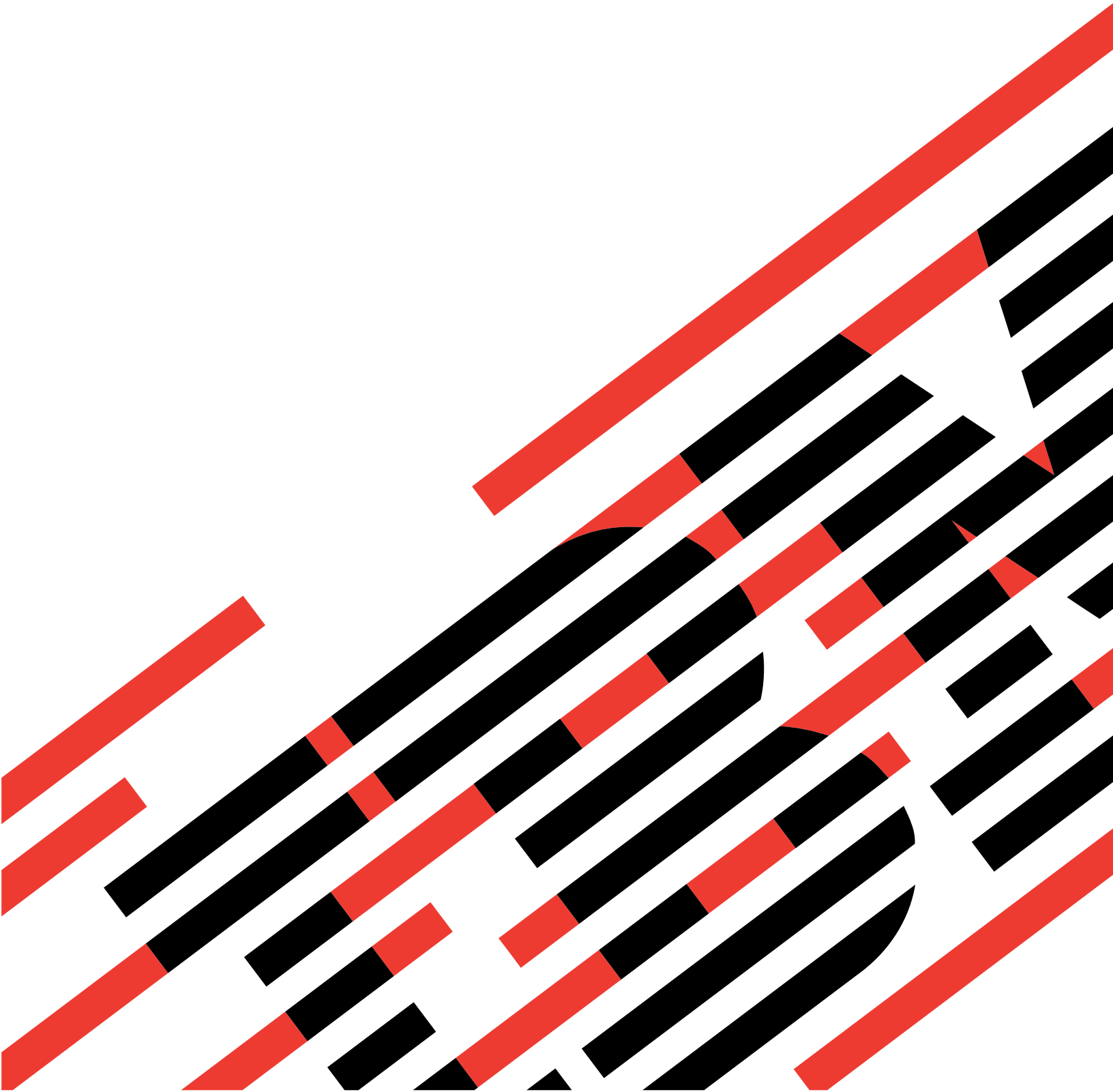
IBM Systems - iSeries

エンタープライズ識別マッピング

バージョン 5 リリース 4



IBM

IBM Systems - iSeries

エンタープライズ識別マッピング

バージョン 5 リリース 4

ご注意！

本書および本書で紹介する製品をご使用になる前に、 143 ページの『特記事項』 に記載されている情報をお読みください。

本書は、IBM i5/OS (製品番号 5722–SS1) のバージョン 5、リリース 4、モディフィケーション 0 に適用されます。また、改訂版で断りがない限り、それ以降のすべてのリリースおよびモディフィケーションに適用されます。このバージョンは、すべての RISC モデルで稼働するとは限りません。また CISC モデルでは稼働しません。

本マニュアルに関するご意見やご感想は、次の URL からお送りください。今後の参考にさせていただきます。

http://www.ibm.com/jp/manuals/main/mail.html

なお、日本 IBM 発行のマニュアルはインターネット経由でもご購入いただけます。詳しくは

http://www.ibm.com/jp/manuals/ の「ご注文について」をご覧ください。

(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原　典： IBM Systems - iSeries
Enterprise Identity Mapping
Version 5 Release 4

発　行： 日本アイ・ビー・エム株式会社

担　当： ナショナル・ランゲージ・サポート

第1刷 2006.2

この文書では、平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、および平成角ゴシック体™W7を使用しています。この(書体*)は、(財) 日本規格協会と使用契約を締結し使用しているものです。フォントとして無断複製することは禁止されています。

注* 平成明朝体™W3、平成明朝体™W7、平成明朝体™W9、平成角ゴシック体™W3、平成角ゴシック体™W5、平成角ゴシック体™W7

目次

エンタープライズ識別マッピング

EIM (エンタープライズ識別マッピング) for iSeries™ は、管理者およびアプリケーション開発者が企業全体の複数のユーザー・レジストリーを管理する際の問題を解決する、IBM® @server インフラストラクチャーの i5/OS™ インプリメンテーションです。ネットワークを使用する企業の大半は複数のユーザー・レジストリーの問題に直面しています。企業内の各個人や各エンティティーが各レジストリーにユーザー ID を持つ必要があるためです。複数のユーザー・レジストリーの必要性は、すぐに管理上の大きな問題になり、ユーザーにも、管理者にも、アプリケーション開発者にも影響を与えます。 EIM (エンタープライズ識別マッピング) は、企業内の複数のユーザー・レジストリーとユーザー ID の管理を容易にするソリューションを低費用で可能にするものです。

EIM により、企業内の個人のさまざまなユーザー・レジストリー内のさまざまなユーザー ID 間の、 アソシエーションと呼ばれる ID マッピングのシステムを作成できます。 EIM はまた、作成した ID マッピングを使用して、ユーザー ID 間の関係を検索できるアプリケーションを開発するために、異種のプラットフォーム間で使用できる API の共通セットを提供します。 さらに、EIM をネットワーク認証サービス (Kerberos の i5/OS インプリメンテーション) と結合して使用し、シングル・サインオン環境を提供することができます。

EIM の構成および管理は、iSeries ナビゲーターという iSeries グラフィカル・ユーザー・インターフェースを使って行えます。 iSeries サーバーでは EIM を使用して、i5/OS のインターフェースでネットワーク認証サービスを用いたユーザー認証を行えるようにしています。 i5/OS だけでなくアプリケーションも Kerberos チケットを受け入れて、 EIM を使用して Kerberos チケットが表している個人と同じ個人を表すユーザー・プロファイルを検索することができます。

EIM がどのように作用するか、EIM の概念、およびユーザーの企業内でどのように EIM を使用できるかについて詳しくは、以下を確認してください。

V5R4 の新機能

このトピックは、EIM (エンタープライズ識別マッピング) for iSeries の V5R4 で加えられた変更を説明します。

EIM の新規または拡張機能

- グループ・レジストリー定義 EIM マッピングを構成するために実行すべき作業の量を削減するため、グループ・レジストリー定義を作成できます。個々のレジストリー定義を管理するのと同じような方法で、グループ・レジストリー定義を管理できます。
- グループ・レジストリー定義の追加 グループ・レジストリー定義を作成し、EIM ドメインに追加するには、このトピックの指示に従ってください。
- グループ・レジストリー定義へのメンバーの追加 グループ・レジストリー定義を保管する EIM ドメインに接続しているときに、このトピックの指示にしたがってグループ・レジストリー定義にメンバーを追加することができます。

EIM 情報の機能拡張

このリリースでは、グループ・レジストリー定義をさまざまな EIM 状況に合わせてインプリメントする方法に関する多くの更新がなされました。

- ポリシー・アソシエーション ここでは、単一のレジストリーおよびドメイン内ですべてのユーザー ID にマッピング関係を設定するために、グループ・レジストリー定義を使用する理由を説明します。
- ルックアップ操作 ここでは、検索フローによって、グループ・レジストリー定義のメンバーであるユーザー・レジストリー内でターゲット・ユーザー ID を戻すルックアップ操作が処理される方法を説明します。
- あいまいな結果 ここでは、個々のユーザー・レジストリー定義を複数のグループ・レジストリー定義のメンバーとして指定すると、ルックアップ操作があいまいな結果を戻す場合があることを説明します。

さらに、トピックシングル・サインオンが更新され、パスワード管理を削減するシングル・サインオン環境の一部としての EIM のインプリメントについての資料を提供します。このトピックは、共通シングル・サインオン状況の詳細な多数のシナリオを、それらをインプリメントする詳細な構成指示とともに記載します。

新規箇所または変更箇所の見分け方

技術上の変更箇所を見分けるために、以下の情報を参考にしてください。

-  イメージは、新規または変更箇所の開始位置を示します。
-  イメージは、新規または変更箇所の終了位置を示します。

このリリースの新規または変更箇所についての他の情報は、 プログラム資料説明書を参照してください。

印刷可能な PDF

この情報を PDF で表示および印刷する場合に参照してください。

この文書の PDF 版を表示またはダウンロードするには、EIM (エンタープライズ識別マッピング) を選択します。

次の関連トピックを表示またはダウンロードできます。

- ネットワーク認証サービス (約 1070 KB) は、EIM と結合するネットワーク認証サービスを構成してシングル・サインオン環境を作成する方法について記載します。
- Directory Server (LDAP) (約 2015 KB) は、EIM ドメイン・コントローラーとして使用できる LDAP サーバーを構成する方法、 および拡張 LDAP 構成についての情報を記載します。

PDF ファイルの保管

表示または印刷のために PDF をワークステーションに保管するには、以下のようにします。

1. ブラウザーで PDF を右クリックする (リンク上で右クリック)。
2. PDF をローカルに保管するオプションをクリックする。
3. PDF を保存したいディレクトリーに進む。
4. 「**保存**」をクリックする。

Adobe Reader のダウンロード

これらの PDF を表示または印刷するには、システムに Adobe Reader がインストールされている必要があります。このアプリケーションは、Adobe Web サイト (www.adobe.com/products/acrobat/readstep.html) から無料でダウンロードできます。

EIM (エンタープライズ識別マッピング) の概要

ここでは、EIM (エンタープライズ識別マッピング) で解決できる問題や、現在の業界がそうした問題に対応する方法、さらには EIM の方法がより良い解決策である理由について知ることができます。

現在のネットワーク環境は、システムとアプリケーションの複合グループによって構成されているため、複数のユーザー・レジストリーを管理する必要があります。複数のユーザー・レジストリーを管理していると、すぐに管理上の大きな問題が発生し、ユーザーにも、管理者にも、アプリケーション開発者にも影響が出てきます。そのため、多くの企業では、システムやアプリケーションの権限と認証を安全に管理することが、大きな課題になっています。管理者やアプリケーション開発者がこの問題にできるだけ容易に、かつ低費用で対応するための IBM @server のインフラストラクチャー・テクノロジーが EIM です。

ここでは、この問題について説明し、現在の業界の対応策を概説し、EIM がより良いアプローチである理由を取り上げます。

複数のユーザー・レジストリーの管理に関する問題

多くの管理者は、さまざまなシステムやサーバーで構成されるネットワークを管理しており、それぞれのネットワークには、各種のユーザー・レジストリーによるユーザー管理の独特の方法があります。管理者はこのような複合のネットワークにおいて、各ユーザー ID とパスワードを複数のシステムで管理する責任があります。さらに、管理者がユーザー ID とパスワードを一致させなければならない場合も多く、ユーザーにとっても、 複数の ID とパスワードを覚えて一致させるという作業が必要になります。こうした環境では、ユーザーにも管理者にも、かなりの負担がかかります。したがって、管理者としては、企業システムを管理するというよりは、失敗ログオンのトラブルシューティングや、ユーザーが忘れたパスワードのリセットなどに貴重な時間を費やすことになります。

複数のユーザー・レジストリーを管理するという問題は、多層構造のアプリケーションや異機種混合のアプリケーションの開発者にも影響を与えます。そのような場合、顧客企業の重要なビジネス・データは、多種多様なシステムに分散しており、それぞれのシステムに独自のユーザー・レジストリーが存在しているという状況があります。したがって、開発者はアプリケーションの独自のユーザー・レジストリーと、関連するセキュリティー・セマンティクスを作成する必要があります。確かに、アプリケーション開発者の問題はこれで解決されますが、ユーザーと管理者の負担は増えてしまいます。

現在の®方法

現在の業界では、複数のユーザー・レジストリーを管理するいくつかの方法がありますが、どれも不十分です。 たとえば、Lightweight Directory Access Protocol (LDAP) は、分散ユーザー・レジストリーというソリューションを提供します。しかし、LDAP (または Microsoft® Passport などの他の一般的なソリューション) を使用すると、管理者は別のユーザー・レジストリーとセキュリティー・セマンティクスを管理する必要があるか、そうしたレジストリーを使用するようになっている既存のアプリケーションを取り替えなければなりません。

このタイプのソリューションを使用すると、管理者は個々のリソースに対して複数のセキュリティー・メカニズムを管理しなければならないため、管理上の負担は増大し、機密が漏れる可能性が高くなります。複数のメカニズムによって 1 つのリソースをサポートすると、1 つのメカニズムの権限だけを変更して、他のメカニズムの権限を変更するのを忘れる可能性も高くなります。たとえば、ユーザーが 1 つのインターフェースからのアクセスを拒否して、他のインターフェースからのアクセスを許可する場合は、結果として機密漏れが生じ得ます。

この作業を完了しても、問題が完全には解決されていないことに管理者は気付きます。一般に、企業は、現行のユーザー・レジストリーとセキュリティー・セマンティクスにあまりにも多額の投資をしてきたため

に、こうしたタイプのソリューションを採用するのが現実的でないという状況があります。別のユーザー・レジストリーと関連したセキュリティー・セマンティクスを作成すると、アプリケーション提供者の問題は解決されますが、ユーザーと管理者の問題は解決されません。

別の可能なソリューションは、シングル・サインオンという方法です。管理者がすべてのユーザー ID とパスワードを含むファイルを管理できるような製品もすでに出回っています。しかし、この方法にはいくつかの欠点があります。

- ユーザーが直面する 1 つの問題にしか対応しません。 ユーザーは 1 つの ID とパスワードを提供して複数のシステムにサインオンできますが、ユーザーが他のシステムのパスワードを所有して管理する必要があることに変わりはありません。
- こうしたファイルにはプレーン・テキストのパスワードや復号化可能なパスワードが格納されるため、機密漏れを生み、新たな問題を持ち込むことになります。もちろん、パスワードは、プレーン・テキスト・ファイルに保存するようなものではありませんし、管理者をはじめとするいかなるユーザーも簡単にアクセスできるようであってはならないはずです。
- この方法では、異機種混合の多層構造のアプリケーションを提供するサード・パーティーのアプリケーション開発者の問題は解決しません。サード・パーティーのアプリケーション開発者は、そうしたアプリケーション用に独自のユーザー・レジストリーを提供する必要があります。

こうした欠点があっても、複数のユーザー・レジストリーの問題がいくらか解消されるのは確かなので、この方法を採用した企業も存在します。

EIM の方法

EIM は、多層構造の異機種混合のアプリケーション環境で、複数のユーザー・レジストリーとユーザー ID をより簡単に管理するための低費用の構築ソリューションを提供する、新しい方法です。 EIM は、企業内の個人やエンティティー (ファイル・サーバーやプリント・サーバーなど) と、企業内でそうした個人やエンティティーを表す多くの ID との関係を記述するためのアーキテクチャーです。また、アプリケーションからそうした関係を確認するための API のセットも用意されています。

たとえば、あるユーザー・レジストリーにおいて指定された個人のユーザー ID に関して、別のユーザー・レジストリーでどのユーザー ID が同じ個人を表すのかを判別できます。 ユーザーが 1 つのユーザー ID ですでに認証され、 そのユーザー ID を別のユーザー・レジストリー内の適切な ID にマップできるのであれば、ユーザーは認証用の信任状を再び提供する必要はありません。このユーザーがだれであるかはすでにわかっているので、別のユーザー・レジストリーでそのユーザーがどのユーザー ID で表されているかということだけを知ればよいわけです。ですから、EIM は、企業の汎用の識別マッピング機能になります。

EIM では、1 対多のマッピングが可能です (つまり、1 人のユーザーが 1 つのユーザー・レジストリー内に 複数のユーザー ID を持つことも可能です)。しかし、管理者は、ユーザー・レジストリー内のすべてのユーザー ID に関する個々のマッピングを持っている必要はありません。また、EIM を使用すると、 多対 1 のマッピングも可能です (つまり、 複数のユーザーが 1 つのユーザー・レジストリー内の 1 つのユーザー ID にマップすることが可能です)。

ユーザーの ID を別個のユーザー・レジストリー間でマップする機能は、非常に便利です。 まず、アプリケーションで、権限用と認証用のユーザー・レジストリーがまったく別でもかまわないという柔軟性が得られます。たとえば、管理者は Kerberos レジストリー内の Windows® ユーザー ID を、別のユーザー・レジストリー内の i5/OS ユーザー・プロファイルにマップして、 i5/OS ユーザー・プロファイルが許可されている i5/OS リソースにアクセスすることができます。

EIM はオープン・アーキテクチャーなので、どのレジストリーの識別マッピングの関係でも表すことができます。既存のデータを新規リポジトリーにコピーして、両方を同期して保持する必要はありません。EIM が導入する唯一の新規データは、関係情報です。 EIM はこのデータを LDAP ディレクトリーで管理します。これにより、データを一元管理しながら、実際に情報を使用する場所でレプリカを保持するという柔軟性が得られます。よって、EIM では、企業やアプリケーション開発者がより多彩な環境でより少ない費用で簡単に作業するための柔軟性が得られるということになります。

EIM を i5/OS インプリメンテーションであるネットワーク認証サービス Kerberos と結合して使用すれば、シングル・サインオン・ソリューションを提供することになります。アプリケーションは、GSS API および EIM を使用して Kerberos チケットを受け入れて、異なるユーザー・レジストリー内の別の関連したユーザー ID にマップするように作成することができます。この ID マッピングを提供するユーザー ID 間のアソシエーションは、 EIM ID によって 1 つのユーザー ID を別のユーザー ID に間接的に関連付ける、 ID アソシエーションを作成することによって、またはグループ内の 1 つのユーザー ID を単一の特定のユーザー ID に直接的に関連付ける、ポリシー・アソシエーションを作成することによって、構築することができます。

識別マッピングを使用するには、管理者が以下を実行する必要があります。

1. ネットワーク内の EIM ドメインを構成する。 iSeries EIM 構成ウィザードを使用して、ドメインのドメイン・コントローラーを作成し、そのドメインへのアクセスを構成できます。このウィザードを使用して、新規 EIM ドメインを作成し、ローカルまたはリモート・システム上にドメイン・コントローラーを作成することを選択できます。または、EIM ドメインがすでに存在している場合には、既存の EIM ドメインに参加することを選択できます。
2. EIM ドメイン・コントローラーが構成されたシステム上のディレクトリー・サーバーに定義された、どのユーザーが EIM ドメイン内の特定の情報を管理またはアクセスするよう許可されているかを判別する。またそれらを適切な EIM アクセス制御グループに割り当てる。
3. EIM ドメインに参加するユーザー・レジストリーの EIM レジストリー定義を作成する。任意のユーザー・レジストリーを EIM ドメインに定義できますが、 EIM 対応のアプリケーションおよびオペレーティング・システムのユーザー・レジストリーを定義しなければなりません。
4. ユーザーの EIM インプリメンテーション要件を基に、EIM 構成を完了させるために以下のどのタスクを実行すべきかを判別する。
   - ドメイン内のそれぞれの固有ユーザーごとに EIM ID を作成し、それらの ID アソシエーションを作成する。
   - ポリシー・アソシエーションを作成する。
   - これらの組み合わせを作成する。

   関連情報

   Information Center のトピック「シングル・サインオン」

EIM (エンタープライズ識別マッピング) の概念

ここでは、EIM を正常にインプリメントするために理解しておくべき重要な EIM の概念について学びます。

各企業でエンタープライズ識別マッピング (EIM) を使用する方法を十分に理解するには、 EIM が動作する方法を概念的に理解することがまず必要です。 EIM API の構成およびインプリメンテーションは、サーバー・プラットフォームによって異なる可能性がありますが、EIM の概念は、 すべての IBM @server プラットフォームで共通です。

図 1 は、企業内の EIM インプリメンテーションの例です。 3 台のサーバーが EIM クライアントとして稼働しており、それらのサーバーには、EIM ルックアップ操作によって EIM データを要求する EIM 対応のアプリケーションが含まれています。 6 ドメイン・コントローラー 1 には、EIM ドメイン 2 に関する情報が保管され、EIM ドメインには EIM ID 3 、EIM ID とユーザー ID との間のアソシエーション 4 、および EIM レジストリー定義 5 が含まれます。

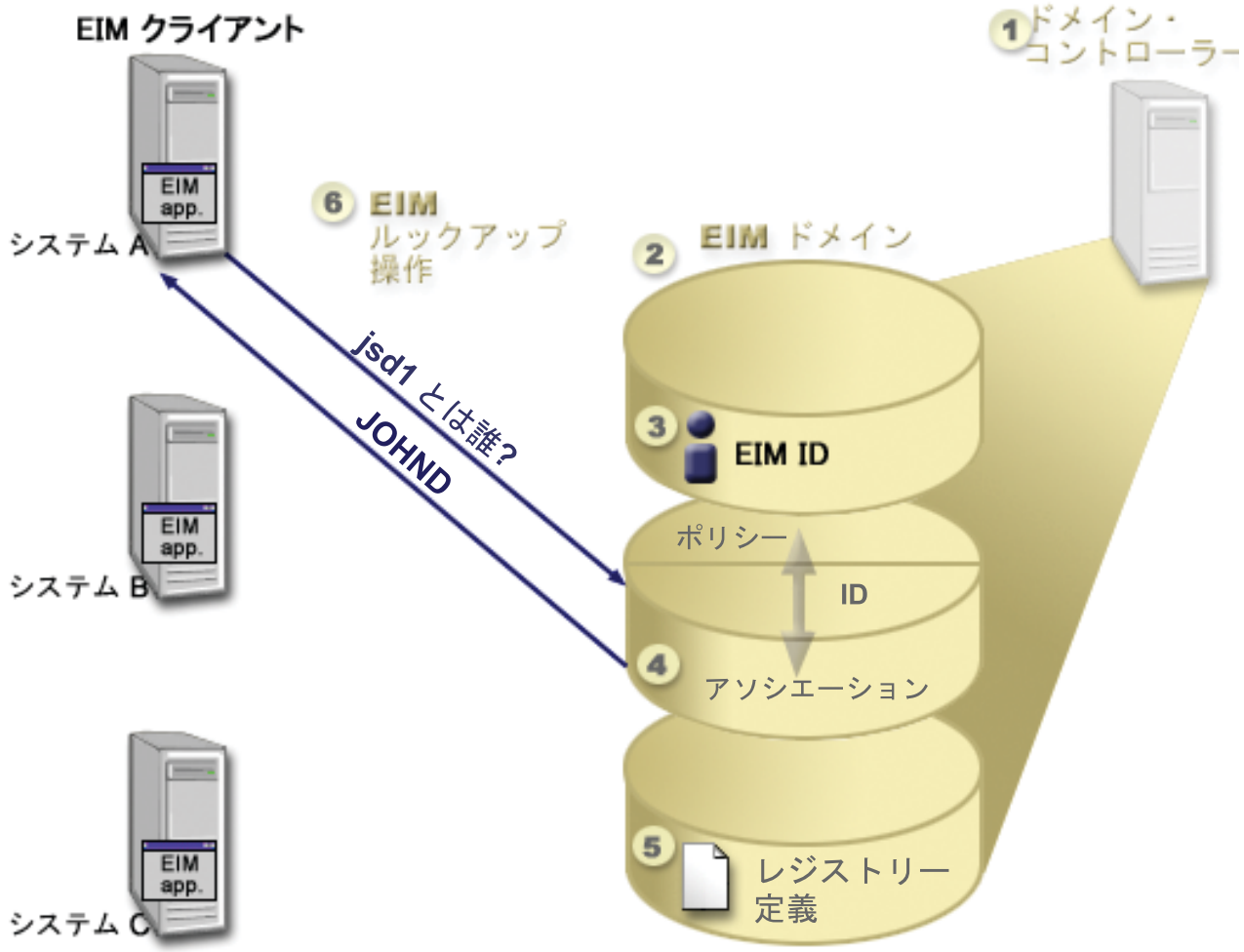


図 1. EIM インプリメンテーションの例

以下の情報を参照して、EIM @server の概念の詳細について確認してください。

関連概念

52 ページの『EIM 用の LDAP の概念』
ここでは、Lightweight Directory Access Protocol (LDAP) を EIM (エンタープライズ識別マッピング) と一緒に使用する方法を説明します。

55 ページの『EIM (エンタープライズ識別マッピング) 用の iSeries の概念』
ここでは、EIM (エンタープライズ識別マッピング) のすべてのアプリケーションをリストします。

EIM ドメイン・コントローラー

ここでは、EIM (エンタープライズ識別マッピング) ドメイン・コントローラーを使用する理由を説明します。

EIM ドメイン・コントローラー は、 1 つ以上の EIM ドメインを管理するために構成された、Lightweight Directory Access Protocol (LDAP) サーバーです。 *EIM ドメイン* は、すべての EIM ID、EIM アソシエーション、およびそのドメインで定義されたユーザー・レジストリーから構成される LDAP ディレクトリーです。 システム (EIM クライアント) は、EIM ルックアップ操作用のドメイン・データを使用して EIM ドメインに参加します。

現在、一部の IBM @server プラットフォーム上の IBM Directory Server を、 EIM ドメイン・コントローラーとして機能するように構成できます。EIM API をサポートするシステムは、クライアントとしてドメインに参加できます。こうしたクライアント・システムは、EIM API を使用して、EIM ドメイン・コントローラーに接続し、 30 ページの『EIM ルックアップ操作』を実行します。 EIM クライアントの位置により、 EIM ドメイン・コントローラーがローカルかリモート・システムかが決まります。 EIM クライアントがドメイン・コントローラーと同一のシステムで稼働している場合には、ドメイン・コントローラーは*ローカル* になります。 EIM クライアントがドメイン・コントローラーとは別のシステムで稼働している場合は、ドメイン・コントローラーはリモート になります。

注 : ディレクトリー・サーバーをリモート・システム上に構成する場合には、そのディレクトリー・サーバーは EIM サポートを提供しなければなりません。 EIM は、ドメイン・コントローラーが、Lightweight Directory Access Protocol (LDAP) バージョン 3 をサポートするディレクトリー・サーバーによってホスティングされることを必要とします。さらに、ディレクトリー・サーバー・プロダクトは、 EIM スキーマを受け入れるように構成しなければなりません。 IBM Directory Server for iSeries および IBM Directory Server V5.1 がこのサポートを提供します。

EIM ドメイン

ここでは、ドメインを使用してすべての ID を保管する方法を説明します。

EIM (エンタープライズ識別マッピング) *ドメイン* は、企業の EIM データを含む Lightweight Directory Access Protocol (LDAP) サーバー内のディレクトリーです。 EIM ドメインは、すべての EIM ID、EIM アソシエーション、およびそのドメインで定義されているユーザー・レジストリー、さらにはデータに対するアクセス制御を含みます。システム (EIM クライアント) は、 EIM ルックアップ操作用のドメイン・データを使用してドメインに参加します。

EIM ドメインはユーザー・レジストリーとは異なります。ユーザー・レジストリーは、オペレーティング・システムやアプリケーションの特定のインスタンスに識別され、信頼されているユーザー ID の集合を定義します。またユーザー・レジストリーには、ユーザーの ID を認証するのに必要な情報が含まれます。さらに、多くの場合、ユーザー・レジストリーには、ユーザー設定、システム特権、その ID の個人情報などの属性も含まれます。

それとは対照的に、EIM ドメインは、ユーザー・レジストリーに定義されているユーザー ID を*参照* します。 EIM ドメインには、種々のユーザー・レジストリー (ユーザー名、レジストリー・タイプ、レジストリー・インスタンス) 内の ID と、 その ID が表している実際の個人やエンティティーとの間の*関係* についての情報が含まれます。

図 2 は、EIM ドメインに保管されているデータを示しています。このデータには、EIM ID、EIM レジストリー定義、EIM アソシエーションが含まれています。 EIM データは、ユーザー ID と企業内でこうした ID が表している個人やエンティティーとの間の関係を定義します。

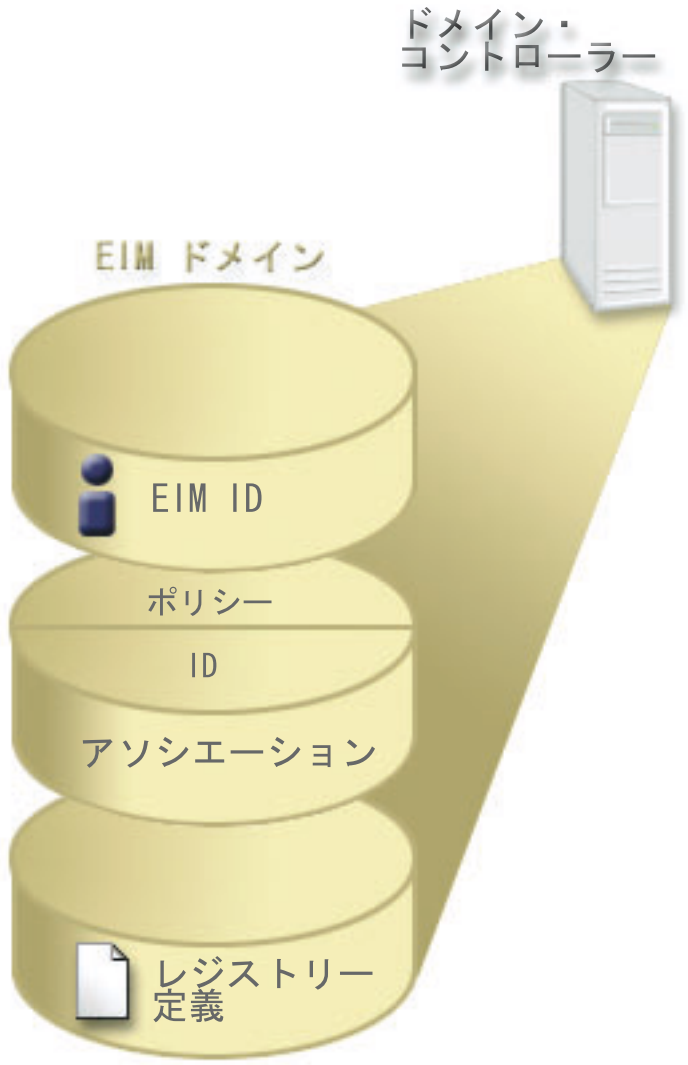


図 2. EIM ドメインおよびドメイン内に保管されているデータ

EIM データには、以下のものが含まれます。

EIM レジストリー定義
作成する各 EIM レジストリー定義は、企業内のシステム上に存在する実際のユーザー・レジストリー (およびそれに含まれるユーザー ID 情報) を表しています。EIM で特定のユーザー・レジストリーを定義すると、そのユーザー・レジストリーは EIM ドメインに参加できます。作成することのできるレジストリー定義には、2 つのタイプがあります。 1 つは、システム・ユーザー・レジストリーを参照するもので、もう 1 つは、アプリケーション・ユーザー・レジストリーを参照するものです。

EIM ID
作成する各 EIM ID は、 企業内の個人またはエンティティー (プリント・サーバーやファイル・

サーバーなど) を一意的に表します。EIM ID が対応する人またはエンティティーに属するユーザー ID 間の 1 対 1 のマッピングが必要な場合には、 EIM ID を作成できます。

EIM アソシエーション

作成する EIM アソシエーションは、 ユーザー ID 間の関係を表します。EIM クライアントが EIM API を使用して EIM ルックアップ操作を正常に実行できるようにするためには、アソシエーションを定義しなければなりません。こうした EIM ルックアップ操作は、EIM ドメインで定義されたアソシエーションを検索します。作成できるアソシエーションには、2 つの異なるタイプがあります。

ID アソシエーション

ID アソシエーションでは、 個人に定義された EIM ID を使用して、ユーザー ID 間の 1 対 1 の関係を定義できます。 作成する各 EIM ID アソシエーションは、EIM ID と企業内の関連したユーザー ID との間の、単一で特定の関係を表します。 ID アソシエーションは、EIM ID を特定のユーザー・レジストリー内の特定のユーザー ID と結び付ける情報を提供し、 ユーザーに関する 1 対 1 の ID マッピングを作成できるようにします。 ID アソシエーションが特に役立つのは、個々の人が特殊権限およびその他の特権を持つユーザー ID を持っており、 それらのユーザー ID 間の 1 対 1 のマッピングを作成することによって、それらを個別に制御したい場合です。

ポリシー・アソシエーション

ポリシー・アソシエーションでは、 1 つ以上のユーザー・レジストリー内のユーザー ID のグループと、別のユーザー・レジストリー内の個々のユーザー ID との間の関係を定義できます。作成する各 EIM ポリシー・アソシエーションにより、 1 つのユーザー・レジストリー内のユーザー ID のソース・グループと、単一のターゲット・ユーザー ID との間の、 多対 1 のマッピングが作成されます。一般に、同じレベルの権限を必要とするユーザーのグループを、そのレベルの権限を持つ単一ユーザー ID にマップする、ポリシー・アソシエーションを作成します。

関連概念

12 ページの『EIM レジストリー定義』
ここでは、レジストリー定義を作成して、システムのすべてのユーザー・レジストリーを保持する方法を説明します。

『EIM ID』
ここでは、企業内のユーザーまたはエンティティーに対して ID を作成する方法を説明します。

30 ページの『EIM ルックアップ操作』
ここでは、EIM (エンタープライズ識別マッピング) のプロセスおよび図で示された例を説明します。

EIM ID

ここでは、企業内のユーザーまたはエンティティーに対して ID を作成する方法を説明します。

EIM (エンタープライズ識別マッピング) *ID* は、企業内の個人やエンティティーを表します。一般的なネットワークは、種々のハードウェア・プラットフォームおよびアプリケーション、またそれらに関連付けられたユーザー・レジストリーから構成されています。ほとんどのプラットフォームや多くのアプリケーションでは、プラットフォーム固有の、またはアプリケーション固有のユーザー・レジストリーが使用されています。こうしたユーザー・レジストリーには、このようなサーバーまたはアプリケーションを使用するユーザーのユーザー識別情報が含まれます。

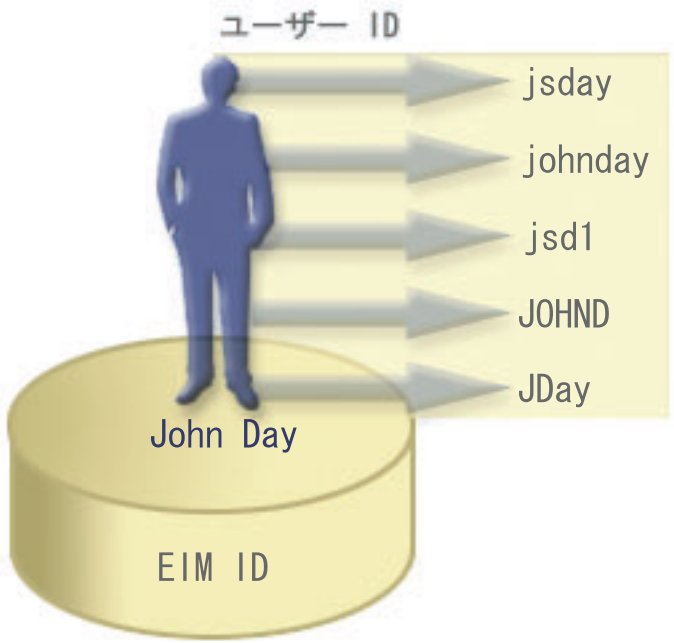
EIM を使用して、企業内の個人やエンティティーに対して固有の EIM ID を作成できます。 その後、EIM ID、および EIM ID が表す個人またはエンティティーのさまざまなユーザー ID との間で ID アソシ

エーション、 すなわち 1 対 1 の ID マッピングを作成できます。このプロセスは、異機種混合の多層構造アプリケーションの構築を簡単にします。また企業内の個人やエンティティーが持つすべてのユーザー ID の管理を含めた管理業務を、より簡単にするツールを構築して使用するのが容易になります。

個人を表す EIM ID

図 3 は企業内の *John Day* という名前の個人を表す EIM ID、およびその種々のユーザー ID の例を示しています。この例では、*John Day* は 5 つのユーザー ID (johnday、jsd1、 JOHND、jsday、および JDay) を、 4 つの別個のユーザー・レジストリーに有しています。

図 3: *John Day* の EIM ID とその種々のユーザー ID との間の関係

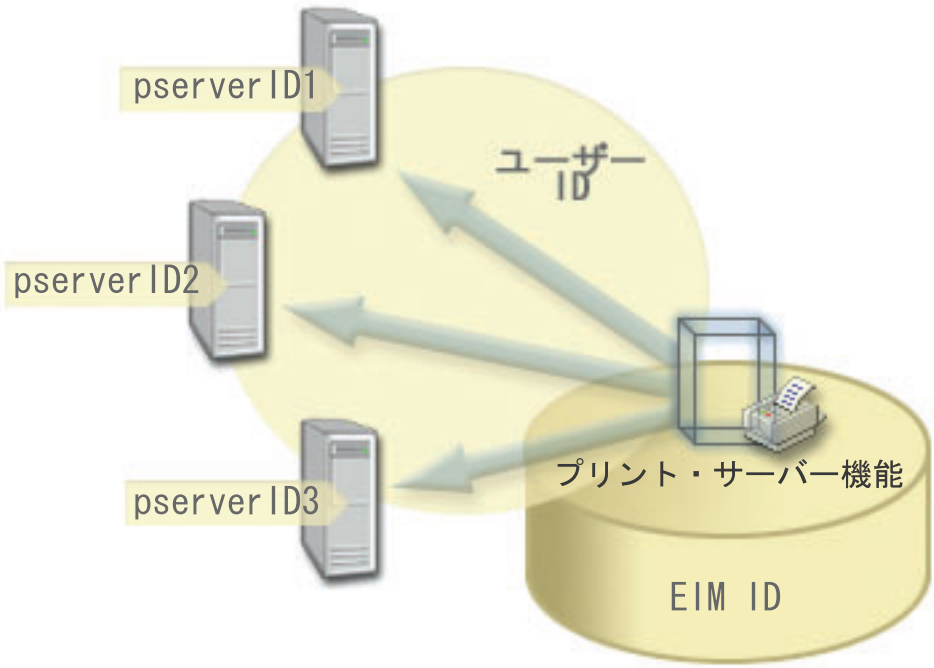


EIM では、John Day ID と *John Day* の異なるそれぞれのユーザー ID との間の関係を定義するアソシエーションを作成できます。こうしたアソシエーションを作成してその関係を定義すると、識別されているユーザー ID に基づいて、不明なユーザー ID を EIM API からルックアップするアプリケーションを、管理者やユーザーが作成できるようになります。

エンティティーを表す EIM ID

ユーザーを表すだけでなく、図 4 に示されているように、EIM ID は企業内のエンティティーを表すこともできます。たとえば、企業内のプリント・サーバー機能は、多くの場合、複数のシステム上で稼働しています。図 4 では、企業内のプリント・サーバー機能は、それぞれ pserverID1、pserverID2、および pserverID3 という異なるユーザー ID を持つ別個の 3 つのシステム上で実行されています。

図 4: プリント・サーバー機能を表す EIM ID とその機能の様々なユーザー ID との間の関係



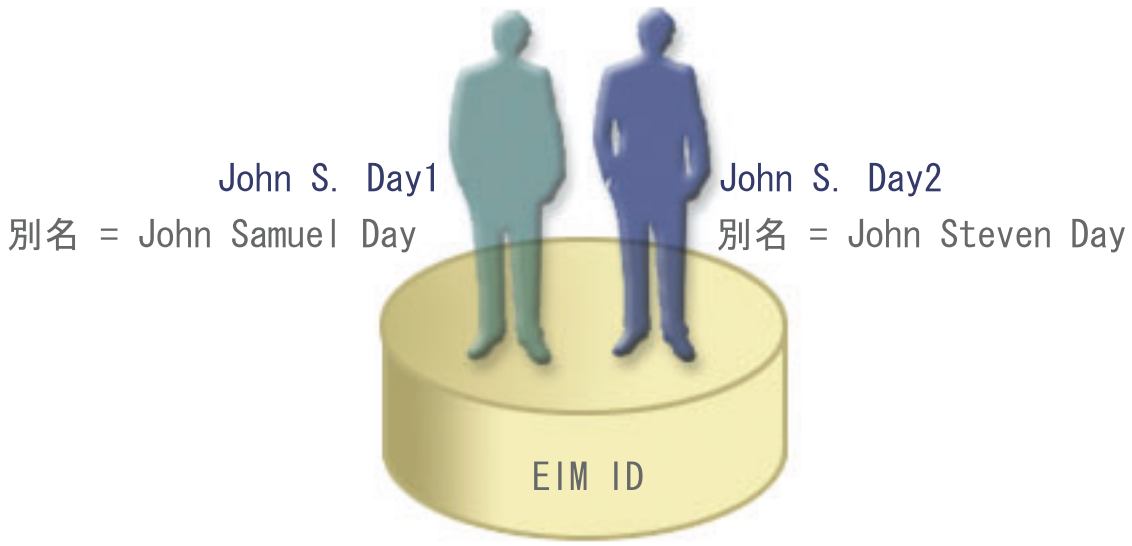
EIM を使用すると、そのプリント・サーバー機能を企業内全体で表す単一の ID を作成できます。 例の示すように、EIM ID プリント・サーバー機能は、企業内における実際のプリント・サーバー機能というエンティティーを表します。アソシエーションを作成して、 EIM ID (プリント・サーバー機能) とこの機能のそれぞれのユーザー ID (pserverID1、pserverID2、および pserverID3) との間の関係を定義します。こうしたアソシエーションによって、アプリケーション開発者は、EIM ルックアップ操作を使用して特定のプリント・サーバー機能を検出できます。それでアプリケーション提供者は、プリント・サーバー機能を企業内でより簡単に管理できる分散アプリケーションを作成できます。

EIM ID および別名の作成

EIM ID 名は EIM ドメイン内で固有でなければなりません。別名は、固有の ID の使用が難しいという状況で有効です。 EIM ID 別名が有用な例として、ある人物の本名が、知られている名前と異なる場合があります。たとえば、企業内の別個の人物が同じ名前であることがあり、その場合、その名前を EIM ID として使用するならば、混乱が生じる可能性があります。

図 5 は、企業内に *John S. Day* という名前の 2 人のユーザーがいるという例を示しています。 EIM 管理者は 2 つの異なる EIM ID John S. Day1 と John S. Day2 を作成して、 2 人を識別します。しかし、それぞれの ID によって表されているのがどちらの *John S. Day* かはすぐには分かりません。

図 5: 共有する *John S. Day* という正式な名前に基づく 2 つの EIM ID の別名



別名を使用すると、 EIM 管理者はそれぞれの EIM ID の個人に関する追加情報を設定できます。 EIM ID はそれぞれ複数の別名を持つことができ、EIM ID が表している *John S. Day* を識別することができます。たとえば、追加の別名には、それぞれのユーザーの従業員番号、部門番号、役職、あるいは区別するための他の属性を含めることが考えられます。この例では、`John S. Day1` の別名は `John Samuel Day`、 `John S. Day2` の別名は `John Steven Day` となるかもしれません。

別名情報を使用すれば、特定の EIM ID を探し出すのに役立ちます。 たとえば、EIM を使用するアプリケーションは、アプリケーションの適切な EIM ID を検出するために使用する別名を指定できます。管理者はこの別名を EIM ID に追加して、アプリケーションが EIM 操作のために固有 ID ではなく別名を使用できるようにすることができます。アプリケーションは、ID からの EIM ターゲット ID の取得 (`eimGetTargetFromIdentifier()`) API を使用して EIM ルックアップ操作を実行し、それが必要とする適切なユーザー ID を検出する際に、この情報を指定できます。

関連概念

7 ページの『EIM ドメイン』
ここでは、ドメインを使用してすべての ID を保管する方法を説明します。

EIM レジストリー定義

ここでは、レジストリー定義を作成して、システムのすべてのユーザー・レジストリーを保持する方法を説明します。

EIM (エンタープライズ識別マッピング) *レジストリー定義* は、企業内のシステムに存在する実際のユーザー・レジストリーを表す、 EIM 内に作成される項目です。ユーザー・レジストリーはディレクトリーのように操作でき、特定のシステムやアプリケーションの有効なユーザー ID のリストが含まれています。基本ユーザー・レジストリーには、ユーザー ID およびパスワードが含まれます。ユーザー・レジストリーの一例としては、z/OS® Security Server Resource Access Control Facility (RACF®) レジストリーがあります。ユーザー・レジストリーには、他の情報も含めることができます。たとえば、Lightweight Directory Access Protocol (LDAP) ディレクトリーには、LDAP に保管されているデータに対するバインド識別名、パスワード、およびアクセス制御が含まれます。一般的なユーザー・レジストリーの他の例には、Kerberos レルム内のプリンシパルまたは Windows Active Directory ドメイン内のユーザー ID、i5/OS ユーザー・プロファイル・レジストリーがあります。

他のユーザー・レジストリーに存在するユーザー・レジストリーも定義できます。アプリケーションの中には、ユーザー・レジストリーの単一インスタンス内でユーザー ID のサブセットを使用するものがあります。たとえば、z/OS Security Server (RACF) レジストリーに、 全体の RACF ユーザー・レジストリー内のユーザーのサブセットである特定のユーザー・レジストリーを含めることができます。

EIM レジストリー定義は、企業内のこうしたユーザー・レジストリーに関する情報を提供します。管理者は、以下の情報を提供して EIM に対してこのようなレジストリーを定義します。

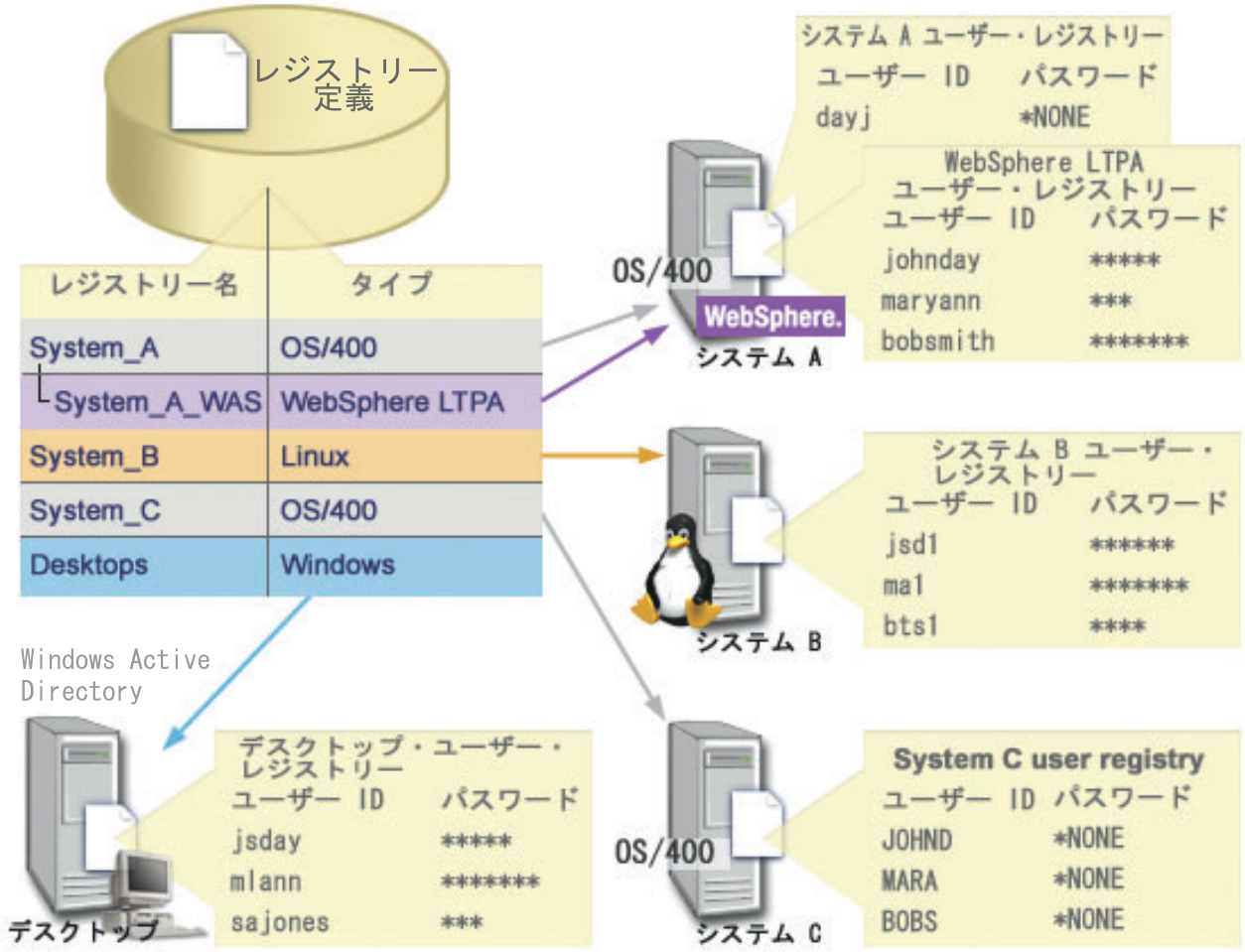
- 固有で、任意の EIM レジストリー名レジストリー定義は、ユーザー・レジストリーの特定のインスタンスをそれぞれ表します。したがって、ユーザー・レジストリーの特定のインスタンスを識別するのに役立つ EIM レジストリー定義を選択しなければなりません。たとえば、システム・ユーザー・レジストリーに対しては TCP/IP ホスト名を選択できますし、アプリケーション・ユーザー・レジストリーに対してはそのアプリケーションの名前と組み合わせたホスト名を選択できます。任意の英数字、英大文字小文字混合の文字、およびスペースを使用して、固有の EIM レジストリー定義名を作成できます。
- ユーザー・レジストリーのタイプほとんどのオペレーティング・システム・ユーザー・レジストリーをカバーする、EIM が提供する多数の事前定義されたユーザー・レジストリー・タイプがあります。それらには以下のものがあります。
  - AIX®
  - Domino® - ロング・ネーム
  - Domino - ショート・ネーム
  - Kerberos
  - Kerberos - ケース・センシティブ
  - LDAP
  - - LDAP - ショート・ネーム
  - Linux®
  - Novell Directory Server
  - - その他
  - - その他 - ケース・センシティブ
  - i5/OS (または OS/400®)
  - Tivoli® Access Manager
  - RACF
  - Windows - ローカル
  - Windows ドメイン (Kerberos) (このタイプはケース・センシティブです)
  - X.509

  注: 事前定義レジストリー定義タイプは、ほとんどのオペレーティング・システム・ユーザー・レジストリーをカバーしていますが、 EIM に事前定義レジストリー・タイプが含まれていないレジストリー定義を作成する必要があることもあります。この状況では、2 つのオプションがあります。ユーザー・レジストリーの特性に一致する既存のレジストリー定義を使用するか、または専用ユーザー・レジストリー・タイプの定義を行うことができます。たとえば、図 6 では、処理を行う管理者は、`System_A_WAS` アプリケーション・レジストリー定義のレジストリー・タイプとして、 `WebSphere LTPA` を必要とし、定義しています。

図 6 では、管理者は、システム A、システム B、システム C、およびユーザーがデスクトップ・ワークステーションにログオンする際に使用する Kerberos プリンシパルを含む Windows Active Directory を表すユーザー・レジストリーに対して、EIM システム・レジストリー定義を作成しています。さらに、管理者

はシステム A 上で実行している WebSphere® (R) Lightweight Third-Party Authentication (LTPA) 用のアプリケーション・レジストリー定義を作成しています。管理者が使用するレジストリー定義名は、そのタイプのユーザー・レジストリーの特定のオカレンスを識別するのに役立ちます。多くのタイプのユーザー・レジストリーでは、IP アドレスまたはホスト名で十分です。この例では、管理者はアプリケーション・レジストリー定義名として System_A_WAS を使用して、 WebSphere LTPA アプリケーションのこの特定のインスタンスを識別します。また、アプリケーション・レジストリー定義の親システム・レジストリーが、System_A レジストリーであることを指定しています。

