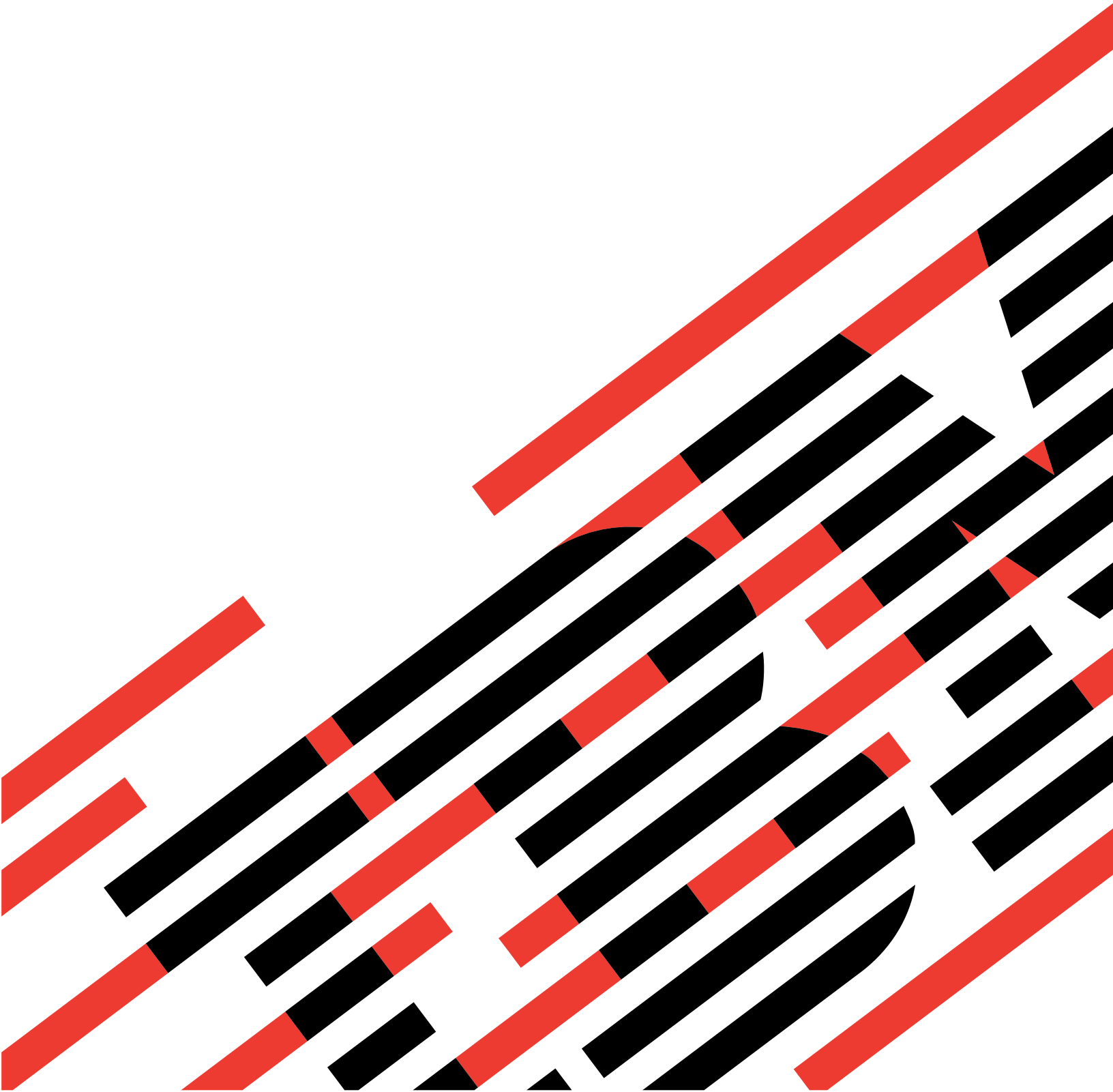
IBM

eserver

iSeries

EIM
(エンタープライズ識別マッピング)



IBM

@server

iSeries

EIM
(エンタープライズ識別マッピング)

目次

EIM (エンタープライズ識別マッピング)

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 は、個人やエンティティーを企業内の様々なレジストリーの対応するユーザー ID にマップする (関連付ける) ためのメカニズムです。 EIM は、これらの ID マッピングの関係を作成および管理するための API の他に、この情報を照会するためにアプリケーションが使用する API も備えています。さらに、OS/400® は、EIM および Kerberos 機能を使用して、シングル・サインオン環境を提供します。

iSeries のグラフィカル・ユーザー・インターフェースである iSeries ナビゲーターには、EIM を構成して管理するためのウィザードが用意されています。また管理者は、ユーザー・プロファイルにおける EIM 情報の管理も iSeries ナビゲーターで行えます。

iSeries™ サーバーでは EIM を使用して、OS/400 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。OS/400 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。

次のトピックには、EIM に関する具体的な情報があります。

トピックの印刷
この EIM トピックと他のアソシエーション・トピックの PDF 版を印刷します。

EIM (エンタープライズ識別マッピング) の概要
EIM 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。

EIM の概念
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 EIM の概念について学びます。

EIM 用の LDAP の概念
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、Lightweight Directory Access Protocol (LDAP) の概念について学びます。

シングル・サインオンの使用可能化
EIM で得られるユーザー・サインオンの単純化による利点を説明しています。

EIM の計画
EIM を構成する前に必要なサービスとアプリケーションをすべて構成していることを確認します。

EIM の構成
「エンタープライズ識別マッピング構成」ウィザード (今後は「EIM 構成」ウィザードと呼びます) を使用して、EIM を開始します。

EIM の管理
EIM のプロパティー、EIM ドメイン、ユーザー・レジストリー、EIM ユーザー権限などを管理します。

EIM の API
アプリケーションおよびネットワークで EIM API を使用します。

EIM のトラブルシューティング
ネットワークで EIM を使用中に起こる可能性がある共通の問題とエラーに対するソリューションが記載されています。

EIM の関連情報
EIM の関連情報にリンクしています。

トピックの印刷

PDF 版をダウンロードし、表示するには、EIM (エンタープライズ識別マッピング)  (約 767 KB、56 ページ) を選択します。

他の情報

次のアソシエーション・トピックをダウンロードし、表示することができます。

- 「ネットワーク認証サービス」 (約 729 KB、66 ページ) には、EIM にアソシエーションして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されています。
- 「iSeries ディレクトリー・サービス (LDAP)」 (約 808 KB、82 ページ) には、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とともに、拡張 LDAP 構成に関する情報が記載されています。

PDF ファイルの保管

表示用または印刷用の PDF ファイルを Netscape Navigator からワークステーションに保存するには、次のようにします。

1. ブラウザーで PDF を開く (上記のリンクをクリックする)。
2. ブラウザーのメニューから**「ファイル」**をクリックする。
3. **「名前を付けて保存」**をクリックする。(IE の場合は、フロッピー・ディスクのアイコン (名前を付けて保存) をクリックする。)
4. PDF を保存したいディレクトリーに進む。
5. **「保存」**をクリックする。

Adobe Acrobat Reader のダウンロード

PDF ファイルを表示したり印刷したりするには Adobe Acrobat Reader が必要です。これは、Adobe Web サイト (www.adobe.com/prodindex/acrobat/readstep.html)  から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

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 の基盤テクノロジーが、エンタープライズ識別マッピング (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。

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、企業内で複数のユーザー・レジストリーとユーザー ID を簡単に管理するための低費用の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 で既に認証され、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。

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能力は、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 SAP リソースにアクセスするために、SAP ID をマップするというようなことが可能になります (よりよい方法として、SAP 自体がマッピングを実行するようなことも可能です)。

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. 企業内の個人やエンティティーを表す EIM ID を作成します。
2. 企業内の既存のユーザー・レジストリーを記述した EIM レジストリー定義を作成します。
3. そのレジストリー内のユーザー ID と EIM ID との関係を定義します。

既存のユーザー・レジストリーについては、コードの変更は不要です。管理者は、ユーザー・レジストリー内のすべての ID をマッピングする必要はありません。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)。ま

た、EIM を使用すると、他対 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 つのユーザー識別を共用することも可能です)。ただし、これは可能ですが、お勧めできる方法ではありません。管理者は、EIM でどのタイプのどのユーザー・レジストリーでも表すことができます。

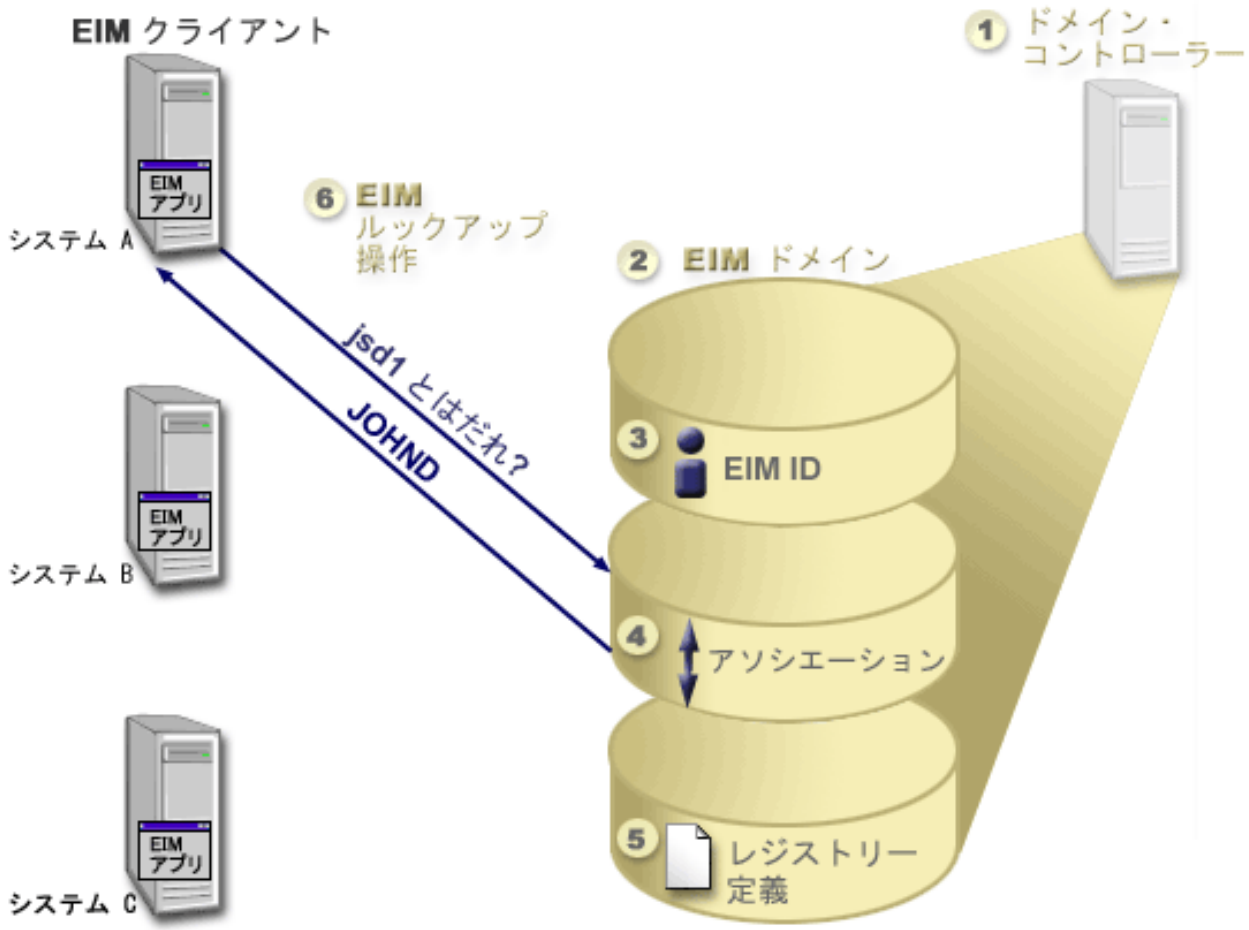
EIM はオープン・アーキテクチャーなので、どのレジストリーの識別マッピングの関係でも表すことができます。既存のデータを新規リポジトリーにコピーして、両方を同期して保持しようとする必要はありません。 EIM が導入する唯一の新規データは、関係情報です。管理者はこのデータを LDAP ディレクトリーで管理します。そのようにして、データを一元管理しながら、実際に情報を使用する場所でレプリカを保持するという柔軟性が得られます。よって、EIM では、企業やアプリケーション開発者がより多彩な環境でより少ない費用で簡単に作業するための柔軟性が得られるということになります。

