―IDC Security Vision Japan 2020 講演―

DX、働き方改革を推進するからこそ必要となるIAMソリューション

～オンプレミスとクラウドサービスのハイブリッド環境を前提としたIDライフサイクル管理の自動化、SSOの実現～

2020年11月26日（木）、IDC Japan主催のIDC Security Vision Japan 2020で、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である野呂昌哉が講演した。

ポイント 1	ポイント 2	ポイント 3
IAM基盤とは何か？	ゼロトラストがDXの前提、IAMもトランスフォーメーションを	大企業で実績のあるIAMの導入

重要な情報へのアクセス、本当に管理できてますか？今、「IAM」に注目すべき理由

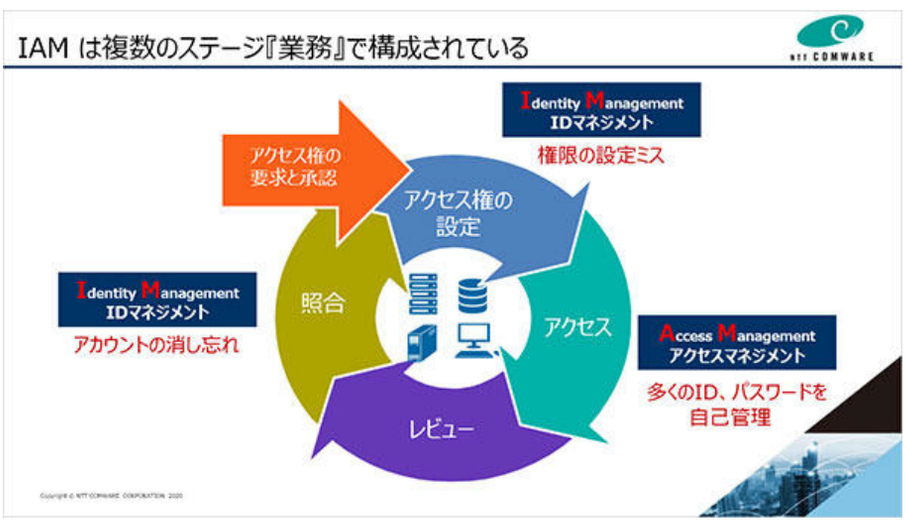
DXや働き方改革の取り組みを進めていくことは、論をまたないところであり、非常に多くの企業が積極的に取り組んでいる。多くの課題に頭を悩ませながら進めていくなかで、見過ごされがちなことにIAM基盤の整備がある。

IAMとは“Identity and Access Management”のことで、IDマネジメントとアクセスマネジメントの2つからなる。IDマネジメントは、「誰に・どのような権限で」情報にアクセスさせるかという、IDや情報システム内のアクセス権限を管理する機能。アクセスマネジメントは、「どのように」情報にアクセスさせるかを管理・制御する機能で、どんな手段でユーザーを本人と認証するのか、どこからのアクセスを許可するのか、どの情報システムへのアクセスを許可するのか、というアクセス制御も担う。

IAMに関わる業務は、「アクセス権の要求と承認」「アクセス権の設定」「実際のアクセス業務」「レビュー（不適切なアクセスがないかの検証・監査）」「照合（アクセス権が正しく維持されているか等の棚卸）」のステージに分けられる。これらは特別に何か新しいテクノロジーを必要とする業務ではなく、社内システムを用いる業務フローの中では、何らかの仕組みで運用される、手間はあっても日常的な情報システム管理業務であるはずだった。

しかし、クラウドサービスが普及し様相が変わってきた。情報システムの構造的変化により、IAMの各ステージに負のインパクトが生じてきたのだ。

すべてを既存のActive Directory認証などのみでカバーすることはできず、システム毎に利用申請と設定が発生することで、「事務手続きが増えた」「設定が複雑」などの負担を感じる企業が増え、ビジネス加速の足かせとなっている。とりわけIDマネジメントの観点では、権限の設定ミス、アカウントの消し忘れがリスク要因となる。アクセスマネジメントの観点ではユーザーが業務遂行のため多くのID、パスワードを自己管理しなければならない状況がリスク要因となる。