図 6: 企業内の 5 つのユーザー・レジストリーの EIM レジストリー定義



注: ユーザー・パスワードを管理する必要をさらに削減するため、図 6 の管理者は、 システム A および System C 上の i5/OS ユーザー・プロファイル・パスワードを *NONE に設定しています。この例の管理者は、シングル・サインオン環境を構成しており、ユーザーは、iSeries ナビゲーターなどの EIM 対応アプリケーションのみを処理します。したがって管理者は、ユーザーも管理者もより少ないパスワードを管理すればよいように、 i5/OS ユーザー・プロファイルからパスワードを除去することを考えています。

関連概念

7 ページの『EIM ドメイン』
ここでは、ドメインを使用してすべての ID を保管する方法を説明します。

システム・レジストリー定義

ここでは、特定のシステムにユーザー・レジストリーを作成する方法について学習します。

システム・レジストリー定義は、ワークステーションまたはサーバー内で別個のユーザー・レジストリーを表してそれを記述する、ユーザーが EIM (エンタープライズ識別マッピング) 内に作成する項目です。ユーザー・レジストリーに対して EIM システム・レジストリー定義を作成できるのは、企業内のレジストリーに以下の特色のいずれかが当てはまる場合です。

- レジストリーが、 AIX、 i5/OS といったオペレーティング・システム、 または z/OS Security Server Resource Access Control Facility (RACF) のようなセキュリティー管理プロダクトによって提供されている場合。
- レジストリーに、Lotus Notes® のようなアプリケーションに対する、固有のユーザー ID が含まれている場合。
- レジストリーに、Kerberos プリンシパルまたは Lightweight Directory Access Protocol (LDAP) 識別名のように、 配布されたユーザー ID が含まれている場合。

EIM ルックアップ操作は、EIM 管理者がレジストリーをシステムまたはアプリケーションのどちらに定義するかに関係なく、正常に実行されます。ただし、別個のレジストリー定義を準備しておけば、マッピング・データをアプリケーション・ベースで管理できます。アプリケーション固有のマッピングを管理する責任は、特定のレジストリーの管理者に割り当てられます。

アプリケーション・レジストリー定義

ここでは、特定のアプリケーションに対してユーザー・レジストリーを作成する方法を学習します。

アプリケーション・レジストリー定義は、EIM (エンタープライズ識別マッピング) 内に作成する、システム・レジストリー内に定義されたユーザー ID のサブセットを記述して表す項目です。これらのユーザー ID は、特定のアプリケーションまたはアプリケーション・セットを使用できるようにする共通の属性または特性のセットを共用します。アプリケーション・レジストリー定義は、他のユーザー・レジストリー内に存在するユーザー・レジストリーを表します。たとえば、z/OS Security Server (RACF) レジストリーに、全体の RACF ユーザー・レジストリー内のユーザーのサブセットである特定のユーザー・レジストリーを含めることができます。この関係のゆえに、作成するアプリケーション・レジストリー定義の親システム・レジストリーの名前を指定する必要があります。

ユーザー・レジストリーに対して EIM アプリケーション・レジストリー定義を作成できるのは、レジストリー内のユーザー ID が、以下の特色を持っている場合です。

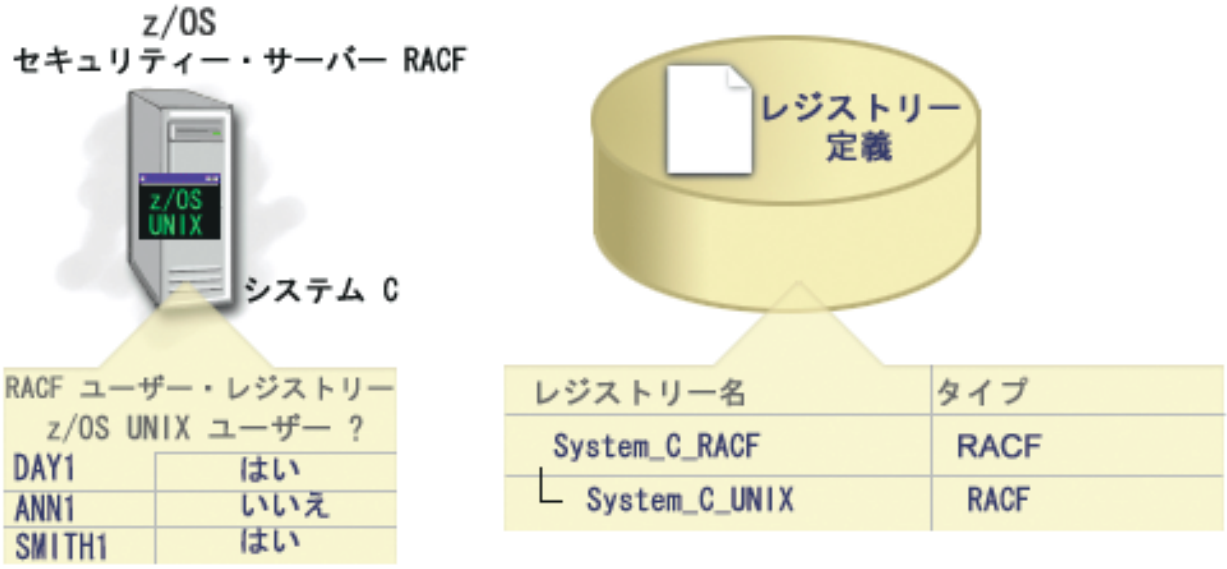
- アプリケーションのユーザー ID が、そのアプリケーション特有のユーザー・レジストリー内に保管されていない場合。
- アプリケーションのユーザー ID が、他のアプリケーションのユーザー ID があるシステム・レジストリー内に保管されている場合。

EIM 管理者がユーザー・レジストリーに対してアプリケーション・レジストリー定義またはシステム・レジストリー定義のどちらを作成するかにかかわりなく、EIM ルックアップ操作は正常に実行されます。ただし、別個のレジストリー定義を準備しておけば、マッピング・データをアプリケーション・ベースで管理できます。アプリケーション固有のマッピングを管理する責任は、特定のレジストリーの管理者に割り当てられます。

たとえば、図 7 では、ある EIM 管理者が z/OS Security Server RACF レジストリーを表すシステム・レジストリー定義をどのように作成したかが示されています。この管理者は、z/OS(TM) UNIX® System Services (z/OS UNIX) を使用する RACF レジストリー内のユーザー ID を表すアプリケーション・レジス

トリー定義も作成しました。システム C には、DAY1、ANN1、SMITH1 といった 3 つのユーザー ID に関する情報を含む RACF ユーザー・レジストリーが含まれています。これらユーザー ID のうちの 2 つ (DAY1 および SMITH1) は、システム C 上で z/OS UNIX にアクセスします。 これらのユーザー ID は、実際には、このユーザー ID を z/OS UNIX ユーザーとして識別する固有の属性を持った RACF ユーザーです。EIM 管理者は、EIM レジストリー定義内で、RACF ユーザー・レジストリーの概要を表す System_C_RACF を定義しました。また、この管理者は、z/OS UNIX 属性を持つユーザー ID を表す System_C_UNIX も定義しています。

図 7: RACF ユーザー・レジストリーおよび z/OS UNIX ユーザーのための EIM レジストリー定義



グループ・レジストリー定義

ここでは、レジストリー定義のグループを説明し、表す EIM ドメイン内での、グループ・レジストリー定義の作成について学習します。

論理的にレジストリー定義をグループ化すると、EIM マッピングを構成するために実行すべき作業の量を削減することができます。個々のレジストリー定義を管理するのと同じような方法で、グループ・レジストリー定義を管理できます。

グループ・レジストリー定義のすべてのメンバーには通常、ターゲットまたはソース・アソシエーションの作成先にするための最低 1 つの共通ユーザー ID があります。メンバーを一緒にグループ化することにより、グループ・レジストリー定義およびユーザー ID に対して、複数のアソシエーションではなく 1 つのアソシエーションだけを作成することができます。

たとえば、John Day はユーザー ID jday を使用して自分の 1 次システムにログオンし、同じユーザー ID JOHND を複数のシステム上で使用します。したがって、各システムのユーザー・レジストリーにはユーザー ID JOHND が入っています。通常、John Day は EIM ID John Day から、ユーザー ID JOHND を持つ個々のユーザー・レジストリーごとに別個のターゲット・アソシエーションを作成します。EIM マッピングを構成するために実行すべき作業の量を削減するため、ユーザー ID JOHND をグループのメンバーとして保持するすべてのユーザー・レジストリーを使って 1 つのグループ・レジストリー定義を作成できます。その後、EIM ID John Day から個々のレジストリー定義ごとに複数のターゲット・アソシエーション

を作成するのではなく、EIM ID John Day からグループ・レジストリー定義に対して単一のターゲット・アソシエーションを作成できます。グループ・レジストリー定義に対する、この単一のターゲット・アソシエーションにより、John Day のユーザー ID jday をユーザー ID JOHND にマップすることができます。

グループ・レジストリー定義に関する以下の情報をお読みください。

- グループ・レジストリー定義のすべてのメンバー (個々のレジストリー定義) の大/小文字の区別は、同じでなければなりません。
- グループ・レジストリー定義のすべてのメンバー (個々のレジストリー定義) は、グループ・レジストリー定義に追加される前に、EIM ドメインで定義することが必要です。
- レジストリー定義は複数のグループのメンバーになることができますが、個々のユーザー・レジストリーを複数のグループ・レジストリー定義のメンバーとして指定すると、ルックアップ操作があいまいな結果を戻す可能性があるので避けてください。グループ・レジストリー定義は、別のグループ・レジストリー定義のメンバーになることはできません。

EIM アソシエーション

ここでは、異なるユーザー・レジストリー内で ID の関連付けを使用する方法を説明します。

EIM (エンタープライズ識別マッピング) アソシエーション は、異なるユーザー・レジストリー内のユーザー ID 間の関係を定義するために、 EIM ドメイン内に作成する項目です。作成するアソシエーションのタイプは、定義される関係が直接的か間接的かを指定します。 EIM には 2 つのタイプのアソシエーション、 すなわち ID アソシエーションおよびポリシー・アソシエーションのうちの 1 つを作成できます。ポリシー・アソシエーションは ID アソシエーションの代わりに、またはそれと組み合わせて使用できます。アソシエーションをどのように使用するかは、全体的な EIM インプリメンテーション計画に依存しています。

アソシエーションの処理について詳しくは、以下の情報で確認してください。

ルックアップ情報

ここでは、このオプショナル・データを使用して、ターゲット・ユーザー ID をさらに識別する方法を学習します。 そのようにして識別されたターゲット・ユーザー ID は、EIM (エンタープライズ識別マッピング) API がマッピング・ルックアップ操作時に使用して、 操作の対象となるターゲット・ユーザー ID の検索を、さらに絞り込めます。

本リリースでは、ターゲット・ユーザー ID をさらに識別するための、ルックアップ情報と呼ばれるオプショナル・データを提供できるようになりました。このターゲット・ユーザー ID は、ID アソシエーションまたはポリシー・アソシエーションのどちらででも指定できます。ルックアップ情報は、eimGetTargetFromSource EIM API または eimGetTargetFromIdentifier EIM API のどちらかがマッピング・ルックアップ操作時に使用して、操作の対象となるターゲット・ユーザー ID の検索をさらに絞り込める、固有の文字ストリングです。ルックアップ情報に指定するデータは、これらの EIM API のレジストリー・ユーザー追加情報パラメーターに対応します。

ルックアップ情報が必要なのは、マッピング・ルックアップ操作が、複数のターゲット・ユーザー ID を戻す可能性がある場合に限られます。マッピング・ルックアップ操作は、以下の状況の 1 つ以上が存在する場合に、複数のターゲット・ユーザー ID を戻す可能性があります。

- EIM ID が、同一のターゲット・レジストリーに対して、複数のターゲット・アソシエーションを持っている場合。

- 複数の EIM ID が、ソース・アソシエーション内に同じユーザー ID を指定しており、 かつ、これらの EIM ID が、同一のターゲット・レジストリーに対してターゲット・アソシエーションを持つ場合 (それぞれのターゲット・アソシエーションに指定されたユーザー ID は異なっているかもしれない)。
- 複数のデフォルトのドメイン・ポリシー・アソシエーションが、同一のターゲット・レジストリーを指定する場合。
- 複数のデフォルトのレジストリー・ポリシー・アソシエーションが、同一のソース・レジストリーおよび同一のターゲット・レジストリーを指定する場合。
- 複数の証明書フィルター・ポリシー・アソシエーションが、同一のソース X.509 レジストリー、証明書フィルター、およびターゲット・レジストリーを指定する場合。

注: マッピング・ルックアップ操作が複数のターゲット・ユーザー ID を戻す場合、 i5/OS アプリケーションおよびプロダクトを含め、そのようなあいまいな結果を処理するようには設計されていない EIM 対応アプリケーションで問題が生じる可能性があります。ただし、iSeries Access for Windows などの基本 i5/OS アプリケーションは、ルックアップ情報を使用して、ルックアップ操作によって戻された複数のターゲット・ユーザー ID を区別することはできません。したがって、ドメインに対するアソシエーションを再定義して、マッピング・ルックアップ操作が単一のターゲット・ユーザー ID を戻すことができるようにし、 基本 i5/OS アプリケーションが正常にルックアップ操作を実行して ID をマップできるようにする必要があるかもしれません。

ルックアップ情報を使用して、マッピング・ルックアップ操作が複数のターゲット・ユーザー ID を戻す可能性がある状況を避けることができます。マッピング・ルックアップ操作が複数のターゲット・ユーザー ID を戻すのを避けるには、各アソシエーションのそれぞれのターゲット・ユーザー ID ごとに、固有のルックアップ情報を定義しなければなりません。このルックアップ情報をマッピング・ルックアップ操作に提供して、操作が固有のターゲット・ユーザー ID を確実に戻すことができるようにしなければなりません。そうしなければ、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。

たとえば、システム A 上に 2 つのユーザー・プロファイルを持つ John Day という名の EIM ID があるとします。2 つのユーザー・プロファイルのうちの 1 つは、システム A 上の JDUSER、もう 1 つは、セキュリティー管理者特殊権限がある JDSECADM です。 John Day ID には 2 つのターゲット・アソシエーションがあります。その 1 つはターゲット・レジストリー System_A 内の JDUSER ユーザー ID に対するもので、ルックアップ情報として JDUSER に指定された user authority を指定しています。 もう 1 つのターゲット・アソシエーションは、ターゲット・レジストリー System_A 内の JDSECADM ユーザー ID に対するもので、ルックアップ情報として JDSECADM に指定されたsecurity officer を指定しています。

マッピング・ルックアップ操作がルックアップ情報を指定しない場合には、ルックアップ操作が JDUSER および JDSECADM の両方のユーザー ID を戻します。マッピング・ルックアップ操作がルックアップ情報として user authority を指定する場合には、ルックアップ操作は JDUSER ユーザー ID だけを戻します。マッピング・ルックアップ操作がルックアップ情報として security officer を指定する場合には、 ルックアップ操作は JDSECADM ユーザー ID だけを戻します。

注: ユーザー ID の最後のターゲット・アソシエーション (ID アソシエーションまたはポリシー・アソシエーションのどちらでも可) を削除すると、 ターゲット・ユーザー ID およびすべてのルックアップ情報もドメインから削除されます。

さまざまな重複した方法で証明書ポリシー・アソシエーションおよびその他のアソシエーションを使用できるので、証明書ポリシー・アソシエーションを作成および使用する前に、 EIM マッピング・ポリシー・サポートやルックアップ操作の動作の両方を、よく理解しておく必要があります。

ID アソシエーション

ここでは、EIM (エンタープライズ識別マッピング) ID およびその人物を表すユーザー・レジストリー内のユーザー ID との間の関係を記述する、 ID アソシエーションの使用法を学習します。 ID アソシエーションは、EIM ID および指定されたユーザー ID との間の、直接的な 1 対 1 のマッピングを作成します。 ID アソシエーションを使用して、EIM ID を介したユーザー ID 間の関係を間接的に定義できます。

EIM ID は、企業内の特定の個人やエンティティーを表します。 EIM ID アソシエーションは、EIM ID と、ユーザー・レジストリー内のやはりその人物を表す単一のユーザー ID との関係を記述します。 EIM ID とすべての個人またはエンティティーのユーザー ID 間のアソシエーションを作成すると、その個人またはエンティティーが企業内のリソースをどのように使用しているかについて完全に一意で認識できます。

ユーザー ID は、認証、権限、またはその両方に使用できます。*認証* は、ユーザー ID を提供するエンティティーまたは個人が、 その ID を持つ権利があるかどうかを検査するプロセスです。この検査は、多くの場合、ユーザー ID を提示した個人に、パスワードのようなそのユーザー ID に関連付けられた秘密や私的な情報を提供させることによって実行されます。*権限* は、正しく認証されたユーザー ID が、 その ID が特権を与えられている機能だけを実行したり、そうしたリソースだけにアクセスできることを確認するプロセスです。これまでは、ほとんどすべてのアプリケーションでは、単一のユーザー・レジストリー内の ID を、認証と権限の両方に対して使用するようにしていました。現在では EIM ルックアップ操作を使用すると、アプリケーションで単一のユーザー・レジストリー内のユーザー ID を認証に使用し、別のユーザー・レジストリー内の関連付けられたユーザー ID を権限に使用することが可能です。

EIM ID は、それらのユーザー ID 間の間接的なアソシエーションを提供します。これによりアプリケーションは、既知のユーザー ID に基づいて、EIM ID に対応する別のユーザー ID を検出できます。 EIM は API を提供し、その API は別の (ソース) ユーザー・レジストリー内の識別されたユーザー・レジストリーを提供して、アプリケーションが特定の (ターゲット) ユーザー・レジストリー内の不明なユーザー ID を検出できるようにします。このプロセスは、識別マッピングと呼ばれています。

EIM では、管理者が EIM ID とユーザー ID の間の関係を記述するために、 3 つのタイプのアソシエーションを定義できます。 ID アソシエーションは、次のいずれかのタイプとなります。ソース、ターゲット、または管理です。作成するアソシエーションのタイプは、ユーザー ID が使用される仕方に基づいています。たとえば、マッピングルックアップ操作に参加させるユーザー ID に対して、ソース・アソシエーションおよびターゲット・アソシエーションを作成します。一般に、ユーザー ID が認証に使用される場合、そのユーザー ID にはソース・アソシエーションを作成します。その後、権限に使用されるユーザー ID に対して、ターゲット・アソシエーションを作成します。

ID アソシエーションを作成する前に、まず適切な EIM ID と、 関連付けられたユーザー ID を含むユーザー・レジストリーに対応する適切な EIM レジストリー定義を作成する必要があります。アソシエーションは、EIM ID とユーザー ID の関係を、以下の情報を使用して定義します。

- EIM ID 名
- ユーザー識別名
- EIM レジストリー定義名
- アソシエーション・タイプ
- オプション : ターゲット・アソシエーションにおけるターゲット・ユーザー ID をさらに識別するためのルックアップ情報

ソース・アソシエーション

ソース・アソシエーションを使用すると、ユーザー ID は EIM ルックアップ操作においてソースとして使用でき、同一の EIM ID に関連付けられた別のユーザー ID を検出します。

ユーザー ID が*認証* に使用される場合、そのユーザー ID は、EIM ID とソース・アソシエーションを持っていなければなりません。たとえば、この形式のユーザー ID を認証に使用するために、 Kerberos プリンシパルのソース・アソシエーションを作成するとします。 EIM ID のためのマッピング・ルックアップ操作を正常に行うためには、単一 EIM ID のソース・アソシエーションおよびターゲット・アソシエーションの両方を使用しなければなりません。

ターゲット・アソシエーション

ターゲット・アソシエーションを使用すると、ユーザー ID は EIM ルックアップ操作の結果として戻すことが可能です。エンド・ユーザーを表すユーザー ID は、通常、ターゲット・アソシエーションのみを必要とします。

ユーザー ID が認証ではなく*権限* に使用される場合、そのユーザー ID は EIM ID とターゲット・アソシエーションを持っていなければなりません。たとえば、i5/OS ユーザー・プロファイルのターゲット・アソシエーションを作成するかもしれません。この形式のユーザー ID は、ユーザーが特定の iSeries システムに対して、どのリソースおよび特権を持つかを判別するからです。 EIM ID のためのマッピング・ルックアップ操作を正常に行うためには、単一 EIM ID のソース・アソシエーションおよびターゲット・アソシエーションの両方を使用しなければなりません。

ソース・アソシエーションおよびターゲット・アソシエーションの関係

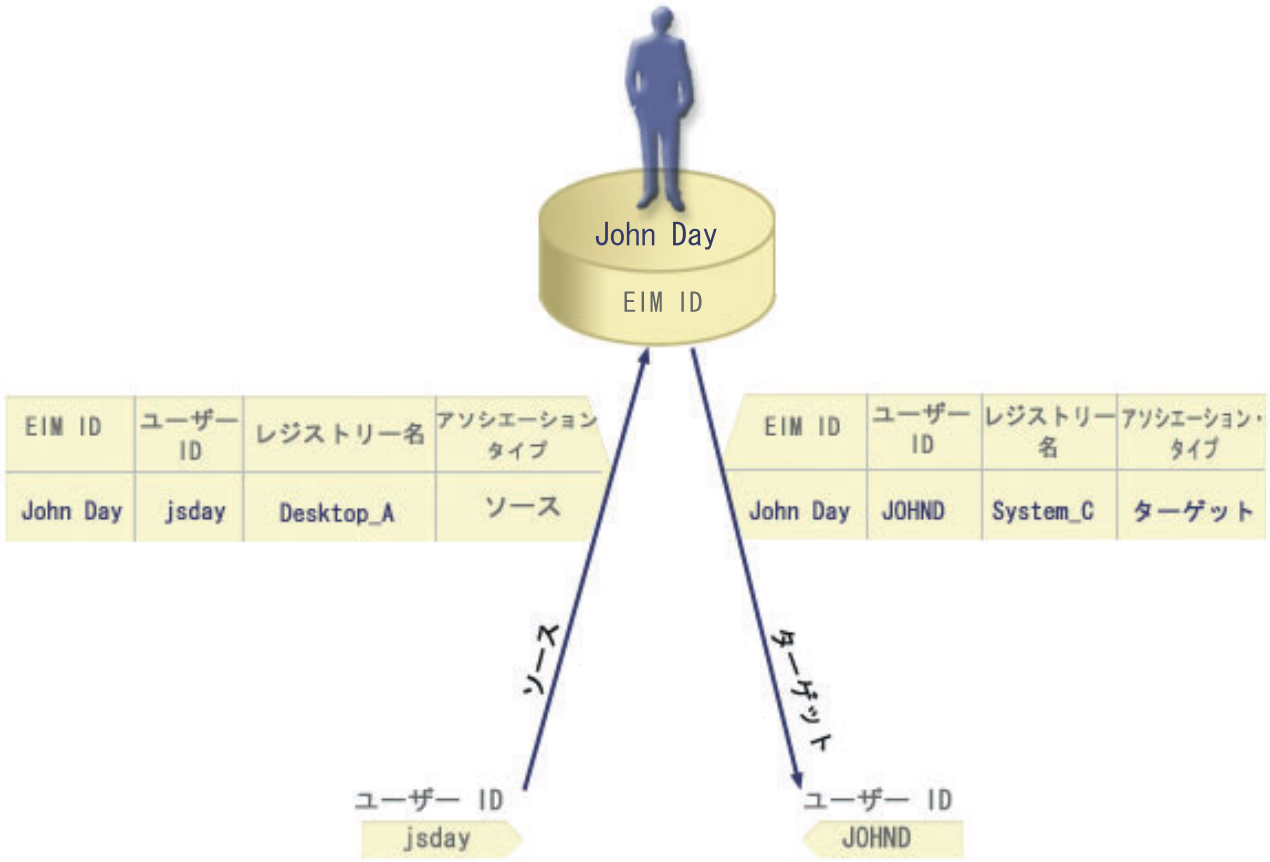
マッピング・ルックアップ操作を正常に行うためには、単一 EIM ID に対して、少なくとも 1 つのソース・アソシエーションと、 1 つ以上のターゲット・アソシエーションを作成する必要があります。一般に、ターゲット・アソシエーションは、ユーザー・レジストリーが対応するシステムまたはアプリケーションへの権限に関して個人が使用できるよう、ユーザー・レジストリー内の各ユーザー ID ごとに作成します。

たとえば、企業内のユーザーが Windows デスクトップに通常にログオンして認証し、iSeries サーバーにアクセスして多数のタスクを実行します。ユーザーがデスクトップにログオンする際には Kerberos プリンシパルを使用し、 iSeries server にログオンする際には i5/OS ユーザー・プロファイルを使用します。この場合、Kerberos プリンシパルを使用してデスクトップに認証し、 iSeries Server には手動で認証しなくてよい、シングル・サインオン環境の作成を考えることでしょう。

それを実現するには、各ユーザーごとに Kerberos プリンシパルに対するソース・アソシエーションと、そのユーザーの EIM ID を作成します。その後、各ユーザーの i5/OS ユーザー・プロファイルごとにターゲット・アソシエーションを、またそのユーザーの EIM ID を作成します。この構成は、i5/OS がマッピング・ルックアップ操作を実行して、デスクトップに認証後 iSeries サーバーにアクセスするユーザーに必要な、正確なユーザー・プロファイルを確実に判別できるようにします。そうすれば、i5/OS は、ユーザーが手動でサーバーに認証しなくても、適切なユーザー・プロファイルに基づいて、サーバー上のリソースへアクセスできるようになります。

図 6 はさらに、EIM 管理者が、EIM ID John Day に対して、ソース・アソシエーションおよびターゲット・アソシエーションの 2 つのアソシエーションを作成して、 この ID と 2 つの関連するユーザー ID との間の関係を定義する例を示しています。管理者は、jsday 用のソース・アソシエーションである Kerberos プリンシパルを、 Desktops ユーザー・レジストリー内に作成します。また管理者は、JOHND のターゲット・アソシエーション、i5/OS ユーザー・プロファイルを、System_C ユーザー・レジストリー内に作成します。こうしたアソシエーションは、EIM ルックアップ操作の一部として、識別されたユーザー ID (ソース、jsday) に基づいて不明のユーザー ID (ターゲット、 JOHND) を入手する手段をアプリケーションに提供します。

図 6: EIM ID John Day の EIM ターゲット・アソシエーションおよびソース・アソシエーション



例を拡張するために、EIM 管理者が、John Day が 5 つの異なるシステム上で同じ i5/OS ユーザー・プロファイル jsd1 を使用することに気付いたとします。この状況では、管理者は EIM ID John Day に 6 つのアソシエーションを作成し、5 つのユーザー・レジストリーでこの ID と関連ユーザー ID 間の関係を定義することが必要です (johnday のソース・アソシエーション、Desktop_A ユーザー・レジストリーおよび jsd1 の 5 つのターゲット・アソシエーションの Kerberos プリンシパル、5 つのユーザー・レジストリー System_B、System_C、System_D、System_E および System_F の i5/OS ユーザー・プロファイル)。EIM マッピングを構成するために実行すべき作業の量を削減するため、EIM 管理者はグループ・レジストリー定義を作成します。グループ・レジストリー定義のメンバーには、System_B、System_C、System_D、System_E、および System_F というレジストリー定義名が含まれます。メンバーを一緒にグループ化することにより、管理者は、複数のアソシエーションを個々のレジストリー定義名に作成するのではなく、単一のターゲット・アソシエーションをグループ・レジストリー定義およびユーザー ID に対して作成できます。ソースおよびターゲット・アソシエーションは、EIM ルックアップ操作の一部として、識別されたユーザー ID (ソース、johnday) に基づいて、グループ・レジストリー定義のメンバーとして表される 5 つのユーザー・レジストリーで不明のユーザー ID (ターゲット、 jsd1) を入手する手段をアプリケーションに提供します。

あるユーザーの場合、同じユーザー ID に対して、ターゲット・アソシエーションとソース・アソシエーションの両方を作成する必要があることがあります。これは、ユーザーが単一システムをクライアントとサーバーの両方に使用する場合や、管理者として役割を果たすユーザーにとって必要となります。

注: 標準的ユーザーを表すユーザー ID は、通常、ターゲット・アソシエーションのみを必要とします。

あるユーザーの場合、同じユーザー ID に対して、ターゲット・アソシエーションとソース・アソシエーションの両方を作成する必要があることがあります。これは、ユーザーが単一システムをクライアントとサーバーの両方に使用する場合や、管理者として役割を果たすユーザーにとって必要となります。

たとえば、管理者は iSeries ナビゲーターのマネージメント・セントラル機能を使用して、セントラル・システムおよびいくつかのエンドポイント・システムを管理します。管理者はさまざまな機能を実行しますが、これらの機能はセントラル・システムまたはエンドポイント・システムで引き起こすことができます。この状況では、それぞれのシステム上の管理者のユーザー ID ごとに、ソース・アソシエーションおよびターゲット・アソシエーションの両方を作成することでしょう。これは、管理者がどのシステムから他のシステムへアクセスしようと、使用するユーザー ID は、管理者がアクセスする後続のシステムの適切なユーザー ID にマップできます。

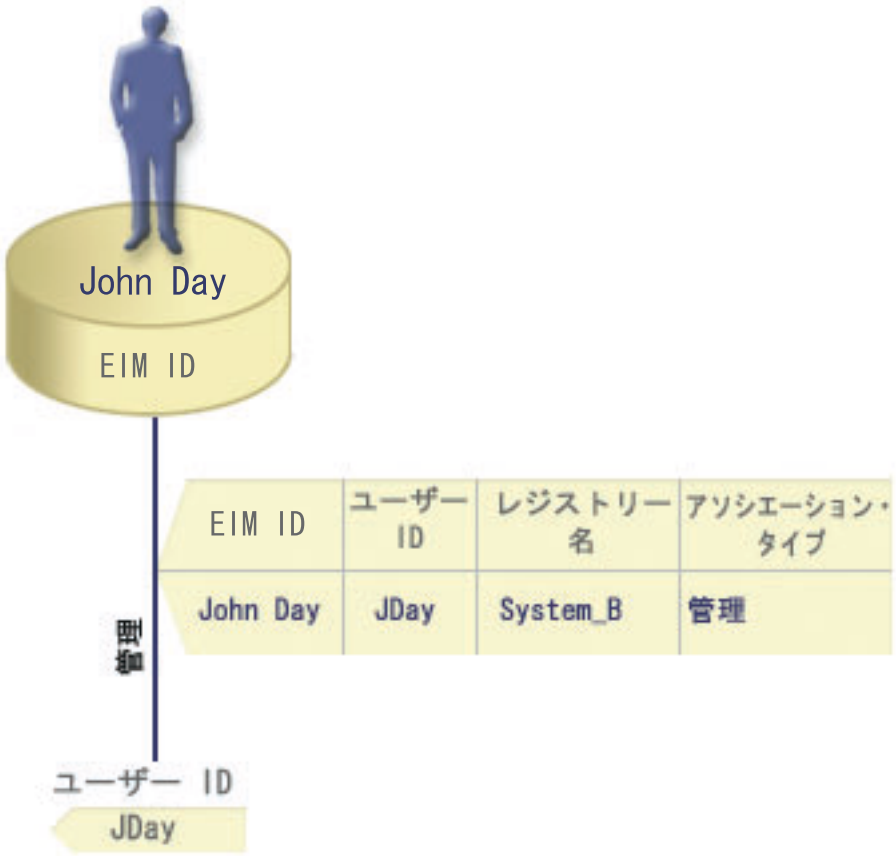
管理アソシエーション

EIM ID の管理アソシエーションは、 通常、EIM ID に登録された個人やエンティティーが、特定のシステムに対して特別なユーザー ID であることを示します。たとえば、このタイプのアソシエーションは、高度な機密のユーザー・レジストリーで使用できます。

管理アソシエーションの特殊な性質であるため、このタイプのアソシエーションは、EIM マッピング・ルックアップ操作には参加できません。したがって、管理アソシエーションを持つソース・ユーザー ID を提供する EIM ルックアップ操作では、結果は戻されません。同様に、管理アソシエーションを持つユーザー ID は、EIM ルックアップ操作の結果として戻されません。

図 7 は、管理アソシエーションの例を示しています。この例では、John Day という名前の従業員は、システム A 上に 1 つのユーザー ID John_Day を、 より高度なセキュア・システムであるシステム B 上には別のユーザー ID JDay を有しています。システム管理者は、ユーザーがシステム B のローカル・ユーザー・レジストリーだけを使用して、システム B に認証することを考えています。管理者は、アプリケーションが別の認証メカニズムを使用して、そのシステムに対して John Day を認証できるようにはしたくありません。システム B での JDay ユーザー ID の管理アソシエーションを使用すれば、 EIM 管理者は John Day がシステム B にアカウントを持っていることを知ることができますが、 EIM は EIM ルックアップ操作が行われても JDay ID の関する情報は戻しません。 EIM ルックアップ操作を活用するアプリケーションがそのシステム上に置かれていても、それらのアプリケーションは管理アソシエーションを持つユーザー ID を検出できません。

図 7: EIM ID John Day の EIM 管理アソシエーション



ポリシー・アソシエーション

ここでは、複数のユーザー ID とユーザー・レジストリー内の単一ユーザー ID との間の関係を記述する、ポリシー・アソシエーションの使用法を学習します。

EIM (エンタープライズ識別マッピング) マッピング・ポリシーにより、 EIM 管理者がポリシー・アソシエーションを作成および使用して、1 つ以上のユーザー・レジストリー内の複数のユーザー ID、および別のユーザー・レジストリー内の単一ユーザー ID との間の関係を定義できるようになりました。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。ポリシー・アソシエーションは、 EIM ID および単一ユーザー ID との間の 1 対 1 マッピングを提供する ID アソシエーションの代わりに、またはそれと組み合わせて使用できます。

ポリシー・アソシエーションは、特定の個々の EIM アソシエーションが存在しないユーザー ID にのみ影響を与えます。 EIM ID とユーザー ID との間に特定の ID アソシエーションが存在する場合には、ポリシー・アソシエーションが存在し使用可能であっても、 ID アソシエーションに登録されたターゲット・ユーザー ID が、ルックアップ操作を実行するアプリケーションに戻されます。

3 つの異なるタイプのポリシー・アソシエーションを作成できます。

関連概念

30 ページの『EIM ルックアップ操作』
ここでは、EIM (エンタープライズ識別マッピング) のプロセスおよび図で示された例を説明します。

デフォルトのドメイン・ポリシー・アソシエーション:

ここでは、ドメイン内のすべてのユーザー ID のマッピング関係を設定する方法を説明します。

デフォルトのドメイン・ポリシー・アソシエーションは、ポリシー・アソシエーションの 1 つのタイプで、 ユーザー ID 間の多対 1 マッピングを作成するために使用できます。デフォルトのドメイン・ポリシー・アソシエーションを使用して、複数のユーザー ID のソース・セット (この場合はドメイン内のすべてのユーザー) を、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID にマップできます。デフォルトのドメイン・ポリシー・アソシエーションでは、ドメイン内のすべてのユーザーがポリシー・アソシエーションのソースであり、単一のターゲット・レジストリーおよびターゲット・ユーザー ID にマップされます。

デフォルトのドメイン・ポリシー・アソシエーションを使用する場合は、そのドメインに対するポリシー・アソシエーションを使用するマッピング・ルックアップを使用可能にしなければなりません。また、ポリシー・アソシエーションのターゲット・ユーザー・レジストリーに対して、マッピング・ルックアップを使用可能にする必要もあります。この使用可能化を構成すると、ポリシー・アソシエーションに関係するユーザー・レジストリーは、マッピング・ルックアップ操作に参加できます。

デフォルトのドメイン・ポリシー・アソシエーションが有効になるのは、マッピング・ルックアップ操作が、ターゲット・レジストリーに対する ID アソシエーション、証明書フィルター・ポリシー・アソシエーション、またはデフォルトのレジストリー・ポリシー・アソシエーションによっては結果を戻せない場合です。その場合には、ドメイン内のすべてのユーザー ID が、デフォルトのドメイン・ポリシー・アソシエーションによって指定された単一のターゲット・ユーザー ID にマップされます。

たとえば、ターゲット・レジストリー `Registry_xyz` 内のターゲット・ユーザー ID `John_Day` を指定してデフォルトのドメイン・ポリシー・アソシエーションを作成するとします。このユーザー ID にマップする ID アソシエーションや他のポリシー・アソシエーションは作成していません。したがって、`Registry_xyz` がルックアップ操作のターゲット・レジストリーとして指定されると、デフォルトのドメイン・ポリシーは、ドメイン内の、他のアソシエーションが定義されていないユーザー ID すべてに対して、 ターゲット・ユーザー ID `John_Day` が戻されるようにします。

デフォルトのドメイン・ポリシー・アソシエーションを定義するために、以下の 2 つのものを指定します。

- **ターゲット・レジストリー**。指定するターゲット・レジストリーは、ドメイン内のすべてのユーザー ID のマップ先となるユーザー ID が登録された EIM (エンタープライズ識別マッピング) レジストリー定義の名前です。
- **ターゲット・ユーザー**。 ターゲット・ユーザーは、このポリシー・アソシエーションに基づいて、 EIM マッピング・ルックアップ操作のターゲットとして戻されるユーザー ID の名前です。

ドメイン内のそれぞれのレジストリーごとに、デフォルトのドメイン・ポリシー・アソシエーションを定義できます。 2 つ以上のドメイン・ポリシー・アソシエーションが同じターゲット・レジストリーを参照する場合には、これらのポリシー・アソシエーションのそれぞれに固有のルックアップ情報を定義して、マッピング・ルックアップ操作がそれらを確実に区別できるようにする必要があります。そうしなければ、マッピング・ルックアップ操作は、複数のターゲット・ユーザー ID を戻す可能性があります。結果がそのようにあいまいであれば、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット・ユーザー ID を判別できないかもしれません。

さまざまな重複した方法でポリシー・アソシエーションを使用できるので、ポリシー・アソシエーションを作成および使用する前に、 EIM マッピング・ポリシー・サポートやルックアップ操作の動作を、よく理解しておく必要があります。

注: グループ・レジストリー定義内に存在するターゲット・ユーザー ID で、デフォルトのドメイン・ポリシー・アソシエーションを作成する必要があるかもしれません。ドメイン内のすべてのユーザーはポリシー・アソシエーションのソースであり、ターゲット・グループ・レジストリー定義のターゲット・ユーザー ID にマップされます。デフォルトのドメイン・ポリシー・アソシエーションで定義されるユーザー ID は、グループ・レジストリー定義のメンバー内に存在します。

たとえば John Day は、システム B、システム C、システム D、システム E、システム F という 5 つの異なるシステム上で同じ i5/OS ユーザー・プロファイル John_Day を使用します。EIM マッピングを構成するために実行すべき作業の量を削減するため、EIM 管理者はGroup_1 というグループ・レジストリー定義を作成します。グループ・レジストリー定義のメンバーには、System_B、System_C、System_D、System_E、および System_F というレジストリー定義名が含まれます。メンバーを一緒にグループ化することにより、管理者は、複数のアソシエーションを個々のレジストリー定義に作成するのではなく、単一のターゲット・アソシエーションをグループ・レジストリー定義およびユーザー ID に対して作成できます。

EIM 管理者は、ターゲット・レジストリー Group_1 内のターゲット・ユーザー ID John_Day を指定してデフォルトのドメイン・ポリシー・アソシエーションを作成します。この場合、他に特定の ID アソシエーションやポリシー・アソシエーションが適用されることはありません。したがって、Group_1 がルックアップ操作のターゲット・レジストリーとして指定されると、デフォルトのドメイン・ポリシーは、ドメイン内の、他のアソシエーションが定義されていないユーザー ID すべてに対して、ターゲット・ユーザー ID John_Day が戻されるようにします。

デフォルトのレジストリー・ポリシー・アソシエーション:

ここでは、単一のレジストリー内のすべてのユーザー ID のマッピング関係を設定する方法を説明します。

デフォルトのレジストリー・ポリシー・アソシエーションは、ポリシー・アソシエーションの 1 つのタイプで ユーザー ID 間の多対 1 マッピングを作成するために使用できます。デフォルトのレジストリー・ポリシー・アソシエーションを使用して、複数のユーザー ID (この場合は単一レジストリー内のユーザー) のソース・セットを、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID にマップできます。デフォルトのレジストリー・ポリシー・アソシエーションでは、単一レジストリー内のすべてのユーザーが、ポリシー・アソシエーションのソースであり、単一ターゲット・レジストリーおよびターゲット・ユーザーにマップされます。

デフォルトのレジストリー・ポリシー・アソシエーションを使用する場合は、そのドメインのポリシー・アソシエーションを使用するマッピング・ルックアップを使用可能にしなければなりません。また、ソース・レジストリーに対して、マッピング・ルックアップを使用可能にし、ポリシー・アソシエーションのターゲット・ユーザー・レジストリーに対して、マッピング・ルックアップおよびポリシー・アソシエーションの使用を使用可能にする必要もあります。この使用可能化を構成すると、ポリシー・アソシエーションに関係するユーザー・レジストリーは、マッピング・ルックアップ操作に参加できます。

デフォルトのレジストリー・ポリシー・アソシエーションが有効になるのは、マッピング・ルックアップ操作が、ターゲット・レジストリーの ID アソシエーション、証明書フィルター・ポリシー・アソシエーション、または他のデフォルトのレジストリー・ポリシー・アソシエーションによっては結果が戻されない場合です。その場合には、ソース・レジストリー内のすべてのユーザー ID が、デフォルトのレジストリー・ポリシー・アソシエーションによって指定された単一ターゲット・ユーザー ID にマップされます。

たとえば、ソース・レジストリーが my_realm.com である、デフォルトのレジストリー・ポリシー・アソシエーションを作成するとします。このソース・レジストリーは、特定の Kerberos レルムにおけるプリンシ

パルです。このポリシー・アソシエーションに対して、ターゲット・レジストリー i5/OS_system_reg 内のターゲット・ユーザー ID general_user1 も指定します。このターゲット・レジストリーは、i5/OS ユーザー・レジストリー内の特定のユーザー・プロファイルです。この場合、ソース・レジストリー内のどのユーザー ID にも、 ID アソシエーションまたはポリシー・アソシエーションは作成していません。したがって、ルックアップ操作において i5/OS_system_reg がターゲット・レジストリーとして指定され、my_realm.com がソース・レジストリーとして指定された場合、デフォルトのレジストリー・ポリシー・アソシエーションは、my_realm.com 内の、 特定の ID アソシエーションまたは証明書フィルター・ポリシー・アソシエーションを定義されていないすべてのユーザー ID に対して、ターゲット・ユーザー ID general_user1 が戻されるようにします。

デフォルトのレジストリー・ポリシー・アソシエーションを定義するために、以下の 3 つのものを指定します。

- **ソース・レジストリー**。これは、ポリシー・アソシエーションがマッピングのソースとして使用するレジストリー定義です。このソース・ユーザー・レジストリー内のすべてのユーザー ID は、ポリシー・アソシエーションの指定ターゲット・ユーザーにマップされます。
- **ターゲット・レジストリー**。 ターゲット・レジストリーとして、 EIM (エンタープライズ識別マッピング) レジストリー定義の名前を指定します。ターゲット・レジストリーには、ソース・レジストリー内のすべてのユーザー ID のマップ先となるターゲット・ユーザー ID が含まれていなければなりません。
- **ターゲット・ユーザー**。 ターゲット・ユーザーは、このポリシー・アソシエーションに基づいて、 EIM マッピング・ルックアップ操作のターゲットとして戻されるユーザー ID の名前です。

デフォルトのレジストリー・ポリシー・アソシエーションは、複数定義できます。ソース・レジストリーが同じである 2 つ以上のポリシー・アソシエーションが、同じターゲット・レジストリーを参照する場合には、それぞれのポリシー・アソシエーションに対して固有のルックアップ情報を定義して、マッピング・ルックアップ操作がそれらを区別できるようにしなければなりません。そうしなければ、マッピング・ルックアップ操作は、複数のターゲット・ユーザー ID を戻す可能性があります。結果がそのようにあいまいであれば、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。

さまざまな重複した方法でポリシー・アソシエーションを使用できるので、ポリシー・アソシエーションを作成および使用する前に、 EIM マッピング・ポリシー・サポートやルックアップ操作の動作を、よく理解しておく必要があります。

注: グループ・レジストリー定義内に存在するターゲット・ユーザー ID で、デフォルトのレジストリー・ポリシー・アソシエーションを作成する必要があるかもしれません。ソース・ユーザー・レジストリー内のすべてのユーザーはポリシー・アソシエーションのソースであり、ターゲット・グループ・レジストリー定義のターゲット・ユーザー ID にマップされます。デフォルトのレジストリー・ポリシー・アソシエーションで定義されるユーザー ID は、グループ・レジストリー定義のメンバー内に存在します。

たとえば John Day は、System_B、System_C、System_D、System_E、および System_F という 5 つの異なるシステム上で同じ i5/OS ユーザー・プロファイル John_Day を使用します。EIM マッピングを構成するために実行すべき作業の量を削減するため、EIM 管理者は Group_1 というグループ・レジストリー定義を作成します。グループ・レジストリー定義のメンバーには、System_B、System_C、System_D、System_E、および System_F というレジストリー定義名が含まれます。メンバーを一緒にグループ化することにより、管理者は、複数のアソシエーションを個々のレジストリー定義に作成するのではなく、単一のターゲット・アソシエーションをグループ・レジストリー定義およびユーザー ID に対して作成できます。

EIM 管理者は、ソース・レジストリーが my_realm.com である、デフォルトのレジストリー・ポリシー・アソシエーションを作成します。このソース・レジストリーは、特定の Kerberos レルムにおけるプリンシパルです。このポリシー・アソシエーションについて、さらに管理者は、John_Day のターゲット・ユーザー ID をターゲット・レジストリー Group_1 で指定します。 この場合、他の ID アソシエーションまたはポリシー・アソシエーションが適用されることはありません。したがって、ルックアップ操作において Group_1 がターゲット・レジストリーとして指定され、my_realm.com がソース・レジストリーとして指定された場合、デフォルトのレジストリー・ポリシー・アソシエーションは、my_realm.com 内の、 特定の ID アソシエーションを定義されていないすべてのユーザー ID に対して、ターゲット・ユーザー ID John_Day が戻されるようにします。

証明書フィルター・ポリシー・アソシエーション:

ここでは、単一 X.509 レジストリー内にあるセットのユーザー ID のマッピング関係を設定 (ディジタル証明書の形式で) する方法を説明します。

証明書フィルター・ポリシー・アソシエーションは、ポリシー・アソシエーションの 1 つのタイプで、 ユーザー ID 間の多対 1 マッピングを作成するために使用できます。証明書フィルター・ポリシー・アソシエーションを使用して、証明書のソース・セットを、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID にマップできます。

証明書フィルター・ポリシー・アソシエーションでは、単一 X.509 レジストリー内の証明書のセットを、ポリシー・アソシエーションのソースとして指定します。これらの証明書は、指定した単一ターゲット・レジストリーおよびターゲット・ユーザーにマップされます。単一レジストリー内のすべてのユーザーがポリシー・アソシエーションのソースである、デフォルトのレジストリー・ポリシー・アソシエーションとは異なり、証明書フィルター・ポリシー・アソシエーションの有効範囲は、より柔軟です。レジストリー内の証明書のサブセットを、ソースとして指定できます。ポリシー・アソシエーションに対して指定する証明書フィルターが、その有効範囲を判別します。

注: X.509 ユーザー・レジストリー内のすべての証明書を、単一のターゲット・ユーザー ID にマップする場合は、デフォルトのレジストリー・ポリシー・アソシエーションを作成および使用してください。

証明書フィルター・ポリシー・アソシエーションを使用する場合は、そのドメインに対して、ポリシー・アソシエーションを使用するマッピング・ルックアップを使用可能にしなければなりません。また、ソース・レジストリーに対して、マッピング・ルックアップを使用可能にし、ポリシー・アソシエーションのターゲット・ユーザー・レジストリーに対して、マッピング・ルックアップおよびポリシー・アソシエーションの使用を使用可能にする必要もあります。この使用可能化を構成すると、ポリシー・アソシエーションに関係するユーザー・レジストリーは、マッピング・ルックアップ操作に参加できます。

ディジタル証明書が EIM (エンタープライズ識別マッピング) マッピング・ルックアップ操作におけるソース・ユーザー ID である場合 (要求側アプリケーションが eimFormatUserIdentity() EIM API を使用してユーザー識別名をフォーマットした後)、 EIM はまず最初に、EIM ID と指定ユーザー ID との間に ID アソシエーションがあるかどうかを調べます。それが存在しない場合、EIM はポリシー・アソシエーションに関して、証明書内の DN 情報を、フィルター内に指定された DN または部分 DN 情報と比較します。 証明書内の DN 情報がフィルターの基準を満たす場合に、 EIM はポリシー・アソシエーションが指定するターゲット・ユーザー ID を戻します。 その結果、ソース X.509 レジストリー内の、証明書フィルター基準を満たす証明書が、証明書フィルター・ポリシー・アソシエーションの指定どおりに、単一のターゲット・ユーザー ID にマップされます。

たとえば、ソース・レジストリーが certificates.x509 である証明書フィルター・ポリシー・アソシエーションを作成するとします。このレジストリーには、会社の従業員すべての証明書が含まれます。その中に

は、人事課のすべての管理者が、特定の専用社内 Web ページ、 および iSeries サーバーによってアクセスする他のリソースにアクセスするために使用する証明書が含まれています。また、このポリシー・アソシエーションに関して、i5/OS ユーザー・レジストリー内の特定のユーザー・プロファイルであるターゲット・レジストリー system_abc にある、hr_managers をターゲット・ユーザー ID として指定します。人事課の管理者に所属する証明書だけがこのポリシー・アソシエーションによってカバーされるようにするには、証明書フィルターを ou=hrmgr,o=myco.com,c=us というサブジェクト識別名 (SDN) とともに指定します。

この場合、ソース・レジストリー内のどのユーザー ID に対しても、 ID アソシエーションまたはその他の証明書フィルター・ポリシー・アソシエーションを作成していません。したがって、ルックアップ操作において system_abc がターゲット・レジストリーとして指定され、 certificates.x509 がソース・レジストリーとして指定されると、証明書フィルター・ポリシー・アソシエーションは、certificates.x509 レジストリー内の、指定された証明書フィルターに一致し、特定の ID アソシエーションが定義されていないすべての証明書に対して、ターゲット・ユーザー ID hr_managers が戻されるようにします。

証明書フィルター・ポリシー・アソシエーションを定義するためには、以下の情報を指定します。

- **ソース・レジストリー**。指定するソース・レジストリー定義は、X.509 タイプ・ユーザー・レジストリーでなければなりません。証明書フィルター・ポリシーは、この X.509 ユーザー・レジストリー内のユーザー ID と、単一の特定のターゲット・ユーザー ID との間のアソシエーションを作成します。このアソシエーションは、そのレジストリー内の、このポリシーに指定した証明書フィルターの基準に合うユーザー ID のみに適用されます。
- **証明書フィルター**。 証明書フィルターは、類似したユーザー証明書属性のセットを定義します。証明書フィルター・ポリシー・アソシエーションは、 X.509 ユーザー・レジストリー内の、これらの定義された属性を持つ証明書を、特定のターゲット・ユーザー ID にマップします。 サブジェクト識別名 (SDN) および発行者識別名 (IDN) の組み合わせに基づいて、マッピングのソースとして使用する証明書に一致するフィルターを指定します。ポリシーに対して指定する証明書フィルターは、EIM ドメイン内にすでに存在していなければなりません。
- **ターゲット・レジストリー**。指定するターゲット・レジストリー定義は、証明書フィルターに一致する証明書のマップ先となるユーザー ID が登録されたユーザー・レジストリーです。
- **ターゲット・ユーザー**。ターゲット・ユーザーは、このポリシー・アソシエーションに基づいて、 EIM マッピング・ルックアップ操作のターゲットとして戻されるユーザー ID の名前です。

さまざまな重複した方法で証明書ポリシー・アソシエーションおよびその他のアソシエーションを使用できるので、証明書ポリシー・アソシエーションを作成および使用する前に、 EIM マッピング・ポリシー・サポートやルックアップ操作の動作の両方を、よく理解しておく必要があります。

注: グループ・レジストリー定義内に存在するターゲット・ユーザー ID で、証明書フィルター・ポリシー・アソシエーションを作成する必要があるかもしれません。証明書フィルターによって指定された基準を満たすソース・レジストリー内のユーザーは、ポリシー・アソシエーションのソースであり、ターゲット・グループ・レジストリー定義中のターゲット・ユーザー ID にマップされます。証明書フィルター・ポリシー・アソシエーションで定義されるユーザー ID は、グループ・レジストリー定義のメンバー内に存在します。

