することができます。どちらのアプローチも、顧客に関するすべてのデータなど、1 つの単位として扱う関連データをグループ化する方法を提供します。ビジネスエンティティは、Multidomain MDM バージョン 10.1 以降に推奨される組織アプローチです。ビジネスエンティティは、ビジネスエンティティサービスや最新のエンティティビューを含むエンティティ 360 フレームワークの中核です。

データのセキュリティを確保するために、Data Director アプリケーションは、オペレーショナル参照ストアで設定されているユーザーロールとリソース特権を使用します。MDM 管理者は Hub コンソールのセキュリティアクセスマネージャワークベンチを使用して、各ユーザーロールのリソース特権を定義することに注意してください。Data Director アプリケーションでは、ユーザーはユーザーロールによって許可されている操作を実行できます。

ビジネスエンティティおよびサブジェクト領域のロール特権は、さまざまな方法でリソース特権から派生するため、セキュリティは多少異なる場合があります。ただし、どちらのアプローチも同等にセキュアです。ビジネスエンティティのセキュリティの詳細については、『*Multidomain MDM のプロビジョニングツールガイド*』を参照してください。サブジェクト領域のセキュリティ設定とデータセキュリティの詳細については、『*Multidomain MDM Data Director の実装ガイド*』を参照してください。

プロビジョニングツール

オペレーショナル参照ストア（ORS）に定義したスキーマ情報に基づいてビジネスエンティティモデルを作成するには、プロビジョニングツールを使用します。ビジネスエンティティモデルは、Data Director のエンティティ 360 フレームワークの基盤となるコンポーネントです。

ビジネスエンティティを設定するには、プロビジョニングツールにログインする必要があります。

構成ファイルに対する作業を行う間、変更は一時ワークスペースに保存されます。プロビジョニングツールでは、変更はパブリッシュされるまで適用されません。複数のユーザーが ORS のビジネスエンティティ設定を同時に変更する場合、最後にパブリッシュされた設定で MDM Hub が更新されます。

プロビジョニングツールは、Hub サーバーと同じアプリケーションサーバー上で実行する必要があります。

詳細については、『*Multidomain MDM のプロビジョニングツールガイド*』を参照してください。

ActiveVOS

Informatica ActiveVOS(R)は、ビジネスプロセスを自動化するためのビジネスプロセス管理（BPM）ツールです。人、プロセス、およびシステムを統合したプロセスモデルを作成し、業務効率を向上させることができます。

ActiveVOS を使用すると、エンティティデータが変更された場合、必ず変更承認ワークフローを経たうえで更新されたレコードがベストバージョンオブトゥルース（BVT）レコードに提供されるようにすることができます。例えば、顧客データへの更新がマスタデータになる前に、シニアマネージャによる確認と承認が必要なビジネスプロセスが考えられます。

変更承認ワークフローをサポートするために、MDM Hub と Data Director が ActiveVOS サーバーと統合されます。定義済み MDM ワークフロー、タスクタイプ、およびロールにより、コンポーネントが相互に同期するようになります。埋め込み ActiveVOS サーバーと連携するように MDM 実装を設定できます。または、ActiveVOS のスタンドアロンインスタンスを実行することもできます。

埋め込み ActiveVOS は、Data Director と MDM Hub からの要求を、MDM と ActiveVOS の両方で信頼されている特定のプリンシパルによって認証します。このプリンシパルは「信頼されたユーザー」と呼ばれます。システム管理者は、信頼されたユーザーのクレデンシャルとロールをアプリケーションサーバーに作成します。

ActiveVOS サーバーは、MDM Hub と同じアプリケーションサーバー上で実行する必要があります。詳細については、『*Multidomain MDM の設定ガイド*』を参照してください。

Dynamic Data Masking

Informatica Dynamic Data Masking は、クライアントとデータベースの間で動作して、機密情報への不正アクセスを防止するデータセキュリティ製品です。 Dynamic Data Masking は、データベースに送信された要求をインターセプトし、そのデータにマスクを適用してから、要求に対する結果をクライアントに送信します。

Dynamic Data Masking は、MDM Hub が管理するデータベースのデータセキュリティレベルを増強します。Dynamic Data Masking 管理コンソールを使用して、オペレーショナル参照ストアへの Dynamic Data Masking の接続を設定し、データのマスキングルールを設定します。 オペレーショナル参照ストアを登録する場合は、Dynamic Data Masking への MDM Hub の接続を設定します。

Dynamic Data Masking は MDM インストーラでは MDM Hub と一緒にはインストールされません。 Dynamic Data Masking は別途インストールが必要です。 Dynamic Data Masking のインストールの詳細については、Dynamic Data Masking のマニュアルを参照してください。

