7割の企業が進めるゼロトラスト、明らかになった課題とその対策とは？

先行事例に学ぶ
陥りやすい“ゼロトラ”3つの落とし穴

ADD VNTR.

Executive summary

01. 従来のセキュリティ対策が通用しないワケ

これまでのように社内ネットワークのみを境界防御で守っているだけでは、安全な環境とは言えない時代となっています。
攻撃者の侵入を前提にした対策や内部不正の脅威など、これまでとは抜本的に異なるセキュリティ対策のアプローチが求められています。

02. 先行する企業が足踏みする、ゼロトラスト実現に向けた3つの課題とその対策

ゼロトラスト実現に向けて先行する企業がはまる落とし穴は大きく3つ。
“ロードマップなき見切り発車”“ユーザビリティの落とし穴”“工数不足が招く運用不全”という先達からの学びを生かしましょう。

03. ゼロトラスト実現に向けたマクニカコンサルティング

マクニカコンサルティングの強みは、
将来を見据えたロードマップを設定したうえで利便性とセキュリティを両立させたゼロトラスト環境の実装が支援できることです。
課題の棚卸から実装に必要なコンポーネントの選定、そして現場への展開まで、ゼロトラスト実現に向けてトータルでサポートします。

01. 従来のセキュリティ対策が通用しないワケ

ビジネスのグローバル化が進むなか、クラウドサービスの利活用やテレワークを活用した働き方改革が加速し、従来とは異なるビジネス環境の整備が求められます。一方で、Emotet※やランサムウェア※など大手企業だけではなくあらゆる企業を狙った高度なセキュリティ攻撃が急増。労働力確保や生産性向上を進めつつ、新たな環境に適用できるセキュリティ対策の強化を早急に推し進めていかなければなりません。ただし、業務基盤のクラウド移行、自宅PCからのネットワーク接続など、守るべき資産が社内外に分散しており、これまでのような境界防御型の対策では対処できない状況にあります。攻撃者の侵入を前提にした対策や内部不正の脅威など、これまでとは抜本的に異なるセキュリティ対策のアプローチが今求められているのです。

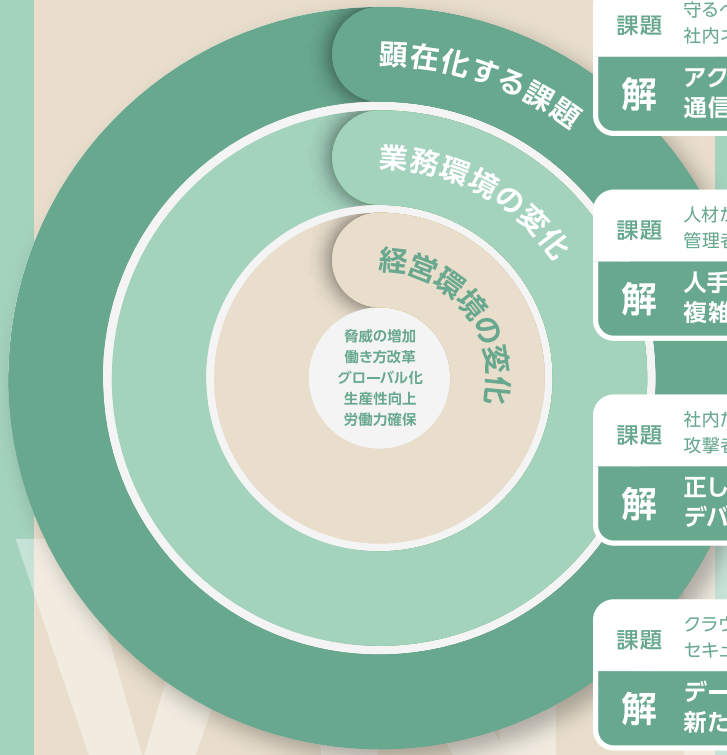
※Emotet：企業名や担当者を騙った不正なメールから感染を拡大させるマルウェア
※ランサムウェア：情報資産を暗号化して金銭を要求する攻撃の総称

ゼロトラストとは

そこで重要なキーワードとなっているのが、「決して信頼せず必ず確認せよ」というゼロトラストと呼ばれる考え方。アクセスするネットワークの場所に関わらず全ての通信を保護しながら、データやコンピュータへのアクセスはその都度許可を与えつつ、状況に応じて動的なポリシーを適用する。常に挙動を監視しながら継続的に確認していく仕組みづくりがゼロトラストには求められます。ゼロトラストは、NIST（米国国立標準技術研究所）においてゼロトラストに関するガイドライン※が提示されているほどで、今後のセキュリティを考えるうえでは必須の考え方となっています。顕在化している課題に対しては、ゼロトラストを前提にした考え方に切り替えていく必要があります。