EIM の概念

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 6 によって EIM データを要求する EIM 対応アプリケーションが含まれています。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 の概念の詳細について理解してください。

- EIM ドメイン・コントローラー
- EIM ドメイン
- EIM ID
- EIM レジストリー定義
- EIM アソシエーション
- EIM ルックアップ操作
- EIM 権限

EIM ドメイン・コントローラー

EIM ドメイン・コントローラー は、少なくとも 1 つの EIM ドメインを管理するために構成された Lightweight Directory Access Protocol (LDAP) サーバーのことです。 *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。少なくとも 1 つの EIM ドメイン・コントローラーが企業内になければなりません。

現在、一部の IBM @server プラットフォームを EIM ドメイン・コントローラーとして機能するよう構成できます。 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、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。

EIM ドメイン

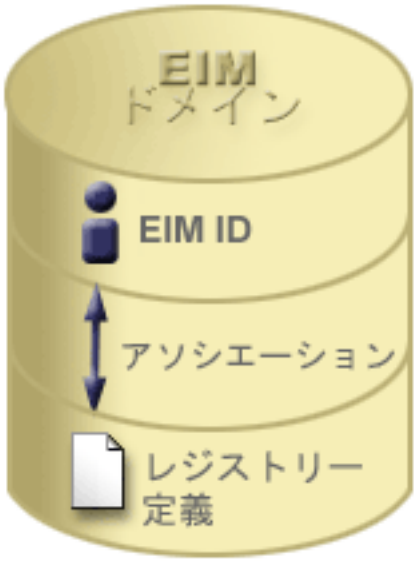
EIM ドメイン は、企業の EIM データを含む Lightweight Directory Access Protocol (LDAP) サーバー内のディレクトリーです。EIM ドメインは、すべての EIM ID、EIM アソシエーション、およびそのドメインで定義されているユーザー・レジストリーのコレクションです。システム (EIM クライアント) は、EIM ルックアップ操作用のドメイン・データを使用してドメインに参加します。

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。 EIM は関係情報のみを管理するので、ユーザー・レジストリーと EIM の間で同期化するべき情報はありません。

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 ID。** 作成する各 EIM ID は、企業内の個人やエンティティー (プリント・サーバーやファイル・サーバーなど) を表しています。詳細は、『EIM ID』を参照してください。
- **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。詳細は、『EIM レジストリー定義』を参照してください。
- **EIM アソシエーション。** 作成する各 EIM アソシエーションは、EIM ID と企業内で関連付けられた ID との間の関係を表しています。EIM ドメインに参加しているユーザー・レジストリー内の ID のアソシエーションを作成します。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ます。 よって、アソシエーションを定義して、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しなければなりません。こうした EIM ルックアップ操作を行うと、EIM ドメインにおいて、EIM ID と、認識されたユーザー・レジストリー内のユーザー ID との間のアソシエーションを検索します。詳細は、『EIM ルックアップ操作』を参照してください。

いったん EIM ID、レジストリー定義、アソシエーションを作成すると、各企業において EIM を使用してユーザー ID をより簡単に編成して処理することができます。

EIM ID

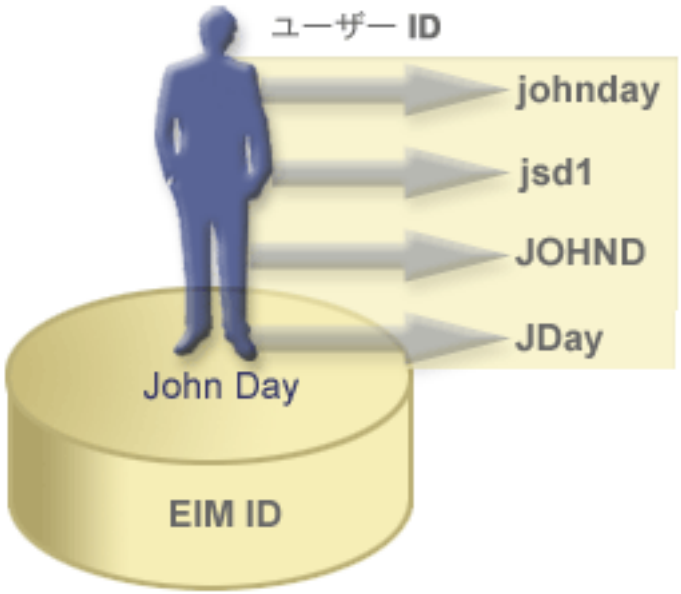
EIM ID は、企業内の個人やエンティティーを表します。一般的なネットワークは、種々のハードウェア・プラットフォームおよびアプリケーション、またそれらに関連付けられたユーザー・レジストリーから構成されています。 ほとんどのプラットフォームや多くのアプリケーションでは、プラットフォーム固有の、またはアプリケーション固有のユーザー・レジストリーが使用されています。こうしたユーザー・レジストリーには、このようなサーバーまたはアプリケーションを使用するユーザーのユーザー識別情報が含まれます。

EIM ID を作成してそれを個人やエンティティーの様々なユーザー ID と関連づけると、たとえばシングル・サインオン環境などの異機種混合で、多層構造のアプリケーションを構築するのが容易になります。また EIM ID およびアソシエーションを作成する場合は、企業内の個人やエンティティーが持っているすべてのユーザー ID の管理を簡単に行うためのツールを構築して使用することが容易になります。

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 4 つのユーザー ID を、4 つの別個のユーザー・レジストリー (`johnday`、`jsd1`、`JOHND`、`JDay`) 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

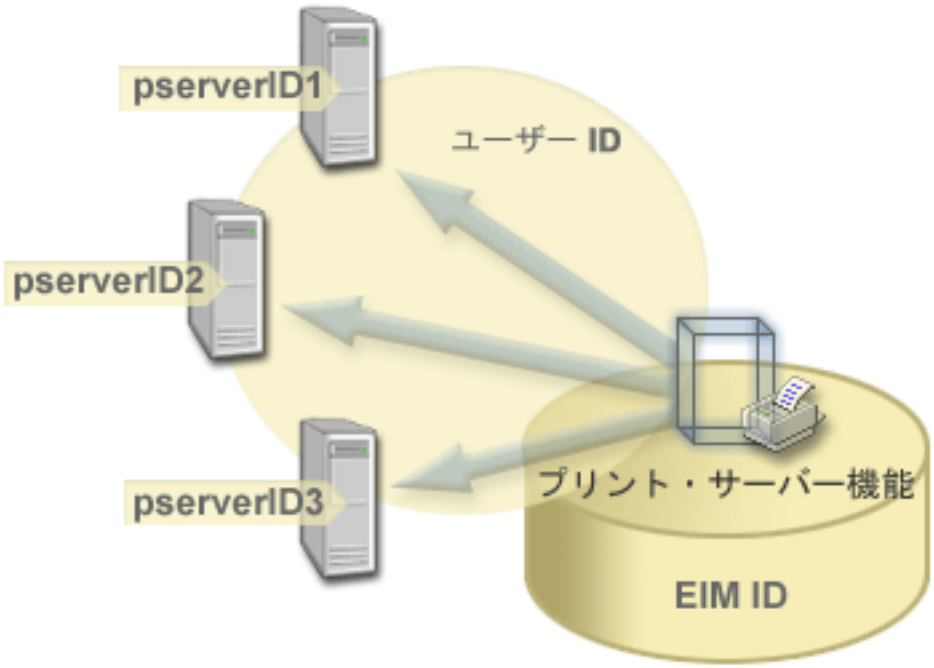


EIM では、`John Day` ID と *John Day* の異なるそれぞれのユーザー ID との間の関係を定義するアソシエーションを作成できます。こうしたアソシエーションを作成してその関係を定義すると、識別されているユーザー ID に基づいて、不明なユーザー ID を EIM API からルックアップするアプリケーションを、管理者やユーザーが作成できるようになります。

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`、`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。この例では、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、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。

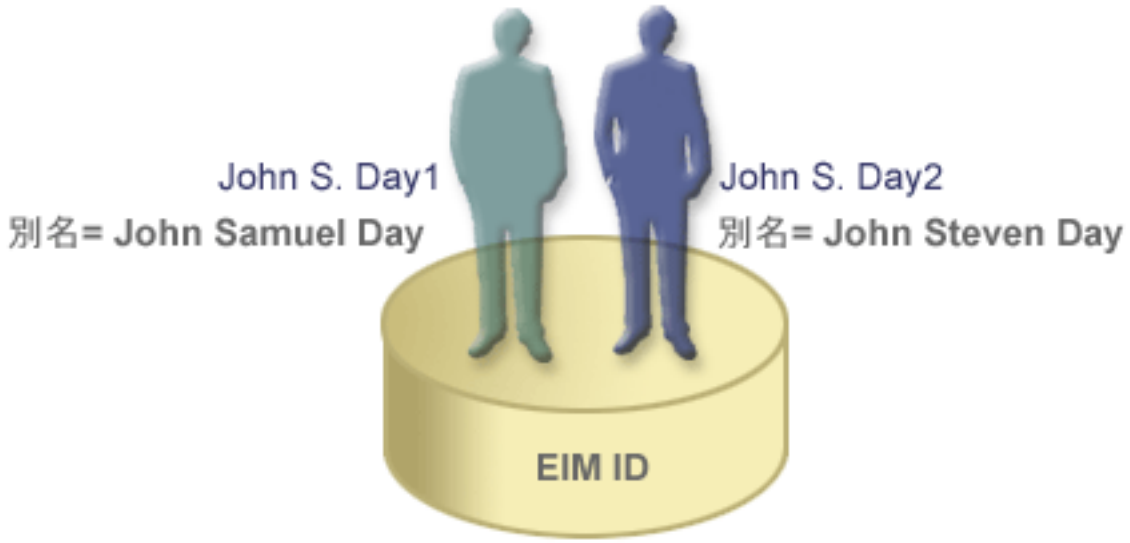
EIM ID および別名の作成

EIM ID の別名を作成することもできます。別名は、EIM ルックアップ操作を実行する際に、EIM ID を特定するのに役立ちます。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は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、企業内の異なる個人が同一名を共有していると、EIM ID として適切な名前を使用する場合に混乱のもとになります。

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 ルックアップ操作でこの情報を使用すれば、ID が表すユーザーを識別できます。たとえば、John S. Day1 の別名は John Samuel Day で、John S. Day2 の別名は John Steven Day となるかもしれません。

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。EIM 管理者はその 2 人をさらに区別しやすくするために、それぞれの EIM ID にさらに他の別名を追加することもできます。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。

EIM レジストリー定義

EIM 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・レジストリーを表しています。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・レジストリーでの他の例には、Kerberos 鍵配布センター (KDC) および OS/400 ユーザー・プロファイル・レジストリーがあります。