注: MDM Hub で Dynamic Data Masking を使用するには、Dynamic Data Masking 9.6.0 と緊急バグフィックス 14590 をインストールしておく必要があります。 これより古いバージョンの Dynamic Data Masking には、MDM Hub との互換性がありません。

Dynamic Data Masking と MDM Hub の統合

Dynamic Data Masking を正しくインストールおよびセットアップしたら、Dynamic Data Masking と MDM Hub を統合することができます。

以下に、統合プロセスの手順を示します。

1. Dynamic Data Masking 管理コンソールで、Dynamic Data Masking サービスを作成します。 クライアントが要求をデータベースに送信するためのポート番号と同じリスナポート番号を設定します。
2. データマスキングを必要とするデータベースにデータベース接続プロパティを定義します。
3. 接続ルールを作成します。 マスクする必要があるデータベース要求を識別するようにルールを設定します。 接続ルールセットにデータベースとセキュリティルールセットを割り当てます。
4. セキュリティルールセットを作成します。 MDM Hub に返送されるデータをマスキングするルールを定義します。
5. Hub コンソールで、Dynamic Data Masking への接続を設定します。

オペレーショナル参照ストアのプロセスを実行すると、Dynamic Data Masking により、ルールがデータベースに適用され、データが MDM Hub に返されます。

注: オペレーショナル参照ストアへの Dynamic Data Masking の接続を追加しない場合には、MDM Hub は定義されたすべての Dynamic Data Masking ルールをバイパスします。

Dynamic Data Masking を設定する方法の詳細については、『*Informatica Dynamic Data Masking Administrator Guide*』を参照してください。

MDM Hub 用の Dynamic Data Masking のベストプラクティス

ご提案するベストプラクティスを利用することで、MDM Hub で Dynamic Data Masking を効率的に使用することができます。

ルールエディタで Dynamic Data Masking **ルールを作成するためのベストプラクティス**

Dynamic Data Masking がルールエディタ内の最上位から最下位までのルールを評価します。 このため、マスキングしないルールを作成する場合には、それらを有効にするため、作成する他のマスキングルールより上位に置く必要があります。

ユーザーがマスキングされないデータを表示できるようにするためのベストプラクティス

Dynamic Data Masking はデータベースのデータをマスキングしません。 MDM Hub でデータを表示しようとしても、データはマスキングされます。 データをマスキングせずに表示する特権をユーザーに付与するには、Dynamic Data Masking で Create View 文を使用します。

ユーザーをブロックするためのベストプラクティス

マスキングが適用されるレコードをユーザーが追加できないようにするには、適用を受けるベースオブジェクトごとに独立したルールを作成する必要があります。 Block 文の処理アクションおよび%INSERT %<BO_NAME>%<ロール名>%としてのテキストマッチャーを定義します。

マスクされたデータを更新できるようにするためのベストプラクティス

デフォルトでは、Dynamic Data Masking エンジンにより、ユーザーはマスクされたデータのあるテーブルを編集できないようになっています。 MDM Hub でマスクされたデータを更新するには、ユーザーがマスクされたカラムを更新できるようにするルールを Dynamic Data Masking ルールエディタで作成します。

MDM_SYSTEM **インジケータを使用してルールを作成するためのベストプラクティス**

MDM Hub では、ユーザー、MDM_SYSTEM は、システム呼び出し用の内部インジケータです。 MDM_SYSTEM は Hub コンソールのロールリストには表示されません。 Dynamic Data Masking は、ユーザーが持っている MDM Hub ロールに基づいてマスキングを適用します。 ルールエディタで Dynamic Data Masking ルールを作成する場合には、MDM_SYSTEM インジケータ専用のルールを作成しないでください。 MDM_SYSTEM はユーザーのユーザー名およびロールと組み合わせて使用する必要があることが、『Chart of Accounts Installation and Configuration Guide』に記載されています。 Dynamic Data Masking で MDM_SYSTEM インジケータとその他のルールを組み合わせて、詳細なルールを作成することができます。

Dynamic Data Masking のオペレーショナルリファレンスストア用セットアップ

Hub コンソールを使用してオペレーショナル参照ストアを登録する場合は、MDM Hub への Dynamic Data Masking の接続を設定します。

1. Hub コンソールを開始します。

   [データベースの変更] ダイアログボックスが表示されます。
2. MDM Hub マスタデータベースを選択して、**[接続]** をクリックします。
3. 設定ワークベンチにある**データベース**ツールを起動します。
4. 書き込みロックを取得します。
5. **[データベースの登録]** ボタンをクリックします。

   Informatica MDM Hub 接続ウィザードが表示され、データベースタイプの選択が求められます。
6. データベースのタイプを選択して **[次へ]** をクリックします。
7. データベースの接続プロパティを設定します。

