

Oracle ホワイト・ペーパー

2010年1月

ガバナンス、リスク、およびコンプライアンス エントリ・レベルの実践ガイド

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. ID 関連の統制機能を備えた GRC フレームワークの構築	4
3. ID ベースの統制ソリューションの選択基準	8
4. Oracle Identity Management を使用した統制の実装	9
5. 結論	10

1. エグゼクティブ・サマリー

多くの組織にとって、ガバナンス、リスク、コンプライアンス（GRC）に関する新たな取組みの実施は、手に負えないように思えるかもしれません。GRCにはさまざまな見方と側面が含まれるため、どこから始めるべきかを把握しにくい可能性があります。進化を続ける規制要件と複雑化するビジネスに取り組む多くのセキュリティ責任者やIT管理者にとって、ITガバナンスは引き続き中心的な焦点となっています。現在の組織は規制を理解するだけでなく、ガバナンス、リスク、コンプライアンス（GRC）要件への対応に関する適切な戦略を構築するよう求められています。さらに事態を深刻化するのは、GRCイニシアチブが、しばしば異なる事業組織やIT組織に管理されるさまざまなインフラストラクチャへと幅広く及ぶ点です。遵守を義務付けられた規制のうち、もっとも有名なものには、米国サーベンス・オクスリー法（SOX）や、グラム・リーチ・ブライリー法（GLB）、また医療保険の相互運用性と説明責任に関する法律（HIPAA）があります。これらの主要要件の多くは、システムやアプリケーション、またデータへのユーザー・アクセスを制御するID管理の要素を中心に展開されています。このため、GRCに関するITイニシアチブや検討事項においては、IDおよびアクセス管理を最優先事項として取り組む必要があります。

このホワイト・ペーパーでは、GRCイニシアチブを同時に対処できる多数の構成要素に分け、もっとも簡単に計画および実施できる要素から始める方法を解決策として提案します。

最初の重点領域を選択することは、おそらく、エンタープライズGRCの全体像から、これを実現するITフレームワークへと、さらにいくつかの扱いやすいフレームワーク要素へと掘り下げることを意味するでしょう。この例として挙げられるのが、ビジネス・ポリシーをサポートするためのアクセス、セキュリティ、その他の統制の実装に関連するITフレームワーク・アプリケーションです。アクセスとセキュリティはIDと表裏一体であるため、ID管理を通じて自動化できる統制機能から開始すると良いでしょう。

このホワイト・ペーパーでは、以下について説明します。

- GRC向けITフレームワークの一部として導入できる、ID関連のアクセスおよびセキュリティ制御の具体例
- ITフレームワーク内のアクセスおよびセキュリティ制御を実現するIDベース・ソリューションの選択ガイドライン
- GRCへの初期の取組みに有効なオラクルのID管理製品ポートフォリオに関する情報

2. ID関連の統制機能を備えたGRCフレームワークの構築

ここでは、GRC向けITフレームワークの一部として導入できる、ID関連のアクセスおよびセキュリティ制御の具体例を示します。これらは、全社的に、または組織内の特定の事業領域に対して実装できます。

認証

エンタープライズ・リソースへのアクセスを要求したユーザーが本人であり、参照するオブジェクトの参照権限や使用するオブジェクトの使用権限を持つことを確認することは、企業のリスクを軽減し、コンプライアンスを強化するためには欠かせない作業です。これを実現するには、強力な認証コンポーネントを備えたアクセス制御機能が必要になります。

幅広い認証機能を持つ ID ベースのアクセス制御テクノロジーを実装すると、エンタープライズ・ポリシーをサポートするための適切な認証レベルが提供されます。ID ベースのソリューションには、少なくとも次の機能が含まれている必要があります。

- 強力なパスワード管理機能 - パスワードの変更頻度などのポリシーを義務付けます。
- エンタープライズ・シングル・サインオン (ESSO) 機能 - ユーザーが1つのパスワードを使用して各種エンタープライズ・リソースにアクセスできるようにすることで、パスワード・ポリシーを遵守しながら、ユーザー・エクスペリエンスを向上します。
- 厳密な制御オプション - 複数ファクタの認証などを通じて、初期のネットワーク・ログイン・レベルでパスワード・ベースのアクセス・セキュリティを強化します。

職務分掌の実施

職務分掌 (SoD) を実施すると、ユーザーが持つロールと割り当てられた職務が原因となって、ユーザーが意図的または無意識にセキュリティ・ポリシーを侵害することを防止できます。職務分掌の典型的な例として、発注書の発行とその承認を同じユーザーに割り当てないというものがあります。SoD の実施は、企業の財務運営の整合性維持を目的とする米国サーベンス・オクスリー法や、その他の規制に含まれる明確な要件を遵守する組織能力に直接影響を及ぼします。

