ホワイトペーパー

企業競争力を高める

ビジネスイネーブラーとしての「ゼロトラスト」

CISOに必要な「ビジネスありきで考えるセキュリティ」視点

©2022 Zscaler, Inc. All rights reserved.

コストセンターと見られがちな情報セキュリティ領域だが、DXと働き方改革が同時進行するいま、企業間競争力・国際競争力を維持発展させるために不可欠で重要な要素として改めてクローズアップされている。20年以上にわたりサイバーセキュリティの最前線で取り組んできた深谷　玄右（ふかたに　ひろあき）氏（ゼットスケーラー株式会社CISO）が、新時代の企業情報セキュリティインフラの望ましい在り方を語った。

©2022 Zscaler, Inc. All rights reserved.

日々進化、セキュリティ対策をすり抜けるサイバー攻撃

個人情報保護法施行（2003年）以来、企業・団体の情報セキュリティ対策は格段に前進したかに見える。しかし、現実のサイバー攻撃は継続して進化しており、最新のセキュリティ対策をすり抜けて被害件数、被害規模とも上昇しているのが実態である。

国内でのサイバー犯罪検挙件数は右肩上がりに増加中※で、近年のランサムウエア攻撃による国内の大手メーカー、病院などの事業一時停止は記憶に新しい。また、米国では石油パイプラインの操業が一時停止するなど、極めて深刻なケースが頻発している。

日本企業が抱えるセキュリティ対策の問題点

日々脅威を増すサイバー攻撃に対策するために、企業の情報システム部門・情報セキュリティ部門はこれまで多大なコストをかけて数々のセキュリティ機器とサービスを導入・運用してきた。しかし、万全の対策を講じていると思われた大手企業やセキュリティ業者までもがサイバー攻撃の被害を受けている現状を見ると、従来のセキュリティ対策の考え方そのものに課題があると言わざるを得ない。

現行のセキュリティ対策の問題点として、深谷氏は3つの根本的課題を指摘する。

ゼットスケーラー株式会社
CISO（最高情報セキュリティ責任者）
ふかたに　ひろあき
深谷 玄右氏

ITセキュリティのサービスプロバイダー、生命保険会社等において20年以上にわたって培ったサイバーセキュリティの知見、元Zscalerユーザーだった経験を生かし、セキュリティ関連の啓蒙活動に取り組む。

1つ目の課題は「パッチワークのように構成されたセキュリティ」である。個々のセキュリティ対策はその時点での攻撃トレンドに最適化されているが、度重なる対策が施されることでセキュリティシステム全体がパッチワークのように複雑化し、整合性を取りにくくなっている状態である。

2つ目の課題は「セキュリティ運用管理の専門人員の不足」である。セキュリティ対策の実効性を保つには、全ての機器を適切に設定し、アップデートやシグネチャ更新などのメンテナンスが常に欠かせない。また、機器からのセキュリティアラートを迅速に処理する必要がある。主にセキュリティ担当者が運用・管理を担っているが、そもそも専門人材が少なく、また、日本では部署・職掌のローテーションにより個人の経験がセキュリティ部門の知見として根付かないことも多い。一方でセキュリティ運用は年々複雑化し、それに対応する標準運用手順マニュアルは追加される。これらの負担を軽減すべくアウトソーシングする企業も多いが、新たな脅威が生じ対策を打つ度に運用コストが跳ね上がる。しかも、自社でのノウハウ蓄積が困難になり、ベンダーの協力なしに運用できない事態も生じている。

3つ目の課題として「クラウドを安全に活用するためのノウハウ不足」が挙げられる。近年、クラウドサービスの利活用が増加したことで、新たなセキュリティリスクが懸念されている。クラウドサービスの多くは各種セキュリティ標準に準拠した機能を備えているが、それを使いこなすには適切な設定と利用者管理、システム環境や業務プロセスの変化に応じた適切な設定変更が欠かせない。複数のSaaSと社内システムを連携させているようなケースでは管理が行き届かず、気付かぬうちにセキュリティホールが生じるリスクも否定できない。

※2022年警察庁発表
（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf）

©2022 Zscaler, Inc. All rights reserved.