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。

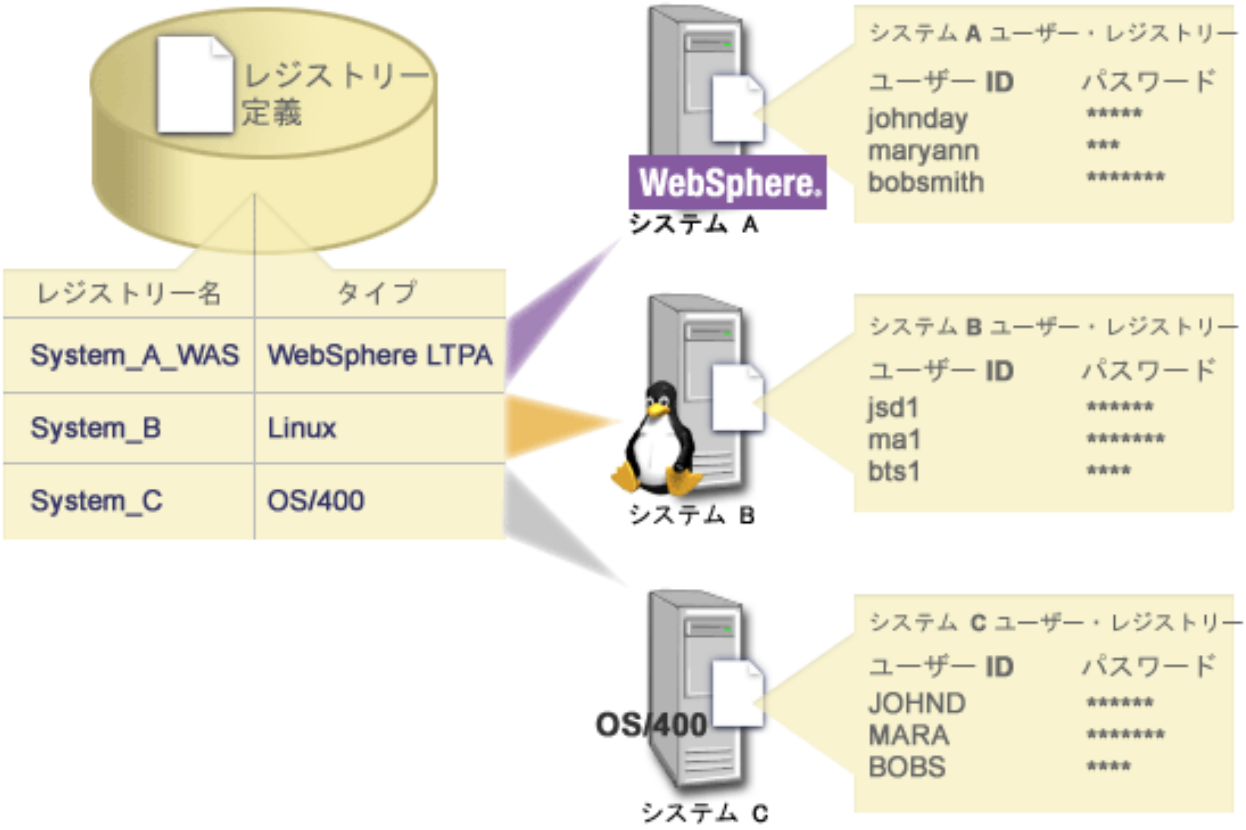
- 固有で、任意の EIM レジストリー名
- ユーザー・レジストリーのタイプ

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。

図 6 は、管理者はシステム A、システム B、システム C を表す、ユーザー・レジストリー用の EIM レジストリー定義の例です。システム A には WebSphere Lightweight Third-Party Authentication (LTPA) 用のユーザー・レジストリーが含まれます。管理者が使用するレジストリー定義名は、特定のタイプのユーザー・レジストリー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 `System_A_WAS` をレジストリー定義名として使用して、特定のユーザー・レジストリーを識別します。その名前に加え、管理者はレジストリーのタイプとして `WebSphere LTPA` も提供します。

図 6: 企業内の 3 つのユーザー・レジストリーの EIM レジストリー定義



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。たとえば、z/OS Security Server (RACF) レジストリーには、 RACF ユーザー・レジストリー全体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。この機能の例に関する詳細は、『システムおよびアプリケーション・レジストリー定義』を参照してください。

EIM レジストリー定義および別名の作成

EIM レジストリー定義の別名を作成することもできます。定義済みの別名タイプを使用することもできますし、独自の別名タイプを定義して使用することも可能です。定義済みの別名タイプには、以下のものが含まれます。

- ドメイン・ネーム・システム (DNS) のホスト名
- Kerberos レルム
- 送出側の識別名 (DN)
- ルートの識別名 (DN)
- TCP/IP アドレス
- LDAP DNS ホスト名

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 レジストリー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。

管理者が別名を EIM レジストリー定義に追加すると、アプリケーションは別名ルックアップを実行して初期設定の EIM レジストリー名を検出できます。別名ルックアップを実行すると、アプリケーションは EIM レジストリー名 (複数も可) を判別して、EIM ルックアップ操作を実行する API への入力として使用できます。

システム・レジストリー定義およびアプリケーション・レジストリー定義

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。EIM は、管理者がこのシナリオをモデル化できるように 2 種類の EIM レジストリー定義を提供しています。それは、システムとアプリケーションです。

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の異なるレジストリーを表します。システム・レジストリー定義を作成できるのは、エンタープライズ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®、OS/400® 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。

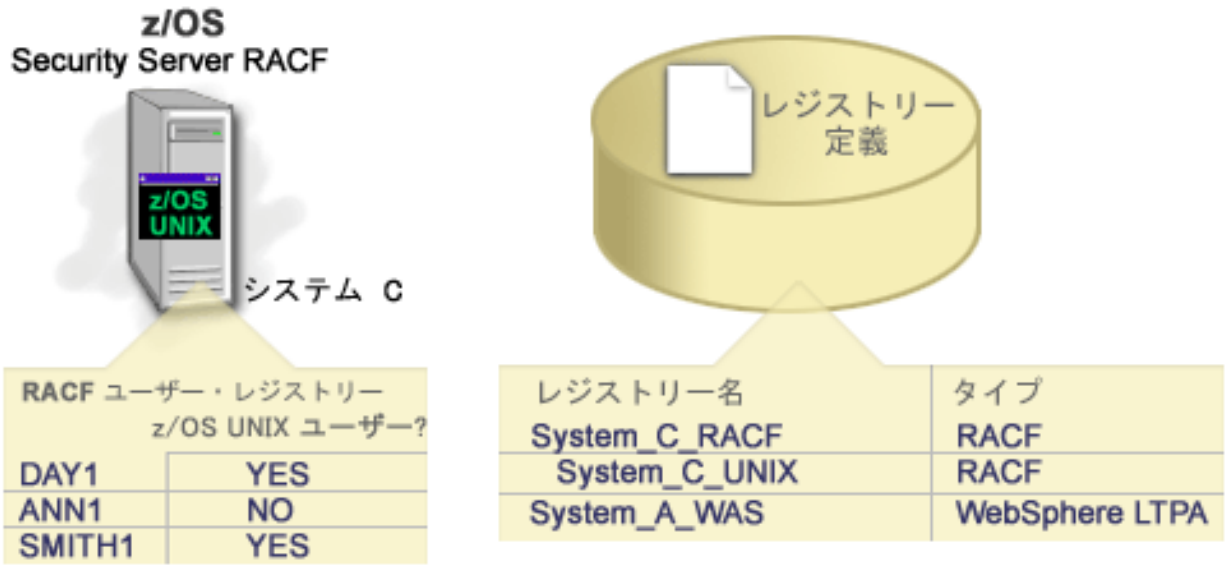
アプリケーション・レジストリー定義は、システム・レジストリー内で定義されたユーザー ID のサブセットを表します。これらのユーザー ID は、特定のアプリケーションまたはアプリケーション・セットを使用できるようにする共通の属性または特性のセットを共用します。アプリケーション・レジストリー定義を作成できるのは、ユーザー ID が以下の特色を持っている場合です。

- アプリケーションまたはアプリケーション・セットのユーザー ID が、そのアプリケーションまたはアプリケーション・セットの特有のユーザー・レジストリー内に保管されていない場合。
- アプリケーションまたはアプリケーション・セットのユーザー ID が、ほか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 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、レジストリーを個別に定義することによって、マッピング・データをアプリケーション・ベースで管理する必要があります。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に対する管理者として割り当てられます。

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 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



EIM アソシエーション

EIM アソシエーション は、特定の個人を表す EIM ID と、ユーザー・レジストリー内の個人を表す単一のユーザー ID の関係です。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。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。

アソシエーションを作成する前に、まずは適切な EIM ID と、関連付けられたユーザー・レジストリーを含むユーザー・レジストリー用の適切な 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 ID 名
- EIM レジストリー定義名

- アソシエーション・タイプ

管理者は、ユーザー ID の使用法に基づいて、EIM ID とユーザー ID の異なるタイプのアソシエーションを作成できます。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・レジストリー内のユーザー 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 では、管理者が EIM ID とユーザー ID で定義できる 3 つのタイプのアソシエーションがあります。ソース・アソシエーション、ターゲット・アソシエーション、管理アソシエーションが、その 3 つです。

ソース・アソシエーション

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。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。単一のソース・アソシエーションのみを持つユーザー ID が EIM ルックアップ操作においてターゲット ID として使用される場合には、関連付けられたユーザー ID は全く戻されません。

ターゲット・アソシエーション

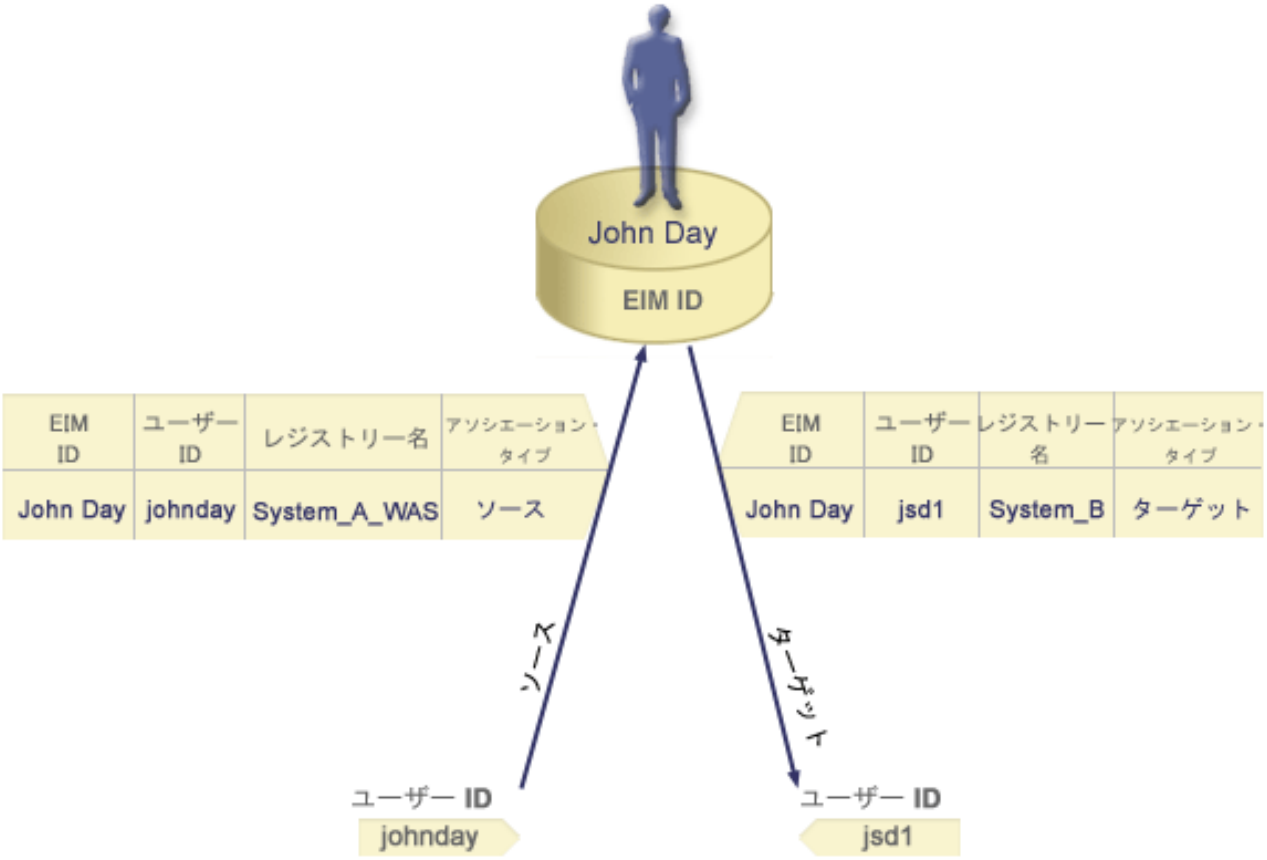
ユーザー ID が認証ではなく*権限* に使用される場合、そのユーザー ID は EIM ID とターゲット・アソシエーションを持っていなければなりません。ターゲット・アソシエーションを使用すると、ユーザー ID は EIM ルックアップ操作の結果として戻すことが可能です。 単一のターゲット・アソシエーションのみを持つユーザー ID が EIM ルックアップ操作においてソース ID として使用される場合には、関連付けられたユーザー ID は全く戻されません。

