Microsoft 365を活用した安全・安心・快適な働き方を提案
日立「ゼロトラスト・アーキテクチャーによる協働ワークシナリオ」

リモートワークの拡大にともない、ゼロトラスト・セキュリティへの移行を検討する企業が増えています。しかし、働き方を考慮しないセキュリティ強化策だけでは生産性を損なう可能性があります。日立は、それぞれの企業の働き方に合わせた適切なデバイス保護やファイル配置、外部連携の仕組みも含めた「ゼロトラスト・アーキテクチャーによる協働ワークシナリオ」を提供いたします。

「働く人」を起点としたゼロトラスト・セキュリティを推進

リモートワークやクラウドサービスを活用した新しい働き方が急速に浸透するなか、暫定的に構築した環境のセキュリティ対策にも抜本的な改革が求められています。

また、コロナ禍の混乱に乗じて、サイバー攻撃が急増しています。標的型メール攻撃で侵害したPCを踏み台に、搾取したID/パスワードを使い社内やクラウドサービス上のさまざまなファイルにアクセスし、情報を盗み出すインシデントが多数報告されています。これは、社内アクセス時の利便性確保のためのシングルサインオンの仕組みが、攻撃者にとっては好都合で、不正アクセスと気づかれずに社内システムを徘徊されてしまっている事例といえます（図1）。

こうした課題には、社内と社外を単純に切り分ける境界防御型のセキュリティ対策では対処できません。そのため多くの企業が、全方位のアクセスを監視・検証するゼロトラスト・セキュリティへの移行を進めようとしています。

一方で、"すべて信頼しない"ゼロトラストの原則を追求し、リモートワークでのデータ活用やクラウドサービスの利用を制限すると、円滑な業務遂行やコラボレーションに支障をきたし、生産性や利便性を損なう可能性が出てきます。

重要なのは、「働く人」を基点として、セキュリティと生産性を両立させるような仕組みを提供することです。そこで日立は、業務内容や働き方、働く場所を考慮して、マネジメントとシステムの両面から、それぞれの企業に適したIT環境をデザインする「ゼロトラスト・アーキテクチャーによる協働ワークシナリオ」を提供しています。

「Microsoft 365」の仕掛けでデータを守る

多くの企業がコラボレーション環境としてMicrosoft 365を採用しています。日立は、Microsoft 365の導入前、導入後によらず、次に挙げるようなポイントを押さえながら、コンサルティングからPoC実施、各種製品・サービスの導入、運用まで、ゼロトラスト・アーキテクチャーによる最新技術を駆使して最適な利活用方法を提案していきます。

まず、業務内容と働き方を考慮した「デバイス環境の見直し」に着目します。例えばオフィスアプリケーションなどのドキュメントを多用する一般的なオフィスワーカーがリモートワーク中心の働き方を行う場合は、「在宅でPCを使用、個人情報など機密性の高いデータを参照」「ファイル共有しつつチームで資料を共同作成」「同僚との日常会話やタスク調整もチャットやリモート会議をフル活用」といったケースが多いと想定されます。

この場合、機密性の高い情報をPC内部に保存せずに、快適な業務やコラボレーションを行えるようにするため、Microsoft 365と連携したファイルアクセスによりドキュメントワークを遂行し、移動時のPC盗難・紛失に備えて、電源OFFによりユーザーデータを自動消去する日立の「PCデータ揮発型セキュリティサービス」を適用し、デバイス側のセキュリティと業務の快適性を両立させる提案を行います。

ゼロトラストで重要なエンドポイントセキュリティも、Microsoft 365を使った業務が中心となる場合、個々に

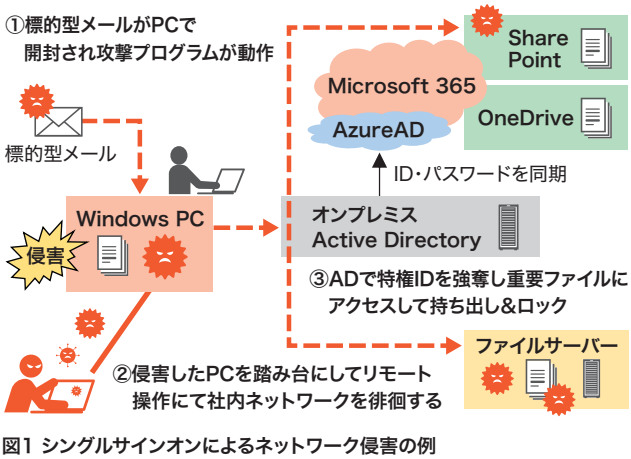

図1 シングルサインオンによるネットワーク侵害の例

ツールをそろえるより、Microsoftのセキュリティクラウドサービスのほうが親和性は高く、総合的な監視・監査業務も効率的です。アンチウイルスはMicrosoft Defender、EDR※1はMicrosoft Defender for Endpoint、ポリシー管理はMicrosoft Endpoint Managerといったように、運用面でもコスト面でも適切なサービスを提案します。

