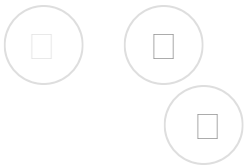
リスク管理の保護

目次



リスク管理の保護

Oracle Risk Management Cloud Risk Managementの保護

19C
部品番号F21368-01

原本著者: David Christie

ニアリング、逆アセンブル、逆コンパイルは互換性のために法律によって規定されている場合を除き、禁止されています。

ここに記載された情報は予告なしに変更される場合があります。また、誤りが無いことの保証はいたしかねます。誤りを見つけた場合は、オラクルまでご連絡ください。

このソフトウェアまたは関連ドキュメントを、米国政府機関もしくは米国政府機関に代わってこのソフトウェアまたは関連ドキュメントをライセンスされた者に提供する場合は、次の通知が適用されます。

U.S. GOVERNMENT END USERS:Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations.As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs.No other rights are granted to the U.S. Government.

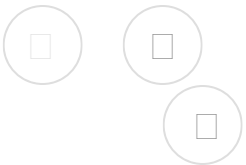
このソフトウェアまたはハードウェアは様々な情報管理アプリケーションでの一般的な使用のために開発されたものです。このソフトウェアまたはハードウェアは、危険が伴うアプリケーション(人的傷害を発生させる可能性があるアプリケーションを含む)への用途を目的として開発されていません。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用する際、安全に使用するために、適切な安全装置、バックアップ、冗長性(redundancy)、その他の対策を講じることは使用者の責任となります。このソフトウェアまたはハードウェアを危険が伴うアプリケーションで使用したことに起因して損害が発生しても、Oracle Corporationおよびその関連会社は一切の責任を負いかねます。

OracleおよびJavaはオラクルおよびその関連会社の登録商標です。その他の社名、商品名等は各社の商標または登録商標である場合があります。

Intel、Intel Xeonは、Intel Corporationの商標または登録商標です。すべてのSPARCの商標はライセンスをもとに使用し、SPARC International, Inc.の商標または登録商標です。AMD、Opteron、AMDロゴ、AMD Opteronロゴは、Advanced Micro Devices, Inc.の商標または登録商標です。UNIXは、The Open Groupの登録商標です。

このソフトウェアまたはハードウェア、そしてドキュメントは、第三者のコンテンツ、製品、サービスへのアクセス、あるいはそれらに関する情報を提供することがあります。適用されるお客様とOracle Corporationとの間の契約に別段の定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスに関して一切の責任を負わず、いかなる保証もいたしません。適用されるお客様とOracle Corporationとの間の契約に定めがある場合を除いて、Oracle Corporationおよびその関連会社は、第三者のコンテンツ、製品、サービスへのアクセスまたは使用によって損失、費用、あるいは損害が発生しても一切の責任を負いかねます。

このドキュメントで使用されている事業所名は架空のものであり、現在または過去に実在する実際の会社を特定するためのものではありません。



- About Oracle
- Contact Us
- Products A-Z
- Terms of Use and Privacy
-
- Ad Choices

Oracle

Integrated Cloud Applications & Platform Services

リスク管理の保護

はじめに

ここでは、アプリケーションを使用する際に役立つ情報ソースについて説明します。

Oracle Applicationsの使用

Applicationsヘルプの使用

アプリケーションでヘルプにアクセスするには、ヘルプ・アイコンを使用します。ページにヘルプ・アイコンが表示されていない場合は、グローバル・ヘッダーにある自分のユーザー・イメージまたは名前をクリックし

て「ヘルプ・アイコンの表示」を選択します。ヘルプ・アイコンがないページもあります。Oracle Applicationsヘルプにもアクセスできます。

視聴: このビデオ・チュートリアルでは、ヘルプの見つけ方とヘルプ機能の使用方法について説明します。

Applicationsヘルプの使用も参照してください。

その他のリソース

- コミュニティ: Oracle Cloud Customer Connectを使用して、オラクル社のエキスパート、パートナ・コミュニティおよび他のユーザーから情報を得ることができます。
- ガイドおよびビデオ: Oracle Help Centerにアクセスしてガイドおよびビデオを参照できます。
- トレーニング: Oracle UniversityでOracle Cloudのコースを受講してください。

表記規則

このガイドで使用されるテキスト表記規則を次の表に示します。

規則	意味
太字	太字は、ユーザー・インタフェース要素、ナビゲータ・パス、または入力する値や選択する値を示します。
固定幅フォント	固定幅フォントは、ファイル名、フォルダ名、ディレクトリ名、コードの例、コマンドおよびURLを示します。
→	右矢印記号は、ナビゲータ・パスの要素を区切ります。

ドキュメントのアクセシビリティについて

オラクルのアクセシビリティについての詳細情報は、Oracle Accessibility ProgramのWebサイトを参照してください。

このガイドに含まれるビデオは、このガイドで使用可能なテキストベースのヘルプ・トピックの代替メディアとして提供するものです。

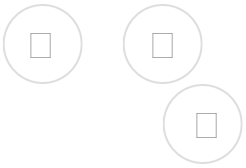
オラクル社への問合せ

Oracle Supportへのアクセス

サポートをご契約のお客様には、My Oracle Supportを通して電子支援サービスを提供しています。詳細情報はMy Oracle Supportか、聴覚に障害のあるお客様はAccessible Oracle Supportを参照してください。

ご意見およびご提案

Oracle Applicationsヘルプやガイドに関するフィードバックをお寄せください。Eメールの宛先はoracle_fusion_applications_help_ww_grp@oracle.comとなります。



このページは役に立ちましたか?

Yes No

リスク管理の保護

1 概要

この章の内容は次のとおりです。

リスク管理のセキュリティの概要

アプリケーションのリスク管理ファミリでは、職務ロールとジョブ・ロールで機能へのアクセス権が付与され、

データ・セキュリティ・ポリシーでデータへのアクセス権が付与されます。

- ジョブ・ロールの概念は、ユーザーが組織で遂行するジョブを表しています。通常は、ジョブに含まれる1つ以上のタスクを表す職務ロールよりも広範囲の機能にアクセスできます。

  しかし、どちらのロール・タイプでも、機能セキュリティ・ポリシーやロール階層、またはその両方を定義できます。機能セキュリティ・ポリシーでは、特定のタスクを完了するための権限を付与します。ロール階層は一連の下位ロールで構成され、親ロールはそこから機能アクセス権を継承します。

  一般的にリスク管理では、下位レベルの職務ロールで機能セキュリティ・ポリシーを使用して個々のタスクを定義します。上位レベルの職務ロールでは、下位レベルの職務ロールからなる階層を定義して、関連するタスクを集めます。ジョブ・ロールでは、上位レベルの職務ロールの階層を定義して、ユーザーに割り当てるのに十分な範囲のアクセス権を指定します。ジョブ・ロールは、ユーザーに直接割り当てることができますが、職務ロールは割り当てることができません。職務ロールは、ジョブ・ロールの階層の要素として間接的にのみユーザーに付与されます。

  セキュリティ・コンソールとも呼ばれるOracle Applicationsセキュリティで、ロールを作成および管理します。
- データ・セキュリティ・ポリシーで一連のデータを定義します。ポリシーはロールにマップするので、ポリシーで定義されたデータに対して、ロールで付与された機能が適用されます。データ・セキュリティ・ポリシーを作成および管理し、それらをロールにマップするには、リスク管理の「セキュリティの管理」ページを使用します。

「ロール」と「データ・セキュリティ・ポリシー」の概念は、リスク管理と他のOracle Cloudアプリケーションの間で異なります。

- 他のアプリケーションの職務ロールでは、機能へのアクセス権を付与しますが、データ定義コンポーネントもあります。実際には、ロールで機能権限を選択しますが、それらの権限のサポートに必要なデータも選択します。

  リスク管理の職務ロールには、データ定義コンポーネントがありません。純粋に機能のみを定義します。つまり職務を構成する一連の機能権限、またはより大きな職務やジョブをサポートするための一連の職務を定義します。
- 他のアプリケーションのデータ・セキュリティ・ポリシーは、職務ロールのデータ定義コンポーネントであるため、職務ロールとは切り離せない一部になっています。

  リスク管理のデータ・セキュリティ・ポリシーは、すべてのロールから完全に独立して構成します。まったく別の基準を使用してデータを定義します。たとえば、観点を使用する場合がありますが、これは他のアプリケーションには存在しません。これは職務ロールまたはジョブ・ロールのどちらかにマップできます。
- 他のアプリケーションでは、職務ロールやジョブ・ロールの要素として、集計権限を含めることができます。これらにも、機能コンポーネントとデータ定義コンポーネントの両方があります。

  リスク管理のロールでは、集計権限を使用しません。
- HCMアプリケーションでは、データ・ロールを定義できます。これらはHCMのセキュリティ・プロファイルに基づいており、ユーザーに直接割り当てることができます。

