ゼロトラスト移行のための２つの最善手
「課題解決型」「全体最適型」とは？

近年、DX（デジタル・トランスフォーメーション）の推進により、クラウドやテレワークの活用が一気に加速する一方でマルウェア感染や情報漏えいのリスクも増大し、セキュリティ強化が喫緊の課題として浮上しています。そこで注目を集めているのが「ゼロトラスト」ですが、「どのようにゼロトラストへ移行していけば良いのか、どこから手をつければ良いのか分からない」といった声も少なくありません。そうした悩みを解消し、企業が効果的にゼロトラスト移行を進めるための2つのアプローチについて解説します。

なぜゼロトラストへの移行は難しいのか

近年、ゼロトラストへの注目が集まる中、「従来の境界型セキュリティからどのようにゼロトラスト環境へ移行すれば良いのか」「どのようなソリューションを実装していけば良いのか」といった悩みを抱える企業は少なくありません。その理由には、ゼロトラストが特定のソリューションを指し示すものではなく、あくまでも概念であること、そして検討すべき領域がエンドポイントからネットワーク、クラウドなど、多岐にわたることが挙げられます。本稿では、富士通 西尾が、ゼロトラスト移行を適切に実現するための２つの方策について解説します。

一般に、ゼロトラストは図1に示すような5つの領域に分けて考えれば、理解しやすいと思います。しかし、それでも「どこから着手すれば良いのか」「どのようなソリューションが自社にとって最適なのか」分からないといった声が数多く寄せられているのも確かです。

富士通株式会社
ネットワーク&セキュリティサービス
事業本部
ゼロトラストサービス事業部
シニアディレクター
西尾 仁

富士通では、企業・組織がゼロトラストへの移行を進めていくにあたって、大きく2つのアプローチがあると考えています。

図1 ゼロトラストで検討すべき5つの領域

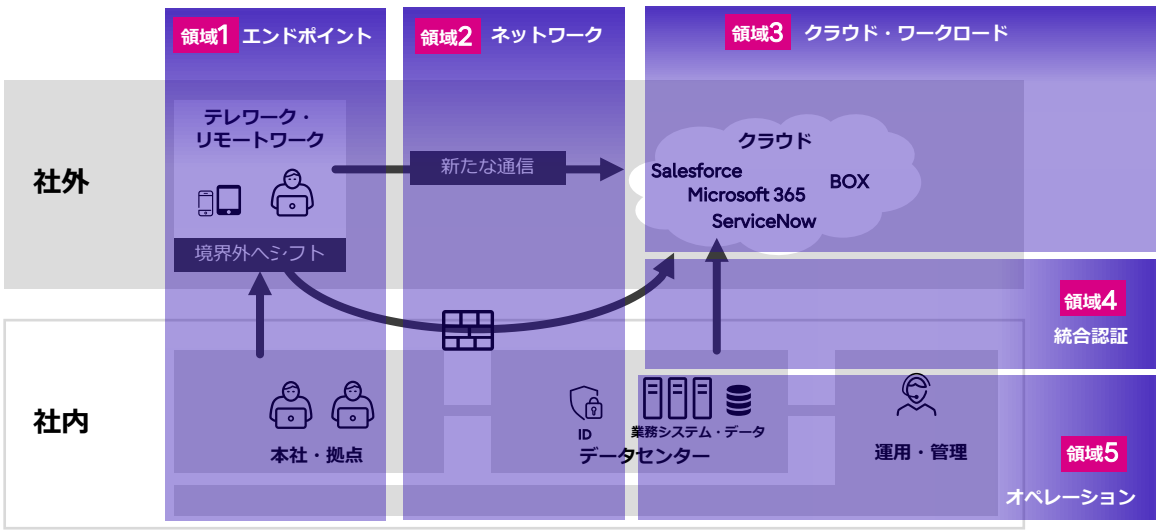


図2 ゼロトラストを実現する2つのアプローチ

1つは「課題解決型アプローチ」、もう1つは、「全体最適型アプローチ」です（図2）。

課題解決型アプローチとは、まずは目前の課題に対して、適宜、必要なソリューションを適用していくというものです。そのメリットは、部分最適による導入のため、シンプルかつ比較的短期間でセキュリティ強化が図れることにあります。ただし、留意すべきポイントとして、対象領域が抱える課題によっては、導入メリット以上に投資コストが発生するケースがあります。また、ゼロトラストで実現すべき最終ゴールに対して、遠回りとなってしまう場合もあるので、十分な検討が必要です。