「ゼロトラスト」の認知拡大とゼットスケーラーの仕組み

このような課題を抱えつつ、最新のサイバー攻撃から組織を保護するために、最も有効な対策と目されているのが「ゼロトラスト」だ。ゼロトラストとは、インターネットはもとより組織内部のネットワークも、ユーザーも、クライアント端末も、一切信頼しないことを原則とするセキュリティの考え方である。脅威が潜んでいる前提で全ての通信を検査し、安全と判断できる通信だけをユーザー・アプリ間、あるいはアプリ・アプリ間で交換できるようにするのがゼロトラストの基本である。

昨今では「情報インフラのゼロトラスト化」が有効なサイバー攻撃対策であるとの認識が広がっている。日本のデジタル庁も政府情報ネットワークへの適用を推奨しているように、もはやゼロトラストの適用を検討する段階は終わり、いつ適用を開始するかの議論へ移行しているのが国内および世界の動向である。

ただしゼロトラスト実現のための考え方は多様で、ソリューションも特定のものに限定されない。例えば、セキュリティ機器やソフトウエアをネットワーク内の必要箇所に配置し、統合的な運用管理を常時実行する方法もある。しかし、国内外に多くの拠点を持ち、多数の従業員のテレワークを実施する企業では、機器導入と運用管理に莫大なコストが掛かるだろう。

その対極にあるソリューションが、ゼロトラストクラウドプラットフォームである。ゼットスケーラーの「Zero Trust Exchange」の場合、組織の通信トラフィックをクラウドプラットフォームに引き込み、適切に配分されたユーザー権限に基づき、在宅勤務などのリモートユーザーとアプリ間（データセンター内のアプリ、社内設置システムのアプリ、外部のSaaSなど）との間にマイクロトンネル（マイクロセグメンテーション）を作り、外部からの盗聴や改ざんができない通信路を形成する。これは「攻撃対象領域（攻撃表面 ／ Attack Surface）を縮小する」というサイバー攻撃対策の基本を確実に実現することになる。

また、プラットフォーム経由の通信中にマルウエアなどの脅威が隠されていないか、あるいは外部に流出するとリスクが高い機密情報が含まれていないかといった検査もなされる（脅威スキャン機能、DLP機能）。SSL/TLS暗号化されたWeb通信であっても同様だ。暗号化された通信を含めたトラフィックの全数検査は、従来のオンプレミスのセキュリティ構成（ファイアウォール、URLフィルター、アンチウイルス、サンドボックスその他）や、それをそのままクラウドに移動させた構成では性能・コスト・運用管理負荷の問題で困難だった。それをゼットスケーラーでは、クラウドプラットフォームならではの柔軟なスケーラビリティと、ゼットスケーラーが特許を持つ独自の並列スキャン技術により解決している。