  リスク管理では、データ・ロールもセキュリティ・プロファイルも使用しません。リスク管理のジョブ・ロールは、ユーザーに直接割り当てられます。
- 通常、ユーザーには少なくとも1つの抽象ロールが割り当てられます。たとえば、従業員ロールでは、特定のジョブに無関係で、すべての従業員が実行するタスクおよび機能にアクセスできます。抽象ロールは、リスク管理のセキュリティに関しては意味がありません。

観点

観点とは、階層的に編成された一連の関連する値のことです。ルート値(他のすべての値と関係がある値)には、組織、地域、規制コード、または意味があると思われる他のすべての概念を設定できます。個別の観点値を個々のリスク管理オブジェクト・レコードに割り当てて、これらのオブジェクト・レコードが存在するコンテキストを確立します。

- 財務レポート・コンプライアンス・モジュールでは、プロセス、リスクおよび統制に観点値を割り当てることができます。
- 拡張統制管理モジュールでは、モデル、拡張統制およびインシデントに観点値を割り当てることができます。
- アクセス証明のコンポーネントには観点値を割り当てません。

たとえば、「組織」観点には、会社の構造をマップする値を含めることができます。ディビジョンは組織の直接的な子になれます。各ディビジョンは一連のビジネス・ユニットの親になることができ、それ以降も同様です。このようにして会社は、個々のリスク、統制または他のオブジェクトを、それらが適用されるディビジョン、ユニットまたは他の企業エンティティに関連付けることができます。

観点とセキュリティ

ジョブ・ロールは、機能アクセスを定義する職務ロールおよび権限で構成されます。データ・セキュリティ・ポリシーは、一連のデータを定義します。ロールはデータ・セキュリティ・ポリシーにマップされるため、ロールを割り当てられたユーザーは、マップされたポリシーによって定義されたデータにその機能を適用できます。

データ・セキュリティ・ポリシーを構成するときには、観点値を割り当てることができます。その場合、同じ観点値に関連付けられているオブジェクトに関するデータへのアクセス権のみを付与します。(ただし、このセキュリティ制限はアクセス証明には適用されません。)

組織の例を使用するには、1つのデータ・セキュリティ・ポリシーに関連付けられたジョブ・ロールをユーザーに割り当てることができます。このポリシーで、特定のビジネス・ユニットの「組織」観点値を指定できます。ユーザーはその値が割り当てられた、つまり値が表すビジネス・ユニットに関連するデータ・レコードにのみアクセスできます。

事前定義済のセキュリティ・ジョブ

リスク管理のロールおよびユーザーへのロールの割当は、セキュリティ・コンソールで管理します。セキュリティ同期化と呼ばれる事前定義済のジョブにより、リスク管理は、セキュリティ・コンソールで行われた変更を認識できます。ジョブでは、現在のセキュリティ定義と一致するようにワークリストが更新されます。

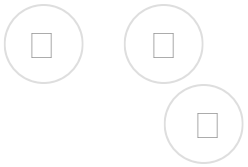
ジョブは、リスク管理を初めて起動したときに実行され、その後はスケジュールされた間隔で実行されます。このジョブを初めて実行すると、事前定義済ロールと事前定義済データ・セキュリティ・ポリシーのマッピングも実行されます。

デフォルトでは、セキュリティ同期化ジョブは週に1回、毎週日曜に実行されます。このデフォルト・スケジュールは変更されることが想定されます。環境内のロール、ユーザー割当て、データ・セキュリティ・ポリシーの変更頻度が反映されたスケジュールが理想的です。「スケジューリング」ページを使用してスケジュールを変更する

か、「即時実行」機能を使用して必要なときにジョブを実行します。

関連項目

- スケジュールの変更



このページは役に立ちましたか?

Yes No

リスク管理の保護

2 ユーザー

この章の内容は次のとおりです。

リスク管理実装ユーザー

テスト環境または本番環境のサービスURL、ユーザー名、仮パスワードは、オラクル社から届くサービスアクティブ化Eメールに記載されています。これらの資格証明を使用して、各環境のリスク管理の設定を担当する実装ユー

ザーを作成します。設定には、次のことが含まれます。

- データ・セキュリティ・ポリシーに組み込む観点の構成。
- セキュリティの構成。少なくともジョブ・ロールおよびデータ・セキュリティ・ポリシーの作成。
- 財務レポート・コンプライアンス・モジュール内のオブジェクトで使用可能な機能およびアセスメント・アクティビティの選択。他の実装タスクとは異なり、このアクティビティでは、アプリケーション・ユーザーが業務系データを作成すると変更できなくなる設定をします。
- リスク管理を使用および定期保守用に構成する管理機能の設定。
- 実装のテスト。実際には、リスク管理の機能を使用して、期待した結果が返されることを確認します。

注意: リスク管理をツールとして使用すれば、他のOracle Cloudオファリングのリスクを管理できます。その場合は、リスク管理の実装を、他のオファリングの実装と調整する必要があります。これには、リスク管理実装ユーザーの他に、他のオファリングの実装ユーザーを作成する必要があるのが普通です。要件の詳細は、他のオファリングのドキュメントを参照してください。

リスク管理実装ユーザーはOracle Human Capital Management (HCM)で作成してください(たとえば、「ユーザーの管理」作業領域で使用可能な「ユーザーの作成」機能を使用)。そうすると、個人レコードが実装ユーザーに関連付けられますが、これはEメール通知機能のテストに必要です。

注意: セキュリティ・コンソールでユーザー・アカウントを作成できます。しかし、これでは個人レコードが作成されないため、リスク管理の実装ユーザーには不適切です。セキュリティ・コンソールではなくHCMを使用して、リスク管理の実装ユーザーを作成してください。

実装ユーザーを作成するときには、次の2つの事前定義済ジョブ・ロールを割り当てます。

- 企業のリスクおよび統制マネージャ: このロールで付与される職務により、モジュール設定と管理設定、観点およびデータ・セキュリティ・ポリシーの作成、および実装のテストを実行できます。
- ITセキュリティ・マネージャ: このロールでは、ユーザーがリスク管理のロールを作成できるセキュリティ・コンソールへのアクセス権が付与されます。

実装が完了したら、「企業のリスクおよび統制マネージャ」ロールの割当を取り消すことをお薦めします。このスーパーユーザー・ロールは、通常使用するものではありません。実装ユーザーがセキュリティ・コンソールでロールを作成するときに、リスク管理の「管理者」ジョブ・ロールを作成して、それと置き換えることができます。このロールには、モジュール、管理、観点およびデータ・セキュリティ・ポリシー管理の職務ロールのみを含めます。

リスク管理ユーザーの準備と管理

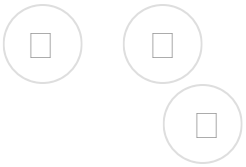
実装時には、アプリケーション・ユーザー向けのOracle Applications Cloudサービスを準備します。タスクには、次を行うかどうかを決定することが含まれます。

- 個人、ユーザーまたはパーティ・レコード作成時の、関連ユーザー・アカウントの自動作成。
- ユーザーへのロールのプロビジョニングの自動化または要求許可。その場合の、ロールプロビジョニング・ルールの作成。
- ユーザーにロールがない場合のユーザー・アカウントの自動休止、ロール割当時の自動再アクティブ化。

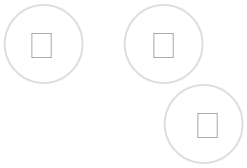
実装中に、「ユーザーの作成」タスクを使用して、テスト用のアプリケーション・ユーザーを作成できます。このタスクでは、デフォルトでは最小限の個人レコードとユーザー・アカウントが作成されます。実装後は、「従業員の採用」タスクを使用してアプリケーション・ユーザーを作成してください。ユーザーをインポートすることもできます。これらのタスクはHCMを介して使用できます。

アプリケーション・ユーザーの準備、作成および管理の詳細は、ERPの保護に関するドキュメントを参照してください。

セキュリティ・コンソールの一般管理ページで、ユーザー・アカウントに一定の標準を設定できます。これらには、ユーザー名(ユーザーが自分自身を識別するためにサインイン時に入力する値)の形式、パスワードの形式とポリシーが含まれます。



リスク管理の保護



3 機能セキュリティ

この章の内容は次のとおりです。

- ロールの分析
- セキュリティ・コンソールの管理

リスク管理ロールの概要

リスク管理のユーザーに割り当てる独自のジョブ・ロールを作成する必要があります。

- 6つの事前定義済ジョブ・ロールのみが存在します。それぞれがスーパーユーザー・ロールで、通常のアプリケーション・ユーザーよりもはるかに多くのアクセス権が付与されています。これらのロールはいずれもアプリケーション・ユーザーには割り当てないでください。かわりに、個々のユーザーが実行するタスクに限定されたアクセス権を付与するロールを作成してください。
- 事前定義済ロールに対する事前定義済データセキュリティ・ポリシーのマッピングは変更できません。したがって、観点ベースのセキュリティを実装するには、観点値が組み込まれたデータ・セキュリティ・ポリシーを作成するだけでなく、マップ先となるジョブ・ロールも作成する必要があります。