GRC の統制環境に SoD ポリシーを適用するには、次の機能を持つ ID のプロビジョニングおよび監査機能が必要になります。

- ユーザーがプロビジョニングされた際に、特に職務に影響する可能性のある業務変更があった場合、すぐに発生しそうな違反を特定できるきめ細かさを持っている。
- 違反を自動的に予防し、インシデントが発生した場合はマネジメント層に報告する。
- 業務変更やパスワード・リセットなど、SoD に影響する可能性のある活動履歴を継続的に保持する。
- 機密や部外秘、またはその他の慎重を期すエンタープライズ・リソースに対するすべてのアクセス試行を記録し、マネジメント層に通知する。

ポリシー定義が完了したら、ID 管理システム内の日常的な機能にこれらのポリシーを適用して適切な統制を実施する必要があります。

予防的統制は、もっとも一般的な統制手法です。名前から分かるとおり、予防的統制とは、望ましくない行動が起きる前にそれを阻止することを指します。こういった統制は、いくつかの領域で実

施できます。アクセス制御ポリシーは、該当する一連の基準（アプリケーションへアクセスしているユーザーの場所や時間など）に基づいて Web アプリケーションへのログインを制限します。また、アクセス権が付与される個所に予防的統制を適用することもできます。ルールがユーザーに付与されるか、または新しいエンタイトルメントがルールにマッピングされることで、このルールに属するすべてのユーザーのアクセスが実質的に変更されます。職務分掌などの予防的統制を配置することで、潜在的にポリシー違反につながるアクションを評価し、違反の発生を防止できます。ユーザーの介入が必要になる場合、通知や承認のワークフローと組み合わせることで対応できます。

ポリシーやプロセス、また予防的統制を使用して、望ましくない行為の発生を防止することはできますが、どのような統制システムも完全無欠ではありません。不適切な行為が行われるという状況の発生を避けることはできません。発見的統制を使用すると、定義されたポリシーに実際のユーザー・アクセスが合致しない状況で違反がすでに発生しているケースを特定できます。この原因としては、不正な試みが行われている場合や、伝統的に予防的統制機能に欠けるレガシー・システムで、アクセスが蓄積されている場合が考えられます。

発見的統制によって例外や違反が検出された場合、相当する *修正制御機能* を配置して、この違反に対処する必要があります。たとえば、電子メール・アラートを適切なレビューアに配信して、違反に対する修正措置を講じることができます。例外の重大度によっては、不適切なアクセスを削除または修正する必要があります。実装された修正制御の種類に応じて、プログラムを使用する場合と手動で処理する場合があります。この制御機能を通知フレームワークやチケットング・システムと統合して手動修正を実施したり、プロビジョニング・システムと統合して自動修正を実施したりすることもできます。

ルール・ベースのアクセス制御

企業内のどのリソースに誰がアクセスできるかを規定したエンタープライズ・ルールとポリシーを、ユーザーのルールに基づいて適用することができます。ルール・ベースのアクセス制御を利用すると、個々のユーザー・アカウントではなくルールに対してポリシーを適用できるため、管理が容易になります。

前述の SoD 実施シナリオと同様に、ここでも ID 主導型のソリューションが理想的です。重要な点は、次の機能を備えた製品を見つけることです。

- 矛盾するアクセス権限を特定し、ユーザーへの権限付与を自動的に防止する。
- アクセス権とアクティビティを監査および認定するプロセス全体にわたる、ルールの管理、アクセス権の付与、アクセスに関する包括的なレポートングを組み合わせた機能を提供する。
- アクセス制御を自動化することで、マネージャーのアクセス認定プロセスを簡素化する。

ルールを使用すると、アクセス認定制御を自動化することもできるため、マネージャーによるアクセス認定プロセスが大幅に簡素化されます。ルール管理に基づいてリソースに対するアクセスの監査と認定を実施すると、企業は実用的なフレームワークを確立して厳密な統制を実装できます。マ

ネジメント層は効率的にエンタープライズ・リソースを保護し、内部のセキュリティ・ポリシーや外部の規制要件を遵守できます。また、ロール・ベースでアクセスを監査し、認定することで、場当たり的なユーザー・アクセス管理に付随する運用上の非効率性が大幅に軽減されます。