もう１つの全体最適型アプローチとは、長期的な視野を見据え、 ゼロトラスト環境に移行していくというものです。つまり、理想となる将来のゼロトラスト像を描いた上で、段階的にセキュリティを強化していくというやり方です。このアプローチの最大のメリットは、将来を見据えた全体最適が図れることにあります。ただし、導入完了まで長期間を要するため、移行手順の十分な検討が必要です。また、全社を通じた大規模なITシステムの変更が生じるため、経営層や関連する各部門を巻き込んだ計画の策定、実施はもとより、「なぜゼロトラストの導入が必要なのか」といった明確な意義の提示が、課題解決型アプローチよりも必要となります。

ここからは、ゼロトラストを実現するための各アプローチにおいて、具体的にどのように進め、どのような対策法を導入していくのが効果的なのか、詳しく解説していきます。

優先度に応じてゼロトラスト移行を行う課題解決型アプローチ

はじめに課題解決型アプローチから見ていきましょう。以下にゼロトラストの移行で検討すべき5領域における主な課題とその解決策を示します。

① エンドポイントにおける対策

「攻撃の高度化によってPCの完全な防御が難しくなっている」ことや、テレワークの普及に伴い「ノートPCが社外にあるため、サイバー攻撃があった時に分析や追跡がすぐにできない」などの悩みの声が増えています。そうした課題を解決するためには、PCやモバイルデバイスなど、エンドポイントに対するセキュリティ対策の強化が必要となります。

サイバー攻撃が高度化する中では、「アンチウイルスソフトさえ入れておけば一先ずは大丈夫」といったセキュリティ意識のままではエンドポイントを攻撃から防御することはできません。したがって、ユーザーの振る舞いや行動分析に基づいて異常を検出し、対処するEDR(Endpoint Detection and Response)などの新たな対策の導入が不可欠となります。

② ネットワークにおける対策

テレワークやクラウド活用の拡大に伴い、VPNトラフィックの急増や帯域幅のひっ迫による通信速度の低下がユーザーの利便性を損なうケースが増えています。また、情報システム担当者においても最新のセキュリティソリューションの導入をはじめ、急増するトラフィックへの対処といった、ネットワークに関する管理負担増が課題として浮上しています。

そうした課題を解決する手段として、社内へのVPNを介さずクラウドに直接、セキュアに接続することでネットワーク接続の利便性と安全性を確保する「SASE(Secure Access Service Edge)」や、多様なロケーションから直接インターネットへアクセスする仕組みを実現するSD-WANなどがあります。また、DNSの仕組みを利用しインターネット上の脅威からネットワークを防御するセキュリティ機能の導入も、ネットワークにおけるセキュリティ強化には有効となります。

③ クラウド・ワークロードにおける対策

企業のクラウドリフト、シフトが進む中、情報システム部の管理が煩雑化していることに加え、クラウド環境の不適切な設定によるセキュリティインシデントが増加しています。

従来型のオンプレミスの環境であれば構築中のシステム環境はネットワークに接続することなく、セキュリティ監査を実施した後に本番環境へ移行させることができました。しかし、昨今では、クラウドの活用によりインターネット上にシステムを構築できるようになっています。このような背景から、インターネットに接続することを考慮した不適切な設定の検知や脆弱性対策といったセキュリティ強化も必須となっています。

④ 統合認証における対策

複数のSaaS／クラウドサービスの利用が進むとともにユーザーのID／パスワードも増加し、情報システム担当者もユーザーもその管理が大きな負担となっているだけでなく、情報漏えいの起点になってしまうケースも少なくありません。

表1 ゼロトラストの5つの領域と対応ソリューション

検討ポイント（課題）		対策ソリューション例
①エンドポイント	ベースとなる端末セキュリティの導入	EPP
	高度化された攻撃への対応	EDR
	社員の内部不正対策	MDM
②ネットワーク	安全かつ快適なアクセス環境の提供	SD-WAN
	トラフィック分散・帯域／VPN性能向上	ZTNA
	統一されたセキュリティポリシーの適用	SWG・ FWaaS・ CASB
③クラウド・ワークロード	クラウド（SaaS）統制	CSPM・ CWPP
	公開システム（IaaS/PaaS）セキュリティ強化	
④認証・認可	ID管理の自動化	IDM
	認証連携によるID利用の簡易化	IDP
⑤オペレーション	セキュリティ人材の確保	SOCアウトソース
	大量アラートへの迅速対応	SIEM・ UEBA・ SOAR