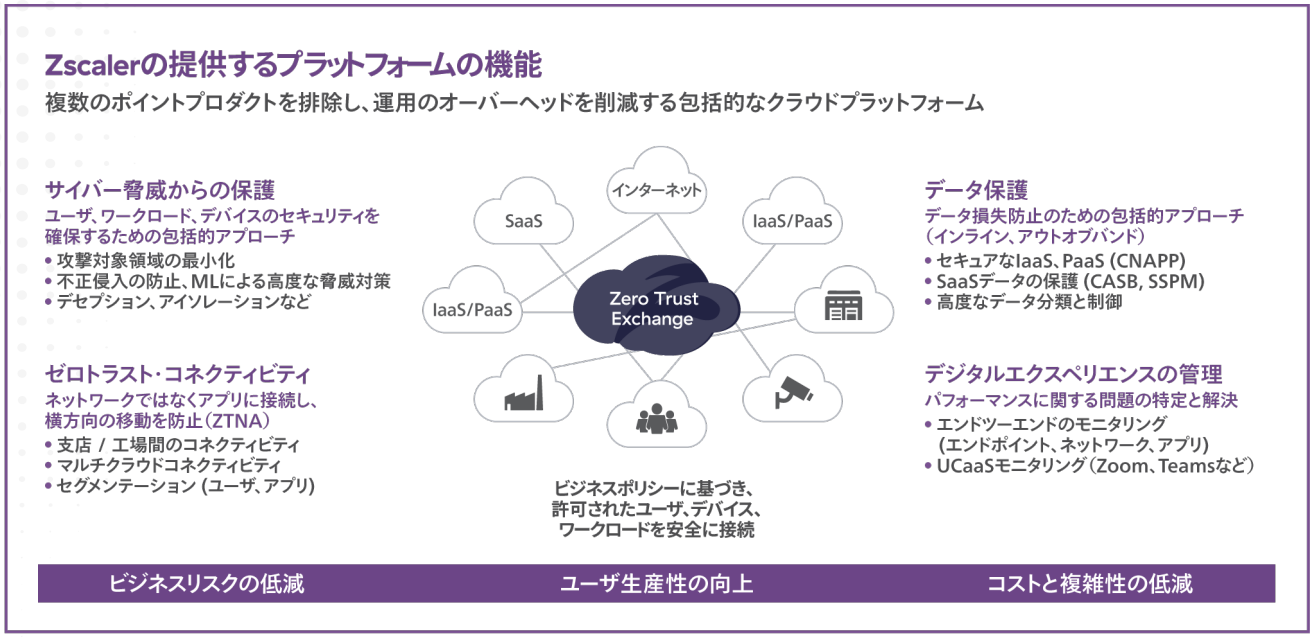
こうした仕組みにより、組織ネットワークに侵入したマルウエアがあったとしても、ネットワーク内の横移動（ラテラルムーブメント）で感染を拡大する常套手段を封じることができる。加えて、最新のデセプションテクノロジーを活用し「おとり」のシステムに攻撃を導くことで、侵入活動の発生を早期に突き止め、排除することも可能になる。

CISOの視点からみたゼロトラストの有効性

このようにゼロトラストクラウドプラットフォームを活用することは「セキュリティをコストセンター（利益を生まずコストとなる部門）からビジネスイネーブラー（ビジネス成長のための手段）へと進化させる手段となります」と深谷氏は強調し、次のように語った。

「情報システムのクラウド化は、企業の競争力確保のためにも不可欠な要素です。また、コロナ禍後もリモートワークの継続が予想されます。組織ネットワークの出入口はこれからも増えていくばかり。安全のために

©2022 Zscaler, Inc. All rights reserved.



サイバー攻撃に対抗するZscalerのゼロトラストクラウドプラットフォーム

システムの出入り口を塞ぎ、ユーザーに厳密なルール遵守を求めて利便性を損なうセキュリティ対策は、すでに時代遅れです。

ゼロトラストクラウドプラットフォームを活用することで、クラウドやリモートワークを安全に利用しつつ業務効率化や生産性向上を図れます。一方で新サービス・新システムの開発・提供においてもクラウドファーストを基本にするのが現在のトレンドです。IaaS/PaaSを利用しながら、開発から運用までセキュリティを一貫して担保できるゼロトラストプラットフォームは、新規ビジネスの迅速な展開にも寄与することでしょう」

また、ゼロトラストは、セキュリティ面において、自由な事業展開を進めるときに道を外さないようにする「ガードレール」のように機能するとした上で「CISOやセキュリティを統括する立場の人は、経営が向かおうとする方向を理解し、何を解決し、将来どのような姿になりたいかという目的を明確にした上で、経営層を巻き込んでゼロトラスト化を推進していくべきです。ゼロトラスト構築を目的とするのではなく、あくまでも企業目標に向けてそれに伴うリスクを理解し、リスクを許容できる範囲に収めて事業展開をスムーズにできるようにゼロトラスト化を推進していく必要があります。また、ゼロトラストの考え方や進め方はDXの進め方と親和性が高いため、DX戦略に組み込んで一体として推進すべきです」と語った。

