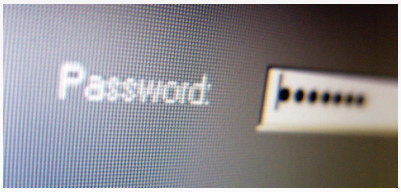
opentext™ | Cybersecurity

製品ハンドアウト

NetIQ Identity Manager

ファイアウォール内外の企業資産への効率的で一貫したセキュアなアクセスを企業が確保するためには、どうすればよいのでしょうか。リソース、モビリティと BYOD がもたらす職場環境の多様化、内部および外部監査の管理、クラウドコンピューティングなどへのニーズが増大する中、企業に必要なのは NetIQ Identity Manager です。



NetIQ Identity Manager の概要
ID を活用したソリューションの基盤となる NetIQ Identity Manager は、モジュール型でありつつも統合された方法で ID ライフサイクル全体を管理できるように設計されているため、現在のニーズだけでなく将来のニーズにも対応できます。

成長に伴う複雑化とセキュリティ上の課題

企業が成長するにつれ、新しいアプリケーションやサービスへのタイムリーなアクセスの提供を絶えず求められることになります。デバイスは爆発的に増加し、IT のコンシューマライゼーションによってアクセスが容易になり、あらゆる場所でインターネットに接続できるようになっています。そのような状況において、企業はアプリケーションやデータへのアクセスを適切に管理しながら、職場でコンシューマーエクスペリエンスを提供するというニーズにも対応することを求められています。企業はこの課題に対処するためにさまざまなプロセスを実装していますが、それらを成功に導くための基盤となるのは、変化するビジネスニーズに対応するうえで必要となる柔軟性を提供できる、堅牢で効果的な ID 管理です。

常時接続がもはや新たな常識となった今、あらゆる場所が仕事場となり、ビジネスユーザーの好みはモバイルデバイスインターフェイスへと移行しています。ユーザーはこう考えています。「なぜ今すぐ必要なものにアクセスできないのか」、「なぜアプリをダウンロードできないのか」、「なぜまたパスワードを要求されるのか」。利便性に対するこうしたコンシューマライゼーションの傾向は、どのテクノロジーを選択するかという点に影響を及ぼします。

これを上回るとはいかないまでも、同程度に重要な課題が、企業の資産およびデータの保護と、社内外の規制への確実な遵守です。しかし、クラウドアプリケーションやモバイルデバイスが IT 部門の管理範囲外にある場合、機密情報への不正アクセスを防ぐのは非常に困難です。

使いやすさと適切な制御のバランスを取ることは、かなり大変な作業になる可能性があります。これらの課題に対応するために組織に必要なのは、さまざまなアプリケーションのユーザー ID とその関連属性を管理できる包括的なソリューションです。ここで言うアプリケーションとは、オンプレミスのアプリケーションである場合もあれば、パートナー企業が提供するアプリケーションの場合もあり、サービスとしてのソフトウェアである場合もあります。特定の ID 基盤があれば適切なアクセスをサポートし、セキュリティデータを強化してユーザーがいつどのように企業資産を利用しているかを把握できるようになります。ID、アクセス、セキュリティに対して統合されたアプローチを採用すれば、コンシューマーと同様のエクスペリエンスをユーザーに提供できると同時に、脅威に対して効率的かつ効果的に対処し、さらには監査にも対応できるようになります。

NetIQ Identity Manager が可能にする、複雑な要件への包括的なアプローチ

NetIQ Identity Manager by OpenText は、ID 管理のライフサイクル全体を強化し、ID とそれに関連する属性を管理して権限の付与を最小限に抑えます。これにより、組織は手作業でのアカウント管理に要したコストを削減し、コンプライアンスを実証できると同時に、不正アクセスのリスクを低減できるようになります。このソリューションを導入すると、組織の重要なステークホルダー全員にメリットがもたらされます。たとえば、次のことが可能になります。

- CIO は、コンプライアンスのコストを削減し、利便性の高いアクセスを提供できるようになるため、ビジネス機会を拡大できます。

図 1. NetIQ Identity Manager を活用した ID 管理のライフサイクル

- CISO は、全社的なアクセスコンプライアンスとセキュリティを強化することができます。
- 事業部門のマネージャーは、役割に応じたリソースへの即時アクセスを提供することで、チームの生産性を維持できます。
- IT マネージャーは、リソースをより適切に管理し、ID の豊富な使用状況データを主要なステークホルダーに提供できます。

NetIQ Identity Manager は、モジュール型でありつつも統合された方法で ID ライフサイクル全体を管理するため、現在のニーズだけでなく将来のニーズにも対応できます。その機能には次のようなものがあります。

アカウントの作成、失効、およびジョブの変更の管理：NetIQ Identity Manager は、統合されたロールベースのワークフローエンジンを備えており、これは現在の市場で最も効率的なソリューションです。また、組織にとって理にかなったものであれば、どのようなプロビジョニングも自動化します。このエンジンは、ビジネスルールとロールベースのプロビジョニングの効率性を組み合わせることで、組織のビジネス手法に適合し、ワークフローエンジンが標準的な承認や職務分掌の競合などの例外を処理できるようにします。