一般に、ジョブ・ロールを開発する際には、製品領域に該当する事前定義済ロールをコピーして、ユーザーに付与する内容以外の職務をコピーから削除します。事前定義済の6つのジョブ・ロールは次のとおりです。

- アプリケーション・アクセス監査者。拡張アクセス統制機能(アクセス証明に適用されるもの以外)、および拡張アクセス統制をサポートする設定機能と管理機能が提供されます。
- ユーザー・アクセス証明マネージャ拡張アクセス統制のアクセス証明コンポーネントの機能、およびアクセス証明をサポートする設定機能と管理機能が提供されます。
- アプリケーション統制マネージャ.拡張財務管理機能、および拡張財務管理をサポートする設定機能と管理機能が提供されます。
- コンプライアンス・マネージャ。財務レポート・コンプライアンス機能、および財務レポート・コンプライアンスをサポートする設定機能と管理機能が提供されます。
- 企業のリスクおよび統制マネージャこれは最も広範なジョブ・ロールです。財務レポート・コンプライアンスの機能に加えて、すべてのリスク管理ツールの機能へのアクセス権も付与されます。特に、これは観点管理へのアクセス権を提供する唯一の事前定義済ジョブ・ロールです。通常、管理ジョブ・ロールおよび実装ジョブ・ロールの作成はここから開始します。
- リスク管理の監査者。このロールは、高度なアクセス統制およびトランザクション統制や、財務レポート・コンプライアンス統制の企業監査を担当するユーザーのアクティビティを編成します。

さらに、Oracleで提供されている多くの事前定義済職務ロールから選択して、自分で作成した各ジョブ・ロールに機能アクセス権を追加できます。事前定義済ロールは変更できません。職務ロールを新規作成することも、事前定義済の職務ロールをコピーしてそのコピーを編集することもできます。ただし、そうすることはほとんどありません。ほとんどの場合は、事前定義済の職務ロールでニーズを満たすことができます。

通常は、どのユーザーにも複数のジョブ・ロールを割り当てることができるようにロールを設計することをお薦めします。各ジョブ・ロールには、ユーザーが必要とする職務ロールのサブセットを含めます。このようにすると柔軟性を保てます。他のジョブ・ロールと様々に組み合せて、各ジョブ・ロールを他のユーザーにも割り当てることができます。

アクセス証明のセキュリティ

拡張アクセス統制のアクセス証明コンポーネントの場合は特別です。通常は、事前定義済ジョブ・ロール(この場合は「ユーザー・アクセス証明マネージャ」)のコピーから職務ロールを削除するか、自分で作成したジョブ・ロールに職務ロールを追加して、ジョブ・ロールを作成できます。ただし、次の点に注意してください。

- 事前定義済の職務ロールのみを使用することが重要です。つまり、アクセス証明管理者、アクセス証明所有者、アクセス証明の証明者、アクセス証明の構成および保守です。これらのコピーを変更したり、新規アクセス証明職務ロールを作成しないでください。

  各アクセス証明ユーザーは、管理者、所有者または証明者のいずれか1つの役割を果たすと想定されています。これを確実に実施するために、ジョブ・ロールには、管理者、所有者または証明者職務ロールのいずれか1つのみを追加します。ただし、これは必須ではありません。構成および保守の職務ロールを使用すると、アクセス証明同期化ジョブをオンデマンドで実行したり、Eメール・アラートを有効にできるため、通常これは管理者に付与します。各職務ロールは、明示的にアクセス証明用のジョブ・ロールに追加することも、アクセス証明と関係ない職務が設定されたジョブ・ロールに追加することもできます。
- 「アクセス証明」ジョブ・ロールには、データ・セキュリティ・ポリシーは必要ありません。アクセス証明に該当しない観点値を指定するポリシーを作成する必要はありません。事前定義済の「アクセス証明」職務ロールを含む各ジョブ・ロールは、その職務ロールにマップされた事前定義済データ・セキュリティ・ポリシーを継承します。

  アクセス証明に関係がない職務が設定されたジョブ・ロールに「アクセス証明」職務ロールを追加すると、そのジョブ・ロールをデータ・セキュリティ・ポリシーにマップして、そのポリシーに観点値を指定できます。その場合、これらは「アクセス証明」職務には影響しません。

ロールの使用方法

Oracle Applicationsセキュリティ内で、リスク管理のロールを構成して、ユーザーにそれらを割り当てることができます。セキュリティ・コンソールでは、次の操作を実行できます。

- 最初からロールを作成するか、既存のロールをコピーしてそのコピーを編集します。ジョブ・ロールを作成または編集する際、それらをユーザーに割り当てることもできます。
- ユーザー、ロールおよび権限の間の階層関係を視覚化します。
- ロールまたはユーザーに対して使用できるナビゲータの各メニューをシミュレートします。
- ロールのバージョンを比較します。

セキュリティ・コンソールを開くには、ホーム・ページで「ツール」を選択します。オプションの中から「セキュリティ・コンソール」を選択します。これを行うには、「ITセキュリティ・マネージャ」ロールが必要です。

セキュリティの視覚化

セキュリティ・コンソールの視覚化グラフは、セキュリティ項目を表すノードで構成されています。これらは、ユーザー、ロール、権限または集計権限です。ノード間をつなぐ矢印は、それらのノードの関係を定義します。ロール階層内の任意の項目から、アクセス権が付与されたユーザーまでのパス、またはロールで付与できる権限までのパスを追跡できます。

次の2つのビューのいずれかを選択できます。

- 放射状: ノードが円形(円弧)パターンを形成します。各円形パターン内のノードは、中心のノードと直接関

連しています。その焦点ノードは、視覚化画像を生成するために選択した項目か、視覚化画像内で展開した項目です。
- レイヤー: ノードが一連の水平線を形成します。各線のノードは、前の線の1つのノードに関連しています。これは、視覚化画像を生成するために選択した項目か、視覚化画像内で展開した項目です。

たとえば、ジョブ・ロールは複数の職務ロールで構成されている場合があります。ジョブ・ロールを視覚化のフォーカスとして選択できます(さらに、権限に向かうパスを表示するようにセキュリティ・コンソールを設定できます)。

- 初期状態の放射状ビューには、ジョブ・ロールを表すノードを囲むように職務ロールを表すノードが表示されます。
- 初期状態のレイヤー・ビューには、ジョブロール・ノードの後に職務ロール・ノードが線で表示されます。

その後、ノードを展開して構成項目を表示するなど、画像を操作できます。

別の方法として、選択した項目に関連する項目をリストした視覚化表を生成できます。たとえば、選択したロールの下位にあるロールや、選択したロールによって継承される権限を表にリストできます。表形式データはExcelファイルにエクスポートできます。

視覚化の生成

視覚化を生成する方法は次のとおりです。

1. セキュリティ・コンソールで、「ロール」をクリックします。
2. 視覚化のベースにするセキュリティ項目を検索します。
   - 「検索」フィールドで、ジョブ・ロール、職務ロール、権限、ユーザーなど、項目タイプの任意の組合せを選択します。
   - 隣のフィールドに、少なくとも3文字を入力します。検索によって一致するレコードが返されます。
   - レコードを選択します。

     または、「検索」をクリックして「検索結果」列にすべての項目をロードし、レコードを選択します。
3. 「グラフの表示」または「表として表示」ボタンを選択します。

   注意: 「管理」ページで、ロールのデフォルト・ビューを決定できます。
4. 「展開方向」リストで「権限」を選択すると、選択した項目からそのロール階層の下位のアイテムへのパスを追跡できます。または、「ユーザー」を選択すると、選択した項目からその階層の上位の項目へのパスを追跡できます。
5. 表ビューがアクティブな場合、「表示」リストで項目タイプ(「ロール」、「権限」または「ユーザー」)を選択します。(使用できるオプションは、「展開方向」の選択内容によって異なります。)選択した項目タイプのレコードが表に表示されます。集計権限はロールとみなされることに注意してください。

視覚化グラフの表示オプション

視覚化グラフ内では、放射状ビューまたはレイヤー・ビューを選択できます。どちらのビューでも、画像をズーム・インまたはズーム・アウトできます。ノードを展開または縮小したり、拡大したり、検索できます。セキュリティ項目のタイプを表すノードを強調表示することもできます。

1. ビューを選択するには、コントロール・パネルの視覚化のボタンの中から「レイアウトの切替え」をクリックします。
2. 「放射状」または「レイヤー」を選択します。

