SOLUTION BRIEF
アイデンティティおよびアクセス・ガバナンス

CA Identity Suite によるアイデンティティ・ガバナンスの簡略化とリスク緩和

ca technologies

セクション 1 : 課題

アイデンティティ・ガバナンスの課題

IT システムの各ユーザに正しい権限を割り当てることは、現在 IT が直面している最も重要な課題の 1 つです。そのため、ガバナンス・プログラムを設計する際には、次の機能分野が最も重要です。

- **ユーザ・エクスペリエンス** — アイデンティティ・サービスは多くの場合、ビジネス・ユーザではなく IT に精通したユーザに焦点を当てた不便なユーザ・インタフェースが問題となっています。これはユーザ満足度を低下させ、企業全体での普及を妨げます。ガバナンスの活動では、アイデンティティ・サービスに対応するのは多くの場合、ビジネス・マネージャであるため、この点は特に重要です。
- **特権ユーザのガバナンス** — 多くの組織では、特権ユーザの正式なガバナンスが存在しないか、あったとしても、特権ユーザや正規ユーザに対するそのメカニズムには一貫性がありません。そのような組織では、管理コストと違反リスクが増大します。
- **役割検出とライフサイクル管理** — 効果のない役割モデルは、多くの兆候によって特定できます。組織によっては、ユーザより多くの役割があったり、1 つの役割に関連付けられているユーザまたはリソースの数が多すぎたり、役割モデルで管理している例外数が多すぎることがあります。多くの場合、組織は管理コストやリスクを増大させる「事実上の」役割が存在することさえ知りません。
- **アイデンティティ・コンプライアンス** — 現在の高度に分散した組織では特に、権限のレビューと承認、正確な役割の維持、アイデンティティのコンプライアンスに役立つビジネス全体にわたるプロセスが必要です。そのようなプロセスには、ビジネス・ユーザのニーズを最もよく理解しているライン・マネージャが参加することが必要です。認定に対する自動化されたビジネス指向のアプローチは、コンプライアンスを証明する上で重要なだけでなく、認定するビジネス・マネージャの生産性を向上させる上でも重要です。
- **権限の品質** —「権限の蓄積」は、すべての IT セキュリティ管理者にとってよくある問題です。不要な権限を削除し、既存の権限が職務分離（SoD）やその他のセキュリティ・ポリシーに違反しないように、すべてのユーザの権限を慎重に監視する必要があります。

アイデンティティ・ガバナンスの課題 - 詳細

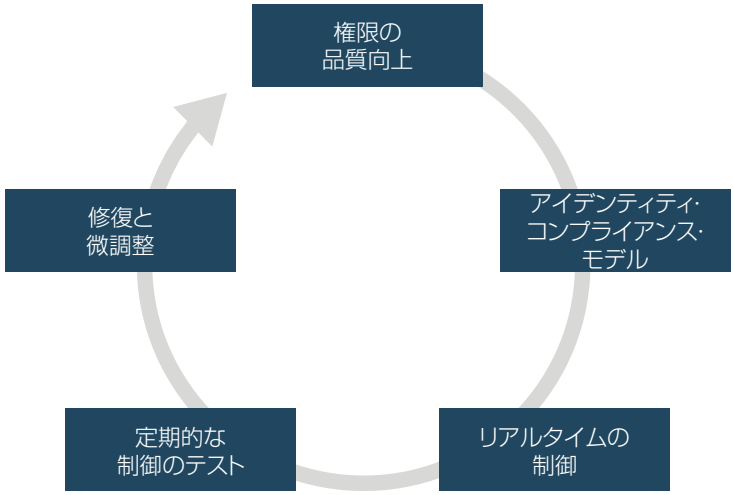
アイデンティティ・コンプライアンス

アイデンティティ･コンプライアンスの活動は、ユーザが保持しているアクセス権が規定要件と内部のセキュリティ･ポリシーを遵守していることを確認することに重点を置いています。そのためには、通常は以下の手順を含む、反復プロセスによるライフサイクルへのアプローチが必要になります。

