ORACLE
FUSION MIDDLEWARE
IDENTITY AND ACCESS
MANAGEMENT SUITE

Oracle Directory Services の Oracle Database Enterprise User Security との統合

Oracle ホワイト・ペーパー | 2015 年 2 月

ORACLE

免責事項

下記事項は、弊社の一般的な製品の方向性に関する概要を説明するものです。また、情報提供を唯一の目的とするものであり、いかなる契約にも組み込むことはできません。以下の事項は、マテリアルやコード、機能を提供することをコミットメント（確約）するものではないため、購買決定を行う際の判断材料になさらないで下さい。オラクルの製品に関して記載されている機能の開発、リリース、および時期については、弊社の裁量により決定されます。

目次

はじめに

IT 部門は、コストを削減し、セキュリティを強化し、コンプライアンスを改善して、ますます競争が激しくなるビジネスをサポートするよう常に迫られています。データベースはエンタープライズ IT インフラストラクチャの主要な要素であり、データベースのユーザーと権限をエンタープライズ ID 管理フレームワークに統合して一元化することが重要です。

しかし、現在でも多くの企業では、データベースごとにユーザーおよび権限を管理しています。これは、エンドユーザーの観点では、各ユーザーが複数のパスワードを覚えておく必要があることになります。管理者の観点では、冗長なユーザー管理によりコストが高くなり、複数のデータベースでユーザー認可を管理するためエラーが発生しやすくなります。また、監査およびコンプライアンスの観点では、データベース全体のユーザー・アクセスおよび権限を予定どおりにプロビジョニング/プロビジョニング解除することが困難になります。

Oracle Database Enterprise Edition の Enterprise User Security（EUS）機能は Oracle Directory Services を利用して、データベース・ユーザーとロール・メンバーシップを LDAP ディレクトリで一元管理できます。EUS を使用すると、管理コストが削減され、セキュリティが強化されます。また、データベース・ユーザー・アカウント管理、データベース・ユーザーのプロビジョニング/プロビジョニング解除、パスワード管理およびセルフサービス式のパスワード・リセット、グローバル・データベース・ロールを使用した認可管理を一元化することで、コンプライアンスも改善します。さらに EUS は、LDAP 準拠のディレクトリに定義され、ユーザー・エントリに格納されたパスワード・ポリシー（アカウントのロックアウト、パスワードの有効期限設定など）を使用できます。

このホワイト・ペーパーでは、Oracle Unified Directory（OUD）および Oracle Internet Directory（OID）を使用する EUS デプロイメント・オプションについて説明します。このドキュメントでは、両方のユースケースを紹介します。OUD と OID は、データベースのユーザーおよび権限の中央ディレクトリ・リポジトリとして使用できます。また、Microsoft Active Directory（AD）、Novell eDirectory、Oracle Directory Server Enterprise Edition（ODSEE）、さらには OUD に基づく既存のディレクトリ・インフラストラクチャを利用する、EUS ディレクトリの仮想化サービスとしての使用も可能です。

OUDを使用したDBアカウントの一元化

➔ OUDに格納されたDBアカウント

OUD は、EUS とシームレスに連携します。データベースのユーザー情報、パスワード、およびデータベースまたはデータベース・ドメインに対する権限情報を OUD に格納できます。

EUS は OUD に格納された既存のユーザーおよびグループ情報を利用して、シングル・パスワード認証、およびエンタープライズ・アプリケーション全体での一貫したパスワード・ポリシーを提供できます。ユーザー・データ、データベース・メタデータ（DB 登録情報など）、ユーザー/ロール・マッピング、その他の EUS 固有のメタデータが、特別な LDAP スキーマを使用して OUD に格納されます。この LDAP スキーマは、すぐに使用でき、サポートされています。これらのメタデータは OracleContext と呼ばれる個別の OUD サフィックスに格納されるため、EUS データとアプリケーション全体で共有されるユーザー情報をクリーンかつ論理的に分離できます。

EUS は、データベース・ユーザーの一元管理に加え、3 つの異なるユーザー認証方法を提供します。

1. X.509 証明書認証（Oracle8i Database で導入）
2. パスワードベース認証（Oracle9i Database 以降）
3. Kerberos 認証（Oracle Database 10g 以降）

OUD による EUS 向けパスワードベース認証のサポートは、OUD 11g Release 2（11.1.2.0.0）で導入されました。その他の認証方法は OUD 11g Release 2 PS1（11.1.2.1）で導入されました。