8. **［ポート］**フィールドに入力するポートは、データベースの Dynamic Data Masking リスナポートと一致している必要があります。
9. **［DDM 接続 URL］**フィールドで、Dynamic Data Masking サーバーの URL を入力します。
10. **［完了］**をクリックします。

    ［データベースの登録］ダイアログボックスが表示されます。
11. **［OK］**をクリックします。

    MDM Hub により、オペレーショナル参照ストアが登録されます。
12. 登録したオペレーショナル参照ストアを選択し、**［データベース接続のテスト］**ボタンをクリックしてデータベース設定をテストします。

    WebSphere を使用している場合は、データベース接続をテストする前に WebSphere を再起動します。

    ［データベースのテスト］ダイアログに、データベース接続テストの結果が表示されます。
13. **［OK］**をクリックします。

    Dynamic Data Masking が、登録したオペレーショナル参照ストアに接続されます。

Linux での WebLogic T3S チャネルのセットアップ

WebLogic T3S は SSL ベースのプロトコルであり、MDM Hub に対してセットアップすることができます。

以下の手順では、キーストアの作成および使用方法、SSL 用のサーバーインスタンスの設定方法、およびチャネルの作成方法に精通していることを前提としています。詳細については、WebLogic のマニュアルを参照してください。

1. 開始する前に、ID の目的で使用するキーストアが必要です。
2. WebLogic 管理コンソールで、MDM で使用するサーバーインスタンスに移動し、次のプロパティを使用して SSL を設定します。
   - **ID と信頼の場所** = **キーストア**
   - **プライベートキーの場所** = **カスタム ID キーストアから**
   - **プライベートキーエイリアス** = <キーストアで定義されたエイリアス>
   - **プライベートキーパスフレーズ** = <キーストアで定義されたパスフレーズ>
   - **証明書の場所** = **カスタム ID キーストアから**
   - **信頼された認証局** = **Java 標準信頼キーストアから**
3. 管理者コマンドプロンプト（cmd）ウィンドウを開き、keytool コマンドを使用して lib/security/cacerts の下にある JDK および JRE ディレクトリにキーストアをインポートします。
   次のサンプルコードは構文を示しています。

   ```
   keytool -import -alias <SSL Private Key Alias> -keystore "<JDK installation directory>/jre/lib/security/
   cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/servers/
   <WebLogic server instance>/keystores/wls12c_server.cer" -v

   keytool -import -alias <SSL Private Key Alias> -keystore "<JRE installation directory>/lib/security/
   cacerts" -file "/data/oracle/Oracle/Middleware/Oracle_Home/user_projects/domains/base_domain/servers/
   <WebLogic server instance>/keystores/wls12c_server.cer" -v
   ```

   注: keytool コマンドのヘルプが必要な場合は、Java のマニュアルを参照してください。
4. <WebLogic domain>/bin/startWebLogic.sh ファイルに移動し、次の Java オプションを設定します。

   ```
   -Doracle.jdbc.J2EE13Compliant=true
   ```

5. WebLogic 管理コンソールで、SSL 設定と一致する T3S チャネルを作成します。以下のプロパティを設定します。
   - **名前** = <チャネルの名前>
   - **プロトコル** = t3s
   - **リスンアドレス** = <キーストアで定義されているホスト名>
   - **リスンポート** = <キーストアで定義されているポート>
   - **［トンネリング有効］**を選択
   - **［双方向 SSL］**を選択
   - **［サーバープライベートキーエイリアス］**に、SSL の設定時に指定したエイリアスが表示されていることを確認します。
6. チャネルを保存し、チャネルがネットワークチャネルの一覧に表示されていることを確認します。
7. Informatica Data Director をエンティティ 360 表示で使用する場合は、<WebLogic domain>/bin/setDomainEnv.sh ファイルに移動し、次の MDM オプションを設定します。
   - e360.mdm.protocol=t3s
   - e360.mdm.host=<T3S channel Listen Address>
   - e360.mdm.port=<T3S channel Listen Port>
8. WebLogic を再起動します。
9. ping によってチャネルが動作していることをテストします。

   ```
   java weblogic.Admin -url t3s://<T3S Channel Listen Address>:<T3S Channel Listen Port> -username <WebLogic username> -password <WebLogic password> PING
   ```
10. これで、HTTPS とセキュアポートを使用して Hub コンソールを起動できます。

    ```
    https://<T3S Channel Listen Address>:<T3S Channel Listen Port>/cmx/
    ```

第 7 章

証明書ベースの認証

この章では、以下の項目について説明します。

- 証明書ベースの認証概要, 55 ページ
- 証明書ベースの認証と外部クライアント, 55 ページ
- 信頼されたアプリケーション, 56 ページ
- 証明書とキーの管理 , 56 ページ

