多様な働き方で、増える情報漏えいリスク

――セキュリティの“新常態”に必要なもの

働き方にテレワークが浸透し、組織を支えるITに「いつでも、どこからでも必要なリソースにアクセスできる」機能が求められる一方で、情報漏えいのリスクが増している。業務を進めやすい環境を維持しつつ、リスクを低減し、かつ情報システム部門の負担を増やさないようなセキュリティの“新常態”に必要な要素とは何か。

ビジネス環境が大きく変わり、デジタルトランスフォーメーション（DX）に向けた取り組みが進む中、セキュリティやガバナンスの在り方も大きな変化を迫られている。SaaS（Software as a Service）を中心としたクラウドの利用が広がり、オンプレミスを想定していた時代のセキュリティは通用しにくくなってきた。テレワークを中心とした新しい働き方に対応するため、社員のアカウントやデバイス、アプリケーション、データをリモートで適切に管理する必要もある。

今注目されるセキュリティとガバナンスのアプローチが「ゼロトラスト」だ。NTTコムウェアの野呂昌哉氏（ネットワーククラウド事業本部 セキュリティオペレーションセンタ長）は、NTTグループをはじめ多様な組織のセキュリティに取り組んだ経験から、ゼロトラストが注目を集める背景について語った。

NTTコムウェアの野呂昌哉氏
（ネットワーククラウド事業本部
セキュリティオペレーションセンタ長）

「従来一般的だった境界防御のアプローチは、ファイアウォールで境界を作り、境界の内側のネットワークを信頼できる（Trusted）、外側を信頼できない（Untrusted）ものとして対策を講じてきました。しかし、DXや働き方改革が進み、境界線の設定自体が難しくなっています。そこで、ITシステムへの接続元を全てUntrustedと見なし、必ず接続リクエストを検証することでセキュリティとガバナンスを確保する考え方が重視されるようになりました」（野呂氏）

ゼロトラストについては、米国立標準技術研究所（NIST）の定義や日本政府によるガイドラインが知られ、実装に当たっての要件も整理されつつある。野呂氏は「ゼロトラストにおける検証作業（接続都度の認証）は、アクセス元となるユーザーIDやデバイスなどの情報とアクセス先となる各種リソースの情報を基に、アクセスの可否を決定します。そのため、ID管理システム、アクセスポリシー、ユーザーアクセス状況の管理は必須です」と説明する。

言い換えれば、アイデンティティー&アクセス管理（IAM）が以前にも増して重要になっているのだ。

従来のID管理システムでは限界、新たに求められる機能とは

IAMの仕組みは従来、オンプレミスシステム向けに構築することが一般的だった。ある程度以上の規模を持ったシステムにおいてはWindowsとの相性の良さからActive Directoryが利用され、メインフレームやホスト、SaaSなどはそれぞれ別のIDとアクセス権で管理する複合的なシステムを構成することが多かった。しかし、クラウドやテレワークが普及するとこうした構成では管理が難しい場面が増えてきた。野呂氏は、IAMに取り組む組織がぶつかりがちな課題を3つ挙げる。