監査とコンプライアンスの自動化

GRC イニシアチブ向けの統制の実装に際して、自動化の重要性は計り知れません。監査およびコンプライアンス機能を自動化すると、アクセス・ポリシーの適用やアクセス監視、また監査とコンプライアンスに対する継続的なレポートニングの実施を費用効果に優れた方法で、簡単に実行できます。

監査およびコンプライアンスに関連するプロセスと手順を手動で持続することは不可能です。人為的エラーは言うに及ばず、これらの作業には多大な労力とコスト、そして時間がかかるためです。たとえば、自動化を実装しない場合、組織はアクセス違反の検出やこれらの手動修正に対して、期末ごとに何週間も費やすことになる場合があります。その上、すべての違反が検出され、正しく修正されたという保証はどこにもありません。一方で、ID 主導型の自動化ソリューションを利用すると、組織内でロールを変更されたユーザーに対して、以前のロールに関連したリソースへのアクセス権限が不適切に残されているケースなどの違反を正確かつ即座に検出できます。

監査およびコンプライアンスのプロセスを自動化する ID ベース・ソリューションにとって理想的なのは、関連する複数のプロセスを自動化する多様な機能を 1 つにまとめることです。

- プロビジョニング、アクセス管理、レポートニングを組み合わせた自動化機能 - 包括的で持続可能な監査およびコンプライアンス・サポートを提供します。
- 全社的な ID およびアクセス情報を自動的に統合するディレクトリ機能 - 認証サービスの第一線をアプリケーションに提供し、ディレクトリ・データの暗号化などの強力なセキュリティ・メカニズムを実現します。・自動ロギングとトランザクション暗号化のサポート - 改ざんが防止された包括的なフォレンジック追跡機能を、必要に応じて監査チームによるレビュー用に提供します。

アクセス認定は一般的に、事業部門のマネージャーやアプリケーション・オーナーによって、定期的にユーザー・アクセスをレビューする目的で実施されます。アクセス認定のサポートには、プロセス自体の自動化（スケジューリング、電子メール通知、承認の割当て、ステータス報告など）に加えて、これらのアクティビティの監査や文書化が含まれます。認定作業は、その性質によってそれぞれ異なるレベルで実行されます。アプリケーション・オーナーは通常、アプリケーションへのアクセス用に作成されたアプリケーション・アカウントを利用した、大まかなユーザー・アクセス認定に関心を持ちます。またビジネス・オーナーは一般に、エンドユーザーに公開されるビジネス機能の種類を決定するユーザー・エンタイトルメントに関心があります。同様に、ロールがアクセス権の付与に使用されるのに対し、ロール・メンバーシップは最終的なユーザー・アクセスを決定するために使用されます。アクセス認定ソリューションの対象者は IT 管理者ではなくビジネス・ユーザーであることが多いため、効果的なソリューションを実現するには適切なレベルの情報を提供する必要があります。リソースやエンタイトルメント、またロールに対してビジネス・フレンドリーな説明を提示する必要があります。

分析

豊富な情報が収集される現在では、潜在的なリスクの兆候となる傾向や行動を発見するために、データを分析することができます。次にその例を示します。

- 今四半期に認証されたアカウントの割合
- 特定の期間中に異常に大量の承認リクエストを受けた承認者はいるかどうか
- 不正アカウントの検出に関して何らかの傾向があるかどうか

リスクを完全に回避することはできないため、ID およびアクセス管理ソリューションが目標とするのは、リスクを軽減することです。分析を手動で実施することもできますが、定期的にスケジューリングしておき、必要に応じて注意を喚起する適切な通知をビジネス・オーナーやアプリケーション・オーナーに送信することもできます。

ID およびアクセス管理の重要な側面は、システムの動作状態だけでなくユーザーの行動を監視できる点にあります。製品の監査サポートに従ってすべての制御を実装すると、十分に役立つ量の ID 情報を収集できます。この情報には、ユーザー作成、アカウント・リクエスト、アクセス・リクエスト、承認、違反、例外修正、ロールの付与、ユーザー・ログインなどが含まれます。包括的なレポート・フレームワークを使用すると、ユーザー・タイプごとにこの情報を参照できます。静的なレポートに加えて、ダッシュボードでは収集データのグラフィカル表現を通じて、さらに有益な情報が提供されます。

3. ID ベースの統制ソリューションの選択基準

ID 主導型のアプローチを採用して IT インフラストラクチャ内の環境を GRC 向けに統制することを検討している組織にとって、自動化は最優先事項になります。しかし自動化以上に重要なのは、複数プロセス（ID のプロビジョニングと監査、アクセス管理、ロール管理）を 1 つにまとめる柔軟性を持つ ID ベースの統制ソリューションを選択することです。

