opentext™ | Cybersecurity

データシート

NetIQ Identity Governance

NetIQ Identity Governance は、アクセス認証の迅速化、不適切なアクセスのリスクの軽減、技術上および業務上の役割に関してのユーザー分析、監査担当者の満足度の向上を実現します。

何に対して誰をアクセス可能にするか、効果的に管理していますか？

アイデンティティガバナンスに関する規制に対応し、リスクを管理するためには、組織はユーザーのアクセス権のインベントリを作成して、分析し、管理する必要があります。機密リソースへのユーザーのアクセス管理ができていないと、企業のリスクが増え、ネガティブな監査結果につながるか、詐欺やデータ侵害の被害を受ける可能性が高まります。

アクセスレビューと再認証のプロセスは、総合的なアイデンティティガバナンスプログラムに欠かせません。しかし、「何に対して誰をアクセス可能にするか」という重要な問いに答えることは簡単ではありません。一般的な従業員の業務と個人が持つ役割との間にある境界線は、モバイルデバイス、クラウドコンピューティング、ソーシャルメディアが使用されるようになったこともあり、労働におけるトレンドを変えつつあります。これに加えて、請負業者、パートナー、サービスプロバイダーの数が増加していることからも、組織は、基幹業務 (LOB) 管理者の参加を促すアクセス認証プロセスを実施するための、より効率的な方法を模索しています。

製品の概要

NetIQ Identity Governance by OpenText™ は、アクセス認証プロセスを効果的に実施するとともに、アイデンティティガバナンスコントロールを導入することで、コンプライアンス要件に対応すると同時にリスクを事前に軽減できるようにサポートするソリューションです。組織内でこのような体制を稼働させるのに、従来のレガシーベンダーが数週間から数か月かかっていたのに対し、NetIQ Identity Governance なら数時間で済むように構築されています。時間がかかるうえにミスが発生しやすく、コンプライアンス違反や過度にアクセス権を提供するリスクを企業にもたらす可能性のある手動のプロセスに代わるソリューションです。

NetIQ Identity Governance では、社内でのユーザーの職位変更に伴い過度の権限が意図せずに付与されている状態になった場合など、対象ユーザーにとって必要のないリソースへのアクセス権を迅速に特定して取り消すことができます。また、複数のシステム、アプリケーション、データからユーザーのエンタイトルメント情報が収集され、一括表示されます。その結果、LOB マネージャーにとってわかりやすいレポートが提供され、マネージャーはそのレポートに基づいて既存従業員のアクセス権が適切かどうかを確認し、必要に応じてアクセス権を取り消すアクションを即座に開始できます。

主な機能

- **エンタイトルメントデータを収集してレビュー**：オンプレミス、ハイブリッド、クラウドのアプリケーションを含むインフラストラクチャ全体からエンタイトルメントデータを収集してレビューし、誰がどのリソースにアクセス可能かを正確に把握できます。
- **分析と役割マイニングを活用**：エンタイトルメントの共通点を特定し、「what if」分析を実行して、コンプライアンスの測定基準とレポートを作成します。
- **アクセス認証を実施**：承認者の意思決定のサポートや管理者への問題のエスカレーションなど、自動通知や進捗報告によってアクセス認証プロセスがスケジュール通りに進むようにします。
- **違反や例外を検出し、それに対処する操作を定義**：職務分掌 (SoD) 違反や放置されたアカウントなどを検出し、それに対処する操作を定義することで、リスクを低減できます。
- **業務に基づく役割と属性権限付与モデルを作成**：これによってアクセス認証やアクセス要求の範囲と期間を縮小し、承認プロセスを短縮できます。すべてのエンタイトルメントではなく、例外に注目できるようになります。
- **繰り返し発生する修正作業を排除**：ServiceNow や Remedy などのサービスデスクソリューションと統合することでチケット発行を自動化したり、NetIQ Identity Manager by OpenText™ と統合することでアクセス権の付与と取り消しを自動化できます。
- **リスク測定によりレビューを優先順位に基づいて実施**：属性値、所属グループ、管理関係、アプリケーション、権限、コスト、リスクなどの基準に基づいたリスク測定により、最も必要性が高いものに注目を促すことで、レビューを優先順位に基づいて実施できます。
- **アイデンティティガバナンスに関するレポートを作成**：エンタイトルメント、認証状況、要求と承認、ポリシー違反が盛り込まれたアイデンティティガバナンスに関するレポートを作成できるため、監査報告が容易になります。スケジューリング機能や配布機能も標準でサポートされています。

主な差別化要因

- **リアルタイムの適応型ガバナンスにより、継続的なリスクの低減が可能です。**競合他社のソリューションでは、特定の時点でのエンタイトルメントは収集されますが、次の収集が行われるまでの間、組織はリスクにさらされたままになります。NetIQ Identity Governance は、変更やイベントが発生したときにそれらに適応し、レビューをトリガーしてコンプライアンスを確保できます。
- **ビジネスインサイトを通じて、アクセスに関する意思決定を向上させます。**リスクやアクセスコストなどのビジネスコンテキスト情報、似たような責任を負う複数のユーザーの比較、およびその他の関連情報が、レビューおよび承認インターフェイスに直接表示されます。そのため、ビジネスユーザーは、ユーザーのアクセスに関してより適切な意思決定を行ううえで必要な知識を得ることができます。