次に「ファイル配置の最適化」も重要です。従来のように境界型ネットワーク内にあるAD※2で認証されるファイルサーバーではサイバー攻撃から重要なデータを守ることはできません。

そこで、ここでもMicrosoftのサービスが効果を発揮します。Microsoft 365のクラウドストレージは、きめ細やかなアクセス権が設定でき、外部・内部を問わず不正なアクセスがないかを総合的に判断できるため、狙われやすい重要データの移行先として有効です。加えてデバイス運用や認証方式の見直しも必要です。Azure ADは、パスワードレスで侵害されにくい多要素認証と生体認証による最新の認証方式を提供しており、従来のオンプレミス型のADからの移行を実現することで、ユーザー管理の簡略化と利便性の両立を図ります。

利用ツールの乱立によって発生するのが「ユーザーの混乱」です。新しい仕組みに慣れず、誤操作やシャドー ITを原因とする「内部からの情報漏えい・情報流出」も是正していく必要があります。これらの多くは社内のITルールが実際の業務実態にマッチしていないこと、ITリテラシーが不十分なことから発生します。そこで、ゼロトラストモデルに沿ったITルールの見直しや、従業員への利活用方法の啓発・定着化を図る継続的な教育プログラムの実施についても、日立はソリューションの一環としてサポートしていきます。

※1 Endpoint Detection and Response
※2 Active Directory

外部とのデータ連携も重要なポイントに

「外部とのファイルやメッセージのやりとり」もポイントとなります。社会課題の解決は一企業で対応することは難しくなっており、積極的な協業や企業間のプロジェクト推進が不可欠になってきました。コミュニケーション場面ではリモート会議が一般化してきましたが、安全にファイル共有できるクラウドストレージやチャット共有の仕組みがあっても、相手企業がクラウドサービスのアクセスをブロックしているケースがあります。結局、メールの添付ファイルでしか企業間の仕事のやりとりができないので、標的型攻撃の原因を抑えることは難しくなります。

そこで日立は、相手企業との協働作業の効率化についても、機密情報をより厳重に保護するMicrosoft Information Protectionの活用や、Microsoft 365の別テナント提供やBoxなどの他のクラウドストレージも含めたプロジェクトデータセグメンテーションの適切な設計・運用の提案をしていきます（図2）。

社会課題の解決にも取り組む

サプライチェーンや公共機関を狙ったサイバー攻撃が激化している現在、個々の企業や組織がセキュリティ対策を講じても、社会全体のリスクを排除することはできません。日立は業種・業界を越えたゼロトラスト・セキュリティを積極的に推進し、お客さま企業の働き方改革と連携させながら、安全・安心・快適な社会の実現に取り組んでいきます。

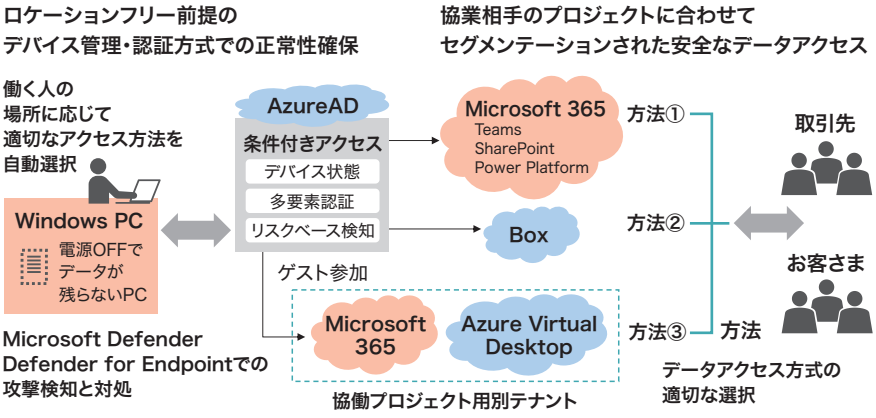

図2 ロケーションフリーで安全・安心・快適な協働ワーク例

お問い合わせ先・情報提供サイト
(株) 日立製作所 IoT・クラウドサービス事業部 働き方改革ソリューション本部
https://www.hitachi.co.jp/products/it/ws_sol/solution/secpc20/