- *ID プロビジョニング機能*と *ID 監査機能*が合理化された単一製品として提供されている場合、効率的にアクセス・リクエストを処理すると同時にアクセスに付随するリスクを特定できるため、実用的です。
- きめ細かい認証機能を含んだ *アクセス管理機能*は、ポリシー違反や規制命令に対する防衛線を確立するために不可欠です。
- *ロール管理機能*はリソースへのアクセス管理プロセスを迅速化するため、大規模で多様なユーザー基盤を持つ企業にとって有益な機能です。

最後に、GRC 向けの統制環境を構築するための ID ベース・ソリューションは、強力なレポート・コンポーネントを備えていなければなりません。このソリューションは、誰が何に対するアクセス権を持ち（ユーザーと情報オーナーの両方）、実際に誰が何にアクセスし（アプリケーション、オペレーティング・システム、その他のリソース（特に社外秘やその他の機密情報に関するリソース）など）、誰がアクセスを承認または認可したかについてレポートするする必要があります。また、レポート機能は、すべてのリソースに対するあらゆるアクセス・アクティビティを含んだ一元化ログを提供する必要があります。こうすることで、組織は監査に必要な情報を素早く正確に収集できます。

4. Oracle Identity Management を使用した統制の実装

オラクルが提供する包括的な ID 管理製品ポートフォリオは、GRC 向け IT フレームワークの一環として、アクセスおよびセキュリティ制御の実装を開始するために必要な機能のすべてを提供します。

Oracle Identity Manager

ID のプロビジョニング機能と監査機能が集約された Oracle Identity Manager は、セキュリティ・ポリシーとコンプライアンス要件を統制環境で適用および実施するために理想的な選択肢として、きめ細かい機能を提供します。おもな機能は次のとおりです。

- プロビジョニングと監査の統合による、予防と検出の両面でのコンプライアンスの実現
- プロビジョニングと監査に対する、一貫した ID 制御の適用
- ポリシー違反の追跡と例外処理のための期限切れ機能

Oracle Access Manager

オラクルのフェデレーテッド ID 製品は、GRC イニシアチブを導入する IT フレームワークでのアクセス制御に不可欠な、シングル・サインオン、認証、認可といった機能を提供します。おもな機能は次のとおりです。

- アプリケーション・セキュリティの一元管理
- ルール・ベースおよびロール・ベースの認可を実施するポリシー・エージェント
- あらかじめ組み込まれた ESSO 機能
- 中心となる認証および認可サービスのパートナーへの拡張

Oracle Identity Analytics

個人のアクセス権限ではなくユーザー・ロールに基づいてエンタープライズ・アクセス・ポリシーを適用することで、Oracle Identity Analytics は GRC 向け IT フレームワークにおけるアクセス制御を飛躍的に簡素化します。おもな機能は次のとおりです。

- ロールの設計と継続的なロール保守
- 事業部門マネージャーやロール・オーナーによる継続的なロール認定
- エンタープライズレベルのアクセス監視によるポリシー違反の検出
- 認定ステータスとポリシー例外を表示するダッシュボード・ビュー

オラクルのディレクトリ製品

Oracle Internet Directory、Oracle Virtual Directory、Oracle Directory Server Enterprise Edition は、企業全体を通じてアクセス情報を統合する包括的なディレクトリ・サービスを提供します。おもな機能は次のとおりです。

- データと通信の暗号化と、パスワード保護を使用した堅牢なセキュリティ
- マルチレベルの Access Control Instruction (ACI) によるデータの保護とリスクの最小化
- 持続的な検索パフォーマンスとリレーショナル・データベースに迫る書込みパフォーマンス
- 柔軟性の極めて高いレプリケーション環境によるデータ可用性の確保

5. 結論

エンタープライズ GRC イニシアチブの導入に意欲的な企業にとって最大の課題は、何から開始すべきか分からない点にあります。一度に 1 つずつの GRC 要素に焦点を合わせることで、最適な結果がもたらされます。特に、ID 関連のインフラストラクチャ制御など、計画と実装の容易な要素から開始すると良いでしょう。オラクルの ID 管理ポートフォリオには多数の製品が含まれており、認証、職務分掌分析、Identity Analytics、ロール・ベースのアクセス管理、監査およびコンプライアンス・プロセスの自動化といった領域の統制を実現します。

オラクルの ID 管理と ID 関連制御について、詳しくは Oracle.com/identity を参照してください。



ガバナンス、リスク、およびコンプライアンス

2010年1月

著者：Neil Gandhi

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