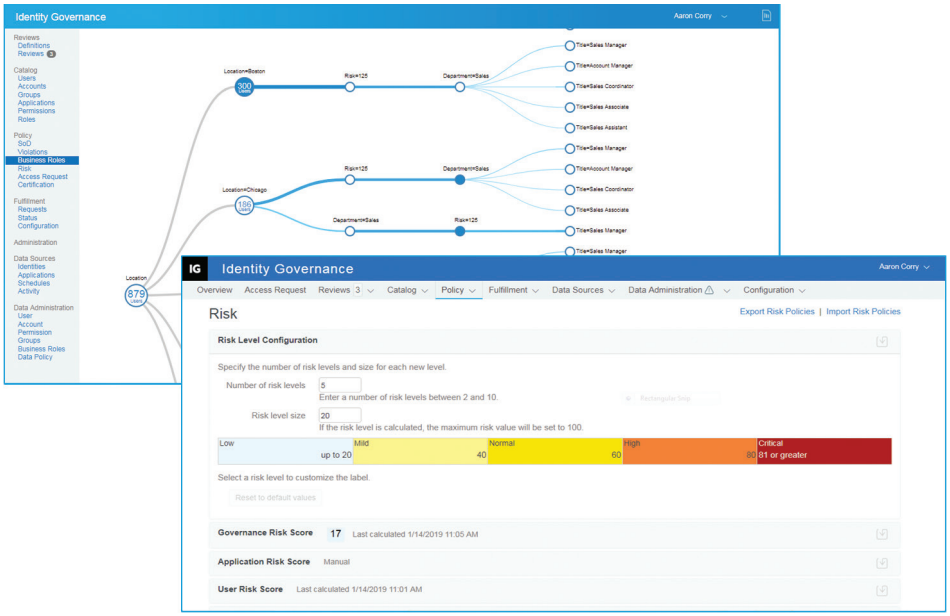

図 1. NetIQ Identity Governance では、役割マイニングを実行してエンタイトルメントの共通点を特定し、分析を表示して役割の活用状況のレポートを提示できます。

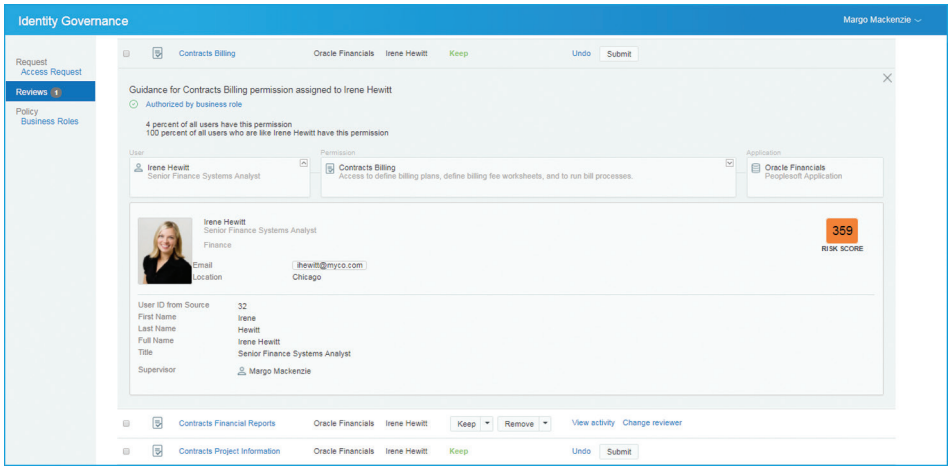

図 2. NetIQ Identity Governance は、アクセス認証時に基幹業務マネージャーの意思決定をサポートし、アクセスが標準から外れているかどうか、リスクが高いかどうかなどを把握できるようにします。

NetIQ Identity Governance では柔軟な配信オプションが用意されており、オンプレミスでの導入も、パブリック / プライベートクラウド、マネージドサービスプロバイダー、または Software as a Service (SaaS) 経由での導入も可能です。

NetIQ Identity Governance の詳細については、**www.microfocus.com/ja-jp/cyberres/identity-access-management/identity-governance** を参照してください。

お問い合わせ
www.opentext.com

opentext™ | Cybersecurity

OpenText Cybersecurity は、あらゆる規模の企業とパートナー様を対象に、包括的なセキュリティソリューションを提供しています。予防から検出、復旧対応、調査、コンプライアンスに至るエンドツーエンドの統合プラットフォームにより、包括的なセキュリティポートフォリオを通じてサイバーレジリエンスの構築をサポートします。コンテキストに基づくリアルタイムの脅威インテリジェンスから得られた実用的なインサイトを活用できるため、OpenText Cybersecurity のお客様は、優れた製品、コンプライアンスが確保されたエクスペリエンス、簡素化されたセキュリティというメリットによって、ビジネスリスクを管理できます。

760-JA0004-005 | O | 05/24 |