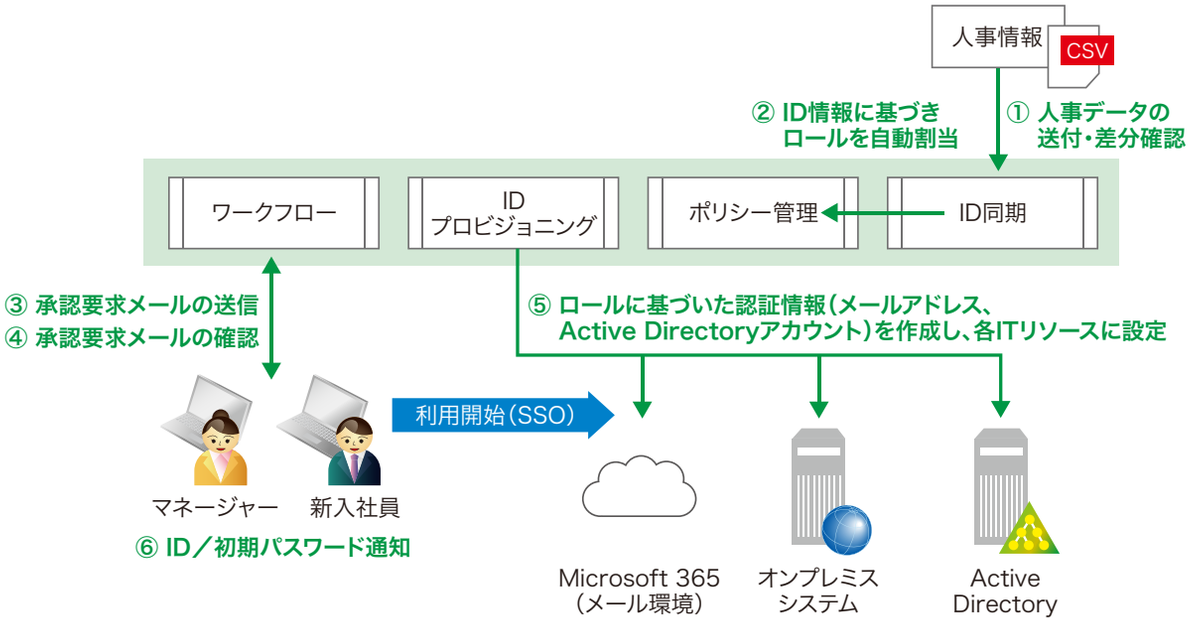
多様な働き方で、増える情報漏えいリスク

「1つ目の課題は、管理すべきIDの増加です。システムやサービスにログインする際に個別のIDとパスワードを入力する場面が増え、情報漏えいのリスクが高まっています。IDの棚卸しも大きな課題です。誰がどのIDを利用しているかを把握しにくくなり、IT監査で指摘を受けるケースが増えています。退職した社員のIDが適切に削除されず、不正アクセスの原因になった事例もあります。複数のIDや権限をどのように管理するかという課題もあります。オンプレミスシステムだけでなく、SaaSも含めたさまざまなIDを一元管理することが求められます」(野呂氏)

1つ目のID数の増加については、シングルサインオン(SSO)が一つの解決策になる。その際には、オンプレミスだけでなくSaaSとの連携(フェデレーション認証)が必要になる。

2つ目の棚卸しについては、IT監査に耐えられるガバナンス機能を実装する必要がある。不要なIDが発生した際は自動的に権限を剥奪できるようにし、誰がどのアプリケーションにアクセスできる権限をいつから割り当てられているのかを棚卸しすることができる仕組みだ。

3つ目の統合管理については、ID管理基盤と統合認証基盤を同時に実装することが重要だ。



入社時のID登録の流れ。
IAMの自動化は、変化を続ける組織のセキュリティにおいて急務となりつつある(出典:NTTコムウェア)