ノード・ラベル

ノードを展開または縮小するか、画像をズーム・インまたはズーム・アウトして、視覚化を拡大または縮小できます。実行すると、ノードを識別するラベルが次のように変わります。

- 画像が大きい場合は、各ノードに、それが表している項目の名前が表示されます。
- 画像が小さい場合は、名前ではなく記号が表示されます。「U」はユーザー、「R」はロール、「S」は事前定義済ロール、「P」は権限、「A」集計権限をそれぞれ意味します。
- 画像がさらに小さい場合は、ノードがラベルなしで表示されます。

ラベル付けに関係なく、ノードにカーソルをあわせると、ノードが表すユーザー、ロールまたは権限の名前と説明が表示されます。

ノードは項目のタイプごとに、項目タイプを簡単に区別できるように視覚的に表示されます。

ノードの展開と縮小

ノードを展開すると、そのノードに接続されているロール、権限またはユーザーを表示できます。ノードを縮小すると、これらの項目が非表示になります。ノードを展開または縮小するには、ノードを選択し、右クリックするか、ノードをダブルクリックします。

コントロール・パネル・ツールの使用

放射状またはレイヤー・ビューを選択するオプションとは別に、コントロール・パネルには次のツールが含まれています。

- ズーム・イン: 画像を拡大します。マウス・ホイールを使用してズーム・インすることもできます。
- ズーム・アウト: 画像を縮小します。マウス・ホイールを使用してズーム・アウトすることもできます。
- 合せてズーム: 画像を中央揃えにして、その画像が表示ウィンドウに完全に収まるようにサイズを変更します。(展開済だったノードは展開されたままになります。)
- 拡大: 拡大鏡をアクティブ化し、ノードの上に配置して一時的に拡大します。虫眼鏡を合せた領域を、マウス・ホイールでズーム・インまたはズーム・アウトできます。「拡大」を2回目にクリックすると、拡大鏡が非アクティブ化されます。
- 検索: テキストを入力して、名前に一致するテキストが含まれるノードを検索します。画像が現在展開されて表示されているノードのみを検索できます。
- コントロール・パネル: コントロール・パネルを非表示にするか、または表示します。

凡例の使用

凡例には、現在表示されている項目のタイプがリストされます。次の処理を実行できます。

- 特定の項目タイプのエントリにカーソルを合せれば、画像内の同じタイプの項目が見つかります。他のすべてのタイプの項目はグレー表示されます。
- 項目タイプのエントリをクリックすれば、そのタイプの項目を画像で無効にできます。そのタイプの項目に子ノードがある場合は、項目がグレー表示されます。そうでない場合は、画像から消えます。無効な項目を復元するには、エントリをもう一度クリックします。
- 凡例のボタンをクリックすれば、凡例を非表示または表示にできます。

概要の使用

画像のプラス記号をクリックして「概要」を開き、視覚化のサムネイル・スケッチを開きます。サムネイルの任意の領域をクリックすると、実際の視覚化がその領域にフォーカスされます。

または、視覚化の背景をクリックして、画像全体を任意の方向に移動できます。

イメージの再フォーカス

視覚化画像内の任意のノードを選択して、新しい視覚化の焦点にすることができます。それには、ノードを右クリックして「フォーカスとして設定」を選択します。

注意: ロール階層は、表ビューまたはグラフィカル・ビューでレビューできます。デフォルトの表示は、「管理」タブの「デフォルトの表形式表示可能」オプションの設定によって決まります。

視覚化表の表示オプション

視覚化表には、選択したセキュリティ項目に関連するロール、権限またはユーザーのレコードが含まれます。表には、一度に1つのタイプのみの項目のレコードが表示されます。

- 視覚化のフォーカスとして権限を選択する場合は、ユーザー向けに展開オプションを選択します。そうしないと、表に結果が表示されません。次に、「表示」オプションを使用して、権限を継承するロールまたはユーザーのレコードを表示します。
- 視覚化のフォーカスとしてユーザーを選択する場合は、権限向けに展開オプションを選択します。そうしないと、表に結果が表示されません。次に、「表示」オプションを使用して、ユーザーに割り当てられているロールまたは権限のレコードを表示します。
- 視覚化のフォーカスとして任意のタイプのロールまたは集計権限を選択した場合、どちらの方向にでも展開できます。
    - 権限の方向に展開する場合は、「表示」オプションを使用して、階層の下位のロールまたはフォーカス・ロールに関連する権限のどちらかのレコードをリストできます。
    - ユーザーの方向に展開する場合は、「表示」オプションを使用して、階層の上位のロールまたはフォーカス・ロールに関連するユーザーのどちらかのレコードをリストできます。

表にはすべてが含まれています。

表名	表示内容
ロール	フォーカス項目に直接または間接的に関連するすべてのロールのレコードが表示されます。各ロールでは、直接関連するロールの名前とコードが継承列に指定されています。
権限	フォーカス項目に直接または間接的に関連するすべての権限のレコードが表示されます。各権限では、その権限を直接所有するロールの名前とコードが継承列に表示されます。
ユーザー	フォーカス項目に直接または間接的に関連するロールが割り当てられたすべてのユーザーのレコードが表示されます。各ユーザーでは、そのユーザーに直接割り当てられたロールの名前とコードが割当済列に表示されます。

表の列は検索対応です。列フィールドに検索テキストを入力して、検索テキストに一致するレコードを取得します。表はExcelにエクスポートできます。

セキュリティ・コンソールでのリスク管理ロールの作成

セキュリティ・コンソールを使用して、リスク管理のジョブ・ロールまたは職務ロールを作成できます。

多くの場合、ロールを作成する際には、既存のロールをコピーして、要件にあわせてそのコピーを編集するのが効率的です。通常、作成するロールと類似した既存のロールがない場合は、ロールを最初から作成します。

ロールを最初から作成するには、セキュリティ・コンソールで「ロール」タブを選択し、「ロールの作成」ボタンをクリックします。一連のロール作成ページで値を入力し、「次」または「戻る」を選択して、ページ間をナビゲートします。

基本情報の設定

「基本情報」ページで、次の手順を実行します。

1. 「ロール名」フィールドで、表示名(North America Risk Managerなど)を作成します。
2. 「ロール・コード」フィールドに、ロールの内部名(GRC_NA_RISK_MGR_JOBなど)を作成します。

   注意: ロール・コードの先頭に「ORA_」を使用しないでください。この接頭辞は、Oracleで事前定義されているロール用に予約されています。ORA_の接頭辞が付いたロールは編集できません。
3. 「ロール・カテゴリ」フィールドで、他のロールと共通する目的を識別するタグを選択します。通常、ロール・タイプおよびそのロールが適用されるアプリケーションをタグに指定します。リスク管理の場合、「GRC - ジョブ・ロール」および「GRC - 職務ロール」というタグを付けるのが適切です。

   職務ロール・カテゴリを選択した場合、作成中のロールをユーザーに直接割り当てることはできません。これを割り当てるには、ジョブ・ロールの階層に含めて、そのロールをユーザーに割り当てます。
4. 必要に応じて、「摘要」フィールドにロールの説明を入力します。

機能セキュリティ・ポリシーの追加

機能セキュリティ・ポリシーで一連の機能権限を選択し、各機能権限でフィールドや他のユーザー・インタフェース機能の使用を許可します。「機能セキュリティ・ポリシー」ページで、職務ロールのポリシーを定義できます。ポリシーは、職務ロールが属する他のロールによって継承される機能権限を選択します。通常、機能セキュリティ・ポリシーはジョブ・ロールに直接追加しません。

ポリシーを定義する際には、個別の権限を追加するか、既存のロールに属するすべての権限をコピーできます。

1. 「機能セキュリティ・ポリシーの追加」を選択します。
2. 「検索」フィールドで、「権限」値やロールのタイプを任意の組合せで選択し、少なくとも3文字を入力します。入力した文字が名前に含まれる、選択したタイプの項目が検索結果として返されます。
3. 権限またはロールを選択します。権限を選択する場合は、「ロールに権限追加」をクリックします。ロールを選択する場合は、「選択した権限の追加」をクリックします。

「機能セキュリティ・ポリシー」ページに、選択したすべての権限がリストされます。必要に応じて、権限の継承元のロールも表示されます。次のことが可能です。

- 権限をクリックすると、その権限が保護しているコード・リソースの詳細が表示されます。
- 権限を削除します。たとえば、ロールに関連付けられている権限を追加しますが、その一部のみを使用する場合は、残りの権限を削除する必要があります。権限を削除するには、その「x」アイコンをクリックします。