パスワード認証のシナリオでは、データベースは OUD にバインドされた LDAP によるユーザー認証を実行しません。その代わりに、ユーザー資格証明の読取り、パスワードのハッシュ化、OUD から取得したパスワード・ハッシュ値の比較を実行します。EUS について詳しくは、Oracle Technology Network のデータベース・ドキュメント・セクションにある、エンタープライズ・ユーザー管理者ガイドを参照してください。

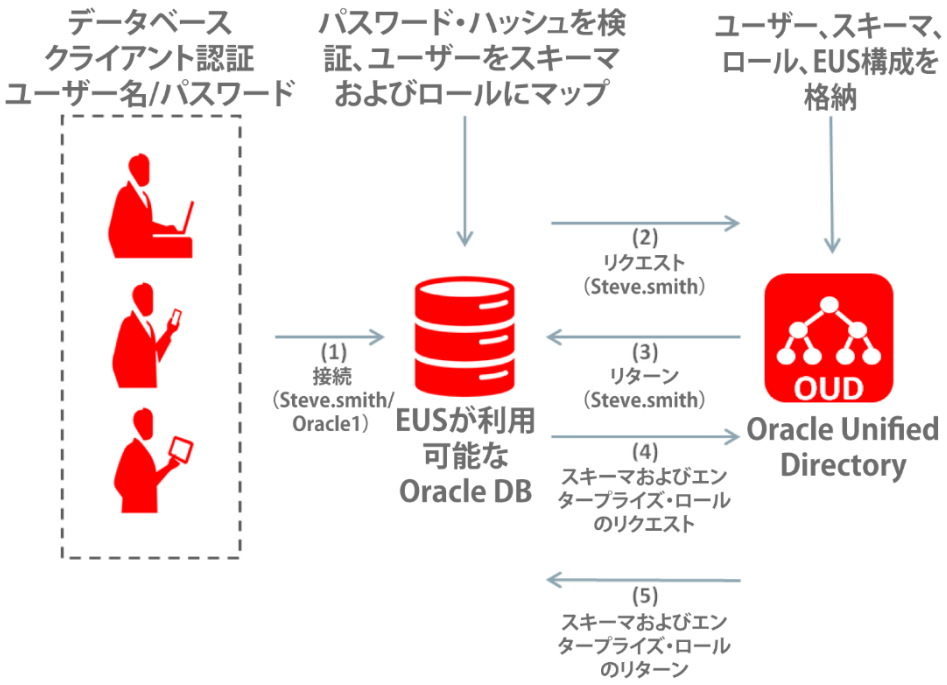

図1：OUDを使用したEUSのアカウント管理

➔ OUDから既存のディレクトリに引き渡されるDBアカウント

多くの企業にはすでに既存の企業ディレクトリがあるため、顧客は EUS を使用して、ディレクトリ間の同期を実施せず、既存のディレクトリ・インフラストラクチャおよびユーザー情報ベースを利用することもできます。この方法では、OUD はユーザー・データへの Oracle データベース情報のリクエストに対するリアルタイムのインタプリタとして動作します。

OUD を使用すると、データベースはサード・パーティのディレクトリとやり取りできます。OUD は、LDAP リクエスト/レスポンスをサード・パーティ・ディレクトリに格納されているユーザー・データとの間でやり取りすることにより、既存のサード・パーティ・ディレクトリ・インフラストラクチャ内の既存のユーザーおよびグループ情報を利用します。データベース・メタデータ（DB 登録情報など）、ユーザー/ロール・マッピング、その他の EUS 固有のメタデータは、OUD 内にローカルに格納されます。既存のサード・パーティ・ディレクトリに EUS 構成を格納するためのスキーマ変更は必要ありません。

OUD 11g Release 2 PS1 は、EUS での Active Directory、Oracle Directory Server Enterprise Edition、Novell eDirectory のサポートを認定しています。これらの製品を使用すると、ユーザー・データの重複および同期を排除でき、結果的に総所有コスト（TCO）を削減できます。

Microsoft Active Directoryのアカウント

パスワードベース認証向けに Active Directory と統合する、または、Active Directory と統合して Kerberos 認証を使用することができます。

