情報セキュリティにおける マイクロソフトでのアプローチの転換

「すべての企業がデジタルを活用したビジネスへと転換しつつある」と、マイクロソフト CEO のサティア・ナデラは言います。あらゆる業界のあらゆる規模の組織が、さらなる成長に向けてデジタル テクノロジによる変革を推進しています。各組織でこうしたデジタル トランスフォーメーションの普及が進むにつれ、従業員が容易かつ安全にコンテンツを見つけ、共有できることが極めて重要になります。なぜなら、それこそが変革の成功に必要な 2 つの要素 — イノベーション力と創造力 — を従業員が短期間で獲得できる条件だからです。しかし、これらの新しいニーズは新たなリスクを生み出します。そのため、マイクロソフトをはじめとするさまざまな組織が、情報セキュリティにおけるアプローチの転換を迅速に進めています。

ほかの組織と同様に、マイクロソフトでも、個人所有のモバイル デバイスを使用し、インターネットからサードパーティのサービスに接続して、クラウド上でコンテンツの共同作業や管理を行う従業員がますます増えています。彼らは、従来型の企業ファイアウォールの境界の外側にあるプラットフォームやサービスを利用して共同作業を行いますが、その範囲は Microsoft IT の一元管理下にないサービスにまで及ぶ場合があります。共同作業におけるこうした傾向が、現代のあらゆる企業、そして業界に影響を及ぼしています。実際に、アナリストは、典型的な組織で採用されているテクノロジの約 50% が IT 部門が選定したものではないと見積もっています。それどころか、個々の部署や従業員がそれらの判断を行っているため、そのプロセスに IT 担当者がかかわっていない場合もあります。

このようなデジタル トランスフォーメーションによって、人々は容易に共同作業を行い、コンテンツを見つけて共有できるようになり、新たな種類のイノベーションや創造力も実現するようになりました。また、業務での効率や生産性も高まります。とはいえ、こうしたプラスの効果がある反面、デジタル トランスフォーメーションはセキュリティ上の課題も生み出します。組織の管理下にあるシステムからコンテンツが離れた途端に、潜在的なセキュリティリスクが生じるためです。

コンテンツの作成、保存、転送が行われる内部システムの保護に重点を置く従来のセキュリティ アプローチでは、もはや十分とは言えません。変革を成功させるには、情報セキュリティと使用する手法に対する考え方を変える必要があります。これは差し迫ったニーズです。共同作業によって企業がコンテンツを保存する場所が実質的に変わるので、共同作業が行われる場所を問わずコンテンツを保護できる新たな手段を採用することが急務になります。つまり、企業ファイアウォールの内側かどうか、会社の管理下にあるシステム上かどうかにかかわらず、コンテンツの流れを説明できるモデルに移行して、保存場所を問わずコンテンツを保護し、従業員にコンテンツのセキュリティ分類レベルとその対象ユーザーを通知できるようにしなければなりません。

職場でのデジタル トランスフォーメーション

これは何年のことでしょうか

インフォメーション ワーカーが各自のワークロードのクラウドソーシングや外部委託を行い、未承認のプラットフォームで共同作業を進め、自分のプロジェクトに役立つ可能性のあるコンテンツを会社のリポジトリから探すためにスカベンジング アプリを利用している。主なインターフェイスは各自のスマートフォンである。自分の全資格情報をサード パーティがホストするソリューションに保存し、自分の全データを個人所有デバイスに同期している。

答えは 2016 年です

これらのテクノロジと手法は現在すべて利用可能で、従業員が使用しているものです。

こうした取り組みを支援すべく、Microsoft Office にはコンテンツの検索と保護に役立つ最新のテクノロジが搭載されています。たとえば、数ある機能の中でも、Microsoft Office Delve を使用すると、従業員が各自の共有コンテンツのセキュリティを評価して、不適切なコンテンツの共有 (一般に「過剰共有」と呼ばれます) が起こるリスクを最小限に抑えることができます。Delve では、各従業員が共有したコンテンツやアクセス権を持つコンテンツの一覧を表示することや、アクセス権を持つ他のユーザーを確認することができます。従業員が機密性の高いコンテンツを過剰共有したことに気付いた場合は、そのコンテンツに対するアクセス制限をさらに厳しくすることも可能です。さらに、Office クライアント向けに提供されている Azure Information Protection を使用すると、従業員が各自のコンテンツを分類し、それを機密度に応じてラベル付けし、必要に応じて暗号化と使用権を適用できるようになります。それらは、コンテンツが組織の境界を離れる場合でも永続的に有効です。また、Microsoft Teams (現在、プレビュー版) は、Office 365 の新しいチャットベースのワークスペースです。人、会話、コンテンツを結び付けると共に、チームに必要なツールを備えているため、セキュリティで保護された方法で容易に共同作業を進めることができます。保存中および転送中のデータの暗号化機能や、多要素認証機能も搭載されています。このような役立つアプリケーション、サービス、ユーティリティ、および機能が、マイクロソフトのセキュリティ ツールボックスに新たに追加されました。