証明書ベースの認証概要

MDM Hub は、証明書ベースの認証メカニズムを使用して、MDM Hub コンポーネントと信頼されたアプリケーション間の通信を保護します。認証メカニズムは、サービス統合フレームワーク（SIF）およびビジネスエンティティサービス API でもサポートされています。

デフォルトでは、証明書ログインモジュールは、Data Director などの Informatica アプリケーションを信頼されたアプリケーションとして認識します。外部アプリケーションに証明書ベースの認証を使用するには、アプリケーションを信頼されたアプリケーションとして登録する必要があります。

信頼されたアプリケーションとして登録されている外部アプリケーションは、MDM Hub にアプリケーション名とユーザー名の連結を渡します。例えば、IDD/admin のようになります。外部アプリケーションで、セキュリティペイロードも渡す必要があります。

証明書ベースの認証と外部クライアント

SiperianClient API などの MDM Hub の外部クライアントは、ユーザー名とパスワード認証を使用して要求を送信できます。ただし、外部クライアントは証明書ベースの認証も使用できます。

MDM Hub 外部のクライアントに対して証明書ベースの認証を設定するには、次の手順を実行します。

1. Hub コンソールで、外部クライアントに関連付けられたユーザーに公開証明書を登録します。
2. 外部クライアントを使用して要求をトリガします。

信頼されたアプリケーション

MDM Hub では、信頼されたアプリケーションとはアプリケーションユーザーと呼ばれるユーザータイプの 1 つです。アプリケーションユーザーは、管理者ユーザーを含む MDM Hub の標準ユーザーの代わりに要求を実行できます。信頼されたアプリケーションは、MDM Hub の信頼されたアプリケーションフレームワークに属しています。

信頼されたアプリケーションは、CMX_SYSTEM スキーマの C_REPOS_USER テーブルの APPLICATION_IND カラムで定義されます。信頼されたアプリケーションはそれぞれ、Hub コンソールのアプリケーションユーザーとして登録されています。デフォルトでは、MDM Hub は MDM Hub 実装で広く使用されている Informatica アプリケーションを、信頼されたアプリケーションとして認識します。例えば、Informatica Data Director と ActiveVOS は信頼されたアプリケーションです。

デフォルトでは、信頼されたアプリケーションはそれぞれ、設定されたパブリックキーとプライベートキーのセットを持ちます。MDM Hub は、次のいずれかの方法で信頼されたアプリケーションからの要求を認証します。

- ユーザークレデンシャルの認証
- 証明書ベースの認証

別のアプリケーションを信頼されたアプリケーションとして設定するには、「ユーザーアカウントの追加」 (ページ 30)を参照してください。

信頼されたアプリケーションとしての外部アプリケーションの追加

外部アプリケーションを MDM Hub の信頼されたアプリケーションフレームワークに追加することもできます。

1. Hub コンソールで、外部アプリケーションに対応するアプリケーションユーザーのユーザーアカウントを追加します。

   注: ［ユーザーの追加］ダイアログボックスで **［アプリケーションユーザー］**チェックボックスを選択し、ユーザーアカウントの名前に小文字のみを使用するようにします。
2. 公開証明書をアプリケーションユーザーアカウントに登録します。
3. 外部アプリケーションを使用して要求をトリガします。

   注: 証明書ベースの認証を使用する場合、要求名を<アプリケーション名>/<ユーザー名>として設定します。<アプリケーション名>は、手順 1 で使用する名前と同じにする必要があります。<ユーザー名>は、要求をトリガする MDM Hub ユーザーの名前です。

証明書とキーの管理

MDM Hub は証明書ベースの認証を使用します。安全な場所に各ユーザーの証明書とプライベートキーのペアを保持する必要があります。

デフォルトでは、MDM Hub は、プライベートキーと証明書を次の場所に保持します。

<MDM Hub installation directory: MDM Hub のインストールディレクトリ>/server/resources/certificates

また、Multidomain MDM のインストール中にカスタム証明書プロバイダを設定できます。

カスタム証明書プロバイダを実装するには、siperian-server-pkiutil.jar ファイルの PKIUtil.java インタフェースを実装する必要があります。このファイルは次のディレクトリにあります。

<MDM Hub installation directory: MDM Hub のインストールディレクトリ>/hub/server/lib/pkiutils

カスタム証明書プロバイダを使用する場合、PKIUtil 実装で使用する、キーストアとパブリック証明書を保持する必要があります。

注: 証明書プロバイダを変更する必要がある場合は、Informatica グローバルカスタマサポートに連絡して、セキュリティ設定ユーティリティを要求してください。