単一のユーザー ID に対しては、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かもしれません。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、通常ユーザーは Windows オペレーティング・システムに認証して、AIX サーバーにアクセスするアプリケーションを実行します。ユーザーのジョブ責任のため、ユーザーは時折 AIX サーバーに記録することも必要になります。このような場合には、AIX ユーザー ID とユーザーの 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作成します。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。

図 8 は、ソース・アソシエーションとターゲット・アソシエーションの例を示しています。この例では、管理者は EIM ID `John Day` に対して 2 つのアソシエーションを作成し、この ID と 2 つの関連付けられたユーザー ID の関係を定義しました。管理者は `johnday` のソース・アソシエーション、 WebSphere Lightweight Third-Party Authentication (LTPA) ユーザー ID を `System_A_WAS` ユーザー・レジストリー内に作成しました。また管理者は `jsd1` のターゲット・アソシエーション、OS/400 ユーザー・プロファイルをシステム B ユーザー・レジストリー内に作成しました。こうしたアプリケーションは、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。

図 8: 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



管理アソシエーション

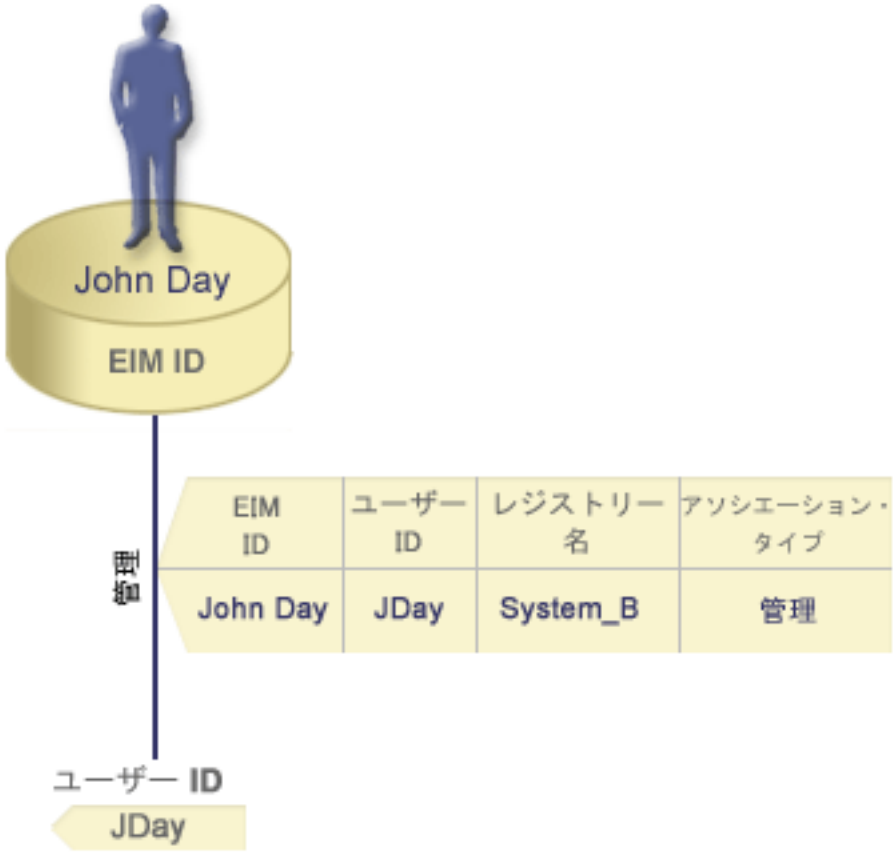
EIM ID との管理アソシエーションは、通常は EIM ID によって表される個人またはエンティティーが、指定されたシステムに対して特定の考慮事項を必要とするユーザー ID を持っていることを示すのに使用します。たとえば、このタイプのアソシエーションは、高度な機密のユーザー・レジストリーで使用できます。

管理アソシエーションの性質上、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は戻されません。

図 9 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 はシステム A 上に 1 つのユーザー ID 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 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、このシステムに認証することを確認したいと考えています。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 9: EIM ID John Day の EIM 管理アソシエーション



EIM ルックアップ操作

EIM ルックアップ操作 とは、既知の信頼ある情報が提供されることによって、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。

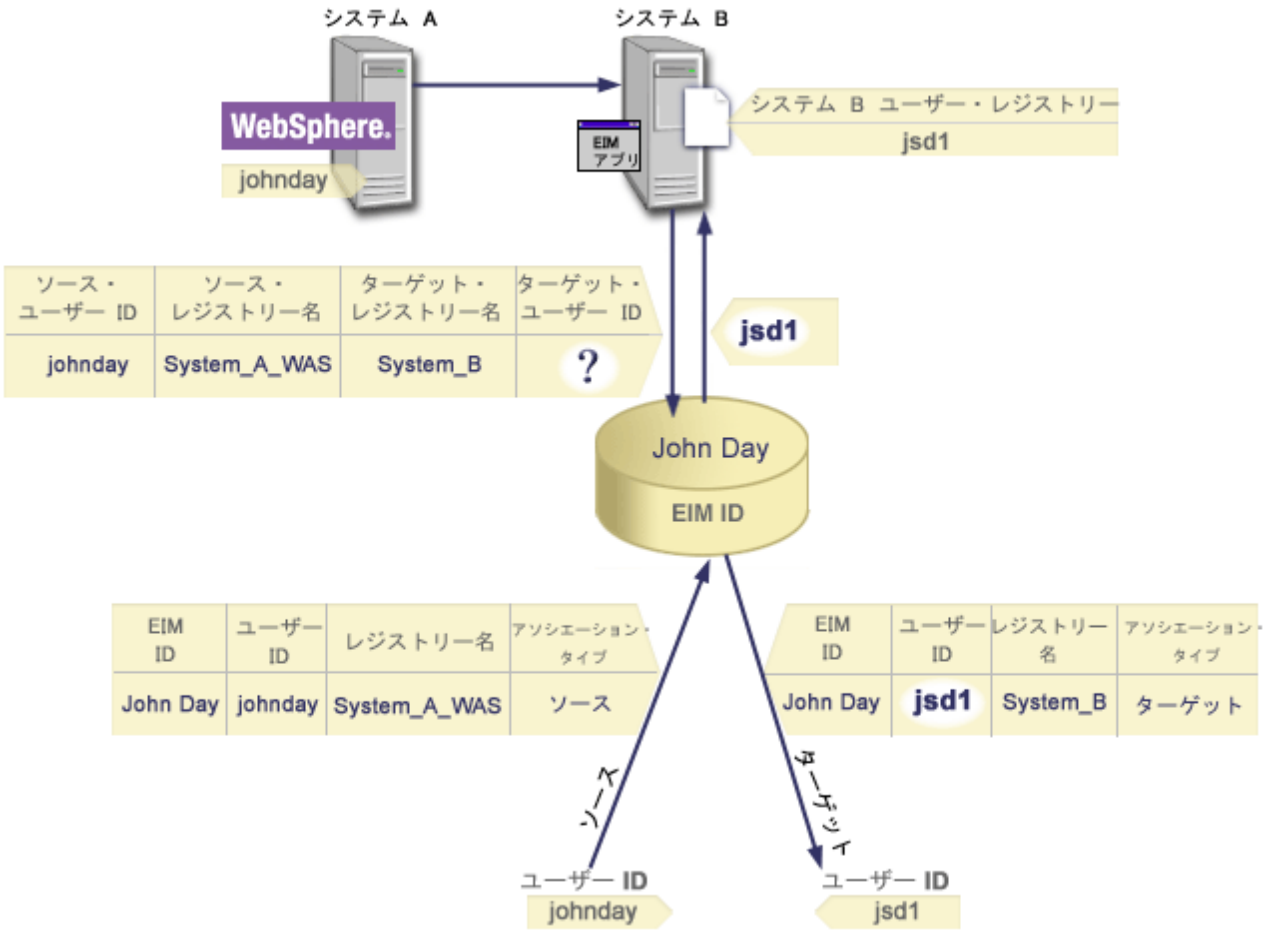
アプリケーションがソースとしてユーザー *ID* を提供する場合、ソース・ユーザー ID 用の EIM レジストリー定義名、および EIM ルックアップ操作のターゲットとなる EIM レジストリー定義名も提供する必要があります。 EIM ルックアップ操作においてソースとして使用するためには、ユーザー ID はそのために定義されたソース アソシエーションを有していなければなりません。

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 *EIM ID* を提供する場合、EIM ルックアップ操作のターゲットとなる EIM レジストリー定義も提供する必要があります。いずれのタイプの EIM 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 に関しては、そのために定義されたターゲット・アソシエーションをユーザー ID が持っていなければなりません。

提供された情報は EIM ドメイン・コントローラーに渡され、そこですべての EIM 情報が保管されて、EIM ルックアップ操作によって提供された情報と一致するソース・アソシエーションが検索されます。(API に提供された、またはソース・アソシエーション情報から判別された) EIM ID に基づき、EIM ルックアップ操作はターゲット EIM レジストリー定義名と一致する、その ID のターゲット・アソシエーションを検索します。

図 10 では、ユーザー ID johnday はシステム 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 上で固有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。固有プログラムは EIM 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 ドメイン・コントローラーに渡され、EIM ルックアップ操作によってこの情報と一致するソース・アソシエーションが検出されます。EIM ルックアップ操作は EIM ID 名を使用して、System_B のターゲット EIM レジストリー定義名と一致する、John Day ID のターゲット・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 10: 既知のユーザー ID johnday に基づく EIM ルックアップ操作



EIM 権限

EIM 権限 は、ユーザーが特定の管理用タスクまたは EIM ルックアップ操作を実行するようにします。他のユーザーの権限の認可や取り消しを行うことを許されているのは、EIM 管理者権限を持っているユーザーのみです。EIM 権限は EIM に認識されるユーザー ID にのみ付与されます。

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) 権限。**この権限は、ユーザーが新しい EIM ドメインを構成できるようにします。この権限を持つユーザーは、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
  - EIM ルックアップ操作の実行
  - アソシエーション、EIM ID、EIM レジストリー定義の検索
  - EIM 権限の情報の追加、除去、リスト
- **EIM 管理者。**この権限は、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。この権限を持つユーザーは、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
  - EIM ルックアップ操作の実行
  - アソシエーション、EIM ID、EIM レジストリー定義の検索
  - EIM 権限の情報の追加、除去、リスト
- **EIM ID 管理者。**この権限は、ユーザーが EIM ID の追加や変更、ソースおよび管理のアソシエーションを管理できるようにします。この権限を持つユーザーは、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
  - アソシエーション、EIM ID、EIM レジストリー定義の検索
- **EIM マッピング・ルックアップ。**この権限は、ユーザーが EIM ルックアップ操作を実行できるようにします。この権限を持つユーザーは、以下の機能を実行できます。
  - EIM ルックアップ操作の実行
  - アソシエーション、EIM ID、EIM レジストリー定義の検索
- **EIM レジストリー管理者。**この権限は、ユーザーが EIM レジストリー定義をすべて管理できるようにします。この権限を持つユーザーは、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
  - EIM ルックアップ操作の実行
  - アソシエーション、EIM ID、EIM レジストリー定義の検索

- **EIM レジストリー X 管理者。**この権限は、ユーザーが特定の EIM レジストリー定義を管理できるようにします。この権限を持つユーザーは、以下の機能を実行できます。
  - EIM レジストリー定義用のターゲット・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
  - アソシエーション、EIM ID、EIM レジストリー定義の検索

以下の表は、API が実行する EIM タスクごとに編成されています。各表は、各 EIM API と、異なる EIM 権限、および各権限が使用できる特定の EIM 機能を示しています。