※「NIST SP800-207 Zero Trust Architecture」：2020年8月11日にNIST（米国国立標準技術研究所）正式版発行したもの。
7つのゼロトラスト原則が示されており、米政府がゼロトラストについて言及する際に、政府標準として扱われるべく提言されています。

課題とそれに対するゼロトラストアプローチ



テレワークの拡大

課題　守るべき場所が多様化したことで、社内ネットワークを保護するだけでは安全が担保できない

解　アクセスしてきたネットワークからの通信かどうかだけで判断しない

人材の流動化

課題　人材が流動化し管理デバイスの増加も含め、管理者の作業工数が圧倒的に不足している

解　人手に頼った運用から脱却し、複雑な構成にも耐えうる運用改革を推進する

攻撃の高度化

課題　社内だから、社員だから安全という性善説での対策では、攻撃者や内部不正者の存在が見抜けない

解　正しいユーザなのか、認められたデバイスなのかといった信頼性で判断する

クラウドサービス活用

課題　クラウドの管理や攻撃前提の構成などセキュリティの視点を抜本的に見直す必要がある

解　データやデバイスそのものを守るという新たなセキュリティ思考を持つ

02. 先行する企業が足踏みする、ゼロトラスト実現に向けた3つの課題とその対策

多くの企業が取り組み始めているゼロトラストだけに、先行する企業においてはゼロトラストを展開する際の課題が顕在化しています。これらの課題を克服しない限り、ゼロトラストを現場に根付かせることが難しいのが現実です。

導入者観点

1つのソリューションで完結できない
“ロードマップなき見切り発車”
将来的なロードマップを見据えず、
目先の機能だけで選択したことが致命傷に！

利用者観点

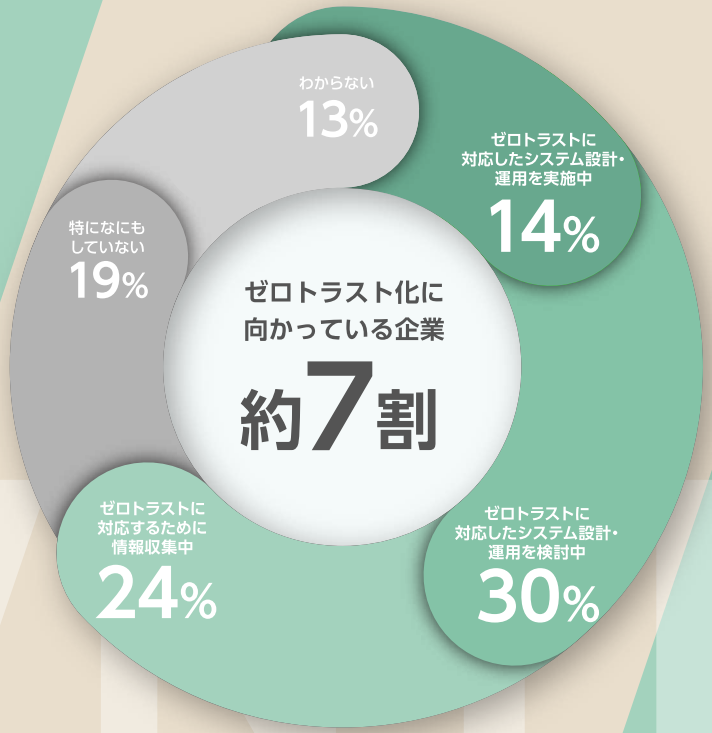
使い勝手を犠牲にするセキュリティ対策で混乱
“ユーザビリティの落とし穴”
セキュリティ強化で現場の業務を阻害、
現場からクレームが殺到！

運営者観点

管理者負担が増大、そもそも運用が回らない
“工数不足が招く運用不全”
境界の監視だけにとどまらず、
監視対象が拡大したことで管理者が疲弊

7割の企業が進めている“ゼロトラスト”アプローチの進捗状況

企業におけるインフラづくりにおいて大きな潮流となっているゼロトラスト。すでに多くの企業がゼロトラスト化に向けた環境整備を推し進めていることが明らかになっています。情報収集を進めている企業も含め、すでに7割の企業がゼロトラスト化に向けたアプローチを進めていること、ご存じですか。