パスワードベース認証向けのActive Directory統合

このシナリオでは、追加のコンポーネントである OUD パスワード変更通知プラグイン（`oidpwdcn.dll`）のデプロイが必要です。Microsoft は独自の実装を使用して、Active Directory のパスワードをハッシュ化します。これは、Oracle DB の要件と互換性がありません。OUD パスワード変更通知プラグインは、パスワードが変更されたときに通知を受け、Active Directory にハッシュを格納します。oidpwdcn DLL は、すべての Active Directory ドメイン・コントローラにインストールする必要があります。

Active Directory スキーマ拡張には、ハッシュ化されたパスワードを格納する必要があります。

データベースは OUD への接続を確立します。OUD はユーザー・データ（ユーザーおよびグループ）を Active Directory から取得します。ユーザー・パスワードは、OUD パスワード変更通知プラグインによって格納されたハッシュ化パスワードから取得されます。EUS メタデータは OUD に格納され、OUD から取得されます。

データベース・バージョンは 10.1 以降である必要があります。それより前のバージョンは、パスワード形式が異なり、互換性がありません。

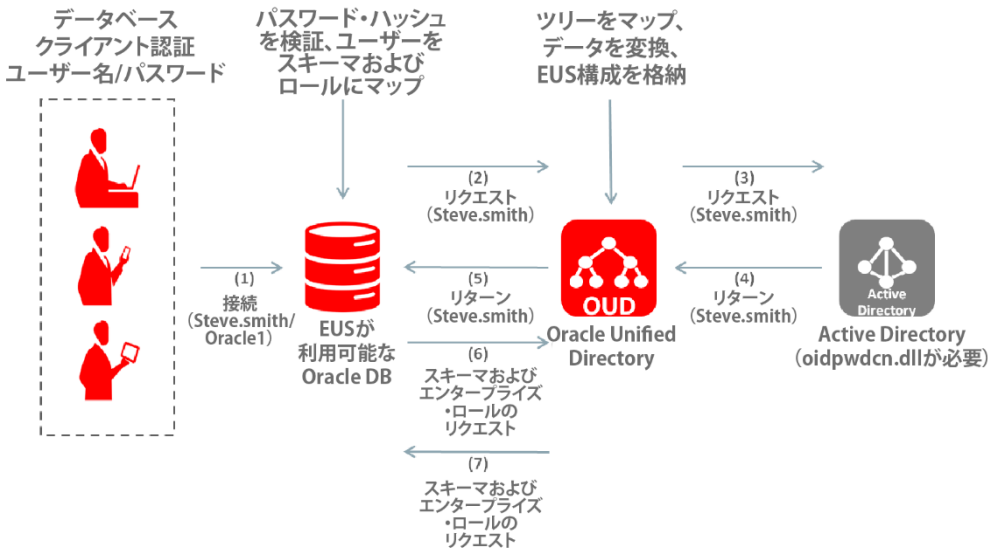

図2：Active Directoryを使用したEUSのアカウント管理

Kerberos認証を使用したActive Directory統合

このシナリオでは、DB 認証に Kerberos が使用されます。EUS で DB Kerberos 認証を使用する場合、標準の EUS 構成以外にデータベースの変更は必要ありません。データベースは OUD への接続を確立します。OUD は、リクエストされた DB 情報を Active Directory で検索します。このオプションを使用するには、すべてのデータベース・クライアントで Kerberos が利用可能である必要があります。この機能は DB バージョン 10.1 以降でのみサポートされます。

データベースは OUD への接続を確立します。OUD はユーザー・データ（ユーザーおよびグループ）を Active Directory から取得します。EUS メタデータは OUD に格納され、OUD から取得されます。ハッシュ化されたユーザー・パスワードにアクセスする必要はないため、スキーマ拡張も、Active Directory へのパスワード変更通知 DLL のデプロイも必要ありません。