関連項目：

- 「セキュリティ設定ユーティリティ」 (ページ 57)

セキュリティ設定ユーティリティ

セキュリティ設定ユーティリティを使用して、MDM Hub 実装のセキュリティ設定の一部を管理できます。

セキュリティ設定ユーティリティを使用すると、次のタスクを実行できます。

- 認証に使用する証明書プロバイダを変更する。
- MDM Hub のユーザーのパスワードをリセットする。
- パスワードのハッシュ化に使用するハッシュアルゴリズムを変更する。
- ハッシュアルゴリズムの作成に使用するカスタマハッシュキーを変更する。

注: セキュリティ設定ユーティリティを入手するには、Informatica グローバルカスタマサポートにお問い合わせください。

第 8 章

パスワードのハッシュ化

この章では、以下の項目について説明します。

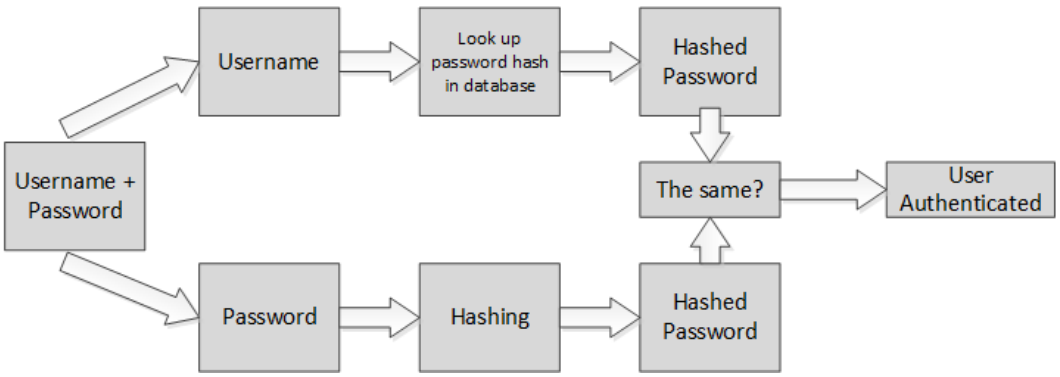
- パスワードのハッシュ化の概要, 58 ページ
- パスワードのハッシュ化オプション, 59 ページ
- パスワードリセットのプロセス , 59 ページ
- セキュリティ設定ユーティリティ, 60 ページ
- トラブルシューティング, 60 ページ

パスワードのハッシュ化の概要

パスワードのハッシュ化とは、パスワードを暗号ハッシュ関数で不可逆的に暗号化することです。MDM Hub は、パスワードハッシュ化方法を使用して、ユーザーのパスワードを保護し、パスワードがデータベースにクリアテキスト形式で格納されないようにします。MDM Hub 管理者は Hub サーバーのインストール時に、アルゴリズムやカスタマハッシュキーなどのパスワードハッシュ化オプションを設定します。

Informatica では、ハッシュアルゴリズムの変更や MDM Hub ユーザーパスワードのリセットなど、MDM Hub 実装のセキュリティ設定を管理するためのセキュリティ設定ユーティリティを提供しています。

次の図は、MDM Hub がユーザーパスワードを認証する方法を示しています。



関連項目：

- 「セキュリティ設定ユーティリティ」 (ページ 57)

パスワードのハッシュ化オプション

Hub サーバーのインストール中に、パスワードハッシュ化の次のオプションを設定します。

- ハッシュアルゴリズムの一部としてカスタムハッシュキーを作成するかどうか
- デフォルトの SHA3 ハッシュアルゴリズムを使用するか、またはカスタムハッシュアルゴリズムを作成するか
- デフォルトの証明書プロバイダを使用するか、またはカスタム証明書プロバイダを使用するか

SHA3 とカスタムハッシュアルゴリズムのどちらを使用しても、MDM Hub ユーザーのパスワードは不可逆的に暗号化されます。クリアテキスト形式でデータベースに格納されることはありません。どのハッシュアルゴリズムを使用する場合でも、アルゴリズムには次のコンポーネントが含まれます。

- ハッシュ関数
- ソルト値
- MDM Hub のインストール中に設定されるオプションのペッパー値またはハッシュキー。MDM Hub 管理者が、このキーを作成して安全に保存する責務を担います。

ペッパー値を作成する場合、桁区切りのない 32 文字までの 16 進数のシーケンスを含むキーを使用することをお勧めします。

重要: ハッシュキーの機密性を保護して、データ侵害のリスクを回避します。ハッシュキーが盗まれた場合は、すべてのパスワードをリセットする必要があります。

パスワードハッシュアルゴリズムと、そのアルゴリズムの基盤となる実装は Hub サーバープロパティに保存されます。Hub サーバープロパティの詳細については、『*Multidomain MDM の設定ガイド*』を参照してください。