- データ収集、アクセス権と該当する所有者の相関付け、および不要なエンティティ（孤立アカウント、過剰なアクセスなど）の基本的なクリーンアップを行う
- 規定を管理ポリシーにマッピングし（制御の目標として）、これらの制御の目標を職務分離の制約などの IT 制御の実装にマッピングするなど、アイデンティティ・コンプライアンス・モデルを策定する
- 特権クリーンアップ、認証、プロビジョニング、その他のアイデンティティ・プロセスの一部として、リアルタイムで IT 制御を検証する
- ビジネス /IT レビューまたは認証テストを行って、IT 制御を定期的にテストする
- 主なテスト結果を修正または軽減し、関連する IT 制御を改善する

図 A

アイデンティティ・コンプライアンス・ライフサイクル



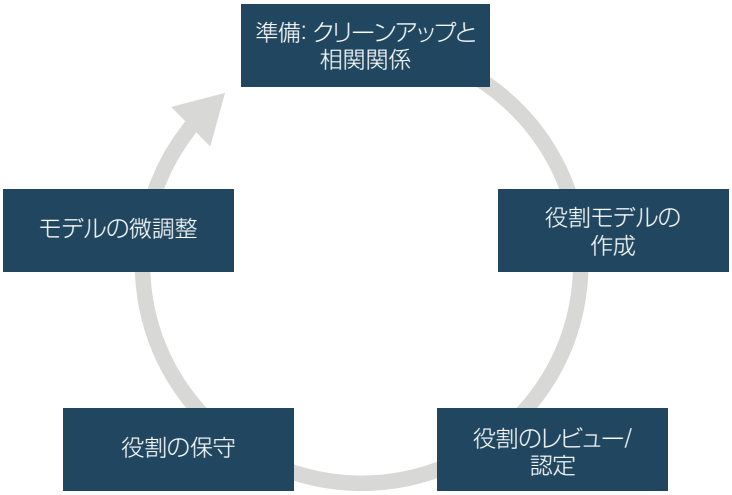
役割管理

役割管理は、役割モデルの構築、テスト、維持、最適化の全ライフサイクルのスピードと費用対効果を向上させることに重点を置きます。一般的な役割ライフサイクル・プロセスには、以下の手順が含まれます。

- データ収集、アクセス権と該当する所有者の相関付け、および不要なエンティティ（孤立アカウント、過剰なアクセスなど）の基本的なクリーンアップを行なう
- サンドボックス環境で複数の役割モデル候補をシミュレートし、技術のメリットとビジネスのメリットを比較し、初期の役割モデルを確立する
- 提案された役割モデルのレビューをビジネスと IT が行う
- 承認された役割とアクセス・モデル、および例外を特定するための実際の割り当ての継続的または定期的なレビューと比較を行う
- 不要な例外をクリーンアップし、組織の進化に合わせてモデルを改良する

図 B

役割管理のライフサイクル



アイデンティティ・コンプライアンスと役割管理は別々の処理と考えられることがよくありますが、これらの手順は相互に大きく依存し、プロセスと情報を共有しています。たとえば、両方ともデータ収集、相関付けおよび特権のクリーンアップの基本的な手順を必要とし、どちらも特定のプロセスで認定を使用できます。