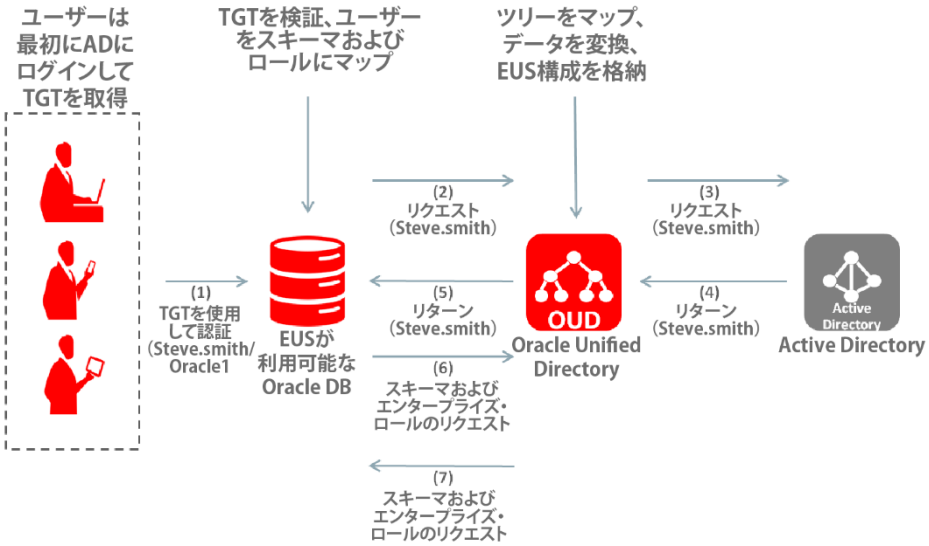

図3：KerberosおよびActive Directoryを使用したEUSのアカウント管理

Oracle Directory Server Enterprise Editionのアカウント

データベースは OUD への接続を確立します。OUD はユーザー・データ（ユーザーおよびグループ）を Oracle Directory Server Enterprise Edition から取得します。EUS メタデータは OUD に格納され、OUD から取得されます。

この統合では、データベースにも、パスワード認証を使用するデータベース・クライアントにも変更は必要ありません。

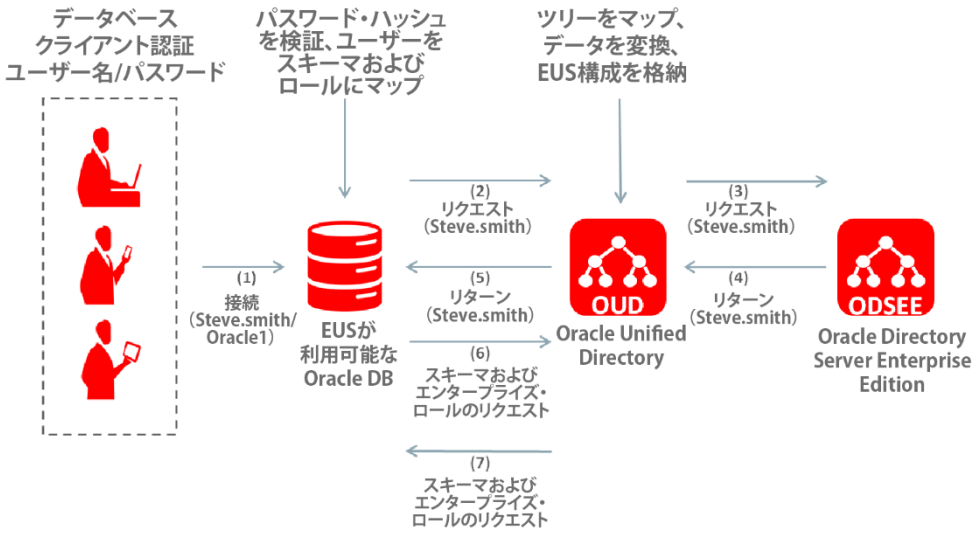

図4：ODSEEを使用したEUSのアカウント管理

Novell eDirectoryのアカウント

データベースは OUD への接続を確立します。OUD はユーザー・データ（ユーザーおよびグループ）を Novell eDirectory から取得します。EUS メタデータは OUD から取得されます。

この統合では、通常 EUS に必要とされる以外のデータベース変更は必要ありません。また、ユーザー/パスワード認証を使用するデータベース・クライアントにも変更は必要ありません。

Novell eDirectory を使用する場合、Oracle パスワード・フィルタは必要ありません。eDirectory でユニバーサル・パスワードを有効化して、管理者がユーザー・パスワードを取得できるようにする必要があります。詳細については、Novell eDirectory のドキュメントのパスワード管理を参照してください。