データ・セキュリティ・ポリシー

データ・セキュリティ・ポリシー(セキュリティ・コンソールで構成可能)は、リスク管理以外のOracle Cloudアプリケーションに適用されます。リスク管理に適したデータ・セキュリティ・ポリシーを作成するには、リスク管理の「セキュリティの管理」ページを使用します。セキュリティ・コンソールの「ロールの作成」トレインにある「データ・セキュリティ・ポリシー」ページには、エントリを作成しないでください。単に「次へ」をクリックして、次のページに移動します。

注意: リスク管理用に、「データ・セキュリティ・ポリシー」ページを読取り専用に設定することもできます。これを行うには、「管理」タブを選択して、「管理」ページの「ロール」タブを選択します。「データ・セキュリティ・ポリシーの編集可能」オプションを見つけて選択を解除します。

ロール階層の構成

「ロール階層」ページには、作成中のロールがフォーカスされた視覚化グラフまたは視覚化表が表示されます。「グラフの表示」ボタンまたは「表として表示」ボタンを選択して、どちらかを選択します。いずれの場合も、作成しているロールを、機能権限の継承元である他のロールにリンクします。

- 職務ロールを作成している場合は、それに職務ロールを追加できます。実際には、ジョブ・ロールに組み込む職務セットを拡張していることになります。
- ジョブ・ロールを作成している場合は、それに職務ロールを追加できます。

ロールを追加するには、次の手順を実行します。

1. 「ロールの追加」を選択します。
2. 「検索」フィールドで、ロール・タイプの組合せを選択し、少なくとも3文字を入力します。入力した文字が名前に含まれる、選択したタイプの項目が検索結果として返されます。

3. 必要なロールを選択し、「ロール・メンバーシップの追加」をクリックします。選択したロールだけでなく、階層全体も追加します。

グラフ・ビューでは、視覚化のコントロール・パネル、凡例および概要ツールを使用して、ロール階層を定義するノードを操作できます。

ユーザーの追加

「ユーザー」ページで、作成中のジョブ・ロールを割り当てるユーザーを選択できます。(職務ロールはユーザーに直接割り当てません。)

注意: 「ユーザー」ページをアクティブにするには、「ユーザー・ロール・メンバーシップの編集可能」オプションを選択する必要があります。これを見つけるには、「管理」タブを選択して、「管理」ページの「ロール」タブを選択します。このオプションを選択しないと、「ユーザー」ページは読取り専用になります。

データ・セキュリティ・ポリシーにジョブ・ロールをマップする前に、ジョブ・ロールにユーザーを追加できます。その場合ユーザーは、ロールで機能アクセス権が付与されているページにアクセスできますが、データにはアクセスできません。データ・セキュリティ・ポリシーにロールをマップすると、これらのページにデータが表示されます。

ユーザーを追加するには、次のようにします。

1. 「ユーザーの追加」を選択します。
2. 「検索」フィールドで、「ユーザー」値やロールのタイプを任意の組合せで選択し、少なくとも3文字を入力します。入力した文字が名前に含まれる、選択したタイプの項目が検索結果として返されます。
3. ユーザーまたはロールを選択します。ユーザーを選択する場合は、「ロールにユーザー追加」をクリックします。ロールを選択した場合、「選択したユーザーの追加」をクリックします。これにより、割り当てられたすべてのユーザーが、作成しているロールに追加されます。

選択したすべてのユーザーが「ユーザー」ページにリストされます。ユーザーを削除できます。たとえば、ロールに関連付けられているすべてのユーザーを追加したとします。ただし、一部のユーザーのみに新しいロールを割り当てる場合は、残りを削除する必要があります。ユーザーを削除するには、その「x」アイコンをクリックします。

ロールの完了

「サマリーおよび影響レポート」ページで、選択内容をレビューします。サマリー・リストには、追加および削除した機能セキュリティ・ポリシー、ロールおよびユーザーの数が表示されます。影響リストには、自分の変更の影響を受けるロールおよびユーザーの数が表示されます。これらのリストのいずれかを展開すれば、その数に含まれるポリシー、ロールまたはユーザーの名前を表示できます。

変更する必要がある場合は、適切なページに戻って変更します。ロールに問題がなければ、「保存してクローズ」を選択します。

セキュリティ・コンソールでのリスク管理ロールの

コピーまたは編集

最初から作成したロールを編集できます。または、任意のロールをコピーし、そのコピーを編集して新しいロールを作成できます。

注意: 事前定義済のロールは編集できません。これは、オラクル社が新しいリリースの仕様で事前定義済ロールを更新すると、アップグレードするたびに編集内容が上書きされるためです。事前定義済ロールは、ロール・コードの「ORA_」という接頭辞によって識別できます。または、オラクル社から出荷されたロールの場合は、「基本情報」ページの「事前定義ロール」チェック・ボックスが選択されています。

セキュリティ・コンソールの「ロール」タブからコピーまたは編集を開始します。次のいずれかを実行します。

- 視覚化グラフを作成し、そのロールのいずれかを選択します。右クリックして「ロールのコピー」または「ロールの編集」を選択します。
- 「ロール」ページの「検索結果」列でロールのリストを生成します。いずれかを選択して、そのメニュー・アイコンをクリックします。メニューで、「ロールのコピー」または「ロールの編集」を選択します。

ロールをコピーする場合は、次の2つのオプションのいずれかを選択する必要があります。

- 最上位ロールのコピー: 選択したロールのみをコピーします。ソース・ロールには階層内のロールへのリンクがあり、そのコピーはそれらのロールの元のバージョンへのリンクを継承します。このオプションを選択した場合、継承されたロールに対する以降の変更は、ソースの最上位ロールのみでなくコピーにも影響します。
- 最上位ロールと継承されたロールのコピー: 選択したロールのみでなく、その階層内のすべてのロールもコピーします。最上位ロールのコピーは、下位ロールの新しいコピーに接続されます。このオプションを選択した場合は、継承されたロールの元のバージョンが変更されても、コピーされたロールには影響しません。

次に、編集トレインが開きます。基本的に、ロールを作成する場合と同じプロセスでロールを編集します。ただし、次の点に注意してください。

- ロール作成の場合と同様に、「ロールの編集」トレインの「データ・セキュリティ・ポリシー」ページはリスク管理には適用されません。リスク管理の「セキュリティの管理」ページを使用して、リスク管理に適したデータ・セキュリティ・ポリシーを作成または編集してください。
- デフォルトでは、コピーされたロールの名前とコードはそのソース・ロールの名前とコードに一致しますが、接頭辞、接尾辞、またはその両方が追加される点が異なります。ロール管理ページで、デフォルトの接頭辞と接尾辞を値ごとに構成できます。
- コピーしたジョブ・ロールは、ソース・ジョブ・ロールからユーザーを継承できません。コピーしたロールのユーザーを選択する必要があります。(ソース・ロールに属するユーザーを含めることができます。)
- 「ロール階層」ページには、コピーしたロールの下位にあるすべてのロールが表示されます。しかし、ロールを追加または削除できるのは、コピーした最上位ロールのみです。

ロールコピー・ジョブのステータスを監視するには、「管理」タブを選択して、「管理」ページの「ロール・コピー・ステータス」タブを選択します。

ロールの比較

任意の2つのロールを比較して、その構造的な相違を確認できます。第2ロールが事前定義済ロールではない場合は、ロールを比較するときに、最初のロールに存在する機能セキュリティ・ポリシーを2番目のロールに追加することもできます。

たとえば、ロールをコピーしてそのコピーを編集したとします。その後、新しいリリースにアップグレードします。前のリリースから編集したロールと、後のリリースで出荷されたロールを比較できます。その後、編集したロールにアップグレードの変更内容を組み込むかどうかを決定できます。変更内容が新しい機能セキュリティ・ポリシーである場合は、編集したロールに新しいポリシーを追加してアップグレードできます。

比較するロールの選択

1. セキュリティ・コンソールで「ロール」タブを選択します。
2. 次のいずれかを実行します。
   - 「ロールの比較」ボタンをクリックします。
   - 視覚化グラフを作成し、そのロールの1つを右クリックして、「ロールの比較」オプションを選択します。
   - 「ロール」ページの「検索結果」列でロールのリストを生成します。いずれかを選択して、そのメニュー・アイコンをクリックします。メニューで、「ロールの比較」を選択します。
3. 比較するロールを選択します。
   - 「ロールの比較」ボタンをクリックして開始した場合は、「第**1**ロール」フィールドと「第**2**ロール」フィールドの両方でロールを選択します。
   - 視覚化グラフまたは「検索結果」列のロールの選択から開始した場合は、選択したロールの名前が「第**1**ロール」フィールドに表示されます。「第**2**ロール」フィールドで、別のロールを選択します。

   どちらのフィールドでも、検索アイコンをクリックしてテキストを入力し、そのテキストを含む名前を持つロールのリストから目的のロールを選択します。

ロールの比較

1. 比較するロールを2つ選択します。
2. 「フィルタ基準」フィールドを使用して、次のアーティファクトを任意に組み合せて、2つのロールをフィルタリングします。
   - 機能セキュリティ・ポリシー
   - 継承されたロール

