

Oracle ホワイト・ペーパー
2010 年 1 月

Oracle Identity Analytics の Identity Warehouse : ベスト・プラクティス

ORACLE®

免責事項

以下の事項は、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。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いたします。

目次

1. エグゼクティブ・サマリー	4
2. Identity Warehouse の要素	5
3. ブロック式アプローチ : Identity Warehouse の構築	7
4. Identity Warehouse の機能	9
5. データ・インポート・プロセス	11
結論	13

1. エグゼクティブ・サマリー

企業の状況は常に変化しています。たとえば、事業拠点を拡大する、従業員数を削減する、コア・ビジネスやコア・サービス以外の領域をアウトソーシングする、組織構造を変更する、機密データにかかわるサード・パーティのサービス・プロバイダと契約するといった変化です。そのため、ビジネス変化に対応していくには、このような継続的な変化を捕捉して、従業員（臨時雇用と正規雇用の両方）と従業員がアクセスできるリソースを大きな視点で経営者および意思決定者に提示してくれるテクノロジーが必要です。

Oracle Identity Analytics は、ロール管理と ID コンプライアンスを実現するオラクルの包括的なソリューションで、すべてのユーザーとそのアクセス対象になっているさまざまなシステムの企業規模のビューを用意するという難題を解決するためのテクノロジーを提供します。Oracle Identity Analytics の Identity Warehouse は、組織の重要なエンタイトルメント・データのすべてを含む中央リポジトリです。このホワイト・ペーパーでは、Identity Warehouse の概要を説明し、ウェアハウス構築のベスト・プラクティスを紹介し、Oracle Identity Analytics で使用できる他の機能で Identity Warehouse のデータがどのように役立つかを説明します。

ビジネスの課題

技術専門職、情報管理責任者、セキュリティ担当者、IT 管理者は、多くの場合、次に示す質問に対する回答を探しています。

- 従業員と臨時請負業者の両方についての、さまざまなアプリケーションとターゲット・システムを横断する企業規模のビューは存在するか。その情報は定期的に更新されているか。現在の情報は最新か。
- 企業内に孤立アカウントはあるか。それらは削除されているか。
- 分かりにくいエンタイトルメントを認定者に分かりやすく説明する用語集はどこに格納できるか。その用語集の更新やメンテナンスはどのような方法で実施できるか。
- 組織のセキュリティ上、慎重に扱う必要のあるエンタイトルメントを分類することはできるか。
- ロールやポリシーなど、ID とアクセス権に関連する情報を格納したり表示したりすることができる中央リポジトリはあるか。
- 職務分掌（SoD）に関するポリシーをロールとポリシー・レベルで定義できるか。

2. Identity Warehouse の要素

Identity Warehouse は、ユーザーとユーザー・エンタイトルメント・データを含む中央リポジトリです。リポジトリのデータは組織内の 1 つまたは複数のデータベースから定期的にインポートされません。Oracle Identity Analytics のインポート・エンジン、テキスト・ファイルまたは XML として保存された複雑なエンタイトルメントからのインポートをサポートします。抽出、変換、ロード (ETL) の処理機能も使用できます。また、Oracle Identity Manager などの市場をリードする ID 管理およびプロビジョニングのソリューションとシームレスに統合することもできるため、自動的に Identity Warehouse がシードされます。各エンタイトルメントに対する用語集のエントリを、インポート・プロセス中に取得することもできます。