事実、従業員の異動や休職、退職のたびにIDを変更するのは煩雑な作業であり、これらをシンプルに統合、管理したいというニーズが増えています。

このような課題に対してユーザーの認証やアクセス制御を統合するシングルサインオン(SSO)などを活用し、ユーザーの利便性向上を実現する必要があります。さらに複数システムのユーザーIDやパスワード、アクセス制御といった情報を一元的に管理することで、システム管理者の負荷や運用コスト軽減が可能となります。

⑤ オペレーションにおける対策

これまで説明してきたような対策を実施していても、運用開始後に発生する大量のアラートへの対処や、各セキュリティツールから生成されるログの収集と相関分析が行えていなければ、インシデント発生時の事後対処も困難となってしまいます。その結果、セキュリティ被害の増大をもたらしてしまうケースも少なくありません。

そうした課題を解決するためには、常時リアルタイム監視(ログの収集・分析・検知など)といった適切なセキュリティ運用により、インシデント発生に際して迅速に対応していかなければなりません。

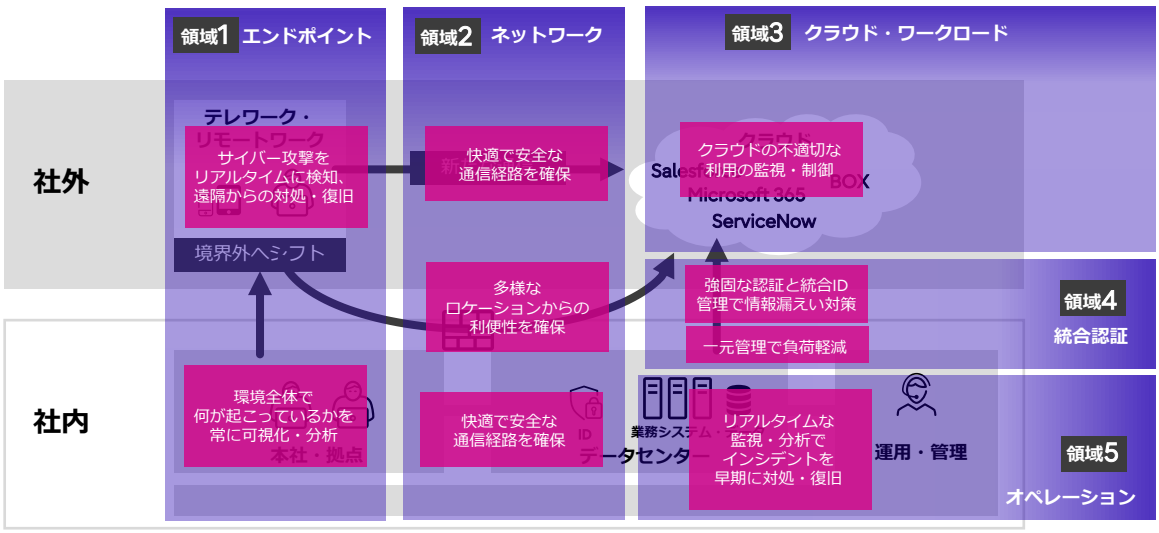
以上、課題解決型アプローチの推進で有効な考え方について、5つの領域ごとに解説してきました。富士通では、各領域における課題を解決するため、様々な対策ソリューションを提供しています(表1)。なお、本アプローチを選択する場合であっても将来像を見据えたソリューションの選定が必要となってきます。

事業の将来像を見据えた ゼロトラスト移行を行う全体最適型アプローチ

続いて、全体最適型アプローチについて解説していきます。全社内を対象としたゼロトラストへの移行には大規模なITシステムの変更が伴うため、経営層の投資判断を促したり、他部門のユーザーの理解を得たりする必要があります。そのためには、DXの推進やユーザーの利便性向上、運用の効率化といったメリットの訴求が不可欠です。それらの導入効果を提示した上で、IT 戦略としてのゼロトラストの実装、およびセキュリティ投資が必要であることを訴える必要があります。

独立行政法人 情報処理推進機構(IPA)をはじめとして、一般にゼロトラストの実装については、次のような手順による進め方が提案されています。まず初めに認証基盤の整備、続いて

図3 お客様が抱えるセキュリティの課題例



は、企業特有の課題に応じて「エンドポイント」「ネットワーク」「クラウド」の中から優先度を定めて導入を推進、最後に「統合運用」を整備するという進め方です。

ただし、ここで示した手順はあくまで概念であり、実導入を考えた際には必ずしもこの順番が最適とは言えないケースもあります。5つの領域において、既にソリューションが導入されているケースもあるでしょうし、そもそも課題の優先順位付け自体に悩まれるお客様も少なくありません。それぞれの企業が固有の課題を抱える中で、「IPAや富士通が推奨しているから」といった理由だけでは、大規模なITシステムの変更に対する承認を得ることは困難です。