たとえば John Day は、システム B、システム C、システム D、システム E、システム F という 5 つの異なるシステム上で同じ i5/OS ユーザー・プロファイル John_Day を使用します。EIM マッピングを構成するために実行すべき作業の量を削減するため、EIM 管理者はグループ・レジストリー定義を作成します。グループ・レジストリー定義のメンバーには、System_B、System_C、System_D、System_E、および System_F というレジストリー定義名が含まれます。メンバー

を一緒にグループ化することにより、管理者は、複数のアソシエーションを個々のレジストリー定義に作成するのではなく、単一のターゲット・アソシエーションをグループ・レジストリー定義およびユーザー ID に対して作成できます。

EIM 管理者は、証明書フィルター・ポリシー・アソシエーションを作成し、そこで単一 X.509 レジストリー内の証明書のサブセットをポリシー・アソシエーションのソースとして定義します。管理者は、John_Day のターゲット・ユーザー ID をターゲット・レジストリー Group_1 で指定します。 この場合、他の特定の ID アソシエーションまたは他の証明書フィルター・ポリシー・アソシエーションが適用されることはありません。したがって、Group_1 がルックアップ操作中にターゲット・レジストリーとして指定されると、ソース X.509 レジストリー内で証明書フィルター基準と一致するすべての証明書が、指定されるターゲット・ユーザー ID にマップされます。

証明書フィルター:

ここでは、X.509 ユーザー・レジストリー内で定義された属性を持つ証明書を特定のターゲット・ユーザー ID にマップする、証明書フィルター・ポリシー・アソシエーションを作成する方法を説明します。

証明書フィルターは、X.509 ソース・ユーザー・レジストリー内のユーザー証明書のグループに対する, 類似した識別名証明書属性のセットを定義します。証明書フィルターは、 証明書フィルター・ポリシー・アソシエーションの基礎として使用できます。ポリシー・アソシエーション内の証明書フィルターは、指定されたソース X.509 レジストリー内のどの証明書を、指定されたターゲット・ユーザーにマップするかを判別します。フィルターの基準を満たすサブジェクト DN および発行者 DN 情報を持つ証明書は、 EIM (エンタープライズ識別マッピング) マッピング・ルックアップ操作中に、指定されたターゲット・ユーザーにマップされます。

たとえば、o=ibm,c=us というサブジェクト識別名 (SDN) を持つ証明書フィルターを作成するとします。cn=JohnDay,ou=LegalDept,o=ibm,c=us という SDN を持つ証明書のように、 指定された DN が SDN 情報の一部として含まれている証明書はすべて、フィルターの基準に合うことになります。証明書が基準に合う、複数の証明書フィルターがある場合は、証明書が最も類似している、特定される度合いが最も高い証明書フィルター値が優先されます。たとえば、o=ibm,c=us という SDN を持つ証明書フィルターと、ou=LegalDept,o=ibm,c=us という SDN を持つ別の証明書があるとします。 ソース X.509 レジストリー内に、cn=JohnDay,ou=LegalDept,o=ibm,c=us という SDN を持つ証明書がある場合には、 2 番目の特定される度合いの高いフィルターが使用されます。ソース X.509 レジストリー内に、cn=SharonJones,o=ibm,c=us という SDN を持つ証明書がある場合には、特定される度合いの低いフィルターが使用されます。その証明書のほうが基準により近いからです。

証明書フィルターを定義するために、次のうちの 1 つまたは両方を指定できます。

- サブジェクト識別名 (SDN)。 フィルターに指定する DN の全部または一部は、ディジタル証明書のサブジェクト DN 部分に対応していなければなりません。これは、証明書の所有者を指定します。サブジェクト DN ストリング全体を供給することもできますし、完全な SDN を構成する 1 つ以上の部分的な DN を供給することもできます。
- 発行者識別名 (IDN)。 フィルターに指定する DN の全部または一部は、 ディジタル証明書の発行者 DN 部分に対応していなければなりません。これは、証明書を発行した認証局を指定します。発行者 DN ストリング全体を供給することもできますし、完全な IDN を構成する 1 つ以上の部分的な DN を供給することもできます。

証明書フィルターの作成を行うために使用できる方法がいくつかあります。その 1 つが、EIM ポリシー・フィルターのフォーマット (Format EIM Policy Filter) (eimFormatPolicyFilter()) API を使用する方法です。この API は、 SDN および IDN の正確な順序およびフォーマットで必要な DN を作成するために証明書をテンプレートとして使用し、証明書フィルターを生成します。

EIM ルックアップ操作

ここでは、EIM (エンタープライズ識別マッピング) のプロセスおよび図で示された例を説明します。

アプリケーションまたはオペレーティング・システムは、 EIM API を使用して*ルックアップ操作* を実行して、 1 つのレジストリー内の 1 つのユーザー ID を、別のレジストリー内の別のユーザー ID にマップできます。 EIM ルックアップ操作とは、既知の信頼ある情報を提供することによって、特定のターゲット・レジストリー内に関連付けられた不明のユーザー ID をアプリケーションまたはオペレーティング・システムが検出するプロセスのことです。 EIM API を使用するアプリケーションは、情報が EIM ドメインに保管されている場合に限り、そうした情報に関して EIM ルックアップ操作を実行できます。アプリケーションが EIM ルックアップ操作のソースとして提供する情報のタイプ (ユーザー ID または EIM ID) に応じて、 2 つのタイプの EIM ルックアップ操作のうちいずれかを実行できます。

アプリケーションまたはオペレーティング・システムは、 `eimGetTargetFromSource()` API を使用して、指定されたターゲット・レジストリーのターゲット・ユーザー ID を取得する際に、ルックアップ操作のソースのユーザー *ID* を供給しなければなりません。 EIM ルックアップ操作においてソースとして使用するためには、ユーザー ID が ID ソース・アソシエーションで定義されているか、またはポリシー・アソシエーションによってカバーされていなければなりません。アプリケーションまたはオペレーティング・システムは、この API を使用する際、以下の 3 つの情報を供給しなければなりません。

- ソースのユーザー ID、または操作の開始点
- ソース・ユーザー ID の EIM レジストリー定義名
- EIM ルックアップ操作のターゲットとなる EIM レジストリー定義名。このレジストリー定義は、アプリケーションが検索するユーザー ID を含むユーザー・レジストリーを記述します。

アプリケーションまたはオペレーティング・システムは、`eimGetTargetFromIdentifier()` API を使用して、指定されたターゲット・レジストリーに対するユーザー ID を取得する際、 EIM ルックアップ操作のソースの *EIM ID* を供給しなければなりません。アプリケーションは、この API を使用する際、以下の 2 つの情報を供給しなければなりません。

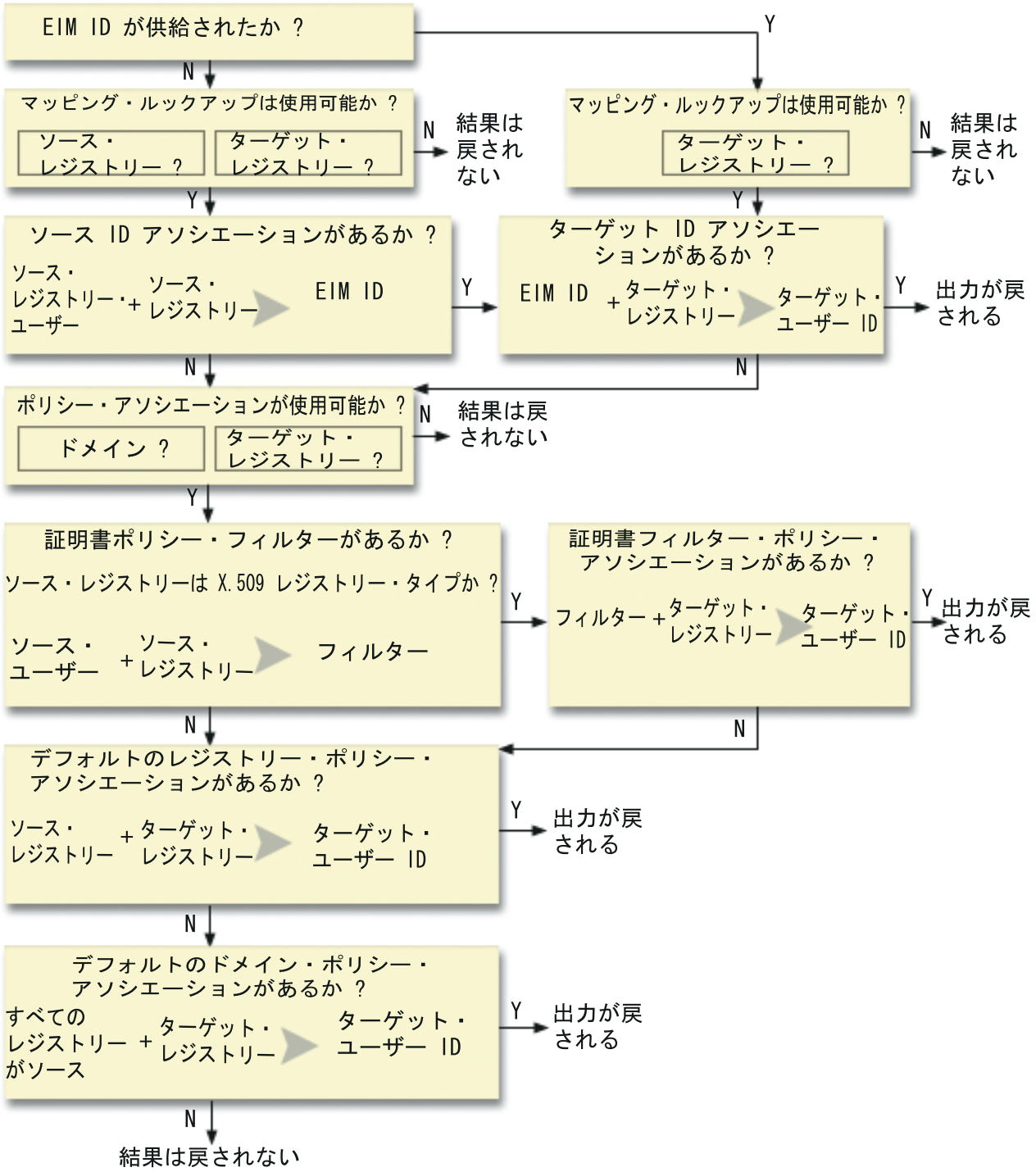
- ソースの EIM ID、または操作の開始点。
- EIM ルックアップ操作のターゲットとなる EIM レジストリー定義名。このレジストリー定義は、アプリケーションが検索するユーザー ID を含むユーザー・レジストリーを記述します。

いずれのタイプの EIM ルックアップ操作でも、そのターゲットとして戻されるユーザー ID は、ターゲット・アソシエーションが定義されていなければなりません。このターゲット・アソシエーションは、 ID ターゲット・アソシエーションまたはポリシー・アソシエーションのどちらであってもかまいません。

提供された情報は EIM に渡され、 図 10 に例示されたとおり、以下の順序で EIM データを検索することにより、 EIM ルックアップ操作がターゲット・ユーザー ID を検索して戻します。

1. EIM ID の ID ターゲット・アソシエーション。 EIM ID は、次の 2 つの方法のうちの 1 つで識別されます。すなわち、`eimGetTargetFromIdentifier()` API によって提供されるか、または、`eimGetTargetFromSource()` API によって提供された情報から判別されます。
2. 証明書フィルター・ポリシー・アソシエーション
3. デフォルトのレジストリー・ポリシー・アソシエーション
4. デフォルトのドメイン・ポリシー・アソシエーション

図 10: EIM ルックアップ操作の一般的な処理フローチャート



注: 以下の流れでは、ルックアップ操作は、指定されたソース・レジストリーまたはターゲット・レジストリーなどの、個々のレジストリー定義を最初にチェックします。個々のレジストリー定義を使用してマッピングを検索するのに失敗した場合、ルックアップ操作は個々のレジストリー定義がグループ・レジストリー定義のメンバーかどうかを判別します。グループ・レジストリー定義のメンバーである場合、ルックアップ操作はグループ・レジストリー定義をチェックして、マッピング・ルックアップ要求を満たすようにします。

ルックアップ操作検索は、次のように行われます。

1. ルックアップ操作は、マッピング・ルックアップが使用可能かどうかをチェックします。ルックアップ操作は、指定されたソース・レジストリー、指定されたターゲット・レジストリー、または指定された両方のレジストリーに対して、マッピング・ルックアップが使用可能であるかどうかを判別します。マッピング・ルックアップが片方または両方のレジストリーに対して使用可能でない場合には、ターゲット・ユーザー ID を戻さずにルックアップ操作が終了します。
2. ルックアップ操作が、ルックアップ基準に一致する ID アソシエーションがあるかどうかをチェックします。 EIM ID が提供されている場合には、ルックアップ操作は指定された EIM ID 名を使用します。それが提供されていない場合には、ルックアップ操作は、提供されたソース・ユーザー ID およびソース・レジストリーに一致する、 特定の ID ソース・アソシエーションがあるかどうかをチェックします。それがある場合には、ルックアップ操作はそれを使用して、適切な EIM ID 名を判別します。その後、ルックアップ操作は EIM ID 名を使用して、 指定されたターゲット EIM レジストリー定義名に一致する、 EIM ID の ID ターゲット・アソシエーションを検索します。一致する ID ターゲット・アソシエーションがある場合には、ルックアップ操作はターゲット・アソシエーションに定義されたターゲット・ユーザー ID を戻します。
3. ルックアップ操作は、ポリシー・アソシエーションの使用が使用可能であるかどうかをチェックします。ルックアップ操作は、ドメインがポリシー・アソシエーションを使用したマッピング・ルックアップを実行できるかどうかをチェックします。ルックアップ操作はまた、ターゲット・レジストリーがポリシー・アソシエーションを使用できるかどうかをチェックします。ドメインまたはレジストリーが、ポリシー・アソシエーションに対して使用可能でない場合には、ターゲット・ユーザー ID を戻さずにルックアップ操作が終了します。
4. ルックアップ操作は、証明書フィルター・ポリシー・アソシエーションをチェックします。ルックアップ操作は、ソース・レジストリーが X.509 レジストリー・タイプであるかどうかをチェックします。それが X.509 レジストリー・タイプである場合には、ルックアップ操作は、ソースおよびターゲット・レジストリー定義名と一致する、証明書フィルター・ポリシー・アソシエーションがあるかどうかをチェックします。ルックアップ操作は、ソース X.509 レジストリー内に、証明書フィルター・ポリシー・アソシエーションで指定された基準を満たす証明書があるかどうかをチェックします。一致するポリシー・アソシエーションがあり、証明書フィルター基準を満たす証明書がある場合には、ルックアップ操作はそのポリシー・アソシエーションに対して適切なターゲット・ユーザー ID を戻します。
5. ルックアップ操作はデフォルトのレジストリー・ポリシー・アソシエーションをチェックします。ルックアップ操作は、ソースおよびターゲット・レジストリー定義名と一致する、デフォルトのレジストリー・ポリシー・アソシエーションがあるかどうかをチェックします。一致するポリシー・アソシエーションがある場合には、ルックアップ操作はそのポリシー・アソシエーションに対して適切なターゲット・ユーザー ID を戻します。
6. ルックアップ操作はデフォルトのドメイン・ポリシー・アソシエーションをチェックします。ルックアップ操作は、ターゲット・レジストリー定義に定義されたデフォルトのドメイン・ポリシー・アソシエーションがあるかどうかをチェックします。一致するポリシー・アソシエーションがある場合には、ルックアップ操作はそのポリシー・アソシエーションに関連したターゲット・ユーザー ID を戻します。
7. ルックアップ操作は結果を戻すことができません。

EIM (エンタープライズ識別マッピング) ルックアップ操作の詳細については、以下の例を参照してください。

関連概念

7 ページの『EIM ドメイン』
ここでは、ドメインを使用してすべての ID を保管する方法を説明します。

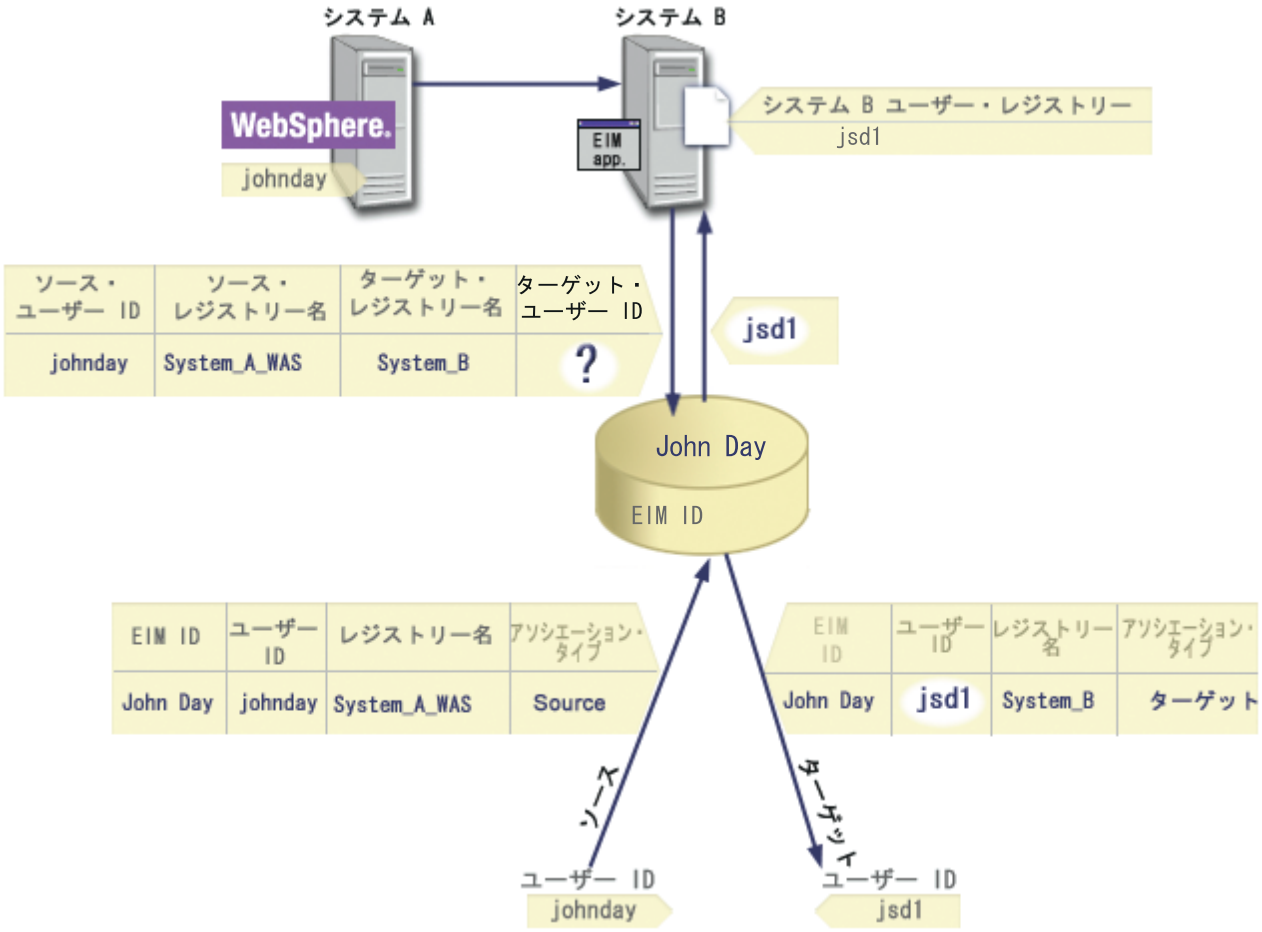
23 ページの『ポリシー・アソシエーション』
ここでは、複数のユーザー ID とユーザー・レジストリー内の単一ユーザー ID との間の関係を記述する、ポリシー・アソシエーションの使用法を学習します。

ルックアップ操作の例 : 例 1

ここでは、既知のユーザー ID を基にした特定の ID アソシエーションからターゲット・ユーザー ID を戻すルックアップ操作が、検索フローによって処理される方法を学習するための例を示します。

図 11 では、 ユーザー ID `johnday` がシステム A 上で Lightweight Third-Party Authentication (LPTA) を使用して、 WebSphere Application Server に認証します。システム A 上の WebSphere Application Server は、 システム B 上の統合プログラムを呼び出して、システム B のデータにアクセスします。統合プログラムは EIM (エンタープライズ識別マッピング) API を使用して、 EIM ルックアップ操作をこの操作におけるソースであるシステム A 上のユーザー ID に基づいて実行します。アプリケーションは、ソース・ユーザー ID として `johnday`、ソース EIM レジストリー定義名として `System_A_WAS`、ターゲット EIM レジストリー定義名として `System_B` をそれぞれ提供してこの操作を実行します。このソース情報は EIM に渡され、 EIM ルックアップ操作によってこの情報と一致する ID ソース・アソシエーションが検出されます。 EIM ID 名 `John Day` を使用して、EIM ルックアップ操作は、 `System_B` のターゲット EIM レジストリー定義名に一致する、この ID に対する ID ターゲット・アソシエーションを検索します。一致するターゲット・アソシエーションが検出されると、EIM ルックアップ操作は、 `jsd1` ユーザー ID をアプリケーションに戻します。

図 11: EIM ルックアップ操作が、既知のユーザー ID `johnday` を基にした特定の ID アソシエーションからターゲット・ユーザー ID を戻す



ルックアップ操作の例 : 例 2

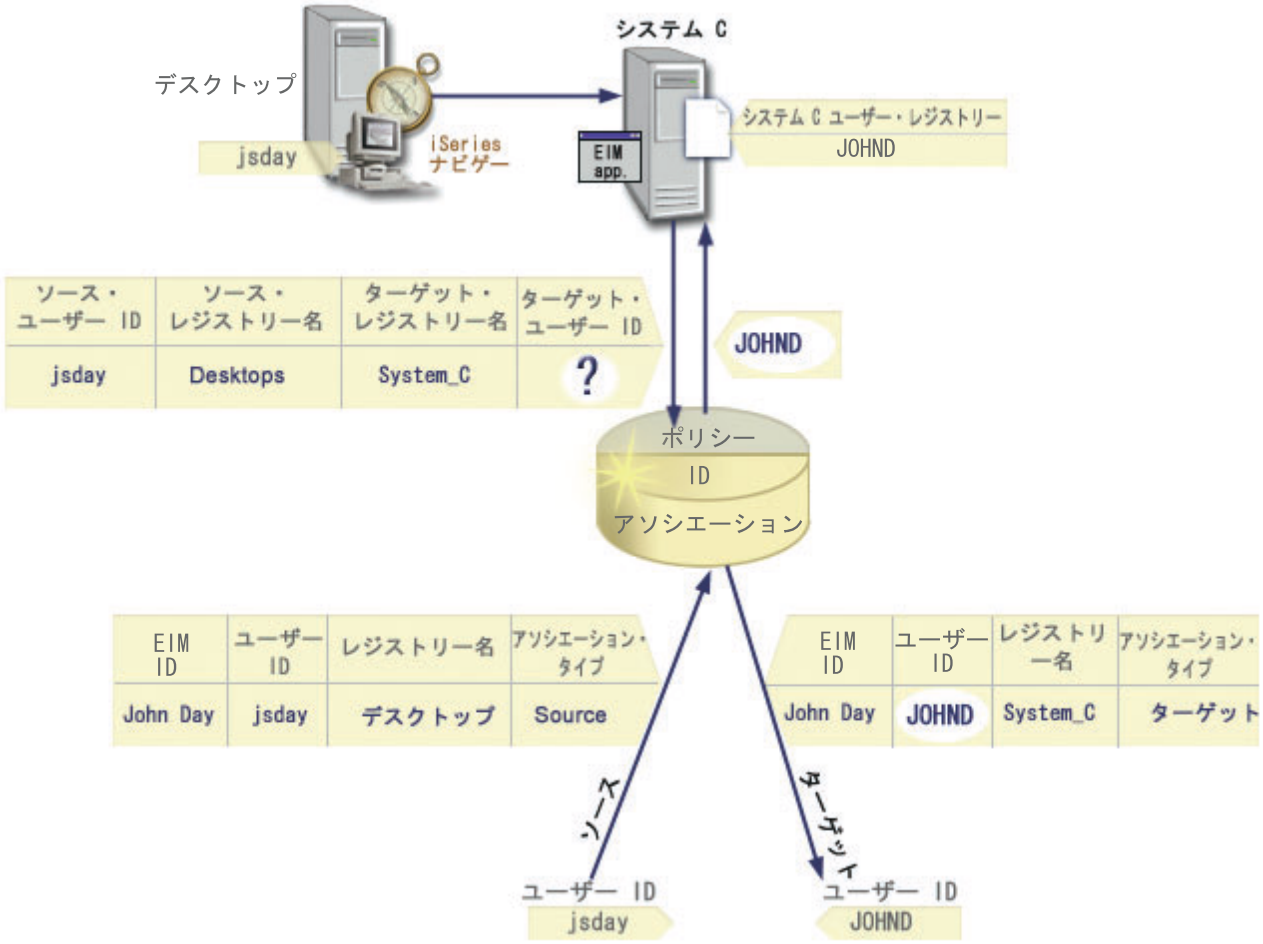
ここでは、既知の Kerberos プリンシパルを基にした特定の ID アソシエーションからターゲット・ユーザー ID を戻すルックアップ操作が、検索フローによって処理される方法を学習するための例を示します。

図 12 では、 管理者が Windows Active Directory レジストリー内の Windows ユーザーを、 i5/OS ユーザー・プロファイルにマップすることを考えています。 Kerberos が Windows が使用する認証方式で、管理者がそれを EIM 内に定義した時点での Windows Active Directory レジストリーの名前は、 Desktops です。 管理者がマップ元として考えているユーザー ID は、jsday という名の Kerberos プリンシパルです。管理者がそれを EIM 内に定義した時点での i5/OS レジストリーの名前は System_C で、 管理者がマップ先として考えているユーザー ID は、JOHND という名のユーザー・プロファイルです。

管理者は John Day という名の EIM ID を作成します。 その後この EIM ID に、以下の 2 つのアソシエーションを追加します。

- Desktops レジストリー内の jsday という名の Kerberos プリンシパルに対するソース・アソシエーション。
- System_C レジストリー内の JOHND という名の i5/OS ユーザー・プロファイルに対するターゲット・アソシエーション。

図 12: EIM ルックアップ操作が、既知の Kerberos プリンシパル jsday を基にした 特定の ID アソシエーションからターゲット・ユーザー ID を戻す



この構成では、次のようにして、マッピング・ルックアップ操作が Kerberos プリンシパルから i5/OS ユーザー・プロファイルにマップできます。

ソース・ユーザー ID およびレジストリー	--->	EIM ID	--->	ターゲット・ユーザー ID
Desktops レジストリー内の jsday	--->	John Day	--->	JOHND (System_C レジストリー内)

ルックアップ操作検索は、次のように行われます。

1. ユーザー jsday が、Windows Active Directory レジストリー Desktops 内のその Kerberos プリンシパルにより、Windows にログオンして認証します。
2. ユーザーが iSeries ナビゲーターを開いて、System_C 上のデータにアクセスします。
3. i5/OS が EIM API を使用し、ソース・ユーザー ID jsday、ソース・レジストリー Desktops、およびターゲット・レジストリー System_C を使用して EIM ルックアップ操作を実行します。
4. マッピング・ルックアップがソース・レジストリー Desktops、およびターゲット・レジストリー System_C に対して使用可能かどうかを、 EIM ルックアップ操作がチェックします。それらは使用可能です。
5. ルックアップ操作は、ソース・レジストリー Desktops 内の、 提供されたソース・ユーザー ID jsday に一致する特定の ID ソース・アソシエーションをチェックします。

6. ルックアップ操作は、一致する ID ソース・アソシエーションを使用して、 適切な EIM ID 名を判別します。それは John Day です。
7. ルックアップ操作はこの EIM ID 名を使用して、 指定されたターゲット EIM レジストリー定義名 System_C に一致する、 その EIM ID に対する ID ターゲット・アソシエーションを検索します。
8. ID ターゲット・アソシエーションが存在する場合、ルックアップ操作はターゲット・アソシエーションに定義されたターゲット・ユーザー ID JOHND を戻します。
9. マッピング・ルックアップ操作が完了すると、iSeries ナビゲーターが JOHND ユーザー・プロファイルの下で実行を開始します。 iSeries ナビゲーター内でリソースにアクセスし、アクションを実行するユーザーの権限は、 jsday ユーザー ID に定義された権限ではなく、 JOHND ユーザー・プロファイルに定義された権限によって判別されます。

ルックアップ操作の例 : 例 3

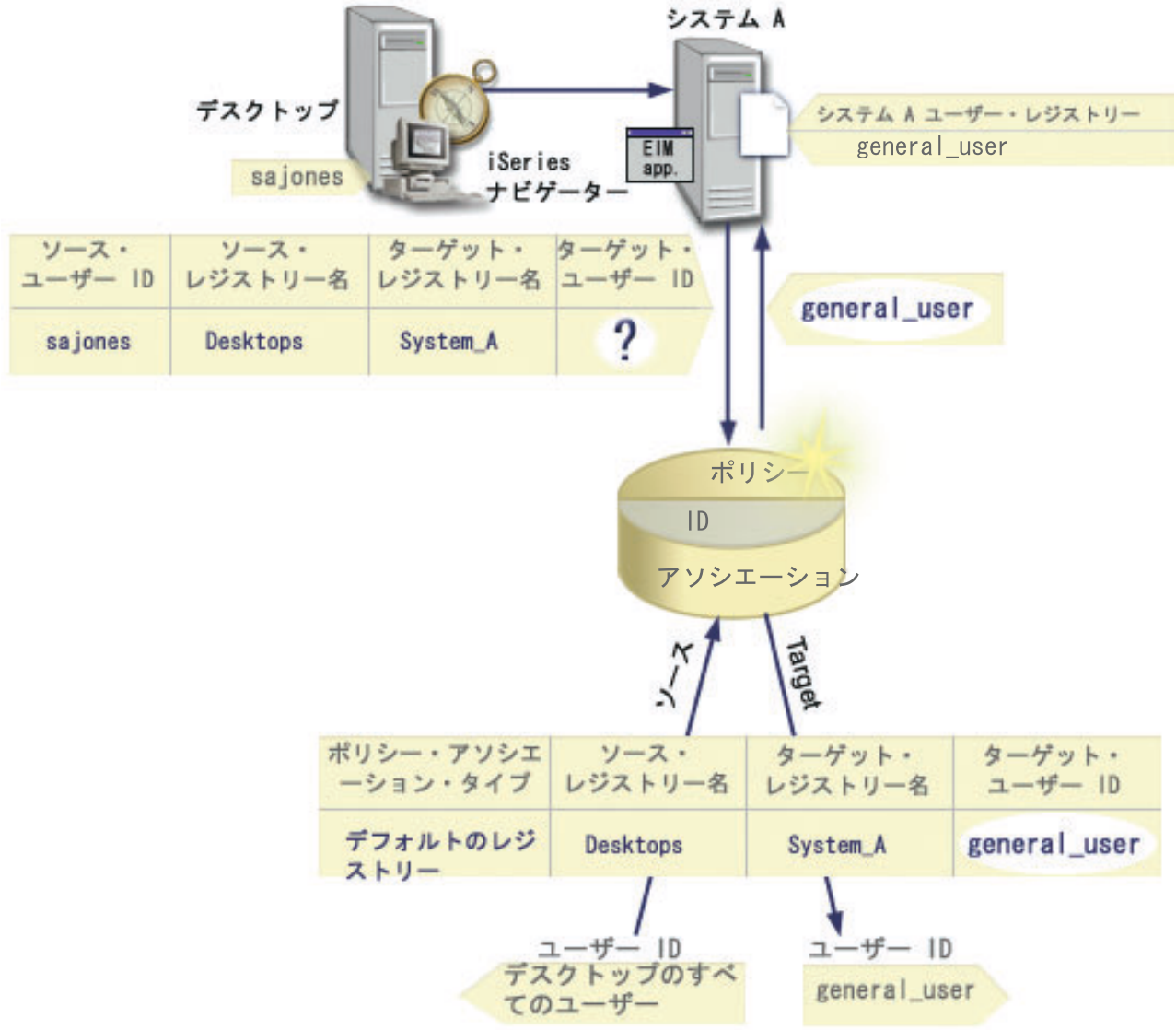
ここでは、デフォルトのレジストリー・ポリシー・アソシエーションからターゲット・ユーザー ID を戻すルックアップ操作が、検索フローによって処理される方法を学習するための例を示します。

図 13 では、 管理者は Windows Active Directory レジストリー内のすべてのデスクトップ・ワークステーション・ユーザーを、 EIM (エンタープライズ識別マッピング) 内で管理者が System_A と名付けた i5/OS レジストリー内の、general_user という名前の単一の i5/OS ユーザー・プロファイルにマップすることを考えています。 Kerberos が Windows が使用する認証方式で、管理者がそれを EIM 内に定義した時点での Windows Active Directory レジストリーの名前は、 Desktops です。 管理者がマップ元として考えている ユーザー ID の 1 つは、sajones という名の Kerberos プリンシパルです。

管理者は、以下の情報を使用して、デフォルトのレジストリー・ポリシー・アソシエーションを作成します。

- ソース・レジストリー Desktops
- ターゲット・レジストリー System_A.
- ターゲット・ユーザー ID general_user

図 13: ルックアップ操作が、デフォルトのレジストリー・ポリシー・アソシエーションからターゲット・ユーザー ID を戻す



この構成では、次のようにして、マッピング・ルックアップ操作が、sajones プリンシパルも含め、Desktops レジストリー内のすべての Kerberos プリンシパルを、 general_user という名前の i5/OS ユーザー・プロファイルにマップできます。

ソース・ユーザー ID およびレジストリー	--->	デフォルトのレジストリー・ポリシー・アソシエーション	--->	ターゲット・ユーザー ID
Desktops レジストリー内の sajones	--->	デフォルトのレジストリー・ポリシー・アソシエーション	--->	general_user (System_A レジストリー内)

ルックアップ操作検索は、次のように行われます。

1. ユーザー sajones が、Desktops レジストリー内の Kerberos プリンシパルによって、その Windows デスクトップにログオンし、認証します。
2. ユーザーが iSeries ナビゲーターを開いて、System A 上のデータにアクセスします。

3. i5/OS が EIM API を使用し、ソース・ユーザー ID sajones、ソース・レジストリー Desktops、およびターゲット・レジストリー System_A を使用して EIM ルックアップ操作を実行します。
4. マッピング・ルックアップがソース・レジストリー Desktops、およびターゲット・レジストリー System_A に対して使用可能かどうかを、 EIM ルックアップ操作がチェックします。それらは使用可能です。
5. ルックアップ操作は、ソース・レジストリー Desktops 内の、 提供されたソース・ユーザー ID sajones に一致する特定の ID ソース・アソシエーションをチェックします。一致する ID アソシエーションを検出されません。
6. ルックアップ操作は、ドメインがポリシー・アソシエーションを使用できるかどうかをチェックします。それは使用できます。
7. ルックアップ操作は、ターゲット・レジストリー (System_A) がポリシー・アソシエーションを使用できるかどうかをチェックします。それは使用できます。
8. ルックアップ操作は、ソース・レジストリー (Desktops) が X.509 レジストリーであるかどうかをチェックします。それは異なります。
9. ルックアップ操作は、ソース・レジストリー定義名 (Desktops) およびターゲット・レジストリー定義名 (System_A) と一致する、デフォルトのレジストリー・ポリシー・アソシエーションがあるかどうかをチェックします。
10. ルックアップ操作はそれがあると判別し、ターゲット・ユーザー ID として general_user を戻します。

EIM ルックアップ操作があいまいな結果を戻すことがあります。これが生じるのは、たとえば、複数のターゲット・ユーザー ID が、指定されたルックアップ操作の基準と一致する場合です。 i5/OS アプリケーションおよびプロダクトを含め、いくつかの EIM 対応アプリケーションは、これらのあいまいな結果を処理するようには設計されていないため、失敗するか、または予期しない結果を戻す可能性があります。この状態を解決するための処置を取る必要があるかもしれません。たとえば、ご使用の EIM 構成を変更するか、またはそれぞれのターゲット・ユーザー ID ごとにルックアップ情報を定義して、一致するターゲット・ユーザー ID が複数生じないようにできます。また、マッピングをテストして、変更内容が期待通りに作動するかを判別します。

ルックアップ操作の例 : 例 4

ここでは、グループ・レジストリー定義のメンバーであるユーザー・レジストリー内でターゲット・ユーザー ID を戻すルックアップ操作が、検索フローによって処理される方法を学習するための例を示します。

管理者は、Windows ユーザーを i5/OS ユーザー・プロファイルにマップすることを考えています。 Kerberos が Windows の使用する認証方式で、管理者が EIM (エンタープライズ識別マッピング) で定義した際の Kerberos レジストリーの名前はDesktop_A です。管理者がマップ元にするユーザー ID は、jday という名前の Kerberos プリンシパルです。管理者がそれを EIM 内に定義した時点での i5/OS レジストリー定義の名前は Group_1 で、管理者がマップ先として考えているユーザー IDは、JOHND という名のユーザー・プロファイルです。これは、3 つの個々のレジストリー System_B、System_C、および System_D にあります。個々のレジストリーはそれぞれ、Group_1 グループ・レジストリー定義のメンバーです。

管理者は John Day という名の EIM ID を作成します。 その後この EIM ID に、以下の 2 つのアソシエーションを追加します。

- Desktop_A レジストリー内の jday という名の Kerberos プリンシパルに対するソース・アソシエーション。
- Group_1 レジストリー内の JOHND という名の i5/OS ユーザー・プロファイルに対するターゲット・アソシエーション。

この構成では、次のようにして、マッピング・ルックアップ操作が Kerberos プリンシパルから i5/OS ユーザー・プロファイルにマップできます。

ソース・ユーザー ID およびレジストリー	--->	EIM ID	--->	ターゲット・ユーザー ID
Desktop_Aレジストリー内の jday	--->	John Day	--->	JOHND (Group_1 グループ・レジストリー定義内)

ルックアップ操作検索は、次のように行われます。

1. ユーザー (jday) がログオンし、Desktop_A 上で Windows に対して認証します。
2. ユーザーが iSeries ナビゲーターを開いて、System_B 上のデータにアクセスします。
3. i5/OS が EIM API を使用し、ソース・ユーザー ID jday、ソース・レジストリー Desktop_A、およびターゲット・レジストリー System_B を使用して EIM ルックアップ操作を実行します。
4. マッピング・ルックアップがソース・レジストリー (Desktop_A)、およびターゲット・レジストリー (System_B) に対して使用可能かどうかを、EIM ルックアップ操作がチェックします。
5. ルックアップ操作は、ソース・レジストリー Desktop_A 内の、 提供されたソース・ユーザー ID jday に一致する特定の個々のソース・アソシエーションをチェックします。
6. ルックアップ操作は、一致するソース・アソシエーションを使用して、適切な EIM ID 名を判別します。それは John Day です。
7. ルックアップ操作はこの EIM ID 名を使用して、 指定されたターゲット EIM レジストリー定義名 System_B に一致する、 その EIM ID に対する個々のターゲット・アソシエーションを検索します。(存在しません。)
8. ルックアップ操作が、ソース・レジストリー (Desktop_A) がいずれかのグループ・レジストリー定義のメンバーかどうかを確認します。(それは異なります。)
9. ルックアップ操作が、ターゲット・レジストリー (System_B) がいずれかのグループ・レジストリー定義のメンバーかどうかを確認します。これは Group_1 グループ・レジストリー定義のメンバーです。
10. ルックアップ操作は EIM ID 名を使用して、 指定されたターゲット EIM レジストリー定義名 Group_1 に一致する、 その EIM ID に対する個々のターゲット・アソシエーションを検索します。
11. 個々のターゲット・アソシエーションが存在する場合、ルックアップ操作はターゲット・アソシエーションに定義されたターゲット・ユーザー ID JOHND を戻します。

注: 複数のターゲット・ユーザー ID が、指定されたルックアップ操作基準と一致すると、EIM ルックアップ操作があいまいな結果を戻すことがあります。EIM が単一のターゲット・ユーザー ID を戻すことができないために、i5/OS アプリケーションおよびプロダクトを含め、これらのあいまいな結果を処理するようには設計されていない EIM 対応アプリケーションは失敗するか、または予期しない結果を戻す可能性があります。この状態を解決するための処置を取る必要があるかもしれません。たとえば、ご使用の EIM 構成を変更するか、またはそれぞれのターゲット・ユーザー ID ごとにルックアップ情報を定義して、一致するターゲット・ユーザー ID が複数生じないようにできます。 マッピングをテストして、変更内容が期待通りに作動するかを判別することができます。

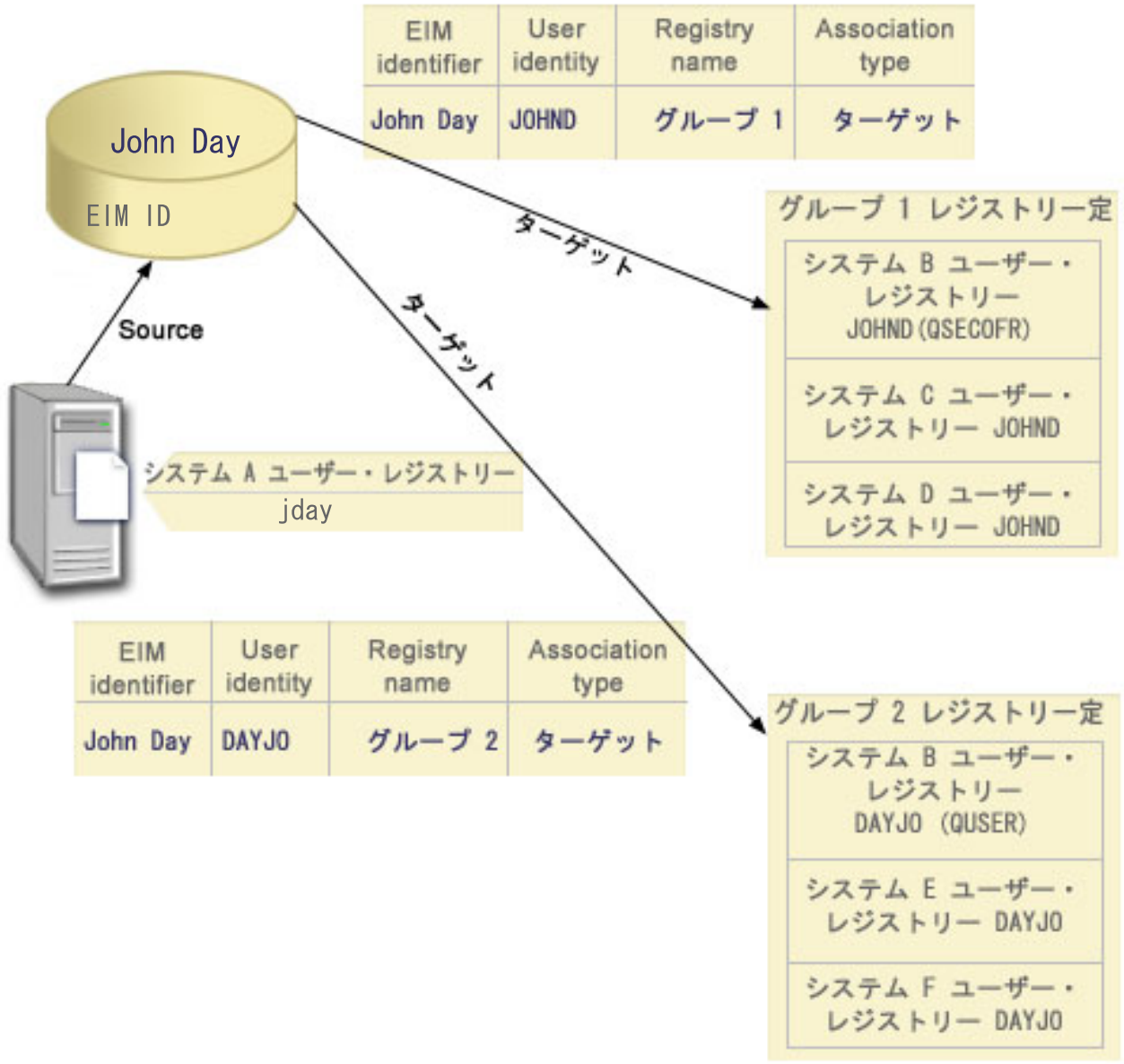
ルックアップ操作の例 : 例 5

この例では、グループ・レジストリー定義が関係する、あいまいな結果を戻すルックアップ操作について学習します。

複数のターゲット・ユーザー ID が、指定されたルックアップ基準と一致すると、マッピング・ルックアップ操作があいまいな結果を戻すことがあります。あいまいな結果の状態は、EIM を使用するアプリケーションでの失敗、または予期しない結果の原因になるので、この状態を予防または解決する処置を取ることが必要です。

特に、個々のユーザー・レジストリー定義を複数のグループ・レジストリー定義のメンバーとして指定すると、ルックアップ操作があいまいな結果を戻す場合があることに注意してください。個々のユーザー・レジストリー定義が複数のグループ・レジストリー定義のメンバーであり、グループ・レジストリー定義をソース・レジストリーかターゲット・レジストリーのどちらかとして使用する個々の EIM ID アソシエーションまたはポリシー・アソシエーションを作成する場合、ルックアップ操作はあいまいな結果を戻すことがあります。たとえば、実行するシステム・タスクの 2 つの異なるタイプに 2 つの異なるユーザー ID を使用することがあります。QSECOFR 権限を持つユーザー ID を必要とするセキュリティー管理者としてタスクを実行し、QUSER 権限を持つユーザー ID を必要とする典型的なユーザー・タスクを実行する場合などです。両方のユーザー ID が、2 つの異なるグループ・レジストリー定義のメンバーである個々のユーザー・レジストリー内にあり、両方のターゲット・ユーザー ID に対してターゲット ID アソシエーションを作成する場合、ルックアップ操作は両方のターゲット・ユーザー ID を検出します。そのため、あいまいな結果を戻します。

以下の例は、個々のユーザー・レジストリーを 2 つのグループ・レジストリー定義のメンバーとして指定し、かつグループ・レジストリー定義の 1 つを 2 つの個別の EIM ID アソシエーションでターゲット・レジストリーとして指定した場合に、どのようにこの問題が発生するかを説明しています。



例:

John Day は、System B ユーザー・レジストリーというシステム・レジストリー定義内に以下のユーザー ID を持っています。

- JOHND
- DAYJO

System B ユーザー・レジストリーは、次のグループ・レジストリー定義のメンバーです。

- Group 1
- Group 2

EIM ID である John Day には、以下の指定がある 2 つのターゲット・アソシエーションを持っています。

| • ターゲット・アソシエーション: ターゲット・レジストリーは Group 1 で、System B ユーザー・レジストリーにユーザー ID JOHND が入っています。
| • ターゲット・アソシエーション: ターゲット・レジストリーは Group 2 で、System B ユーザー・レジストリーにユーザー ID DAYJO が入っています。

この状況では、マッピング・ルックアップ操作はあいまいな結果を戻します。これは、複数のターゲット・ユーザー ID が、指定されたテスト基準と一致する、つまり両方のユーザー ID (JOHND および DAYOJO) が指定されたルックアップ基準と一致するためです。

同様に、グループ・レジストリー定義をターゲット・レジストリーとして使用する 2 つのポリシー・アソシエーション (個々の EIM ID アソシエーションではない) を作成すると、マッピング・ルックアップ操作はあいまいな結果を戻すことがあります。

ルックアップ操作が、グループ・レジストリー定義の関係するあいまいな結果を戻さないようにするため、以下のガイドラインを考慮してください。

| • 個々のユーザー・レジストリーを、複数のグループ・レジストリー定義のメンバーとして指定しないでください。
| • グループ・レジストリー定義をソース・レジストリーまたはターゲット・レジストリーとして使用する、個々の EIM ID アソシエーションまたはポリシー・アソシエーションの作成時には注意が必要です。グループ・レジストリー定義が、1 つのグループ・レジストリー定義のメンバーであることを確認してください。ターゲット・グループ・レジストリー定義のメンバーが、別のグループ・レジストリー定義のメンバーでもある場合、ルックアップ操作があいまいな結果を戻す可能性があることを意識しておく必要があります。
| • 個々のレジストリー定義を複数のグループ・レジストリー定義のメンバーとして指定し、かつこれらのグループ・レジストリー定義の 1 つをソース・レジストリーかターゲット・レジストリーとして使用する個々の ID アソシエーションまたはポリシー・アソシエーションを作成するために、あいまいな結果が戻される状態が生じる場合には、各アソシエーション内のターゲット・ユーザー ID ごとに固有のルックアップ情報を定義して、さらに検索を絞り込むことができます。

John Day の例の場合、ターゲット・ユーザー ID ごとに以下のルックアップ情報を定義できます。

| • JOHND の場合: Administrator をルックアップ情報として定義する
| • DAYJO の場合: User をルックアップ情報として定義する

ただし、iSeries Access for Windows などの 基本 i5/OS アプリケーションは、ルックアップ情報を使用して、ルックアップ操作によって戻された複数のターゲット・ユーザー ID を区別することはできません。したがって、ドメインに対するアソシエーションを再定義して、マッピング・ルックアップ操作が単一のターゲット・ユーザー ID を戻すことができるようにし、 基本 i5/OS アプリケーションが正常にルックアップ操作を実行して ID をマップできるようにする必要があるかもしれません。

EIM マッピング・ポリシー・サポートおよび使用可能化

ここでは、ドメインに対してポリシー・アソシエーションを使用可能にしたり使用不可にしたりする方法を説明します。

EIM (エンタープライズ識別マッピング) マッピング・ポリシー・サポートにより、 EIM ドメイン内の特定の ID のアソシエーションだけでなく、ポリシー・アソシエーションも使用できます。ポリシー・アソシエーションは ID アソシエーションの代わりに、またはそれと組み合わせて使用できます。

EIM マッピング・ポリシー・サポートは、ドメイン全体、またはそれぞれの特定のターゲット・ユーザー・レジストリーに対して、ポリシー・アソシエーションの使用を可能にしたり不可にしたりする手段を提供します。また EIM により、特定のレジストリーが、一般にマッピング・ルックアップ操作に参加できるかどうかを設定できます。したがって、マッピング・ポリシー・サポートを使用して、マッピング・ルックアップ操作が結果を戻す仕方を、より正確に制御できます。

EIM ドメインのデフォルト設定では、ポリシー・アソシエーションを使用するマッピング・ルックアップが、ドメインに対して使用不可になっています。ポリシー・アソシエーションの使用がドメインに対して使用不可の場合には、そのドメインに対するすべてのマッピング・ルックアップ操作は、ユーザー ID および EIM ID 間の特定の ID アソシエーションのみを使用して結果を戻します。

個々のレジストリーのデフォルト設定では、マッピング・ルックアップ参加が使用可能であり、ポリシー・アソシエーションは使用不可です。個々のターゲット・レジストリーに対してポリシー・アソシエーションを使用可能にする場合には、この設定がドメインに対しても使用可能になっていることを確認する必要があります。

次の 3 つの方法の 1 つで、個々のレジストリーに対するマッピング・ルックアップ参加およびポリシー・アソシエーションの使用を構成できます。

- マッピング・ルックアップ操作が、特定のレジストリーに対して全く使用できないようにする。つまり、そのレジストリーに関係するマッピング・ルックアップ操作を実行するアプリケーションは、結果を戻さない。
- マッピング・ルックアップ操作が、ユーザー ID および EIM ID 間の特定の ID アソシエーションのみを使用できるようにする。マッピング・ルックアップは、レジストリーに対して使用可能だが、ポリシー・アソシエーションの使用は、そのレジストリーに関して使用不可である。
- マッピング・ルックアップ操作が、特定の ID アソシエーションが存在する場合はそれらを使用し、特定の ID アソシエーションが存在しない場合 (すべての設定が使用可能となっている) はポリシー・アソシエーションを使用できるようにする。

関連タスク

99 ページの『ドメインのポリシー・アソシエーションを使用可能にする』

107 ページの『ターゲット・レジストリーに対してマッピング・ルックアップ・サポートおよびポリシー・アソシエーションを使用可能にする』

EIM アクセス制御

ここでは、ユーザーが LDAP ユーザー・グループにアクセスし、ドメインを制御できるようにする方法を説明します。

EIM (エンタープライズ識別マッピング) ユーザーは、特定のドメインに事前定義された Lightweight Directory Access Protocol (LDAP) ユーザー・グループ内のメンバーに基づく EIM アクセス制御を所有するユーザーです。あるユーザーの EIM *アクセス制御* を指定すると、そのユーザーが特定のドメインに対する特定の LDAP ユーザー・グループに追加されます。 各 LDAP グループは、そのドメインに対する特定の EIM 管理用タスクを実行する権限を持っています。ルックアップ操作を含め、どのタイプの管理用タスクを EIM ユーザーが実行できるかは、 EIM ユーザーが属するアクセス制御グループによって判別されます。