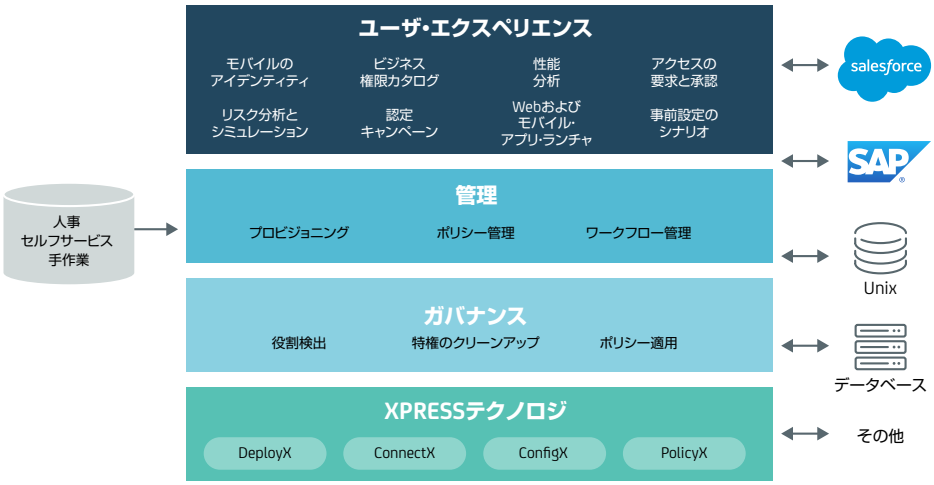
セクション 2 : ソリューション

CA Identity Suite — 主な機能

CA Identity Suiteは、堅牢な機能と直観的で便利なビジネス指向エクスペリエンスを組み合わせた、アイデンティティ管理とガバナンスの機能の統合スイートです。CA Identity Suite のユーザ・エクスペリエンスは、ビジネス・ユーザの生産性と満足度が向上することで、大企業におけるアイデンティティ / アクセスマネジメントソリューションの価値を大幅に向上させると同時に、IT 組織の管理作業を大幅に軽減します。CA Identity Suite のコンポーネントは、次の図のとおりです。

図 C

CA Identity Suite



CA Identity Suite の詳細については、http : //www.ca.com/jp/securecenter/ca-identity-suite.aspx をご覧ください。

CA Identity Governance は、一元化された権限ウェアハウス、プロセス自動化、強力な分析エンジンを基盤とした統合型ライフサイクル・アプローチにより、アイデンティティ・コンプライアンスと役割管理の課題に対応します。そのアプローチでは、たとえば、対応可能なアクセス権の範囲を拡大（通常 70 ～ 80%）し、ビジネスのニーズや優先事項との整合性を強化した役割モデルを迅速に（数か月ではなく数週間で）確立することができるなど、迅速な価値実現が可能になります。

以下では、分析と役割管理など、CA Identity Suite の主要なガバナンス機能について説明します。

分析エンジン

CA Identity Governance のユニークでパワフルな要素として、特許取得のパターン認識エンジンがあります。この堅牢な分析エンジンでは、権限や役割をすばやくテストし、異常なアクセス権が強調表示されます。また、削除またはビジネス役割への集約を検討すべき権限も表示されます。このような分析は、十分な特権範囲を持つ役割モデルをすばやく構築したり、正確な権限基盤を展開したりする場合に非常に役に立ちます。

分析によって、既存の特権セットでは見えないパターンが明らかになるだけでなく、パターンに一致しない、削除が必要な特権を検出できます。現在の組織の多くが合併、買収および組織再編を経て進化し、特権の割り当てが過剰になっていることが多いため、このプロセスは重要です。このような複雑さに加え、社員が千人単位の中規模の組織でさえも、アクセス権の割り当てが膨大な数に上ることがあるため、分析すべきデータや関係の量も拡大しています。

CA Identity Governance の堅牢な分析機能（スケーラビリティと使用するアルゴリズムの強度に基づく）は、予備の役割検出ツールとしてだけでなく、多くのアイデンティティ関連のビジネス・プロセスを合理化する戦略的意思決定サポート・エンジンとしても利用できます。分析によりメリットがあるアクティビティの例を、以下に紹介します。

- エンタープライズ・アプリケーションで所有しているアカウントとユーザのマッピング
- 過剰な誤ったアクセス権のクリーンアップ
- 既存のユーザおよびアカウント情報を使用した役割の候補の検出または役割構造の最適化
- 役割モデリングで異なる戦略を比較し、現在のアクセス割り当てに基づいたビジネスおよび IT 要件でバランスを図る最適な手法を特定
- 権限認証プロセスで疑わしい割り当てを強調表示
- プロビジョニング処理中に疑わしい特権割り当てを予防制御として強調表示

役割検出

CA Identity Governance では、ユーザ、役割および特権の関係を確認し、候補となる役割が表示されます。分析エンジンは、パターン認識と他の高度なアルゴリズムを適用して、役割を示す共通のアクセス割り当てを自動的に検出します。このような共通条件を特定するため、多数の検出方法が提供されており、役割エンジニアは、組織の特質に基づいて、1 つ、複数または全部の方法を選択できます。各検出手法には、検索適用範囲、許容範囲しきい値または属性関連パラメータなど、変更可能な入力データが含まれます。以下のような手法があります。