これら5つの領域に対して、自社が抱える課題の優先度に応じながら、各領域に対応するソリューションを適切に導入していくには、どのような方策が必要となるのでしょうか。それは、将来的な企業の理想像を見据えたロードマップの策定です(図4)。

まずは現状の評価とあるべき姿を定義した後、課題の優先度やコストなどに基づき、ゼロトラストへの移行までの最適解を定めていくというものです。これらの過程を経て「IT戦略として投資する必要がある」と訴求するためのロードマップを策定する必要があります。

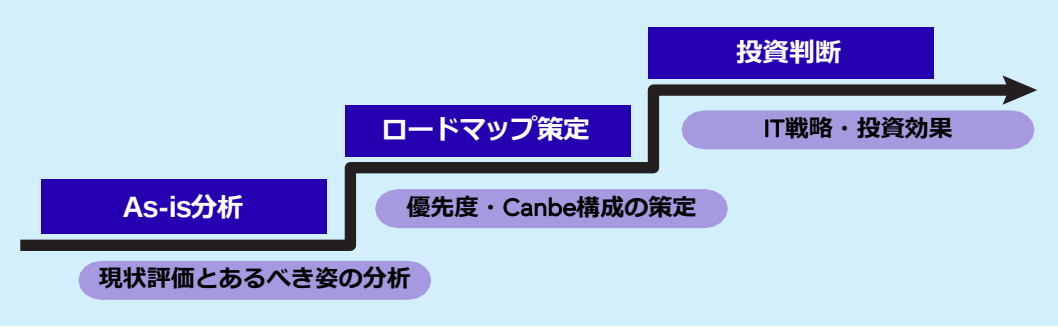
富士通ではこれらの取り組みを支援するため、「ゼロトラストロードマップ策定支援サービス」、および「ゼロトラストセキュリティ構築・運用サービス」を提供しています。

ゼロトラストロードマップ策定支援は、ゼロトラストをどのように進めたら良いのか悩んでいる企業に対して、自社の現状と課題を抽出した上で、移行計画や最適なロードマップの策定を支援するものです。具体的にはヒアリングやアンケートによる調査を行い現状と課題を洗い出した後、ゼロトラストの対応状況を評価し、ゼロトラストの成熟度を判定するとともに、移行計画やロードマップをアウトプットとして提供します。さらに企業ごとに異なる業務に基づいた投資効果についても協議を行い、ゼロトラスト推進のための予算確保や上申を支援します。無償による簡易的な調査から、本格的なゼロトラストへの移行を見据えた計画策定を支援する有償版まで、幅広いメニューを用意していることも特長です。

一方、ゼロトラストの実現に必要な対策の導入を全方位で支援するのが、ゼロトラストセキュリティ構築・運用サービスです。同サービスの最大のメリットは、5つの領域において設計・導入・運用を一気通貫でサポートできることにあります。策定されたロードマップをいざ実行しようとした際に、個々のソリューション導入を支援するベンダーが異なる場合には、コミュニケーションの齟齬が生じたり、相互連携が図れなかったりすることで、期待した通りに実装が進まないケースが少なくありません。対して、ゼロトラストセキュリティ構築・運用サービスは、富士通がソリューション全体の導入を一貫してサポートするので、安心してゼロトラスト環境へと移行可能です。さらに、自社ではカバーできない本番稼働後の運用支援を提供することも特長です。

以上、ゼロトラストの移行に向けた2つのアプローチについて解説してきました。富士通は企業がゼロトラストを実装していくにあたり、必要なソリューションを一気通貫で提供しています。また、自社内だけでは対応が困難な監視、運用管理といった仕組みについても様々なサービスを用意、ソリューション導入後の最適な運用体制の構築も支援できます。「課題解決型」「全体最適型」のいずれのアプローチを選択するにあたっても、サイバーセキュリティに関する数多くの経験とノウハウを有する富士通であれば、お客様にとって最適な支援を提供可能です。ゼロトラストへの移行にお悩みでしたら、ぜひ一度お声がけいただきたいと思います。

図4　全体最適型アプローチの推進には、お客様事業の将来像を描いてロードマップの策定が必要



[2023年掲載]

本記事中に記載の肩書きや数値、固有名詞等は掲載日現在のものであり、このページの閲覧時には変更されている可能性があることをご了承ください。

お問い合わせ先

製品・サービスについてのお問い合わせはコチラ
富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中4-1-1