この構成は、DB バージョン 10.1 以降でのみ使用できます。それより前の DB バージョンでは、パスワード形式に互換性がありません。

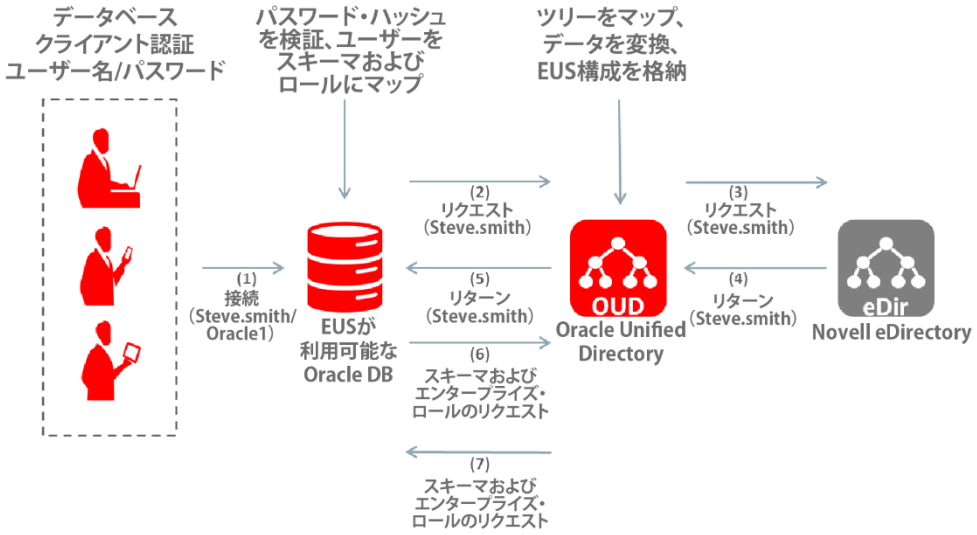

図5：eDirectoryを使用したEUSのアカウント管理

OIDを使用したDBアカウントの一元化

➔ OIDに格納されたDBアカウント

EUS デプロイメントでは、ユーザー認証/認可情報と組み合わせて、OID と、OID に登録されたデータベース・インスタンスを使用できます。

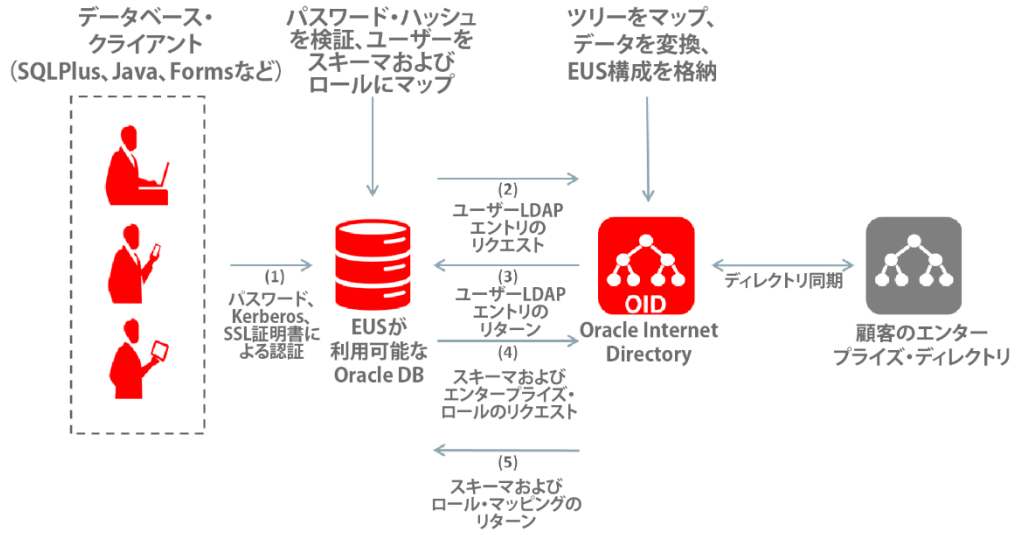

図 6：OID を使用した EUS のアカウント管理

データベース間の通信は SSL で保護できます（Oracle Database の Advanced Security オプションが必要です）。SSL 接続は、ユーザー認証のためではなく、OID/データベース間の相互認証のために使用されます。データベースは複数の LDAP 検索操作により、ユーザー/パスワード情報を検索します。OID は、データベース向けのデータ・ストレージとしてのみ使用され、実際に LDAP バインド操作によるユーザー認証を行いません。データベースがユーザーを認証します。