- **基本的な役割**では、リソースに対する共通の権限を共有しながら、既存の役割構造では未分類のユーザを特定します。検索が既存の特権の割り当てから始まるため、この手法は通常、「ボトムアップ」法と呼ばれます。
- **明白な役割**は、まったく同じリソースまたはまったく同じユーザを持つリソースの組み合わせを共有するグループのユーザです。
- **特徴的な役割**は、組織の業務単位、機能、場所およびレポーティングの構造など、論理グループに関連して存在するリソース割り当てのパターンを利用します。検索が組織構造から開始され、ユーザをビジネス機能にマップするため、この手法は「トップダウン」法と呼ばれます。
- **ルールベースの役割**は、組織および組織タイプなどのユーザ属性条件セットを満たし、共通リソースへのアクセスを共有するユーザまたはリソースを特定します。
- **階層の役割**は、親 / 子役割間の関係や、ユーザおよび / またはリソースを共有するが、親でも、サブ役割でもない関連する役割を検出します。SAP またはメインフレーム・システムを含むエンドポイントは、階層的な関連する役割を使用するため、このような関係を考慮する必要があります。
- **モデルとなる役割**は、既存のユーザ・グループまたはリソース・グループの権限に基づいて役割を構成します。CA Identity Governance では、このようなグループを他のユーザまたはリソースのモデルとして使用できます。

また、CA Identity Governance は可能性のあるそれぞれの役割モデルに対して、網羅率、役割対ユーザ比率および役割対リソース比率など、数値化が可能な主要パフォーマンス指標（KPI）を提供します。これにより、役割エンジニアは、各手法と結果として得られる役割モデルの組み合わせを一貫して評価できます。役割検出は、（初期役割モデルを示す）既存の役割がない環境、または（最適化と改善を示す）既存の役割がある環境に適用できます。

役割ライフサイクル管理

CA Identity Governance には、検出後に役割モデルを可視化および管理する堅牢な機能セットが含まれています。これには、作成、更新、削除操作、ワークフロー対応承認プロセス、シンプルで直感的なユーザ・インタフェースが含まれます。また、役割はビジネス用語、役割記述、オーナーシップ、論理グループへの集約および組織の指向などを含む、ビジネス・コンテキストにより強化できます。アイデンティティ関連プロセスで役割がビジネス・ユーザに表示されるため、この追加コンテキストは非常に需要です。

役割モデルは、ベスト・プラクティスとして、組織または他のビジネス上の変更に基づいて、更新がないかどうかを定期的に分析する必要があります。このため、CA Identity Governance では、本番環境を中断することなく、既存の役割モデルのインポートと最適化をサポートしています。この処理は、本番環境からは分離された複数のサンドボックス構成を使用して実行します。構成は、比較、結合または本番環境へ昇格することができます。複数のサンドボックス構成は、What-if シナリオをテストし、本番環境に導入できるようになるまで役割モデルを継続的に調整および改善する安全な方法となります。

特権ユーザのガバナンス

CA Identity Governance は一般ユーザと権限ユーザの両方に共通のガバナンス・メカニズムを提供するために、CA Privileged Access Manager と統合されています。これにより一貫性がサポートされ、不適切な特権アクセスを持つユーザのリスクが軽減されます。

CA Identity Suite を使用すると、特権アカウントへのアクセスのプロビジョニング、および現在の特権ユーザの識別が可能になり、権限が過剰なユーザの修正に役立ちます。特権アカウントへのアクセスは、シンプルでビジネス中心のユーザ・エクスペリエンスが提供される CA Identity Suite の標準機能を使用して要求、承認および認定できます。違反の大半が特権アカウントへの不適切なアクセスに起因していることから、この機能は全体的なリスクを低減する上で重要です。

パターンベースの監査

監査カードは、パターンベースのアルゴリズムまたはコンプライアンス・ポリシーに基づく特定の基準を満たすユーザ、役割、および特権のオンデマンドのレポートです。CA Identity Governance の既存の権限を調べて、孤立アカウントと過剰なアクセス権を特定し、特権の品質を向上させる基礎になります。たとえば、「疑わしい収集ユーザ」の基準を使用する監査カードでは、アナリストが指定した特権よりも多くの特権を持つユーザが特定されます。これらのユーザとそのアクセス権は、「疑わしい」とマークされ、過剰な権利の詳細なレビューとクリーンアップが求められます。