企業全体での ID およびアクセス変更の管理：NetIQ Identity Manager はイベントベースのアーキテクチャを活用しており、接続されたすべてのシステムに ID 権限を適用します。これにより、ID は適切なソースからのみ作成されるようになります。さらに、NetIQ Identity Manager によって属性権限が適用されます。つまり、ID のコンポーネントを「所有」しているシステムのみがその属性を変更でき、権限のないソースで変更された場合は、権限のあるソース内の値に自動的に再設定されます。これはどちらも、プロビジョニングポリシーとアクセスポリシーを属性に基づいて設定する場合、重要な機能です。NetIQ Identity Manager はイベントベースのアーキテクチャを使用してリアルタイムで処理します。入社、退職、昇進、職務変更などのユーザーライフサイクルイベントが発生した場合に、人の手をほとんど、あるいはまったく介すことなく、データ管理エンジンがポリシーベースのプロセスを実行します。

さらに、Microsoft SharePoint や SAP システムなどの各種アプリケーションには、独自のポリシー制御機能が備わっています。Identity Manager では、そのリソースリコンシリエーションサービスを利用して、さまざまなエンタイトルメントを集約されたカタログに簡単に統合できます。この機能を使用すると、パーミッションが自動的に検出され、視覚的な操作でリソースを適切な役割またはリソースにマッピングできます。

さまざまなポリシー制御が 1 つのシステムにシームレスに統合されるため、統一されたガバナンスメカニズムが迅速に構築されます。このメカニズムにより、適切な担当者がユーザーの権限を完全に把握でき、適切なユーザーに適切なリソースへのアクセス権が付与されているかどうかを、十分な情報に基づいて評価および確認できます。初期セットアップの操作がしやすいだけでなく、エンタイトルメントが継続的にメンテナンスされるため、接続されたすべてのシステムにわたって (オンプレミスのシステムかクラウドのシステムかを問わず) リソースとエンタイトルメントを管理するアジャイルなシステムを組織は利用できるようになります。

常時接続がもはや新たな常識となった今、あらゆる場所が仕事場となり、ビジネスユーザーの好みはモバイルデバイスインターフェイスへと移行しています。ユーザーはこう考えています。「なぜ今すぐ必要なものにアクセスできないのか」、「なぜアプリをダウンロードできないのか」、「なぜまたパスワードを要求されるのか」

Designer for NetIQ Identity Manager では、人為的ミスを大幅に削減できるアクセス要求ワークフローを作成できます。作成にあたってプログラミングもカスタマイズも一切必要ありません。管理者はグラフィカルなインターフェイスで、スクリプトを記述することなく、さまざまなアカウント管理設定の設計やシミュレーションなどプロジェクトライフサイクル全体を管理できます。NetIQ Identity Manager を環境全体のアプリケーションに拡張すると、「データのクリーンアップ」という課題に時間を取られる場合があります。Designer の機能の 1 つである Analyzer for NetIQ Identity Manager では、ID ボールトのデータと接続システムのデータを効率的に表示して比較できます。これにより、アプリケーションを ID インフラストラクチャに統合する準備に要する時間と、さらには新しいシステムとの接続に要する時間とコストも、最小限に抑えることができます。

ユーザーセルフサービスのアクセス要求と承認のプロセス：ビジネスユーザーが使いやすい直感的なダッシュボードを使用して、ビジネスユーザーはアクセス要求の作成とトラッキング、ならびに承認タスクを一元管理できます。このセルフサービス機能により、ユーザーは自身の ID 情報を管理できるようになるため、ユーザーの生産性が確保されると同時に、要求の処理にかかる IT 部門の作業負荷が軽減されます。また、プロビジョニングシステムと完全に統合されているため、ユーザーは手動での対応を待つことなく、必要なアクセス権をほぼ即座に取得できます。

承認者が出張中か移動中のビジネスマネージャーであることはよくあることです。承認者がオフィスに戻るまでユーザーからの要求が待機状態になるようでは、生産性が低下します。今日の世界では、仕事とは活動そのものであり、場所は関係ありません。Mobile Approval Application for NetIQ Identity Manager は、ネイティブのセキュアなモバイルアプリケーションです。あらゆるモバイルデバイスに簡単にインストールできるため、承認者はどこにいても即座にアラートを受け取り、承認依頼に対応することができます。

パスワードセルフサービス：ヘルプデスクの最大のコストの 1 つが、ユーザーのパスワードリセットのサポートにかかるコストです。NetIQ Self Service Password Reset (SSPR) by OpenText を利用すると、企業が必要とするセキュリティを維持しながら、ユーザーが自身のパスワードを管理およびリセットしたり、さらにはロックされたアカウントを再度有効にしたりできるようになるため、ヘルプデスクの関与を実質的にゼロにできます。