次の表に、Identity Warehouse の要素の一覧と説明を示します。

要素	説明
ユーザー	業務上、企業の情報資産にアクセスしたりそれらを変更したりする必要がある、個別の識別可能なエンティティです。ユーザーには、さまざまなユーザー管理機能およびロール管理機能をユーザーに対して実行する職務を担うマネージャーまたはアプリケーション承認者がいます。
リソースおよびリソース・タイプ	リソースとは、ユーザーが職務を実行するうえで必要なアプリケーションと企業情報資産のことです。Oracle Identity Analytics では、リソース・タイプに含まれる 1 つのインスタンスをリソースといい、類似したリソースをグループ化したものがリソース・タイプです。たとえば、複数の Oracle [®] データベース・インスタンスをまとめたものが Oracle という名前のリソース・タイプであるのに対し、各データベース・インスタンスはリソースです。 一般的なリソース・タイプには、プラットフォーム (Windows 2000、UNIX [®] 、メインフレーム) やビジネス・アプリケーション (請求や買掛金のアプリケーション) などがあります。各リソースには、リソースに対するさまざまな操作 (ユーザー・エンタイトルメントのレビューなど) を処理する所有者がいます。
アプリケーション	Identity Warehouse でいうアプリケーションとは、複数のリソース・タイプおよびリソース全体のビューのことです。
ビジネス構造	ビジネス構造は、組織内の部門または下位部門として定義されます。組織は、組織内のチームおよび下位チームを表現するのに必要なだけの階層レベルを使用して、必要な数のビジネス構造に分割できます。
ロール	ロールとは、ジョブ機能のことです。ロールには、個々のユーザーがディレクトリ上に保持するアクセス権を記述したポリシーが含まれます。ロールは、ドメイン内でユーザーが実行する特有のジョブ機能を表現します。たとえば、マネージャー、開発者、およびトレーナーとして機能できる人がいるとします。この場合、それぞれのジョブ機能には異なる権限と異なるリソースへのアクセス権が必要であるため、各ジョブ機能を表す 3 つのロールが存在します。 ロールは、ネストされたロールとしてロール内部に埋め込むことができます。ロールの階層は、組織で必要となる任意のレベルまで定義できます。

ポリシー	ポリシーとは、異なるプラットフォームまたはアプリケーションに対してユーザーが保持するアカウント属性と権限を定義したものです。1つのポリシーには、特定の1つのデータ・リソースに対する特定の1つの権限が含まれます。ポリシーはロールに割り当て、ロールはユーザーに割り当てます。ポリシーを使用すれば、組織横断的でも組織内でも、一貫性のあるディレクトリ権限とユーザー権限を、ロール内のすべてのユーザーに提供できます。
孤立アカウント	孤立アカウントとは、すでに組織または統括ビジネス・ユニットに属していないユーザーに帰属するアカウント（ユーザーはすでに組織を離れているか部署を異動している可能性があるが、その際無効にしなかったアカウント）のことです。
用語集	用語集には、分かりにくいエンタイトルメントを分かりやすく説明した用語が含まれます。
データ所有者	データ所有者とは、属性値の所有者または管理者のことです。データ所有者は、特権情報にアクセスできるユーザーに対する責任を負います。
データの分類	データの分類とは、SoD ルールの作成に使用できるユーザー・エンタイトルメント・データのビジネス・レベルの分類のことです。たとえば、売掛金と買掛金は、SoD ルール内のエンタイトルメント・セットを1つ持つ2つの分類です。SoD ルールでは、データの分類レベルをチェックして、売掛金と買掛金の両方のエンタイトルメントがユーザーに付与されるのを防止できます。
アカウント	アカウントとは、ユーザーが特定のリソース・タイプにアクセスできるようにするエンタイトルメントまたは権限のことです。

3. ブロック式アプローチ：Identity Warehouse の構築



図 1.1：Oracle Identity Analytics のコンポーネント

図 1.1 に示すとおり、Identity Warehouse の構築は、Oracle Identity Analytics を使用するための最初の手順です。その他のモジュール（ID 認定、ID 監査、ロール・モデリングおよびメンテナンス）は、Identity Warehouse への移入が完了すると使用できるようになります。