監査カードの結果は、直ちに使用することも、データベースに恒久的に格納しておくことも、XML（Extensible Markup Language）でファイル / システムにエクスポートすることもできます。監査人、IT 担当者、ビジネス・ユーザなど、さまざまなタイプのユーザが使用できます。たとえば以下のようになります。

- 監査担当者は、監査カードをオフライン・モードで使用して、アーカイブしたサンドボックス構成に関する証拠のアドホック・クエリに回答できます。
- 役割エンジニアは、監査カードを使用して、役割モデル変更を構成スナップショットに適用し、本番構成およびサンドボックス構成の上で監査カード・クエリを実行することで、What-if シナリオをテストし、結果を比較できます。
- 権限認定などのビジネス・プロセスにおいて、これらの結果の中で重要な結果のみを強調表示したり、ビジネス・ユーザに提示するデータ量を絞り込む場合、ビジネス・マネージャは、監査カードを間接的に使用することができます。

アイデンティティ・ポリシーの適用

CA Identity Governance では、一連のビジネス・プロセス・ルール（BPR）を作成、実施および検証し、職務の分離や、ユーザ、役割および特権間の関係に関する他の論理制約条件を実装できます。たとえば、BPR では、「X へのアクセスが許可されたユーザは、Y へのアクセスが許可されない」という制約条件や、「アクセス A を持つユーザのみが B を実行する許可権を持つ」という依存関係を適用することができます。

BPR 構文では、役割、特権またはこれら 2 つを組み合わせたレベルでの制約条件の定義がサポートされ、組織の役割モデルを利用して、必要な制約条件で対応すべき最小ポリシー数を定義できます。BPR には、ビジネス記述、リスク評点、組織分野および論理階層へのルールのグループ分けを含め、幅広いビジネス・コンテキストを含めることができます。BPR は、ビジネスと技術の知識レベルが異なるさまざまなタイプのユーザに使用されるため、これは BPR の定義では重要な部分です。

BPR エンジンは、すべてのアイデンティティ関連のコンプライアンス・ルールとすべての関連ビジネス・プロセスに対する一元化サービスとして機能し、以下のように柔軟な制御をサポートします。

- **検出コントロール：**このアドホック・クエリの手法では、BPR を監査カードの基盤として使用し、1 つの BPR または複数のコンプライアンス・ポリシー・セットに対して検出されたポリシー違反を識別します。
- **是正コントロール：**権限認定プロセスに組み込まれ、特定の権限の必要性を検証してユーザのコンテキストに基づいて BPR 違反を強調表示できます。
- **予防コントロール：**CA Identity Manager のプロビジョニングのアクションに BPR を統合し、新しいコンプライアンス・ポリシー違反の原因になるアクセス権変更を防止できます。

アクセスの認定：

規定およびコーポレート・コンプライアンス条件を満たす共通の方法は、ユーザがコーポレート・リソースへの適切なアクセス権を持っているかどうかを定期的に検証することです。権限の認定では、マネージャは直属の部下の特権リストを確認し、アクセスの必要性を認定または拒否します。CA Identity Suite ではこのプロセスが簡略化されて直観的に理解できるため、ユーザの満足度と生産性が向上します。

認定プロセスを組織固有のニーズに合わせて調整することは、アクセスを効果的に検証し、プロセスへの参加を促す上で重要です。CA Identity Suite では、ユーザ管理者、リソース所有者、役割エンジニアなど、複数の視点からレビューを依頼できます。認定プロセスは、キャンペーンと呼ばれ、異なるスケジュール、ワークフローおよび認定者により、このような観点で実行できます。また、複数のキャンペーンを同時に実行し、各キャンペーンの範囲を組織の要素に合わせたり（たとえば、特定の事業部門のユーザ）、異なるタイプのアクセスを強調表示したりできます（たとえば、疑わしい割り当てのみ、役割モデル外で取得したアクセス権）。

CA Identity Suite には、堅牢な管理制御とワークフローが含まれており、要件に基づいたキャンペーンの進行を保証できます。これには、高レベルのマネージャからの承認を要求する電子メール通知、リマインダ・アラートおよびエスカレーション・プロセスが含まれます。さらに、堅牢なリアルタイム分析が提供されるため、主要な識別プロセス（認証など）の実際の効率と有効性を容易に判断できます。ボトルネックを迅速に特定して修正できるため、SLA も確実に遵守できます。