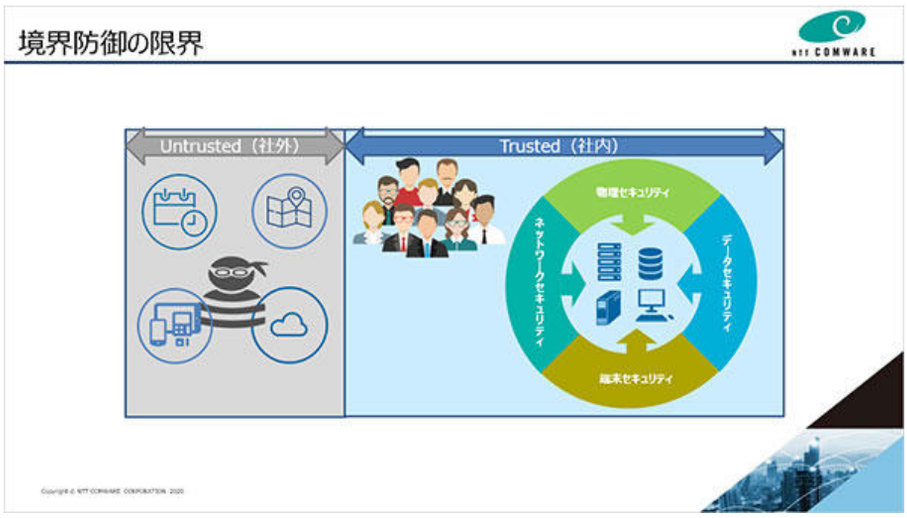


「ゼロトラスト」を前提としなければ、経営者がめざす真のDXは進められない

DXや働き方改革の時代。ワークスタイルが変化し、クラウドサービスの活用が進むことで、「いつでも、どこからでも、さまざまなデバイスで」情報システムにアクセスできるようになった。これがセキュリティー対策に変化を迫っている。

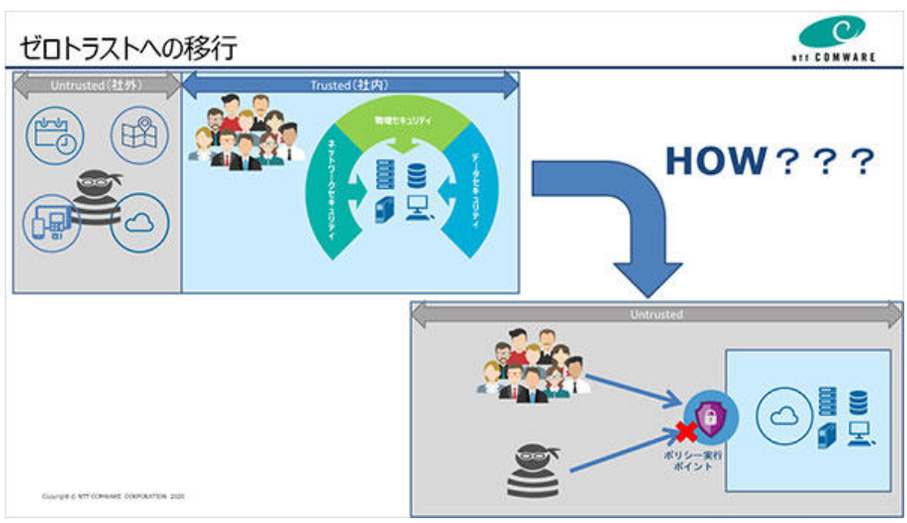
これまでの情報システムは社内ネットワークをTrusted、社外ネットワークをUntrustedとする「境界防御」という考え方で保護されてきた。

－IDC Security Vision Japan 2020講演－
DX、働き方改革を推進するからこそ必要となるIAMソリューション



しかし、境界防御に基づく保護は限界を迎えつつある。保護すべき情報資産は社内だけでなく社外にも存在するようになり、また、Untrustedな社外からの利用もDXにより求められている。さらにTrustedなはずの社内への侵入という脅威も近年では考慮すべきであり、「すべてをUntrusted」、信頼しない前提とする必要が出てきたからだ。

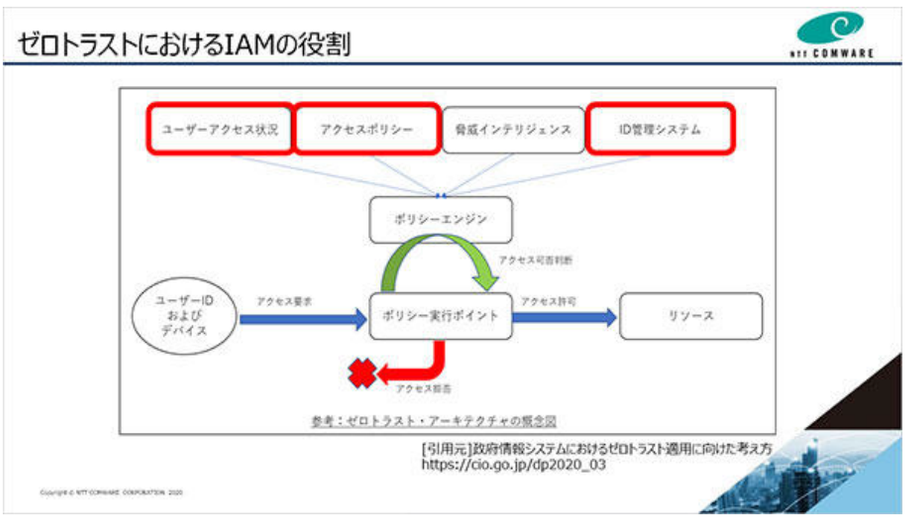
これが最近、話題となっている「ゼロトラスト」の基本的な考え方である。



「ゼロトラスト」ではアクセス元をすべてUntrustedとし、必ず、ポリシー実行ポイントを経由したアクセスを求める。そこでは動的にポリシーの適用が行われ、アクセス元やアクセス先のリソースに対して必ず検証が行われる。そしてアクセスの可否が決められる。