注: EIM を構成するには、ユーザーが特定の 1 つのシステムによってではなく、ネットワークのコンテキスト内で信頼されていることを証明する必要があります。 EIM を構成する権限は、i5/OS ユーザー・プロファイル権限ではなく、 EIM アクセス制御権限に基づいています。 EIM はネットワーク・リソースですが、1 つの特定のシステムのリソースではありません。したがって、EIM は構成のための

*ALLOBJ や *SECADM といった、i5/OS 固有の特殊権限を認識しません。ただし、EIM が構成されたならば、タスクを実行する権限を、i5/OS ユーザー・プロファイルを含め、多数の異なるユーザー・タイプに基づいて決定できます。たとえば、IBM Directory Server for iSeries (LDAP) は、 *ALLOBJ および *IOSYSCFG 特殊権限を持つ i5/OS プロファイルを、ディレクトリー管理者として扱います。

EIM 管理者アクセス制御を持つユーザーだけが、他のユーザーを EIM アクセス制御グループに追加したり、他のユーザーのアクセス制御設定を変更したりできます。あるユーザーが EIM アクセス制御グループのメンバーになる前に、そのユーザーは EIM ドメイン・コントローラーとして機能するディレクトリー・サーバー内に項目を持っていなければなりません。また特定のタイプのユーザーだけが、EIM アクセス制御グループのメンバーとなることができます。そのユーザー ID は、それがディレクトリー・サーバーに定義されている限り、 Kerberos プリンシパル、LDAP 識別名、または i5/OS ユーザー・プロファイルのいずれの形式でもかまいません。

注 : EIM において Kerberos プリンシパル・ユーザー・タイプを使用可能にするには、システム上にネットワーク認証サービスが構成されていなければなりません。 EIM において i5/OS ユーザー・プロファイル・タイプを使用可能にするには、ディレクトリー・サーバー上でシステム・オブジェクト接尾部を構成しなければなりません。これにより、ディレクトリー・サーバーは i5/OS ユーザー・プロファイルなどの i5/OS システム・オブジェクトを参照できます。

個々の EIM 権限グループが実行できる機能の説明を以下に示します。

Lightweight Directory Access Protocol (LDAP) 管理者

LDAP 管理者は、ディレクトリー全体の管理者の、ディレクトリー内での特殊識別名 (DN) です。 したがって LDAP 管理者は、すべての EIM 管理機能へのアクセスと、ディレクトリー全体へのアクセスを行います。このアクセス制御を持つユーザーは、以下の機能を実行できます。

- ドメインの作成
- ドメインの削除
- EIM ID の作成と除去
- EIM レジストリー定義の作成と除去
- ソース、ターゲット、管理の各アソシエーションの作成と除去
- ポリシー・アソシエーションの作成と除去
- 証明書フィルターの作成と除去
- ドメインに対するポリシー・アソシエーションの使用を使用可能および使用不可にする
- レジストリーに対するマッピング・ルックアップを使用可能および使用不可にする
- レジストリーに対するポリシー・アソシエーションの使用を使用可能および使用不可にする
- EIM ルックアップ操作の実行
- ID アソシエーション、ポリシー・アソシエーション、証明書フィルター、EIM ID、および EIM レジストリー定義の検索
- EIM アクセス制御情報の情報の追加、除去、リスト
- レジストリー・ユーザーの信任状情報の変更、除去

EIM 管理者

このアクセス制御グループのメンバーシップは、ユーザーがこの EIM ドメイン中の EIM データをすべて管理できるようにします。このアクセス制御を持つユーザーは、以下の機能を実行できます。

- ドメインの削除

- EIM ID の作成と除去
- EIM レジストリー定義の作成と除去
- ソース、ターゲット、管理の各アソシエーションの作成と除去
- ポリシー・アソシエーションの作成と除去
- 証明書フィルターの作成と除去
- ドメインに対するポリシー・アソシエーションの使用を使用可能および使用不可にする
- レジストリーに対するマッピング・ルックアップを使用可能および使用不可にする
- レジストリーに対するポリシー・アソシエーションの使用を使用可能および使用不可にする
- EIM ルックアップ操作の実行
- ID アソシエーション、ポリシー・アソシエーション、証明書フィルター、EIM ID、および EIM レジストリー定義の検索
- EIM アクセス制御情報の情報の追加、除去、リスト
- レジストリー・ユーザーの信任状情報の変更、除去

ID 管理者

このアクセス制御グループのメンバーシップは、ユーザーが EIM ID の追加や変更、またソースおよび管理のアソシエーションの管理を行えるようにします。このアクセス制御を持つユーザーは、以下の機能を実行できます。

- EIM ID の作成
- ソース・アソシエーションの追加と除去
- 管理アソシエーションの追加と除去
- EIM ルックアップ操作の実行
- ID アソシエーション、ポリシー・アソシエーション、証明書フィルター、EIM ID、および EIM レジストリー定義の検索

EIM マッピング操作

このアクセス制御グループのメンバーシップは、ユーザーが EIM マッピング・ルックアップ操作を行えるようにします。このアクセス制御を持つユーザーは、以下の機能を実行できます。

- EIM ルックアップ操作の実行
- ID アソシエーション、ポリシー・アソシエーション、証明書フィルター、EIM ID、および EIM レジストリー定義の検索

レジストリー管理者

このアクセス制御グループのメンバーシップは、ユーザーがすべての EIM レジストリー定義を管理できるようにします。このアクセス制御を持つユーザーは、以下の機能を実行できます。

- ターゲット・アソシエーションの追加と除去
- ポリシー・アソシエーションの作成と除去
- 証明書フィルターの作成と除去
- レジストリーに対するマッピング・ルックアップを使用可能および使用不可にする
- レジストリーに対するポリシー・アソシエーションの使用を使用可能および使用不可にする
- EIM ルックアップ操作の実行

- ID アソシエーション、ポリシー・アソシエーション、証明書フィルター、EIM ID、および EIM レジストリー定義の検索

選択されたレジストリーの管理者

このアクセス制御グループのメンバーシップは、指定されたユーザー・レジストリー定義 (Registry_X など) のみの EIM 情報を管理できるようにします。また、指定されたユーザー・レジストリー定義のターゲット・アソシエーションのみ、追加および除去できるようにします。マッピング・ルックアップ操作およびポリシー・アソシエーションの利点を最大限に活用するには、このアクセス制御を持つユーザーは、**EIM マッピング操作**アクセス制御も持っている必要があります。このアクセス制御により、特定の許可されたレジストリー定義に対して、以下の機能を実行できます。

- 指定された EIM レジストリー定義のみに対するターゲット・アソシエーションの作成、除去、およびリスト
- デフォルトのドメイン・ポリシー・アソシエーションの追加と除去
- 指定されたレジストリー定義のみに対するポリシー・アソシエーションの追加と除去
- 指定されたレジストリー定義のみに対する証明書フィルターの追加と除去
- 指定されたレジストリー定義のみに対するマッピング・ルックアップを使用可能および使用不可にする
- 指定されたレジストリー定義のみに対するポリシー・アソシエーションの使用を使用可能および使用不可にする
- EIM ID の検索
- 指定されたレジストリー定義のみに対する ID アソシエーションと証明書フィルターの検索
- 指定されたレジストリー定義のみに対する EIM レジストリー定義情報の検索

注: 指定されたレジストリー定義がグループ・レジストリー定義である場合、選択されたレジストリーに対する管理者アクセス制御を持つユーザーは、グループのメンバーにではなく、グループのみに管理者アクセス権限を持ちます。

選択されたレジストリーの管理者と **EIM マッピング・ルックアップ操作**の両方のアクセス制御を持つユーザーは、以下の機能を実行する能力を持ちます。

- 指定されたレジストリーのみに対するポリシー・アソシエーションの追加と除去
- EIM ルックアップ操作の実行
- すべての ID アソシエーション、ポリシー・アソシエーション、証明書フィルター、EIM ID、 および EIM レジストリー定義の検索

信任状ルックアップ

このアクセス制御グループは、ユーザーがパスワードなどの信任状情報を検索できるようにします。

このアクセス制御を持つユーザーが追加の EIM 操作を実行する場合、そのユーザーは、対象となる EIM 操作の権限を提供するアクセス制御グループのメンバーであることが必要です。たとえば、このアクセス制御を持つユーザーがソース・アソシエーションからターゲット・アソシエーションを検索する場合、そのユーザーは以下のアクセス制御グループのいずれかのメンバーである必要があります。

- EIM 管理者
- ID 管理者
- EIM マッピング・ルックアップ操作
- レジストリー管理者

EIM アクセス制御グループ : API 権限

ここでは、API が実行する EIM (エンタープライズ識別マッピング) 操作により編成される表を示します。

次の各表は、各 EIM API、各種の EIM アクセス制御グループ、およびアクセス制御グループが特定の EIM 機能を実行する権限を持つかどうかを示しています。

表 1. ドメインの処理

EIM API	LDAP 管理者	EIM 管理者	ID 管理者	EIM マッピング・ルックアップ	レジストリー管理者	選択されたレジストリーの管理者
eimChangeDomain	X	X	-	-	-	-
eimCreateDomain	X	-	-	-	-	-
eimDeleteDomain	X	X	-	-	-	-
eimListDomains	X	X	-	-	-	-

表 2. ID の処理

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimAddIdentifier	X	X	X	-	-	-
eimChangeIdentifier	X	X	X	-	-	-
eimListIdentifiers	X	X	X	X	X	X
eimRemoveIdentifier	X	X	-	-	-	-
eimGetAssociated Identifiers	X	X	X	X	X	X

表 3. レジストリーの処理

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimAddApplication Registry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChange RegistryUser	X	X	-	-	X	X
eimChangeRegistryAlias	X	X	-	-	X	X
eimGetRegistry NameFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistry Associations	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X
eimListRegistry Users	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

表 4. ID アソシエーションの処理： `eimAddAssociation()` および `eimRemoveAssociation()` API の場合、追加または除去されるアソシエーション・タイプを判断する 4 つのパラメーターがあります。 これらの API に対する権限は、これらのパラメーター内で指定されているアソシエーション・タイプによって異なります。以下の表には、これらの API に対するアソシエーション・タイプが記載されています。

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimAddAssociation (管理)	X	X	X	-	-	-
eimAddAssociation (ソース)	X	X	X	-	-	-
eimAddAssociation (ソースおよび ターゲット)	X	X	X	-	X	X
eimAddAssociation (ターゲット)	X	X	-	-	X	X
eimListAssociations	X	X	X	X	X	X
eimRemoveAssociation (管理)	X	X	X	-	-	-
eimRemoveAssociation (ソース)	X	X	X	-	-	-
eimRemoveAssociation (ソース および ターゲット)	X	X	X	-	X	X
eimRemoveAssociation (ターゲット)	X	X	-	-	X	X

表 5. ポリシー・アソシエーションの処理

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimAddPolicyAssociation	X	X	-	-	X	X
eimAddPolicyFilter	X	X	-	-	X	X
eimListPolicyFilters	X	X	X	X	X	X
eimRemove PolicyAssociation	X	X			X	X
eimRemovePolicyFilter	-	-	-	-	-	

表 6. マッピングの処理

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimGetAssociatedIdentifier	X	X	X	X	X	X
eimGetTargetFromIdentifier	X	X	X	X	X	X
eimGetTargetFromSource	X	X	X	X	X	X

表 7. アクセスの処理

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimAddAccess	X	X	-	-	-	-
eimListAccess	X	X	-	-	-	-
eimListUserAccess	X	X	-	-	-	-
eimQueryAccess	X	X	-	-	-	-

表 7. アクセスの処理 (続き)

EIM API	LDAP 管理者	EIM 管理者	EIM ID 管理者	EIM マッピング・ルックアップ	EIM レジストリー管理者	EIM レジストリー X 管理者
eimRemoveAccess	X	X	-	-	-	-

EIM アクセス制御グループ : EIM タスク権限

ここでは、各種 EIM (エンタープライズ識別マッピング) アクセス制御グループと、 それらが実行できる EIM タスクとの間の関係を説明する表を示します。

LDAP 管理者は表にリストされていませんが、新規 EIM ドメインを作成するためには、このレベルのアクセス制御が必要です。 また、LDAP 管理者には EIM 管理者と同じアクセス制御がありますが、 EIM 管理者が LDAP 管理者アクセス制御を自動的に持つわけではありません。

表 8. 表 1: EIM アクセス制御グループ

EIM タスク	EIM 管理者	ID 管理者	EIM マッピング・ルックアップ操作	レジストリー管理者	選択されたレジストリーの管理者	信任状ルックアップ
ドメインの作成	-	-	-	-	-	
ドメインの削除	X	-	-	-	-	
ドメインの変更	X	-	-	-	-	
ドメインのポリシー・アソシエーションの使用可能化 / 使用不可化	X	-	-	-	-	
ドメインの検索	X	-	-	-	-	
システム・レジストリーの追加	X	-	-	-	-	
アプリケーション・レジストリーの追加	X	-	-	-	-	
レジストリーの除去	X	-	-	-	-	
レジストリーの変更	X	-	-	X	X	
レジストリーのマッピング・ルックアップの使用可能化 / 使用不可化	X	-	-	X	X	

表 8. 表 1: EIM アクセス制御グループ (続き)

EIM タスク	EIM 管理者	ID 管理者	EIM マッピング・ルックアップ操作	レジストリー管理者	選択されたレジストリーの管理者	信任状ルックアップ
レジストリーのポリシー・アソシエーションの使用可能化 / 使用不可化	X	-	-	X	X	
レジストリーの検索	X	X	X	X	X	
ID の追加	X	X	-	-	-	
ID の除去	X	-	-	-	-	
ID の変更	X	X	-	-	-	
ID の検索	X	X	X	X	X	
関連した ID の検索	X	X	X	X	X	
管理アソシエーションの追加 / 除去	X	X	-	-	-	
ソース・アソシエーションの追加 / 除去	X	X	-	-	-	
ターゲット・アソシエーションの追加 / 除去	X	-	-	X	X	
ポリシー・アソシエーションの追加 / 除去	X	-	-	X	X	
証明書フィルターの追加 / 除去	X	-	-	X	X	
証明書フィルターの検索	X	X	X	X	X	
アソシエーションの検索	X	X	X	X	X	
ポリシー・アソシエーションの検索	X	X	X	X	X	

表 8. 表 1: EIM アクセス制御グループ (続き)

EIM タスク	EIM 管理者	ID 管理者	EIM マッピング・ルックアップ操作	レジストリー管理者	選択されたレジストリーの管理者	信任状ルックアップ
ソース・アソシエーションからのターゲット関連の検索	X	X	X	X	-	
ID からのターゲット・アソシエーションの検索	X	X	X	X	X	
レジストリー・ユーザーの変更	X	-	-	X	X	
レジストリー・ユーザーの検索	X	X	X	X	X	
レジストリー別名の変更	X	-	-	X	X	
レジストリー別名の検索	X	X	X	X	X	
別名からのレジストリーの検索	X	X	X	X	X	
EIM アクセス制御の追加 / 除去	X	-	-	-	-	
アクセス制御グループ・メンバーの表示	X	-	-	-	-	
指定されたユーザーの EIM アクセス制御の表示	X	-	-	-	-	
EIM アクセス制御の照会	X	-	-	-	-	
信任状の変更	X	-	-	-	-	-
信任状の検索	X	-	-	-	-	X
1 - 指定されたレジストリー定義がグループ・レジストリー定義である場合、選択されたレジストリーに対する管理者アクセス制御を持つユーザーは、グループのメンバーにではなく、グループのみに管理者アクセス権限を持ちます。						

EIM 用の LDAP の概念

ここでは、Lightweight Directory Access Protocol (LDAP) を EIM (エンタープライズ識別マッピング) と一緒に使用する方法を説明します。

EIM は、LDAP サーバーをドメイン・コントローラーとして使用し、EIM データを保管します。したがって、企業内で EIM を構成および使用することに関連した LDAP の概念をいくらか理解しておく必要があります。たとえば、LDAP 識別名は、EIM を構成し EIM ドメイン・コントローラーに認証するためのユーザー ID として使用できます。

EIM の構成および使用についてより良く理解するために、 LDAP の以下の概念を理解する必要があります。

関連概念

5 ページの『EIM (エンタープライズ識別マッピング) の概念』
ここでは、EIM を正常にインプリメントするために理解しておくべき重要な EIM の概念について学びます。

識別名

ここでは、Lightweight Directory Access Protocol (LDAP) で識別名 (DN) を使用する方法について学習します。

識別名 (DN) は、ディレクトリー (LDAP) サーバー内の項目を一意的に識別し記述する LDAP 項目です。EIM (エンタープライズ識別マッピング) 構成ウィザードを使用して、EIM ドメイン情報を保存するようにディレクトリー・サーバーを構成できます。 EIM は ディレクトリー・サーバーを使用して EIM データを保管するので、 EIM ドメイン・コントローラーに認証する方法として識別名を使用できます。

識別名は、識別名だけでなく項目自体の名前から成り立っており、最下部から最上部まで順番に、 LDAP ディレクトリー内でその項目名より上にあるオブジェクトから成り立っています。完全識別名の例は、`cn=Tim Jones、o=IBM、c=US` です。各項目は、項目を命名するために使用される属性が少なくとも一つあります。この命名属性は、項目の相対識別名 (RDN™) と呼ばれます。 指定された RDN より上位の項目は、RDN の 53 ページの『親識別名』と呼ばれます。この例では、`cn=Tim Jones` という名前が項目に付けられるので、この名前がその項目の RDN になります。 `o=IBM、c=US` は、`cn=Tim Jones` の親 DN です。

EIM はディレクトリー・サーバーを使用して EIM データを保管するので、 ドメイン・コントローラーに認証するユーザー ID として、 識別名を使用することができます。また、iSeries サーバー用の EIM を構成するユーザー ID に、識別名を使用することもできます。たとえば、以下の事柄を行う場合に、識別名を使用できます。

- EIM ドメイン・コントローラーとして機能するようにディレクトリー・サーバーを構成する場合。これは、ディレクトリー・サーバー用の LDAP 管理者を識別する識別名を作成し、使用することによって行います。ディレクトリー・サーバーが前もって構成されていない場合には、 EIM 構成ウィザードを使用して新規ドメインを作成し結合する際に、ディレクトリー・サーバーを構成できます。
- EIM 構成ウィザードを使用して、 ウィザードが EIM ドメイン・コントローラーに接続するために使用する必要のあるユーザー ID のタイプを選択する場合。選択可能なユーザー・タイプの中から 1 つ選択することができます。識別名は、ディレクトリー・サーバーのローカル・ネームスペース内にオブジェクトを作成することを許可されているユーザーを表していなければなりません。
- EIM 構成ウィザードを使用して、オペレーティング・システム機能の代わりに EIM 操作を実行するユーザーのタイプを選択する場合。これらの操作には、マッピング・ルックアップ操作や、ローカル i5/OS ユーザー・プロファイルを削除する場合のアソシエーションの削除が含まれます。選択可能なユーザー・タイプの中から 1 つ選択することができます。

- EIM 管理を行うためにドメイン・コントローラーに接続する場合。たとえば、レジストリーや ID の管理、およびマッピング・ルックアップ操作の実行など。
- 証明書フィルターを作成して、証明書フィルター・ポリシー・アソシエーションの有効範囲を決定する場合。証明書フィルターを作成する時には、対象 DN または発行者 DN のいずれかの識別名情報、またはポリシー・アソシエーションによって影響を受ける証明書を判別するためにフィルターが使用する基準を指定する証明書を提供しなければなりません。

関連情報

ディレクトリー・サーバーの概念

親識別名

ここでは、識別名 (DN) 階層について学習します。

親識別名 (DN) は、 Lightweight Directory Access Protocol (LDAP) ディレクトリー・サーバーのネームスペース内の項目です。 LDAP サーバー項目は、政治上、地理上、組織上、またはドメイン境界を反映する階層構造内に割り当てられます。識別名は、指定された DN に対してすぐ上位のディレクトリー項目であるときに、その DN は親 DN と見なされます。

完全識別名の例は、`cn=Tim Jones`、`o=IBM`、`c=US` です。各項目は、項目を命名するために使用される属性が少なくとも一つあります。この命名属性は、項目の相対識別名 (RDN) と呼ばれます。 指定された RDN より上位の項目は、RDN の親識別名と呼ばれます。この例では、`cn=Tim Jones` という名前が項目に付けられるので、この名前がその項目の RDN になります。 `o=IBM`、`c=US` は、`cn=Tim Jones` の親 DN です。

EIM (エンタープライズ識別マッピング) はディレクトリー・サーバーを、EIM ドメイン・データを保管するためのドメイン・コントローラー として使用します。親 DN は EIM ドメイン・ネームと結合して、ディレクトリー・サーバー・ネームスペース内の EIM ドメイン・データの位置を指定します。 EIM 構成ウィザードを使用して新規ドメインを作成および結合するとき、作成しているドメインの親 DN を指定することを選択できます。 親 DN を使用することによって、 LDAP ネームスペースのどこにドメイン用の EIM データを置くかを指定できます。 親 DN を指定しないと、EIM データはネームスペース内の自身の接尾部に置かれます。 EIM ドメイン・データのデフォルトの位置は `ibm-eimDomainName=EIM` です。

関連情報

ディレクトリー・サーバーの概念

LDAP スキーマおよびその他の EIM 考慮事項

ここでは、ディレクトリー・サーバーが EIM (エンタープライズ識別マッピング) を使用して機能するのに何が必要かについて学習します。

EIM は、ドメイン・コントローラーが、 Lightweight Directory Access Protocol (LDAP) バージョン 3 をサポートするディレクトリー・サーバーによってホスティングされることを必要とします。さらに、ディレクトリー・サーバー・プロダクトは、EIM スキーマを受け入れ、次の属性およびオブジェクト・クラスを理解することができなければなりません。

- ibm-entryUUID 属性
- ibmattributetypes:
  - acIEntry
  - acIPropagate
  - acISource
  - entryOwner
  - ownerPropagate

  - ownerSource
- EIM 属性 (ポリシー・アソシエーション・サポートのための 3 つの新規属性を含む)
  - ibm-eimAdditionalInformation
  - ibm-eimAdminUserAssoc
  - ibm-eimDomainName, ibm-eimDomainVersion,
  - ibm-eimRegistryAliases
  - ibm-eimRegistryEntryName
  - ibm-eimRegistryName
  - ibm-eimRegistryType
  - ibm-eimSourceUserAssoc
  - ibm-eimTargetIdAssoc
  - ibm-eimTargetUserName
  - ibm-eimUserAssoc
  - ibm-eimFilterType
  - ibm-eimFilterValue
  - ibm-eimPolicyStatus
- EIM オブジェクト・クラス (ポリシー・アソシエーション・サポートのための 3 つの新規クラスを含む)
  - ibm-eimApplicationRegistry
  - ibm-eimDomain
  - ibm-eimIdentifier
  - ibm-eimRegistry
  - ibm-eimRegistryUser
  - ibm-eimSourceRelationship
  - ibm-eimSystemRegsitry
  - ibm-eimTargetRelationship
  - ibm-eimFilterPolicy
  - ibm-eimDefaultPolicy
  - ibm-eimPolicyListAux

IBM Directory Server for iSeries の V5R3 以降のバージョンは、このサポートを提供します。どの IBM Directory Server プロダクトが EIM で必要とされるサポートを提供するのかについての詳細、および EIM ドメイン・コントローラーのその他の考慮事項については、EIM ドメイン・コントローラーの計画を参照してください。

現在 EIM ドメイン・コントローラーとして、V5R2 iSeries システム上のディレクトリー・サーバーを使用している場合には、 LDAP スキーマおよびこのディレクトリー・サーバーの EIM サポートを更新して、V5R3 以降の EIM ドメイン・データを管理するために引き続き使用できるようにしなければなりません。

関連情報

iSeries LDAP

EIM (エンタープライズ識別マッピング) 用の iSeries の概念

ここでは、EIM (エンタープライズ識別マッピング) のすべてのアプリケーションをリストします。

EIM は、任意の IBM @server プラットフォームにインプリメントできます。ただし、EIM を iSeries サーバー上にインプリメントする場合には、 iSeries サーバー・インプリメンテーションに特有のいくつかの情報に注意する必要があります。以下の情報を検討して、EIM で使用可能な i5/OS アプリケーション、ユーザー・プロファイル考慮事項、およびその他の EIM を iSeries システム上で効果的に使用するのに役立つトピックについて学習してください。

関連概念

5 ページの『EIM (エンタープライズ識別マッピング) の概念』
ここでは、EIM を正常にインプリメントするために理解しておくべき重要な EIM の概念について学びます。

EIM 用の i5/OS ユーザー・プロファイル考慮事項

EIM (エンタープライズ識別マッピング) でタスクを実行できることは、i5/OS ユーザー・プロファイル権限にではなく、43 ページの『EIM アクセス制御』 権限に基づいています。ただし、i5/OS が EIM を使用するようにセットアップするためには、いくつかの追加タスクを実行する必要があります。これらの追加タスクは、ユーザーが i5/OS ユーザー・プロファイルを適切な特殊権限とともに持っていることを必要とします。

iSeries ナビゲーターを使用して i5/OS が EIM を使用するようにセットアップするには、ユーザーのユーザー・プロファイルに以下の特殊権限がなければなりません。

- セキュリティー管理者 (*SECADM)
- すべてのオブジェクト (*ALLOBJ)
- システム構成 (*IOSYSCFG)

EIM ID 用の i5/OS ユーザー・プロファイル・コマンドの機能強化

ご使用のシステム用に EIM を構成したならば、 「ユーザー・プロファイルの作成」(CRTUSRPRF) および「ユーザー・プロファイルの変更」(CHGUSRPRF) の 2 つのコマンドに対して、 新規パラメーター EIMASSOC を利用できます。 このパラメーターを使用して、ローカル・レジストリー用に指定されたユーザー・プロファイルに対して、EIM ID アソシエーションを定義できます。

このパラメーターを使用する際には、以下の情報を指定できます。

- EIM ID 名。これは新規名でも既存 ID 名でもかまいません。
- アソシエーションのアクション・オプション。これは、指定したアソシエーションを追加 (*ADD)、 置換 (*REPLACE)、または除去 (*REMOVE) することができます。

  注: *ADD を使用して、新規アソシエーションをセットアップします。 *REPLACE オプションは、たとえば、以前に間違った ID に対してアソシエーションを定義した場合に使用します。 *REPLACE オプションは、ローカル・レジストリーの、他の ID に対する指定されたタイプの既存アソシエーションを除去した後、そのパラメーターに指定されたものを追加します。 *REMOVE オプションを使用して、指定された ID から指定されたアソシエーションを除去します。
- ID アソシエーションのタイプ。これは、ターゲット・アソシエーション、ソース・アソシエーション、ターゲットおよびソース両方のアソシエーション、または管理アソシエーションを指定できます。
- 指定された EIM ID がまだ存在していない場合に、それを作成するかどうか。

一般に、特に単一シングル・サインオン環境で、i5/OS プロファイルに対してターゲット・アソシエーションを作成します。コマンドを使用して、ユーザー・プロファイル (また必要であれば EIM ID) に対して必要なターゲット・アソシエーションを作成した後、対応するソース・アソシエーションを作成する必要があるかもしれません。 iSeries ナビゲーターを使用して、ユーザーがネットワークにサインオンする際に使用する Kerberos プリンシパルなど、 別のユーザー ID のソース・アソシエーションを作成できます。

システム用に EIM を構成する際、オペレーティング・システムのために EIM 操作を実行する際に使用する、システム用のユーザー ID およびパスワードを指定しました。 このユーザー ID は、ID を作成しアソシエーションを追加するための十分な EIM アクセス制御権限を持っていなければなりません。

i5/OS ユーザー・プロファイル・パスワードおよび EIM

管理者として、シングル・サインオン環境の一部として EIM を構成する主な目的は、企業内の一般的なエンド・ユーザーのために実行しなければならないユーザー・パスワード管理の量を減らすことです。 EIM の提供する ID マッピングを Kerberos 認証と組み合わせて使用することによって、エンド・ユーザーが実行しなければならないログオンの数と、覚えて管理しておかなければならないパスワードの数が減ることになります。エンド・ユーザーがパスワードを忘れてしまったときにパスワードをリセットするために呼び出しを受けるなど、マップされたユーザー ID に関する問題を処理するための呼び出しを受ける回数も減るので、これは管理者にとっても益となります。ただし、セキュリティー・ポリシー・パスワードの規則はやはり有効なので、パスワード期限切れがいつであろうと、ユーザーごとのこれらのユーザー・プロファイルを管理する必要は依然として存在します。

ご使用のシングル・サインオン環境からさらに益を受けるには、 ID マッピングのターゲットであるユーザー・プロファイルのパスワード設定を変更することを考慮することができます。 ID マッピングのターゲットとして、ユーザーは iSeries システムまたは EIM 対応 i5/OS リソースにアクセスする際に、ユーザー・プロファイル用のパスワードを供給する必要がなくなりました。一般ユーザーの場合には、パスワード設定を *NONE に変更して、ユーザー・プロファイルではパスワードを使用しないようにすることができます。 ID マッピングおよびシングル・サインオンのおかげで、ユーザー・プロファイルの所有者はパスワードが不要になりました。パスワードを *NONE に設定することにより、管理者もエンド・ユーザーも、パスワード有効期限を管理する必要がなくなるので、管理者はさらに益を得ます。さらに、プロファイルを使用して直接 iSeries にサインオンしたり、EIM 対応 i5/OS リソースにアクセスしたりすることが誰にもできなくなります。ただし、管理者が直接 iSeries システムにサインオンする必要がある場合には、引き続き管理者がユーザー・プロファイルのパスワード値を持つほうがよいかもしれません。たとえば、ご使用の EIM ドメイン・コントローラーがダウンし、ID マッピングが行えない場合には、ドメイン・コントローラーの問題が解決するまで、管理者は iSeries システムに直接サインオンする必要があるかもしれません。

EIM 用の i5/OS 監査

どの監査を実行するかは、全体のセキュリティー計画で重要な考慮事項です。 EIM (エンタープライズ識別マッピング) を構成および使用する際、ディレクトリー・サーバー用に監査サポートを構成して、ユーザーのセキュリティー・ポリシーが必要とする適切なレベルの責任能力を提供できるようにすることができます。たとえば、監査サポートは、 ポリシー・アソシエーションによってマップされるどのユーザーが、システム上でアクションを実行したか、またはオブジェクトを変更したかを判別する際に役立ちます。

IBM Directory Server for iSeries (LDAP) 用の監査サポートについての詳細は、IBM Directory Server for iSeries (LDAP) Information Center のトピックにある、監査 (Auditing) を参照してください。この情報はまた、ディレクトリー・サーバー監査を正しく構成できるようにするために必要な、 i5/OS 監査考慮事項および設定についての該当する資料も記載しています。

i5/OS 用の EIM 対応アプリケーション

以下の i5/OS アプリケーションは、EIM (エンタープライズ識別マッピング) を使用するように構成できます。

- i5/OS ホスト・サーバー (現在 iSeries Access for Windows および iSeries ナビゲーターによって使用されている)
- Telnet Server (現在 PC5250 および IBM Websphere host on demand によって使用されている)
- QFileSrv.400 ODBC (SQL を介したシングル・サインオンの使用を許可する)
- JDBC (SQL を介した EIM の使用を許可する)
- 分散リレーショナル・データベース体系™ (DRDA®) (SQL を介した EIM の使用を許可する)
- IBM WebSphere Host On-Demand バージョン 8 (Web 高速ログオン機能)
- NetServer™
- QFileSvr.400

EIM (エンタープライズ識別マッピング) のシナリオ

ここでは、シングル・サインオン環境内において、異なるシステム間でユーザー ID を管理する方法を学習します。

EIM (エンタープライズ識別マッピング) は、企業全体のユーザー ID を追跡して管理できる、 IBM インフラストラクチャー・テクノロジーです。一般に、EIM はネットワーク認証サービスなどの認証テクノロジーとともに使用して、シングル・サインオン環境をインプリメントします。

したがって、EIM のこのより広い使用法に関心がある場合には、「シングル・サインオン」という Information Center トピックの シナリオ (Scenarios) を検討する必要があります。

EIM (エンタープライズ識別マッピング) の計画

ここでは、EIM (エンタープライズ識別マッピング) インプリメンテーション計画を作成する方法について学習し、iSeries または混合プラットフォーム環境用の EIM を確実に構成できるようにします。

企業内で EIM (エンタープライズ識別マッピング) を正常に構成して使用するためには、インプリメンテーション計画が不可欠です。計画を作成するために、EIM を使用するシステム、アプリケーション、ユーザーに関するデータを収集する必要があります。収集した情報を使用して、その企業の EIM を構成する最良の方法について判断します。

EIM は、すべての IBM プラットフォームに対して使用可能な IBM @server インフラストラクチャー・テクノロジーであるので、インプリメンテーションをどのように計画するかは、企業内のプラットフォームに依存しています。それぞれのプラットフォームに特有の多数の計画アクティビティーがありますが、多くの EIM 計画アクティビティーは、すべての IBM プラットフォームに適用されます。 共通の EIM 計画アクティビティーを作業して、全体的なインプリメンテーション計画を作成する必要があります。
EIM インプリメンテーションの計画方法について詳しくは、以下のページを参照してください。

eServer™ 用の EIM (エンタープライズ識別マッピング) の計画

プラットフォームが混合している企業で、EIM (エンタープライズ識別マッピング) を正常に構成して使用するためには、インプリメンテーション計画が不可欠です。インプリメンテーション計画を作成するため

に、 EIM を使用するシステム、アプリケーション、ユーザーに関するデータを収集する必要があります。収集した情報を使用して、プラットフォームが混合している環境で EIM を構成する最良の方法について判断します。

以下のリストは、プラットフォームが混合している環境で EIM を構成および使用する前に完了すべき、計画タスクのロードマップを提供します。これらのページにある情報を読み通して、インプリメンテーション・チームが必要とするスキル、収集する必要のある情報、および行う必要のある構成上の決定など、EIM 構成要件をどのように計画するかを学習してください。 EIM 計画ワークシート (下記のリストの 8) を印刷すれば、計画プロセスを進めてゆくにつれてそれらを完成させることができます。

eServer 用の EIM (エンタープライズ識別マッピング) セットアップ要件

企業内で EIM (エンタープライズ識別マッピング) を正常にインプリメントするために、適合していることを確認しなければならない 3 セットの要件があります。

1. エンタープライズ・レベルまたはネットワーク・レベルの要件
2. システム要件
3. アプリケーション要件

エンタープライズ・レベルまたはネットワーク・レベルの要件

企業またはネットワーク内の 1 つのシステムを、 EIM ドメイン・コントローラーとして作動するように構成しなければなりません。これは、EIM ドメイン・データを保管し供給する、特別に構成された Lightweight Directory Access Protocol (LDAP) サーバーです。どのディレクトリー・サービス・プロダクトをドメイン・コントローラーとして使用するよう選択するかについては、多数の考慮事項があります。その 1 つは、必ずしもすべての LDAP サーバー・プロダクトが EIM ドメイン・コントローラー・サポートを提供するわけではないという事実です。

別の考慮事項は、管理ツールの可用性です。 1 つのオプションとして、ユーザーの所有アプリケーションで EIM API を使用して、管理機能を実行することができます。 Directory Server for iSeries (LDAP) プロダクトを EIM ドメイン・コントローラーとして使用する場合は、 iSeries Navigator を使用して EIM を管理できます。 IBM Directory プロダクトを使用する場合には、 V1R4 LDAP SPE の一部である eimadmin ユーティリティーを使用できます。

以下の情報は、 どの IBM プラットフォームが、 EIM をサポートするディレクトリー・サーバー・プロダクトを提供するかについての基本的な情報を提供します。 EIM ドメイン・コントローラー・サポートを提供するディレクトリー・サーバーの選択についての詳細は、 EIM ドメイン・コントローラーの計画に記載しています。

システムおよびアプリケーションの要件

EIM ドメインに参加するそれぞれのシステムは、次の要件に合っていなければなりません。

- LDAP クライアント・ソフトウェアがインストール済み。
- EIM API のインプリメンテーションがある。

EIM ドメインに参加するそれぞれのアプリケーションは、 EIM API を使用してマッピング・ルックアップその他の操作を実行できなければなりません。

注: 分散アプリケーションの場合に、サーバー・サイドおよびクライアント・サイドの両方が EIM API を使用できることは、必ずしも必要ではありません。一般に、アプリケーションのサーバー・サイドだけが、EIM API を使用する必要があります。

次のテーブルは、@server プラットフォームが提供する EIM サポートに関する情報を提供します。情報はプラットフォームごとに編成されており、次のことを示す列があります。

- EIM API をサポートするためにプラットフォームで必要とされる EIM クライアント
- そのプラットフォームで使用可能な EIM 構成および管理ツールのタイプ
- そのプラットフォームにインストールできる、 EIM ドメイン・コントローラーとして作動するディレクトリー・サーバー・プロダクト

プラットフォームは、EIM ドメインに参加するために、 EIM ドメイン・コントローラーとして作動することができなければならないとは限りません。

表 9. eServer EIM サポート

プラットフォーム	EIM クライアント (API サポート)	ドメイン・コントローラー	EIM 管理ツール
pSeries® 上の AIX	AIX R5.2	IBM Directory V5.1	使用不可
Linux • PPC64 上の SLES8 • i386 上の Red Hat 7.3 • zSeries® 上の SLES7	次のうちの 1 つをダウンロード • IBM Directory V4.1 クライアント • IBM Directory V5.1 クライアント • Open LDAP v2.0.23 クライアント	IBM Directory V5.1	使用不可
iSeries 上の i5/OS	OS/400 V5R2 および i5/OS V5R3 以降	OS/400 V5R2 および i5/OS V5R3 以降の Directory Server	iSeries Navigator V5R2 および V5R3 以降
xSeries® 上の Windows 2000	次のうちの 1 つをダウンロード • IBM Directory V4.1 クライアント • IBM Directory V5.1 クライアント	IBM Directory V5.1 クライアント	使用不可
zSeries 上の z/OS	z/OS V1R4 LDAP SPE OW57137	z/OS V1R4 LDAP	V1R4 LDAP SPE OW57137

注: IBM Directory Server プロダクトについて詳しくは、 IBM Web プロダクト Web サイト (http://www-3.ibm.com/software/network/help-directory/) を参照してください。

プラットフォームが EIM クライアント (API) サポートを提供する限り、そのシステムは EIM ドメインに参加できます。プラットフォームを企業の EIM ドメイン・コントローラーとして使用するのでない限り、プラットフォームが EIM ドメイン・コントローラー・サポートを必ずしも提供しなくてもかまいません。

すべての EIM 要件が適合していることを確認した後、 EIM を構成するために、必要なスキル、 役割、および権限の識別を開始できます。

必要なスキル、役割、および権限の識別

EIM (エンタープライズ識別マッピング) は、小さな組織で一人の人が構成および管理の責任を簡単に果たすことができるように設計されています。または、大きな組織では、多数の異なる人が、これらの責任を持つようにするほうがよいかもしれません。チームに必要な人数は、各チーム・メンバーが所有する必要なスキルの種類、 EIM インプリメンテーションに関係するプラットフォームのタイプ、および組織がそのセキュリティー役割および責任をどのように分割するか、によって異なります。

正常な EIM インプリメンテーションでは、いくつかのソフトウェア・プロダクトの構成および相互作用が必要とされます。これらのプロダクトのそれぞれは、特定のスキルおよび役割を必要とするので、特に大きな組織で作業する場合には、いくつか異なる分野の人材から成る EIM インプリメンテーション・チームを作成することを選択できます。

以下の情報は、EIM を正常にインプリメントするために必要なスキルおよび 43 ページの『EIM アクセス制御』権限を説明しています。これらのスキルは、そのスキルにおける専門家の役職の用語で示されています。たとえば、Lightweight Directory Access Protocol (LDAP) スキルを必要とするタスクは、ディレクトリー・サーバー管理者のタスクと呼ばれます。

チーム・メンバーおよびそれらの役割

以下の情報は、EIM の管理に必要な役割の責任および必要な権限を説明しています。この役割リストを使用して、前提条件プロダクトをインストールおよび構成し、 EIM および 1 つ以上の EIM ドメインを構成するために必要なチーム・メンバーを判別できます。

まず定義する必要のある役割のセットの 1 つは、EIM ドメインの管理者の数とタイプです。 EIM 管理の仕事と権限を与えられたすべての人は、 EIM インプリメンテーション・チームのメンバーとして、EIM 計画プロセスに関係する必要があります。

注: EIM 管理者は、組織において重要な役割を果たし、システム上のユーザー ID を作成することのできる人と同じ権限を持ちます。 EIM 管理者は、ユーザー ID の EIM アソシエーションを作成する際に、コンピューター・システムにアクセスすることのできる人、およびそうするときの特権を指定します。この権限は、ユーザーの会社のセキュリティー・ポリシーに基づき、高いレベルで信頼を置ける人に与えるようお勧めします。

以下の表は、EIM の構成および管理に必要とされる、可能性のあるチーム・メンバー役割、タスク、およびスキルをリストしています。それぞれの役割が実行できる EIM 管理用タスクの詳細については、 43 ページの『EIM アクセス制御』を参照してください。

注: 組織内の一人の人が、すべての EIM 構成および管理タスクの責任を持つ場合には、その人に EIM 管理者の役割および権限が与えられる必要があります。

表 10. EIM の構成のための役割、タスク、およびスキル

役割	許可されるタスク	必要なスキル
EIM 管理者	• ドメイン操作の調整 • ユーザー ID のレジストリー定義、EIM ID、およびアソシエーションの追加、除去、および変更 • EIM ドメイン内のデータに対するコントローラー権限	EIM 管理ツールの知識

表 10. EIM の構成のための役割、タスク、およびスキル (続き)

役割	許可されるタスク	必要なスキル
EIM ID 管理者	• EIM ID の作成および変更 • 管理アソシエーションおよびソース・アソシエーションの追加および除去 (ターゲット・アソシエーションの追加や除去はできない)	EIM 管理ツールの知識
EIM レジストリー管理者	すべての EIM レジストリー定義の管理 : • ターゲット・アソシエーションの追加および除去 (ソース・アソシエーションおよび管理アソシエーションの追加や除去はできない) • EIM レジストリー定義の更新	次のものに関する知識 : • EIM ドメインに定義されたすべてのユーザー・レジストリー (ユーザー ID に関する情報など) • EIM 管理ツール
EIM レジストリー X 管理者	特定の EIM レジストリー定義の管理 • 特定のユーザー・レジストリー (たとえば、レジストリー X) のターゲット・アソシエーションの追加および除去 • 特定の EIM レジストリー定義の更新	次のものに関する知識 : • EIM ドメインに定義された特定のユーザー・レジストリー (ユーザー ID に関する情報など) • EIM 管理ツール
ディレクトリー・サーバー (LDAP) 管理者	• ディレクトリー・サーバーのインストールおよび構成 (必要な場合) • EIM 用のディレクトリー・サーバー構成のカスタマイズ • EIM ドメインの作成 (注を参照) • EIM ドメイン・コントローラーにアクセスする許可を与えられるユーザーの定義 • オプション : 最初の EIM 管理者の定義 **注:** ディレクトリー・サーバー管理者は、 EIM 管理者が行えることすべてを行えます。	次のものに関する知識 : • ディレクトリー・サーバー・インストール、構成、およびカスタマイズ • EIM 管理ツール
ユーザー・レジストリー管理者	• 特定のユーザー・レジストリー用のユーザー・プロファイルまたはユーザー ID の設定 • オプション : 指定されたユーザー・レジストリーに対して EIM レジストリー管理者としてサービス提供	次のものに関する知識 : • ユーザー・レジストリーの管理ツール • EIM 管理ツール
システム・プログラマーまたはシステム管理者	必要なソフトウェア・プロダクトのインストール (EIM のインストールも含むかもしれない)	次のものに関する知識 : • システム・プログラミングまたは管理のスキル • プラットフォームのインストール手順

表 10. EIM の構成のための役割、タスク、およびスキル (続き)

役割	許可されるタスク	必要なスキル
アプリケーション・プログラマー	EIM API を使用するアプリケーションの作成	次のものに関する知識 : • プラットフォーム • プログラミング・スキル • プログラムのコンパイル

企業内の EIM の構成および管理を行うために使用する役割を識別したならば、EIM ドメインの計画を行うことができます。

EIM (エンタープライズ識別マッピング) ドメインの計画

初期 EIM (エンタープライズ識別マッピング) インプリメンテーション計画プロセスの一部で、 EIM ドメインの定義が必要とされます。マッピング情報の中央制御リポジトリーを持つことから最大の利点を引き出すためには、多数のアプリケーションおよびシステムで共用されるドメインを計画する必要があります。

EIM 計画トピックの作業を進めながら、ドメインを定義するために必要な情報を収集し、それを計画ワークシートに記録します。ワークシートのセクション例は、このトピックのそれぞれの計画段階で、必要な情報を収集して記録するのを援助します。

以下の表は、ドメインを計画する際に収集する必要のある情報をリストし、必要なそれぞれの情報項目ごとに、責任のある EIM インプリメンテーション・チームの役割 (複数も可) を提案します。

注: 表では、記述された情報を収集する責任を割り当てるための特定の役割を、提案としてリストしますが、ユーザーの組織の必要とセキュリティー・ポリシーに基づいて、役割を割り当てる必要があります。たとえば、小さい組織では、EIM の計画、構成、および管理のすべての局面に責任を持つ EIM 管理者として、一人の人を指定するほうがよいかもしれません。

表 11. EIM ドメイン計画に必要な情報

必要な情報	役割
1. 使用できる要件に適した既存のドメインがあるか、または新規にそれを作成するか。	EIM 管理者
2. どのディレクトリー・サーバーが EIM ドメイン・コントローラーとして機能するか。 (ドメイン・コントローラーの選択についての詳細は、 EIM ドメイン・コントローラーの計画を参照してください。)	ディレクトリー・サーバー (LDAP) 管理者または EIM 管理者
3. ドメインの名前。 (オプションの記述を提供することもできます。)	EIM 管理者
4. ディレクトリーのどこに EIM ドメイン・データを保管するか。 **注:** ディレクトリー・サーバーをホスティングするシステムをどれにするか、また EIM ドメイン・データを保管するディレクトリーをどれにするかによっては、ドメインを作成する前に、いくつかのディレクトリー・サービス構成タスクを実行する必要があるかもしれません。	ディレクトリー・サーバー (LDAP) 管理者または EIM 管理者の両方

表 11. EIM ドメイン計画に必要な情報 (続き)

必要な情報	役割
5. ドメインに参加するアプリケーションおよびオペレーティング・システム。最初のドメインを構成している場合には、この初期設定は、1 つのシステムだけから成っているかもしれません。 (詳しくは、EIM レジストリー定義命名計画の作成を参照してください。)	EIM チーム
6. ドメインに参加する人およびエンティティー。 **注:** 初期テストを簡単にするには、参加者の数を 1 人か 2 人に限定できます。	EIM チーム

これで、EIM ドメインを定義するために必要な情報について理解できたので、 EIM ドメイン・データを保管するために、EIM ドメイン・コントローラーの計画を始めることができます。

EIM (エンタープライズ識別マッピング) ドメイン・コントローラーの計画

EIM (エンタープライズ識別マッピング) ドメインを定義するために情報を収集する際、どのディレクトリー・サーバー・プロダクトが EIM ドメイン・コントローラーとして機能するかを判別する必要があります。 EIM は、ドメイン・コントローラーが、Lightweight Directory Access Protocol (LDAP) バージョン 3 をサポートするディレクトリー・サーバーによってホスティングされることを必要とします。さらに、ディレクトリー・サーバー・プロダクトは、 LDAP スキーマおよびその他の EIM 考慮事項を受け入れて、特定の属性およびオブジェクト・クラスを理解できなければなりません。

企業が EIM ドメイン・コントローラーをホスティングできる複数のディレクトリー・サーバーを所有する場合には、 2 次複製ドメイン・コントローラーを使用するかどうかを考慮する必要もあります。たとえば、大量の EIM マッピング・ルックアップ操作が生じることが予想される場合には、レプリカがあれば、ルックアップ操作のパフォーマンスを向上できます。

また、大量のマッピング・ルックアップ操作を実行することが予想されるシステムとの関係において、ドメイン・コントローラーを*ローカル* または*リモート* のどちらにするかを考慮する必要があります。ドメイン・コントローラーを大ボリュームのシステムに対してローカルにすれば、ローカル・システムのルックアップ操作のパフォーマンスが向上します。計画ワークシートを使用して、これらの計画上の判断を、ドメインおよび他のディレクトリー情報に関して行った判断とともに記録します。

企業内のどのディレクトリー・サーバーが EIM ドメイン・コントローラーをホスティングするかを判別した後、ドメイン・コントローラー・アクセスに関するいくつかの決定を行う必要があります。

ドメイン・コントローラー・アクセスの計画

ユーザーおよび EIM 対応アプリケーションおよびオペレーティング・システムが、 EIM ドメイン・コントローラーをホスティングするディレクトリー・サーバーにアクセスする方法を計画する必要があります。EIM ドメインにアクセスするには、以下の条件があります。

1. EIM ドメイン・コントローラーにバインドできなければなりません。
2. バインド対象は、EIM アクセス制御グループのメンバーであるか、または LDAP 管理者であることを確認してください。詳しくは、 EIM アクセス制御の管理を参照してください。

EIM バインディングのタイプを選択する

EIM API は、EIM ドメイン・コントローラーとの接続を確立する (バインディングとも言われる) ための、いくつもの異なるメカニズムをサポートします。それぞれのタイプのバインディング・メカニズムは、接続のための異なるレベルの認証および暗号化を提供します。可能な選択として、次のものがあります。

- **単純バインド** 単純バインドは、認証のためのバインド識別名およびバインド・パスワードを、LDAP クライアントが LDAP サーバーに提供する LDAP 接続です。 バインド識別名およびパスワードは、LDAP 管理者によって LDAP ディレクトリーに定義されます。これは、認証の最も弱い形式で、最低レベルのセキュアです。なぜなら、バインド識別名およびパスワードは暗号化されずに送信されるので、盗聴に対してぜい弱であるからです。 CRAM-MD5 (ユーザー確認のための質問への応答認証メカニズム) を使用して、追加レベルの保護をバインド・パスワードに追加します。 CRAM-MD5 プロトコルでは、クライアントは認証のために、平文パスワードの代わりに、ハッシュされた値をサーバーに送信します。
- **Secure Sockets Layer (SSL) によるサーバー認証 - サーバー・サイドの認証** LDAP サーバーは SSL または Transport Layer Security (TLS) 接続用に構成できます。 LDAP サーバーはディジタル証明書を使用して、それ自体を LDAP クライアントに認証し、それらの間で暗号化された通信セッションを確立します。 LDAP サーバーだけが、証明書によって認証されます。エンド・ユーザーは、バインド識別名およびパスワードによって認証されます。認証の強度は、単純バインドと同じですが、すべてのデータ (バインド識別名およびパスワードを含む) がプライバシーのために暗号化されます。
- **SSL によるクライアント認証** LDAP サーバーは、 LDAP サーバーとの SSL または TLS セキュア接続用のバインド識別名およびパスワードではなく、ディジタル証明書によって、エンド・ユーザーが認証されることを要求するように構成できます。クライアントおよびサーバーの両者は認証されて、セッションが暗号化されます。このオプションは、より強いレベルのユーザー認証を提供し、伝送されるすべてのデータのプライバシーを保護します。
- **Kerberos 認証** LDAP クライアントは、バインド識別名およびパスワードのオプションの置換として、Kerberos チケットを使用して、サーバーに対して認証されることができます。 (Kerberos)、これはトラステッド・サード・パーティー・ネットワーク認証システムで、プリンシパル (ユーザーまたはサービス) が、非セキュア・ネットワーク内の別のサービスに対してその ID を証明できる手段です。プリンシパルの認証は、鍵配布センター (KDC) と呼ばれる、中央制御されたサーバーによって完了されます。KDC は Kerberos チケットを持つユーザーを認証します。これらのチケットは、プリンシパルの ID を、ネットワーク内の他のサービスに証明します。プリンシパルがこれらのチケットによって認証された後、プリンシパルおよびサービスは暗号化されたデータを、ターゲット・サービスと交換できます。このオプションは、より強いレベルのユーザー認証を提供し、認証情報のプライバシーを保護します。

バインド・メカニズムの選択は、EIM 対応アプリケーション、 および EIM ドメインをホスティングする LDAP サーバーによってサポートされる認証メカニズムが必要とする、セキュリティーのレベルを基にして行われます。

また、LDAP サーバーが、ユーザーが選択した認証メカニズムを使用できるようにするために、追加の構成タスクを実行する必要があるかもしれません。ご使用のドメイン・コントローラーをホスティングする LDAP サーバーの資料を調べて、実行する必要のある他の構成タスクを判別してください。