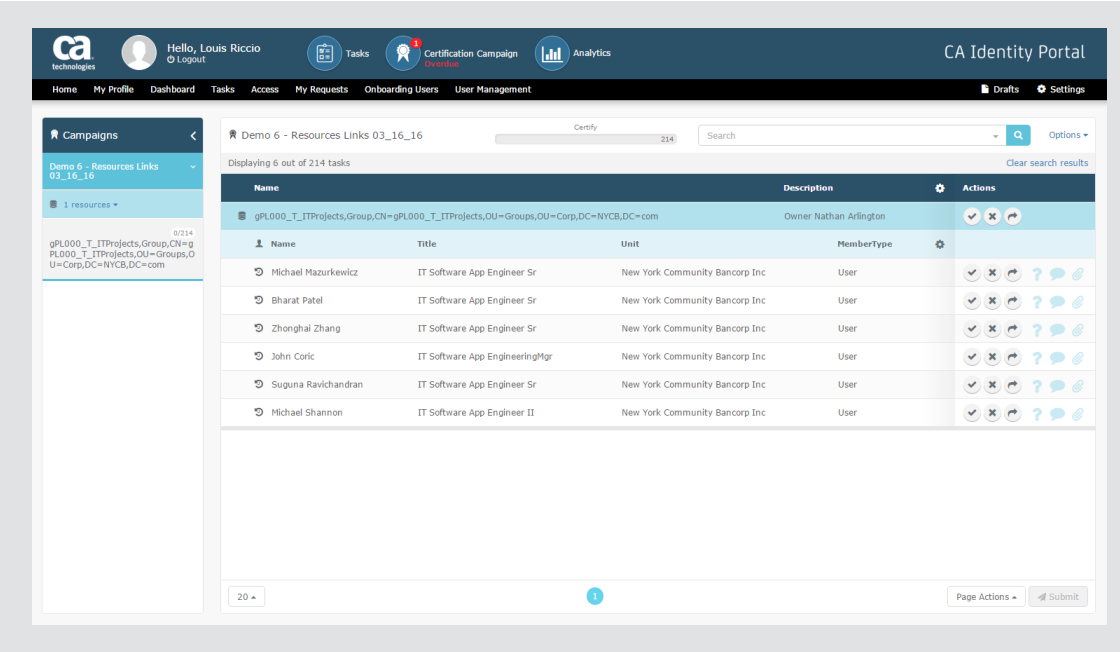
アクセス認定のユーザ・エクスペリエンスはシンプルでビジネス指向です。マネージャは、単一のユーザでも複数のユーザでもアクセスを容易に認定できます。承認は、他のマネージャに委任することもできます。ワークフローによってその認定をもう一方のマネージャに再割り当てします。また、他のマネージャに「相談」することもできます。他のマネージャに意見を求めることで、認定プロセスに正しい権限を容易に反映できるようになります。さらに、承認するマネージャは、最後の認定時に回答した内容を（ワンクリックで）簡単に確認できるため、プロセス全体が大幅に簡略化されます。

認定の操作を行うと、現在のポリシー準拠に関するコンテキスト情報と各アクセス権のリスク・レベルが表示されます。この情報は、不適切なアクセスを認定するリスクを緩和するために、マネージャにとって不可欠です。

以下のスクリーンショットは、直観的な認定のインタフェースを示しています。

図 D

アクセス認定インタフェース



ワークフロー

キャンペーンの作成時に、さまざまな事前定義済みのワークフロー・パラメータを設定できます。また、ワークフローをカスタマイズし、マルチレベル承認、電子メール通知、最小数の認定担当者の要求など、特定のビジネスニーズに対処する代替の動作を作成できます。ワークフローは、編集可能なプロセス・セットとして外部化できます。

これらのプロセスは、中核の CA Identity Governance 機能をモジュラ・パッケージに組み込んだ構成ブロックを使用して作成します。デフォルト・プロセスへの変更や、新しいプロセスの作成は、構成ブロック・モジュールのライブラリを使用して実行できます。構成ブロックの動作は、パラメータ設定によって変更できます。その後、管理者はこれらのプロセスを CA Identity Governance ワークフロー・タスクにマッピングし、カスタム動作を利用可能にします。