表 1: ドメインの処理

EIM API	LDAP 管理者	EIM 管理者	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
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	-	-	-	-

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
eimAddApplicationRegistry	X	X	-	-	-	-
eimAddSystemRegistry	X	X	-	-	-	-
eimChangeRegistry	X	X	-	-	X	X
eimChangeRegistryUser	X	X	-	-	X	X
eimChgRegistryAlias	X	X	-	-	X	X
eimGetRegistryFromAlias	X	X	X	X	X	X
eimListRegistries	X	X	X	X	X	X
eimListRegistryAliases	X	X	X	X	X	X

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
eimListRegistryUsers	X	X	X	X	X	X
eimRemoveRegistry	X	X	-	-	-	-

表 4: 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てい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、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。以下の表は、各 API に対するアソシエーション・タイプをまとめたものです。

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: 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 6: 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	-	-	-	-
eimRemoveAccess	X	X	-	-	-	-

EIM 用の LDAP の概念

エンタープライズ識別マッピング (EIM) は、 EIM ドメイン・コントローラーとして Lightweight Directory Access Protocol (LDAP) サーバーを使用して、EIM データを保管します。EIM ドメイン・コントローラーからの認証を得る手段として、iSeries サーバー用の EIM を構成するときには、この LDAP 識別名を使用できます。

EIM を構成して管理するときに LDAP 識別名を使用するには、LDAP の以下の概念を理解する必要があります。

- LDAP 識別名
- LDAP 親識別名

LDAP 識別名

LDAP 識別名 (DN) は、LDAP サーバー用の許可ユーザーを識別し、記述する Lightweight Directory Access Protocol (LDAP) 項目です。EIM 構成ウィザードを使用して、LDAP サーバーを EIM ドメイン情報を保存するように構成することができます。iSeries サーバーがシングル・サインオン環境内に加わることができるようにするため、この EIM データにアクセスおよびこの EIM データを検索する方法として LDAP 識別名を使用することができます。

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 LDAP 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 LDAP 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 が LDAP 親識別名を使用する方法の詳細については、『LDAP 親識別名』を参照してください。

EIM は LDAP 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 LDAP 識別名を使用することができます。ご使用の iSeries サーバー用の EIM を構成するとき、LDAP 識別名を使用することもできます。たとえば、以下の場合に、LDAP 識別名を使用することができます。

- EIM ドメイン・コントローラーとして機能するように LDAP サーバーを構成する場合。これは、LDAP サーバー用の LDAP 管理者を識別する LDAP 識別名を作成し、使用することによって行うことがきます。LDAP 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、結合するときに、LDAP サーバーを構成することができます。

- 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。LDAP 識別名は、LDAP 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、ローカル OS/400 ユーザー・プロファイルを削除する場合のルックアップのマッピングと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。

識別名および LDAP が識別名を使用する方法の詳細については、『LDAP に関する基本事項』を参照してください。

LDAP 親識別名

LDAP 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。DN が LDAP サーバーのネームスペースの最高位であるとき、識別名は親 DN と見なされます。

完全 LDAP 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 は LDAP 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 LDAP 識別名を使用することができます。ご使用の iSeries サーバー用の EIM を構成するとき、LDAP 識別名および親識別名も使用します。たとえば、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 DN を指定することを選択することができます。親 DN を使用することによって、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。

識別名および識別名を使用する方法の詳細については、『LDAP に関する基本事項』を参照してください。

EIM を介したシングル・サインオンの使用可能化

EIM は、費用のかからない、エンタープライズ全体のシングル・サインオンを使用可能にするメカニズムを提供します。OS/400 は、EIM と Kerberos をインプリメントすることにより、多層かつ異機種混合の真のシングル・サインオン環境を実現します。エンタープライズ内でシングル・サインオン環境が使用可能であるとき、ユーザー、管理者、およびアプリケーション開発者にとって複数の利点があります。

ユーザーの利点

シングル・サインオン環境では、ユーザーが新しいシステムにアクセスするたびに認証を行います。ただし、パスワードを求めるプロンプトは出されません。EIM を使用すると、ユーザーが、ネットワーク内のその他のシステムにアクセスするために複数のユーザー名およびパスワードを追跡および管

理する必要が削減されます。いったんユーザーがネットワークに認証されると、これらの異なるシステムに複数のパスワードを入力しなくても、エンタープライズを介してサービスおよびアプリケーションにアクセスすることができます。

管理者の利点
管理者の場合、シングル・サインオンは、エンタープライズのセキュリティー管理全体を単純化します。シングル・サインオンしない場合、ユーザーおよびアプリケーションは、異なるシステムへのパスワードをキャッシュに入れることがあるので、ネットワーク全体のセキュリティーが危うくなる可能性があります。管理者は、これらのセキュリティー・リスクを減らすためにソリューションに時間とお金を費やします。シングル・サインオンすると、認証管理における管理オーバーヘッドが削減され、ネットワーク全体のセキュリティーが保たれます。また、シングル・サインオンすると、忘れてしまったパスワードを再設定するための管理コストが削減されます。

アプリケーション開発者の利点
異種ネットワーク内で実行しなければならないアプリケーションの開発者に対して、EIM は複数のプラットフォームで作業するアプリケーションを開発するためのインフラストラクチャーを提供します。EIM API を使用することにより、プログラマーは、権限用の異なるユーザー・レジストリーを使用している間、認証用の最適な既存のユーザー・レジストリーを使用するアプリケーションを開発できるようになります。EIM は、ユーザー・レジストリーにあるユーザー ID を単一の EIM ID にマップするアプリケーションを作成するためのインフラストラクチャーを提供するので、アプリケーション開発者は、作成するアプリケーション内のプラットフォーム固有のユーザー・レジストリーをサポートする必要がなくなります。さらに、EIM を使用すると、プログラマーは、アソシエーションしたセキュリティー・セマンティクス、およびアプリケーション・レベルのセキュリティーを変更しないで、これらのアプリケーションを保守することができるので、複数層の、プラットフォーム間のアプリケーションのインプリメントのコストが著しく低下します。

iSeries におけるシングル・サインオン実現
シングル・サインオン環境を使用可能にするには、IBM は、EIM とネットワーク認証サービスの 2 つのテクノロジーを使用します。これは、Kerberos および GSS API の IBM のインプリメンテーションです。これらの 2 つのテクノロジーを構成することによって、管理者は、シングル・サインオン環境を実現することができます。Windows 2000、XP、AIX、および zSeries は、Kerberos プロトコルを使用して、ネットワークでユーザーを認証します。Kerberos は、ネットワークにプリンシパル (Kerberos ユーザー) を認証する、ネットワーク・ベースの、セキュアな、鍵配布センターを使用しています。ユーザーは、一元管理された鍵配布センターから Kerberos チケットを受け取ります。このチケットは、エンタープライズ内のその他のサービスに対してユーザーの認証を行います。チケットは、ユーザーからチケットを受け入れるサービスに渡すことができます。チケットを受け入れるサービスでは、チケットを使用して、(Kerberos ユーザー・レジストリーおよびレルム内の) どのユーザーが請求しているか、そして、実際に請求しているのは誰かを判別します。

ネットワーク認証サービスにより、iSeries サーバーが Kerberos レルムに参加する間、エンタープライズ全体にそのユーザーを示す単一 EIM ID にこれらの Kerberos プリンシパルを関連付けるメカニズムを提供します。OS/400 ユーザー名などのその他のユーザー ID は、この EIM ID と関連付けることもできます。これらのアソシエーションに基づいて、Kerberos プリンシパルによって示された個人またはエンティティーを示している OS/400 ユーザー・プロファイルを判別するための OS/400 およびアプリケーションのメカニズムを提供します。EIM の情報を「木」にたとえると、EIM ID は根に相当し、EIM ID と関連付けられたユーザー ID のリストを枝にたとえることができます。

下記の図を例として使用して、John Smith などのユーザーが Windows PC を介してネットワークにサインオンし、Kerberos 使用可能アプリケーションにアクセスするために OS/400 のインスタンスにアクセスす

ると想定してください。 John は、OS/400 ユーザー名を入力するプロンプトが出されていません。これらのアプリケーションは、OS/400 ユーザー名を検索するために John の EIM ID へのアソシエーションを検索することができます。ユーザー・プロファイルは認証用に使用されず、権限用にのみ使用されるため、John Smith は、OS/400 ユーザー・プロファイルへのパスワードを必要としません。

図 11. シングル・サインオン環境

『シナリオ: シングル・サインオンの使用可能化』では、管理者が、シングル・サインオン環境を可能にするために、ネットワーク認証サービスおよび EIM を構成する方法の例を提供します。

以下のアプリケーションは、シングル・サインオンによってアクセスできます。

- iSeries ナビゲーター
- PC5250 エミュレーター
- Distributed Relational Database Architecture™ (DRDA)®
- NetServer
- QFileSvr.400

EIM の計画

iSeries サーバー上で EIM 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。

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。

計画ワークシート	答え
OS/400 V5R2 (5722-SS1) 以降がインストールされていますか?	
ご使用の iSeries サーバー上に Cryptographic Access Provider (5722-AC3) がインストールされていますか?	
ご使用のネットワーク内の該当する PC (iSeries サーバーを処理するために使用される PC) 上およびご使用の iSeries サーバー上に iSeries Access for Windows (5722-XE1) がインストールされていますか?	
ご使用のネットワーク内のすべての PC およびご使用の iSeries システム上に iSeries ナビゲーターのネットワーク・サブコンポーネントがインストールされていますか?	
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?	
LDAP サーバーが現在構成されている場合、LDAP サーバー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?	

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のための完全なワークシートについては、『ネットワーク認証サービスの計画』を参照してください。

ネットワーク認証サービスおよび EIM を構成してシングル・サインオンを使用可能にするには、ある会社がこの両方のプロダクトを構成した方法を示す『シナリオ: シングル・サインオンの使用可能化』を参照してください。

必要な iSeries ナビゲーター・オプションのインストール

EIM 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化するには、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 サーバーで作業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」**をクリックします。
2. ダイアログの指示に従ってください。**「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」**オプションを選択します。
   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ります。
3. 選択セットアップの残りを続行します。

ネットワーク認証サービスの構成

ネットワーク認証サービスを使用すると、ご使用の iSeries サーバー上で Kerberos 認証を使用することができます。このサービスは、ご使用のサーバー上で EIM を使用するための前提条件ではありません。ただし、ご使用のネットワーク内でセキュリティー用の Kerberos 認証を使用することには、多くの利点があります。

ネットワーク認証サービスは、EIM とともに使用するとき、シングル・サインオン環境を使用可能にする方法を提供します。シングル・サインオン環境は、ユーザーおよび管理者にとって利点となります。ユーザーは、管理しやすいようにあまり多くのユーザー名およびパスワードを持ちません。よって、管理者は、追跡すべきユーザー情報が少なくて済みます。シングル・サインオンの使用可能化は、ネットワーク内にある可能性のありうる複数のプラットフォームと異なるシステムとの間のギャップを埋める助けにもなるため、アプリケーション開発および一般管理コストを削減することができます。

ご使用の iSeries サーバー上またはご使用のネットワーク内のすべてのサーバー上にネットワーク認証サーバーがまだ構成されていない場合には、はじめに計画に関する情報を得るために、『ネットワーク認証サービスの計画』を参照してください。ネットワーク認証サービスに精通している場合は、構成プロセスを開始するために、『ネットワーク認証サービスの構成』を参照してください。

EIM の構成

基礎となるセキュリティー・ポリシーを変更しないでシングル・サインオン環境を複数のプラットフォーム間で使用可能にするには、ネットワーク認証サービスだけでなく、EIM も構成する必要があります。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。

iSeries サーバーをシングル・サインオン環境に加えるために EIM を構成するプロセスを開始するには、EIM 構成ウィザードを使用します。構成上のニーズに応じて、ウィザードを使用して既存のドメインを結合するか、新しいドメインを作成して結合することができます。