しかし、従来の「境界防御」から「ゼロトラスト」への移行はたいへん難しく、情報システムが多い大企業ほどその難度は上がる。理由は、抜本的な見直しが必要であり、単純なソリューションの導入で実現できるものではないからである。そのため、「ゼロトラスト」の実現には段階的な移行が必要である。

これらを踏まえ、内閣府IT総合戦略室出典のディスカッションペーパー「政府情報システムにおけるゼロトラスト適用に向けた考え方」を参照すると、ゼロトラストのアーキテクチャの構成要素である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が、IAM基盤の整備によって可能となることがわかる。したがって「ゼロトラスト」をめざすには、まずIAM基盤の整備をお薦めしたい。



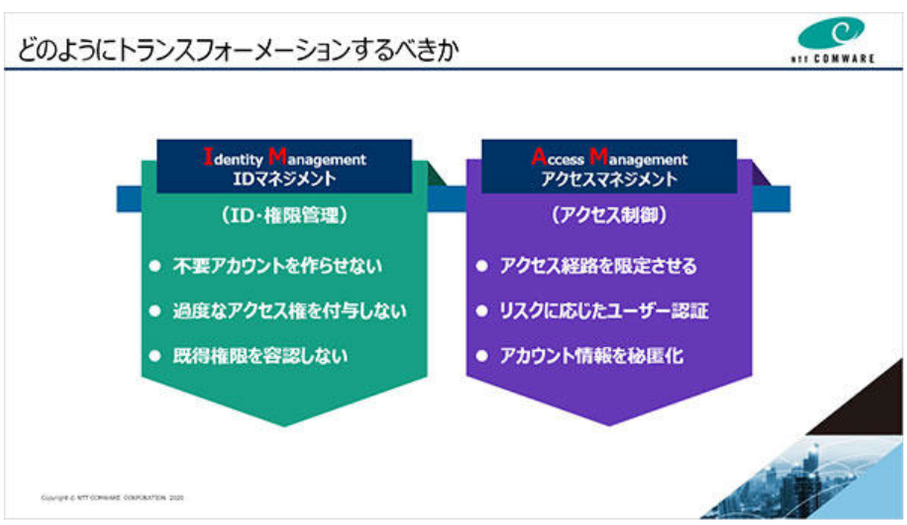
IAMのトランスフォーメーションとは？

IAMに対する考え方そのものも時代に合わせてトランスフォーメーションする必要がある。

では、どのようにトランスフォーメーションするべきか。

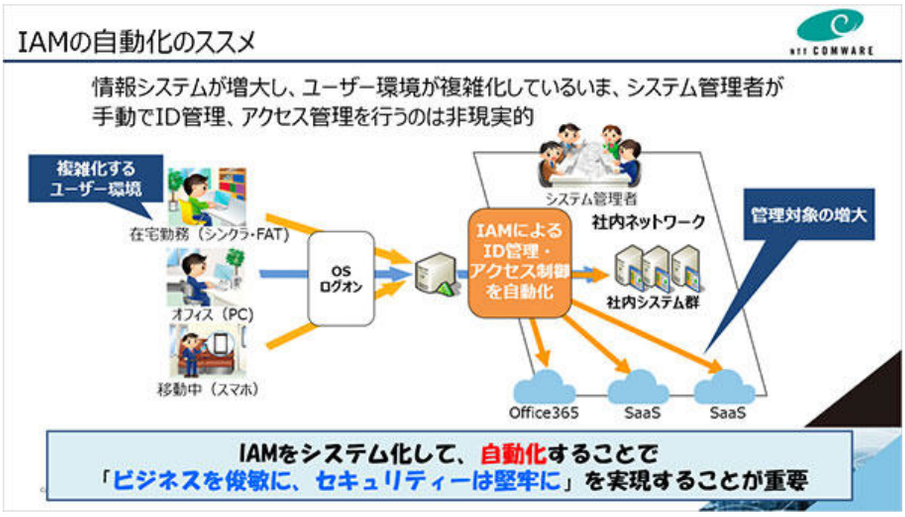
IDマネジメントでは、標的型攻撃により不正利用される恐れのある不要なアカウントを作らせないこと、内部不正されないように過度なアクセス権を付与しないことが重要である。そして、各システム上の「アカウント権限の棚卸しができる仕組み」へとトランスフォーメーションすべきである。