共同作業と生産性を向上させる

"デジタル トランスフォーメーション" とは、組織が情報やテクノロジの利用方法を大幅に転換することによって、技術的なプラットフォームにかかわらず、従業員が生産性と共同作業を向上させることができるようにすることを言います。これは緩やかな変化ではなく、コンテンツが作成され使用される方法における破壊的な変革です。

かつて従業員は、イントラネット専用アプリケーションでコンテンツを作成していましたが、今では、ビジネス向けにセキュリティ レベルの異なるさまざまなコンシューマー指向のアプリを使うことが一般的になっています。このリスクを伴いかねない変革の中心には、次のような傾向とテクノロジがあります。

- **ソーシャル ワークフロー。**クラウドソーシング、マス コラボレーション、共同編集ツール、"No-Email" キャンペーン、外部のピアツーピア コミュニティ、および非構造化プロセスが主流になっています。
- **ユビキタス接続。**デバイスに依存しない常時接続状態に近付くなか、会話が複数のデバイスにまたがって行われ、リアルタイムの対話式操作が標準になっています。
- **組織の境界を越えることも珍しくない、急激なコンテンツの増加。**最新のデータ分析プラットフォームでは、配信元を難読化することができ、統合された情報ビューを表示するために内部と外部のソースからコンテンツを収集する場合もあります。
- **緩やかに結合された、大量かつ時には無料のテクノロジ。**どの部署も、IT 部門からのみテクノロジを調達することはなくなり、組織の管理下にない無料のサード パーティ ソリューションを使うことも珍しくありません。デバイスの使用は、可視化プラットフォームやウェアラブルにまで拡大しています。ほとんどが、ドメインベースのアーキテクチャによって制御されることはなくなりました。今や、従業員の ID が新たな境界となっています。
- **データを収集、処理、保存するための新たな方法。**人工知能、機械学習、およびボットが主流になりつつあります。これらのテクノロジは、従業員にコンテンツの集約された見方を提供します。また、自然言語システム、スマート アドバイザー、デジタル デクステラティ、拡張現実、および人間増補も台頭しつつあります。

デジタル トランスフォーメーションは多くの面でメリットをもたらします。デジタル トランスフォーメーションによって、顧客エンゲージメントの強化、従業員の生産性の向上、業務の最適化、および技術的ソリューションの変革が促進されます。マイクロソフト CEO のサティア・ナデラが、中核的な全社規模のイニシアチブにおいてデジタル トランスフォーメーションを焦点に据えたのはそのためです。マイクロソフトでは、各部署および従業員が、ビジネス上の意思決定をより迅速かつ適切に行うために、より多くのコンテンツで対話式操作や共同作業を行えるようになっています。ほかにも多くの組織が同様の転換を進めており、業界アナリストは、デジタル トランスフォーメーションが今後ますます急速に普及するだろうと予想しています。

システムだけでなく、コンテンツも保護する

Microsoft IT の目標は、従業員が俊敏性と生産性を向上できるようにすること、そして、データの質を高めてより良いビジネス成果を達成できるようにすることです。デジタル トランスフォーメーションはこの目標に即しているとはいえ、セキュリティにおける長年のアプローチの転換が求められます。自社のコンテンツのセキュリティを維持するには、IT 上のリスクとセキュリティ上の戦略を更新し、強化する必要があります。そのため、今すぐ行動を起こさなければなりません。

従来、マイクロソフトでは、コンテンツへの未承認のアクセスを防ぐことを目的としたテクノロジの構成とセキュリティ強化に重点を置いてきました。これは、正しい鍵を組み合わせたときにだけ開けられる金庫の中にお金を入れることに似ています。しかし現在、従業員は他のユーザーとさまざまな方法でコンテンツの共同作業や共有を行うようになり、もはやデジタルの資産は会社所有のネットワークやシステムに限られたものではなくなりました。従業員の個人所有デバイスやパブリック プラットフォーム上にデジタルの資産が存在することも考えられます。保護しなければ、重要な企業データや個人情報が侵害されてしまう可能性があります。そのため、コンテンツの場所を問わず、セキュリティで保護されたシステムを離れた場合でも、常に保護が有効でなければなりません。これは簡単そうに聞こえるかもしれませんが、マイクロソフトでのセキュリティと、一般的な IT におけるセキュリティについて考える必要があるという点で、極めて大きな変化です。