計画ワークシート例 : ドメイン・コントローラー情報

EIM ドメイン・コントローラーに関する決定を行った後、計画ワークシートを使用して、ご使用の EIM 対応オペレーティング・システムおよびアプリケーションが必要とする、 EIM ドメイン・コントローラー情報を記録してください。このプロセスの一部として収集した情報は、LDAP 管理者により使用され、EIM ドメイン・コントローラーをホスティングする LDAP ディレクトリー・サーバーに対する、アプリケーションまたはオペレーティング・システムのバインド ID を定義できます。

以下の計画ワークシートの部分例は、収集する必要のある情報のタイプを示しています。また、EIM ドメイン・コントローラーを構成する際に使用できるサンプル値も組み込まれています。

表 12. EIM 計画ワークシート用のドメインおよびドメイン・コントローラー情報

EIM ドメインおよびドメイン・コントローラーを構成するために必要とされる情報	**回答例**
ドメインの分かりやすい名前。これは、ドメインを使用する会社、部門、またはアプリケーションの名前でもかまいません。	MyDomain
オプション：EIM ドメインを既存の LDAP ディレクトリー内に構成する場合には、ドメインの親識別名を指定します。これは、ディレクトリー情報ツリー階層において、ご使用のドメイン名項目のすぐ上の項目を表す識別名です (例、 o=ibm,c=us)。	o=ibm,c=us
生成される、完全に修飾された EIM ドメイン識別名。これは、EIM ドメイン・データのディレクトリー位置を記述する、 EIM ドメインの完全に定義された名前です。完全に修飾されたドメイン識別名は、少なくとも、ドメインの DN (ibm-eimDomainName=)、および指定したドメイン名から成っています。ドメインの親 DN を指定することを選択した場合は、完全に修飾されたドメイン DN は、相対ドメイン DN (ibm-eimDomainName=)、ドメイン名 (MyDomain)、 および親 DN (o=ibm,c=us) から成ります。 **注:**	以下のいずれか (親 DN を選択するかどうかによって異なる) • ibm-eimDomainName=MyDomain • ibm-eimDomainName=MyDomain,o=ibm,c=us
ドメイン・コントローラーの接続アドレス。これは、接続タイプ (基本 ldap またはセキュア ldap。たとえば、ldap:// または ldaps://) および次の情報から成っています。	ldap://
• オプション：ホスト名または IP アドレス • オプション：ポート番号	• some.ldap.host • 389
生成される、ドメイン・コントローラーの完全な接続アドレス。	ldap://some.ldap.host:389
アプリケーションまたはシステムが必要とする BIND メカニズム。 以下のものから選択できます。 • 単純バインド • CRAM MD5 • サーバー認証 • クライアント認証 • Kerberos	Kerberos

EIM 構成および管理チームが、複数のチーム・メンバーから成っている場合には、各チーム・メンバーがそれぞれの役割に基づいて EIM ドメインにアクセスするために使用すべき、バインド ID およびメカニズムを判別する必要があります。また、EIM アプリケーションのエンド・ユーザーのための、バインド ID およびメカニズムを判別する必要もあります。以下のワークシートは、この情報を収集するための例として役立つことでしょう。

表 13. バインド ID 計画ワークシート例

EIM 権限または役割	BIND ID	BIND メカニズム	必要な理由
EIM 管理者	eimadmin@krbrealm1.com	kerberos	EIM の構成および管理
LDAP 管理者	cn=administrator	単純バインド	EIM ドメイン・コントローラーの構成
EIM レジストリー X 管理者	cn=admin2	CRAM MD5	特定のレジストリー定義の管理
EIM マッピング・ルックアップ	cn=MyApp,c=US	単純バインド	アプリケーション・マッピング・ルックアップ操作の実行

ドメイン・コントローラーの構成に必要な情報を収集した後、 ID マッピング計画の作成を行うことができます。

EIM (エンタープライズ識別マッピング) レジストリー定義命名計画の作成

EIM (エンタープライズ識別マッピング) を使用して 1 つのユーザー・レジストリー内のユーザー ID を、別のユーザー・レジストリー内の相当ユーザー ID にマップする場合、両方のユーザー・レジストリーが EIM に定義されていなければなりません。 EIM レジストリー定義を、 EIM ドメインに参加するそれぞれのアプリケーションまたはオペレーティング・システムごとに作成する必要があります。ユーザー・レジストリーは、Resource Access Control Facility (RACF) または i5/OS などのオペレーティング・システム・レジストリー、 Kerberos などの分散レジストリー、またはアプリケーションによって排他的に使用されるシステム・レジストリーのサブセットを表すことができます。

EIM ドメインには、任意のプラットフォーム上に存在するユーザー・レジストリーのレジストリー定義を含めることができます。たとえば、i5/OS 上のドメイン・コントローラーによって管理されるドメインには、 i5/OS 以外のプラットフォーム用のレジストリー定義を含めることがあります (AIX レジストリーなど)。任意のユーザー・レジストリーを EIM ドメインに定義できますが、 EIM 対応のアプリケーションおよびオペレーティング・システムのユーザー・レジストリーを定義しなければなりません。

EIM レジストリー定義には、それが EIM ドメイン内で固有である限り、任意の名前を付けることができます。たとえば、ユーザー・レジストリーをホスティングするシステムの名前に基づいて、 EIM レジストリー定義を命名できます。これが類似した定義からそのレジストリー定義を区別するのに不十分な場合には、ピリオド (.) または下線 (_) を使用して、定義しているユーザー・レジストリーのタイプを追加できます。使用することを選択した基準にかかわりなく、 EIM レジストリー定義の命名規則を作成することを考慮すべきです。そうするならば、確実に定義名がドメイン全体で整合し、定義されるユーザー・レジストリーのタイプおよびインスタンス、およびその使用法を適切に記述することになります。たとえば、そのレジストリーを使用するアプリケーションまたはオペレーティング・システム名、および企業内でのそのユーザー・レジストリーの物理的な位置を組み合わせて、それぞれのレジストリー定義の名前を選択できます。

EIM を使用するように作成されるアプリケーションは、ソース・レジストリー別名またはターゲット・レジストリー別名のいずれか、またはその両方の別名を指定できます。 EIM レジストリー定義を作成する際には、ご使用のアプリケーションの資料を調べて、レジストリー定義に 1 つ以上の別名を指定する必要があるかどうかを判別する必要があります。ユーザーがこれらの別名を適切なレジストリー定義に割り当てると、アプリケーションは別名ルックアップを実行して、アプリケーション内の別名に一致する EIM レジストリー定義を検出できます。

以下の計画ワークシートの部分例は、ユーザー・レジストリーの参加についての情報を記録する指針として役立つことでしょう。実際のワークシートを使用して、それぞれのユーザー・レジストリーごとにレジスト

リー定義名を指定し、それが別名を使用するかどうかを指定し、ユーザー・レジストリーの位置と使用法を記述できます。アプリケーションのインストールおよび構成の資料は、ワークシートに必要な情報のいくらかを提供します。

表 14. EIM レジストリー定義情報計画ワークシート例

レジストリー定義名	ユーザー・レジストリー・タイプ	レジストリー定義別名	レジストリー記述
System_C	i5/OS システム・ユーザー・レジストリー	アプリケーションの資料を参照	システム C 上の i5/OS のメイン・システム・ユーザー・レジストリー
System_A_WAS	WebSphere LTPA	app_23_alias_source	システム A 上の WebSphere LTPA ユーザー・レジストリー
System_B	Linux	アプリケーションの資料を参照	システム B 上の Linux ユーザー・レジストリー
System_A	i5/OS システム・ユーザー・レジストリー	app_23_alias_target app_xx_alias_target	システム A 上の i5/OS のメイン・システム・ユーザー・レジストリー
System_D	Kerberos ユーザー・レジストリー	app_xx_alias_source	legal.mydomain.com Kerberos レルム
System_4	Windows 2000 ユーザー・レジストリー	アプリケーションの資料を参照	システム 4 上の人事課アプリケーション・ユーザー・レジストリー

注: それぞれのレジストリーごとのアソシエーション・タイプについては、計画プロセスの後ほどで判別します。

計画ワークシートのこのセクションを完成した後、 ID マッピング計画の作成を行って、それぞれの定義されたユーザー・レジストリー内のユーザー ID に必要なマッピングを作成するために、 ID アソシエーション、ポリシー・アソシエーションのいずれを使用するのか、それともその両方のタイプのアソシエーションを使用するのかを判別する必要があります。

ID マッピング 計画の作成

初期 EIM (エンタープライズ識別マッピング) インプリメンテーション計画プロセスの重要な部分として、企業内で ID マッピングをどのように使用するかを判別する必要があります。 EIM 内の ID をマップするために使用できる、次の 2 つの方法があります。

- **ID アソシエーション**は、 EIM ID とその人物を表すユーザー・レジストリー内のユーザー ID との間の関係を記述します。 ID アソシエーションは、EIM ID および指定されたユーザー ID との間の、直接的な 1 対 1 のマッピングを作成します。 ID アソシエーションを使用して、EIM ID を介したユーザー ID 間の関係を間接的に定義できます。

  ご使用のセキュリティー・ポリシーが詳細にわたりレベルが高い場合、 ID マッピング・インプリメンテーションに対して ID アソシエーションをほとんど排他的に使用する必要があるかもしれません。 ID アソシエーションを使用して、ユーザーが所有するユーザー ID の 1 対 1 マッピングを作成するので、オブジェクトまたはシステムに対してアクションを実行した人を、常に正確に判別できます。
- **ポリシー・アソシエーション**は、複数のユーザー ID とユーザー・レジストリー内の単一ユーザー ID との間の関係を記述します。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。

ポリシー・アソシエーションが役立つのは、 1 つ以上の大きなユーザー・グループが、企業内のシステムまたはアプリケーションにアクセスする必要があり、それらのユーザーにはこのアクセスを得るための特定のユーザー ID を持たせたくない場合です。たとえば、特定の内部アプリケーションにアクセスする Web アプリケーションを保守しているとします。この内部アプリケーションに対して認証すべきユーザー ID を数え切れないほどセットアップするようなことは、したくないことでしょう。 この状況では、この Web アプリケーションのすべてのユーザーが、アプリケーションを実行するために必要とされる最低レベルの権限を持つ単一ユーザー ID にマップされるように、 ID マッピングを構成できます。このタイプの ID マッピングは、ポリシー・アソシエーションを使用して作成できます。

企業内のユーザー ID の最良の制御を提供しつつ、最も簡素化されたパスワード管理を行うためには、 ID アソシエーションを使用するよう決定できます。または、適切な箇所ではシングル・サインオンを整備しつつ、管理者用のユーザー ID に対する特定の制御を保守するために、ポリシー・アソシエーションと ID アソシエーションを混合して使用することを決定できるかもしれません。ユーザーのビジネス要件やユーザーのセキュリティー・ポリシーに適合する ID マッピングのタイプにかかわらず、 ID マッピング計画を作成して、ID マッピングを適切にインプリメントする必要があります。

ID マッピング計画を作成するには、次のことを行う必要があります。

関連概念

114 ページの『アソシエーションの作成』

EIM (エンタープライズ識別マッピング) アソシエーションの計画: アソシエーションは、異なるユーザー・レジストリー内のユーザー ID 間の関係を定義するために、 EIM (エンタープライズ識別マッピング) ドメイン上に作成する項目です。 EIM に 2 つのタイプのアソシエーションのうちの 1 つを作成できます。 すなわち、1 対 1 のマッピングを定義する ID アソシエーション、および多対 1 のマッピングを定義するポリシー・アソシエーションです。ポリシー・アソシエーションは、ID アソシエーションの代わりに、またはそれと組み合わせて使用できます。

どちらのタイプのアソシエーションを作成するかは、特定のユーザー ID の使用法、 および全体の ID マッピング計画に依存しています。

以下のタイプの ID アソシエーションの任意のものを作成できます。

- **ターゲット・アソシエーション**

  通常は、他のクライアント・システムからサーバーとしてこのシステムにアクセスするだけのユーザー用の、ターゲット・アソシエーションを定義します。このタイプのアソシエーションを使用するのは、アプリケーションがマッピング・ルックアップ操作を実行する場合です。
- **ソース・アソシエーション**

  ソース・アソシエーションを定義するのは、システムまたはネットワークにサインオンするためにユーザーが提供する最初のものが、ユーザー ID である場合です。このタイプのアソシエーションを使用するのは、アプリケーションがマッピング・ルックアップ操作を実行する場合です。
- **管理アソシエーション**

  管理アソシエーションを定義するのは、ユーザー ID が特定のユーザーに属している事実を追跡できるようにはしたいが、マッピング・ルックアップ操作にそのユーザー ID を使用できるようにはしたくない場合です。このタイプのアソシエーションを使用して、企業内の個人が使用するすべてのユーザー ID を追跡できます。

ポリシー・アソシエーションは常に、ターゲット・アソシエーションを定義します。

単一のレジストリー定義が、それが参照するユーザー・レジストリーの使用法に基づいて、複数のタイプのアソシエーションを持つことができます。定義できるアソシエーションの数や組み合わせには制限はありませんが、 EIM ドメインの管理を単純化するために、その数を最小にしてください。

一般にアプリケーションは、それがソース・レジストリーおよびターゲット・レジストリーに対して予期するレジストリー定義に関する指針を提供しますが、アソシエーション・タイプに関しては指針は提供しません。アプリケーションの各エンド・ユーザーは、最低 1 つのアソシエーションによってアプリケーションにマップされる必要があります。このアソシエーションは、 それらの固有の EIM ID と要求されたターゲット・レジストリー内のユーザー ID との間の、1 対 1 のマッピングであっても、ユーザー ID がそのメンバーとなっているソース・レジストリーと要求されたターゲット・レジストリーとの間の、多対 1 のマッピングであってもかまいません。どのタイプのアソシエーションを使用するかは、 ID マッピング要件およびアプリケーションが提供する基準によって異なります。

計画プロセスの一部としてすでに、組織内のユーザー ID に関する 2 つのワークシートを、 必要な EIM ID および EIM レジストリー定義に関する情報で完成させています。ここでは、企業内のユーザー ID をマップするために使用するアソシエーションのタイプを指定することによって、この情報をまとめる必要があります。特定のアプリケーションおよびそのユーザーのレジストリーに対してポリシー・アソシエーションを定義するか、それともシステムまたはアプリケーション・レジストリー内のそれぞれのユーザー ID ごとに、 特定の ID アソシエーション (ソース、ターゲット、または管理) を定義するかを判別する必要があります。このことは、レジストリー定義計画ワークシート、およびそれぞれのアソシエーション・ワークシートの対応する行の両方に、必要なアソシエーション・タイプに関する情報を記録することによって行えます。

ID マッピング計画を完成させるには、以下のワークシート例を、 ID マッピングのインプリメント計画の全体図を記述するために必要な、アソシエーション情報を記録するのに役立つ指針として使用できます。

表 15. EIM レジストリー定義情報計画ワークシート例

レジストリー定義名	ユーザー・レジストリー・タイプ	レジストリー定義別名	レジストリー記述	アソシエーション・タイプ
System_C	i5/OS システム・ユーザー・レジストリー	アプリケーションの資料を参照	システム C 上の i5/OS のメイン・システム・ユーザー・レジストリー	ターゲット
System_A_WAS	WebSphere LTPA	app_23_alias_source	システム A 上の WebSphere LTPA ユーザー・レジストリー	主なソース
System_B	Linux	アプリケーションの資料を参照	システム B 上の Linux ユーザー・レジストリー	ソースおよびターゲット
System_A	i5/OS システム・ユーザー・レジストリー	app_23_alias_target app_xx_alias_target	システム A 上の i5/OS のメイン・システム・ユーザー・レジストリー	ターゲット
System_D	Kerberos ユーザー・レジストリー	app_xx_alias_source	legal.mydomain.com Kerberos レルム	ソース
System_4	Windows 2000 ユーザー・レジストリー	アプリケーションの資料を参照	システム 4 上の人事課アプリケーション・ユーザー・レジストリー	管理

表 15. EIM レジストリー定義情報計画ワークシート例 (続き)

レジストリー定義名	ユーザー・レジストリー・タイプ	レジストリー定義別名	レジストリー記述	アソシエーション・タイプ
order.mydomain.com	Windows 2000 ユーザー・レジストリー		受注部門従業員のメイン・ログオン・レジストリー	デフォルトのレジストリー・ポリシー (ソース・レジストリー)
System_A_order_app	受注部門アプリケーション		注文更新のためのアプリケーション特定のレジストリー	デフォルトのレジストリー・ポリシー (ターゲット・レジストリー)
System_C_order_app	受注部門アプリケーション		注文更新のためのアプリケーション特定のレジストリー	デフォルトのレジストリー・ポリシー (ターゲット・レジストリー)

表 16. EIM ID 計画ワークシートの例

固有 ID 名	ID またはユーザー ID 記述	ID 別名
John S Day	人事部門管理者	app_23_admin
John J Day	法律部門	app_xx_admin
Sharon A. Jones	受注部門管理者	

表 17. ID アソシエーション計画ワークシートの例

ID 固有の名前 : _____John S Day_____		
ユーザー・レジストリー	**ユーザー ID**	**アソシエーション・タイプ**
システム A 上のシステム A WAS	johnday	ソース
システム B 上の Linux	jsd1	ソースおよびターゲット
システム C 上の i5/OS	JOHND	ターゲット
Windows 2000 人的資源システム上のレジストリー 4	JDAY	管理

表 18. ポリシー・アソシエーション用の計画ワークシート例

ポリシー・アソシエーション・タイプ	ソース・ユーザー・レジストリー	ターゲット・ユーザー・レジストリー	ユーザー ID	記述
デフォルトのレジストリー	order.mydomain.com	System_A_order_app	SYSUSERA	認証された Windows 受注部門ユーザーから、適切なアプリケーション・ユーザー ID へマップする
デフォルトのレジストリー	order.mydomain.com	System_C_order_app	SYSUSERB	認証された Windows 受注部門ユーザーから、適切なアプリケーション・ユーザー ID へマップする

EIM ID 命名計画の作成: EIM (エンタープライズ識別マッピング) ID マッピングの計画が必要なとき、1 人のユーザーのユーザー ID 間の 1 対 1 マッピングを作成する場合には、 企業内の EIM 対応のアプリ

ケーションおよびオペレーティング・システムのユーザーに対して、固有の EIM ID を作成できます。ID アソシエーションを使用して 1 対 1 マッピングを作成することにより、 EIM が提供するパスワード管理の利点を最大限に活用できます。

作成する命名計画は、ビジネス要件および設定によって異なります。 EIM ID に関するただ一つの要件は、それらが固有であることです。ある会社は、各人の正式なフルネームを使用することを望むかもしれず、他の会社は、別のタイプのデータ (各人の従業員番号など) を使用することを望むかもしれません。各人のフルネームに基づいて EIM ID を作成する場合には、名前の重複が予期されるかもしれません。重複した名前をどのように処理するかは、個人で設定できます。それぞれの ID 名に事前に決めた文字ストリングを追加して固有な名前にすることによって、それぞれのケースを手動で処理できます。たとえば、それぞれの人の部門番号を追加できます。

EIM ID 命名計画の作成の一部として、 全体の ID マッピング計画を決定する必要があります。そうすれば、企業内の ID のマッピングに、ID および ID アソシエーションを使用するのか、それともポリシー・アソシエーションを使用するのかを判断するのに役立ちます。 EIM ID 命名計画を作成するために、組織内のユーザー ID に関する情報を収集し、 ユーザー ID の EIM ID を計画するのに役立つ、下記のワークシートを使用できます。ワークシートは、EIM 管理者が、アプリケーションのユーザーに対して EIM ID またはポリシー・アソシエーションを作成する際に知る必要のある種類の情報を表しています。

表 19. EIM ID 計画ワークシートの例

固有 ID 名	ID またはユーザー ID 記述	ID 別名
John S Day	人事部門管理者	app_23_admin
John J Day	法律部門	app_xx_admin
Sharon A. Jones	受注部門管理者	

EIM を使用するよう作成されるアプリケーションは、アプリケーションのための適切な EIM ID を検出するために使用する別名を指定できます。アプリケーションはこれを使用して、使用すべき特定のユーザー ID を判別できます。ご使用のアプリケーションの資料を調べて、 ID に 1 つ以上の別名を指定する必要があるかどうかを判別する必要があります。 EIM ID またはユーザー ID 記述フィールドはフリー・フォームで、そのユーザーに関する説明情報を提供できます。

一度に企業内のすべてのメンバーの EIM ID を作成する必要はありません。 初期 EIM ID を作成し、それを使用して EIM 構成をテスト後、ユーザーの組織で EIM を使用する目的に基づいて、追加の EIM ID を作成できます。たとえば、部門やエリアを基にして EIM ID を追加できます。 または、追加の EIM アプリケーションを配置する際に、EIM ID を追加できます。

EIM ID 命名計画を作成するために必要な情報を収集した後、ユーザー ID に対するアソシエーションの計画を実行できます。

EIM (エンタープライズ識別マッピング) インプリメンテーション計画ワークシート

EIM (エンタープライズ識別マッピング) 計画プロセスを作業するにつれて、 企業内で EIM を構成および使用するために必要な情報を収集するために、このワークシートを使用するのが役立つことにお気付きのことでしょう。ワークシートの完成したセクションの例が、計画ページの適切な箇所で提供されています。

これらのワークシートは、 EIM インプリメンテーション計画を作成するために必要なタイプのワークシートの例として提供されています。提供されている項目の数は、ユーザーの EIM 情報に必要な数よりおそらく少ないことでしょう。これらのワークシートを編集して、ユーザーの状況により役立つようにすることができます。

表 20. ドメインおよびドメイン・コントローラー情報ワークシート

EIM ドメインおよびドメイン・コントローラーを構成するために必要とされる情報	**回答**
ドメインの分かりやすい名前。これは、ドメインを使用する会社、部門、またはアプリケーションの名前でもかまいません。	
オプション : ドメインの親識別名。これは、ディレクトリー情報ツリー階層において、ご使用のドメイン名項目のすぐ上の項目を表す識別名です (例、 `o=ibm,c=us`)。	
生成される、完全に修飾された EIM ドメイン識別名。これは、EIM ドメイン・データのディレクトリー位置を記述する、 EIM ドメインの完全に定義された名前です。完全に修飾されたドメイン識別名は、少なくとも、ドメインの DN (`ibm-eimDomainName=`)、および指定したドメイン名から成っています。ドメインの親 DN を指定することを選択した場合は、完全に修飾されたドメイン DN は、 相対ドメイン DN (`ibm-eimDomainName=`)、ドメイン名 (MyDomain)、 および親 DN (`o=ibm,c=us`) から成ります。	
ドメイン・コントローラーの接続アドレス。これは、接続タイプ (基本 ldap またはセキュア ldap。たとえば、`ldap://` または `ldaps://`) および次の情報から成っています。	
• オプション : ホスト名または IP アドレス • オプション : ポート番号	
生成される、ドメイン・コントローラーの完全な接続アドレス。	
アプリケーションまたはシステムが必要とする BIND メカニズム。 以下のものから選択できます。 • 単純バインド • CRAM MD5 • サーバー認証 • クライアント認証 • Kerberos	

このワークシートの使用例は、『EIM ドメイン・コントローラーの計画』を参照してください。

表 21. BIND ID 計画ワークシート

EIM 権限または役割	**BIND ID**	**BIND メカニズム**	**必要な理由**

表 21. BIND ID 計画ワークシート (続き)

このワークシートの使用例は、『EIM ドメイン・コントローラーの計画』を参照してください。

表 22. EIM レジストリー定義情報計画ワークシート

レジストリー定義名	ユーザー・レジストリー・タイプ	レジストリー定義別名	レジストリー記述	アソシエーション・タイプ

このワークシートの使用例は、『EIM レジストリー定義命名計画の作成』を参照してください。

表 23. EIM ID 計画ワークシート

固有 ID 名	ID またはユーザー ID 記述	ID 別名

このワークシートの使用例は、『EIM ID 命名計画の作成』を参照してください。

表 24. ID アソシエーション計画ワークシート

ID 固有の名前 : _____John S Day_____		
ユーザー・レジストリー	ユーザー ID	アソシエーション・タイプ

このワークシートの使用例は、『EIM アソシエーションの計画』を参照してください。

表 25. ポリシー・アソシエーション計画ワークシート

ポリシー・アソシエーション・タイプ	ソース・ユーザー・レジストリー	ターゲット・ユーザー・レジストリー	ユーザー ID	記述

このワークシートの使用例は、『EIM アソシエーションの計画』を参照してください。

EIM (エンタープライズ識別マッピング) アプリケーション開発の計画

EIM (エンタープライズ識別マッピング) を使用してドメインに参加するアプリケーションの場合、そのアプリケーションは EIM API を使用できなければなりません。 EIM API 資料およびプラットフォーム固有の EIM 資料を調べて、 EIM API を使用するアプリケーションを作成または適用する際に理解しておくべき、特殊な計画考慮事項があるかどうかを判別する必要があります。たとえば、EIM API の呼び出しを行う C または C++ アプリケーションには、コンパイルその他の考慮事項があるかもしれません。アプリケーションのプラットフォームによっては、リンク・エディットその他の考慮事項もあるかもしれません。

i5/OS 用の EIM (エンタープライズ識別マッピング) の計画

iSeries サーバー上で EIM (エンタープライズ識別マッピング) が包含している複数のテクノロジーおよびサービスがあります。ご使用のサーバー上で EIM を構成する前に、EIM およびシングル・サインオン機能を使用して、インプリメントしたい機能を決定する必要があります。

EIM をインプリメントする前に、ご使用のネットワークの基本的なセキュリティー要件を決定し、そのセキュリティー手段をインプリメントしている必要があります。 EIM は、エンタープライズ全体で、管理者にとってもユーザーにとっても簡単な ID 管理手段を提供します。ネットワーク認証サービスとともに使用する場合、EIM はエンタープライズにシングル・サインオン機能を提供します。

シングル・サインオン・インプリメンテーションの一部として、 Kerberos を使用してユーザー認証を行いたい場合、ネットワーク認証サービスも構成する必要があります。ネットワーク認証サービスの計画については、 ネットワーク認証サービスを計画するを、シングル・サインオン環境の計画については、 シングル・サインオンの計画 (Plan single signon) を参照してください。

iSeries EIM 構成の計画方法については、以下の情報を参照してください。

iSeries の EIM インストール前提条件

以下の計画ワークシートは、EIM の構成に先立ってインストールする必要のあるサービスを識別します。

表 26. EIM インストール計画ワークシート

EIM 前提条件計画ワークシート	回答
ご使用のオペレーティング・システムは V5R4 (5722-SS1) ですか ?	
以下のオプションおよびライセンス交付を受けたプロダクトが iSeries™ にインストールされていますか ? • i5/OS Host Servers (5722-SS1 オプション 12) • iSeries Access for Windows® (5722-XE1) • Qshell Interpreter (5722-SS1 オプション 30) EIM だけでなくネットワーク認証サービスも構成する場合は必要	
以下のサブコンポーネントも含めて、iSeries ナビゲーターが管理者 PC 上にインストールされていますか ? • セキュリティー EIM だけでなくネットワーク認証サービスも構成する場合は必要 • ネットワーク	
最新の iSeries Access for Windows Service Pack をインストールしていますか ? 最新の Service Pack については、iSeries Access  を参照してください。	
ディレクトリー・サーバー (たとえば IBM Directory Server for iSeries (LDAP)) が現在構成されており、それを EIM ドメイン・コントローラーとして使用したい場合、LDAP 管理者識別名 (DN) およびパスワードが分かっていますか ?	
ディレクトリー・サーバーが現在構成されている場合、それを一時的に停止できますか? (EIM 構成プロセスを完了するために、これが必要です。)	
*SECADM、*ALLOBJ、および *IOSYSCFG 特殊権限を持っていますか?	
最新のプログラム一時修正 (PTF) を適用しましたか?	

必要な iSeries ナビゲーター・オプションのインストール

EIM (エンタープライズ識別マッピング) およびネットワーク認証サービスを使用してシングル・サインオン環境を使用可能にするには、iSeries ナビゲーターの**ネットワーク**・オプションと**セキュリティー**・オプションの両方をインストールしなければなりません。EIM は**ネットワーク**・オプション内に、ネットワーク認証サービスは**セキュリティー**・オプション内にそれぞれ配置されます。ご使用のネットワーク内でネットワーク認証サービスを使用することを計画していない場合には、 iSeries ナビゲーターの**セキュリティー**・オプションをインストールする必要はありません。

iSeries ナビゲーターのネットワーク・オプションをインストールするか、またはこのオプションが現在インストールされているかを検査するには、まず iSeries Access for Windows が、iSeries サーバーを管理するために使用している PC 上にインストールされているかを確認してください。

ネットワーク・オプションをインストールするには、次のようにしてください。

1. 「**スタート**」>「**プログラム**」>「**IBM iSeries Access for Windows**」>「**選択セットアップ**」をクリックする。

2. ダイアログの指示に従う。「**コンポーネント選択**」ダイアログで、「**iSeries ナビゲーター**」を展開し、「**ネットワーク**」オプションを選択する。 ネットワーク認証サービスを使用することを計画している場合には、「**セキュリティー**」オプションも選択する必要がある。
3. 「**選択セットアップ**」の残りを続行する。

EIM のためのバックアップおよびリカバリー考慮事項

EIM ドメイン・コントローラーをホスティングするディレクトリー・サーバーで万一問題が生じた場合に、 EIM データが保護されリカバリーできるようにするために、 EIM (エンタープライズ識別マッピング) データのためのバックアップおよびリカバリー計画を作成する必要があります。リカバリーの方法を理解するために必要な、重要な EIM 構成情報もあります。

EIM ドメイン・データのバックアップおよびリカバリー:

EIM データの保管方法は、 EIM データ用のドメイン・コントローラーとして機能するディレクトリー・サーバーのこの局面を管理する方法によって異なります。

データをバックアップする 1 つの方法は (特に災害時回復において)、データベース・ライブラリーを保管することです。デフォルトで、これは QUSRDIRDB です。 changelog が使用可能な場合には、ライブラリー QUSRDIRCL を保管することも必要です。ライブラリーを復元するシステム上のディレクトリー・サーバーは、元のディレクトリー・サーバーと同じ LDAP スキーマおよび構成を持っていなければなりません。この情報を保管するファイルは、/QIBM/UserData/OS400/DirSrv です。追加の構成データは、QUSRSYS/QGLDCFG (*USRSPC オブジェクト) および QUSRSYS/QGLDVLDL (*VLDL オブジェクト) に保管されています。ご使用のディレクトリー・サーバーのすべての完全なバックアップを作成するためには、両方のライブラリー、統合ファイル・システム・ファイル、および QUSRSYS オブジェクトを保管しなければなりません。

IBM Directory Server for iSeries (LDAP) Information Center トピックの ディレクトリー・サーバー情報の保管および復元 (Save and restore Directory Server information) を参照すれば、重要なディレクトリー・サーバー・データの保管および復元方法についての詳細を確認できます。

たとえば、ディレクトリー・サーバーの内容の全部または一部を保管するために、LDIF ファイルを使用できます。 IBM Directory Server for iSeries ドメイン・コントローラーのドメイン情報をバックアップする場合は、次のステップを実行します。

1. iSeries ナビゲーターで、「**ネットワーク**」>「**サーバー (Servers)**」>「**TCP/IP**」を展開する。
2. 「**IBM Directory Server**」を右マウス・ボタン・クリックし、「**ツール (Tools)**」を選択し、「**ファイルのエクスポート**」を選択して、表示されたページで、ディレクトリー・サーバー内容のどの部分をファイルにエクスポートするかを指定する。
3. バックアップ・ディレクトリー・サーバーとして使用する iSeries サーバーに、エクスポート・ファイルを転送する。
4. バックアップ・サーバー上の iSeries ナビゲーターで、「**ネットワーク**」>「**サーバー (Servers)**」>「**TCP/IP**」を展開する。
5. 「**IBM Directory Server**」を右マウス・ボタン・クリックし、「**ツール (Tools)**」、「**インポート**」を選択し、転送ファイルの内容を新規ディレクトリー・サーバーにロードする。

EIM ドメイン・データの保管方法として考慮できる別の方法は、レプリカ・ディレクトリー・サーバーを構成および使用することです。 EIM ドメイン・データに対するすべての変更は自動的にレプリカ・ディレ

クトリー・サーバーに転送されるので、ドメイン・コントローラーをホスティングするディレクトリー・サーバーに障害が起きるか、または EIM データを消失した場合には、そのレプリカ・サーバーからデータを取り戻すことができます。

レプリカ・ディレクトリー・サーバーの構成および使用の方法は、使用するよう選択する複製モデルのタイプによって異なります。複製および複製用ディレクトリー・サーバーの構成について詳しくは、IBM Directory Server for iSeries (LDAP) Information Center トピックの、複製 (Replication) および複製の管理 (Manage replication) を参照してください。

EIM 構成情報のバックアップおよびリカバリー:

ご使用のシステムがダウンした場合、そのシステムに関する EIM 構成情報を復元する必要があります。この情報を複数のシステムで保管および復元するのは、簡単にはできません。

EIM 構成を保管および復元するために、以下のオプションを使用できます。

- それぞれのシステム上で、「セキュリティー・データの保管」(SAVSECDTA) コマンドを使用して、EIM および他の重要な構成情報を保管する。その後、それぞれのシステム上で QSYS ユーザー・プロファイルを復元する。

  注: EIM 構成を持つそれぞれのシステム上で個別に、SAVSECDTA コマンドを使用し、 QSYS ユーザー・プロファイル・オブジェクトを復元しなければなりません。 QSYS ユーザー・プロファイルを、それを保管したのとは別のシステム上でリカバリーしようとすると、問題が発生する場合があります。
- EIM 構成ウィザードを再実行するか、または EIM 構成フォルダー・プロパティーを手動で更新する。この処理を簡単にするために、EIM インプリメンテーション計画ワークシートを保管するか、それぞれのシステムごとに EIM 構成情報の記録を作成する必要があります。

さらに、シングル・サインオン環境のインプリメントの一部として、ネットワーク認証サービスを構成した場合には、ネットワーク認証サービス・データのバックアップおよびリカバリーの方法を考慮し計画する必要があります。

EIM (エンタープライズ識別マッピング) の構成

ここでは、EIM (エンタープライズ識別マッピング) 構成ウィザードを使用して、 ご使用の iSeries サーバー用に EIM を構成する方法を学習します。

EIM 構成ウィザードを使用すれば、 ご使用の iSeries 用の EIM の基本構成をすばやく簡単に完了できます。ウィザードは 3 つの EIM システム構成オプションを提供します。特定のシステム上で EIM を構成するためにウィザードを使用する方法は、企業内で EIM を使用する全体的な計画、および EIM 構成要件によって異なります。たとえば、多くの管理者は EIM をネットワーク認証サービス (network authentication service) と合わせて使用し、基礎となるセキュリティー・ポリシーを変更する必要なく、複数のシステムおよびプラットフォームにまたがるシングル・サインオン (single signon) 環境を作成することを考えます。 したがって、EIM 構成ウィザードを使用すれば、EIM 構成の一部として、ネットワーク認証サービスを構成できます。ただし、ネットワーク認証サービスを構成して使用しなければ、 EIM を構成し使用できないということではありません。

1 つ以上のシステム用に EIM を構成するプロセスを開始する前に、 EIM インプリメンテーションの計画を行って、必要な情報を収集してください。たとえば、以下の事柄に関して決定を行う必要があります。

- どの iSeries サーバーを、 EIM ドメインの EIM ドメイン・コントローラーとして構成するか ? EIM 構成ウィザードを使用して、まずこのシステム上に新規ドメインを作成し、その後ウィザードを使用して、追加の iSeries サーバーすべてをこのドメインに結合するように構成します。
- EIM 用に構成するそれぞれのシステム上で、ネットワーク認証サービスを構成するか ? 構成する場合には、EIM 構成ウィザードを使用して、それぞれの iSeries サーバー上に、基本ネットワーク認証サービス構成を作成できます。ただし、ネットワーク認証サービス構成を完了するためには、他のタスクを実行しなければなりません。

EIM 構成ウィザードを使用してそれぞれの iSeries サーバー用に基本構成を作成した後もまだ、EIM 構成を完了する前に実行しなければならないいくつかの EIM 構成タスクがあります。ネットワーク認証サービスおよび EIM を使用して、架空の会社がシングル・サインオン環境を構成した方法を示す例については、シナリオ： シングル・サインオンの使用可能化 (Scenario: Enable single signon) を参照してください。

EIM を構成するには、以下の特殊権限のすべてを持っていなければなりません。

- セキュリティー管理者 (*SECADM)
- すべてのオブジェクト (*ALLOBJ)
- システム構成 (*IOSYSCFG)

EIM 構成ウィザードを使用する前に、 57 ページの『EIM (エンタープライズ識別マッピング) の計画』のすべてのステップを完了して、 EIM をどのように使用するのかをはっきりと決めておく必要があります。シングル・サインオン環境の作成の一部として EIM を構成している場合には、 シングル・サインオンの計画 (single signon planning) のすべてのステップも完了する必要があります。

EIM 構成ウィザードにアクセスするには、以下のステップを実行してください。

1. iSeries ナビゲーターを開始する。
2. EIM を構成したい iSeries サーバーにサインオンする。複数の iSeries サーバーの EIM を構成する場合は、 EIM のドメイン・コントローラーを構成したいサーバーから始めてください。
3. 「**ネットワーク**」 → 「**エンタープライズ識別マッピング**」を展開する。
4. 「**構成**」を右マウス・ボタン・クリックして、「**構成... (Configure...)**」を選択し、EIM 構成ウィザードを立ち上げる。
5. EIM 構成オプションを選択して、ウィザードが示す指示に従い、ウィザードを完了する。
6. 必要であれば、「**ヘルプ**」をクリックして、ウィザードを進める際にどの情報を指定すべきかを判断する。

計画が完了したならば、EIM 構成ウィザードを使用して、 3 つのうちの 1 つの EIM 基本構成を作成できます。ウィザードを使用して、既存のドメインを結合するか、または新しいドメインを作成して結合できます。 EIM 構成ウィザードを使用して新規ドメインを作成および結合する場合、ローカルまたはリモートのどちらのシステム上に EIM ドメイン・コントローラーを構成するかを選択できます。以下の情報は、ユーザーが必要とする EIM 基本構成のタイプに基づく、EIM 構成のための指示です。

新規ローカル・ドメインの作成と結合

ここでは、企業用の新しい EIM (エンタープライズ識別マッピング) ドメインを作成し、 ローカル・ディレクトリー・サーバーを、その新しいドメインの EIM ドメイン・コントローラーになるように構成する方法を説明します。

EIM 構成ウィザードを使用して新規ドメインを作成および結合するとき、 EIM 構成の作成の一部として、EIM ドメイン・コントローラーをローカル・システム上に構成することを選択できます。 EIM 構成

ウィザードは必要な場合に、ディレクトリー・サーバーの基本構成情報を提供することを求めます。また、現在 iSeries サーバーで Kerberos が構成されていない場合は、ネットワーク認証サービス構成ウィザードを立ち上げることを求めるプロンプトが出されます。

EIM 構成ウィザードを完了すると、以下のタスクを完了することができます。

- 新規 EIM ドメインの作成
- EIM ドメイン・コントローラーとして機能するようにローカル・ディレクトリー・サーバーを構成する
- システム用のネットワーク認証サービスの構成
- ローカル i5/OS レジストリーおよび Kerberos レジストリー用の EIM レジストリー定義の作成
- 新規 EIM ドメインに参加するようシステムを構成する

システムを新規 EIM ドメインを作成して結合するよう構成するには、以下の特殊権限のすべてを持っていなければなりません。

- セキュリティー管理者 (*SECADM)
- すべてのオブジェクト (*ALLOBJ)
- システム構成 (*IOSYSCFG)

新しいローカル・ドメインを作成して結合するために EIM 構成ウィザードを使用するには、以下のステップを行ってください。

1. iSeries ナビゲーターで、 EIM を構成するシステムを選択し、「**ネットワーク**」>「**エンタープライズ識別マッピング**」を展開する。
2. 「**構成**」を右マウス・ボタン・クリックして、「**構成... (Configure...)**」を選択し、EIM 構成ウィザードを開始する。

   注: EIM が以前にシステム上で構成済みの場合には、このオプションには「**再構成... (Reconfigure..)**」というラベルが付いています。
3. ウィザードの「**ウェルカム**」ページで、「**新規ドメインの作成と結合**」を選択して「**次へ**」をクリックする。
4. 「**EIM ドメイン・ロケーションの指定**」ページで、「**ローカル・ディレクトリー・サーバー上**」を選択し、「**次へ**」をクリックする。

   注: このオプションは、 EIM ドメイン・コントローラーとして機能するようにローカル・ディレクトリー・サーバーを構成します。このディレクトリー・サーバーはドメインのすべてのデータを保管するので、 EIM マッピング・ルックアップその他の操作をサポートするためには、アクティブのままでなければなりません。

   現在 iSeries サーバーでネットワーク認証サービスが構成されていない場合、またはシングル・サインオン環境を構成するために追加のネットワーク認証構成情報が必要な場合には、「**ネットワーク認証サービスの構成**」ページが表示されます。このページでは、ネットワーク認証サービス構成ウィザードを開始して、 ネットワーク認証サービスを構成することができます。または後ほど、iSeries ナビゲーターにより、このサービスに対して構成ウィザードを使用して、ネットワーク認証サービスを構成できます。ネットワーク認証サービスの構成が完了したら、EIM 構成ウィザードは次に進みます。
5. ネットワーク認証サービスを構成するには、以下のステップを完了する。
   a. 「**ネットワーク認証サービスの構成**」ページで、「**はい**」を選択して、ネットワーク認証サービス構成ウィザードを開始する。このウィザードで、いくつかの i5/OS インターフェースおよびサービスを、 Kerberos レルムに参加するように構成し、 また EIM およびネットワーク認証サービスの両方を使用するシングル・サインオン環境を構成できます。

b. 「**レルム情報の指定**」ページで、「**デフォルト・レルム**」フィールドに、デフォルトのレルムの名前を指定する。 Kerberos 認証に Microsoft Active Directory を使用する場合には、「**Kerberos 認証に Microsoft Active Directory を使用**」を選択して、「**次へ**」をクリックする。

c. 「**KDC 情報の指定**」ページで、「**KDC**」フィールドに、このレルムの Kerberos サーバーの完全修飾名を指定し、「**ポート**」フィールドには 88 を指定して、「**次へ**」をクリックする。

d. 「**パスワード・サーバー情報の指定**」ページで、パスワード・サーバーのセットアップについて、「**はい**」または「**いいえ**」を選択する。パスワード・サーバーにより、プリンシパルは Kerberos サーバー上のパスワードを変更できます。「**はい**」を選択した場合には、「**パスワード・サーバー**」フィールドにパスワード・サーバー名を入力します。「**ポート**」フィールドでは、デフォルト値 464 を受け入れて、「次へ」をクリックします。

e. 「**キー・タブ項目の選択**」ページで、「**i5/OS Kerberos 認証**」を選択し、「**次へ**」をクリックする。

   注: さらに、IBM Directory Server for iSeries (LDAP)、iSeries NetServer、および iSeries HTTP サーバーが Kerberos 認証を使用するようにする場合には、これらのサービス用のキー・タブ項目も作成できます。これらのサービスが Kerberos 認証を使用する前に、それらに対して追加の構成を実行する必要があるかもしれません。

f. 「**i5/OS キー・タブ項目の作成**」ページで、パスワードを入力して確認し、「**次へ**」をクリックする。これは、i5/OS プリンシパルを Kerberos サーバーに追加する際に使用するのと同じパスワードです。

g. 任意: 「**バッチ・ファイルの作成**」ページで、「**はい**」を選択し、以下の情報を指定して、「**次へ**」をクリックする。

   - 「**バッチ・ファイル**」フィールドで、ディレクトリー・パスを更新する。「**参照**」をクリックして適切なディレクトリー・パスを探し出すか、または「**バッチ・ファイル**」フィールドでパスを編集する。
   - 「**パスワードの組み込み (Include password)**」フィールドで、「**はい**」を選択する。これにより、i5/OS サービス・プリンシパルと関連したすべてのパスワードが、バッチ・ファイルに組み込まれます。パスワードが平文で表示され、バッチ・ファイルへの読み取りアクセスを持つすべての人が読めるようにすることは重要です。したがって、バッチ・ファイルを使用した後、すぐにそれを Kerberos サーバーおよび PC から削除することは重要です。パスワードを組み込まない場合には、バッチ・ファイルの実行時にパスワードを入力するようプロンプトが出されます。

     注: ウィザードによって生成されるサービス・プリンシパルを、 Microsoft Active Directory に手動で追加することもできます。これを行う方法については、i5/OS プリンシパルを Kerberos サーバーに追加する (Add i5/OS principals to the Kerberos server) で確認してください。

   - 「**要約**」ページで、ネットワーク認証サービス構成の詳細を見直し、「**完了**」をクリックして EIM 構成ウィザードに戻る。

6. ローカル・ディレクトリー・サーバーが現在構成されていない場合は、EIM 構成ウィザードが再開する際に、「**ディレクトリー・サーバーの構成**」ページが表示される。以下の情報を供給して、ローカル・ディレクトリー・サーバーを構成する。

   注: EIM 構成ウィザードを使用する前にローカル・ディレクトリーを構成する場合には、代わりに「**接続のユーザーを指定**」ページが表示されます。このページを使用して、LDAP 管理者の識別名およびパスワードを指定し、ウィザードが EIM ドメインおよびその中のオブジェクトを管理するための十分な権限を持つようにし、この手順の次のステップを続行してください。必要であれば、「**ヘルプ**」をクリックして、このページにどの情報を供給すべきかを判断してください。

a. 「**ポート**」フィールドで、デフォルトのポート番号 389 を受け入れるか、ディレクトリー・サーバーとの非セキュア EIM 通信に使用する別のポート番号を入力する。

b. 「**識別名**」フィールドに、ディレクトリー・サーバー用の LDAP 管理者を識別する LDAP 識別名 (DN) を指定する。 EIM 構成ウィザードは、この LDAP 管理者 DN を作成し、ディレクトリー・サーバーを、作成中の新規ドメインのドメイン・コントローラーとして構成するために使用します。

c. 「**パスワード**」フィールドに、LDAP 管理者のパスワードを指定する。

d. 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

e. 「**次へ**」をクリックする。

7. 「**ドメインの指定**」ページで、以下の情報を指定する。

a. 「**ドメイン**」フィールドに、作成したい EIM ドメインの名前を指定する。 EIM というデフォルトの名前を受け入れるか、意味のある任意の一連の文字を入力する。ただし、**= + < > , # ; ¥** および * などの特殊文字は使用できません。

b. 「**記述**」フィールドに、ドメインを説明するテキストを入力する。

c. 「**次へ**」をクリックする。

8. 「**ドメインの親 DN を指定**」ページで、「**はい**」を選択して、作成中のドメイン用の親 DN を指定するか、または「**いいえ**」を指定して、 EIM ドメイン・ネームから派生した接尾部を持つディレクトリー位置に EIM データを保管する。

注: ローカル・ディレクトリー・サーバー上にドメインを作成する場合は、親 DN はオプションです。 親 DN を指定することによって、 ローカル LDAP ネーム・スペースのどこにドメイン用の EIM データを置くかを指定できます。 親 DN を指定しないと、EIM データはネーム・スペース内の自身の接尾部に置かれます。「**はい**」を選択する場合は、 親 DN として使用するローカル LDAP 接尾部を選択するためのリスト・ボックスを使用するか、新しい親 DN を作成してそれに名前を付けるためのテキストを入力します。新しいドメイン用の親 DN を指定する必要はありません。 親 DN の使用について詳しくは、「**ヘルプ**」をクリックしてください。

9. 「**レジストリー情報**」ページで、レジストリー定義としてローカル・ユーザー・レジストリーを EIM ドメインに追加するかどうかを指定する。以下のユーザー・レジストリー・タイプのいずれかまたは両方を選択します。

注: レジストリー定義はこの時点で作成する必要はありません。後でレジストリー定義を作成することを選択する場合には、 システム・レジストリー定義の追加および EIM 構成プロパティーの更新を行う必要があります。

a. 「**ローカル i5/OS**」を選択して、ローカル・レジストリーのレジストリー定義を追加する。 提供されたフィールドで、レジストリー定義名のデフォルト値を受け入れるか、または別の値を指定する。 EIM レジストリー名は、そのレジストリーのレジストリー・タイプと特定のインスタンスを表す任意のストリングです。

b. 「**Kerberos**」を選択して、 Kerberos レジストリーのレジストリー定義を追加する。提供されたフィールドで、レジストリー定義名のデフォルト値を受け入れるか、または別の値を指定する。 デフォルトのレジストリー定義名は、レルム名と同じです。デフォルト名を受け入れて、レルム名と同じ Kerberos レジストリー名を使用することにより、レジストリーからの情報検索のパフォーマンスを向上させることができます。必要であれば、「**Kerberos ユーザー識別で大文字小文字を区別**」を選択してください。

c. 「**次へ**」をクリックする。

10. 「**EIM システム・ユーザーの指定**」ページで、オペレーティング・システム機能の代わりに EIM 操作を実行する場合にシステムが使用する「**ユーザー・タイプ**」を選択する。 これらの操作には、マッ

ピング・ルックアップ操作や、ローカル i5/OS ユーザー・プロファイルを削除する場合のアソシエーションの削除が含まれます。「**識別名およびパスワード**」、「**Kerberos キー・タブ・ファイルおよびプリンシパル**」、または「**Kerberos プリンシパルおよびパスワード**」のいずれかのユーザー・タイプを選択できます。どのユーザー・タイプを選択できるかは、現行のシステム構成によって異なります。たとえば、システムに対してネットワーク認証サービスが構成されていない場合には、 Kerberos ユーザー・タイプが選択できない場合があります。ページを完了するために必要となる他の情報は、以下のように、選択するユーザー・タイプによって異なります。

注: EIM ドメイン・コントローラーをホスティングしている、現在ディレクトリー・サーバー内で定義されているユーザーを指定しなければなりません。指定するユーザーは、少なくとも、マッピング・ルックアップを実行する権限と、ローカル・ユーザー・レジストリーのレジストリー管理を実行する特権を持っている必要があります。指定するユーザーがこれらの特権を持っていない場合は、シングル・サインオンの使用およびユーザー・プロファイルの削除に関連した特定のオペレーティング・システム機能は失敗することがあります。

このウィザードを実行する前に、ディレクトリー・サーバーを構成していない場合、選択できるユーザー・タイプは「**識別名およびパスワード**」、指定できる識別名は LDAP 管理者の DN に限定されます。

- 「**識別名およびパスワード**」を選択する場合は、以下の情報を指定する。
  - 「**識別名**」フィールドに、 EIM 操作を実行する時に使用するシステムのユーザーを識別する LDAP 識別名を指定する。
  - 「**パスワード**」フィールドに、識別名のパスワードを指定する。
  - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。
- 「**Kerberos プリンシパルおよびパスワード**」を選択する場合は、以下の情報を指定する。
  - 「**プリンシパル**」フィールドに、 EIM 操作の実行時に使用するシステムの Kerberos プリンシパル名を指定する。
  - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
  - 「**パスワード**」フィールドに、ユーザーのパスワードを入力する。
  - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。
- 「**Kerberos キー・タブ・ファイルおよびプリンシパル**」を選択する場合は、以下の情報を指定する。
  - 「**キー・タブ・ファイル**」フィールドに、 EIM 操作を実行する時に使用するシステムの Kerberos プリンシパルを含む完全修飾パスおよびキー・タブ・ファイル名を指定する。または、「**参照...**」をクリックして、 iSeries 統合ファイル・システム内のディレクトリーを参照し、キー・タブ・ファイルを選択する。
  - 「**プリンシパル**」フィールドに、 EIM 操作の実行時に使用するシステムの Kerberos プリンシパル名を指定する。
  - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
- 「**接続の検査**」をクリックして、ウィザードが指定されたユーザー情報を使用して、 EIM ドメイン・コントローラーへの接続を正常に確立できることを確認する。

- 「**次へ**」をクリックする。

11. 「**要約**」パネルで、指定した構成情報を見直す。すべての情報が正しければ、「**完了**」をクリックする。

ドメインの EIM 構成の完了

ウィザードが完了すると、新規ドメインが「**ドメイン管理**」フォルダーに追加され、このサーバーの基本 EIM 構成が作成されています。しかし、ドメインの EIM 構成を完了するには、以下の作業を実行する必要があります。