カスタムハッシュアルゴリズム

パスワードリセットのプロセス

パスワードを忘れた場合や、ハッシュアルゴリズムの秘密のコンポーネントのセキュリティに問題があると考えられる場合は、パスワードをリセットできます。パスワードをリセットするには、Informatica グローバルカスタマサポートにお問い合わせください。

パスワードをリセットするとき、一時パスワードが記載された電子メールを受け取ります。そのパスワードを使用して MDM Hub にログインし、自分にとってわかりやすいパスワードに変更します。Hub コンソール、または Informatica Data Director からパスワードを変更できます。

セキュリティ設定ユーティリティ

セキュリティ設定ユーティリティを使用して、MDM Hub 実装のセキュリティ設定の一部を管理できます。

セキュリティ設定ユーティリティを使用すると、次のタスクを実行できます。

- 認証に使用する証明書プロバイダを変更する。
- MDM Hub のユーザーのパスワードをリセットする。
- パスワードのハッシュ化に使用するハッシュアルゴリズムを変更する。
- ハッシュアルゴリズムの作成に使用するカスタマハッシュキーを変更する。

注: セキュリティ設定ユーティリティを入手するには、Informatica グローバルカスタマサポートにお問い合わせください。

トラブルシューティング

問題が発生した場合、次の情報を使用して問題のトラブルシューティングを行います。

MDM Hub ユーザーがログインできない

Hub サーバーのインストール後、MDM Hub によって CMX_SYSTEM スキーマが再作成される場合、ハッシュパスワードは認識されません。その結果、ユーザーは MDM Hub にログインできません。

この問題を解決するには、`postInstallSetup` スクリプトを手動で再実行します。このスクリプトにより、MDM Hub ユーザーのパスワードが再度ハッシュされ、ユーザーがログインできるようになります。

postInstallSetup スクリプトの詳細については、『*Multidomain MDM のインストールガイド*』を参照してください。

付録 A

用語集

authentication: **認証**

ユーザーが指定した ID がそのユーザーのものであるかどうかを確認するプロセス。 Informatica MDM Hub では、ユーザーが指定した資格情報（ユーザー名/パスワードまたはセキュリティペイロード、あるいはその両方の組み合わせ）に基づいてユーザーが認証されます。 Informatica MDM Hub では、内部認証メカニズムが用意されているほか、サードパーティの認証プロバイダを使用したユーザー認証もサポートされています。

authorization: **認証**

ユーザーが要求した Informatica MDM Hub のリソースにアクセスするために必要な特権を持っているかどうかを確認するプロセス。 Informatica MDM Hub では、リソース特権はロールに割り当てられています。 ユーザーとユーザーグループはロールに割り当てられます。 ユーザーのリソース特権は、ユーザーが割り当てられているロール、およびユーザーが属するユーザーグループに割り当てられているロールで決まります。

base object: **ベースオブジェクト**

ビジネスに関係するエンティティ（顧客やアカウントなど）に関する情報を格納するテーブル。

batch group: **バッチグループ**

1 つのコマンドで実行できる個々のバッチジョブ（ステージジョブ、ロードジョブ、一致ジョブなど）の集合。 グループ内の各バッチジョブは、他のジョブと順番に実行することも並行して実行することも可能です。

Configuration workbench: **設定ワークベンチ**

各種の MDM Hub オブジェクト（オペレーショナル参照ストア、ユーザー、セキュリティ、メッセージキュー、メタデータの検証など）を設定するためのツールが含まれています。

database: **データベース**

Hub Store 内の整理されたデータの集まり。 Informatica MDM Hub では、2 種類のデータベースをサポートしています。マスターデータベースとオペレーショナル参照ストア（ORS）です。

Data Manager: **データマネージャ**

すべてのマージ（自動マージを含む）の結果を確認し、必要に応じてデータのコンテンツを修正するためのツール。 このツールでは、各ベースオブジェクトレコードのデータリネージを確認できます。 また、既存のマージ済みレコードをマージ解除したり、統合された各レコードに関する各種の履歴を表示したりできます。

データマネージャツールでは、レコードの検索、それらの相互参照の表示、レコードのマージ解除、レコードのリンク解除、履歴レコードの表示、新しいレコードの作成、レコードの編集、および信頼の設定のオーバーライドを行うことができます。 データマネージャには、定義した検索条件を満たすすべてのレコードが表示されます。

data steward: **データスチュワード**

データ品質に関する主な責任を担う Informatica MDM Hub ユーザー。 データスチュワードは、Informatica MDM Hub に Hub コンソールからアクセスし、Informatica MDM Hub のツールを使用して、Hub ストア内のオブジェクトの設定を行います。