当社は、もはや IT 部門が管理するテクノロジだけを使ってコンテンツを管理することはできないことを認識しています。コンテンツ自体を管理する必要もあります。同時に、適切なユーザーに適切なコンテンツへのアクセス権を付与したいとも考えています。そのためには、従来のやり方でシステムのセキュリティを強化するだけでなく、次のような新たな手法を組み合わせて利用する必要があります。

- **ラベル付け。**従業員が、透かしや、ファイル ヘッダー、コード ヘッダー、および共有対象としてふさわしいユーザーを示すその他の表示によって、コンテンツ自体にラベルを付けます。また、機密度 ("社外秘" や "極秘" など) に応じてコンテンツを分類することもできます。
- **通知。**通知によって、従業員は共有しようとしているコンテンツの内容や、共有相手を知ることができます。通知は、コンテンツの機密度を示すコンテンツ ラベルで構成されます。また、コンテンツの共有相手も示します。
- **アクセス権管理。**使用権を適用することで、分類 (ビジネスへの影響) と、そのコンテンツへのアクセス権を取得しようとする人物の役割に応じて、コンテンツを利用できるようにします。対象ユーザーは、コンテンツの特定の分類に対する権限を持っている必要があります。従業員が、コンテンツを分類し、対象ユーザーを選択してから、特定のコンテンツに対象ユーザーがアクセスできるようにアクセス権を割り当てます。アクセス権管理は、コンテンツが保存されているシステムでサポートされている限り有効です。
- **役割の割り当て。**従業員に役割を割り当てることで (特定のグループに割り当てるなどして)、従業員がアクセスできるコンテンツの種類を管理できます。

- **トレーニング。**トレーニングは極めて重要です。従業員は、通知、コンテンツの分類方法、その作業が必要な理由を理解する必要があります。過剰共有を行わないための理由を理解することで、従業員はコンテンツを適切に処理する手順に従うようになります。
- **保持。**アイテム保持ポリシーによって、コンテンツの保存期間を制御できます。規制、法律、会社の各要件に従って必要な期間だけコンテンツを保存するためにアイテム保持ポリシーを使用することで、アクセスされ悪用される可能性のあるコンテンツの数を減らすことができます。
- **暗号化。**基盤となるシステムに依存しない最も重要な制御手法です。暗号化は、コンテンツの場所に関係なく常に有効なためです。コンテンツにアクセスするには、暗号化キーが必要になります。承認されていない人物がコンテンツへのアクセス権を取得しても、暗号化キーがなければ、コンテンツを表示することも使用することもできません。これが、IT 部門が管理するネットワークやシステム以外に移動されるコンテンツを保護するうえで最も安全な方法となります。
- **監査とログ。**この手法によって、コンテンツの配置場所とコンテンツにアクセスできる人物を追跡できます。

セキュリティにおける 4 方向のアプローチを定義する

Microsoft IT では、デジタル トランスフォーメーションに沿った新しいセキュリティ モデルを開発しました。コンテンツを作成または保存するときに使用された基盤となるテクノロジがわからない場合でも、コンテンツへのアクセスを管理する必要があります。それにより、従業員がコンテンツを共有して共同作業を行う際のセキュリティ侵害を防ぐことができます。したがって、当社の新しいモデルでは、テクノロジはもとより、コンテンツ自体をセキュリティで保護することに重点を置いています。

図 1. 効果的なセキュリティ戦略の 4 つの区分。セキュリティの専門家は、左側の基本事項に対応することに留意しながらも、できるだけ右側の区分に取り組みを転換することを勧めています。

このモデルは、コンテンツをセキュリティで保護するための 4 方向のアプローチを詳述したものです (図 1 参照)。左側の列は、当社が長年運用してきた、テクノロジ制御に基づく従来型のセキュリティ アプローチを示しています。一方、右側の列は、コンテンツに従って、コンテンツ自体をセキュリティで保護する、当社の新しいアプローチを示しています。下段は、承認されていない人物がシステムやコンテンツへのアクセス権を取得することを防ぐための手法に関する事項、上段は、アクティビティを検出するための手法に関する事項です。

この 4 方向のセキュリティ モデルによって、マイクロソフトでの情報セキュリティのレベルを適切に評価できます。このモデルから、当社の手法のどの部分を改善する必要があるかを知り、どのテクノロジを採用すべきかを判断することができます。またこのモデルは、従業員が使用するアプリケーションへのアクセス権を制御するといった従来型のアプローチにのみ依存する状況を打開し、従業員が作成して共有するコンテンツを配置場所に関係なく管理するのに役立ちます。