1. ドメインの結合を行うそれぞれの追加サーバー上で、EIM 構成ウィザードを使用する。
2. 必要であれば、EIM ドメインに参加させる、他の非 iSeries のサーバーとアプリケーション用の EIM レジストリー定義を、 EIM ドメインに追加する。 これらのレジストリー定義は、ドメインに参加しなければならない実際のユーザー・レジストリーを参照します。 EIM インプリメンテーション要件に応じて、 システム・レジストリー定義の追加またはアプリケーション・レジストリー定義の追加のいずれかを行えます。
3. インプリメンテーション要件を基に、以下を行うかどうかを判別する。
   - ドメイン内のそれぞれの固有ユーザーまたはエンティティーごとに行う EIM ID の作成、およびそれらに対する ID アソシエーションの作成
   - ユーザーのグループを単一ターゲット・ユーザー ID にマップする、 ポリシー・アソシエーションの作成
   - これらの組み合わせの作成
4. EIM マッピングのテスト機能を使用して、 EIM 構成の ID マッピングをテストする。
5. 定義した EIM ユーザーだけが LDAP 管理者の DN である場合には、 EIM ユーザーには、ディレクトリー・サーバー上のすべてのデータに対する高水準の権限があります。したがって、1 つ以上の DN を、EIM データに対するより適切で限定されたアクセス制御を持つ追加ユーザーとして作成することを考慮できるかもしれません。 ディレクトリー・サーバー用の DN の作成については、IBM Directory Server for iSeries (LDAP) のトピックの 識別名 (Distinguished names) で確認してください。追加の EIM ユーザーをいくつ定義するかは、ご使用のセキュリティー・ポリシーが、セキュリティー上の義務および責任の分離にどの程度重きを置いているかによって異なります。一般に、以下のタイプのうちの少なくとも 2 つの DN を作成します。
   - **EIM 管理者アクセス制御を持つユーザー。**

     この EIM 管理者 DN は、 EIM ドメインを管理する責任を持つ管理者に、適切なレベルの権限を提供します。 iSeries ナビゲーターによって EIM ドメインのすべての局面を管理する際に、 この EIM 管理者 DN を使用してドメイン・コントローラーに接続できます。
   - **以下のアクセス制御のすべてを持つ、少なくとも 1 つのユーザー。**
     - ID 管理者
     - レジストリー管理者
     - EIM マッピング操作

     このユーザーは、オペレーティング・システムのために EIM 操作を実行するシステム・ユーザーに必要な、適切なレベルのアクセス制御を提供します。

   注: LDAP 管理者 DN の代わりに、システム・ユーザーのこの新規 DN を使用するには、 iSeries サーバー用の EIM 構成プロパティーを変更しなければなりません。システム・ユーザー DN を変更する方法については、EIM 構成プロパティーの管理で確認してください。

さらに、EIM ドメイン・コントローラーへのセキュア接続の構成を行って、EIM データの送信を保護するために、 Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を使用できます。ディレクトリー・サーバーに対して SSL を使用可能にする場合には、iSeries サーバーが安全な SSL 接続を使用することを指定するために、 EIM 構成プロパティーを更新しなければなりません。また、iSeries ナビゲーターによってドメインを管理するため EIM が SSL 接続を使用することを指定するために、ドメインのプロパティーを更新する必要があります。

注: 基本ネットワーク認証サービス構成を作成した場合、特にシングル・サインオン環境をインプリメントしている場合には、追加のタスクを実行する必要があるかもしれません。これらの追加ステップについては、i5/OS用のシングル・サインオンを使用可能にする (Enable single signon for i5/OS) のシナリオによって示された、完全な構成ステップを検討してください。

新規リモート・ドメインの作成と結合

ここでは、企業用の新しい EIM (エンタープライズ識別マッピング) ドメインを作成し、 リモート・ディレクトリー・サーバーを、その新しいドメインの EIM ドメイン・コントローラーになるように構成する方法を説明します。

EIM 構成ウィザードを使用して新規ドメインを作成および結合するとき、EIM 構成の作成の一部として、リモート・システム上のディレクトリー・サーバーが EIM ドメイン・コントローラーとして機能するように構成することを選択できます。 EIM を構成できるように、リモート・ディレクトリー・サーバーへの接続のために適切な情報を指定しなければなりません。現在 iSeries サーバーで Kerberos が構成されていない場合は、ネットワーク認証サービス構成ウィザードを開始することを求めるプロンプトが出されます。

注: リモート・システム上のディレクトリー・サーバーは、 EIM サポートを提供しなければなりません。EIM は、ドメイン・コントローラーが、 Lightweight Directory Access Protocol (LDAP) バージョン 3 をサポートするディレクトリー・サーバーによってホスティングされることを必要とします。さらに、ディレクトリー・サーバー・プロダクトは、EIM スキーマを構成する必要があります。たとえば、IBM Directory Server V5.1 がこのサポートを提供します。 EIM ドメイン・コントローラー要件について詳細は、EIM ドメイン・コントローラーの計画を参照してください。

EIM 構成ウィザードを完了すると、以下のタスクを完了することができます。

- 新規 EIM ドメインの作成
- EIM ドメイン・コントローラーとして機能するようにリモート・ディレクトリー・サーバーを構成する
- システム用のネットワーク認証サービスの構成
- ローカル i5/OS レジストリーおよび Kerberos レジストリー用の EIM レジストリー定義の作成
- 新規 EIM ドメインに参加するようシステムを構成する

システムを新規 EIM ドメインを作成して結合するよう構成するには、以下の特殊権限のすべてを持っていなければなりません。

- セキュリティー管理者 (*SECADM)
- すべてのオブジェクト (*ALLOBJ)
- システム構成 (*IOSYSCFG)

EIM 構成ウィザードを使用して、リモート・システム上のドメインを作成して結合するには、以下のステップを完了してください。

1. リモート・システム上のディレクトリー・サーバーがアクティブであることを確認する。

2. iSeries ナビゲーターで、 EIM を構成するシステムを選択し、「**ネットワーク**」>「**エンタープライズ識別マッピング**」を展開する。
3. 「**構成**」を右マウス・ボタン・クリックして、「**構成... (Configure...)**」を選択し、EIM 構成ウィザードを開始する。

   注: EIM が以前にシステム上で構成済みの場合には、このオプションには「**再構成... (Reconfigure..)**」というラベルが付いています。
4. ウィザードの「**ウェルカム**」ページで、「**新規ドメインの作成と結合**」を選択して「**次へ**」をクリックする。
5. 「**EIM ドメイン・ロケーションの指定**」ページで、「**ローカル・ディレクトリー・サーバー上**」を選択し、「**次へ**」をクリックする。

   注: このオプションは、 EIM ドメイン・コントローラーとして機能するようにローカル・ディレクトリー・サーバーを構成します。このディレクトリー・サーバーはドメインのすべてのデータを保管するので、 EIM マッピング・ルックアップその他の操作をサポートするためには、アクティブのままでなければなりません。

   現在 iSeries サーバーでネットワーク認証サービスが構成されていない場合、またはシングル・サインオン環境を構成するために追加のネットワーク認証構成情報が必要な場合には、「**ネットワーク認証サービスの構成**」ページが表示されます。このページでは、ネットワーク認証サービス構成ウィザードを開始して、 ネットワーク認証サービスを構成することができます。または後ほど、iSeries ナビゲーターにより、このサービスに対して構成ウィザードを使用して、ネットワーク認証サービスを構成できます。ネットワーク認証サービスの構成が完了したら、EIM 構成ウィザードは次に進みます。
6. ネットワーク認証サービスを構成するには、以下のステップを完了する。
   a. 「**ネットワーク認証サービスの構成**」ページで、「**はい**」を選択して、ネットワーク認証サービス構成ウィザードを開始する。このウィザードで、いくつかの i5/OS インターフェースおよびサービスを、 Kerberos レルムに参加するように構成し、 また EIM およびネットワーク認証サービスの両方を使用するシングル・サインオン環境を構成できます。
   b. 「**レルム情報の指定**」ページで、「**デフォルト・レルム**」フィールドに、デフォルトのレルムの名前を指定する。 Kerberos 認証に Microsoft Active Directory を使用する場合には、「**Kerberos 認証に Microsoft Active Directory を使用**」を選択して、「**次へ**」をクリックする。
   c. 「**KDC 情報の指定**」ページで、「**KDC**」フィールドに、このレルムの Kerberos サーバーの完全修飾名を指定し、「**ポート**」フィールドには 88 を指定して、「**次へ**」をクリックする。
   d. 「**パスワード・サーバー情報の指定**」ページで、パスワード・サーバーのセットアップについて、「**はい**」または「**いいえ**」を選択する。パスワード・サーバーにより、プリンシパルは Kerberos サーバー上のパスワードを変更できます。「**はい**」を選択した場合には、「**パスワード・サーバー**」フィールドにパスワード・サーバー名を入力します。「**ポート**」フィールドでは、デフォルト値 464 を受け入れて、「次へ」をクリックします。
   e. 「**キー・タブ項目の選択**」ページで、「**i5/OS Kerberos 認証**」を選択し、「**次へ**」をクリックする。

      注: さらに、IBM Directory Server for iSeries (LDAP)、iSeries NetServer、および iSeries HTTP サーバーが Kerberos 認証を使用するようにする場合には、これらのサービス用のキー・タブ項目も作成できます。これらのサービスが Kerberos 認証を使用する前に、それらに対して追加の構成を実行する必要があるかもしれません。

f. 「**i5/OS キー・タブ項目の作成**」ページで、パスワードを入力して確認し、「**次へ**」をクリックする。これは、i5/OS プリンシパルを Kerberos サーバーに追加する際に使用するのと同じパスワードです。

g. 任意: 「**バッチ・ファイルの作成**」ページで、「**はい**」を選択し、以下の情報を指定して、「**次へ**」をクリックする。

- 「**バッチ・ファイル**」フィールドで、ディレクトリー・パスを更新する。「**参照**」をクリックして適切なディレクトリー・パスを探し出すか、または「**バッチ・ファイル**」フィールドでパスを編集する。
- 「**パスワードの組み込み (Include password)**」フィールドで、「**はい**」を選択する。これにより、i5/OS サービス・プリンシパルと関連したすべてのパスワードが、バッチ・ファイルに組み込まれます。パスワードが平文で表示され、バッチ・ファイルへの読み取りアクセスを持つすべての人が読めるようにすることは重要です。したがって、バッチ・ファイルを使用した後、すぐにそれを Kerberos サーバーおよび PC から削除することは重要です。パスワードを組み込まない場合には、バッチ・ファイルの実行時にパスワードを入力するようプロンプトが出されます。

  注: ウィザードによって生成されるサービス・プリンシパルを、 Microsoft Active Directory に手動で追加することもできます。これを行う方法については、i5/OS プリンシパルを Kerberos サーバーに追加する (Add i5/OS principals to the Kerberos server) で確認してください。
- 「**要約**」ページで、ネットワーク認証サービス構成の詳細を見直し、「**完了**」をクリックして EIM 構成ウィザードに戻る。

7. 「**EIM ドメイン・コントローラーの指定**」ページで、構成するリモート EIM ドメイン・コントローラーに関する、次のような接続情報を指定する。

a. 「**ドメイン・コントローラー名**」フィールドに、作成しているドメインの EIM ドメイン・コントローラーとして構成するリモート・ディレクトリー・サーバーの名前を指定する。 EIM ドメイン・コントローラー名には、ディレクトリー・サーバー TCP/IP ホストおよびドメイン名、またはディレクトリー・サーバー・アドレスを指定できます。

b. ドメイン・コントローラーに接続するための、次のような接続情報を指定する。

- 「**セキュア接続 (SSL または TLS) を使用**」を選択して、 EIM ドメイン・コントローラーに対するセキュア接続を使用する。これを選択すると、接続は Secure Sockets Layer (SSL) または Transport Layer Security (TLS) のいずれかを使用して、インターネットなどの非トラステッド・ネットワーク上での EIM データ伝送を保護するセキュア接続を確立します。

  注: EIM ドメイン・コントローラーが、セキュア接続を使用するように構成されているかどうかを検査しなければなりません。そうでなければ、ドメイン・コントローラーへの接続は失敗します。
- 「**ポート**」フィールドで、ディレクトリー・サーバーが listen する TCP/IP ポートを指定する。デフォルトのポートは、「**セキュア接続の使用**」が選択された場合には 636、選択されなかった場合には 389 です。

c. 「**接続の検査**」をクリックして、ウィザードが指定された情報を使用して、リモート EIM ドメイン・コントローラーへの接続を正常に確立できることをテストする。

d. 「**次へ**」をクリックする。

8. 「**接続のユーザーを指定**」ページで、接続に使用する「**ユーザー・タイプ**」を選択する。 「**識別名およびパスワード**」、「**Kerberos キー・タブ・ファイルおよびプリンシパル**」、「**Kerberos プリンシパルおよびパスワード**」、または「**ユーザー・プロファイルおよびパスワード**」のいずれかのユーザー・タイプを選択できます。 2 つの Kerberos ユーザー・タイプは、 ローカル iSeries システムに対して

ネットワーク認証サービスが構成されている場合にのみ使用可能です。ダイアログを完了するために必要となる他の情報は、以下のように、選択するユーザー・タイプによって異なります。

注: 必要な EIM オブジェクトをディレクトリー内に作成するための十分の権限をウィザードが持っていることを確認するには、ユーザー・タイプとして「**識別名およびパスワード**」を選択し、ユーザーとして LDAP 管理者 DN およびパスワードを指定します。

別のユーザーを接続に指定できます。ただし、指定するユーザーは、リモート・ディレクトリー・サーバーに対して LDAP 管理者と同等の権限を持っている必要があります。

a. 「**識別名およびパスワード**」を選択する場合は、以下の情報を指定する。
   - 「**識別名**」フィールドに、 LDAP 管理者の識別名 (DN) とパスワードを指定して、 EIM ドメインおよびその中のオブジェクトを管理するための十分な権限をウィザードが確実に持つようにする。
   - 「**パスワード**」フィールドに、識別名のパスワードを指定する。
   - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

b. 「**Kerberos キー・タブ・ファイルおよびプリンシパル**」を選択する場合は、以下の情報を指定する。
   - 「**キー・タブ・ファイル**」フィールドに、ウィザードが EIM ドメインに接続する時に使用する、 Kerberos プリンシパルを含む完全修飾パスおよびキー・タブ・ファイル名を指定する。または、「**参照...**」をクリックして、 iSeries 統合ファイル・システム内のディレクトリーを参照し、キー・タブ・ファイルを選択する。
   - 「**プリンシパル**」フィールドに、ユーザーを識別するために使用する Kerberos プリンシパルの名前を指定する。
   - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。

c. 「**Kerberos プリンシパルおよびパスワード**」を選択する場合は、以下の情報を指定する。
   - 「**プリンシパル**」フィールドで、 EIM ドメインに接続するときにウィザードが使用する Kerberos プリンシパルの名前を指定する。
   - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
   - 「**パスワード**」フィールドに、Kerberos プリンシパルのパスワードを指定する。
   - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

d. 「**ユーザー・プロファイルおよびパスワード**」を選択する場合は、以下の情報を指定する。
   - 「**ユーザー・プロファイル**」フィールドで、 EIM ドメインに接続するときにウィザードが使用するユーザー・プロファイル名を指定する。
   - 「**パスワード**」フィールドに、ユーザー・プロファイルのパスワードを指定する。
   - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

e. 「**接続の検査**」をクリックして、ウィザードが指定されたユーザー情報を使用して、 EIM ドメイン・コントローラーへの接続を正常に確立できることをテストする。

f. 「**次へ**」をクリックする。

9. 「**ドメインの指定**」ページで、以下の情報を指定する。
   a. 「**ドメイン**」フィールドに、作成したい EIM ドメインの名前を指定する。 EIM というデフォルトの名前を受け入れるか、意味のある任意の一連の文字を入力する。ただし、**= + < > , # ; ¥** および * などの特殊文字は使用できません。
   b. 「**記述**」フィールドに、ドメインを説明するテキストを入力する。
   c. 「**次へ**」をクリックする。
10. 「**ドメインの親 DN を指定**」ダイアログで、「**はい**」を選択して、 作成中の EIM ドメインの位置にウィザードが使用する親 DN を指定する。 これは、ディレクトリー情報ツリー階層においてユーザーのドメイン名項目のすぐ上の項目を表す DN です。または「**いいえ**」を指定して、 EIM ドメイン名から派生した接尾部を持つディレクトリー位置に EIM データを保管する。

    注: ウィザードを使用してリモート・ドメイン・コントローラー上にドメインを構成する際には、ドメインの適切な親 DN を指定する必要があります。親 DN に必要なすべての構成オブジェクトはすでに存在していなければならず、そうでなければ EIM 構成が失敗するので、 手動で DN 情報を入力するよりも、「参照」を使用して適切な親 DN を選択する必要があります。 親 DN の使用について詳しくは、「**ヘルプ**」をクリックしてください。
11. 「**レジストリー情報**」ページで、レジストリー定義としてローカル・ユーザー・レジストリーを EIM ドメインに追加するかどうかを指定する。以下のユーザー・レジストリー・タイプのいずれかまたは両方を選択します。

    注: レジストリー定義はこの時点で作成する必要はありません。後でレジストリー定義を作成することを選択する場合には、 システム・レジストリー定義の追加および EIM 構成プロパティーの更新を行う必要があります。
    a. 「**ローカル i5/OS**」を選択して、ローカル・レジストリーのレジストリー定義を追加する。提供されたフィールドで、レジストリー定義名のデフォルト値を受け入れるか、または別の値を指定する。 EIM レジストリー名は、そのレジストリーのレジストリー・タイプと特定のインスタンスを表す任意のストリングです。
    b. 「**Kerberos**」を選択して、 Kerberos レジストリーのレジストリー定義を追加する。提供されたフィールドで、レジストリー定義名のデフォルト値を受け入れるか、または別の値を指定する。デフォルトのレジストリー定義名は、レルム名と同じです。デフォルト名を受け入れて、レルム名と同じ Kerberos レジストリー名を使用することにより、レジストリーからの情報検索のパフォーマンスを向上させることができます。必要であれば、「**Kerberos ユーザー識別で大文字小文字を区別**」を選択してください。
    c. 「**次へ**」をクリックする。
12. 「**EIM システム・ユーザーの指定**」ページで、オペレーティング・システム機能の代わりに EIM 操作を実行する場合にシステムが使用する「**ユーザー・タイプ**」を選択する。 これらの操作には、マッピング・ルックアップ操作や、ローカル i5/OS ユーザー・プロファイルを削除する場合のアソシエーションの削除が含まれます。「**識別名およびパスワード**」、「**Kerberos キー・タブ・ファイルおよびプリンシパル**」、または「**Kerberos プリンシパルおよびパスワード**」のいずれかのユーザー・タイプを選択できます。どのユーザー・タイプを選択できるかは、現行のシステム構成によって異なります。たとえば、システムに対してネットワーク認証サービスが構成されていない場合には、 Kerberos ユーザー・タイプが選択できない場合があります。ページを完了するために必要となる他の情報は、以下のように、選択するユーザー・タイプによって異なります。

    注: EIM ドメイン・コントローラーをホスティングしている、現在ディレクトリー・サーバー内で定義されているユーザーを指定しなければなりません。指定するユーザーは、少なくとも、マッピング・ルックアップを実行する権限と、ローカル・ユーザー・レジストリーのレジストリー管理を実

行する特権を持っている必要があります。指定するユーザーがこれらの特権を持っていない場合は、シングル・サインオンの使用およびユーザー・プロファイルの削除に関連した特定のオペレーティング・システム機能は失敗することがあります。

このウィザードを実行する前に、ディレクトリー・サーバーを構成していない場合、選択できるユーザー・タイプは「**識別名およびパスワード**」、指定できる識別名は LDAP 管理者の DN に限定されます。

a. 「**識別名およびパスワード**」を選択する場合は、以下の情報を指定する。
   - 「**識別名**」フィールドに、 EIM 操作を実行する時に使用するシステムのユーザーを識別する LDAP 識別名を指定する。
   - 「**パスワード**」フィールドに、識別名のパスワードを指定する。
   - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

b. 「**Kerberos プリンシパルおよびパスワード**」を選択する場合は、以下の情報を指定する。
   - 「**プリンシパル**」フィールドに、 EIM 操作の実行時に使用するシステムの Kerberos プリンシパル名を指定する。
   - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、 キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
   - 「**パスワード**」フィールドに、ユーザーのパスワードを入力する。
   - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

c. 「**Kerberos キー・タブ・ファイルおよびプリンシパル**」を選択する場合は、以下の情報を指定する。
   - 「**キー・タブ・ファイル**」フィールドに、 EIM 操作を実行する時に使用するシステムの Kerberos プリンシパルを含む完全修飾パスおよびキー・タブ・ファイル名を指定する。または、「**参照...**」をクリックして、 iSeries 統合ファイル・システム内のディレクトリーを参照し、キー・タブ・ファイルを選択する。
   - 「**プリンシパル**」フィールドに、 EIM 操作の実行時に使用するシステムの Kerberos プリンシパル名を指定する。
   - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、 キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。

d. 「**接続の検査**」をクリックして、ウィザードが指定されたユーザー情報を使用して、 EIM ドメイン・コントローラーへの接続を正常に確立できることを確認する。

e. 「**次へ**」をクリックする。

13. 「**要約**」パネルで、指定した構成情報を見直す。すべての情報が正しければ、「**完了**」をクリックする。

ドメインの EIM 構成の完了

ウィザードが完了すると、新規ドメインが「**ドメイン管理**」フォルダーに追加され、このサーバーの基本 EIM 構成が作成されています。しかし、ドメインの EIM 構成を完了するには、以下の作業を実行する必要があります。

1. 新規ドメインの結合を行うそれぞれの追加サーバー上で、 EIM 構成ウィザードを使用する。

2. 必要であれば、EIM ドメインに参加させる、他の非 iSeries のサーバーとアプリケーション用の EIM レジストリー定義を、 EIM ドメインに追加する。これらのレジストリー定義は、ドメインに参加しなければならない実際のユーザー・レジストリーを参照します。 EIM インプリメンテーション要件に応じて、 システム・レジストリー定義の追加 またはアプリケーション・レジストリー定義の追加 のいずれかを行えます。
3. インプリメンテーション要件を基に、以下を行うかどうかを判別する。
   a. ドメイン内のそれぞれの固有ユーザーまたはエンティティーごとに行う EIM ID の作成、およびそれらに対する ID アソシエーションの作成
   b. ユーザーのグループを単一ターゲット・ユーザー ID にマップする、 ポリシー・アソシエーションの作成
   c. これらの組み合わせの作成
4. EIM マッピングのテスト機能を使用して、 EIM 構成の ID マッピングをテストする。
5. 定義した EIM ユーザーだけが LDAP 管理者の DN である場合には、 EIM ユーザーには、ディレクトリー・サーバー上のすべてのデータに対する高水準の権限があります。 したがって、1 つ以上の DN を、EIM データに対するより適切で限定されたアクセス制御を持つ追加ユーザーとして作成することを考慮できるかもしれません。ディレクトリー・サーバー用の DN の作成については、IBM Directory Server for iSeries (LDAP) のトピックの 識別名 (Distinguished names) で確認してください。追加の EIM ユーザーをいくつ定義するかは、ご使用のセキュリティー・ポリシーが、セキュリティー上の義務および責任の分離にどの程度重きを置いているかによって異なります。一般に、以下のタイプのうちの少なくとも 2 つの DN を作成します。
   - **EIM 管理者アクセス制御を持つユーザー。**

     この EIM 管理者 DN は、 EIM ドメインを管理する責任を持つ管理者に、適切なレベルの権限を提供します。 iSeries ナビゲーターによって EIM ドメインのすべての局面を管理する際に、 この EIM 管理者 DN を使用してドメイン・コントローラーに接続できます。
   - **以下のアクセス制御のすべてを持つ、少なくとも 1 つのユーザー。**
     - ID 管理者
     - レジストリー管理者
     - EIM マッピング操作

     このユーザーは、オペレーティング・システムのために EIM 操作を実行するシステム・ユーザーに必要な、適切なレベルのアクセス制御を提供します。

   注: LDAP 管理者 DN の代わりに、システム・ユーザーのこの新規 DN を使用するには、 iSeries サーバー用の EIM 構成プロパティーを変更しなければなりません。システム・ユーザー DN を変更する方法については、EIM 構成プロパティーの管理で確認してください。

基本ネットワーク認証サービス構成を作成した場合、特にシングル・サインオン環境をインプリメントしている場合には、追加のタスクを実行する必要があるかもしれません。これらの追加ステップについては、i5/OS 用のシングル・サインオンを使用可能にする (Enable single signon for i5/OS) のシナリオによって示された、完全な構成ステップを検討してください。

既存ドメインの結合

ここでは、EIM (エンタープライズ識別マッピング) 構成ウィザードを 1 つの iSeries システム上で使用して、ドメイン・コントローラーを構成しEIM ドメインを作成してから、そのウィザードを使用して他の iSeries サーバーがドメインに参加するように構成する方法を説明します。

1 つのシステム上で EIM ドメインを作成しディレクトリー・サーバーをドメイン・コントローラーとして構成した後、追加のすべての iSeries サーバー (V5R2 またはそれ以降) を構成して、 既存の EIM ドメインに結合できます。ウィザードで作業する際は、 EIM ドメイン・コントローラーへの接続情報を含めたドメインに関する情報を入力する必要があります。 EIM 構成ウィザードを使用して既存のドメインを結合するとき、システム上での EIM の構成の一部として Kerberos を構成することを選択する場合には、ウィザードはやはりネットワーク認証サービス構成ウィザードを立ち上げるオプションを提供します。

既存のドメインを結合するために EIM 構成ウィザードを完了すると、以下のタスクを完了できます。

- システム用のネットワーク認証サービスの構成
- ローカル i5/OS レジストリーおよび Kerberos レジストリー用の EIM レジストリー定義の作成
- 既存 EIM ドメインに参加するようシステムを構成する

ご使用のシステムを既存 EIM ドメインに結合するよう構成するには、以下の特殊権限のすべてを持っていなければなりません。

- セキュリティー管理者 (*SECADM)
- すべてのオブジェクト (*ALLOBJ)

EIM 構成ウィザードの使用を開始して既存の EIM ドメインを結合するには、以下のステップを実行してください。

1. リモート・システム上のディレクトリー・サーバーがアクティブであることを確認する。
2. iSeries ナビゲーターで、 EIM を構成するシステムを選択し、「**ネットワーク**」>「**エンタープライズ識別マッピング**」を展開する。
3. 「**構成**」を右マウス・ボタン・クリックして、「**構成... (Configure...)**」を選択し、EIM 構成ウィザードを開始する。

   注: EIM が以前にシステム上で構成済みの場合には、このオプションには「**再構成... (Reconfigure..)**」というラベルが付いています。
4. ウィザードの「**ウェルカム**」ページで、「**既存ドメインの結合**」を選択して「**次へ**」をクリックする。

   注: 現在 iSeries サーバーでネットワーク認証サービスが構成されていない場合、またはシングル・サインオン環境を構成するために追加のネットワーク認証構成情報が必要な場合には、「**ネットワーク認証サービスの構成**」ページが表示されます。このページでは、ネットワーク認証サービス構成ウィザードを開始して、 ネットワーク認証サービスを構成することができます。または後ほど、iSeries ナビゲーターにより、このサービスに対して構成ウィザードを使用して、ネットワーク認証サービスを構成できます。ネットワーク認証サービスの構成が完了したら、EIM 構成ウィザードは次に進みます。
5. ネットワーク認証サービスを構成するには、以下のステップを完了する。
   a. 「**ネットワーク認証サービスの構成**」ページで、「**はい**」を選択して、ネットワーク認証サービス構成ウィザードを開始する。このウィザードで、いくつかの i5/OS インターフェースおよびサービスを、 Kerberos レルムに参加するように構成し、 また EIM およびネットワーク認証サービスの両方を使用するシングル・サインオン環境を構成できます。
   b. 「**レルム情報の指定**」ページで、「**デフォルト・レルム**」フィールドに、デフォルトのレルムの名前を指定する。 Kerberos 認証に Microsoft Active Directory を使用する場合には、「**Kerberos 認証に Microsoft Active Directory を使用**」を選択して、「**次へ**」をクリックする。
   c. 「**KDC 情報の指定**」ページで、「**KDC**」 フィールドに、このレルムの Kerberos サーバーの完全修飾名を指定し、「**ポート**」フィールドには 88 を指定して、「**次へ**」をクリックする。

d. 「**パスワード・サーバー情報の指定**」ページで、パスワード・サーバーのセットアップについて、「**はい**」または「**いいえ**」を選択する。パスワード・サーバーにより、プリンシパルは Kerberos サーバー上のパスワードを変更できます。「**はい**」を選択した場合には、「**パスワード・サーバー**」フィールドにパスワード・サーバー名を入力します。「**ポート**」フィールドでは、デフォルト値 464 を受け入れて、「次へ」をクリックします。

e. 「**キー・タブ項目の選択**」ページで、「**i5/OS Kerberos 認証**」を選択し、「**次へ**」をクリックする。

注: さらに、IBM Directory Server for iSeries (LDAP)、iSeries NetServer、および iSeries HTTP サーバーが Kerberos 認証を使用するようにする場合には、これらのサービス用のキー・タブ項目も作成できます。これらのサービスが Kerberos 認証を使用する前に、それらに対して追加の構成を実行する必要があるかもしれません。

f. 「**i5/OS キー・タブ項目の作成**」ページで、パスワードを入力して確認し、「**次へ**」をクリックする。これは、i5/OS プリンシパルを Kerberos サーバーに追加する際に使用するのと同じパスワードです。

g. 任意: 「**バッチ・ファイルの作成**」ページで、「**はい**」を選択し、以下の情報を指定して、「**次へ**」をクリックする。

- 「**バッチ・ファイル**」フィールドで、ディレクトリー・パスを更新する。「**参照**」をクリックして適切なディレクトリー・パスを探し出すか、または「**バッチ・ファイル**」フィールドでパスを編集する。
- 「**パスワードの組み込み (Include password)**」フィールドで、「**はい**」を選択する。これにより、i5/OS サービス・プリンシパルと関連したすべてのパスワードが、バッチ・ファイルに組み込まれます。パスワードが平文で表示され、バッチ・ファイルへの読み取りアクセスを持つすべての人が読めるようにすることは重要です。したがって、バッチ・ファイルを使用した後、すぐにそれを Kerberos サーバーおよび PC から削除することは重要です。パスワードを組み込まない場合には、バッチ・ファイルの実行時にパスワードを入力するようプロンプトが出されます。

  注: ウィザードによって生成されるサービス・プリンシパルを、 Microsoft Active Directory に手動で追加することもできます。これを行う方法については、i5/OS プリンシパルを Kerberos サーバーに追加する (Add i5/OS principals to the Kerberos server) で確認してください。

- 「**要約**」ページで、ネットワーク認証サービス構成の詳細を見直し、「**完了**」をクリックして EIM 構成ウィザードに戻る。

6. 「**ドメイン・コントローラーの指定**」ページで、以下の情報を指定する。

注: この EIM 構成を正常に完了するためには、ドメイン・コントローラーとして機能するディレクトリー・サーバーはアクティブでなければなりません。

a. 「**ドメイン・コントローラー名**」フィールドに、 iSeries サーバーを結合する EIM ドメイン用のドメイン・コントロール・サーバーとして機能するシステムの名前を指定する。

b. EIM ドメイン・コントローラーに対するセキュア接続を使用する場合は、「**セキュア接続 (SSL または TLS) を使用**」をクリックする。これを選択すると、接続は Secure Sockets Layer (SSL) または Transport Layer Security (TLS) のいずれかを使用して、インターネットなどの非トラステッド・ネットワーク上での EIM データ伝送を保護するセキュア接続を確立します。

注: EIM ドメイン・コントローラーが、セキュア接続を使用するように構成されているかどうかを検査しなければなりません。そうでなければ、ドメイン・コントローラーへの接続は失敗します。

c. 「**ポート**」フィールドで、ディレクトリー・サーバーが listen する TCP/IP ポートを指定する。デフォルトのポートは、「**セキュア接続の使用**」が選択された場合には 636、選択されなかった場合には 389 です。

d. 「**接続の検査**」をクリックして、ウィザードが指定された情報を使用して、EIM ドメイン・コントローラーへの接続を正常に確立できることをテストする。

e. 「**次へ**」をクリックする。

7. 「**接続のユーザーを指定**」ページで、接続に使用する「**ユーザー・タイプ**」を選択する。次のいずれかのユーザー・タイプを選択できます: 「**識別名およびパスワード**」、「**Kerberos キー・タブ・ファイルおよびプリンシパル**」、「**Kerberos プリンシパルおよびパスワード**」、または「**ユーザー・プロファイルおよびパスワード**」。 2 つの Kerberos ユーザー・タイプは、 ローカル iSeries システムに対してネットワーク認証サービスが構成されている場合にのみ使用可能です。ダイアログを完了するために必要となる他の情報は、以下のように、選択するユーザー・タイプによって異なります。

   注: 必要な EIM オブジェクトをディレクトリー内に作成するための十分の権限をウィザードが持っていることを確認するには、ユーザー・タイプとして「**識別名およびパスワード**」を選択し、ユーザーとして LDAP 管理者 DN およびパスワードを指定します。

   別のユーザーを接続に指定できます。ただし、指定するユーザーは、リモート・ディレクトリー・サーバーに対して LDAP 管理者と同等の権限を持っている必要があります。

   - 「**識別名およびパスワード**」を選択する場合は、以下の情報を指定する。
     - 「**識別名**」フィールドに、 LDAP サーバーのローカル・ネームスペースにオブジェクトを作成する権限のあるユーザーを識別する LDAP 識別名 (DN) を指定する。 以前のステップで、LDAP サーバーを構成するためにこのウィザードを使用したことがある場合は、そのステップで作成した LDAP 管理者の識別名を入力する必要があります。
     - 「**パスワード**」フィールドに、識別名のパスワードを指定する。
     - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。
   - 「**Kerberos キー・タブ・ファイルおよびプリンシパル**」を選択する場合は、以下の情報を指定する。
     - 「**キー・タブ・ファイル**」フィールドに、ウィザードが EIM ドメインに接続する時に使用する、 Kerberos プリンシパルを含む完全修飾パスおよびキー・タブ・ファイル名を指定する。または、「**参照...**」をクリックして、 iSeries 統合ファイル・システム内のディレクトリーを参照し、キー・タブ・ファイルを選択する。
     - 「**プリンシパル**」フィールドに、ユーザーを識別するために使用する Kerberos プリンシパルの名前を指定する。
     - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
   - 「**Kerberos プリンシパルおよびパスワード**」を選択する場合は、以下の情報を指定する。
     - 「**プリンシパル**」フィールドで、 EIM ドメインに接続するときにウィザードが使用する Kerberos プリンシパルの名前を指定する。
     - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。

- 「**パスワード**」フィールドに、Kerberos プリンシパルのパスワードを指定する。
- 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

• 「**ユーザー・プロファイルおよびパスワード**」を選択する場合は、以下の情報を指定する。
- 「**ユーザー・プロファイル**」フィールドで、 EIM ドメインに接続するときにウィザードが使用するユーザー・プロファイル名を指定する。
- 「**パスワード**」フィールドに、ユーザー・プロファイルのパスワードを指定する。
- 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。

• 「**接続の検査**」をクリックして、ウィザードが指定されたユーザー情報を使用して、 EIM ドメイン・コントローラーへの接続を正常に確立できることをテストする。

• 「**次へ**」をクリックする。

8. 「**ドメインの指定**」ページで、結合するドメインの名前を選択して「**次へ**」をクリックする。
9. 「**レジストリー情報**」ページで、レジストリー定義としてローカル・ユーザー・レジストリーを EIM ドメインに追加するかどうかを指定する。以下のユーザー・レジストリー・タイプのいずれかまたは両方を選択します。

• 「**ローカル i5/OS**」を選択して、ローカル・レジストリーのレジストリー定義を追加する。提供されたフィールドで、レジストリー定義名のデフォルト値を受け入れるか、または別の値を指定する。EIM レジストリー名は、そのレジストリーのレジストリー・タイプと特定のインスタンスを表す任意のストリングです。

注: ローカル i5/OS レジストリー定義はこの時点で作成する必要はありません。後で i5/OS レジストリー定義を作成することを選択する場合には、 システム・レジストリー定義の追加 および EIM 構成プロパティーの更新を行う必要があります。

• 「**Kerberos**」を選択して、 Kerberos レジストリーのレジストリー定義を追加する。提供されたフィールドで、レジストリー定義名のデフォルト値を受け入れるか、または別の値を指定する。デフォルトのレジストリー定義名は、レルム名と同じです。デフォルト名を受け入れて、レルム名と同じ Kerberos レジストリー名を使用することにより、レジストリーからの情報検索のパフォーマンスを向上させることができます。必要であれば、「**Kerberos ユーザー識別で大文字小文字を区別**」を選択してください。

注: 別のシステム上の EIM 構成ウィザードを使用して、 この iSeries システムがサービス・プリンシパルを持つ Kerberos レジストリー用のレジストリー定義を追加した場合には、この構成の一部として Kerberos レジストリー定義を追加する必要はありません。しかし、ウィザードを終了した後、このシステムの構成プロパティーで Kerberos レジストリーの名前を指定する必要があります。

• 「**次へ**」をクリックする。

10. 「**EIM システム・ユーザーの指定**」ページで、オペレーティング・システム機能の代わりに EIM 操作を実行する場合にシステムが使用する「**ユーザー・タイプ**」を選択する。 これらの操作には、マッピング・ルックアップ操作や、ローカル i5/OS ユーザー・プロファイルを削除する場合のアソシエーションの削除が含まれます。「**識別名およびパスワード**」、「**Kerberos キー・タブ・ファイルおよびプリンシパル**」、または「**Kerberos プリンシパルおよびパスワード**」のいずれかのユーザー・タイプを選択できます。どのユーザー・タイプを選択できるかは、現行のシステム構成によって異なります。たとえば、システムに対してネットワーク認証サービスが構成されていない場合には、 Kerberos ユーザー・タイプが選択できない場合があります。ページを完了するために必要となる他の情報は、以下のように、選択するユーザー・タイプによって異なります。

注: EIM ドメイン・コントローラーをホスティングしている、現在ディレクトリー・サーバー内で定義されているユーザーを指定しなければなりません。指定するユーザーは、少なくとも、マッピング・ルックアップを実行する権限と、ローカル・ユーザー・レジストリーのレジストリー管理を実行する特権を持っている必要があります。指定するユーザーがこれらの特権を持っていない場合は、シングル・サインオンの使用およびユーザー・プロファイルの削除に関連した特定のオペレーティング・システム機能は失敗することがあります。

- 「**識別名およびパスワード**」を選択する場合は、以下の情報を指定する。
  - 「**識別名**」フィールドに、 EIM 操作を実行する時に使用するシステムのユーザーを識別する LDAP 識別名を指定する。
  - 「**パスワード**」フィールドに、識別名のパスワードを指定する。
  - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。
- 「**Kerberos プリンシパルおよびパスワード**」を選択する場合は、以下の情報を指定する。
  - 「**プリンシパル**」フィールドに、 EIM 操作の実行時に使用するシステムの Kerberos プリンシパル名を指定する。
  - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
  - 「**パスワード**」フィールドに、ユーザーのパスワードを入力する。
  - 「**確認パスワード**」フィールドに、妥当性検査の目的でもう一度パスワードを指定する。
- 「**Kerberos キー・タブ・ファイルおよびプリンシパル**」を選択する場合は、以下の情報を指定する。
  - 「**キー・タブ・ファイル**」フィールドに、 EIM 操作を実行する時に使用するシステムの Kerberos プリンシパルを含む完全修飾パスおよびキー・タブ・ファイル名を指定する。または、「**参照...**」をクリックして、 iSeries 統合ファイル・システム内のディレクトリーを参照し、キー・タブ・ファイルを選択する。
  - 「**プリンシパル**」フィールドに、 EIM 操作の実行時に使用するシステムの Kerberos プリンシパル名を指定する。
  - 「**レルム**」フィールドで、そのプリンシパルがメンバーとなる、完全に修飾された Kerberos レルム名を指定する。プリンシパルおよびレルムの名前は、キー・タブ・ファイル内の Kerberos ユーザーを一意的に識別します。たとえば、レルム `ordept.myco.com` のプリンシパル `jsmith` は、キー・タブ・ファイル内で `jsmith@ordept.myco.com` と表されます。
- 「**接続の検査**」をクリックして、ウィザードが指定されたユーザー情報を使用して、 EIM ドメイン・コントローラーへの接続を正常に確立できることを確認する。
- 「**次へ**」をクリックする。

11. 「**要約**」ページで、指定した構成情報を見直す。すべての情報が正しければ、「**完了**」をクリックする。

ドメインの EIM 構成の完了

ウィザードが完了すると、ドメインが「**ドメイン管理**」フォルダーに追加され、このサーバーの基本 EIM 構成が作成されています。しかし、ドメインの EIM 構成を完了するには、以下の作業を実行する必要があるかもしれません。

1. 必要であれば、EIM ドメインに参加させる、他の非 iSeries のサーバーとアプリケーション用の EIM レジストリー定義を、 EIM ドメインに追加する。 これらのレジストリー定義は、ドメインに参加しな

ければならない実際のユーザー・レジストリーを参照します。 EIM インプリメンテーション要件に応じて、 システム・レジストリー定義の追加またはアプリケーション・レジストリー定義の追加のいずれかを行えます。

2. インプリメンテーション要件を基に、以下を行うかどうかを判別する。
   - ドメイン内のそれぞれの固有ユーザーまたはエンティティーごとに行う EIM ID の作成、およびそれらに対する ID アソシエーションの作成
   - ユーザーのグループを単一ターゲット・ユーザー ID にマップする、 ポリシー・アソシエーションの作成
   - これらの組み合わせの作成
3. EIM マッピングのテスト機能を使用して、 EIM 構成の ID マッピングをテストする。
4. 定義した EIM ユーザーだけが LDAP 管理者の DN である場合には、 EIM ユーザーには、ディレクトリー・サーバー上のすべてのデータに対する高水準の権限があります。 したがって、1 つ以上の DN を、EIM データに対するより適切で限定されたアクセス制御を持つ追加ユーザーとして作成することを考慮できるかもしれません。ディレクトリー・サーバー用の DN の作成については、IBM Directory Server for iSeries (LDAP) のトピックの 識別名 (Distinguished names) で確認してください。追加の EIM ユーザーをいくつ定義するかは、ご使用のセキュリティー・ポリシーが、セキュリティー上の義務および責任の分離にどの程度重きを置いているかによって異なります。一般に、以下のタイプのうちの少なくとも 2 つの DN を作成します。
   - **EIM 管理者アクセス制御を持つユーザー。**

     この EIM 管理者 DN は、 EIM ドメインを管理する責任を持つ管理者に、適切なレベルの権限を提供します。 iSeries ナビゲーターによって EIM ドメインのすべての局面を管理する際に、 この EIM 管理者 DN を使用してドメイン・コントローラーに接続できます。
   - **以下のアクセス制御のすべてを持つ、少なくとも 1 つのユーザー。**
     - ID 管理者
     - レジストリー管理者
     - EIM マッピング操作

     このユーザーは、オペレーティング・システムのために EIM 操作を実行するシステム・ユーザーに必要な、適切なレベルのアクセス制御を提供します。

   注: LDAP 管理者 DN の代わりに、システム・ユーザーのこの新規 DN を使用するには、 iSeries サーバー用の EIM 構成プロパティーを変更しなければなりません。システム・ユーザー DN を変更する方法については、EIM 構成プロパティーの管理で確認してください。

基本ネットワーク認証サービス構成を作成した場合、特にシングル・サインオン環境をインプリメントしている場合には、追加のタスクを実行する必要があるかもしれません。これらの追加ステップについては、i5/OS用のシングル・サインオンを使用可能にする (Enable single signon for i5/OS) のシナリオによって示された、完全な構成ステップを検討してください。

EIM ドメイン・コントローラーへのセキュア接続の構成

ここでは、SSL または TLS を使用して、ドメイン・コントローラーへのセキュア接続をセットアップする方法を説明します。

Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を使用して、 EIM (エンタープライズ識別マッピング) ドメイン・コントローラーへのセキュア接続を確立し、 EIM データの送信を保護することができます。

SSL または TLS を EIM 用に構成するには、以下の作業を完了する必要があります。

1. 必要であれば、Digital Certificate Manager (DCM) を使用して、ディレクトリー・サーバーが SSL に使用する 証明書の作成 (create a certificate) を行う。
2. EIM ドメイン・コントローラーをホスティングするローカル・ディレクトリー・サーバーに対して SSL を使用可能にする (Enable SSL for the local directory server)。
3. iSeries サーバーがセキュア SSL 接続を使用することを指定するために、EIM 構成プロパティーを更新する。 EIM 構成プロパティーを更新するには、以下のようにします。
   a. iSeries ナビゲーターで、 EIM を構成するシステムを選択し、「**ネットワーク**」 → 「**エンタープライズ識別マッピング**」を展開する。
   b. 「**構成**」を右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
   c. 「**ドメイン**」ページで、「**セキュア接続 (SSL または TLS) を使用**」を選択し、「**ポート**」フィールドで、ご使用のディレクトリー・サーバーが listen するセキュア・ポートを指定するか、またはデフォルト値 636 を受け入れて、「**OK**」をクリックする。
4. EIM が iSeries ナビゲーターを使用してドメインを管理するときに SSL 接続を使用することを指定するために、EIM ドメインのプロパティーを更新する。 EIM ドメイン・プロパティーを更新するには、以下のようにします。
   a. iSeries ナビゲーターで、 EIM を構成するシステムを選択し、「**ネットワーク**」 → 「**エンタープライズ識別マッピング**」 → 「**ドメイン管理**」を展開する。
   b. 処理する EIM ドメインを選択する。
      - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 ドメイン管理への EIM ドメインの追加を参照してください。
      - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
   c. 現在接続している EIM ドメインを右マウス・ボタン・クリックし、「**プロパティー**」を選択する。
   d. 「**ドメイン**」ページで、「**セキュア接続 (SSL または TLS) を使用**」を選択し、「**ポート**」フィールドで、ご使用のディレクトリー・サーバーが listen するセキュア・ポートを指定するか、またはデフォルト値 636 を受け入れて、「**OK**」をクリックする。

EIM (エンタープライズ識別マッピング) の管理

ここでは、EIM (エンタープライズ識別マッピング) ドメイン、ID、アソシエーション、レジストリー定義、 EIM アクセス制御などの管理方法を含め、 EIM ドメインおよびドメイン・データの管理方法を学習します。

iSeries サーバーに EIM (エンタープライズ識別マッピング) を構成した後は、EIM ドメインとドメインのデータを管理するための、多くの管理タスクを常時実行する必要があります。企業内での EIM の管理についてさらに詳しくは、以下のページで確認してください。

EIM (エンタープライズ識別マッピング) ドメインの管理

ここでは、EIM (エンタープライズ識別マッピング) ドメインおよび EIM ドメイン・プロパティーを管理する方法を説明します。

iSeries ナビゲーターを使用することによって、 すべての EIM ドメインを管理できます。 EIM ドメインを管理するには、iSeries ナビゲーターの「**ネットワーク**」フォルダーの下の「**ドメイン管理**」フォルダーにそのドメインがリストされていなければならず、リストされていないなら追加する必要があります。EIM

構成ウィザードを使用して新しい EIM ドメインを作成して構成すると、そのドメインが「**ドメイン管理**」フォルダーに自動的に追加されて、そのドメインおよびドメイン内の情報が管理できるようになります。

同じネットワーク上のどこかにある EIM ドメインであれば、 使用している iSeries がそのドメインに参加していない場合であっても、任意の iSeries 接続を使用してそれを管理できます。

ドメインに対して、以下の管理用タスクを実行できます。

EIM ドメインをドメイン管理フォルダーに追加する

このタスクを実行するためには、ユーザーが *SECADM 特殊権限を持っていること、また、追加するドメインが、「**ドメイン管理**」フォルダーに追加されるより前に存在していることが必要です。

既存の EIM (エンタープライズ識別マッピング) ドメインを「**ドメイン管理**」フォルダーに追加するには、以下のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」を展開する。
2. 「**ドメイン管理**」を右マウス・ボタン・クリックして、「**ドメインの追加...**」を選択する。
3. 「**ドメインの追加**」ダイアログで、必要なドメインと接続情報を指定する。または、「**参照**」をクリックして、指定されたドメイン・コントローラーが管理するドメインのリストを表示する。

   注: 「**参照...**」をクリックすると、「**EIM ドメイン・コントローラーへの接続**」ダイアログが表示されます。ドメインのリストを表示するには、 LDAP 管理者アクセス制御または EIM 管理者アクセス制御のいずれかでドメイン・コントローラーに接続しなければなりません。ドメイン・リストの内容は、ユーザーが持っている EIM アクセス制御によって異なります。 LDAP 管理者アクセス制御を持っている場合には、ドメイン・コントローラーが管理するすべてのドメインのリストを表示できます。それ以外の場合は、リストには、ユーザーが EIM 管理者アクセス制御を持つドメインのみ表示します。
4. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断する。
5. 「**OK**」をクリックして、ドメインを追加する。

EIM ドメインに接続する。

EIM (エンタープライズ識別マッピング) ドメインを処理する前に、 まずそのドメインの EIM ドメイン・コントローラーに接続する必要があります。 EIM ドメインには、iSeries サーバーが現行でそのドメインに参加するように構成されていなくても、接続できます。

EIM ドメイン・コントローラーに接続するには、それに接続するユーザーが、 43 ページの『EIM アクセス制御』グループのメンバーでなければなりません。ユーザーの EIM アクセス制御グループ・メンバーシップが、そのドメインでユーザーが実行できるタスク、およびユーザーが表示または変更することのできる EIM データを判別します。

EIM ドメインに接続するには、以下のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 接続するドメインを右マウス・ボタン・クリックする。

   注: 処理したいドメインが「**ドメイン管理**」にリストされていない場合には、 『EIM ドメインをドメイン管理フォルダーに追加する』必要があります。
3. 接続する EIM ドメインを右マウス・ボタン・クリックし、「**接続...**」を選択する。

4. 「**EIM ドメイン・コントローラーへの接続**」ダイアログで、「**ユーザー・タイプ**」を指定し、そのユーザーに必要な識別情報を提供し、ドメイン・コントローラーに接続するためのパスワード・オプションを選択する。
5. 必要であれば、「**ヘルプ**」をクリックして、ダイアログ内のそれぞれのフィールドにどの情報を指定すべきかを判断する。
6. 「**OK**」をクリックして、ドメイン・コントローラーに接続する。

ドメインのポリシー・アソシエーションを使用可能にする

ポリシー・アソシエーションは、ユーザー ID と EIM (エンタープライズ識別マッピング) との間のアソシエーションが存在しない場合に、多対 1 のマッピングを作成する手段を提供します。ポリシー・アソシエーションを使用して、複数のユーザー ID (単一ユーザー ID ではなく) のソース・セットを、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID にマップできます。ただし、ポリシー・アソシエーションを使用する前に、まず最初に、マッピング・ルックアップ操作のためにポリシー・アソシエーションを、ドメインが使用できるようにしておく必要があります。

ドメインのポリシー・アソシエーションを使用するためのマッピング・ポリシー・サポートを使用可能にするには、処理する EIM ドメインに接続し、 また EIM 管理者アクセス制御を持っている必要があります。

ドメインのポリシー・アソシエーションを使用するマッピング・ルックアップ・サポートを使用可能にするには、次のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。 (「**マッピング・ポリシー...**」オプションは、ドメインに接続していない場合は選択できません。)
3. 「**一般**」ページで、「**ドメインのポリシー関連を使用してマッピング・ルックアップを使用可能にする**」を選択する。
4. 「**OK**」をクリックする。

注: ポリシー・アソシエーションが定義されているそれぞれのターゲット・レジストリーごとにマッピング・ルックアップおよびポリシー・アソシエーションの使用を使用可能にする必要があります。ターゲット・レジストリー定義に対してマッピング・ルックアップを使用可能にしないならば、そのレジストリーは EIM マッピング・ルックアップ操作に参加できなくなります。ターゲット・レジストリーがポリシー・アソシエーションを使用できると指定しない場合には、そのレジストリーに定義されたポリシー・アソシエーションが EIM マッピング・ルックアップ操作によって無視されます。

関連概念

42 ページの『EIM マッピング・ポリシー・サポートおよび使用可能化』
ここでは、ドメインに対してポリシー・アソシエーションを使用可能にしたり使用不可にしたりする方法を説明します。

EIM マッピングのテスト

EIM (エンタープライズ識別マッピング) マッピング・テスト・サポートにより、ご使用の EIM 構成に対して、 EIM マッピング・ルックアップ操作を発行することができます。テストを使用して、特定のソー

ス・ユーザー ID が適切なターゲット・ユーザー ID に正確にマップされることを確認できます。そのようなテストは、EIM マッピング・ルックアップ操作が、指定された情報を基にして、正確なターゲット・ユーザー ID を確実に戻せるようにします。

マッピング・テスト機能を使用して EIM 構成をテストするためには、 処理する EIM ドメインに接続し、 以下のうちの 1 つの EIM アクセス制御を持っている必要があります。