EIM 構成ウィザードを使用すれば、EIM の基本構成を簡単に完了できます。たとえば、まだ LDAP サーバーを構成していない場合や、ネットワーク認証サービスを構成していない場合は、EIM 構成ウィザードはこれらの作業を実行するのに役立ちます。

ウィザードを使用して EIM の基本構成を実行した後に、いくつかの追加の構成ステップを実行することでシングル・サインオン環境を使用することができるようになります。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』を参照してください。

EIM 構成ウィザードを使用する前に、 計画のすべてのステップを完了しておく必要があります。これは、シングル・サインオン環境を使用可能にするために、EIM とネットワーク認証サービスをどのように使用

するのかをはっきりと決めるためのステップです。計画が完了したら、ウィザードを使用して EIM を iSeries サーバー用に構成することができます。その際、新しいドメインを作成する方法と既存のドメインを結合する方法のどちらかを用います。次のトピックには、EIM を構成するための説明があります。

新しいドメインの作成と結合
この作業を実行して、ネットワーク用の EIM ドメインを作成し、 iSeries サーバーをそのドメインに参加させます。ウィザードは、新しいドメインを作成し、ローカル LDAP 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します。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。この作業が完了したら、他の iSeries サーバーをドメインに参加するように構成できます。そのためには、構成するサーバーに接続し、EIM 構成ウィザードで既存の EIM ドメインを結合します。

既存のドメインの結合
ドメイン・コントローラーと EIM ドメインを構成するために EIM ウィザードを使用した後で、この作業を実行して他の iSeries サーバーをドメインに参加するように構成します。この作業は、ネットワーク内の EIM を使用する iSeries サーバーごとに行う必要があります。ウィザードを完了した後、EIM ドメイン・コントローラーへの接続情報 (ポート番号や Transport Layer Security (TLS)/Secure Sockets Layer (SSL) を使用するかどうかなど) も含めて、結合するドメインについての情報を提供する必要があります。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 構成ウィザードにアクセスする方法

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. **「既存のドメインの結合 (Join an existing domain)」**または**「新しいドメインの作成と結合 (Create and join a new domain)」**パスを選択する。

EIM 構成ウィザードを使用してドメイン・コントローラーを作成し、 iSeries サーバーをドメインに参加するように構成し終えたら、EIM の構成を完了するために以下のタスクを実行する必要があります。

1. EIM ドメインへ EIM ドメインに参加させたい非 iSeries のサーバーとアプリケーション用の EIM レジストリーを追加する。
2. ドメインで EIM ドメインに参加するシステムの各固有ユーザーまたはエンティティー用の EIM ID を作成する。
3. 個人またはエンティティーのさまざまなユーザー ID と、これらの EIM ID 間のアソシエーションを作成する。

新しいドメインの作成と結合

EIM 構成ウィザードを使用して、 iSeries サーバー上の LDAP サーバーを、新しいドメイン用の EIM ドメイン・コントローラーになるように構成することができます。 EIM 構成ウィザードは必要な場合に、LDAP 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。このウィザードが完了すると、新しい EIM ドメインが構成され、新しいドメインに参加するように iSeries システムが構成され、指定したユーザー・レジストリーがドメインに追加されます。

この作業を行うためにウィザードを使用する場合は、セキュリティー管理者 (*SECADM)、全オブジェクト (*ALLOBJ)、およびシステム構成 (*IOSYSCFG) 特殊権限を持っている必要があります。

新しい EIM ドメインを作成して結合するために EIM 構成ウィザードを開始して使用するには、 iSeries ナビゲーターから以下のステップを完了してください。

注: また、このウィザードでは、ローカル LDAP サーバーが新しい EIM ドメイン・コントローラーとして構成されます。

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、**「構成... (Configure...)」**を選択し、EIM 構成ウィザードを立ち上げる。
3. ウィザードの**「ウェルカム (Welcome)」**ページで、**「新しいドメインの作成と結合 (Create and join a new domain)」**を選択して**「次へ」**をクリックする。
4. 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は、**「ネットワーク認証サービスの構成 (Network Authentication Services Configuration)」**ダイアログが表示される。このダイアログでは、ネットワーク認証サービスを構成するかどうかを尋ねるプロンプトが出されます。**「はい」**を選択すると、ネットワーク認証サービス構成ウィザードが起動します。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. ローカル LDAP サーバーが現在構成されていない場合は、**「ディレクトリー・サーバーの構成 (Configure Directory Server)」**ダイアログが表示される。ローカル LDAP サーバーを構成するには、ダイアログで以下の情報を提供します。
   - **「ポート (Port)」**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。
   - **「識別名 (Distinguished name)」**フィールドに、 LDAP サーバー用の LDAP 管理者を識別する LDAP 識別名 (DN) を入力する。 EIM 構成ウィザードは、この LDAP 管理者 DN を作成し、LDAP サーバーを作成中の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。
   - **「パスワード」**フィールドに、LDAP 管理者のパスワードを入力する。
   - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。
   - **「次へ」**をクリックする。
6. **「ドメイン・コントローラーの指定 (Specify Domain Controller)」**ダイアログで、以下の情報を指定する。
   - **「ドメイン (Domain)」**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。

- **「説明 (Description)」**フィールドに、ドメインを説明するテキストを入力する。
- **「次へ」**をクリックする。

7. **「ドメインの親 DN (Specify Domain Parent DN)」**ダイアログで、作成中のドメインの親 DN を指定するかどうかを選択する。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 (Yes)」**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。
8. **「接続に使用するユーザーの指定 (Specify User For Connection)」**ダイアログで、接続に使用する**「ユーザー・タイプ (user type)」**を選択する。「識別名とパスワード (Distinguished name and password)」、「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」、または「Kerberos プリンシパルとパスワード (Kerberos principal and password)」のいずれかのユーザー・タイプを選択できます。 2 つの Kerberos のユーザー・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。
   - **「識別名とパスワード (Distinguished name and password)」**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) を入力する。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、ユーザーのパスワードを入力する。
     - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。
   - **「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」**を選択する場合は、以下の情報を指定する。
     - **「keytab ファイル (Keytab file)」**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 iSeries サーバー上の keytab ファイル名の名前を入力する。あるいは、**「参照」**をクリックして keytab ファイルを選択します。
     - **「プリンシパル (Principal)」**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入力する。
     - **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。
   - **「Kerberos プリンシパルとパスワード (Kerberos principal and password)」**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、 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 Kerberos プリンシパルの名前を入力する。
     - **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。
     - **「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。
     - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。

- ドメイン・コントローラーに接続するためのユーザー構成情報をテストするために、**「接続の検査」**をクリックする。
- **「次へ」**をクリックする。

9. **「レジストリー情報 (Registry Information)」**ダイアログで、EIM ドメインに追加したいユーザー・レジストリーのタイプを選択する。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・レジストリーを表すユーザー・レジストリーを EIM ドメインに追加するには、**「OS400」**を選択する。表示されるフィールドに、ドメインに作成するレジストリーの名前を入力します。 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。
   - Kerberos ユーザー・レジストリーを EIM ドメインに追加するには、**「Kerberos」**を選択する。表示されるフィールドに、ドメインに作成するレジストリーの名前を入力し、必要に応じて**「Kerberos ユーザー ID の大文字小文字を区別する (Kerberos user identities are case sensitive)」**を選択します。
   - **「次へ」**をクリックする。
10. **「EIM システム・ユーザーの指定 (Specify EIM System User)」**ダイアログで、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のタイプを選択する。これらの操作には、ローカル OS/400 ユーザー・プロファイルを削除する場合のルックアップのマッピングとアソシエーションの削除が含まれます。「識別名とパスワード (Distinguished name and password)」、「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」、または「Kerberos プリンシパルとパスワード (Kerberos principal and password)」のいずれかのユーザー・タイプを選択できます。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: 指定するユーザーは、少なくとも、ルックアップのマッピングを実行する権限と、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。

11. **「識別名とパスワード (Distinguished name and password)」**を選択する場合は、以下の情報を指定する。
    - **「識別名 (Distinguished name)」**フィールドに、EIM ドメイン・コントローラーに接続する時に使用する OS/400 のユーザーを識別する LDAP 識別名を入力する。
    - **「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。
    - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。
12. **「Kerberos プリンシパルとパスワード (Kerberos principal and password)」**を選択する場合は、以下の情報を指定する。
    - **「プリンシパル (Principal)」**フィールドに、EIM ドメイン・コントローラーに接続する時に使用する OS/400 のユーザーを識別する Kerberos プリンシパルの名前を入力する。
    - **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。
    - **「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。
    - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。

13. **「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」**を選択する場合は、以下の情報を指定する。
    - **「Keytab ファイル (Keytab file)」**フィールドに、EIM ドメイン・コントローラーに接続する時に使用する OS/400 のユーザーを識別する iSeries サーバー上の keytab ファイル名を入力する。あるいは、**「参照」**をクリックして keytab ファイルを選択します。
    - **「プリンシパル (Principal)」**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入力する。
    - **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。
14. 作成したシステム・ユーザーのドメイン・コントローラーへの接続をテストするために、**「接続の検査」**をクリックします。
15. **「次へ」**をクリックする。
16. **「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」**をクリックします。

ウィザードが終了したら、基本の EIM 構成は終了です。しかし、このサーバーの 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. 「EIM ドメイン管理 (EIM Domain Management)」フォルダーに、作成したドメインを追加する。
2. EIM ドメインへ EIM ドメインに参加させたい他のサーバーとアプリケーション用の EIM レジストリーを追加する。
3. ドメインで EIM ドメインに参加するシステムの各固有ユーザーまたはエンティティー用の EIM ID を作成する。
4. 個人またはエンティティーのさまざまなユーザー ID と、これらの EIM ID 間のアソシエーションを作成する。

さらに、ドメイン・コントローラーへのセキュア接続を構成するために、Secure Sockets Layer (SSL) または Transport Layer Security (TLS) を使用することができます。

EIM ドメイン・コントローラーへのセキュア接続の構成

新しいドメインを作成して結合するのウィザードでの作業を終了したら、EIM ドメイン・コントローラーへのセキュア接続を確立するために、 Secure Sockets Layer (SSL) または Transport Layer Security Protocol (TLS) を使用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. LDAP サーバー・ドメイン・コントローラーで SSL を使用可能にする。
2. ディレクトリー・サーバーが SSL に使用する必要のある証明書を作成するためにディジタル証明書マネージャー (DCM) を使用する。
3. LDAP サーバーに対して、証明書を割り当てるために DCM を使用する。
4. 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する。
5. 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。

既存のドメインの結合

EIM 構成ウィザードを使用して、既存の EIM ドメインを結合することができます。ネットワークにすでに EIM ドメインとドメイン・コントローラーが構成されている場合は、EIM 構成ウィザード内のこのオプションを使用します。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。ウィザードはこの情報を iSeries サーバー上に保管します。そして、この情報を使用して EIM ドメイン・コントローラーに接続します。また、ウィザードはこの iSeries サーバー上の OS/400 ユーザー・プロファイル・レジストリーを表す EIM ユーザー・レジストリーを作成します。

ウィザードを使用してこのタスクを完了するには、セキュリティー管理者 (*SECADM) および全オブジェクト (*ALLOBJ) 特殊権限を持っていなければなりません。

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、 iSeries ナビゲーターを使用して以下のステップを実行してください。

1. **「ネットワーク」—>「エンタープライズ識別マッピング」**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 構成ウィザードを立ち上げる。ウィザードが開始したら、順番に表示されるダイアログに以下の情報を指定します。
3. ウィザードの**「ウェルカム」**ダイアログで、**「既存のドメインの結合 (Join an existing domain)」**を選択して**「次へ」**をクリックする。
4. 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は、**「ネットワーク認証サービスの構成 (Network Authentication Services Configuration)」**ダイアログが表示される。このダイアログでは、ネットワーク認証サービスを構成するかどうかを尋ねるプロンプトが出されます。**「はい」**を選択すると、ネットワーク認証サービス構成ウィザードが起動します。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. **「ドメイン・コントローラーの指定 (Specify Domain Controller)」**ダイアログが表示されたら、以下の情報を指定する。
   - **「ドメイン・コントローラー名 (Domain controller name)」**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。
   - ドメイン・コントローラーからの EIM 情報の検索の際に SSL が使用されるようにして EIM データの伝送を保護する場合は、**「Secure Sockets Layer (SSL) を使用する (Use Secure Sockets Layer (SSL))」**をクリックする。
   - **「接続の検査」**をクリックして、ドメイン・コントローラーの構成情報を検査する。