一般的にユーザー情報は、デフォルトの OID ユーザー・ディレクトリ情報ツリー（DIT）に格納されます。データベース・メタデータ（DB 登録情報など）、ユーザー/ロール・マッピングなどは、OID 内の独立したコンテナである OracleContext に格納されます。

EUS は、さまざまな認証方法をサポートします。

1. X.509 証明書認証（Oracle8i Database で導入）
2. パスワードベース認証（Oracle9i Database で導入）
3. Kerberos 認証（Oracle Database 10g で導入）

これらの認証方法は、Oracle Database（EUS なし）と Advanced Security オプションで提供される認証メカニズムと区別することが重要です。

EUS の実装には、OID 内のユーザー・フットプリント（ユーザー・パスワードなど）が必要です。OID は、OracleContext の格納以外に、EUS 関連データを保護するアクセス制御を実施するために使用されます。

EUS について詳しくは、Oracle Technology Network のデータベース・ドキュメント・セクションにある、エンタープライズ・ユーザー管理者ガイドを参照してください。

➔ OIDを介して参照される既存ディレクトリのDBアカウント

EUS は、サード・パーティのディレクトリを使用している環境にデプロイされることがよくあり、OID とその他のディレクトリとの統合には、一貫したユーザー情報を確保することが求められます。次のユースケースでは、Active Directory と ODSEE の統合について説明します。

パスワード認証向けのActive Directory統合

パスワード認証を使用するこのユースケースでは、パスワードおよびエンタープライズ・ロールなどのユーザー・アカウントは OID に格納する必要があります。

DIPとADパスワード・フィルタを使用した、パスワード変更のソースとしてのAD統合

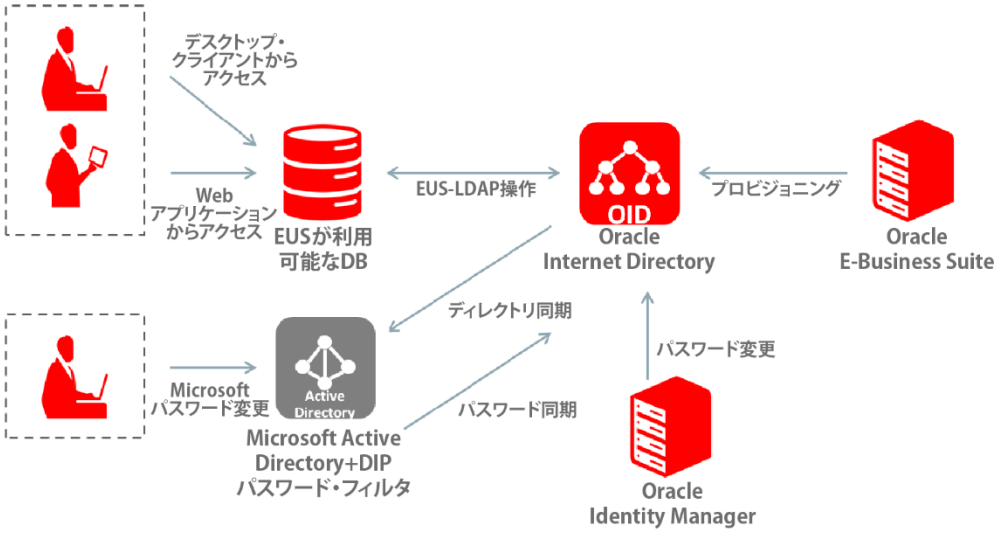

図 7：OID および AD を使用した EUS のアカウント管理（AD がパスワード変更のソース）

Active Directory のユーザーおよびグループの OID との同期は、Directory Integration Platform（DIP）を使用して実行されます。この処理は、Directory Integration Platform（dipassistant など）を使用した 1 回のブートストラップによって実行されます。ユーザー集団が Active Directory で変更されない場合は、DIP サーバーは常に稼働している必要はありません。