コンテンツを保護するための適切な安定した制御を実現するには、このセキュリティ モデルの 4 つの区分すべてに挙げられた手法を利用する必要があります。つまり、引き続き左側の基本事項に対応しながらも、右側の列に取り組みの重点を置く必要があるということです。このまま左側の列の手法だけを使用し続けると、コンテンツを制御できる人々から格好の標的にされる可能性があります。

コンテンツ自体をセキュリティで保護するための右側の列のタスクには、IT 部門にとって新しいタスクが含まれます。これらは次の 2 つのフェーズで実行します。

- **予防フェーズ。**このフェーズでは、コンテンツへのアクセス権を分類し、保存し、管理することを目指します。そのためには、テクノロジをセキュリティで保護する (ベースライン構成のセキュリティを強化して、テクノロジ イベントを監視する) ことからさらに考えを広げ、組織内でコンテンツが実際に作成され管理される方法 (未承認のテクノロジ、適切に分類されていないコンテンツ、管理されていないリポジトリ、過剰に広範なアクセス権などの事例を特定する方法) について考える必要があります。その後、脆弱かつ重要なコンテンツのセキュリティを強化するための対策を講じます。
- **検出フェーズ。**このフェーズでは、共有されているコンテンツを知り、他の人の視点からそれがどのように確認できるかを把握することを目指します。組織で最も脆弱な部分を見つける作業もこのフェーズで行います。組織の機密情報が適切に保護されているか、あるいは誰でも利用できる保護されていないリポジトリに散在していないかを確認します。

コンテンツを保護するために最新テクノロジを利用する

監視と警告を目的とする従来型のツールを使用するだけでなく、コンテンツが共有されている方法を検出し、過剰共有の防止を促進するタスクをサポートするために、マイクロソフトでは、次のような Office 365 で提供する検出と予防を目的としたテクノロジを利用しています。

- **Delve (検出)**。従業員は、各自の Delve サイト内で、社内のどのリポジトリに自分のコンテンツが配置され、誰がそのコンテンツにアクセスできるかを確認できます。コンテンツを作成するためにどのアプリケーションが使用されたか、または、正確にネットワーク上のどこにコンテンツが保存されているかは問題ではありません。マイクロソフトでは、従業員に各自の Delve サイトを定期的にレビューし、過剰共有されているコンテンツがないか確認するよう促しています。また、社内のグループが、Delve で検索を行い、グループのコンテンツが保存されている場所と、そのコンテンツへのアクセス権を持つ人物を確認できるユーザーを割り当てることも可能です。必要に応じて、リポジトリのセキュリティを強化することや、機密性の高いコンテンツをより適切に保護するためにそのコンテンツの分類方法を変更することもできます。

- **Azure Information Protection (予防)。**Azure Information Protection では、従業員がコンテンツの分類、ラベル付け、保護を行うことができます。従業員が各自のコンテンツを分類することも、IT 部門が機密情報 (クレジット カードや社会保障番号など) を含むコンテンツの分類を自動化することもできます。必要に応じて、機密性の高いコンテンツの暗号化を指定し、使用権を定義することも可能です。分類ラベルと保護は、コンテンツの保存場所やコンテンツにアクセスできる人物にかかわらず永続的に有効です。また、Azure Information Protection が適用されている場合、従業員は各自のコンテンツへのアクセス権を持つ人物やコンテンツの配置場所を確認できます。これは、コンテンツが組織の境界から離れる場合に特に便利です。
- **SharePoint、OneDrive for Business、および Exchange (予防)。**ビジネス上の理由から、マイクロソフトの従業員は社内および社外の人とコンテンツを頻繁に共有します。当社の共有サイト (SharePoint および OneDrive for Business) は、サイトに保存されたコンテンツの機密度に基づいて共有の選択肢をガイドする通知を従業員に提供します。サイト所有者がどの通知を表示するかを決定します。それらのサイトは、特定の個人またはグループだけがコンテンツにアクセスできるようにするためにセキュリティで保護できます。また、Exchange では、社外の人にメッセージを送信する場合や、電子メールに機密データが含まれている場合に、従業員に通知します。
- **Microsoft Teams (予防)。**Microsoft Teams は、共同作業を行うための安全な場所をチームに提供し、セキュリティで保護されていないプラットフォームでコンテンツを共有するリスクを低減します。チームがアプリ内で直接共同作業を行うために必要なすべての機能にアクセスできる、チャットベースのハブです。Microsoft Teams には、Office 365 のエンタープライズ向けのセキュリティおよびコンプライアンス機能、幅広いコンプライアンス標準のサポート、常時 (保存中および転送中) のデータの暗号化、そして、ID の保護を強化するための多要素認証が含まれます。