注: SSL を使用することを指定した結果、エラー・メッセージを受け取った場合、そのエラー・メッセージは、LDAP サーバーが SSL を使用するように構成されていないことを示している可能性があります。

   - **「次へ」**をクリックする。
6. **「接続に使用するユーザーの指定 (Specify User For Connection)」**ダイアログで、接続に使用する**「ユーザー・タイプ (user type)」**を選択する。「識別名とパスワード (Distinguished name and password)」、「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」、または「Kerberos プリンシパルとパスワード (Kerberos principal and password)」のいずれかのユーザー・タイプを選択できます。 2 つの Kerberos のユーザー・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。
   - **「識別名とパスワード (Distinguished name and password)」**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)を入力する。
– **「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。
– **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。

- **「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」**を選択する場合は、以下の情報を指定する。
  – **「keytab ファイル (Keytab file)」**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 iSeries サーバー上の keytab ファイル名の名前を入力する。あるいは、**「参照」**をクリックして keytab ファイルを選択します。
  – **「プリンシパル (Principal)」**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入力する。
  – **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。
- **「Kerberos プリンシパルとパスワード (Kerberos principal and password)」**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、 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 Kerberos プリンシパルの名前を入力する。
  – **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。
  – **「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。
  – **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。
- ドメイン・コントローラーに接続するためのユーザー構成情報をテストするために、**「接続の検査」**をクリックする。
- **「次へ」**をクリックする。

7. **「ドメインの指定 (Specify Domain)」**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。
8. **「レジストリー情報 (Registry Information)」**ページで、EIM ドメインに追加したいユーザー・レジストリーのタイプを選択する。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・レジストリーを表すユーザー・レジストリーを EIM ドメインに追加するには、**「OS400」**を選択する。表示されるフィールドに、ドメインに作成するレジストリーの名前を入力します。 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。
   - Kerberos ユーザー・レジストリーを EIM ドメインに追加するには、**「Kerberos」**を選択する。表示されるフィールドに、ドメインに作成するレジストリーの名前を入力し、必要に応じて**「Kerberos ユーザー ID の大文字小文字を区別する (Kerberos user identities are case sensitive)」**を選択します。デフォルト値の「Kerberos レジストリー名をレルム名と同じにする (the Kerberos registry name is the same as the realm name)」を受け入れることができます。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。 EIM 内でユーザー・レジストリーを定義する方法の詳細は、『EIM レジストリー定義』を参照してください。

- **「次へ」**をクリックする。

9. **「EIM システム・ユーザーの指定 (Specify EIM System User)」**ダイアログで、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のタイプを選択する。これらの操作には、ローカル OS/400 ユーザー・プロファイルを削除する場合のルックアップのマッピングとアソシエーションの削除が含まれます。「識別名とパスワード (Distinguished name and password)」、「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」、または「Kerberos プリンシパルとパスワード (Kerberos principal and password)」のいずれかのユーザー・タイプを選択できます。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。
   - **「識別名とパスワード (Distinguished name and password)」**を選択する場合は、以下の情報を指定する。
     - **「識別名 (Distinguished name)」**フィールドに、EIM ドメイン・コントローラーに接続する時に使用する OS/400 のユーザーを識別する LDAP 識別名を入力する。
     - **「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。
     - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。
   - **「Kerberos プリンシパルとパスワード (Kerberos principal and password)」**を選択する場合は、以下の情報を指定する。
     - **「プリンシパル (Principal)」**フィールドに、EIM ドメイン・コントローラーに接続する時に使用する OS/400 のユーザーを識別する Kerberos プリンシパルの名前を入力する。
     - **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。
     - **「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。
     - **「パスワードの確認 (Confirm password)」**フィールドに、パスワードを再入力する。プリンシパルおよびレルムの名前は、keytab 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、keytab ファイル内で jsmith@ordept.myco.com と表されます。
   - **「Kerberos keytab ファイルとプリンシパル (Kerberos keytab file and principal)」**を選択する場合は、以下の情報を指定する。
     - **「Keytab ファイル (Keytab file)」**フィールドに、EIM ドメイン・コントローラーに接続する時に使用する OS/400 のユーザーを識別する iSeries サーバー上の keytab ファイル名を入力する。あるいは、**「参照」**をクリックして keytab ファイルを選択します。
     - **「プリンシパル (Principal)」**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入力する。
     - **「レルム (Realm)」**フィールドに、プリンシパルの Kerberos レルムの名前を入力する。
   - 作成したシステム・ユーザーの接続をテストするために、**「接続の検査」**をクリックします。
   - **「次へ」**をクリックする。
10. **「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」**をクリックします。

ウィザードが終了したら、基本の EIM 構成は終了です。しかし、このサーバーの 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. 「EIM ドメイン管理 (EIM Domain Management)」フォルダーに、結合したドメインを追加する。

2. EIM ドメインへ EIM ドメインに参加させたい非 iSeries のサーバーとアプリケーション用の EIM レジストリーを追加する。
3. EIM ドメインで EIM ドメインに参加するシステムの各固有ユーザーまたはエンティティー用の EIM ID を作成する。
4. 個人またはエンティティーのさまざまなユーザー ID と、これらの EIM ID 間のアソシエーションを作成する。

また、シングル・サインオン環境を使用可能にするには、iSeries サーバー用にネットワーク認証サービスを構成する必要があります。

EIM の管理

iSeries サーバーに EIM を構成した後は、EIM ドメインと情報を管理するための多くのタスクを実行できるようになります。以下のトピックでは、 iSeries システム上とネットワーク・エンタープライズ内の EIM の管理に使用する特定のタスクについて説明します。

EIM ドメインの管理
EIM ドメインと EIM ドメイン・プロパティーに含まれる EIM 情報を処理します。

アソシエーションの管理
エンタープライズ内のすべてのユーザーのユーザー ID 対 EIM ID のアソシエーションを保守します。

EIM ID の管理
エンタープライズ内のユーザーと関連付けられた EIM ID を保守します。

EIM ユーザー権限の管理
EIM 権限を操作してユーザーが実行できる EIM の機能と操作を制御することによって、EIM 情報のセキュリティーを保守します。

ユーザー・レジストリーの管理
EIM ドメインに追加したユーザー・レジストリーを操作します。

EIM ドメインの管理

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。 新しい EIM ドメインを作成して構成した後は、そのドメイン内の情報を管理するためにそれを「ドメイン管理」フォルダーに追加する必要があります。

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、どの iSeries 接続を使用しても管理できます。ドメインを管理するために、iSeries ナビゲーターが接続している iSeries がそのドメインに参加している必要はありません。

EIM ドメインの管理で完了する必要のあるタスクは、以下のとおりです。

- 「ドメイン管理」へのドメインの追加
- ドメインへの接続
- ドメインの削除
- 「ドメイン管理」からのドメインの除去

「ドメイン管理」へのドメインの追加

ドメインを追加するには、*SECADM 特殊権限を持っている必要があります。既存の EIM ドメインを「ドメイン管理」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... (Add Domain...)」**を選択する。
3. 必要なドメインと接続情報を指定する。
4. **「OK」**をクリックしてドメインを追加する。

ドメインへの接続

作業する EIM ドメインに現行で接続していない場合は、まずそのドメイン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選択する。処理したいドメインがリストされていない場合、「ドメイン管理」へのドメインの追加を行う必要があります。
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... (Connect...)」**を選択する。
4. 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。
5. **「OK」**をクリックする。

ドメインの削除

このタスクを完了するには、 LDAP 管理者または EIM 管理者のいずれかの権限を持っていなければなりません。 EIM ドメインを削除する前に、まずすべてのレジストリーと EIM ID 情報をドメインから除去する必要があります。

EIM ドメインを削除するには、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. すべてのユーザー・レジストリーを EIM ドメインから除去する。
3. すべての EIM ID を EIM ドメインから削除する。
4. 削除するドメインを右マウス・ボタン・クリックし、**「削除... (Delete...)」**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。

「ドメイン管理」からのドメインの除去

必須ではありませんが、変更を加えるときに EIM ドメインを「ドメイン管理」フォルダーから除去することができます。

ドメインを除去するには、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」**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... (Remove Domain...)」**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。

アソシエーションの管理

アソシエーションは、レジストリー内の EIM ID とユーザー ID の間の関係を定義します。たとえば、OS/400 ユーザー・プロファイルや Kerberos プリンシパルと EIM ID の間にアソシエーションを作成できます。そして、このアソシエーションは、どの EIM ID がローカル iSeries ユーザー・プロファイルや Kerberos プリンシパルに対応しているのかを判別するために使用することができます。

ユーザー ID の適切な EIM ID と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。

さらに、アソシエーションを管理することにより、ネットワークでシングル・サインオンを使用可能にすることのメリットを享受できます。安全なシングル・サインオン・ネットワークをインプリメントする場合、現行のアソシエーションを保持していることは重要です。

作成できるアソシエーションには、ソース、ターゲット、管理という 3 つのタイプがあります。ユーザー ID と適切な EIM ID の間のアソシエーションを作成または保守するには、以下のタスクを実行します。

- アソシエーションの作成
- アソシエーションの削除

アソシエーションの作成

シングル・サインオン環境を使用可能にするには、種々の個人またはエンティティーであるユーザー ID と、単一の個人またはエンティティーとして、EIM ID とアソシエーションを作成する必要があります。ターゲット、ソース、管理という 3 つのタイプのアソシエーションを作成できます。

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、 ID 管理者または EIM 管理者のいずれかの権限を持っていなければなりません。ターゲット・アソシエーションを作成するには、すべてのレジストリーのレジストリー管理者か、特定のレジストリーのレジストリー管理者か、あるいは EIM 管理者の権限を持っていなければなりません。

EIM ID のアソシエーションを作成するには、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. 作業したい EIM ドメインに接続する必要がある。
   - 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、『ドメインへの接続』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 EIM ID のリストを表示する。
5. 適切な EIM ID を右マウス・ボタン・クリックして、**「プロパティー... (Properties...)」**を選択する。
6. **「アソシエーション」**タブをクリックする。
7. **「追加... (Add...)」**をクリックして**「アソシエーションの追加 (Add association)」**ダイアログを表示する。
8. フィールドを埋めるために詳しい情報が必要な場合は、**「ヘルプ」**をクリックする。
9. 必要な情報を指定したら、**「OK」**をクリックする。

アソシエーションの削除

管理またはソース・アソシエーションを削除するには、 ID 管理者または EIM 管理者の権限を持っていなければなりません。ターゲット・アソシエーションを削除するには、選択されたレジストリー (作業したいレジストリーを含む) の管理者か、レジストリー管理者か、あるいは EIM 管理者の権限を持っていなければなりません。

アソシエーションを除去するには、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. 作業したい EIM ドメインに接続する必要がある。
   - 処理したい EIM ドメインが「ドメイン管理」の下にリストされていない場合は、『「ドメイン管理」へのドメインの追加』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、『ドメインへの接続』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。
5. 必要な 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. **「アソシエーション」**タブをクリックして、EIM ID の現行のアソシエーションを表示する。
7. 除去するアソシエーションを選択する。
8. **「除去 (Remove)」**をクリックしてアソシエーションを除去する。
9. **「OK」**をクリックする。

EIM ID の管理

セキュリティーのため、ネットワーク内のユーザーを表す EIM ID の保守は重要です。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、エリアの間を移動するユーザーがいます。このような変化のために、ユーザーのアカウントとネットワーク内のシステムへのアクセスをトラッキングする必要があります。 EIM ID を作成してそれを各ユーザーのユーザー ID に関連付けると、このトラッキング・タスクは容易になります。

シングル・サインオンを使用可能にすると、ユーザーがエンタープライズ内の他の部門またはエリアに移動する場合にも、そのタスクはより簡単になります。また、ユーザーのセキュリティー許可やシステム・アクセス要件が変更されていることもあります。シングル・サインオンを使用可能にすれば、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はなくなります。