出展
調査名：ゼロトラストセキュリティに関するアンケート／調査期間：2022/2/28～2022/3/10／実査機関：日経BPコンサルティング／調査手法：ネットリサーチ／有効回答数（回答者属性）：228件（「社内向け情報システムの構築・運用に関わる方」を対象とし、IT製品の導入・選定に関与している方を中心に調査を実施）

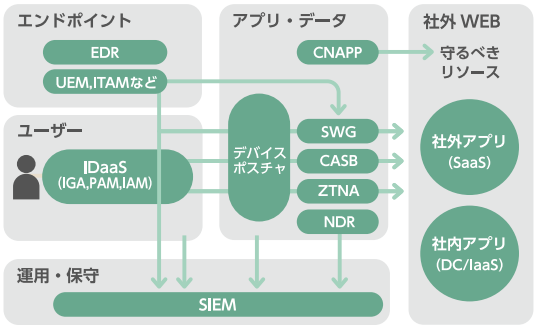
導入者観点

1つのソリューションで完結できない

“ロードマップなき見切り発車”

ゼロトラストは1つのソリューションを導入すれば完結するものではありません。図のように、ユーザーやエンドポイント、通信経路上のアプリやデータ、運用保守基盤に至るまで異なるソリューションを上手に組み合わせて環境づくりを進めていく必要があります。その際には、目先の機能だけに目を奪われることなく、将来的な全体像やロードマップを意識したうえでソリューションを選択していかなければなりません。最適な選択を行うためには、自社に適した全体像をうまく見定めてくれる、経験豊富なパートナーの力が強力な推進力となってきます。

ゼロトラスト実現に向けたコンポーネント群



ゼロトラスト実現に必要なコンポーネント、どこから手を付けていいのだろう…

自社にはどこまで必要？ 見極め方がわからない…

異なるベンダーのソリューション、どう組み合わせればいい？ 自分で検証できないけど…

多岐にわたるコンポーネントを最適かつ段階的に導入するための最適解を知るパートナーの力を利用せよ

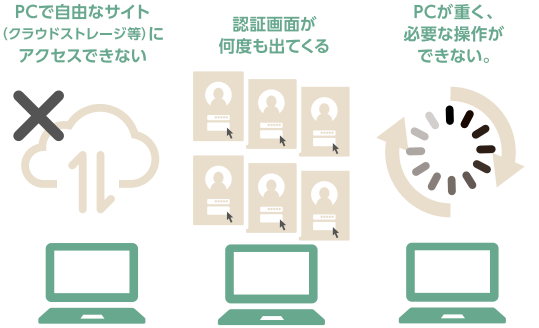
利用者観点

使い勝手を犠牲にするセキュリティ対策で混乱

“ユーザビリティの落とし穴”

二律背反として語られがちなセキュリティと使い勝手をうまく両立させない限り、現場からは総スカンを食らってしまい、プロジェクトが頓挫してしまうことも十分起こり得ます。SaaS利用を制限しながら顧客とのやり取りでうまくクラウド活用できる環境を用意する、仮想デスクトップ経由で悪化した画面のレスポンス解消に向けて通信経路を工夫するなど、現場の業務を阻害しない環境づくりに腐心することが何よりも重要です。

ゼロトラスト



これまで自由だったSaaSに利用制限が。いつもの機能が使えない、使いづらい。

認証許可でログインが複雑に。アクセスの仕方が分からず、仕事が始められない！

PCに様々なセキュリティソフトが導入。画面がなかなか開かず、メールもすぐに確認できない。

現場の業務を阻害することなく、使い勝手を犠牲にしないゼロトラストアプローチが成功の鍵となる

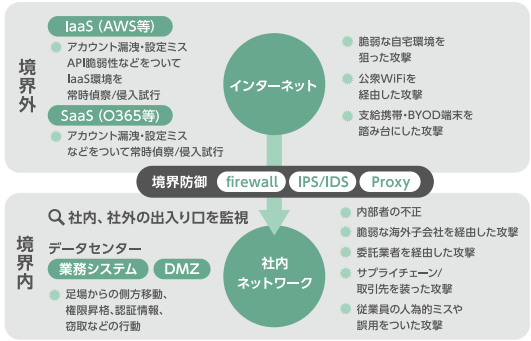
運営者観点

管理者負担が増大、そもそも運用が回らない

“工数不足が招く運用不全”

どれだけ優れたソリューションであっても、管理が複雑で運用が回らなければ意味がありません。自宅やクラウドも含めた多岐にわたる監視対象を効率的に管理できるよう、脅威の検知や通信ブロックなどの制御を自動化し、複雑なソリューションながら管理負担が軽減できる仕組みづくりがゼロトラスト成功の必須要件となってきます。