   データ・セキュリティ・ポリシー・オプションは、リスク管理には適用されません。
3. 「表示」フィールドを使用して、次の結果を比較で返すかどうかを決定します。
   - 各ロールに存在するすべてのアーティファクト
   - 一方のロールにのみ存在するか、もう一方のロールにのみ存在するアーティファクト
   - 両方のロールに存在するアーティファクトのみ
4. 「比較」ボタンをクリックします。

比較の結果をスプレッドシートにエクスポートできます。「**Excel**にエクスポート」オプションを選択します。

最初の比較を作成した後、フィルタ・オプションと表示オプションを変更できます。変更すると、新しい比較が自動的に生成されます。

ロールへのポリシーの追加

1. 比較するロールを2つ選択します。
   - 「第1ロール」として、ポリシーがすでに存在するロールを選択します。
   - 「第2ロール」として、ポリシーを追加するロールを選択します。これはカスタム・ロールである必要があります。事前定義済のロールは変更できません。
2. 「フィルタ基準」フィールドで、「機能セキュリティ・ポリシー」を選択します。「データ・セキュリティ・ポリシー」オプションはリスク管理には適用されず、「継承されたロール」オプションはすべてのアプリケーションに対して除外されます。
3. 「表示」の値として、「第1ロールでのみ」を選択します。
4. 「比較」ボタンをクリックします。
5. 比較で返されたアーティファクトの中から、コピーするアーティファクトを選択します。
6. 「第2ロールに追加」オプションがアクティブになります。これを選択します。

セキュリティ・コンソールのナビゲータ・メニューのシミュレート

ロールまたはユーザーに対して使用できるナビゲータの各メニューをシミュレートできます。シミュレーションから、ロールに固有のアクセス権、またはユーザーに付与されたアクセス権をレビューできます。また、そのアクセス権を変更してロールを作成する方法も決定できます。

シミュレーションのオープン

シミュレートされたメニューを開くには、次のようにします。

1. セキュリティ・コンソールで「ロール」タブを選択します。
2. 視覚化グラフを作成します。または、ロールまたはユーザーを選択して「検索結果」列に情報を移入します。
3. 視覚化グラフで、ロールまたはユーザーを右クリックします。または、「検索結果」列で、ユーザーまたはロールを選択して、そのメニュー・アイコンをクリックします。
4. 「ナビゲータのシミュレート」を選択します。

シミュレーションの操作

「ナビゲータのシミュレート」ページで、次の手順を実行します。

- 「すべて表示」を選択すると、「ナビゲータ」メニューに含めることができるすべてのメニューとタスクのエントリが表示されます。
- 付与されたアクセス権の表示を選択すると、選択したロールまたはユーザーに実際に割り当てられているメニューおよびタスクのエントリが表示されます。

どちらのビューでも、次のようになります。

- 南京錠のアイコンは、メニューまたはタスクのエントリをロールまたはユーザーに対して承認できる(ただし今はできない)ことを示します。
- 感嘆符のアイコンは、項目が変更されたために、その権限を持つユーザーまたはロールに対して非表示になる可能性がある項目を示しています。

この承認をどのように変更するかを計画する手順:

1. 「ナビゲータのシミュレート」ページで任意のメニュー項目をクリックします。
2. 次の2つのオプションのどちらかを選択します。
    - アクセス権を付与するロールの表示: メニュー項目に対するアクセス権を付与するロールがリストされます。
    - メニューに必要な権限の表示: メニュー項目へのアクセスに必要な権限がリストされます。

ロールの分析

Oracle Cloudインスタンスに存在するロールに関する統計をレビューできます。

「分析」ページで、「ロール」タブをクリックします。次に、次の分析を表示します。

- ロール・カテゴリ。各ロールは、共通の目的が定義されたカテゴリに属しています。通常、1つのカテゴリには、1つのアプリケーションのために構成されたロール・タイプ(たとえば「財務 - 職務ロール」)が含まれています。
  各カテゴリについて、「ロール・カテゴリ」グリッドに次のものの数が表示されます。
    - ロール
    - ロール・メンバーシップ(カテゴリ内の他のロールに属しているロール)
    - それらのロールに対して作成されるセキュリティ・ポリシー

  さらに、「カテゴリ別ロール」円グラフによって、各カテゴリのロール数が他のカテゴリと比較されます。
- カテゴリ内のロール。「ロール・カテゴリ」グリッドでカテゴリをクリックすると、そのカテゴリに属するロールがリストされます。各ロールについて、「カテゴリ内のロール」グリッドに次のものの数も表示されます。
    - ロール・メンバーシップ
    - セキュリティ・ポリシー
    - ロールに割り当てられたユーザー
- 個々のロールの統計。「カテゴリ内のロール」グリッドでロールの名前をクリックすると、そのロールに関連付けられているセキュリティ・ポリシーおよびユーザーがリストされます。このページには、ロールが所属する階層の縮小可能な図も表示されます。
  「エクスポート」をクリックすると、このページからスプレッドシートへデータをエクスポートできます。

セキュリティ・コンソールの管理

セキュリティ・コンソールを使用できるように準備するために、セキュリティ・データをリフレッシュするバックグラウンド・プロセスが実行されるように用意します。セキュリティ・コンソールの「管理」ページを使用して、一般オプションとロール指向のオプションを選択し、ロールコピー・ジョブのステータスを追跡できます。通知テンプレートを選択、編集または追加することもできます。

バックグラウンド・プロセスの実行

実行する必要があるバックグラウンド・プロセスを次に示します。

- 最新の**LDAP**変更の取得: このプロセスでは、LDAPディレクトリのデータがOracle Cloud Applicationsのセキュリティ表にコピーされます。これは実装時に1回実行します。
- ユーザーおよびロールのインポートのアプリケーション・セキュリティ・データ: このプロセスは、ユーザー、ロール、権限およびデータ・セキュリティ・ポリシーを、アイデンティティ・ストア、ポリシー・ストアおよびOracle Cloud Applicationsのセキュリティ表からコピーします。これらの表を更新するために、このプロセスの定期的な実行をスケジュールします。

「最新の**LDAP**変更の取得」プロセスを実行するには、次の手順を実行します。

1. 「設定および保守」作業領域で、「ユーザーおよびロール同期化プロセスの実行」タスクを検索して選択します。
2. 「送信」をクリックします。
3. 確認メッセージを確認し、「**OK**」をクリックします。

「ユーザーおよびロールのインポートのアプリケーション・セキュリティ・データ」プロセスを実行するには、次の手順を実行します。

1. 「ツール」作業領域で、「スケジュール済プロセス」を選択します。
2. 「新規プロセスのスケジュール」をクリックします。
3. 「ユーザーおよびロールのインポートのアプリケーション・セキュリティ・データ」プロセスを検索して選択します。
4. 「**OK**」をクリックします。
5. 「送信」をクリックします。
6. 確認メッセージを確認し、「**OK**」をクリックします。

一般的な管理オプションの構成

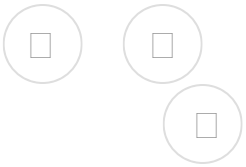
1. セキュリティ・コンソールで、「管理」をクリックします。
2. 「証明書プリファレンス」で証明書の有効期間のデフォルト日数を設定します。証明書は、Oracle Cloudアプリケーションが他のアプリケーションと交換するデータの暗号化および復号化に使用するキーを確立します。
3. 「同期プロセス・プリファレンス」で、「ユーザーおよびロールのインポートのアプリケーション・セキュリティ・データのインポート」プロセスが最後に実行されてからの時間数を指定します。「ロール」タブを選択すると、この期間にプロセスが実行されていない場合は警告メッセージが表示されます。

ロール管理オプションの構成

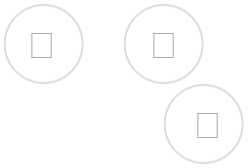
1. セキュリティ・コンソールで、「管理」をクリックします。
2. 「ロール」タブで、ロール・コピーの名前およびコードに追加する接頭辞および接尾辞を指定します。各ロールにはロール名(表示名)とロール・コード(内部名)があります。ロール・コピーでは、ソース・ロールの名前とコードが採用され、この接頭辞または接尾辞(あるいは両方)が追加されます。このように追加して、コピーとソースを区別します。デフォルトでは、接頭辞はなし、ロール名の接尾辞は「Custom」、ロール・コードの接尾辞は「_CUSTOM」です。
3. 「グラフ・ノード制限」フィールドで、視覚化グラフに表示できるノードの最大数を設定します。視覚化グラフに多数のノードが含まれる場合、視覚化によって表ビューが推奨されます。
4. 「ロール」タブから生成された視覚化を放射状グラフ・ビューにする場合は、「デフォルトの表形式表示可能」の選択を解除します。
5. データ・セキュリティ・ポリシーの編集可能:「ロール」タブから使用できるロール作成トレインおよびロール編集トレインの「データ・セキュリティ・ポリシー」ページに、ユーザーがデータを入力できるかどうかを決定します。
6. ユーザー・ロール・メンバーシップの編集可能:「ロール」タブから使用できるロール作成トレインおよびロール編集トレインの「ユーザー」ページに、ユーザーがデータを入力できるかどうかを決定します。