コンテンツを保護するための従業員との連携

コンテンツをセキュリティで保護するという課題に取り組むなかで、マイクロソフトは、最も重要な目標の 1 つに従業員との連携の実現を掲げました。そのためには、共同作業をどのように行いたいと考えているのか、また、業務を効果的および効率的に進めるうえで何が役立つのかを、従業員から正確に聞き出さなければなりません。次に、共同作業上のニーズとセキュリティ上のニーズのバランスを取るための的確なソリューションによって対応する必要があります。さらに、コンテンツのセキュリティを維持するための方法について従業員にトレーニングを行い、このバランスを理解して配慮できるよう支援して、従業員がセキュリティ対策を回避しないようにする必要があります。従業員がセキュリティ対策を回避しようとする場合、それに気付き、従業員がより安全な方法でコンテンツを保護するように促すことができなければなりません。

次の表に、マイクロソフトがデジタル トランスフォーメーションにおける新たなセキュリティの課題に対応するために従業員と連携する際の、現在の情報セキュリティのゴールとアプローチをまとめました。

表 1. コンテンツを保護するためのゴールとアプローチ

強化されたセキュリティのゴール	アプローチ
組織内のすべての共同作業ワークフローをサポートする便利なソリューションを提供する。シンプルなソリューションを提供し、従業員が回避する可能性を低減する。	従業員と連携して、共同作業における従業員のニーズを理解し、それらのニーズに対応できるようにします。グループとアクセス権の管理によって、SharePoint Online、OneDrive for Business、および Exchange Online をセットアップします。従業員がプロジェクトで共同作業を行うためのチームやグループをセットアップするように促します。
承認されていないテクノロジを通じてやりとりされるコンテンツを検出するメカニズムを使用する。	ネットワーク境界からの既知のサード パーティ サービスの接続を監視すると共に、承認されていないデータ転送を助長するサード パーティ クライアントがないかワークステーションをスキャンします。
各コンテンツ アイテムの価値、保存場所、およびコンテンツにアクセスできる人物を知る。	キーワードの設定、コンテンツの分類 (制限あり/なし)、人の分類 (グループ名と定義) を行うために全社的な標準を設定します。使用するリポジトリ テクノロジを設定し、リポジトリの場所をセットアップします。従業員に対してこれらのツールに関するトレーニングを行います。
すべての従業員が確立された標準に基づいて各自のコンテンツを分類する。	従業員に対して Office Rights Management および Azure Information Protection に関するトレーニングを行います。従業員がコンテンツの作成プロセスでこれらのツールを使用するように促します。

強化されたセキュリティのゴール	アプローチ
すべての共同作業ワークフローとそれに関するテクノロジで、コンテンツの分類が表示され、そのコンテンツにアクセスできる人物がリストされるようにする。分類と対象ユーザーが一致していることを従業員が確認して、過剰共有を低減できるようにする。	各自の通信やプロジェクトでのコンテンツの共有、共同作業、管理におけるベスト プラクティスについて従業員に教育を行います。従業員がコンテンツの分類方法とコンテンツへの使用権の割り当て方法を理解できるようにします。そして、確立された標準に従って従業員がこの作業を行っていることを確認します。

今後の展望

マイクロソフトでは、社内および世界中のその他の組織でデジタル トランスフォーメーションの普及が今後も続くと考えています。新しい方法でコンテンツを使用し、共有できるようになることで、従業員は洞察を得て、業務での生産性を向上させることができるでしょう。サティア・ナデラは、「デジタル トランスフォーメーションに成功した組織は顧客エンゲージメントを強化し、業務の運用を最適化して、デジタル コンテンツによって製品やサービスを変革できるだろう」と述べています。マイクロソフトでは、組織が各自のコンテンツのセキュリティを維持できるよう支援しながら、デジタル トランスフォーメーションをサポートするテクノロジの開発に精力的に取り組んでいます。Delve、Azure Information Protection、および Teams は、そうした新しいマイクロソフト テクノロジの一部です。

詳細情報

Microsoft IT

microsoft.com/ITShowcase (英語)

Satya Nadella: Why businesses should embrace digital transformation, not only to survive – but also to thrive (英語)

Azure Information Protection

Data Classification Wizard (英語)

Enterprise Mobility + Security

Office 365 グループについて

Microsoft Office Delve

Microsoft Teams

Monitoring and protecting sensitive data in Office 365 (英語)

Office 365 news in September at Ignite—intelligence, security and collaboration (英語)