Dynamic Data Masking

クライアントとデータベースの間で動作して、機密情報への不正アクセスを防止するデータセキュリティ製品。 Dynamic Data Masking は、データベースに送信された要求をインターセプトし、その要求にデータマスキングルールを適用してから、要求に対する結果をクライアントに返します。

hierarchy: **階層**

階層マネージャで、リレーションタイプをまとめたもの。 これらのリレーションタイプは、階層のエンティティの位置に基づいてランク付けされるわけではなく、相互に関連するとも限りません。 単に分類や識別がしやすいようにグループ分けされたリレーションタイプです。

Hierarchy Manager: **階層マネージャ**

階層マネージャを使用すると、MDM Hub で管理されているレコードに関連付けられている階層データを管理できます。詳細については、『*Multidomain MDM の設定ガイド*』および『*Multidomain MDM のデータスチュワードガイド*』を参照してください。

Hub Console: Hub **コンソール**

管理者およびデータスチュワード向けの一連のツールで構成される Informatica MDM Hub のユーザーインタフェース。 それぞれのツールで、特定のアクション、または関連する一連のアクションを実行することができます。例えば、データモデルの構築、バッチジョブの実行、データフローの設定、Informatica MDM Hub のリソースに対する外部アプリケーションからのアクセスの設定など、システムの設定や操作に関するタスクを実行できます。

Hub Server

共通のコアサービス（アクセス、セキュリティ、セッションの管理など）に使用される中間層（アプリケーションサーバー）のランタイムコンポーネント。

Hub Store

Informatica MDM Hub 実装で、マスターデータベースと 1 つ以上のオペレーショナル参照ストア（ORS）データベースを格納するデータベース。

Kerberos

コンピュータネットワーク認証プロトコル。このプロトコルにより、セキュアではないネットワークを介して通信するノード間で、別のノードに対して自身の ID をセキュアな方法で証明できます。このプロトコルはマサチューセッツ工科大学（MIT）が開発し、MIT により Kerberos の自由な実装が認められています。

metadata: **メタデータ**

他のデータを記述するために使用されるデータ。 Informatica MDM Hub では、Informatica MDM Hub 実装で使用されるスキーマ（データモデル）を、メタデータや関連する構成設定を使用して記述します。

package: **パッケージ**

*パッケージ*とは、Informatica MDM Hub の 1 つ以上の基本テーブルの公開されたビューです。 パッケージは、それらのテーブル内のカラムのサブセットを、そのテーブルに結合された他のテーブルと一緒に示します。 パ

ッケージはクエリに基づきます。 基になるクエリで、テーブルまたは別のパッケージからレコードのサブセットを選択することができます。

password policy: **パスワードポリシー**

Informatica MDM Hub ユーザーアカウントのパスワードの特性（パスワード長、有効期限、ログイン設定、パスワードの再利用およびその他の要件）を指定します。 Informatica MDM Hub 実装のすべてのユーザーアカウントに対するグローバルパスワードポリシーを定義して、個別のユーザーについてこれらの設定を上書きすることができます。

policy decision points (PDPs): **ポリシー決定ポイント（PDP）**

ユーザー ID を認証し、MDM Hub リソースへのユーザーアクセスを許可する特定のセキュリティチェックポイント。

policy enforcement points (PEPs): **ポリシー適用ポイント（PEP）**

実行時にセキュリティポリシーを認証要求および承認要求に適用する、特定のセキュリティチェックポイント。

private resource: **非公開リソース**

ロールツールに公開されていない Informatica MDM Hub リソース。Services Integration Framework （SIF）の操作からアクセスできません。 Hub コンソールで新しいリソース（新しいベースオブジェクトなど）を追加すると、デフォルトで非公開リソースに設定されます。

privilege: **特権**

MDM Hub のリソースにユーザーがアクセスする権限。 MDM Hub の内部承認では、各ロールに以下のいずれかの特権が割り当てられます。

特権	許可する操作
読み取り	データの表示。
作成	Hub Store 内にデータレコードを作成。
更新	Hub Store 内のデータレコードの更新。
マージ	データのマージおよびアンマージ。
実行	クレンジング関数およびバッチグループの実行。
削除	Hub Store からデータレコードを削除。