以下に、実行可能なワークフロー・プロセスの例を示します。

- 並行承認は、複数のレビュー担当者が許可します。
- Y 人のうち X 人の承認では、たとえば、5 人の承認者のうち 3 人がアクセス権を承認する必要があります。最小数の承認を要求するのは、ビジネス変更での投票と同じです。
- 特権リンクを承認または拒否する場合、高レベルのレビュー担当者を他の担当者より優先させることができます。
- 加重承認は、各レビュー担当者の承認に数値的加重を割り当てます。承認全体は、承認のしきい値によって決まります。承認応答の加重合計が、このしきい値を満たすか、上回ると、レビュー作業が終了します。
- 委任では、ユーザはオフィスにいない間に自分のタスクを代わりに処理してもらう別のスタッフを指定できます。タスクを別のユーザに委任した場合、委任されたユーザがそのタスクのオーナーとなります。

レポートとダッシュボード

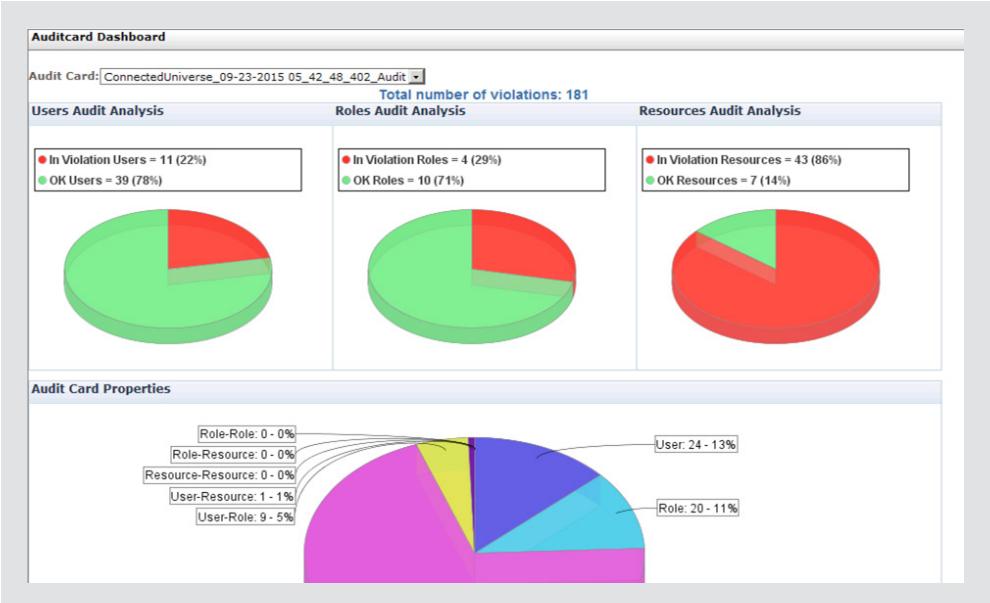
CA Identity Suite に組み込まれたアイデンティティ・プロセス分析機能では、詳細情報が表示され、処理が簡略化されるよう、主要なアイデンティティ・プロセスの操作（ユーザのオンボーディングなど）が強調表示されます。これらの分析機能は、ボトルネックを特定および修復し、サービスレベル契約を確実に遵守するのに役立ちます。

CA Identity Governance には、導入後すぐに使用できるレポートとダッシュボードの広範なセットが含まれ、証拠が必要な場合のアドホック・クエリもサポートされます。異なるタイプのユーザのニーズに対応するために、レポートはビジネス・レベルによって異なり、提供される技術情報も異なります。これには、たとえば、ビジネス・マネージャ、役割エンジニア、コンプライアンス担当者、監査担当者および IT スタッフなど向けの個別のレポートが含まれます。レポートは、以下のグループにカテゴリ化されます。