Active Directory パスワード・フィルタは、各ドメイン・コントローラで使用されるため、それぞれにインストールする必要があります。フィルタが Active Directory LSA に接続し、公開されている Microsoft API を介してパスワード変更を取得して、SSL で OID に送信されます。パスワード変更が OID にプッシュできない場合（OID に接続していないなど）、パスワードは、OID への接続が確立するまで Active Directory に暗号化されて格納されます。

ただし、フィルタはすべてのドメイン・コントローラに格納する必要があります。パスワードは専用の Microsoft スキーマを使用して暗号化されるため、グローバル・カタログ・サーバーは、パスワード・フィルタと一緒には使用できません。

DIPを使用した、パスワード変更のソースとしてのOID統合

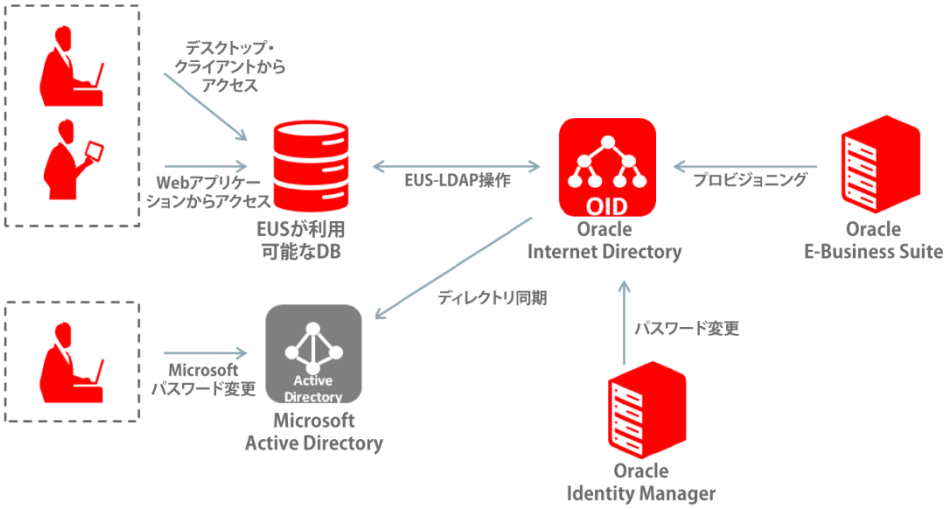

図 8：OID および AD を使用した EUS のアカウント管理（OID がパスワード変更のソース）

Active Directory のユーザー名を使用したパスワードベース認証を、Active Directory ユーザー・フットプリント（samAccountName、krbUserPrincaplName などの Active Directory 属性で構成されます）と、OID および AD グループ情報を同期することで実現します。パスワード変更は OID から SSL で Active Directory に同期されます。つまり、パスワードは 2 回保存されます。このモデルでは、OID はデプロイメントの中央ソースとなります。

最初のユーザー・パスワードは OID で生成される必要があり、ユーザーは自身のパスワードを OID で変更する必要があります。

Kerberos認証向けのActive Directory統合

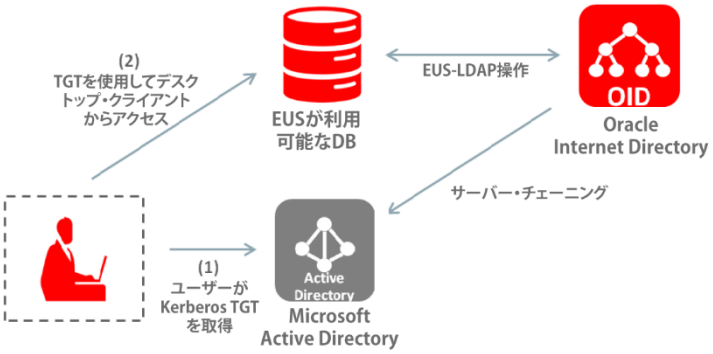

図 9：AD にチェーニングした OID を使用した EUS のアカウント管理

Kerberos と OID サーバー・チェーニングを使用すると、OID でユーザー・フットプリントを作成するための DIP 同期や、Active Directory でのパスワード変更を取得するための Active Directory パスワード・フィルタのインストールが不要になります。OID は Kerberos 対応ではないことに注意してください。OID サーバー・チェーニングを使用すると、DB の代わりに Active Directory でユーザーおよびグループ情報を検索できます。