Identity Warehouse は、次の手順に従って段階的に構築することをお勧めします。

1. ユーザーのインポート：ユーザーをインポートする作業は、Identity Warehouse にシードするための予備手順です。必ず、信頼できるソースからユーザー・セットをインポートするようにし、ユーザーを毎晩インポートするためのプロセスを作成します。Oracle Identity Analytics により変更が更新され、最新のビューが提供されます。
2. ユーザー・エンタイトルメントのインポート：ユーザー・エンタイトルメントをインポートする作業は、Identity Warehouse を構築する際の 2 つめの手順です。Oracle Identity Analytics は複雑なエンタイトルメントのインポートに対応しており、詳細なメタデータ情報が表示されます。この情報は、認定プロセス中に活用できます。
 - a. データの相互関連付けの実行：ユーザーとエンタイトルメントの関連付けは重要な手順です。この手順を慎重に実行しないと、孤立アカウントやエンタイトルメントのないユーザーが発生することがあります。Oracle Identity Analytics は、高度な相関ルールに対応させることもできます。
 - b. 孤立アカウントの相互関連付け：ユーザー・エンタイトルメントのインポートでは、孤立アカウントが発生することがよくあります。資産またはアプリケーションの所有者は、ここで次のアクションのいずれかを実行できます。
 - i 孤立アカウントをユーザーに割り当てる（クレーム ID と呼ばれるプロセス）
 - ii 孤立アカウントを無効化し、それらが存在しなくなっていることを確認する

3. ビジネス構造の作成 : ビジネス構造とは、ユーザーを論理的にグループ化したものです。現在の組織の構造および階層をビジネス構造に反映させることができます。ビジネス構造はマネージャーに割り当て、そのマネージャーにユーザー・アクセスのレビューを担当させる必要があります。
 - a. ビジネス構造ルールの作成 : ユーザーは、ビジネス構造ルールに従って、指定された条件に基づいてビジネス構造に直接割り当てられます。ビジネス構造ルールを定義しておけば、新しいフィードがインポートされるたびに、ビジネス構造も必ず更新されます。
4. 用語集のインポート : 用語集をインポートし、分かりにくいエンタイトルメントが分かりやすい用語でビジネス・マネージャーに表示されるようにします。ユーザー・マネージャーがユーザー・アクセスを認定する際には、この情報が不可欠です。
5. アプリケーションの作成 : エンタイトルメントをインポートしたら、データを分析してエンタイトルメントに優先順位を付けます。エンタイトルメントの重要度に基づいて、ユーザーをグループ分けするアプリケーションを作成します。アプリケーション・ビューは、さまざまなリソースおよびリソース・タイプをまたぐことがあります。必要に応じて、もっとも詳細なレベルまでドリルダウンします。
6. ID データの管理 : Identity Warehouse には、データを格納する機能の他にデータ管理機能もあります。これは Identity Warehouse のメンテナンスの重要な側面です。必ず次のことを実行してください。
 - a. 所有者の割当て : 重要な属性値に所有者を割り当てます。
 - b. データの分類 : 組織にとって重要な基準に基づいて、属性値にラベルを付けます。たとえば、データの特徴は高リスク、中リスク、低リスクに分類できます。
 - c. 特権データを識別します。

4. Identity Warehouse の機能

Identity Warehouse を構築し終わると、ユーザーは次に示す利点の一部をすぐに認識できます。

機能	利点
ユーザー・データの取得	Identity Warehouse はすべてのユーザーの包括的な HR データを取得します。このデータは、認定、ロール・モデリング、または ID 監査のときに活用できます。
アプリケーション・ビュー	アプリケーション・ビューは認定のプロセスに不可欠なもので、マネージャーはアプリケーションに基づいてアクセス情報の並べ替えやレビューができます。
データ所有者の割当て	データの所有者または属性に基づいて認定を開始できます。
データの分類の作成	データの分類は、組織内の職務分掌 (SoD) ポリシーの定義に使用できます。また、ID 監査モジュールでも活用できます。
ビジネス構造	ID 監査や ID 認定など、Oracle Identity Analytics のすべての操作は、ビジネス構造に基づいて実行されます。
ロール・ビュー	ロール・ビューは、組織内で作成されたロールの統合ビューで、ロールの履歴とバージョンが表示されます。このビューでは、必要に応じて、非定型のロールを作成することもできます。
ポリシー・ビュー	ポリシー・ビューはポリシーの統合ビューで、所有者、履歴、バージョンなどが表示されます。
用語集	用語集ビューは、ユーザー・マネージャーがさまざまなエンタイトルメントの意味を理解するのに役立ちます。用語集ビューを使用することで、ユーザー・マネージャーは認定プロセス中により適切な判断ができます。