エンタープライズ内のユーザーの EIM ID の管理には、おそらく平常的な多数のタスクが含まれます。ネットワークおよびドメイン内の EIM ID の管理には、以下のタスクを使用することができます。

- EIM ID の作成
- EIM ID への別名の追加
- EIM ID の削除

アソシエーションに管理については、『アソシエーションの管理』を参照してください。

EIM ID の作成

EIM ID を作成するには、ID 管理者か EIM 管理者のいずれかの権限を持っていなければなりません。

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. 作業したい EIM ドメインに接続する必要がある。
   - 作業したい EIM ドメインが**「ドメイン管理」**の下にリストされていない場合は、『「ドメイン管理」へのドメインの追加』を参照してください。
   - 作業したい EIM ドメインに現行で接続していない場合は、『ドメインへの接続』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. いずれかのフィールドに関する詳しい情報が必要な場合は、**「ヘルプ」**をクリックする。
6. 必要な情報を指定したら、**「OK」**をクリックする。

EIM ID への別名の追加

EIM ID 用の付加的な識別情報を提供するために、別名を作成することができます。別名を使用すれば、ある EIM ID と別の EIM ID を区別することができます。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。

ID に別名を追加するには、ID 管理者か EIM 管理者のいずれかの権限を持っていなければなりません。

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. 作業したい EIM ドメインに接続する必要がある。
   - 処理したい EIM ドメインが「ドメイン管理」の下にリストされていない場合は、『「ドメイン管理」へのドメインの追加』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、『ドメインへの接続』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. 必要な 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。 EIM ID が存在しない場合は、『EIM ID の作成』を参照してください。
5. この EIM ID に追加したい別名を指定して**「追加」**をクリックする。
6. **「OK」**をクリックして変更内容を保管する。

EIM ID の削除

EIM ID を削除するには、EIM 管理者権限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. 作業したい EIM ドメインに接続する必要がある。
   - 処理したい EIM ドメインが「ドメイン管理」の下にリストされていない場合は、『「ドメイン管理」へのドメインの追加』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、『ドメインへの接続』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。
5. 削除する 1 つ以上の EIM ID を選択する。

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 (Yes)」**をクリックして、選択した EIM ID を除去する。

EIM ユーザー権限の管理

EIM は、ドメイン内で各種の操作を実行するのに必要な各種の EIM 権限を定義します。この操作には、ID の作成、レジストリーのリスト、およびマッピング・ルックアップ操作の実行などのドメイン管理機能が含まれます。 他のユーザーの権限の認可や取り消しを行うことを許されているのは、EIM 管理者権限を持っているユーザーのみです。

各権限グループの簡単な定義および各権限が使用できる特定の EIM 機能の詳細については、『EIM 権限』を参照してください。

ユーザーの EIM 権限を変更するには、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. 作業する EIM ドメインを展開する。このドメインに現在接続していない場合は、接続することを求めるプロンプトが出されます。 EIM 管理者権限を持つユーザーでドメインに接続するようにしてください。
3. EIM ドメインを右マウス・ボタン・クリックして、**「権限... (Authority...)」**を選択する。
4. **「EIM 権限の編集 (Edit EIM Authority)」**ダイアログで、EIM 権限を変更するユーザーを指定する。
5. **「OK」**をクリックする。
6. **「EIM 権限の編集 (Edit EIM Authority)」**ダイアログで、ユーザーの権限に必要な変更を行う。
7. 完了したら**「OK」** をクリックして、権限に対する変更を保管する。

ユーザー・レジストリーの管理

ユーザー・レジストリーに含まれている ID と該当する EIM ID 間のアソシエーションを作成できるようにするには、その前にまず EIM ドメインにユーザー・レジストリーを定義しなければなりません。

以下のタスクは、EIM ドメイン中のユーザー・レジストリー管理の一部です。

- ユーザー・レジストリーの追加
- 別名のユーザー・レジストリーへの追加
- EIM 中の専用ユーザー・レジストリー・タイプの定義
- ユーザー・レジストリーの除去
- 別名のユーザー・レジストリーからの除去

ユーザー・レジストリーの追加

ユーザー・レジストリーを追加するには、EIM 管理者権限を持っている必要があります。この権限およびこの権限を持つユーザーが利用できるアクセスの詳細については、『EIM 権限』を参照してください。

EIM ドメインにユーザー・レジストリーを追加するには、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. EIM 管理者権限のあるユーザーで、EIM ドメインに接続する。
   - 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、『ドメインへの接続』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」**を右クリックして、**「レジストリーの追加... (Add Registry...)」**を選択する。
5. 必要なユーザー・レジストリー情報を指定する。また、ユーザー・レジストリーの別名情報も指定できます。
6. **「OK」**をクリックして、情報を保管し、ユーザー・レジストリーを EIM ドメインに追加する。

別名のユーザー・レジストリーへの追加

管理者またはアプリケーション開発者は、別名を作成して、ユーザー・レジストリーに関する追加の識別情報を提供することができます。 その後、他のユーザーたちは別名を使用して、ユーザー・レジストリー同士を区別できます。たとえば、アプリケーション開発者や管理者はユーザー・レジストリーに関する別名を使用して、アプリケーションで使用する必要のある EIM レジストリーを伝達します。別名をユーザー・レジストリーとともに使用する方法の詳細については、『EIM レジストリー定義』を参照してください。

ユーザー・レジストリーに別名を追加するには、EIM 管理者、すべてのレジストリーに関するレジストリー管理者、またはこのタスクの実行対象にする特定のレジストリーに関するレジストリー管理者のうちの、いずれかの権限がなければなりません。

EIM ドメイン中のユーザー・レジストリー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. 作業したい EIM ドメインに接続する必要がある。
   - 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、『ドメインへの接続』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、ドメイン中のレジストリーのリストを表示する。
5. 別名の追加先のユーザー・レジストリーを右クリックして、**「プロパティー...」**を選択する。
6. **「プロパティー」**ダイアログの**「別名」**タブをクリックする。
7. 追加したい別名の名前とタイプを指定する。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。
8. **「追加」**をクリックする。
9. **「OK」**をクリックして変更内容を保管する。

EIM 中の専用ユーザー・レジストリー・タイプの定義

EIM 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** は値 **caseExact** か値 **caseIgnore** のどちらかになります。たとえば、OS/400 の 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することができます。

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。 ANSI の Web サイト (http://web.ansi.org/public/services/reg_org.html) の意思決定用紙を利用して、メールで申込書を取り寄せられます。組織向けの ANSI の 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 2.16.840.1.NEWNUM を作成します。
- 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。国家の ISO 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。
- 別の方法として、ISO DCC NSAP スキームの International Register が第一歩になるかもしれません。NSAP はネットワーク・サービス・アクセス・ポイント (Network Service Access Point) のことで、さまざまな国際規格で使用されています。スキームのレジストリーは、 http://www.fei.org.uk の ISO DCC NSAP という見出しの下で取得できます。この Web サイトには現在 13 の命名機関の連絡先情報がリストされており、その一部は OID の割り当ても行っています。
- 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。申込ページは、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。

証明書ポリシーの OID について詳しくは、 http://csrc.nist.gov/csor/pkireg.htm を参照してください。

ユーザー・レジストリーの除去

EIM ドメインからユーザー・レジストリーを除去すると、ユーザー・レジストリー中のユーザー ID の EIM ID とのアソシエーションがすべて失われます。ユーザー・レジストリーを除去してから、再度ユーザー・レジストリーを EIM ドメイン中に追加し直しても、アソシエーションの関係はリセットされません。

ユーザー・レジストリーを削除するには、EIM 管理者権限を持っている必要があります。

ユーザー・レジストリーを除去するには、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. 作業したい EIM ドメインに接続する必要がある。
   - 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、『ドメインへの接続』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、ドメイン中のユーザー・レジストリーのリストを表示する。
5. 除去したいユーザー・レジストリーを右クリックして、**「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、ユーザー・レジストリーを削除する。

別名のユーザー・レジストリーからの除去

ユーザー・レジストリーから別名を削除するには、レジストリー管理者権限、選択レジストリー (処理したいレジストリーを含む) の管理者権限、または EIM 管理者権限がなければなりません。

EIM ドメイン中のユーザー・レジストリー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. 作業したい EIM ドメインに接続する必要がある。
   - 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、『ドメインへの接続』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、ドメイン中のレジストリーのリストを表示する。
5. 別名を除去する対象のユーザー・レジストリーを右クリックして、**「プロパティー」**を選択する。
6. **「プロパティー」**ダイアログの**「別名」**タブをクリックする。
7. 除去したい別名を選択して、**「除去」**をクリックする。
8. **「OK」**をクリックして変更内容を保管する。

EIM の API

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。

EIM API は、以下の 4 つ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 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。

iSeries サーバーで使用できる EIM API の詳細と完全なリストについては、『Enterprise Identity Mapping (EIM) APIs』のトピックを参照してください。

EIM のトラブルシューティング

EIM 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。問題のトラブルシューティングを行う方法は多数あるので、以下のトピックに、発生する可能性のある共通エラーの一部に対してトラブルシューティングや修正を行う方法に関する詳細や指示が記載されています。

- ドメイン・コントローラーに接続できない
- EIM ID のリスト表示に長時間かかる
- 終了処理中に EIM 構成ウィザードがハングする
- EIM ハンドルが有効でなくなった
- Kerberos 認証および診断メッセージ

ドメイン・コントローラーに接続できない

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。以下の項目を検査すると、問題の原因を検出するのに役立ちます。

- 以下の項目について、指定されている情報が正しいかどうかを検査する。
  - ドメイン・コントローラー名
  - 指定ポート
  - ユーザー ID およびパスワード
- ドメイン・コントローラーがアクティブになっているかどうかを検査する。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」—>「TCP/IP」**を展開する。

2. 「ディレクトリー・サーバー (Directory Server)」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、**「ディレクトリー・サーバー (Directory Server)」**を右クリックして、**「開始... (Start...)」**を選択する。

ドメイン・コントローラーがアクティブになったら、ドメインへの再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. 接続するドメインを選択する。 EIM ドメインがリストされていないか、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」へのドメインの追加』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、**「接続... (Connect...)」**を選択する。
4. 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。
5. **「OK」**をクリックする。

EIM ID のリスト表示に長時間かかる

iSeries ナビゲーターの「ID」フォルダーをオープンする際に、 ID のリストを生成するのに長時間かかることがあります。ドメイン中に多数の EIM ID がある場合は、EIM のリストを表示する際の検索基準を狭めることもできます。

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、**「このビューの最適化」—>「組み込み...」**を選択する。
4. 必要な表示基準を指定する。ワイルドカード文字として (*) 文字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。すべての EIM ID を表示したい場合は、上記のステップを使用して、ビューの最適化オプションとして**「すべての ID (All Identifiers)」**を選択してください。

終了処理中に EIM 構成ウィザードがハングする

終了処理中にウィザードが停止したように見える場合、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機している可能性があります。 LDAP サーバーの始動時にエラーが起きなかったかどうかを検査してください。 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 ハンドルが有効でなくなった

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ユーザーが受け取った場合は、ドメイン・コントローラーに対する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. 処理したいドメインを右クリックして、**「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。

Kerberos 認証および診断メッセージ

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は、認証や ID マッピング操作が失敗するたびに、診断メッセージ CPD3E3F がジョブ・ログに書き込まれます。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。

EIM の関連情報

EIM 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うえで参考になります。

- **ネットワーク認証サービスの構成**
  このトピックには、iSeries でのネットワーク認証サービスの構成に関する情報があります。ネットワーク認証サービスによって、iSeries は既存の Kerberos ネットワークに加わることができます。 EIM で使用する場合、ネットワーク認証サービスはシングル・サインオンを提供します。
- **ディレクトリー・サービスの構成 (LDAP)**
  このトピックには、ディレクトリー・サービス (LDAP) の構成や概念に関する情報があります。 EIM は LDAP サーバーを使用して EIM データおよびマッピング・アソシエーションを保管します。

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