ロール・コピー・ステータスの表示

1. セキュリティ・コンソールで、「管理」をクリックします。
2. 「ロール・コピー・ステータス」タブでは、ロールをコピーするジョブのレコードを表示できます。これらのジョブは「ロール」ページで開始されたものです。ジョブのステータスは、最終ステータス(通常は「完了済」)になるまで自動的に更新されます。
3. 「削除」アイコンをクリックすると、コピー・ジョブを表す行を削除できます。



リスク管理の保護



4 データ・セキュリティ

この章の内容は次のとおりです。

リスク管理データ・セキュリティ・ポリシーの概要

リスク管理のデータ・セキュリティ・ポリシーは、ポリシーでアクセス権が付与されたデータを選択するフィルタで構成されています。各フィルタは、属性と値の関係を表しています。定義された関係を満たすデータに対してアクセス権を付与できます。または、そのようなアクセスを禁止するように構成して、他のすべてのデータへのアクセス権を付与することもできます。

たとえば、属性が「地域」などの観点の名前である場合があります。この場合の値はその観点のノード(「北米」など)になります。次に、作成された時に「北米」という値が割り当てられたオブジェクトのレコードがフィルタで選択されます。または、これらのオブジェクトを除外して、他のすべての地域に関連付けられたオブジェクトを選択することもできます。

データ・セキュリティ・ポリシーは、セキュリティ・コンソールで管理されているロールにマップされます。ロールによって付与される機能アクセスは、マップされたデータ・セキュリティ・ポリシーによって指定されたデータに適用されます。

事前定義済の職務ロールで構成される階層を、各ジョブ・ロールで定義するようにジョブ・ロールを設計できます。その場合は、職務ロール用のデータ・セキュリティ・ポリシーを作成する必要がありません。これは、すべての事前定義済ロールが事前定義済データ・セキュリティ・ポリシーにマップされているためです。リスク管理を初めて実行すると、セキュリティ同期化プロセスにより、そのマッピングが自動的に完了します。

それでも、自分が設計したジョブ・ロールに対してデータ・セキュリティ・ポリシーを作成する場合があります。これらのポリシーは、観点を割り当てることができるオブジェクトをユーザーが直接操作できるようにするロールに適用します。財務レポート・コンプライアンスでは、プロセス、リスクおよび統制がこれらに含まれます。拡張財務管理では、モデル、拡張統制およびインシデントがこれらに含まれます。通常このようなポリシーのフィルタは、次のように動作します。

- ジョブ・ロールの階層に含まれるすべての職務ロールにすでにマップされているデータ・セキュリティ・ポリシーを選択する。ここまでのポリシーでは、そのメンバー・ポリシーで定義されているすべてのデータへのアクセス権が付与されます。
- 観点値を選択する。ジョブレベルのポリシーでは、その職務レベルのポリシーによって付与されるアクセス権が、観点値が関連付けられたデータに制限されるようになります。

注意: ここでは、ジョブ・レベルで観点ベースのデータ・セキュリティを実装するための戦略を説明しています。職務レベルでも観点ベースのセキュリティを実装できますが、お薦めしません。職務レベルのアプローチでは、より多くのロールとポリシーの作成および保守が必要になります。

職務ロールを作成できます。その場合は、それらのデータ・セキュリティ・ポリシーを作成する必要があります。これらのポリシーのフィルタでは、次を指定できます。

- モジュール・データの適用先。
- 1つ以上の状態(ポリシーが状態にアクセス権を付与するためには、状態にデータが存在している必要があります)。
- 指定したいずれかの状態のデータに対して実行できる処理。
- (オプション)他の職務レベルのデータ・セキュリティ・ポリシー。それらのポリシーが付与するデータ・アクセス権も取り入れる場合に指定します。
- 「アクティビティ」観点の値(ロールがアセスメント・アクティビティをサポートしている場合)。これにより、ポリシーの対象が特定のタイプのアセスメントに必要なデータに限定されます。

事前定義済職務ロールをコピーしてコピーを変更できます。その場合は、ソース・ロールにマップされているデータ・セキュリティ・ポリシーをコピーし、コピーしたポリシーをコピーしたロールにマップできます。

データ・セキュリティ・ポリシーを操作するには、ホーム・ページで「リスク管理ツール」を選択します。オプションの中から「設定および管理」を選択します。次に、「セキュリティ構成」タブを選択します。

関連項目

- 観点

リスク管理データ・セキュリティ・ポリシーの作成または編集

リスク管理のデータ・セキュリティ・ポリシーを作成するには、次のようにします。

1. 「セキュリティの管理」ページで「データ・セキュリティ・ポリシーの作成」処理を選択します。
2. ポリシーの名前および必要に応じて摘要を指定します。ステータスとして、「アクティブ」または「非アクティブ」を選択します。
3. 「ポリシー」セクションで「追加」を選択します。新しい行が表示されるので、そこにフィルタを定義します。「フィルタ名」フィールドに、名前を入力します。
4. フィルタで観点値を指定する場合は、「オブジェクト」フィールドで「観点」を選択します。他のタイプのフィルタには、「データ属性」を選択します。
5. 「オブジェクト」フィールドで「データ属性」を選択した場合は、「属性」フィールドを使用して、作成するフィルタに適した値を選択します。
   - 「モジュール」。特定のモジュールのデータへのアクセス権を付与するフィルタの場合は、財務レポート・コンプライアンスまたは拡張統制管理のどちらかです。一般に、モジュール・フィルタは職務ロールにマップするポリシーに適しています。
   - 「状態」。1つ以上の状態を選択するフィルタの場合は、ポリシーがアクセス権を付与する状態にデータが存在する必要があります。一般に、状態フィルタは職務ロールにマップするポリシーに適しています。
   - 「状態に基づく処理」。指定した状態のデータに実行できる処理を指定するフィルタの場合。一般に、「状態に基づく処理」フィルタは職務ロールにマップするポリシーに適しています。
   - 「データ・ポリシー」。別のポリシーを選択するフィルタの場合は、そのデータ定義も適用されます。一般に、データ・ポリシー・フィルタは職務ロールにマップするポリシーに適しています。

   「オブジェクト」フィールドで「観点」を選択した場合は、「属性」フィールドで観点階層の名前を選択します。観点フィルタはジョブ・ロールにマップするポリシーによく適用されます。ただし、アセスメント・アクティビティをサポートする職務ロールにマップするポリシーに使用することもあります。
6. 「オブジェクト」フィールドで「データ属性」を選択した場合は、「条件」フィールドで「次と等しい」または「次と等しくない」を選択します。

   「オブジェクト」フィールドで「観点」を選択した場合は、「条件」フィールドで「次と等しい」、「次と等しくない」または「子を含める」を選択します。最後の指定では、選択したノードとそのすべての子ノードに関連付けられたデータがフィルタに指定されます。
7. 「値」フィールドで「追加」ボタンをクリックし、「属性」および「条件」フィールドですでに開始した関係定義を完了するための値を選択します。

たとえば、属性が「状態」で、条件が「次と等しい」の場合、値は特定の状態の名前(「編集中」など)にします。これにより、指定した名前の状態で存在するデータが指定されます。または、「次と等しくない」条件を選択した場合は、指定した名前以外のすべての状態で存在するデータがフィルタに指定されます。

または、属性が「アクティビティ・タイプ」の観点である場合もあります。条件が「次と等しい」の場合は、値を「アクティビティ・タイプ」階層のノードの名前(「証明」など)にできます。こうすると、そのノードに関連付けられているデータが指定されます。

8. 「含める」を選択して定義したデータへのアクセスを許可するか、「除外」を選択してそのデータへのアクセスを禁止します。
9. ポリシーに必要な残りのフィルタごとにこれらのステップを繰り返します。

ポリシーを編集するには、次のようにします。

- 「セキュリティの管理」ページでポリシーを選択し、「データ・セキュリティ・ポリシーの編集」処理を選択します。
- フィルタを追加または変更できます。ポリシーを作成する場合と同様に作業します。
- フィルタを削除できます。フィルタを選択し、「削除」処理を選択します。