- **特権の品質**では、既存および提案のアクセス品質に関する主要な測定データやサポート詳細が提供されます。これには、ユーザ、役割、リソース、重複する役割リスト、および不適切と疑われるアクセス権についての統計データが含まれます。これらのレポートは通常、現状と希望の状態の間のギャップを把握したり、特権クリーンアップの必要な分野を特定したりするために使用します。
- **エンティティ中心**では、特定のユーザ、ポリシー、役割、リソースまたはその他のタイプのエンティティに完璧なビューを表示します。また、これらのレポートでは、BPR ポリシーに違反するエンティティや、パターン外れが疑われるエンティティなどの重要な検出結果も強調表示されます。
- **役割分析**では各種の役割モデリング方法の結果を比較し、現在の役割構造に詳細な分析を行ないます（たとえば、同様の特権を持つが、現在同じ役割のメンバーではないユーザなど）。役割エンジニアは、これらのレポートを使用して、疑わしい役割を評価したり、役割がビジネスのベスト・プラクティスに適合している証拠を提示したりできます。
- **コンプライアンス**では、ビジネス・マネージャ、コンプライアンス担当者および監査担当者は、ポリシー制御、キャンペーンの進捗状況および関連するリスクの堅牢なビューを表示できます。これには、明確なポリシー違反や疑わしい割り当てなどの重要な検出結果を評価する、監査カード・レポートが含まれます。権限認証レポートには、プロセスの進捗状況とプロセスの詳細が表示されます。

図 E

監査カードダッシュボードでは、複数のポリシー違反の概要が 1 ページに表示されます。



セクション 3 : メリット

アイデンティティ・ガバナンスのためのビジネス・ユーザ中心のアプローチの利点

CA Identity Suite のアイデンティティ・ガバナンス機能では、アクセスの要求と承認の簡略化、認定の合理化、役割管理の複雑さの軽減、不適切なアクセス権の修復が行えます。このソリューションでは、他のソリューションよりもはるかに優れた以下のような機能と利点が提供されます。

直観的なビジネス指向のユーザ・エクスペリエンス

CA Identity Suite は優れたユーザ・エクスペリエンスを提供します。アクセス要求、認定、役割管理などの主要なアイデンティティ管理機能は、直観的なビジネス指向エクスペリエンスで利用できます。また、アクセスの要求と承認はそれぞれのユーザの言語にローカライズできるため、特に多国籍企業にとっては使用性が向上します。その結果、ユーザ満足度も生産性も向上します。

このビジネス指向のユーザ・エクスペリエンスは、重要なガバナンス・プログラムの成功要因の 1 つです。ビジネス・マネージャはユーザの役割と権限を理解しているため、これらのプロセスに直接関わる必要があると当社は考えています。アイデンティティ・サービスはより幅広いユーザ、特に非技術系ユーザが直接使用するため、ユーザ・エクスペリエンスはプログラムの成功にとって非常に重要になります。採用率の増加は、プログラム全体が幅広い支持を得ていることを意味します。

リスクの低減

より正確な権限、役割およびポリシーの基盤に基づいてプロセスと制御を自動化することで、各ユーザの固有の役割に対して適切なアクセス権を維持できます。また、特権クリーンナップ機能によって過度の特権が強調表示されるため、大量のユーザの特権の潜在的なセキュリティ・ポリシー違反を特定できます。リスクベースのアクセス承認では、承認者に各アクセス要求のリスク・レベルに関する重要なコンテキスト情報も提供されます。これにより、企業のセキュリティ・リスクを低減し、内外の監査人に対するコンプライアンスの証明を簡略化することができます。また、特権ユーザのガバナンスによって、すべての特権アカウントへのアクセスが適切に許可されたユーザのみに制限されます。

役割管理の簡略化 :

特許出願中の高度な特権分析エンジンは、大量のユーザおよび特権のデータを効率的に並び替えて、事実上の役割を識別し、基礎となる役割モデルを単純化するのに役立ちます。この機能により、正確な権限と役割を迅速に評価、構築、および維持することができます。一元化されたエンジンによって、一貫したビジネスと規制遵守のポリシーの確立と適用が簡略化されます。

ca.com/jp/でCA Technologiesにアクセスしてください。

CA Technologies（NASDAQ : CA）は、企業の変革を推進するソフトウェアを作成し、アプリケーション・エコノミーにおいて企業がビジネス・チャンスを獲得できるよう支援します。ソフトウェアはあらゆる業界であらゆるビジネスの中核を担っています。プランニングから開発、管理、セキュリティまで、CA は世界中の企業と協力し、モバイル、プライベート・クラウドやパブリック・クラウド、分散環境、メインフレーム環境にわたって、人々の生活やビジネス、コミュニケーションの方法に変化をもたらしています。詳細については **ca.com/jp** をご覧ください。

CS200-230092_1116