注意事項：Kerberos のインストールと構成は複雑です。OID サーバー・チェーニングはパフォーマンスに影響を与える可能性があります。DB バージョン 10.1 以降でのみ EUS Kerberos がサポートされています。OID サーバー・チェーニングは、1 つの Active Directory サーバーしか使用できません。

ODSEEの統合

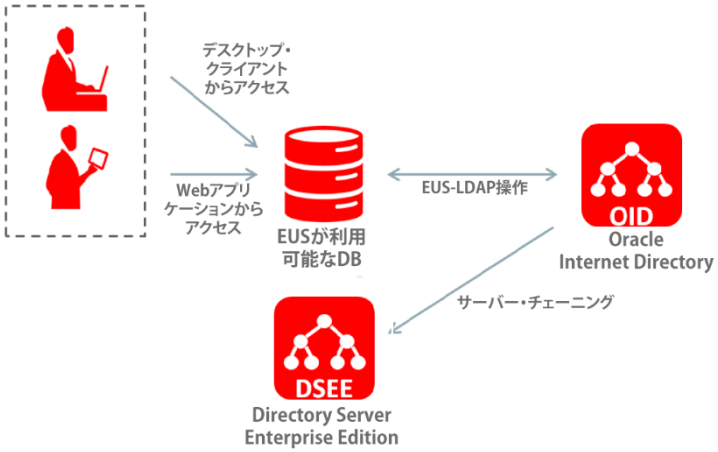

図 10：ODSEE にチェーニングした OID を使用した EUS のアカウント管理

OID サーバー・チェーニングを使用すると、OID でユーザー・フットプリントを作成するための DIP のインストールが不要になります。パスワードは ODSEE でのみ管理されます。OID サーバー・チェーニングを使用すると、ODSEE/OUD でパスワード、ユーザーおよびグループ情報を検索できます。パスワードは ODSEE にのみ格納されます。

サーバー・チェーニングはパフォーマンスに影響を与える可能性があることに注意してください。DB バージョン 10.1 以降でのみ使用できます。DB バージョン 9i では、DB パスワードは Oracle 独自のパスワード検証機能を使用して、'orclpassword'属性に格納されます。このパスワード検証機能は ODSEE ディレクトリでは利用できないため、DB バージョン 9i はこのシナリオでサポートされません。ODSEE でのユーザーおよびグループ変更は、OID に伝播しません。このようなマッピングは OID に格納され、更新されません。

結論

Oracle Database Enterprise User Security を使用してデータベースのユーザー・アカウントとロール・メンバーシップを一元管理することにより、セキュリティが強化され、管理コストが削減され、コンプライアンスが改善されます。OUD では、EUS をネイティブにサポートすることも、既存の ODSEE、Active Directory、または Novell eDirectory を利用し総所有コスト（TCO）を削減することもできます。

付録A：サポートされるデプロイメントと最低限のバージョン番号

認証タイプ	サード・パーティ・ディレクトリ	DB	OID	OUD
証明書		8i以降	8i以降	
証明書		10g、11g以降		11.1.2.1
証明書		11g以降		11.1.2.2以降
パスワード		9i以降	9i以降	
パスワード		10g、11g		11.1.2.0、 11.1.2.1
パスワード		11g以降		11.1.2.2以降
Kerberos		10g、11g	10g以降	11.1.2.1
Kerberos		11g以降	10g以降	11.1.2.2以降
パスワード	AD + DIP + OIM	9.2.0.3以降	10g以降	
パスワード	AD + DIP + パスワード・フィルタ	10.1以降	10.1.4	
パスワード	ODSEE	10.1以降	10.1.4	
パスワード	ODSEE + OIDサーバー・チェーニング	10.1以降	10.1.4	
Kerberos	AD + OIDサーバー・チェーニング	10.1以降	10.1.4	
Kerberos	AD + OUD	10.1以降		11.1.2.1以降
パスワード	AD + OUD	10.1以降		11.1.2.1以降
パスワード	ODSEE + OUD	10.1以降		11.1.2.1以降
パスワード	eDir + OUD	10.1以降		11.1.2.1以降

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

海外からのお問い合わせ窓口
電話：+1.650.506.7000
ファクシミリ：+1.650.506.7200

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Hardware and Software, Engineered to Work Together

Oracle is committed to developing practices and products that help protect the environment