ポリシーでの複数の観点値の適用方法

データ・セキュリティ・ポリシーには、複数の観点値を指定するフィルタを含めることができます。

- フィルタで列挙されている観点値は1つでも、「子を含む」条件を使用している場合があります。その場合は、選択したノードまたはその子ノードのいずれかでタグ付けされたオブジェクトがフィルタで選択されます。
- (セミコロンで区切った)複数の観点値を1つのフィルタに含めることができます。その場合は、OR (論理和)が適用されます。いずれかの値または値の組合せでタグ付けされたオブジェクトがフィルタで選択されます。
- 複数のフィルタを含めて、それぞれに観点値を指定できます。その場合は、AND (論理積)が適用されます。すべてのフィルタの値でタグ付けされたオブジェクトのみへのアクセス権がポリシーで付与されます。

たとえば、「組織」観点に「Division1」、「Division2」および「Division3」の3つの値があるとします。1つのフィルタで「組織」観点を列挙し、値として「Division1;Division2」を含めます。このフィルタを含むポリシーでは、「Division1」、「Division2」またはその両方でタグ付けされたオブジェクトが選択されます。「Division3」でタグ付けされたオブジェクトは、そのオブジェクトが「Division1」または「Division2」でもタグ付けされている場合以外は選択されません。

次に、「地域」観点に「North」と「South」の2つの値があるとします。ポリシーには、組織がDivision1に等しい1つ目のフィルタと、リージョンがNorthに等しい2つ目のフィルタが含まれます。このポリシーでは、「Division1」と「North」の両方の値でタグ付けされたオブジェクトのみが選択されます。

最後に、ポリシーに「組織」値が「Division1;Division2」に設定された1つ目のフィルタと、リージョンが「North」に設定された2つ目のフィルタがあるとします。このポリシーでは、「Division1」と「North」の値または「Division2」と「North」の値のどちらかでタグ付けされたオブジェクトが選択されます。

ロールへのリスク管理データ・セキュリティ・ポリシーのマッピング

リスク管理の「セキュリティの管理」ページを使用して、職務ロールまたはジョブ・ロールをデータ・セキュリティ・ポリシーにマップします。これを行えるのは、セキュリティ・コンソールで最初から作成したロール、または既存のロールのコピーを編集して作成したロールに対してのみです。ポリシーへの事前定義済ロールのマッピングは変更できません。

ロールのデータ・セキュリティ・ポリシーを選択するには、次のようにします。

1. 「セキュリティの管理」ページの「セキュリティ・オブジェクト」リージョンで、データ・セキュリティ・ポリシーをマップするロールを検索します。

   注意: セキュリティ・コンソールで作成したロールがリスク管理で認識されるようにするには、セキュリティ同期化プロセスを実行する必要があります。デフォルトでは、毎週実行されるようにスケジュールされています。このプロセスが最後に実行された後に作成されたロールを操作する場合は、次の定期実行を待つことができます。または、「設定および管理」作業領域の「スケジューリング」タブにある「スケジューリング」ページから手動でこれを実行することもできます。

2. 次のいずれかを実行します。
   - ロールの行をクリックして「編集」アイコンを選択します。
   - ロールの名前をクリックして、ロールの詳細が表示されるページを開きます。そのページで、「編集」ボタンをクリックします。
3. 「編集」ページが開きます。「選択した権限」リージョンを使用して、ロールのデータ・セキュリティ・ポリシーを追加または削除します。
   - ポリシーを追加するには、「追加」処理を選択します。次に、「権限」ダイアログで検索して、1つ以上のポリシーを選択します。(任意の数のデータ・セキュリティ・ポリシーをロールに適用できます。)「OK」をクリックして選択を完了し、ダイアログを閉じます。
   - ポリシーを削除するには、「選択した権限」リージョンでその行を選択し、「削除」処理を選択します。
4. 選択内容に問題がなければ、「保存してクローズ」をクリックします。

ロールへのデータ・セキュリティ・ポリシー・マッピングの例

特定の状況下では、単一のデータ・セキュリティ・ポリシーを特定のロールにマップできます。他の状況では、複数のポリシーをロールにマップできます。同じ機能アクセスが指定されたロールのコピーを複数作成して、異なるデータ・セキュリティ・ポリシーをそれぞれにマップできます。

次の例では、会社に2つのビジネス・ユニットがあるとします。一方はロサンゼルスの業務用で、他方はニューヨークの業務用です。

ロールへの単一のポリシーのマップ

David Chetleyはロサンゼルスのビジネス・ユニットの統制管理を担当し、Neil Sturbushはニューヨークのビジネス・ユニットで同じ仕事を担当しています。同じ機能アクセス権が両方に必要ですが、それぞれ自分のビジネス・ユニットに適したデータに限定する必要があります。

1つのセットの機能権限に別々のセットのデータ・アクセス権を割り当てるには、次のようにします。

- 統制管理に必要な機能アクセスが含まれるジョブ・ロールの作成作業から始めます。ジョブ・ロールのコピーを2つ(ビジネス・ユニットごとに1つずつ)作成します。一方をControlManagerLA、他方をControlManagerNYと呼ぶことにします。
- 「組織」観点階層を作成します。ここに会社の構造をマップするので、ビジネス・ユニットを表すノードも含めます。これらのノードをBU_LAおよびBU_NYという名前にします。
- 2つのデータ・セキュリティ・ポリシー(ビジネス・ユニットごとに1つずつ)を作成します。これらには職務ロール(ジョブロールのコピーの階層)にマップされたポリシーを選択するフィルタが含まれており、大部分が類似しています。しかしLAControlPolicyの方には、BU_LAの値を選択する観点フィルタが含まれています。もう一方のNYControlPolicyには、BU_NYの値を選択する観点フィルタが含まれています。
- LAControlPolicyをControlManagerLAジョブ・ロールにマップし、David Chetleyに割り当てます。NYControlPolicyをControlManagerNYジョブ・ロールにマップし、Neil Sturbushに割り当てます。

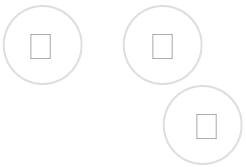
ロールへの複数ポリシーのマップ

Barry Campbellは、David ChetleyおよびNeil Sturbushの仕事を監督するため、両方のビジネス・ユニットのデータにアクセスする必要があります。このアクセス権を付与するために、ControlManagerAllという名前で、ベース・ジョブ・ロールのコピーをもう1つ作成できます。次に、LAControlPolicyおよびNYControlPolicyの両方のデータ・セキュリティ・ポリシーをこのロールにマップしてBarry Campbellに割り当てます。

リスク管理のデータ・セキュリティ・ポリシーにマップされたロールを編集するとどうなりますか。

「アプリケーション・セキュリティ」でロールを編集しても、リスク管理のデータ・セキュリティ・ポリシーへのマッピングには影響しません。(ただし、ロールの変更後も、データ・セキュリティ・ポリシーへのロールのマッピングが引き続き適切かどうかを考慮することをお薦めします。)

「アプリケーション・セキュリティ」でロールを削除すると、データ・セキュリティ・ポリシーへのマッピングがリスク管理から削除されます。データ・セキュリティ・ポリシーは変更されないため、他のロールにマップできます。



Integrated Cloud Applications & Platform Services

リスク管理の保護

用語集

D | J | P | R

D

データ・セキュリティ・ポリシー
データを選択する一連のフィルタ。ポリシーは職務ロールまたはジョブ・ロールにマップされます。これらのロールの1つを割り当てられたユーザーは、マップ済ポリシーによって定義されたデータにアクセスでき、ロールによって定義された機能をそのデータに適用できます。

職務ロール

特定のタスクまたは一連の関連タスクを完了するために必要な権限に対するアクセス権の付与。

J

ジョブ・ロール

幅広いタスクを完了するために必要な職務に対するアクセス権の付与。ジョブ・ロールは、ユーザーに割り当てることができます。すべての個人が必要な業務を遂行できるように、ジョブ・ロールを組み合せて割り当てます。

P

観点階層

関連する階層構造の値のセット。リスク管理オブジェクトに観点値を割り当てて、それらのオブジェクトが存在するコンテキストを定義します。財務レポート・コンプライアンスでは、これらのオブジェクトにはプロセス、リスクおよび統制が含まれます。拡張統制管理では、これらのオブジェクトにはモデル、拡張統制およびインシデントが含まれます。これらはフィルタリング値として機能しますが、Risk Management Cloudの保護においても重要な役割を果たします。

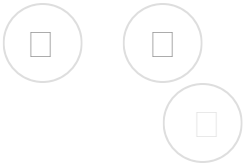
権限

アプリケーションがユーザーに使用可能にできる特定の機能。

R

ロール階層

ロール間の親子関係の定義。親ロールは、階層内の子ロールから機能アクセス権を継承します。たとえば、ジョブ・ロールの階層には職務ロールを含めることができ、職務ロールの階層には、さらに絞り込んだ職務ロールを含めることができます。



- Terms of Use and Privacy
-
- Ad Choices

Oracle

Integrated Cloud Applications & Platform Services