外部アプリケーションユーザーが MDM Hub リソースに対して持つアクセス権は、特権によって決まります。例えば、特定のパッケージおよびパッケージカラムに、読み取り、作成、更新、およびマージ特権を設定できます。 設定は Hub コンソールの使用にある程度影響しますが、これらの特権は Hub コンソールを使用する場合に実行されません。

profile: **プロファイル**

階層マネージャでは、HM ユーザーが表示、編集、または追加できるフィールドおよびレコードを表します。例えば、2 つのプロファイルを用意し、一方ではすべてのエンティティおよびリレーションに対する完全な読み取り/書き込みアクセスを許可し、もう一方は読み取り専用にする（追加や編集の操作を許可しない）ことも可能です。

provider: **プロバイダ**

*security provider: セキュリティプロバイダ (ページ 64)*を参照してください。

security: **セキュリティ**

Informatica MDM Hub の実装内のデータおよびその他リソースに対する不正アクセスや改ざんを防ぐことで、情報のプライバシー、機密性、およびデータ整合性を保護する機能。

Security Access Manager workbench: Security Access Manager **ワークベンチ**

ユーザー、グループ、リソース、およびロールに対するツールを含みます。

security payload: **セキュリティペイロード**

以降の認証や承認に必要な補足データを含めることができる、MDM Hub 操作の要求に提供される RAW バイナリデータ。

security provider: **セキュリティプロバイダ**

ユーザーが Informatica MDM Hub にアクセスする際のセキュリティサービス（認証、承認、およびユーザープロファイルサービス）を提供するサードパーティ製アプリケーション。

workbench: **ワークベンチ**

Hub コンソールにおける、同様のツールをグループ化するメカニズム。 ワークベンチとは、関連するツールの論理的集合です。 例えば、モデルワークベンチには、スキーマ、クエリ、パッケージ、マッピングといった、データモデリングのためのツールが含まれています。

オペレーショナル参照ストア（ORS）

マスタデータを含むデータベースとマスタデータに適用されるルール。ルールには、マスタデータ処理のルール、マスタデータオブジェクトセット管理のルール、および MDM Hub がベストバージョン オブ トゥルースを定義するために使用する処理ルールと補助ロジックが含まれます。MDM Hub の構成には、1 つ以上のオペレーショナル参照ストアを含めることができます。ORS のデフォルト名は CMX_ORS です。

セキュリティアクセスマネージャ（SAM）

セキュリティアクセスマネージャ（SAM）は、MDM Hub リソースを未承認アクセスから保護するセキュリティモジュールです。 実行時に、SAM は MDM Hub 実装に対する組織のセキュリティポリシー決定を実施し、セキュリティ設定に従ってユーザーの認証とアクセス承認を処理します。

ロール

セキュアな Informatica MDM Hub リソースにアクセスするための一連の特権を定義します。

書き込みロック

Hub コンソールにおける、基になるスキーマに変更を加えるために必要なロック。 データスチュワード以外のすべてのツール（オペレーショナル参照ストアセキュリティツールを除く）は、書き込みロックを取得しない限り読み取り専用モードになります。 書き込みロックによって、複数の同時ユーザーがスキーマに変更を加えることができるようになります。

索引

D

Dynamic Data Masking
  概要 10

J

JDBC データソース
  セキュリティ、設定 34

P

providers.properties ファイル
  例 45

お

オペレーショナルリファレンスストア（ORS）
  ユーザーの割り当て 38

か

外部アプリケーションユーザー 30

く

グローバル
  パスワードポリシー 33

し

認証
  外部承認 12
  外部ディレクトリ認証 11
  外部認証プロバイダ 11
  承認の概要 12
  内部承認 12
  内部認証 11
  認証の概要 11

せ

セキュリティ
  JDBC データソース、設定 34
  認証 11, 12
  設定 9
セキュリティアクセスマネージャ（SAM） 11
セキュリティプロバイダツール
  セキュリティプロバイダの概要 40
セキュリティプロバイダツール *(続く)*
  プロバイダファイル 41
セキュリティプロバイダファイル
  アップロード 41
  削除 42
  セキュリティプロバイダファイルの概要 40

て

データベース
  ユーザーアクセス 32

と

トラブルシューティング
  パスワードのハッシュ化 60

は

パスワード
  グローバルパスワードポリシー 33
  プライベートパスワード 34
パスワードポリシー
  グローバルパスワードポリシー 33
  プライベートパスワードポリシー 34

ふ

プライベートパスワードポリシー 34
プロバイダ
  カスタムで追加 44

ゆ

ユーザー
  オペレーショナルリファレンスストア（ORS）への割り当て 38
  外部アプリケーションユーザー 30
  グローバルパスワードポリシー 33
  データベースアクセス 32
  パスワード設定 32
  プライベートパスワードポリシー 34
  補足情報 31
ユーザーグループ
  ユーザーの割り当て 37

よ

用語解説 61

り

リソース特権、ロールへの割り当て 26
リソースグループ
  追加 21
  編集 21

ろ

ロール
  編集 25
  ロールへのリソース特権の割り当て 26