想定される脅威例



基幹システムのメンテナンス、ユーザー対応… セキュリティ以外の仕事が山積みなのに…

アラート件数が膨大、優先順位が付けられない！

脅威は検知はしたものの、通信遮断するなど 対策が後手に回ってしまう…

想定されるさまざまな脅威を自動検知、一元的に可視化、管理できる仕組みづくりが絶対条件に

03. ゼロトラスト実現に向けたマクニカコンサルティング

ゼロトラスト実現に向けたマクニカのアプローチ

導入者観点

多岐にわたるコンポーネントを
最適かつ段階的に
導入するための最適解を知る
パートナーの力を利用せよ

1次代理店として
さまざまな製品を販売、
構築することで培った
製品知見をフル活用、
異なるベンダーの製品を
柔軟に連携させながら、
統合的なシステム設計が可能

利用者観点

現場の業務を阻害することなく、
使い勝手を犠牲にしない
ゼロトラストアプローチが
成功の鍵となる

プリセールスや年間数千件の
サポート問い合わせから得られた
ユーザーの声を熟知した
コンサルタントだからこそ、
使い勝手に配慮した
ゼロトラストコンサルティングを実現

運営者観点

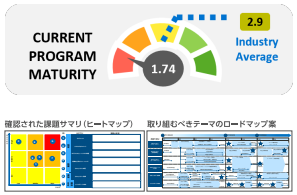
想定されるさまざまな脅威を
自動検知、一元的に可視化、
管理できる仕組みづくりが
絶対条件に

製品を知り尽くす
1次代理店だからこそ
運用の勘所を理解、
細かなアラート対応はもちろん、
ゼロトララボで培った
情報収集箇所と対処箇所との
連携のノウハウを実運用に適用可能

ゼロトラスト実現に向けたマクニカコンサルティングの力

マクニカコンサルティングの強みは、将来を見据えたロードマップを設定したうえで利便性とセキュリティを両立させたゼロトラスト環境の実装が支援できることです。現場の課題をしっかりと棚卸したうえで、国際標準のガイドラインや独自ノウハウを交えたアセスメントを実施、ゼロトラスト実現に向けた最新のコンポーネントを最適な形に組み合わせながら、顧客の実態に即したゼロトラスト環境の整備から運用支援までをサポートします。

現状把握から実装まで、3フェーズでゼロトラスト実現をトータルで支援

	約2〜3ヶ月 Assessment phase	約3〜6ヶ月 Design phase	約3〜6ヶ月 Implement phase
実施内容	アセスメントからロードマップの策定 ●理想像策定 /現状分析 ●実施優先順位付け ●実行計画策定  	開発/運用設計/ベンダー選定/実装 ●PROJECTの体制構築 ●要件定義（RFP） ●製品選定（POC含む） 	製品の導入支援/運用サービス ●プロダクトチームによる展開支援 ●設定のチューニング支援 ●運用支援サービス okta netskope splunk> CROWDSTRIKE Skyhigh Security S&J
アウトカム	自社の現状と課題、改善施策が明確化されており、施策の実行ロードマップが計画されている状態	改善施策を実行するための組織や具体的なシステム（製品）が決定された状態	製品が導入され、ゼロトラスト運用が円滑に実行されている状態

ゼロトラスト実現を支援するコンサルタント

セキュリティと使い勝手を両立させながら、実装まで継続支援するゼロトラストコンサルティング

脅威の高度化に伴って、多くの企業がゼロトラストへの歩みを進めています。複雑なコンポーネントを組み合わせながら、お客さまにとって理想的なセキュリティ環境を提供し、利便性低下を最小限にとどめるべく、これまでの知見を活かした提案を行います。海外の先行事例も踏まえた現実的なゼロトラスト実装に向け、お客さまの環境づくりをバックアップします。

小林 真也
Shinya Kobayashi

株式会社マクニカ DXコンサルティング室
テクニカルコンサルタント

マクニカに入社後、VPN機器の販売や導入業務に従事。国内最大規模の導入実績を持つ。2020年ごろのゼロトラストが世間で話題になり始めた当初からリモートアクセスの現場経験を活かし活動の幅を広げる。2021年からコンサル業務を兼務し、お客様先に出向きゼロトラ化推進に向けた、支援を実施している。

まずはお気軽にご相談ください。メールからのお問い合わせはこちら add-venture@macnica.co.jp