アクセスマネジメントでは、各情報システムへのアクセスを把握するためにアクセス経路を限定し、ロケーション・デバイス・振る舞いなどに基づき、リスクに応じたセキュリティーレベルでユーザー認証を行うことが重要となる。また、アカウント情報の漏えいリスクを最小限にするためには、各システムで使用する「ID、パスワードをユーザーに開示しない運用」へとトランスフォーメーションするべきである。



IAMをトランスフォーメーションする上でもう1つの重要な視点は、「オンプレミス、クラウドサービスを分け隔てることなく、ハイブリッドに対応可能にすること」である。

さらに「IAMの自動化」を強くお薦めしたい。情報システムの数も規模も増大し、個々のユーザー環境が複雑化しているなかで、システム管理者が手動でID管理やアクセス管理を行うことはもはや非現実的である。IAMを自動化することで初めて「ビジネスを俊敏に、セキュリティーは堅牢に」を実現し、真のDXにつながるといえる。



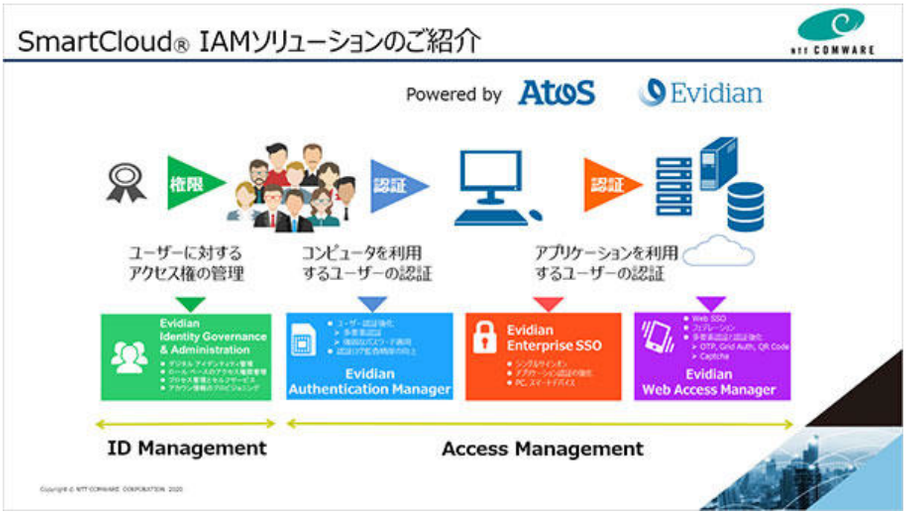
NTTコムウェア自身も2018年度からトランスフォーメーションに取り組み、社内のIAM基盤を刷新した。NTTグループ統合認証基盤と連携しつつ、オンプレミスのレガシーシステムとのインターフェースを変更せずにシングルサインオン（SSO）を実現する必要があった。さらにクラウドサービスに必要なSAML認証連携に対応した認証基盤を実現するため、Atos社のEvidian IAM Suiteを導入。いまでは、ハイブリッド環境での社内システム70以上へのSSOを実現し、年間2,500万円のコスト削減を実現している。

情報システムの多い大企業への導入を実践した、最適なIAMソリューションの提案

NTTコムウェアは、社内IAM基盤へのEvidian IAM Suite導入をきっかけとして、Atos社とアライアンスを締結。Atos社のグローバル市場での豊富なIAMソリューションの提供実績とNTTコムウェアの大規模認証基盤構築・運用の実績という双方の強みを活かして、より高度なIAMソリューションとオペレーションの実現に取り組んでいる。

「SmartCloud® IAMソリューション」は、必要とされるID・アクセス権限の管理、アクセス制御までを一貫して管理・制御できる。ハイブリッド環境に対応したIDライフサイクル管理の自動化やSSO・フェデレーションの実現ができることが大きな特長だ。

－IDC Security Vision Japan 2020講演－
DX、働き方改革を推進するからこそ必要となるIAMソリューション



DXや働き方改革が企業にとっての優先課題となり、そのためにレガシーなオンプレミスだけでなく新たなクラウドサービスの活用が一般的になってきたのは自然な流れである。

こうした肥大化するハイブリッド環境で大きな変化に直面している今だからこそ、最適なIAMソリューションを導入し、企業の業務環境の根幹を支えるIAM基盤の整備にぜひ取り組んでいただきたい。

NTTコムウェア株式会社
URL：https://www.nttcom.co.jp/
WEB 掲載：2020.12