ビジネス構造 - ユーザー・ルール	ビジネス構造ルールは、ユーザーの属性の変化に基づいてビジネス構造を最新の状態に維持するのに役立ちます。たとえば、ユーザーの所属部門が変更されると、Identity Warehouse にもこの変更が反映されます。
孤立アカウントのクリーンアップ	孤立アカウント・ビューには、アクセス権を持っていてもすでに存在しないか、アクセス権を必要としないユーザーについての、セキュリティに関連する重要な情報が取得されます。このビューを使用すると、アクセス権の無効化や適切なユーザーへのアクセス権の割当てを簡単に実行できます。
アカウントへのアカウント・タイプの割当て	アカウントを Identity Warehouse にインポートするとき、アカウント・タイプもインポートできます。たとえば、プロビジョニング・アカウント、システム・アカウント、サービス・アカウント、テスト・アカウント、開発アカウントなどのアカウント・タイプをインポートできます。この設定は、Identity Manager を使用する統合プロセスで役立ちます。
ユーザー・ビュー	ユーザー・ビューは、Identity Warehouse の中でもっとも重要なビューです。このビューは、すべてのユーザーとエンタイトルメントを n レベルの階層とともに全社的に表示する単一のビューです。
'n 番目'の階層レベルの取得	Oracle Identity Analytics では、もっとも詳細な階層レベルでエンタイトルメントを取得できます。これらの詳細な属性を、SoD スキャンまたは監査スキャン中に Identity Warehouse で表示、認定、評価できます。
標準のインポート・プロセス	Oracle Identity Analytics では、CSV ファイルおよび XML ファイルを使用してユーザー、アカウント、ロール、ポリシー、ビジネス構造および用語集をインポートできます。インポート・プロセスが簡潔であることは、新しいアプリケーションまたはターゲット・システムを導入するときの大きなメリットです。

5. データ・インポート・プロセス

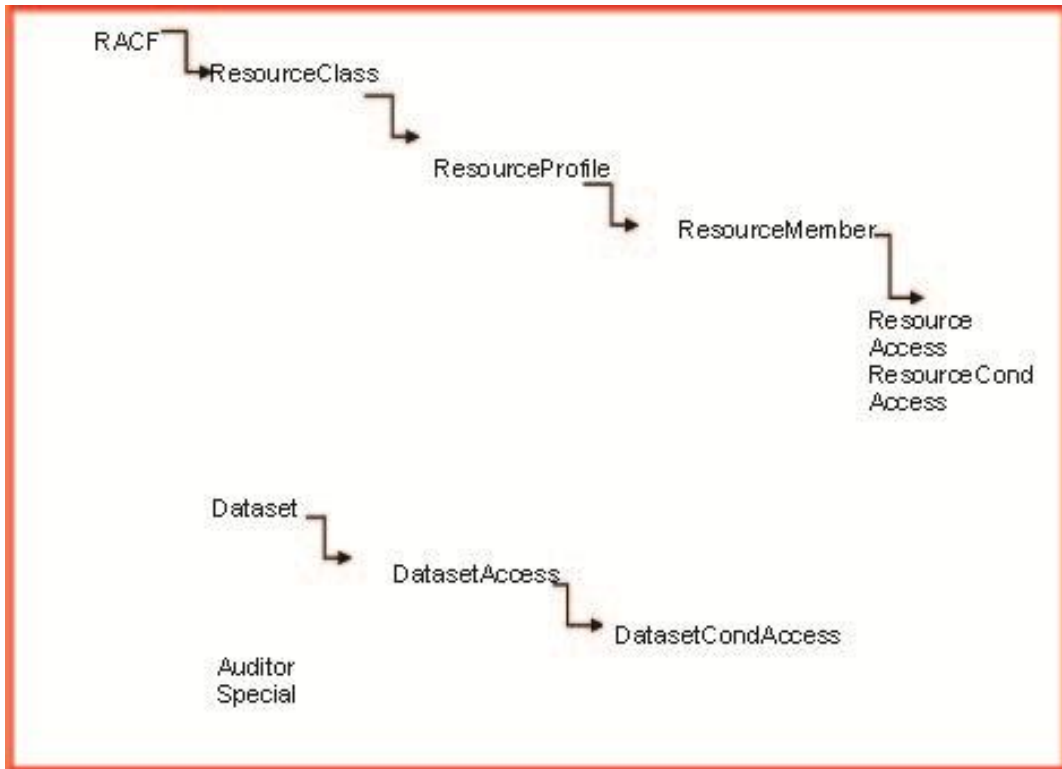
Identity Warehouse へのインポートはおもにインポート・プロセスで実行されます。必要な要素をインポートするプロセスにはアプリケーション所有者が携わり、ユーザー・インタフェースにデータが正確に表示されるようにします。インポート・プロセスのスケジュールは、組織の要件に合わせて柔軟に作成できます。