- EIM 管理者
- ID 管理者
- レジストリー管理者
- EIM マッピング・ルックアップ操作

マッピング・テスト・サポートを使用して EIM 構成をテストするには、以下のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 ドメイン管理への EIM ドメインの追加を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 接続する EIM ドメインを右マウス・ボタン・クリックし、「**マッピングのテスト...**」を選択する。
4. 「**マッピングのテスト**」ダイアログで、以下の情報を指定する。
   a. 「**ソース・レジストリー**」フィールドに、マッピング・ルックアップ操作テストのソースとして使用するユーザー・レジストリーを参照するレジストリー定義名を供給する。
   b. 「**ソース・ユーザー**」フィールドに、マッピング・ルックアップ操作テストのソースとして使用するユーザー ID 名を供給する。
   c. 「**ターゲット・レジストリー**」フィールドに、マッピング・ルックアップ操作テストのターゲットとして使用するユーザー・レジストリーを参照するレジストリー定義名を供給する。
   d. オプション: 「**ルックアップ情報**」フィールドに、ターゲット・ユーザーに定義されたルックアップ情報を供給する。
5. 必要であれば、「**ヘルプ**」をクリックして、ダイアログ内のそれぞれのフィールドにどの情報が必要かについての詳細を調べる。
6. 「**テスト**」をクリックして、マッピング・ルックアップ操作の結果が表示されたときに、それらを検討する。

   注: マッピング・ルックアップ操作があいまいな結果を戻す場合、「マッピングのテスト - 結果 (Test a Mapping - Results)」ダイアログが表示され、エラー・メッセージおよびルックアップ操作が検索したターゲット・ユーザーのリストを示します。

   a. あいまいな結果のトラブルシューティングをするため、ターゲット・ユーザーを選択し、「**詳細**」をクリックする。
   b. 「マッピングのテスト - 詳細 (Test a Mapping - Details)」ダイアログが表示され、指定されたターゲット・ユーザーに関するマッピング・ルックアップ操作結果についての情報が表示される。マッピング・ルックアップ操作結果の詳細情報については、「ヘルプ」をクリックしてください。
   c. 「**クローズ**」をクリックし、「**マッピングのテスト - 結果 (Test a Mapping - Results)**」ダイアログを終了する。
7. 構成のテストを継続するか、または「**クローズ**」をクリックして終了する。

テスト結果の処理と問題の解決:

テストを実行すると、ターゲット・ユーザー ID は、 管理者が提供したソース・ユーザー ID およびターゲット・ユーザー・レジストリーの間のアソシエーションを、テスト処理が検出したかどうかを戻します。またテストは、2 つのユーザー ID 間に検出されたアソシエーションのタイプを示します。提供された情報を基にしてテスト処理がアソシエーションを検出しなかった場合には、テストは none というターゲット・ユーザー ID を戻します。

テストは、EIM マッピング・ルックアップ操作と同様、以下の順序で検索して、最初に検出された適切なターゲット・ユーザー ID を戻します。

1. 特定の ID アソシエーション
2. 証明書フィルター・ポリシー・アソシエーション
3. デフォルトのレジストリー・ポリシー・アソシエーション
4. デフォルトのドメイン・ポリシー・アソシエーション

あるケースでは、ドメインに対してアソシエーションが構成されているにもかかわらず、テストがターゲット・ユーザー ID の結果を戻さないことがあります。テストのために正確な情報を提供したかどうかを確認してください。情報が正確であるのに、テストが結果を戻さない場合には、以下のいずれか 1 つによって問題が生じたことが考えられます。

- ポリシー・アソシエーション・サポートが、ドメイン・レベルで使用できない。 ドメインのポリシー・アソシエーションを使用可能にする必要があるかもしれません。
- マッピング・ルックアップ・サポートまたはポリシー・アソシエーション・サポートが、個々のレジストリー・レベルで使用できない。 ターゲット・レジストリーに対してマッピング・ルックアップ・サポートおよびポリシー・アソシエーションを使用可能にする必要があるかもしれません。
- EIM ID のターゲット・アソシエーションまたはソース・アソシエーションが正しく構成されていない。たとえば、Kerberos プリンシパル (または windows ユーザー) に対するソース・アソシエーションがないか、もしくはそれが不正確である。または、ターゲット・アソシエーションが不正確なユーザー ID を指定している。 EIM ID のすべての ID アソシエーションの表示を行って、特定の ID のアソシエーションを確認してください。
- ポリシー・アソシエーションが正確に構成されていない。 ドメインのすべてのポリシー・アソシエーションの表示を行って、ドメイン内で定義されているすべてのポリシー・アソシエーションのソース情報およびターゲット情報を確認してください。
- レジストリー定義およびユーザー ID が、大文字小文字が違うために、一致しない。レジストリーまたはアソシエーションを削除し、大文字小文字を正確に指定して再作成できます。

他のケースとして、テストの結果があいまいなこともあります。そのような場合には、そのことを示すエラー・メッセージが表示されます。テストがあいまいな結果を戻すのは、複数のターゲット・ユーザー ID が、指定されたテスト基準と一致する場合です。マッピング・ルックアップ操作は、以下の状況の 1 つ以上が存在する場合に、複数のターゲット・ユーザー ID を戻す可能性があります。

- EIM ID が、同一のターゲット・レジストリーに対して、複数のターゲット・アソシエーションを持っている場合。
- 複数の EIM ID が、ソース・アソシエーション内に同じユーザー ID を指定しており、 かつ、これらの EIM ID が、同一のターゲット・レジストリーに対してターゲット・アソシエーションを持つ場合 (それぞれのターゲット・アソシエーションに指定されたユーザー ID は異なっているかもしれない)。
- 複数のデフォルトのドメイン・ポリシー・アソシエーションが、同一のターゲット・レジストリーを指定する場合。

- 複数のデフォルトのレジストリー・ポリシー・アソシエーションが、同一のソース・レジストリーおよび同一のターゲット・レジストリーを指定する場合。
- 複数の証明書フィルター・ポリシー・アソシエーションが、同一のソース X.509 レジストリー、証明書フィルター、およびターゲット・レジストリーを指定する場合。

複数のターゲット・ユーザー ID を戻すマッピング・ルックアップ操作は、 i5/OS アプリケーションおよびプロダクトを含め、EIM 対応アプリケーションに関して問題が生じることがあります。したがって、あいまいな結果の原因、およびその状態を解決するために取る必要のある処置を判別する必要があります。原因に応じて、以下の 1 つ以上の処置を行えます。

- テストが、不要な複数のターゲット ID を戻す。これは、ドメインのアソシエーション構成が、次のいずれかの理由のため、不正確であることを示しています。
  - EIM ID のターゲット・アソシエーションまたはソース・アソシエーションが正しく構成されていない。たとえば、Kerberos プリンシパル (または windows ユーザー) に対するソース・アソシエーションがないか、もしくはそれが不正確である。または、ターゲット・アソシエーションが不正確なユーザー ID を指定している。 EIM ID のすべての ID アソシエーションの表示を行って、特定の ID のアソシエーションを確認してください。
  - ポリシー・アソシエーションが正確に構成されていない。 ドメインのすべてのポリシー・アソシエーションの表示を行って、ドメイン内で定義されているすべてのポリシー・アソシエーションのソース情報およびターゲット情報を確認してください。
- テストが複数のターゲット ID を戻し、アソシエーションの構成からするとこれらの結果が妥当な場合には、それぞれのターゲット・ユーザー ID ごとにルックアップ情報を指定する必要があります。同じソース (ID アソシエーションの場合には EIM ID、ポリシー・アソシエーションの場合にはソース・ユーザー・レジストリー) を持つすべてのターゲット・ユーザー ID に対して、固有のルックアップ情報を定義する必要があります。それぞれのターゲット・ユーザー ID ごとにルックアップ情報を定義することにより、ルックアップ操作が、考えられるすべてのターゲット・ユーザー ID ではなく、 単一のターゲット・ユーザー ID を戻すようにすることができます。 ターゲット・ユーザー ID にルックアップ情報を追加するを参照してください。マッピング・ルックアップ操作について、このルックアップ情報を指定しなければなりません。

  注: この方法は、アプリケーションがルックアップ情報を使用できる場合にのみ有効です。ただし、iSeries Access for Windows などの 基本 i5/OS アプリケーションは、ルックアップ情報を使用して、ルックアップ操作によって戻された複数のターゲット・ユーザー ID を区別することはできません。したがって、ドメインに対するアソシエーションを再定義して、マッピング・ルックアップ操作が単一のターゲット・ユーザー ID を戻すことができるようにし、 基本 i5/OS アプリケーションが正常にルックアップ操作を実行して ID をマップできるようにする必要があるかもしれません。

ここに説明されたもの以外の、可能性のあるマッピング問題および解決策についての追加情報は、 137 ページの『EIM マッピング問題のトラブルシューティング』を参照してください。

EIM ドメインをドメイン管理フォルダーから除去する

管理する必要のなくなった EIM ドメインは、「**ドメイン管理**」フォルダーから除去できます。ただし、「**ドメイン管理**」フォルダーからドメインを除去することは、ドメインを削除することと同じ**ではなく**、ドメイン・データはドメイン・コントローラーから削除されません。ドメインおよびすべてのドメイン・データを実際に削除したい場合には、 ドメインの削除を参照してください。

ドメインを除去するために 43 ページの『EIM アクセス制御』は必要ありません。

管理する必要のなくなった EIM (エンタープライズ識別マッピング) ドメインを「**ドメイン管理**」フォルダーから除去するには、以下のステップに従ってください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」を展開する。
2. 「**ドメイン管理**」を右マウス・ボタン・クリックして、「**ドメインの除去...**」を選択する。
3. 「**ドメイン管理**」から除去する EIM ドメインを選択する。
4. 「**OK**」をクリックしてドメインを除去する。

EIM ドメインおよびすべての構成オブジェクトの削除

EIM ドメインを削除する前に、ドメイン内のすべてのレジストリー定義、およびすべての EIM (エンタープライズ識別マッピング) ID を削除する必要があります。ドメインおよびすべてのドメイン・データを削除したくないが、もうそのドメインを管理したくない場合には、代わりにドメインの除去を行えます。

EIM ドメインを削除するには、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- LDAP 管理者
- EIM 管理者

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 必要であれば、 EIM ドメインからすべてのレジストリー定義の削除を行う。
3. 必要であれば、 EIM ドメインからすべての EIM ID の削除を行う。
4. 削除するドメインを右マウス・ボタン・クリックし、「**削除...**」を選択する。
5. 「**削除の確認**」ダイアログで「**はい**」をクリックする。

| **注:** 「進行中の削除 (Delete in Progress)」ダイアログが表示され、プロセスが完了するまでドメイン削
| 除の状況を示します。

EIM (エンタープライズ識別マッピング) レジストリー定義の管理

ここでは、企業内の、EIM (エンタープライズ識別マッピング) に参加するユーザー・レジストリー用の EIM レジストリー定義を作成および管理する方法を説明します。

ユーザー・レジストリーおよびそれらが含むユーザー ID を、 EIM ドメインに参加させるには、それらに対して レジストリー定義を作成しなければなりません。そうすれば、これらの EIM レジストリー定義を管理することによって、ユーザー・レジストリーおよびそれらのユーザー ID が EIM に参加する方法を管理できます。

レジストリー定義に対して、以下の管理用タスクを実行できます。

関連概念

116 ページの『ポリシー・アソシエーションの作成』

関連タスク

130 ページの『ポリシー・アソシエーションの削除』

システム・レジストリー定義の追加

システム・レジストリー定義を作成するには、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、 また EIM 管理者アクセス制御を持っている必要があります。

EIM ドメインにシステム・レジストリー定義を追加するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「ドメイン管理」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 98 ページの『EIM ドメインに接続する。』を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ユーザー・レジストリー**」を右マウス・ボタン・クリックし、「**レジストリーの追加**」、「**システム...**」を選択する。
5. 「**システム・レジストリーの追加**」ダイアログ・ボックスで、システム・レジストリー定義に関する、次のような情報を供給する。
   a. システム・レジストリー定義の名前
   b. レジストリー定義タイプ
   c. システム・レジストリー定義の記述
   d. (オプション) ユーザー・レジストリー URL
   e. システム・レジストリー定義の、1 つ以上の別名 (必要な場合)。
6. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を供給すべきかを判断する。
7. 「**OK**」をクリックして、情報を保管し、レジストリー定義を EIM ドメインに追加する。

アプリケーション・レジストリー定義の追加

アプリケーション・レジストリー定義を作成するには、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、 また EIM 管理者アクセス制御を持っている必要があります。

EIM ドメインにアプリケーション・レジストリー定義を追加するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「ドメイン管理」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 98 ページの『EIM ドメインに接続する。』を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ユーザー・レジストリー**」を右マウス・ボタン・クリックし、「**レジストリーの追加**」、「**アプリケーション...**」を選択する。
5. 「**アプリケーション・レジストリーの追加**」ダイアログで、アプリケーション・レジストリー定義に関する、次のような情報を供給する。
   a. アプリケーション・レジストリー定義の名前。
   b. 定義しているアプリケーション・ユーザー・レジストリーがサブセットとなっているシステム・レジストリー定義の名前。指定するシステム・レジストリー定義が、すでに EIM 内に存在していなければなりません。そうでなければ、アプリケーション・レジストリー定義の作成が失敗します。
   c. レジストリー定義タイプ
   d. アプリケーション・レジストリー定義の記述。

e. アプリケーション・レジストリー定義の、1 つ以上の別名 (必要な場合)。

6. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を供給すべきかを判断する。
7. 「**OK**」をクリックして、情報を保管し、レジストリー定義を EIM ドメインに追加する。

グループ・レジストリー定義の追加

グループ・レジストリー定義を作成するには、処理する EIM ドメインに接続し、 また EIM 管理者アクセス制御を持っている必要があります。

EIM ドメインにグループ・レジストリー定義を追加するには、以下のステップを完了してください。

1. 「**ネットワーク**」 → 「**エンタープライズ識別マッピング**」 → 「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   a. 処理したい EIM ドメインが「ドメイン管理」フォルダーの下にリストされていない場合は、ドメイン管理への EIM ドメインの追加を参照してください。
   b. 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ユーザー・レジストリー**」を右マウス・ボタン・クリックし、「**レジストリーの追加**」、「**グループ...**」を選択する。
5. 「グループ・レジストリーの追加 (Add Group Registry)」ダイアログで、グループ・レジストリー定義に関する、次のような情報を供給する。
   a. グループ・レジストリー定義の名前。
   b. グループ・レジストリー定義のすべてのメンバーが大/小文字を区別する場合、「**グループ・レジストリー・メンバーに大/小文字の区別あり (Group registry members are case sensitive)**」を選択する。
   c. グループ・レジストリー定義の記述。
   d. グループ・レジストリー定義の、1 つ以上の別名 (必要な場合)。
6. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を供給すべきかを判断する。
7. 7.「**OK**」をクリックして、情報を保管し、レジストリー定義を EIM ドメインに追加する。

別名のレジストリー定義への追加

管理者またはアプリケーション開発者は、 レジストリー定義に関する追加の識別情報を指定できます。このことは、レジストリー定義の別名を作成することによって行えます。そうすれば、ユーザー自身や他のユーザーは、レジストリー定義の別名を使用して、ユーザー・レジストリー同士をより良く区別できます。

この別名サポートによって、プログラマーは、アプリケーションを展開する管理者が選択する任意の EIM (エンタープライズ識別マッピング) レジストリー定義名を事前に把握しなくても、アプリケーションを作成できます。 EIM 管理者には、アプリケーションが使用する別名を付属する資料で知らせます。この情報を使用して、EIM 管理者はこの別名を、管理者がアプリケーションで使用したい実際のユーザー・レジストリーを表す EIM レジストリー定義に割り当てることができます。

別名をレジストリー定義に追加する場合、処理する EIM ドメインに接続し、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (修正するレジストリー) の管理者
- EIM 管理者

EIM レジストリー定義に別名を追加するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「ドメイン管理」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 98 ページの『EIM ドメインに接続する。』を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ユーザー・レジストリー**」をクリックして、ドメイン中のレジストリー定義のリストを表示する。

   注: 選択されたレジストリー・アクセス制御の管理者である場合には、リストには特に許可されたレジストリー定義だけが含まれます。
5. 別名の追加先のレジストリー定義を右マウス・ボタン・クリックして、「**プロパティー...**」を選択する。
6. 「**別名**」ページを選択して、追加する別名の名前とタイプを指定する。

   注: タイプのリストに含まれていない別名タイプも指定できます。
7. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断する。
8. 「**追加**」をクリックする。
9. 「**OK**」をクリックして、レジストリー定義に対する変更を保管する。

EIM 中の専用ユーザー・レジストリー・タイプの定義

EIM (エンタープライズ識別マッピング) レジストリー定義を作成する際に、多数の事前定義ユーザー・レジストリー・タイプのうちの 1 つを指定して、企業内のシステム上に存在する実際のユーザー・レジストリーを表すことができます。事前定義レジストリー定義タイプは、ほとんどのオペレーティング・システム・ユーザー・レジストリーをカバーしていますが、 EIM に事前定義レジストリー・タイプが含まれていないレジストリー定義を作成する必要があることもあります。この状況では、2 つのオプションがあります。すなわち、そのユーザー・レジストリーの特性に一致する既存のレジストリー定義を使用するか、または専用ユーザー・レジストリー・タイプを定義できます。

EIM が認識するよう事前定義されていないユーザー・レジストリー・タイプを定義するには、レジストリー・タイプを **ObjectIdentifier-normalization** という形式で指定する、 オブジェクト ID (OID) を使用しなければなりません。ここで、**ObjectIdentifier** は 1.2.3.4.5.6.7 などのドット 10 進数のオブジェクト ID、**normalization** は **caseExact** か **caseIgnore** のどちらかの値になります。たとえば、iSeries のオブジェクト ID (OID) は、`1.3.18.0.2.33.2-caseIgnore` です。

確実に固有の OID を作成し使用するには、必要な OID を正規の OID 登録局から入手する必要があります。 固有の OID を使用することによって、他の組織やアプリケーションによって作成された OID と競合する可能性を排除できます。

OID を入手するには以下の 2 つの方法があります。

- **オブジェクトを登録局に登録する。**これは、情報を表すのに少数の固定の OID が必要な場合に良い方法です。 たとえば、これらの OID で会社のユーザーの証明書ポリシーを表すことができるかもしれません。
- **必要に応じて、登録局から arc 割り当てを取得し、独自の OID を割り当てる。**これは、ドット 10 進数のオブジェクト ID の範囲の割り当てのことですが、 多数の OID が必要な場合や、OID 割り当てが変更の対象になる場合は、これを取得することをお勧めします。 arc 割り当てはドット 10 進数から成り、これをベースとして **ObjectIdentifier** の先頭に持ってこなければなりません。たとえば、arc 割り当てが 1.2.3.4.5. であるとします。 この基本 arc に数値を追加して OID を作成できます。たとえば、1.2.3.4.5.x.x.x) という形式の OID を作成できます。

以下のインターネット・リソースを調べることによって、OID を登録局に登録することについてさらに学ぶことができます。

- ANSI は組織名に関する米国の登録局です。International Standards Organization (ISO) や International Telecommunication Union (ITU) によって確立された国際的な登録処理に基づいています。登録済みアプリケーション・プロバイダー ID (Registered Application Provider Identifier (RID)) の適用に関する Microsoft Word の意思決定用紙は、 ANSI 共用文書ライブラリー Web サイト (http://public.ansi.org/ansionline/Documents/) にあります。「**他のサービス (Other Services)**」> 「**登録プログラム (Registration Programs)**」を選択することによって、意思決定用紙を見つけることができます。組織の ANSI OID arc は 2.16.840.1 です。 ANSI による OID arc の割り当てには料金がかかります。 ANSI から割り当てられた OID arc を受け取るまでには、約 2 週間を要します。 ANSI は数値 (NEWNUM) を割り当て、新しい OID arc を作成します。例、2.16.840.1.NEWNUM
- ほとんどの国や地域では、国の標準化機関が OID レジストリーを保守しています。 ANSI の arc と同様、これらの arc は通常 OID 2.16 の下に割り当てられています。 特定の国や地域の OID 登録局を見つけるには、多少の調査が必要かもしれません。 ISO 国際メンバーになっている団体のアドレスは、http://www.iso.ch/addresse/membodies.html で見つかるかもしれません。この情報には、郵便番号と電子メールが含まれています。ほとんどの場合、Web サイトも指定されています。
- Internet Assigned Numbers Authority (IANA) は、 arc 1.3.6.1.4.1 の中で専用の企業番号 (OID) を割り当てています。 IANA はこれまで 7500 を超える企業に arc を割り当ててきました。申し込みページは、http://www.iana.org/cgi-bin/enterprise.pl の、 Private Enterprise Numbers の下にあります。IANA による割り当てには約 1 週間かかります。 IANA の OID は無料です。 IANA は数値 (NEWNUM) を割り当てるので、 新しい OID arc は 1.3.6.1.4.1.NEWNUM になります。
- 米国の連邦政府は、Computer Security Objects Registry (CSOR) を保守しています。 CSOR は、arc 2.16.840.1.101.3 の命名機関で、現在セキュリティー・ラベル、暗号アルゴリズム、および証明書ポリシーのオブジェクトを登録しています。証明書ポリシーの OID は、arc 2.16.840.1.101.3.2.1 の形式で定義されます。 CSOR は、米国の連邦政府の機関にポリシー OID を割り当てます。 CSOR について詳しくは、http://csrc.nist.gov/csor/ を参照してください。

  関連情報

  http://csrc.nist.gov/csor/pkireg.htm

ターゲット・レジストリーに対してマッピング・ルックアップ・サポートおよびポリシー・アソシエーションを使用可能にする

EIM (エンタープライズ識別マッピング) マッピング・ポリシー・サポートにより、ユーザー ID と EIM ID との間のアソシエーションが存在しない場合に、多対 1 のマッピングを作成する手段として、ポリシ

ー・アソシエーションを使用できます。ポリシー・アソシエーションを使用して、複数のユーザー ID (単一ユーザー ID ではなく) のソース・セットを、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID にマップできます。

ただし、ポリシー・アソシエーションを使用する前に、まず最初に、 ドメインのポリシー・アソシエーションを使用したマッピング・ルックアップを使用可能にする必要があります。また、それぞれのレジストリーごとに 1 つか 2 つの設定を使用可能にする必要があります。

- **レジストリーのマッピング・ルックアップを使用可能にする** このオプションを選択すると、レジストリーにポリシー・アソシエーションが定義されているかどうかにかかわりなく、レジストリーが EIM マッピング・ルックアップ操作に参加できるようになります。
- **ポリシー・アソシエーションを使用** このオプションを選択すると、このレジストリーをポリシー・アソシエーションのターゲット・レジストリーとし、それが EIM マッピング・ルックアップ操作に参加できるようにすることができます。

レジストリーに対してマッピング・ルックアップを使用可能にしない場合には、そのレジストリーは EIM マッピング・ルックアップ操作に全く参加できません。レジストリーがポリシー・アソシエーションを使用するように指定しない場合には、そのレジストリーが操作のターゲットとなるとき、 EIM マッピング・ルックアップ操作は、レジストリーに対するポリシー・アソシエーションを無視します。

ターゲット・レジストリーに対してポリシー・アソシエーションを使用するマッピング・ルックアップを使用可能にするには、処理する EIM ドメインに接続し、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- EIM 管理者
- レジストリー管理者
- 選択されたレジストリー (使用可能にするレジストリー) の管理者

一般的にはマッピング・ルックアップ・サポートを使用可能にし、個々の例ではターゲット・レジストリーに対するポリシー・アソシエーションを使用できるようにするには、以下のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**ユーザー・レジストリー**」を選択して、ドメインのレジストリー定義のリストを表示する。

   注: 選択されたレジストリー・アクセス制御の管理者である場合には、リストには特に許可されたレジストリー定義だけが含まれます。
4. ポリシー・アソシエーションのマッピング・ポリシー・サポートを使用可能にしたいレジストリー定義を、右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
5. 「**一般**」ページで、「**レジストリーのマッピング・ルックアップを使用可能にする**」を選択する。このオプションを選択すると、レジストリーが EIM マッピング・ルックアップ操作に参加できます。このオプションが選択されない場合には、レジストリーがルックアップ操作においてソース・レジストリーであるかターゲット・レジストリーであるかにかかわらず、ルックアップ操作はレジストリーのデータを戻すことができません。

6. 「**ポリシー関連を使用**」を選択する。このオプションを選択すると、レジストリーがルックアップ操作のターゲットであるときに、ルックアップ操作が、データを戻すための基礎としてポリシー・アソシエーションを使用できます。
7. 「**OK**」をクリックして、変更を保管する。

注: レジストリーがポリシー・アソシエーションを使用する前に、 ドメインのポリシー・アソシエーションを使用可能にする必要もあります。

関連概念

42 ページの『EIM マッピング・ポリシー・サポートおよび使用可能化』
ここでは、ドメインに対してポリシー・アソシエーションを使用可能にしたり使用不可にしたりする方法を説明します。

レジストリー定義の削除

EIM (エンタープライズ識別マッピング) ドメインからレジストリー定義を削除すると、レジストリー定義が参照するユーザー・レジストリーには影響しませんが、そのユーザー・レジストリーは EIM ドメイン内に参加できなくなります。ただし、レジストリー定義を削除する際、以下の事柄を考慮する必要があります。

- レジストリー定義を削除すると、そのユーザー・レジストリーのアソシエーションすべてが失われます。レジストリーをドメインに再定義する場合、必要なアソシエーションを再度作成する必要があります。
- X.509 レジストリー定義を削除すると、そのレジストリーに定義されたすべての証明書フィルターも失われます。 X.509 レジストリーをドメインに再定義する場合、必要な証明書フィルターを再度作成する必要があります。
- システム・レジストリー定義を親レジストリーとして指定するアプリケーション・レジストリー定義がある場合には、そのシステム・レジストリー定義は削除できません。

レジストリー定義を削除するには、処理する EIM ドメインに接続し、 また EIM 管理者アクセス制御を持っている必要があります。

EIM レジストリー定義を削除するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ユーザー・レジストリー**」をクリックして、ドメインのレジストリー定義のリストを表示する。

   注: 選択されたレジストリー・アクセス制御の管理者である場合には、リストには特に許可されたレジストリー定義だけが含まれます。
5. 削除するユーザー・レジストリーを右マウス・ボタン・クリックし、「**削除...**」を選択する。
6. **確認**ダイアログ上で「**はい**」をクリックして、レジストリー定義を削除する。

別名のレジストリー定義からの除去

別名を EIM (エンタープライズ識別マッピング) レジストリー定義から除去する場合、処理する EIM ドメインに接続し、以下のうちの 1 つの 43 ページの『EIM アクセス制御』 を持っている必要があります。

- レジストリー管理者
- (処理するレジストリー定義の) 選択されたレジストリーの管理者
- EIM 管理者

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ユーザー・レジストリー**」をクリックして、ドメインのレジストリー定義のリストを表示する。

   注: 選択されたレジストリー・アクセス制御の管理者である場合には、リストには特に許可されたレジストリー定義だけが含まれます。
5. レジストリー定義を右マウス・ボタン・クリックし、「**プロパティー...**」を選択する。
6. 「**別名**」ページを選択する。
7. 除去する別名を選択して、「**除去**」をクリックする。
8. 「**OK**」をクリックして、変更を保管する。

グループ・レジストリー定義へのメンバーの追加

メンバーをグループ・レジストリー定義に追加する場合、処理する EIM ドメインに接続し、以下のうちの 1 つの EIM アクセス制御を持っている必要があります。

- EIM 管理者
- レジストリー管理者
- 選択されたレジストリーの管理者 (メンバーを追加するグループ・レジストリー定義、および追加する個々のメンバーに対するグループ・レジストリー定義の両方)

グループ・レジストリー定義にメンバーを追加するには、以下のステップを完了してください。

1. 「**ネットワーク**」 → 「**エンタープライズ識別マッピング**」 → 「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   a. 処理したい EIM ドメインが「ドメイン管理」フォルダーの下にリストされていない場合は、ドメイン管理への EIM ドメインの追加を参照してください。
   b. 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 4.「**ユーザー・レジストリー**」をクリックして、ドメイン中のレジストリー定義のリストを表示する。
5. 5. メンバーの追加先のグループ・レジストリー定義を右マウス・ボタン・クリックし、「**プロパティー...**」を選択する。
6. 6. 「**メンバー**」ページを選択し、「**追加**」をクリックする。

| 7. 7. 「**EIM グループ・レジストリー・メンバーの追加 (Add EIM Group Registry member)**」**ダイアログ**で、1 つ以上のレジストリー定義を選択して「**OK**」をクリックする。 リストの内容は、ユーザーが持っている EIM アクセス制御のタイプによって異なり、グループの他のメンバーと同じ大/小文字の区別をするレジストリー定義に制限されます。
| 8. 8.「**OK**」をクリックして終了する。

EIM (エンタープライズ識別マッピング) ID の管理

ここでは、ドメイン用の EIM (エンタープライズ識別マッピング) ID を作成し管理する方法を説明します。

ネットワーク内のユーザーを表す EIM ID を作成して使用すれば、特定のユーザー ID を所有する人を追跡するのに役立つので、たいへん有用です。企業の中のユーザーは常に変化しています。出入りするユーザーや、部門を移動するユーザーがいます。これらの変更は、ネットワーク内のシステムおよびアプリケーションのユーザー ID およびパスワードのトラックを保持するという、すでに存在している管理上の問題に加えて、さらに問題を増し加えます。さらに、企業内のパスワード管理には多大の時間がかかります。EIM (エンタープライズ識別マッピング) ID を作成し、それらを各ユーザーのユーザー ID に関連付けることにより、 特定のユーザー ID を所有する人の追跡を処理できるようになります。そうすれば、パスワード管理がたいへん簡単になります。

シングル・サインオン (single signon) 環境をインプリメントすると、特にユーザーが企業内の別の部門やエリアに移動する場合に、そのユーザー ID の管理プロセスもより簡単になります。シングル・サインオンを使用可能にすれば、ユーザーが新しいシステム用の新しいユーザー名とパスワードを覚える必要がなくなります。

注: EIM ID を作成および使用する方法は、組織の要件によって異なります。詳しくは、 70 ページの『EIM ID 命名計画の作成』を参照してください。

「**ドメイン管理**」フォルダーで選択可能な、任意の EIM ドメインの EIM ID を管理できます。以下のタスクの任意のものを実行して、EIM ドメイン内の EIM ID を管理できます。

EIM ID の作成

EIM ID を作成するには、 処理する EIM (エンタープライズ識別マッピング) ドメインに接続しており、以下のうちの 1 つのレベルの 43 ページの『EIM アクセス制御』を持っている必要があります。

- ID 管理者
- EIM 管理者

企業内の人またはエンティティーの EIM ID を作成するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」を右マウス・ボタン・クリックし、「**新しい ID... (New identifier...)**」を選択する。
5. 「**新規 EIM ID**」ダイアログで、EIM ID に関する、次のような情報を供給します。

a. ID の名前
b. 必要であれば、システムに固有の名前を生成させるかどうか
c. ID の記述
d. 必要であれば、ID の 1 つ以上の別名

6. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断する。
7. 必要な情報を入力した後、「**OK**」をクリックして、EIM ID を作成する。

注: 多数の EIM ID を作成すると、「**ID**」フォルダーを展開する際、 ID のリストが表示されるまでに時間がかかることがあります。大量の EIM ID がある場合にパフォーマンスを改善するには、 114 ページの『EIM ID ビューのカスタマイズ』を行うことができます。

EIM ID への別名の追加

9 ページの『EIM ID』 用の付加的な識別情報を提供するために、別名を作成できます。 別名は、EIM ルックアップ操作を実行する際に、特定の EIM (エンタープライズ識別マッピング) ID を探し出すのに役立ちます。たとえば、ある人物の本名が知られている名前と異なる場合に、別名が役に立ちます。

EIM ID 名は EIM ドメイン内で固有でなければなりません。別名は、固有の ID の使用が難しいという状況で有効です。たとえば、企業内の別個の人物が同じ名前であることがあり、その場合、その名前を EIM ID として使用するならば、混乱が生じる可能性があります。たとえば、John J. Johnson という名前のユーザーが 2 人いる場合は、 各ユーザーの ID を区別するために John Joseph Johnson という別名と John Jeffrey Johnson という別名を作成できます。他にも、それぞれのユーザーの従業員番号、部門番号、役職、あるいは区別するための他の属性を含めて、別名を作成できます。

別名を EIM ID に追加する場合、処理する EIM ドメインに接続し、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- EIM 管理者
- ID 管理者

EIM ID に別名を追加するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックし、右側の画面区画に、ドメイン内の使用可能な EIM ID のリストを表示する。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 114 ページの『EIM ID ビューのカスタマイズ』を行えます。
5. 別名の追加先の EIM ID を右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
6. 「**別名**」フィールドで、 この EIM ID に追加する別名を指定して、「**追加**」をクリックする。
7. 「**OK**」をクリックして、EIM ID に対する変更を保管する。

EIM ID からの別名の除去

別名を EIM (エンタープライズ識別マッピング) ID から除去する場合、処理する EIM ドメインに接続し、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- ID 管理者
- EIM 管理者

EIM ID から別名を除去するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックし、右側の画面区画に、ドメイン内の使用可能な EIM ID のリストを表示する。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 114 ページの『EIM ID ビューのカスタマイズ』を行えます。
5. 別名の追加先の EIM ID を右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
6. 除去する別名を選択して、「**除去**」をクリックする。
7. 「**OK**」をクリックして、変更を保管する。

EIM ID の削除

EIM ID を削除するには、 処理する EIM (エンタープライズ識別マッピング) ドメインに接続しており、EIM 管理者アクセス制御を持っている必要があります。

EIM ID を削除するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックする。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 114 ページの『EIM ID ビューのカスタマイズ』を行えます。
5. 削除する EIM ID を選択する。 複数の ID を削除するには、EIM ID を選択して **Ctrl** キーを押します。
6. 選択した EIM ID を右マウス・ボタン・クリックして「**削除**」を選択する。

7. 「**削除の確認 (Delete Confirmation)**」ダイアログで「**はい**」をクリックして、選択した EIM ID を削除する。

EIM ID ビューのカスタマイズ

「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM (エンタープライズ識別マッピング) ID がある場合にパフォーマンスを改善するには、「**ID**」フォルダーのビューをカスタマイズできます。

「**ID**」フォルダー・ビューをカスタマイズするには、以下のステップに従ってください。

1. 「**ネットワーク**」->「**エンタープライズ識別マッピング**」->「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**ID**」フォルダーを右マウス・ボタン・クリックして、「**このビューのカスタマイズ (Customize this view...)**」を選択する。
4. ドメイン内の EIM ID を表示するために使用する基準を指定する。表示される EIM ID の数を絞りたい場合には、 ID のソートに使用する文字を指定します。 ID 名に 1 つ以上のワイルドカード文字 (*) を指定できます。たとえば、「**ID**」フィールドのソート基準として、 `*JOHNSON*` を入力できます。 その結果、文字ストリング `JOHNSON` が EIM ID 名の一部として定義されているすべての EIM ID、および文字ストリング `JOHNSON` が EIM ID の別名の一部として定義されている EIM ID が戻されます。
5. 「**OK**」をクリックして、変更を保管する。

アソシエーションの管理

ここでは、EIM (エンタープライズ識別マッピング) を使用して管理できるさまざまなタイプのアソシエーションを学習します。

EIM では、ユーザー ID 間の直接的または間接的な関係を定義する、 2 種類のアソシエーションを作成および管理できます。すなわち、ID アソシエーションおよびポリシー・アソシエーションです。 EIM では、EIM ID およびそれらのユーザー ID 間の ID アソシエーションを作成および管理できます。これによりユーザー ID 間の、間接的ですが、特定した個々の関係を定義できます。また EIM により、ポリシー・アソシエーションを作成して、 1 つ以上のレジストリー内の複数のユーザー ID と、別のレジストリー内の個々のターゲット・ユーザー ID 間の関係を記述できます。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。どちらのタイプのアソシエーションも企業内のユーザー ID 間の関係を定義するので、アソシエーションの管理は EIM の管理において重要な要素です。

ドメイン内のアソシエーションを保守することは、ネットワーク内の種々のシステムについてのアカウントを持つのはどのユーザーか、ということを把握しておくために必要とされる管理タスクを簡素化するためのかぎです。セキュアなシングル・サインオン・ネットワークをインプリメントする場合、現行の ID アソシエーションおよびポリシー・アソシエーションを保持していることは重要です。

アソシエーションに対して、以下の管理用タスクを実行できます。

アソシエーションの作成

アソシエーションは、 2 つの方法のうちの 1 つで作成できます。

- ID アソシエーションの作成を行って、 1 人の人が使用する 2 つのユーザー ID 間の関係を間接的に定義できます。 ID アソシエーションは、 ユーザー・レジストリー内の EIM ID とユーザー ID の間の関係を記述します。 ID アソシエーションにより、EIM ID と、EIM ID が表すユーザーに関連したさまざまなユーザー ID の各々との間の、 1 対 1 のマッピングを作成できます。
- ポリシー・アソシエーションの作成を行って、 1 つ以上のレジストリー内の複数のユーザー ID、および別のレジストリー内の個々のターゲット・ユーザー ID 間の関係を記述できます。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。ポリシー・アソシエーションにより、異なるユーザー・レジストリー内の関連したユーザー ID 間の大量のマッピングをすばやく作成できます。

ID アソシエーションを作成するか、ポリシー・アソシエーションを作成するか、またはその両方を混用するかは、 EIM インプリメンテーションの要件によって異なります。

関連概念

67 ページの『ID マッピング 計画の作成』

ID アソシエーションの作成:

ID アソシエーションは、 EIM (エンタープライズ識別マッピング) ID が参照する人またはエンティティーの、企業内における EIM ID とユーザー ID の間の関係を定義します。ターゲット、ソース、管理という 3 つのタイプの ID アソシエーションを作成できます。また、アソシエーションおよびそれらが ID をマップする方法に関連した、生じる可能性のある問題を防ぐため、アソシエーションの定義を開始する前に、企業の全体的な ID マッピング計画の作成を行う必要があります。

ID アソシエーションを作成するには、処理する EIM ドメインに接続し、また作成するアソシエーションのタイプによって必要とされる 43 ページの『EIM アクセス制御』を持っている必要があります。

ソース・アソシエーションまたは管理アソシエーションを作成するには、以下のうちの 1 つの EIM アクセス制御を持っている必要があります。

- ID 管理者
- EIM 管理者

ターゲット・アソシエーションを作成するには、以下のうちの 1 つの EIM アクセス制御を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (ターゲット・ユーザー ID を含むユーザー・レジストリーを参照するレジストリー定義) の管理者
- EIM 管理者

ID アソシエーションを作成するには、以下のステップを完了してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックして、ドメインの EIM ID のリストを表示する。

注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 114 ページの『EIM ID ビューのカスタマイズ』を行えます。

5. アソシエーションを作成する EIM ID を右マウス・ボタン・クリックして、「**プロパティー...**」を選択する。
6. 「**関連**」ページを選択して、「**追加...**」をクリックする。
7. 「**関連の追加**」ダイアログで、アソシエーションを定義するための、以下のような情報を提供する。
   - EIM ID と関連付けたいユーザー ID を含むレジストリーの名前。既存のレジストリー定義の正確な名前を指定するか、または参照から 1 つを選択する。
   - EIM ID と関連付けたいユーザー ID の名前。
   - アソシエーションのタイプ。以下の 3 つのタイプのうち 1 つのアソシエーションを作成できます。
     - 管理
     - ソース
     - ターゲット
8. 必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断する。
9. オプション。ターゲット・アソシエーションに対して、「**拡張...**」をクリックして、「**関連の追加 - 拡張**」ダイアログを表示する。ターゲット・ユーザー ID のルックアップ情報を指定して、「**OK**」をクリックし、「**関連の追加**」ダイアログに戻る。
10. 必要な情報を供給した後、「**OK**」をクリックしてアソシエーションを作成する。

ポリシー・アソシエーションの作成: ポリシー・アソシエーションは、1 つ以上のレジストリー内の複数のユーザー ID と、別のレジストリー内の個々のターゲット・ユーザー ID 間の関係を定義する手段を提供します。ポリシー・アソシエーションは、EIM (エンタープライズ識別マッピング) マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。ポリシー・アソシエーションはさまざまな重複した仕方で使用できるので、ポリシー・アソシエーションを作成および使用する前に、 マッピング・ポリシー・サポートをよく理解しておく必要があります。また、アソシエーションおよびそれらが ID をマップする方法に関連した、生じる可能性のある問題を防ぐため、アソシエーションの定義を開始する前に、企業の全体的な ID マッピング計画の作成を行う必要があります。

ID アソシエーションを作成するか、ポリシー・アソシエーションを作成するか、またはその両方を混用するかは、 EIM インプリメンテーションの要件によって異なります。

ポリシー・アソシエーションの作成方法は、ポリシー・アソシエーションのタイプによって異なります。ポリシー・アソシエーションの作成方法についてさらに確認するには、以下を参照してください。

関連概念

103 ページの『EIM (エンタープライズ識別マッピング) レジストリー定義の管理』
ここでは、企業内の、EIM (エンタープライズ識別マッピング) に参加するユーザー・レジストリー用の EIM レジストリー定義を作成および管理する方法を説明します。

デフォルトのドメイン・ポリシー・アソシエーションの作成:

デフォルトのドメイン・ポリシー・アソシエーションを作成する場合、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- EIM 管理者
- レジストリー管理者

注: ポリシー・アソシエーションは、複数のユーザー ID と、ターゲット・ユーザー・レジストリー内の単一のユーザー ID との間の関連を記述します。ポリシー・アソシエーションを使用して、複数のユーザー ID のソース・セットと、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID との間の関連を記述できます。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。

ポリシー・アソシエーションはさまざまな重複した仕方で使用できるので、ポリシー・アソシエーションを作成および使用する前に、 マッピング・ポリシー・サポートをよく理解しておく必要があります。また、アソシエーションおよびそれらが ID をマップする方法に関連した、生じる可能性のある問題を防ぐため、アソシエーションの定義を開始する前に、企業の全体的な ID マッピング計画の作成を行う必要があります。

デフォルトのドメイン・ポリシー・アソシエーションでは、ドメイン内のすべてのユーザーが、ポリシー・アソシエーションのソースであり、単一ターゲット・レジストリーおよびターゲット・ユーザーにマップされます。ドメイン内のそれぞれのレジストリーごとに、デフォルトのドメイン・ポリシー・アソシエーションを定義できます。 2 つ以上のドメイン・ポリシー・アソシエーションが同じターゲット・レジストリーを参照する場合には、これらのポリシー・アソシエーションのそれぞれについて、固有のルックアップ情報を定義して、マッピング・ルックアップ操作が確実にそれらを区別できるようにすることができます。そうしなければ、マッピング・ルックアップ操作は、複数のターゲット・ユーザー ID を戻す可能性があります。結果がそのようにあいまいであれば、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。

デフォルトのドメイン・ポリシー・アソシエーションを作成するには、以下のステップを完了します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**一般**」ページの「**ドメインのポリシー関連を使用してマッピング・ルックアップを使用可能にする**」を選択する。
4. 「**ドメイン**」ページを選択して、「**追加...**」をクリックする。
5. 「**デフォルト・ドメイン・ポリシー関連の追加**」ダイアログで、以下の必要な情報を指定する。
   - ポリシー・アソシエーションの「**ターゲット・レジストリー**」のレジストリー定義名
   - ポリシー・アソシエーションの「**ターゲット・ユーザー**」のユーザー ID
6. 必要であれば、「**ヘルプ**」をクリックして、このダイアログおよび後続のダイアログを完了する方法の詳細を参照する。
7. オプション。「**拡張...**」をクリックして、「**関連の追加 - 拡張**」ダイアログを表示する。ポリシー・アソシエーションの「**ルックアップ情報**」を指定して、「**OK**」をクリックし、「**デフォルト・ドメイン・ポリシー関連の追加**」ダイアログに戻る。

   注: 2 つ以上のデフォルトのドメイン・ポリシー・アソシエーションが同じターゲット・レジストリーを参照する場合には、これらのポリシー・アソシエーションのそれぞれのターゲット・ユーザー

ID ごとに、固有のルックアップ情報を定義しなければなりません。この状況にあるそれぞれのターゲット・ユーザー ID ごとにルックアップ情報を定義することにより、マッピング・ルックアップ操作がそれらを確実に区別できるようにします。そうしなければ、マッピング・ルックアップ操作は、複数のターゲット・ユーザー ID を戻す可能性があります。結果がそのようにあいまいであれば、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。

8. 「**OK**」をクリックして、新規ポリシー・アソシエーションを作成し、「**ドメイン**」ページに戻ります。これで、新規ポリシー・アソシエーションが、「**デフォルト・ポリシー関連**」テーブルに表示されます。
9. 新規ポリシー・アソシエーションがターゲット・レジストリーに対して使用可能であることを確認する。
10. 「**OK**」をクリックして変更を保管し、「**マッピング・ポリシー**」ダイアログを終了する。

注: マッピング・ポリシー・サポートおよびターゲット・ユーザー・レジストリーに対するポリシー・アソシエーションの使用が正しく使用可能となっていることの確認を行う。使用可能となっていない場合には、ポリシー・アソシエーションを有効にできません。

デフォルトのレジストリー・ポリシー・アソシエーションの作成:

デフォルトのレジストリー・ポリシー・アソシエーションを作成する場合、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- EIM 管理者
- レジストリー管理者

注: ポリシー・アソシエーションは、複数のユーザー ID と、ターゲット・ユーザー・レジストリー内の単一のユーザー ID との間の関連を記述します。ポリシー・アソシエーションを使用して、複数のユーザー ID のソース・セットと、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID との間の関連を記述できます。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。

ポリシー・アソシエーションはさまざまな重複した仕方で使用できるので、ポリシー・アソシエーションを作成および使用する前に、 マッピング・ポリシー・サポートをよく理解しておく必要があります。また、アソシエーションおよびそれらが ID をマップする方法に関連した、生じる可能性のある問題を防ぐため、アソシエーションの定義を開始する前に、企業の全体的な ID マッピング計画の作成を行う必要があります。

デフォルトのレジストリー・ポリシー・アソシエーションでは、単一レジストリー内のすべてのユーザーが、ポリシー・アソシエーションのソースであり、単一ターゲット・レジストリーおよびターゲット・ユーザーにマップされます。ターゲット・レジストリーのデフォルトのレジストリー・ポリシー・アソシエーションを使用可能にすると、ポリシー・アソシエーションは、これらのソース・ユーザー ID がすべて、単一の指定されたターゲット・レジストリーおよびターゲット・ユーザーに確実にマップされるようにします。

デフォルトのレジストリー・ポリシー・アソシエーションを作成するには、以下のステップを完了します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。

- 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
- 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。

3. 「**一般**」ページの「**ドメインのポリシー関連を使用してマッピング・ルックアップを使用可能にする**」を選択する。
4. 「**一般**」ページの「**ドメインのポリシー関連を使用してマッピング・ルックアップを使用可能にする**」を選択する。
5. 「**デフォルト・レジストリー・ポリシー関連の追加**」ダイアログで、以下の必要な情報を指定する。
   - ポリシー・アソシエーションの「**ソース・レジストリー**」のレジストリー定義名
   - ポリシー・アソシエーションの「**ターゲット・レジストリー**」のレジストリー定義名
   - ポリシー・アソシエーションの「**ターゲット・ユーザー**」のユーザー ID
6. 必要であれば、「**ヘルプ**」をクリックして、このダイアログおよび後続のダイアログを完了する方法の詳細を参照する。
7. オプション。「**拡張...**」をクリックして、「**関連の追加 - 拡張**」ダイアログを表示する。ポリシー・アソシエーションの「**ルックアップ情報**」を指定して、「**OK**」をクリックし、「**デフォルト・レジストリー・ポリシー関連の追加**」ダイアログに戻る。 同じソース・レジストリーを持つ 2 つ以上のポリシー・アソシエーションが、同じターゲット・レジストリーを参照する場合には、これらのポリシー・アソシエーションのそれぞれのターゲット・ユーザー ID ごとに、固有のルックアップ情報を定義しなければなりません。この状況にあるそれぞれのターゲット・ユーザー ID ごとにルックアップ情報を定義することにより、マッピング・ルックアップ操作がそれらを確実に区別できるようにします。そうしなければ、マッピング・ルックアップ操作は、複数のターゲット・ユーザー ID を戻す可能性があります。結果がそのようにあいまいであれば、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。
8. 「**OK**」をクリックして、新規ポリシー・アソシエーションを作成し、「**レジストリー**」ページに戻ります。これで、新規デフォルト・レジストリー・ポリシー・アソシエーションが、「**デフォルト・ポリシー関連**」に表示されます。
9. 新規ポリシー・アソシエーションがターゲット・レジストリーに対して使用可能であることを確認する。
10. 「**OK**」をクリックして変更を保管し、「**マッピング・ポリシー**」ダイアログを終了する。

注: マッピング・ポリシー・サポートおよびターゲット・ユーザー・レジストリーに対するポリシー・アソシエーションの使用が正しく使用可能となっていることの確認を行う。使用可能となっていない場合には、ポリシー・アソシエーションを有効にできません。

証明書フィルター・ポリシー・アソシエーションの作成:

証明書フィルター・ポリシー・アソシエーションを作成する場合、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- EIM 管理者
- レジストリー管理者

注: ポリシー・アソシエーションは、複数のユーザー ID のソース・セットと、指定されたターゲット・ユーザー・レジストリー内の単一のターゲット・ユーザー ID との間の関連を記述します。ポリシー・アソシエーションは、EIM マッピング・ポリシー・サポートを使用して、 EIM ID とは無関係に、ユーザー ID 間の多対 1 マッピングを作成します。

ポリシー・アソシエーションはさまざまな重複した仕方で使用できるので、ポリシー・アソシエーションを作成および使用する前に、 マッピング・ポリシー・サポートをよく理解しておく必要があります。また、アソシエーションおよびそれらが ID をマップする方法に関連した、生じる可能性のある問題を防ぐため、アソシエーションの定義を開始する前に、企業の全体的な ID マッピング計画の作成を行う必要があります。

証明書フィルター・ポリシー・アソシエーションでは、単一 X.509 レジストリー内の証明書のセットを、ポリシー・アソシエーションのソースとして指定します。これらの証明書は、指定した単一ターゲット・レジストリーおよびターゲット・ユーザーにマップされます。単一レジストリー内のすべてのユーザーがポリシー・アソシエーションのソースである、デフォルトのレジストリー・ポリシー・アソシエーションとは異なり、証明書フィルター・ポリシー・アソシエーションの有効範囲は、より柔軟です。レジストリー内の証明書のサブセットを、ソースとして指定できます。ポリシー・アソシエーションに対して指定する証明書フィルターが、その有効範囲を決定します。

注: X.509 ユーザー・レジストリー内のすべての証明書を、単一のターゲット・ユーザー ID にマップしたい場合には、デフォルトのレジストリー・ポリシー・アソシエーションを作成して使用してください。

証明書フィルターは、証明書フィルター・ポリシー・アソシエーションが、ユーザー ID の 1 つのソース・セットを (この場合はディジタル証明書)、特定のターゲット・ユーザー ID にマップする仕方を制御します。したがって、証明書フィルター・ポリシー・アソシエーションを作成する前に、使用する証明書フィルターが存在していなければなりません。

証明書フィルター・ポリシー・アソシエーションを作成する前に、まず最初に、ポリシー・アソシエーションの基礎として使用する、 証明書フィルターの作成を行う必要があります。

証明書フィルター・ポリシー・アソシエーションを作成するには、以下のステップを完了します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**一般**」ページの「**ドメインのポリシー関連を使用してマッピング・ルックアップを使用可能にする**」を選択する。
4. 「**証明書フィルター**」ページを選択して、「**追加...**」をクリックし、「**証明書フィルター・ポリシー関連の追加**」ダイアログを表示する。
5. 必要であれば、「**ヘルプ**」をクリックして、このダイアログおよび後続のダイアログを完了する方法の詳細を参照する。
6. 以下の必要な情報を指定して、ポリシー・アソシエーションを定義する。
   a. ポリシー・アソシエーションの「**ソース X.509 レジストリー**」として使用する、 X.509 ユーザー・レジストリーのレジストリー定義名を入力する。または、「**参照...**」をクリックして、ドメインのレジストリー定義のリストから 1 つを選択する。

b. 「**選択**」をクリックして、「**証明書フィルターの選択**」ダイアログを表示し、新規証明書フィルター・ポリシー・アソシエーションの基礎として使用する、既存の証明書フィルターを選択する。