IAMに取り組む上で重要なポイントについて、野呂氏は「マニュアル作業を減らし、ポリシーによる自動化を推進することです」と話す。

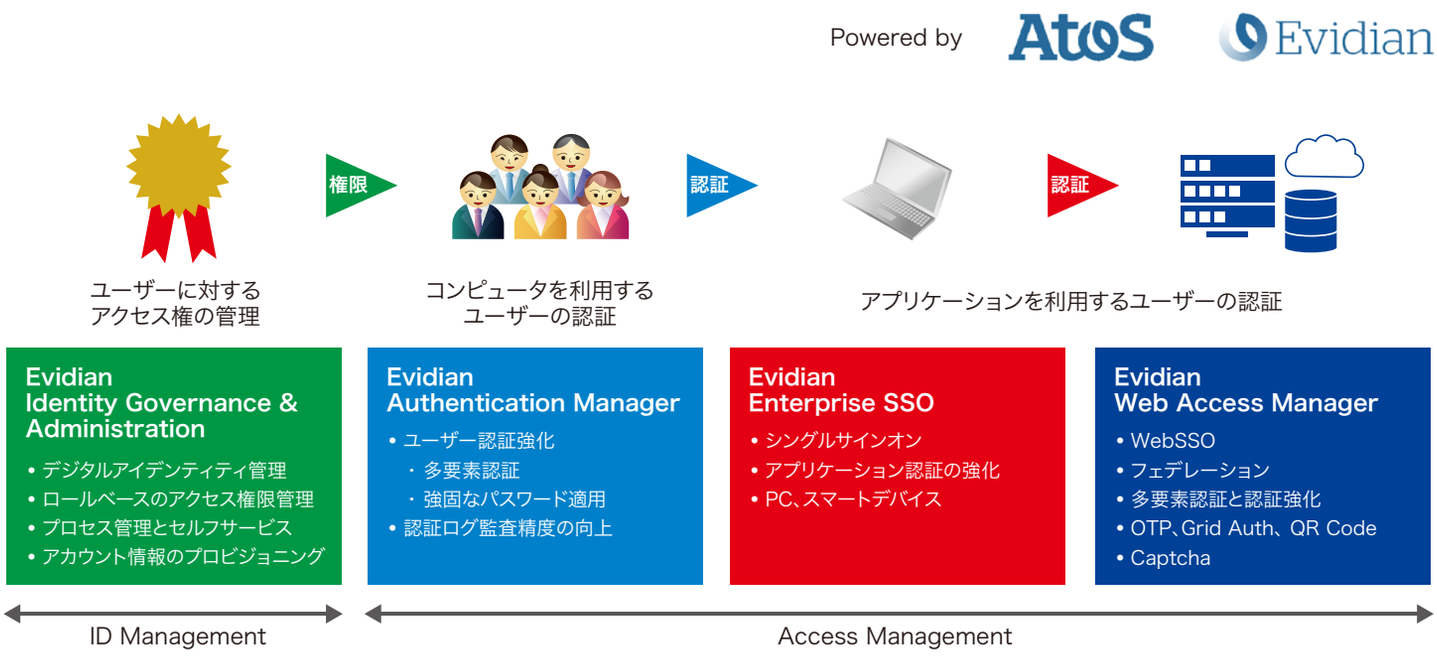
IAMを自動化する「SmartCloud IAMソリューション」

IAMの課題を解消し、自動化を実現するためにNTTコムウェアが提供しているのが「SmartCloud IAMソリューション」だ。最大の特長は、ID管理と統合認証の両方を同時に実現できる点にある。

ID管理においては、共通基盤を使ったID権限情報の一元管理を実現する。IDの申請や承認などのワークフローを一元的に制御することでIDライフサイクルを適切に管理し、監査対応を含めたガバナンスを確保する。その上で、複数のアプリケーションの認証機能を統合した基盤を構築し、オンプレミスとパブリッククラウドにまたがるハイブリッドSSOを実現する。

多様な働き方で、増える情報漏えいリスク

「ID管理からアクセス制御までを一貫して管理、制御可能です。ID管理と認証基盤を同時に導入することで、プロビジョニング設定の容易さ、保守サポートのしやすさといったメリットを提供します。また、ID管理と統合認証のどちらか一方だけを導入することもでき、段階導入も可能です」と野呂氏は話す。



SmartCloud IAMソリューションの概要（出典：NTTコムウェア）

もともとSmartCloud IAMソリューションは、NTTコムウェアのDXと働き方改革を推進するための統合認証基盤として構築されたものだ。SaaSを中心としたクラウドサービスとの連携に必要なSAML認証だけでなく、オンプレミスのレガシーな認証方式にも対応することで自社内に存在していた多様なシステムへのSSOを可能にした。現在は70を超える業務システムのSSOを実現した。

「IAMを自動化することで、ユーザーはSSOによって利便性が向上したサービスを利用できるようになり、管理者はアカウント管理の負担を大幅に軽減できます。業務の標準化と省力化によって設定不備をなくし、セキュリティリスクを縮小できます」（野呂氏）

NTTグループでの運用実績と、多様なニーズに応えるSI力が強み

SmartCloud IAMソリューションは、フランスを拠点とするグローバルIT企業Atosとの提携の下、同社が手掛けるIAM製品「Evidian IAM Suite」を活用し、NTTコムウェアのSIおよびサポートによって提供される。

同ソリューションを構成する製品は、ID管理機能を提供する「Evidian Identity Governance & Administration」、多要素認証機能を提供する「Evidian Authentication Manager」、SSOやフェデレーション機能を提供する「Evidian Enterprise SSO」および「Evidian Web Access Manager」がある。

ユーザーは、上記4つの製品から必要に応じて一つだけ導入することも可能だ。ニーズに合わせて取捨選択できる柔軟性が強みだという。

多様な働き方で、増える情報漏えいリスク

「NTTグループの大規模な認証基盤の構築実績と、その運用を支えてきたという経験も大きな強みです。小規模から大規模まで、ニーズに応じた形でソリューションをご提案できます」（野呂氏）

組織のITシステムやユーザー環境が複雑化する中、システム管理者が手動で社員のIDやアクセス権を管理することは現実的ではなくなりつつある。IAMの自動化は、変化の激しいビジネス環境に俊敏に対応し、ゼロトラストにおけるセキュリティ対策につながるものだ。

NTTコムウェアは今後、SmartCloud IAMソリューションに新機能を追加する構想を進めている。その中には、コンテキストに応じて認証レベルを自動的に変更する機能やFIDO2に準拠した生体認証への対応などが含まれる。コロナ禍などグローバルな環境の変化に応じて、新たな機能をスピーディーに実装し、ユーザーに提供する予定だ。

「これからはIAMの自動化にとどまらず、セキュリティ全体の自動化（Security Automation）へと進んでいくでしょう。また、セキュリティは運用と組み合わせてセキュアな状態を安定的に継続できることが重要です。お客さまが『ビジネスを俊敏に、セキュリティを堅牢に』という世界を実現できるよう日々取り組んでいきます」（野呂氏）

●関連リンク

SmartCloud IAMソリューション ▶ https://sc.nttcom.co.jp/smartcloud-si/security/id/

転載元：ITmedia エンタープライズ
ITmedia エンタープライズ　2021年1月26日掲載記事より転載
本記事はITmedia エンタープライズより許諾を得て掲載しています
https://www.itmedia.co.jp/enterprise/articles/2101/26/news008.html

NTTコムウェア株式会社
URL：https://www.nttcom.co.jp/