セルフサービスのパスワードリセットでは、ユーザーがいくつかの方法で本人確認を行った後に、パスワードを安全な方法でリセットすることが可能になります。どの方法を選択しても、組織が必要とする適切なセキュリティレベルが反映され、新しいパスワードは、入力時にパスワードルールが適用されることで常に要件に準拠します。これにより、強力なパスワードが、指定された要件を満たしていない弱いパスワードで置き換えられる心配がなくなります。新しいパスワードとロック解除されたアカウントは即座に有効になり、ユーザーはシステムやアプリケーションにすぐにアクセスできるようになります。

ユーザーアクティビティの監視：誰が何に対してアクセス権を持っているかを把握し管理することが、監視のすべてではありません。そのアクセス権を使用して何を行っているのかを、履歴とリアルタイム表示の両方から把握することも、同様に重要となります。コンプライアンス違反に当たる行為、悪意のある行為、または不適切な行為を不用意に許可してしまうと、多額の罰金、監査の不合格、企業のデータストアやビジネスの評判への深刻な被害につながる可能性があります。Identity Tracking for NetIQ Identity Manager は、NetIQ Identity Manager の強力な情報およびプロビジョニング機能にリアルタイム相関エンジンを組み合わせることで、誰が何にアクセスでき、そのアクセスによって何を行っているかを完全に把握できるようにします。このユーザーアクティビティ監視 / 修正ソリューションは、NetIQ Identity Manager がプロビジョニングするすべてのシステムで機能し、コンプライアンス違反に当たる行為、悪意のある行為、不適切な行為によって企業が損害を被るリスクを大幅に軽減します。

アクセス認証：定期的なアクセスレビューはコンプライアンス要件の 1 つですが、この作業には膨大な時間を要する場合があります。IT 部門はアクセス権付与に時間を消耗し、事業部門はその権限付与の認証を行うために多大な労力を強いられます。NetIQ Identity Manager を補完する NetIQ Identity Governance by OpenText により、組織は企業全体でアプリケーションやシステムへのユーザーアクセスをレビューして認証できるようになるため、この認証プロセスの大部分を自動化できます。NetIQ Identity Governance を使用すると、管理対象および管理対象外アプリケーションのレビュー、イベント駆動型の定期的なレビュー、スーパーバイザーのレビュー、アプリケーションレビューとパーミッションオーナーレビューの両方のサポート、リスクに基づいたレビューの効率化、レビュー決定の自動または手動での実行が可能になります。

コンプライアンスレポート：NetIQ Identity Manager には、アクセスにおけるコンプライアンスの証明に必要な包括的なレポート機能が備わっています。このレポートには、ユーザーが現在どのシステムにアクセス可能であるかに加えて、特定の日付や 2 つの時点の間にアクセス可能であったシステムが表示されます。また、レポーティングフレームワークにより、特定の要件に合ったカスタムレポートを作成して、後で使用できるようにそのレポートを保存することもできます。ポリシーベースのデータ収集およびストレージ機能がコンプライアンスを強力にサポートするため、次の監査に備えて常に準備を整えておくことができます。

まとめ

実績があり、かつ受賞歴のある Identity Manager は、ファイアウォール内とクラウド内の両方において、企業全体で誰が何にアクセスできるかを制御する包括的なソリューションです。コンプライアンス要件を満たしながら、重要な情報へのセキュアで便利なアクセスをビジネスユーザーに提供できるようになります。コモンクライテリア (CC) 認定で拡張保証付きの評価保証レベル 3 (EAL3+) を取得しており、信頼性も抜群です。

「一元的なユーザー ID 管理により、シームレスな方法で当社のサービスを提供できるようになりました。お客様はもう、さまざまなサービスにアクセスするために、いくつものIDとパスワードを覚えておく必要はありません」

Kanon Cozad 氏
上席副社長兼アプリケーション開発部門ディレクター
UMB Financial Corporation

お問い合わせ
www.opentext.com

NetIQ は世界中の何千社ものお客様が導入しており、拡張性が極めて高く、差別化された ID 管理基盤によって、競争力、俊敏性、安全性を低コストで維持することが可能です。統合されたアプローチにより、全社規模のソリューション、あるいは個別の ID およびアクセス管理製品を導入することができ、最も差し迫ったニーズに最初に対応できます。当社の製品とソリューションを使用することで、お客様は過去、現在、将来の IT 投資から最大限の価値を得ることができます。

NetIQ by OpenText について

このたび、OpenText による、CyberRes を含む Micro Focus の買収が完了しました。両社の専門知識の融合によって、セキュリティ製品 / サービスの提供が拡張され、権限とアクセスの制御の自動化を通じて、アプリケーション、データ、リソースへの適切なアクセスを確保することにより、お客様の機密情報の保護を支援しま す。NetIQ Identity and Access Management は OpenText Cybersecurity の一部であり、あらゆる規模の企業やパートナーに包括的なセキュリティソリューションを提供します。

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。