Oracle Identity Analytics では、次の要素をインポートできます。

1. ユーザー
2. アカウント
3. ロール
4. ポリシー
5. ビジネス構造
6. 用語集の項目
7. リソース・メタデータ
8. リソース

複雑なユーザー・エンタイトルメントを含むアカウントをインポートする場合は、リソースと属性が作成されます。Oracle Identity Analytics では、CSV フラット・ファイルまたは XML ファイルをインポートできます。フラット・ファイルを使用するインポート・プロセスでは、スキーマが必要です。複数值属性または n レベル階層を伴うアカウントには、XML ファイルを推奨します。

たとえば、RACF などのメインフレーム・システムの構造は次のようになっています。このアプリケーションは、XML ファイルを使用してインポートできます。Oracle Identity Analytics では n 番目の階層レベルを取得できるため、'ResourceAccess'および'ResourceCondAccess'レベルまで下ってエンタイトルメントをインポートできます。



Identity Warehouse のメンテナンスは、構築と同じくらい重要です。柔軟なインポート・スケジュール、定期的なデータ・インポート、および絶え間ない検証により、現在の情報のみが表示されるようになります。組織内のユーザーとそのエンタイトルメントの現在のビューを提供することが、Identity Warehouse のもっとも重要な機能です。

結論

本書では、現在ほとんどの企業が直面している問題を紹介し、ID およびアクセス管理情報の一元化ビューについて説明した後、Identity Warehouse を"推奨する理由と"ブロック式アプローチ"によるウェアハウス構築についての基本事項を説明しました。また、Identity Warehouse の利点である、ユーザー・エンタイトルメントを一元化した全社的なビューの提供、孤立アカウントのクリーンアップ、アプリケーションにアクセスするユーザーの相互関連付けによるアプリケーション・ビューのモデリング、ビジネス構造に存在するユーザーとビジネス構造との相互関連付け、n 番目のエンタイトルメント階層レベルの取得、ビジネス用語集、データ所有者、データ分類などを通じた全方向的なユーザー・エンタイトルメント・データ・ビューの提供などについて説明しました。最後に、Identity Warehouse のさまざまなコンポーネントのメンテナンスの重要性についても説明しました。

Oracle Identity Analytics は、ロール管理と ID コンプライアンスを実現するオラクルの包括的なソリューションで、すべてのユーザーとそのアクセス対象になっているさまざまなシステムの企業規模のビューを用意するという難題を解決するためのテクノロジーを提供します。Oracle Identity Analytics の Identity Warehouse は、組織の重要なエンタイトルメント・データのすべてを含む中央リポジトリです。

ORACLE

Oracle Identity Analytics の
Identity Warehouse : ベスト・プラクティス
2010 年 1 月
著者 : Neil Gandhi
共著者 : Viresh Garg

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

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
www.oracle.com



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

Copyright © 2009, Oracle and/or its affiliates. All rights reserved. 本文書は情報提供のみを目的として提供されており、ここに記載される内容は予告なく変更されることがあります。本文書は一切間違いがないことを保証するものではなく、さらに、口述による明示または法律による黙示を問わず、特定の目的に対する商品性もしくは適合性についての黙示的な保証を含み、いかなる他の保証や条件も提供するものではありません。オラクルは本文書に関するいかなる法的責任も明確に否認し、本文書によって直接的または間接的に確立される契約義務はないものとします。本文書はオラクルの書面による許可を前もって得ることなく、いかなる目的のためにも、電子または印刷を含むいかなる形式や手段によっても再作成または送信することはできません。

Oracle は米国 Oracle Corporation およびその子会社、関連会社の登録商標です。その他の名称はそれぞれの会社の商標です。

0109