   注: 既存の証明書フィルターを使用**しなければなりません**。使用したい証明書フィルターがリストにない場合には、「**追加...**」をクリックして、 新規証明書フィルターの作成を行ってください。

c. 「**ターゲット・レジストリー**」のレジストリー定義名を指定するか、または「**参照...**」をクリックして、ドメインの既存レジストリー定義のリストから 1 つを選択する。

d. 「**ソース X.509 レジストリー**」内の、証明書フィルターに一致するすべての証明書のマップ先となる、「**ターゲット・ユーザー**」の名前を指定する。または、「**参照...**」をクリックして、ドメインに対して既知のユーザーのリストから 1 つを選択する。

e. オプション。「**拡張...**」をクリックして、「**関連の追加 - 拡張**」ダイアログを表示する。ターゲット・ユーザー ID の「**ルックアップ情報**」を指定して、「**OK**」をクリックし、「**証明書フィルター・ポリシー関連の追加**」ダイアログに戻る。

   注: 同じソース X.509 レジストリーおよび同じ証明書フィルター基準を持つ 2 つ以上のポリシー・アソシエーションが、同じターゲット・レジストリーを参照する場合には、これらのポリシー・アソシエーションのそれぞれのターゲット・ユーザー ID に対して、固有のルックアップ情報を定義しなければなりません。この状況にあるそれぞれのターゲット・ユーザー ID ごとにルックアップ情報を定義することにより、マッピング・ルックアップ操作がそれらを確実に区別できるようにします。そうしなければ、マッピング・ルックアップ操作は、複数のターゲット・ユーザー ID を戻す可能性があります。結果がそのようにあいまいであれば、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。

7. 「**OK**」をクリックして、証明書フィルター・ポリシー・アソシエーションを作成し、「**証明書フィルター**」ページに戻ります。新規ポリシー・アソシエーションがリスト内に表示されます。
8. 新規ポリシー・アソシエーションがターゲット・レジストリーに対して使用可能であることを確認する。
9. 「**OK**」をクリックして変更を保管し、「**マッピング・ポリシー**」ダイアログを終了する。

注: マッピング・ポリシー・サポートおよびターゲット・ユーザー・レジストリーに対するポリシー・アソシエーションの使用が正しく使用可能となっていることの確認を行う。使用可能となっていない場合には、ポリシー・アソシエーションを有効にできません。

証明書フィルターの作成:

証明書フィルターは、X.509 ソース・ユーザー・レジストリー内のユーザー証明書のグループに対する, 類似した識別名証明書属性のセットを定義します。証明書フィルターは、証明書フィルター・ポリシー・アソシエーションの基礎として使用できます。ポリシー・アソシエーション内の証明書フィルターは、指定されたソース X.509 レジストリー内のどの証明書を、指定されたターゲット・ユーザーにマップするかを判別します。フィルターの基準を満たすサブジェクト DN および発行者 DN 情報を持つ証明書は、 EIM (エンタープライズ識別マッピング) マッピング・ルックアップ操作中に、指定されたターゲット・ユーザーにマップされます。

証明書フィルターを作成する場合、処理する EIM ドメインに接続し、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- EIM 管理者
- レジストリー管理者
- 選択されたレジストリー (証明書フィルターを作成したい X.509 ユーザー・レジストリーを参照するレジストリー定義)の管理者

ディジタル証明書からの特定の識別名 (DN) 情報に基づいた証明書フィルターを作成します。指定する DN 情報として、サブジェクト識別名 (証明書の所有者を指定する)、 または発行者識別名 (証明書の発行者を指定する) のいずれかを指定できます。 証明書フィルターには DN の全情報または部分情報のいずれかを指定できます。

証明書フィルターを証明書フィルター・ポリシー・アソシエーションに追加すると、証明書フィルターは X.509 レジストリー内のどの証明書が、ポリシー・アソシエーションによって指定されたターゲット・ユーザー ID にマップされるかを判別します。ディジタル証明書が EIM マッピング・ルックアップ操作におけるソース・ユーザー ID であり (要求側アプリケーションが `eimFormatUserIdentity()` EIM API を使用してユーザー識別名をフォーマットした後)、証明書フィルター・ポリシー・アソシエーションが適用される場合には、 EIM は証明書内の DN 情報を、フィルター内で指定された DN 情報または DN の部分情報と比較します。 証明書内の DN 情報がフィルターに一致する場合には、 EIM は証明書フィルター・ポリシー・アソシエーションが指定したターゲット・ユーザー ID を戻します。

証明書フィルターを作成する際には、以下の 3 つのうちの 1 つの方法で、必要な識別名情報を提供できます。

- 特定の証明書の全 DN または部分 DN を、「**サブジェクト DN**」、「**発行者 DN**」、またはその両方に入力できます。
- 特定の証明書からの情報をクリップボードにコピーして、それを使用して、証明書内の識別名情報に基づいて、証明書フィルター候補のリストを生成できます。その後、証明書フィルターに使用する DN を選択できます。

  注: 必要な識別名情報を生成して証明書フィルターを作成したい場合には、このタスクを実行する前に、証明書の情報をクリップボードにコピーしなければなりません。また、証明書は base64 エンコード形式でなければなりません。適正な形式の証明書を取得する方法について詳しくは、証明書フィルターを参照してください。
- EIM ID との既存のソース・アソシエーションがあるディジタル証明書からの識別名情報に基づいて、証明書フィルター候補のリストを生成できます。その後、証明書フィルターに使用する DN を選択できます。

証明書フィルター・ポリシー・アソシエーションの基礎として使用する証明書フィルターを作成するには、以下のステップを完了します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**証明書フィルター**」ページを選択して、「**証明書フィルター...**」をクリックし、「**証明書フィルター**」ダイアログを表示する。

   注: ポリシー・アソシエーションを選択せずに「**証明書フィルター...**」をクリックすると、「**EIM レジストリーの参照**」ダイアログが表示されます。このダイアログにより、ドメイン内の X.509 レジストリー定義のリストから、証明書フィルターを表示したい X.509 レジストリーを選択できます。リストの内容は、ユーザーが持っている EIM アクセス制御のタイプによって異なります。
4. 「**追加...**」をクリックして「**証明書フィルターの追加**」ダイアログを表示する。

5. 「**証明書フィルターの追加**」ダイアログで、単一証明書フィルターを追加するか、それとも特定のディジタル証明書を基に証明書フィルターを生成するかを選択しなければなりません。必要であれば、「**ヘルプ**」をクリックして、このダイアログおよび後続のダイアログを完了する方法の詳細を参照してください。
   a. 「**単一証明書フィルターの追加**」を選択した場合、特定の「**サブジェクト DN**」の全体または一部、または「**発行者 DN**」の全体または一部、またはその両方を入力できます。「**OK**」をクリックして、証明書フィルターを作成し、「**証明書フィルター**」ダイアログに戻ります。これで、フィルターがリストに表示されます。
   b. 「**ディジタル証明書から証明書フィルターを生成 (Generate certificate filter from a digital certificate)**」を選択した場合には、「**OK**」をクリックして、「**証明書フィルターの生成**」ダイアログを表示する。
      1) すでにクリップボードにコピーしている証明書情報の base64 エンコード・バージョンを、「**証明書情報**」フィールドに貼り付ける。
      2) 「**OK**」をクリックして、証明書の「**サブジェクト DN**」および「**発行者 DN**」を基にして、可能性のある証明書フィルターのリストを生成する。
      3) 「**証明書フィルターの参照**」ダイアログから、これらの証明書フィルターの 1 つ以上を選択する。「**OK**」をクリックして、「**証明書フィルターの選択 (Select Certificate Filters)**」ダイアログに戻る。そこには、選択された証明書フィルターが現在表示されている。
   c. 「**X.509 ユーザーのソース関連から証明書フィルターを生成 (Generate certificate filter from a source association for an X.509 user)**」を選択した場合には、「**OK**」をクリックして、「**証明書フィルターの生成**」ダイアログを表示する。このダイアログは、ドメイン内の EIM ID とのソース・アソシエーションを持つ X.509 ユーザー ID のリストを表示します。
      1) 1 つ以上の証明書フィルター候補を生成するために使用したいディジタル証明書を持つ X.509 ユーザー ID を選択し、「**OK**」をクリックする。
      2) 「**OK**」をクリックして、証明書の「**サブジェクト DN**」および「**発行者 DN**」を基にして、可能性のある証明書フィルターのリストを生成する。
      3) 「**証明書フィルターの参照**」ダイアログから、これら可能性のある証明書フィルターの 1 つ以上を選択する。「**OK**」をクリックして、「**証明書フィルターの選択 (Select Certificate Filters)**」ダイアログに戻る。そこには、選択された証明書フィルターが現在表示されている。

これで、 証明書フィルター・ポリシー・アソシエーションの作成の前提として新規証明書フィルターが使用できるようになりました。

ターゲット・ユーザー ID にルックアップ情報を追加する

ルックアップ情報は、オプションの、アソシエーション内で定義されたターゲット・ユーザー ID の固有の識別データです。このアソシエーションは、ID ターゲット・アソシエーションまたはポリシー・アソシエーションのいずれかであることが可能です。ルックアップ情報が必要なのは、マッピング・ルックアップ操作が、複数のターゲット・ユーザー ID を戻す可能性がある場合に限られます。そのような場合には、i5/OS アプリケーションおよびプロダクトを含め、これらのあいまいな結果を処理するようには設計されていない EIM (エンタープライズ識別マッピング) 対応アプリケーションで問題が生じることがあります。

必要な場合には、それぞれのターゲット・ユーザー ID ごとに固有のルックアップ情報を追加して、それぞれのターゲット・ユーザー ID をさらに記述する、より詳細な ID 情報を提供できます。 ターゲット・ユーザー ID のルックアップ情報を定義する場合には、このルックアップ情報をマッピング・ルックアッ

プ操作に提供して、操作が固有のターゲット・ユーザー ID を確実に戻すことができるようにしなければなりません。そうしなければ、 EIM を信頼するアプリケーションは、使用すべき正確なターゲット ID を判別できないかもしれません。

注: EIM ルックアップ操作が複数のターゲット・ユーザー ID を戻すことができるようにしたくない場合には、ルックアップ情報を使用して状況を解決する代わりに、EIM アソシエーション構成を訂正する必要があります。詳しくは、 137 ページの『EIM マッピング問題のトラブルシューティング』を参照してください。

ターゲット・ユーザー ID をさらに定義するためにルックアップ情報を追加する方法は、ターゲット・ユーザー ID が、 ID アソシエーションまたはターゲット・アソシエーションのどちらで定義されるのかによって異なります。ルックアップ情報を追加するために使用する方法にかかわらず、指定する情報は、そのユーザー ID が見つかる ID アソシエーションまたはポリシー・アソシエーションではなく、ターゲット・ユーザー ID に結び付けられます。

ID アソシエーション内のターゲット・ユーザー ID にルックアップ情報を追加する:

ルックアップ情報を ID アソシエーション内のターゲット・ユーザー ID に追加する場合、処理する EIM ドメインに接続して、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (ターゲット・ユーザー ID を含むユーザー・レジストリーを参照するレジストリー定義) の管理者
- EIM 管理者

ID アソシエーション内のターゲット・ユーザー ID にルックアップ情報を追加する場合は、以下のステップを実行します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックして、ドメインの EIM ID のリストを表示する。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 ID を表示するために使用する検索値を限定することによって、「**ID**」フォルダー・ビューをカスタマイズできます。「**ID**」を右マウス・ボタン・クリックし、「**このビューのカスタマイズ (Customize this view...)**」>「**組み込み (Include)**」を選択して、ビューに組み込む EIM ID のリストを生成するために使用する表示基準を指定します。
5. EIM ID を右マウス・ボタン・クリックし、「**プロパティー...**」を選択する。
6. 「**関連**」ページを選択し、ルックアップ情報を追加したいターゲット・アソシエーションを選択して、「**詳細...**」をクリックする。必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断してください。

7. 「**関連 - 詳細**」ダイアログで、このアソシエーションのターゲット・ユーザー ID をさらに識別するために使用する「**ルックアップ情報**」を指定して、「**追加**」をクリックする。
8. アソシエーションに追加するそれぞれのルックアップ情報項目ごとに、このステップを繰り返す。
9. 「**OK**」をクリックして、変更を保管し、「**関連 - 詳細**」ダイアログに戻る。
10. 「**OK**」をクリックして終了する。

ポリシー・アソシエーション内のターゲット・ユーザー ID にルックアップ情報を追加する:

ルックアップ情報をポリシー・アソシエーション内のターゲット・ユーザー ID に追加する場合、処理する EIM ドメインに接続して、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (ターゲット・ユーザー ID を含むユーザー・レジストリーを参照するレジストリー定義)の管理者
- EIM 管理者

ポリシー・アソシエーション内のターゲット・ユーザー ID にルックアップ情報を追加する場合は、以下のステップを実行します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**マッピング・ポリシー**」ダイアログで、ドメインのポリシー・アソシエーションを表示するページを使用する。
4. ルックアップ情報を追加するターゲット・ユーザー ID を含むターゲット・レジストリーのポリシー・アソシエーションを検出して選択する。
5. 「**詳細...**」をクリックして、選択したタイプのポリシー・アソシエーションに適切な「**ポリシー関連 - 詳細**」ダイアログを表示する。必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断してください。
6. このポリシー・アソシエーションのターゲット・ユーザー ID をさらに識別するために使用する「**ルックアップ情報**」を指定して、「**追加**」をクリックする。アソシエーションに追加するそれぞれのルックアップ情報項目ごとに、このステップを繰り返す。
7. 「**OK**」をクリックして、変更を保管し、元の「**ポリシー関連 - 詳細**」ダイアログに戻る。
8. 「**OK**」をクリックして終了する。

ターゲット・ユーザー ID のルックアップ情報を除去する

ルックアップ情報は、オプションの、アソシエーション内で定義されたターゲット・ユーザー ID の固有の識別データです。このアソシエーションは、ID ターゲット・アソシエーションまたはポリシー・アソシエーションのいずれかであることが可能です。ルックアップ情報が必要なのは、マッピング・ルックアップ操作が、複数のターゲット・ユーザー ID を戻す可能性がある場合に限られます。そのような場合には、i5/OS アプリケーションおよびプロダクトを含め、これらのあいまいな結果を処理するようには設計されていない EIM (エンタープライズ識別マッピング) 対応アプリケーションで問題が生じることがあります。

このルックアップ情報をマッピング・ルックアップ操作に提供して、操作が固有のターゲット・ユーザー ID を確実に戻すことができるようにしなければなりません。ただし、以前に定義されたルックアップ情報が必要でなくなった場合には、そのルックアップ情報を除去して、それがルックアップ操作のために供給される必要がないようにすることができます。

ターゲット・ユーザー ID からルックアップ情報を除去する方法は、ターゲット・ユーザー ID が、 ID アソシエーションまたはターゲット・アソシエーションのどちらで定義されるのかによって異なります。ルックアップ情報は、そのユーザー ID が見つかる ID アソシエーションまたはポリシー・アソシエーションではなく、ターゲット・ユーザー ID に結び付いています。したがって、そのターゲット・ユーザー ID を定義する最後の ID アソシエーションまたはポリシー・アソシエーションが削除されると、ユーザー ID およびルックアップ情報の両方が EIM ドメインから削除されます。

ID アソシエーション内のターゲット・ユーザー ID のルックアップ情報を除去する:

ID アソシエーション内のターゲット・ユーザー ID のルックアップ情報を除去する場合、処理する EIM ドメインに接続して、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (ターゲット・ユーザー ID を含むユーザー・レジストリーを参照するレジストリー定義) の管理者
- EIM 管理者

ID アソシエーション内のターゲット・ユーザー ID のルックアップ情報を除去する場合は、以下のステップを実行します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックして、ドメインの EIM ID のリストを表示する。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 ID を表示するために使用する検索値を限定することによって、「**ID**」フォルダー・ビューをカスタマイズできます。「**ID**」を右マウス・ボタン・クリックし、「**このビューのカスタマイズ (Customize this view...)**」>「**組み込み (Include)**」を選択して、ビューに組み込む EIM ID のリストを生成するために使用する表示基準を指定します。
5. EIM ID を右マウス・ボタン・クリックし、「**プロパティー...**」を選択する。
6. 「**関連**」ページを選択し、ルックアップ情報を除去したいユーザー ID のターゲット・アソシエーションを選択して、「**詳細...**」をクリックする。
7. 「**関連 - 詳細**」ダイアログで、ターゲット・ユーザー ID から除去するルックアップ情報を選択して、「**除去**」をクリックする。

   注: 「**除去**」をクリックすると、確認プロンプトは出されません。
8. 「**OK**」をクリックして、変更を保管し、「**関連 - 詳細**」ダイアログに戻る。

9. 「**OK**」をクリックして終了する。

ポリシー・アソシエーション内のターゲット・ユーザー *ID* のルックアップ情報を除去する:

ポリシー・アソシエーション内のターゲット・ユーザー ID のルックアップ情報を除去する場合、処理する EIM ドメインに接続して、 以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (ターゲット・ユーザー ID を含むユーザー・レジストリーを参照するレジストリー定義)の管理者
- EIM 管理者

ポリシー・アソシエーション内のターゲット・ユーザー ID のルックアップ情報を除去する場合は、以下のステップを実行します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 「**マッピング・ポリシー**」ダイアログで、ドメインのポリシー・アソシエーションを表示するページを使用する。
4. ルックアップ情報を除去するターゲット・ユーザー ID を含むターゲット・レジストリーのポリシー・アソシエーションを検出し選択する。
5. 「**詳細...**」をクリックして、選択したタイプのポリシー・アソシエーションに適切な「**ポリシー関連 - 詳細**」ダイアログを表示する。
6. ターゲット・ユーザー ID から除去するルックアップ情報を選択して、「**除去**」をクリックする。

   注: 「**除去**」をクリックすると、確認プロンプトは出されません。
7. 「**OK**」をクリックして、変更を保管し、元の「**ポリシー関連 - 詳細**」ダイアログに戻る。
8. 「**OK**」をクリックして終了する。

EIM ID のすべての ID アソシエーションの表示

EIM (エンタープライズ識別マッピング) ID のすべてのアソシエーションを表示するには、処理する EIM ドメインに接続し、このタスクを実行するために 43 ページの『EIM アクセス制御』のいくつかを持っていなければなりません。選択されたレジストリー・アクセス制御の、管理者以外のアクセス制御レベルを持つ、すべてのアソシエーションを表示できます。このアクセス制御レベルにより、EIM マッピング・ルックアップ操作アクセス制御も持っているのでない限り、ユーザーが明示的な権限を持つレジストリーに対するアソシエーションだけをリストして表示できます。

EIM ID と、 EIM ID にアソシエーションが定義されているユーザー ID (複数も可) との間のすべてのアソシエーションを表示するには、以下のステップを完了します。

ID のアソシエーションを表示するには、以下のようにします。

.

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。

2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックして、ドメインの EIM ID のリストを表示する。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 ID を表示するために使用する検索値を限定することによって、「**ID**」フォルダー・ビューをカスタマイズできます。「**ID**」を右マウス・ボタン・クリックし、「**このビューのカスタマイズ (Customize this view...)**」>「**組み込み (Include)**」を選択して、ビューに組み込む EIM ID のリストを生成するために使用する表示基準を指定します。
5. EIM ID を選択し、その EIM ID の上で右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
6. 「**関連**」ページを選択して、選択された EIM ID に関連したユーザー ID のリストを表示する。
7. 「**OK**」をクリックして終了する。
8.

ドメインのすべてのポリシー・アソシエーションの表示

ドメインに定義されたすべてのポリシー・アソシエーションを表示するには、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、このタスクを実行するために 43 ページの『EIM アクセス制御』のいくつかを持っていなければなりません。選択されたレジストリー・アクセス制御の、管理者以外のアクセス制御レベルを持つ、すべてのポリシー・アソシエーションを表示できます。このアクセス制御レベルにより、ユーザーが明示的な権限を持つレジストリーに対するアソシエーションだけをリストして表示することができます。したがって、EIM マッピング・ルックアップ操作アクセス制御も持っているのでない限り、このアクセス制御では、デフォルトのドメイン・ポリシー・アソシエーションをリストしたり表示したりすることはできません。

ドメインのすべてのポリシー・アソシエーションを表示するには、次のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 以下のように、ドメインに定義されたポリシー・アソシエーションを表示するページを選択する。
   a. ドメインに定義されたデフォルトのドメイン・ポリシー・アソシエーション、およびポリシー・アソシエーションがレジストリー・レベルで使用可能であるかどうかを表示する、「**ドメイン**」ページを選択する。
   b. ドメインに定義されたデフォルトのレジストリー・ポリシー・アソシエーションを表示する、「**レジストリー**」ページを選択する。また、どのソース・レジストリーおよびターゲット・レジストリーに、ポリシー・アソシエーションが影響するかも表示できます。

c. 「**証明書フィルター**」ページを選択して、レジストリー・レベルで定義されて使用可能となっている証明書フィルター・ポリシー・アソシエーションを表示する。

4. 「**OK**」をクリックして終了する。

レジストリー定義のすべてのポリシー・アソシエーションの表示

特定のレジストリーに定義されたすべてのポリシー・アソシエーションを表示するには、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、このタスクを実行するために 43 ページの『EIM アクセス制御』のいくつかを持っていなければなりません。選択されたレジストリー・アクセス制御の、管理者以外のアクセス制御レベルを持つ、すべてのポリシー・アソシエーションを表示できます。このアクセス制御レベルにより、ユーザーが明示的な権限を持つレジストリーに対するアソシエーションだけをリストして表示することができます。したがって、EIM マッピング・ルックアップ操作アクセス制御も持っているのでない限り、このアクセス制御では、デフォルトのドメイン・ポリシー・アソシエーションをリストしたり表示したりすることはできません。

レジストリー定義のすべてのポリシー・アソシエーションを表示するには、次のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 処理するレジストリー定義を右マウス・ボタン・クリックし、「**マッピング・ポリシー...**」を選択する。
4. 以下のように、指定されたレジストリー定義に定義されたポリシー・アソシエーションを表示するページを選択する。
   - レジストリーに定義されたデフォルトのドメイン・ポリシー・アソシエーションを表示する、「**ドメイン**」ページを選択する。
   - レジストリーに定義され使用可能にされたデフォルトのレジストリー・ポリシー・アソシエーションを表示する、「**レジストリー**」ページを選択する。
   - レジストリーに定義され使用可能となっている証明書フィルター・ポリシー・アソシエーションを表示する、「**証明書フィルター**」ページを選択する。
5. 「**OK**」をクリックして終了する。

ID アソシエーションの削除

ID アソシエーションを削除するには、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、また削除するアソシエーションのタイプによって必要とされる 43 ページの『EIM アクセス制御』を持っている必要があります。

ソース・アソシエーションまたは管理アソシエーションを削除するには、以下のうちの 1 つの EIM アクセス制御を持っている必要があります。

- ID 管理者
- EIM 管理者

ターゲット・アソシエーションを削除するには、以下のうちの 1 つの EIM アクセス制御を持っている必要があります。

- レジストリー管理者
- 選択されたレジストリー (ターゲット・ユーザー ID を含むユーザー・レジストリーを参照するレジストリー定義) の管理者
- EIM 管理者

ID アソシエーションを削除するには、以下のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 現在接続している EIM ドメインを展開する。
4. 「**ID**」をクリックして、ドメインの EIM ID のリストを表示する。

   注: 「**ID**」フォルダーを展開しようとすると、 ID のリストが表示されるまでに時間がかかることがあります。ドメイン内に大量の EIM ID がある場合にパフォーマンスを改善するには、 ID を表示するために使用する検索条件を限定することによって、「**ID**」フォルダー・ビューをカスタマイズできます。「**ID**」を右マウス・ボタン・クリックし、「**このビューのカスタマイズ (Customize this view...)**」>「**組み込み (Include)**」を選択して、ビューに組み込む EIM ID のリストを生成するために使用する表示基準を指定します。
5. EIM ID を選択し、その EIM ID の上で右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
6. 「**関連**」ページを選択して、選択された EIM ID に関連したユーザー ID のリストを表示する。
7. 削除するアソシエーションを選択し、「**除去**」をクリックしてアソシエーションを削除する。

   注: 「**除去**」をクリックすると、確認プロンプトは出されません。
8. 「**OK**」をクリックして、変更を保管する。

注: ターゲット・アソシエーションを除去する際、削除されるアソシエーションで使用されるターゲット・レジストリーに対するマッピング・ルックアップ操作は、影響を受けるターゲット・レジストリーに他のアソシエーション (ポリシー・アソシエーションまたは ID アソシエーションのいずれか) が存在しない場合には、失敗する可能性があります。

EIM にユーザー ID を定義できるのは、 アソシエーション (ID アソシエーションまたはポリシー・アソシエーションのいずれか) の作成の一部として、 ユーザー ID を指定するときだけです。 したがって、ユーザー ID の最後のターゲット・アソシエーションを削除すると (個々のターゲット・アソシエーションを除去するか、またはポリシー・アソシエーションを除去することによって)、そのユーザー ID は EIM にもはや定義されていません。したがって、ユーザー ID 名およびそのユーザー ID のルックアップ情報は失われます。

ポリシー・アソシエーションの削除

ポリシー・アソシエーションを削除する場合、処理する EIM (エンタープライズ識別マッピング) ドメインに接続し、以下のうちの 1 つの 43 ページの『EIM アクセス制御』を持っている必要があります。

- レジストリー管理者
- EIM 管理者

ポリシー・アソシエーションを削除するには、以下のステップを完了します。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 削除したいポリシー・アソシエーションのタイプに適切なページを選択する。
4. そのページ上で、適切なポリシー・アソシエーションを選択し、「**除去**」をクリックする。

   注: 「**除去**」をクリックすると、確認プロンプトは出されません。
5. 「**OK**」をクリックして、「**マッピング・ポリシー**」ダイアログを終了し、変更を保管する。

注: ターゲット・ポリシー・アソシエーションを除去する際、削除されたポリシー・アソシエーションの使用に頼るターゲット・レジストリーに対する マッピング・ルックアップ操作は、影響を受けるターゲット・レジストリーに他のアソシエーション (ポリシー・アソシエーションまたは ID アソシエーションのいずれか) が存在しない場合には、失敗する可能性があります。

EIM にユーザー ID を定義できるのは、 アソシエーション (ID アソシエーションまたはポリシー・アソシエーションのいずれか) の作成の一部として、 ユーザー ID を指定するときだけです。 したがって、ユーザー ID の最後のターゲット・アソシエーションを削除すると (個々のターゲット・アソシエーションを除去するか、またはポリシー・アソシエーションを除去することによって)、そのユーザー ID は EIM にもはや定義されていません。したがって、ユーザー ID 名およびそのユーザー ID のルックアップ情報は失われます。

関連概念

103 ページの『EIM (エンタープライズ識別マッピング) レジストリー定義の管理』
ここでは、企業内の、EIM (エンタープライズ識別マッピング) に参加するユーザー・レジストリー用の EIM レジストリー定義を作成および管理する方法を説明します。

EIM ユーザー・アクセス制御の管理

ここでは、LDAP を使用したユーザーのアクセスを管理する方法を説明します。

EIM (エンタープライズ識別マッピング) ユーザーは、事前定義された Lightweight Directory Access Protocol (LDAP) ユーザー・グループ内での、それらのメンバーシップに基づく 43 ページの『EIM アクセス制御』 を所有するユーザーです。あるユーザーの EIM アクセス制御を指定すると、そのユーザーが特定の LDAP ユーザー・グループに追加されます。 各 LDAP グループには、ドメイン内でさまざまな EIM 管理用タスクを実行する権限を持っています。ルックアップ操作を含め、どのタイプの管理用タスクを EIM ユーザーが実行できるかは、 EIM ユーザーが属するアクセス制御グループによって判別されます。

LDAP 管理者アクセス制御または EIM 管理者アクセス制御のいずれかを持つユーザーだけが、他のユーザーを EIM アクセス制御グループに追加したり、他のユーザーのアクセス制御設定を変更したりできます。あるユーザーが EIM アクセス制御グループのメンバーになる前に、そのユーザーは EIM ドメイン・コントローラーとして機能するディレクトリー・サーバー内に項目を持っていなければなりません。また特定のタイプのユーザーだけが、EIM アクセス制御グループのメンバーとなることができます。すなわち、Kerberos プリンシパル、識別名、および i5/OS ユーザー・プロファイルです。

注: Kerberos プリンシパル・ユーザー・タイプを EIM で使用可能にするには、システム上にネットワーク認証サービスが構成されていなければなりません。 EIM において i5/OS ユーザー・プロファイル・タイプを使用可能にするには、ディレクトリー・サーバー上でシステム・オブジェクト接尾部を構成しなければなりません。これにより、ディレクトリー・サーバーは i5/OS ユーザー・プロファイルなどの i5/OS システム・オブジェクトを参照できます。

既存ディレクトリー・サーバーのアクセス制御を管理したり、既存ユーザーを EIM アクセス制御グループに追加したりするには、以下のステップに従ってください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 処理する EIM ドメインを選択する。
   - 処理したい EIM ドメインが「**ドメイン管理**」フォルダーの下にリストされていない場合は、 98 ページの『EIM ドメインをドメイン管理フォルダーに追加する』を参照してください。
   - 処理したい EIM ドメインに現在接続していない場合は、 EIM ドメイン・コントローラーへの接続を参照してください。
3. 接続する EIM ドメインを右マウス・ボタン・クリックし、「**アクセス制御...**」を選択する。
4. 「**EIM アクセス制御の編集**」ダイアログで、「**ユーザー・タイプ**」を選択し、ユーザーの識別情報を提供するために必要なフィールドを表示する。
5. その EIM アクセス制御を管理したいユーザーを識別するのに必要なユーザー情報を入力し、「**OK**」をクリックして、「**EIM アクセス制御の編集**」パネルを表示する。必要であれば、「**ヘルプ**」をクリックして、それぞれのフィールドにどの情報を指定すべきかを判断してください。
6. そのユーザーの 1 つ以上の**アクセス制御**グループを選択し、「**OK**」をクリックして、選択されたグループにユーザーを追加する。各グループがどの権限を持つかについての詳細と、特殊な要件について確認するには、「**ヘルプ**」をクリックしてください。
7. 必要な情報を供給した後、「**OK**」をクリックして、変更を保管する。

EIM 構成プロパティーの管理

ここでは、ドメイン、ユーザー ID、およびレジストリー定義などのさまざまな EIM (エンタープライズ識別マッピング) プロパティーを構成する方法を学習します。

サーバーに対していくつかの異なる EIM 構成プロパティーを管理できます。一般に、これは頻繁に行う必要のない事柄です。しかし、構成プロパティーを変更する必要のある状況があります。たとえば、ご使用のシステムがダウンして、EIM 構成プロパティーを再作成する必要がある場合、 EIM 構成ウィザードを再実行するか、またはここでプロパティーを変更するかのいずれかを行います。別の例として、EIM 構成ウィザードの実行時に、ローカル・レジストリーのレジストリー定義を作成するよう選択しなかった場合があります。その場合にはここで、レジストリー定義情報を更新できます。

変更できるプロパティーには、以下のものがあります。

- サーバーが参加している EIM ドメイン
- EIM ドメイン・コントローラーの接続情報
- オペレーティング・システム機能のために EIM 操作を実行するためにシステムが使用するユーザー ID
- オペレーティング・システム機能のために EIM 操作を実行時にシステムが使用できる実際のユーザー・レジストリーを参照するレジストリー定義名。これらのレジストリー定義名は、EIM 構成ウィザードの実行時に作成できるローカル・ユーザー・レジストリーを参照します。

  注: レジストリーがすでに EIM ドメインに定義されていたか、または後でそれらをドメインに定義することを選択したために、 EIM 構成ウィザードの実行時にローカル・レジストリー定義名を作成しな

いことを選択した場合には、ここでこれらのレジストリー定義名を持つシステム構成プロパティーを更新する必要があります。オペレーティング・システム機能のために EIM 操作を実行するために、システムはこのレジストリー定義情報を必要とします。

EIM 構成プロパティーを変更するには、以下の特殊権限を持っていなければなりません。

- セキュリティー管理者 (*SECADM)
- すべてのオブジェクト (*ALLOBJ)

ご使用の iSeries サーバーの EIM 構成プロパティーを変更するには、以下のようにします。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」を展開する。
2. 「**構成**」を右マウス・ボタン・クリックして、「**プロパティー**」を選択する。
3. EIM 構成情報に対して変更を行う。
4. 「**ヘルプ**」をクリックして、ダイアログ内のそれぞれのフィールドにどの情報を指定すべきかを判断する。
5. 「**構成の確認**」をクリックして、指定されたすべての情報で、システムが EIM ドメイン・コントローラーへの接続を正常に確立できることを確認する。
6. 「**OK**」をクリックして、変更を保管する。

注: EIM 構成ウィザードを使用してドメインを作成または結合しなかった場合に、構成プロパティーを手動で指定して EIM 構成を作成しようとしないでください。ウィザードは、これらのプロパティーを構成する以上のことを行うので、ウィザードを使用して基本 EIM 構成を作成することによって、生じる可能性のある問題を回避できます。

EIM (エンタープライズ識別マッピング) のトラブルシューティング

ここでは、EIM を構成および使用する際に直面する共通問題およびエラー、 さらにはそれらに対して考えられる解決策について学習します。

EIM (エンタープライズ識別マッピング) は、複数のテクノロジーと多数のアプリケーションと機能から構成されています。したがって、多くの領域で問題が発生する可能性があります。以下の情報は、EIM の使用時に直面する可能性のあるいくつかの共通問題およびエラー、およびこれらのエラーおよび問題を訂正する方法についての提案を記述します。

関連情報

シングル・サインオン構成のトラブルシューティング

ドメイン・コントローラー接続問題のトラブルシューティング

ドメイン・コントローラーに接続しようとする際に生じる問題の原因となる要素は多数あります。以下の表を使用して、生じる可能性のあるドメイン・コントローラーの接続問題の解決方法を判断してください。

表 27. 共通 EIM ドメイン・コントローラー接続問題および解決策

起こりうる問題	考えられる解決策
iSeries ナビゲーターを使用して EIM を管理するときに、ドメイン・コントローラーに接続できない。	間違ったドメイン・コントローラー接続情報が、管理するドメインに指定されている可能性があります。以下のようにして、ドメイン接続情報を検査してください。 • 「**ネットワーク**」-->「**エンタープライズ識別マッピング**」-->「**ネットワーク**」->「**ドメイン管理**」を展開する。管理するドメインを右マウス・ボタン・クリックし、「**プロパティー**」を選択する。 • 「**ドメイン・コントローラー**」の名前が正確であり、「**親 DN**」が指定されていれば、それが正確であることを確認する。 • ドメイン・コントローラーの「**接続**」情報が正確であることを確認する。「**ポート**」番号が正確であることを確認する。「**セキュア接続 (SSL または TLS) を使用**」が選択されている場合には、ディレクトリー・サーバーが SSL を使用するように構成されていなければなりません。「**接続の検査**」をクリックして、指定された情報を使用して、ドメイン・コントローラーへの接続を正常に確立できることをテストする。 • 「**ドメイン・コントローラーへの接続 (Connect to Domain Controller)**」パネルのユーザー情報が、正確であることを確認する。

表 27. 共通 EIM ドメイン・コントローラー接続問題および解決策 (続き)

起こりうる問題	考えられる解決策
オペレーティング・システムまたはアプリケーションが、EIM データにアクセスするためにドメイン・コントローラーに接続することができない。たとえば、システムに代わって実行した EIM マッピング・ルックアップ操作が失敗する。これは、1 つかそれ以上のシステム上で EIM 構成に誤りがあるために生じることがあります。	ご使用の EIM 構成の検査。認証しようとしているシステム上で、「**ネットワーク**」-->「**エンタープライズ識別マッピング**」-->「**構成**」の順に展開します。「**構成**」フォルダーを右マウス・ボタン・クリックして、「**プロパティー**」を選択し、以下のものを検査してください。 • **ドメイン**・ページ: – ドメイン・コントローラー名およびポート番号が正確である。 – 「**構成の確認**」をクリックして、ドメイン・コントローラーがアクティブであることを確認する。 – ローカル・レジストリー名が正確に指定されている。 – Kerberos レジストリー名が正確に指定されている。 – 「**このシステムの EIM 操作の使用可能**」が選択されている。 • **システム・ユーザー**・ページ : – 指定されたユーザーが、マッピング・ルックアップを実行するための十分な EIM アクセス制御を持ち、そのユーザーに対してパスワードが有効である。オンライン・ヘルプを参照して、各種タイプのユーザーの信任状について確認してください。 **注:** ディレクトリー・サーバー内の指定されたシステム・ユーザーのパスワードを変更した場合には、このパスワードも変更しなければなりません。これらのパスワードが一致しない場合には、システム・ユーザーはオペレーティング・システムに対して EIM 機能を実行できず、マッピング・ルックアップ操作が失敗します。 – 「**接続の検査**」をクリックして、指定されたユーザー情報が正確であることを確認する。
構成情報は正確のようだが、ドメイン・コントローラーに接続できない。	• EIM ドメイン・コントローラーとして機能するディレクトリー・サーバーがアクティブであることを確認します。ドメイン・コントローラーが iSeries サーバーの場合は、 iSeries ナビゲーターを使用して、以下のステップに従うことができます。 1. 「**ネットワーク**」>「**サーバー (Servers)**」>「**TCP/IP**」を展開する。 2. 「ディレクトリ」サーバーが「**開始**」の状況になっているかどうかを検査する。サーバーが停止している場合は、「**ディレクトリ**」を右クリックして、「**開始...**」を選択する。

接続情報およびディレクトリー・サーバーがアクティブであることを確認したならば、 次のようにして、ドメイン・コントローラーへの接続を試行してください。

1. 「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。
2. 接続する EIM ドメインを右マウス・ボタン・クリックし、「**接続...**」を選択する。
3. EIM ドメイン・コントローラーに接続するために使用するユーザー・タイプと必要なユーザー情報を指定する。
4. 「**OK**」をクリックする。

一般 EIM 構成問題およびドメイン問題のトラブルシューティング

ユーザーのシステム用に EIM を構成する際に直面する可能性のある多数の一般問題、および EIM ドメインにアクセスする際に直面する可能性のある問題があります。以下の表を使用して、これらの問題を解決するために使用できる、いくつかの共通問題および考えられる解決策を確認してください。

表 28. 共通 EIM 構成とドメイン問題、および解決策

起こりうる問題	考えられる解決策
終了処理中に EIM 構成ウィザードがハングする	ドメイン・コントローラーが開始するのをウィザードが待っていることがあります。ディレクトリー・サーバーの始動時にエラーが起きなかったかどうかを確認してください。 iSeries サーバーの場合は、 QSYSWRK サブシステム中の QDIRSRV ジョブのジョブ・ログを調べてください。ジョブ・ログを調べるには、以下のステップに従ってください。 1. iSeries ナビゲーターで、「**実行管理機能**」>「**サブシステム**」>「**Qsyswrk**」を展開する。 2. 「**Qdirsrv**」を右クリックして、「**ジョブ・ログ**」を選択する。
EIM 構成ウィザードを使用してリモート・システム上にドメインを作成している際に、次のエラー・メッセージを受け取る。「The parent distinguished name (DN) you entered is not valid. The DN must exist on the remote directory server. Specify or select a new or existing parent DN.」	リモート・ドメインに指定された親 DN が存在していません。 EIM 構成ウィザードの使用法については、84 ページの『新規リモート・ドメインの作成と結合』で確認してください。また、オンライン・ヘルプで、ドメインの作成時に親 DN を指定することについての詳細な情報を参照してください。
EIM ドメインが存在しないことを示すメッセージを受け取る。	EIM ドメインを作成しなかった場合には、EIM 構成ウィザードを使用してください。このウィザードは、ユーザー用の EIM ドメインを作成するか、 または既存の EIM ドメインを構成できるようにします。 EIM ドメインを作成した場合には、指定されたユーザーが、それにアクセスするための十分な権限を持つ 43 ページの『EIM アクセス制御』グループのメンバーであることを確認してください。
EIM オブジェクト (ID、レジストリー、アソシエーション、ポリシー・アソシエーション、または証明書フィルター) が見つからなかったこと、またはユーザーが EIM データに対して許可されていないことを示すメッセージを受け取る。	EIM オブジェクトが存在すること、および指定されたユーザーがそのオブジェクトに対して十分な権限を持つ 43 ページの『EIM アクセス制御』グループのメンバーであるかどうかを確認する。

表 28. 共通 EIM 構成とドメイン問題、および解決策 (続き)

起こりうる問題	考えられる解決策
「**ID**」フォルダーを展開すると、 ID のリストが表示されるまでに時間がかかることがあります。	このことは、ドメイン内に大量の EIM ID がある場合に生じることがあります。このことを解決するには、ID を表示するために使用する検索条件を限定することによって、「**ID**」フォルダー・ビューをカスタマイズできます。 EIM ID の表示をカスタマイズするには、以下のステップに従ってください。 1. iSeries ナビゲーターで、「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。 2. 表示したい EIM ID のあるドメインを展開する。 3. 「**ID**」を右クリックして、「**このビューのカスタマイズ (Customize this view...)**」>「**組み込み...**」を選択する。 4. ビューに組み込む EIM ID のリストを生成するために使用する表示基準を指定する。 **注:** ワイルドカード文字としてアスタリスク (*) を使用することもできます。 5. 「**OK**」をクリックする。 次回「**ID**」をクリックすると、指定した基準に合致する EIM ID だけが表示されます。
iSeries ナビゲーターを使用して EIM を管理している際に、EIM ハンドルが有効でなくなったことを示すエラーを受け取る。	ドメイン・コントローラーへの接続が失われています。ドメイン・コントローラーに再接続するには、以下のステップに従ってください。 1. iSeries ナビゲーターで、「**ネットワーク**」>「**エンタープライズ識別マッピング**」>「**ドメイン管理**」を展開する。 2. 処理するドメインを右マウス・ボタン・クリックし、「**再接続... (Reconnect...)**」を選択する。 3. 接続情報を指定する。 4. 「**OK**」をクリックする。
EIM と共に Kerberos プロトコルを使用して認証を行っている場合に、診断メッセージ CPD3E3F がジョブ・ログに書き込まれる。	このメッセージは、認証または ID マッピング操作が失敗した場合に必ず生成されます。この診断メッセージには、問題が起きた場所を示すメジャーおよびマイナー状況コードが含まれます。最も一般的なエラーとリカバリーがメッセージ中に記述されます。問題のトラブルシューティングを始める際には、診断メッセージに関連したヘルプ情報を参照してください。 シングル・サインオン構成のトラブルシューティング (Troubleshoot single signon configuration) を検討することも役立つでしょう。

EIM マッピング問題のトラブルシューティング

EIM (エンタープライズ識別マッピング) マッピングが全体として失敗するか、期待どおりに作動しない、いくつかの共通問題があります。以下の表を使用して、どの問題が EIM マッピングを失敗させているか、およびその問題に対する、考えられる解決策についての情報を見つけてください。 EIM マッピングが失敗

する場合、マッピングを失敗させている問題 (1 つまたは複数) を確実に検出して解決するために、表中のそれぞれの解決策を処理する必要があるかもしれません。

表 29. 共通 EIM マッピング問題および解決策

起こりうる問題	考えられる解決策
ドメイン・コントローラー用の接続情報が、正確でないか、またはドメイン・コントローラーがアクティブでない。	ドメイン・コントローラー接続問題を参照して、ドメイン・コントローラー用の接続情報の確認方法、およびドメイン・コントローラーがアクティブであることを検査する方法を確認してください。
システムに代わって実行する EIM マッピング・ルックアップ操作が失敗する。これは、1 つかそれ以上のシステム上で EIM 構成に誤りがあるために生じることがあります。	ご使用の EIM 構成の検査。認証しようとしているシステム上で、「**ネットワーク**」--> 「**エンタープライズ識別マッピング**」--> 「**構成**」の順に展開します。「**構成**」フォルダーを右マウス・ボタン・クリックして、「**プロパティー**」を選択し、以下のものを検査してください。 • **ドメイン**・ページ: – ドメイン・コントローラー名およびポート番号が正確である。 – 「**構成の確認**」をクリックして、ドメイン・コントローラーがアクティブであることを確認する。 – ローカル・レジストリー名が正確に指定されている。 – Kerberos レジストリー名が正確に指定されている。 – 「**このシステムの EIM 操作の使用可能**」が選択されている。 • **システム・ユーザー**・ページ : – 指定されたユーザーが、マッピング・ルックアップを実行するための十分な EIM アクセス制御を持ち、そのユーザーに対してパスワードが有効である。オンライン・ヘルプを参照して、各種タイプのユーザーの信任状について確認してください。 **注:** ディレクトリー・サーバー内の指定されたシステム・ユーザーのパスワードを変更した場合には、このパスワードも変更しなければなりません。これらのパスワードが一致しない場合には、システム・ユーザーはオペレーティング・システムに対して EIM 機能を実行できず、マッピング・ルックアップ操作が失敗します。 – 「**接続の検査**」をクリックして、指定されたユーザー情報が正確であることを確認する。

表 29. 共通 EIM マッピング問題および解決策 (続き)

起こりうる問題	考えられる解決策
マッピング・ルックアップ操作が、複数のターゲット・ユーザー ID を戻すことがある。これが生じる可能性があるのは、以下の状況の 1 つ以上が存在する場合です。 • EIM ID が、同一のターゲット・レジストリーに対して、複数のターゲット・アソシエーションを持っている場合。 • 複数の EIM ID が、ソース・アソシエーション内に同じユーザー ID を指定しており、 かつ、これらの EIM ID が、同一のターゲット・レジストリーに対してターゲット・アソシエーションを持つ場合 (それぞれのターゲット・アソシエーションに指定されたユーザー ID は異なっているかもしれない)。 • 複数のデフォルトのドメイン・ポリシー・アソシエーションが、同一のターゲット・レジストリーを指定する場合。 • 複数のデフォルトのレジストリー・ポリシー・アソシエーションが、同一のソース・レジストリーおよび同一のターゲット・レジストリーを指定する場合。 • 複数の証明書フィルター・ポリシー・アソシエーションが、同一のソース X.509 レジストリー、証明書フィルター、およびターゲット・レジストリーを指定する場合。	EIM マッピングのテスト機能を使用して、特定のソース・ユーザー ID が、適切なターゲット・ユーザー ID に正確にマップされることを確認してください。問題の訂正方法は、テストでどのような結果が出るかによって異なります。次のとおりです。 • テストにおいて、以下のいずれかの理由で不要な複数のターゲット ID を戻す。 – これは、ドメインのアソシエーション構成が、次のいずれかの理由のため、不正確であることを示している可能性があります。 - EIM ID のターゲット・アソシエーションまたはソース・アソシエーションが正しく構成されていない。たとえば、Kerberos プリンシパル (または windows ユーザー) に対するソース・アソシエーションがないか、もしくはそれが不正確である。または、ターゲット・アソシエーションが不正確なユーザー ID を指定している。 EIM ID のすべての ID アソシエーションの表示を行って、特定の ID のアソシエーションを確認してください。 - ポリシー・アソシエーションが正確に構成されていない。ドメインのすべてのポリシー・アソシエーションの表示を行って、ドメイン内で定義されているすべてのポリシー・アソシエーションのソース情報およびターゲット情報を確認してください。 – これは、共通のメンバーを含むグループ・レジストリー定義が、EIM ID アソシエーションかポリシー・アソシエーションのソースまたはターゲット・レジストリーであることを示す可能性があります。テスト・マッピング・ルックアップ操作により提供される詳細を使用して、ソースまたはターゲット・レジストリーがグループ・レジストリー定義かどうかを判別してください。そうである場合、グループ・レジストリー定義プロパティーをチェックし、グループ・レジストリー定義に共通メンバーが入っているかどうかを判別します。 – テストが複数のターゲット ID を戻すが、これはアソシエーションの構成は妥当である場合。この場合には、それぞれのターゲット・ユーザー ID ごとに ルックアップ情報を指定して、ルックアップ操作が、考えられるすべてのターゲット・ユーザー ID ではなく、 単一のターゲット・ユーザー ID を戻すようにする必要があります。 ターゲット・ユーザー ID にルックアップ情報を追加するを参照してください。 **注:** この方法は、アプリケーションがルックアップ情報を使用できる場合にのみ有効です。ただし、iSeries Access for Windows などの 基本 i5/OS アプリケーションは、ルックアップ情報を使用して、ルックアップ操作によって戻された複数のターゲット・ユーザー ID を区別することはで

表 29. 共通 EIM マッピング問題および解決策 (続き)

起こりうる問題	考えられる解決策
EIM ルックアップ操作が、何も結果を戻さず、ドメインに対してアソシエーションが構成されない。	EIM マッピングのテスト機能を使用して、特定のソース・ユーザー ID が、適切なターゲット・ユーザー ID に正確にマップされることを確認してください。テストのために正確な情報を提供したかどうかを確認してください。情報が正確であるのに、テストが結果を戻さない場合には、以下のいずれか 1 つによって問題が生じたことが考えられます。 • アソシエーション構成が間違っている。前の項目で提供されている問題解決情報を使用して、アソシエーション構成を確認してください。 • ポリシー・アソシエーション・サポートが、ドメイン・レベルで使用できない。 ドメインのポリシー・アソシエーションを使用可能にする必要があるかもしれません。 • マッピング・ルックアップ・サポートまたはポリシー・アソシエーション・サポートが、個々のレジストリー・レベルで使用できない。 ターゲット・レジストリーに対してマッピング・ルックアップ・サポートおよびポリシー・アソシエーションを使用可能にする必要があるかもしれません。 • レジストリー定義およびユーザー ID が、大文字小文字が違うために、一致しない。レジストリーまたはアソシエーションを削除し、大文字小文字を正確に指定して再作成できます。

EIM (エンタープライズ識別マッピング) API

ここでは、EIM API について、およびアプリケーションやネットワーク内でのそれらの使用法について学習します。

EIM (エンタープライズ識別マッピング) は、クロスプラットフォーム・ユーザー ID 管理のためのメカニズムを提供します。 EIM には、複数のアプリケーション・プログラミング・インターフェース (API) があり、 アプリケーションでこれらの API を使用してそのアプリケーションやアプリケーション・ユーザーのために EIM 操作を実行することができます。 これらの API を使用して、ID マッピング・ルックアップ操作、さまざまな EIM の管理と構成の機能、および情報の変更や QUERY の機能を実行できます。 これらの API のおのおのは、複数の IBM プラットフォーム間でサポートされます。

EIM API は、以下のカテゴリーに分類できます。

- EIM ハンドルおよび接続の操作
- EIM ドメインの管理
- レジストリーの操作
- EIM ID の操作
- EIM アソシエーションの管理
- EIM マッピング・ルックアップ操作
- EIM 権限の管理

これらの API を使用して EIM ドメイン中の EIM 情報を管理したり利用したりするアプリケーションは、通常は以下のプログラミング・モデルに従います。

1. EIM ハンドルを取得する。
2. EIM ドメインに接続する。
3. 通常のアプリケーション処理を行う。
4. EIM 管理または EIM ID マッピング・ルックアップ操作 API を使用する。
5. 通常のアプリケーション処理を行う。
6. 終了する前に、EIM ハンドルを破棄する。

関連情報

EIM (エンタープライズ識別マッピング) API

EIM (エンタープライズ識別マッピング) の関連情報

ここでは、EIM の使用に関連するその他のリソースおよび情報について学習します。

EIM (エンタープライズ識別マッピング) に関連した他のテクノロジーについても知りたいと思われるかもしれません。次に挙げる Information Center のトピックは、関連したテクノロジーを理解する上で参考になります。

- **シングル・サインオン (Single signon)** このトピックは、シングル・サインオンが企業にとってどのように有益かを判別するために使用できる多数のシナリオを含め、企業のシングル・サインオン環境を構成および管理する方法についての情報を記載します。
- **ネットワーク認証サービス** このトピックは、ネットワーク認証サービス、すなわち Kerberos プロトコルの iSeries インプリメンテーションについての構成情報およびその他の情報を提供します。ネットワーク認証サービスを EIM と合わせて作動するように構成すれば、企業のシングル・サインオン環境を作成できます。
- **IBM iSeries 用ディレクトリー・サービス (LDAP) (IBM Directory Server for iSeries (LDAP))** このトピックは、 IBM Directory Server for iSeries (LDAP) の構成および概念的な情報を提供します。 EIM はディレクトリー・サーバーを EIM ドメイン・コントローラーのホストとして機能させ、それを使用して EIM ドメイン・データを保管できます。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することは できません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、 IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

付録. 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032
東京都港区六本木 3-2-31
IBM World Trade Asia Corporation
Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。 IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、IBM 機械コードのご使用条件、またはそれと同等の条項に基づいて、 IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。 IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年). このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。 © Copyright IBM Corp. _年を入れる_. All rights reserved.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

以下は、IBM Corporation の商標です。

AIX
Distributed Relational Database Architecture
Lotus Domino
DRDA
eServer
i5/OS
IBM
iSeries
Lotus Notes
NetServer
OS/400
pSeries
RACF
RDN
Tivoli
WebSphere
xSeries
z/OS
zSeries

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

UNIX は、The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することは できません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、 IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

Printed in Japan

日本アイ・ビー・エム株式会社
〒106-8711　東京都港区六本木3-2-12