リモートワークのコスト削減効果も期待

深谷氏は身近な一例を挙げた。リモートワーク社員がシンクライアント端末とVPNで社内システムにアクセスする場合、端末起動、ログイン、VPN起動・認証、シンクライアント起動・認証、仮想デスクトップ起動といった手順を踏むため、少なくとも数分を要する。仮に従業員の時間単価が2500円、リモート勤務者が100人/日、VPNとシンクライアント側の起動に要する待機時間が3分/回だとすると、1日1万2500円、年間275万円を費やしていることになる（年間220日勤務の場合）。実際には、端末がスリープモードに入ったり、日中に移動したりすることでネットワーク接続が途切れ、VPNの再接続が必要になることもあるため、待機

©2022 Zscaler, Inc. All rights reserved.

時間はもう少し増えるだろう。また、「シンクライアントの画面の応答がなくなることも多く、ストレスを感じることが多かった」と深谷氏。

しかし、Zero Trust Exchangeなら、端末ログイン後はVPN起動以降の手順が不要なため、待機時間と損失金額を削減することができる。従業員のストレス軽減効果も大きいだろう。

この他にも全社規模でのコストを考えると見過ごせないIT利用領域が潜んでいる可能性があり、Zero Trust Exchangeはそれら損失の削減効果も期待できる。

ゼロトラストのROIの考え方は?

システムの運用管理負荷や機器購入・メンテナンスコストばかりでなく、業務部門全体のIT利用を効率化することも含めて、ROI（投資対効果）を計算することも重要だ。もっともROIの算出はそれほど容易ではない。将来起きる可能性があるサイバー攻撃被害による損失や、知財の流出に伴う損失、将来のビジネスに影響あるブランドを毀損する損失なども含め、ゼロトラスト導入・運用コストを算出しなければならないからだ。

ゼットスケーラーでは投資効果の整理、移行プランの策定、技術優位性の検証（PoV）もサポートしており、ROIを検討した上で導入計画を練ることができる。事前に得られる情報は、企業の意思決定を進めるのにも役立つだろう。

ゼロトラストプラットフォームの8つのチェックポイント

現在、各社からさまざまなゼロトラストプラットフォームが提供されている。外見上はゼロトラストを実現する製品・サービスであり機能的には同じに見えるため、付加機能の差異で選びそうになるが、製品のコンセプトや内部の構成が異なると実際に得られる効果が異なる。より自社に適切で、信頼性の高いものを選択するポイントとして、深谷氏は8つの項目を挙げた。

1. パフォーマンスや可用性に拡張性が十分あり、グローバルなプラットフォームの運用実績があるか
2. 正しいゼロトラストアーキテクチャに基づく構成か
3. 脅威防御・データ漏えい防止（DLP）に必要なSSL/TLS通信を全数検査するキャパシティーがあるか
4. 自社に最適な展開、管理をできる柔軟性、拡張性、多用性があるか
5. アプリケーションへの接続経路の最適化ができるか
6. ユーザー体験（UX）低下の検出・原因特定を迅速に行い、ユーザーのロスタイムを最小限に抑えられるか
7. サードパーティー製品との深い連携があり、必要な自動処理が可能か
8. SSE（セキュリティサービスエッジ）ソリューションのアーキテクチャはシンプルで、パイロット（実展開に向けての評価のため、先行して小規模に導入すること）での価値確認がしやすいか

電源投入時、スタンバイからの復帰時	
Zscaler	VPN
●電源を投入し、ログイン画面が表示されるのを待つ ●Windowsにログイン ●アプリケーションを起動する	●電源を投入し、ログイン画面が表示されるのを待つ ●Windowsにログイン **●VPNクライアントを立ち上げる** **●VPNクライアントにID、パスワード、ワンタイムトークンを入力する** **●シンクライアントのクライアントアプリケーションを起動し、サーバにログイン** **●サーバ側で、仮想デスクトップが起動するのを待つ** ●アプリケーションを起動する

Zero Trust Exchangeを利用する場合とVPN+シンクライアントの手順比較

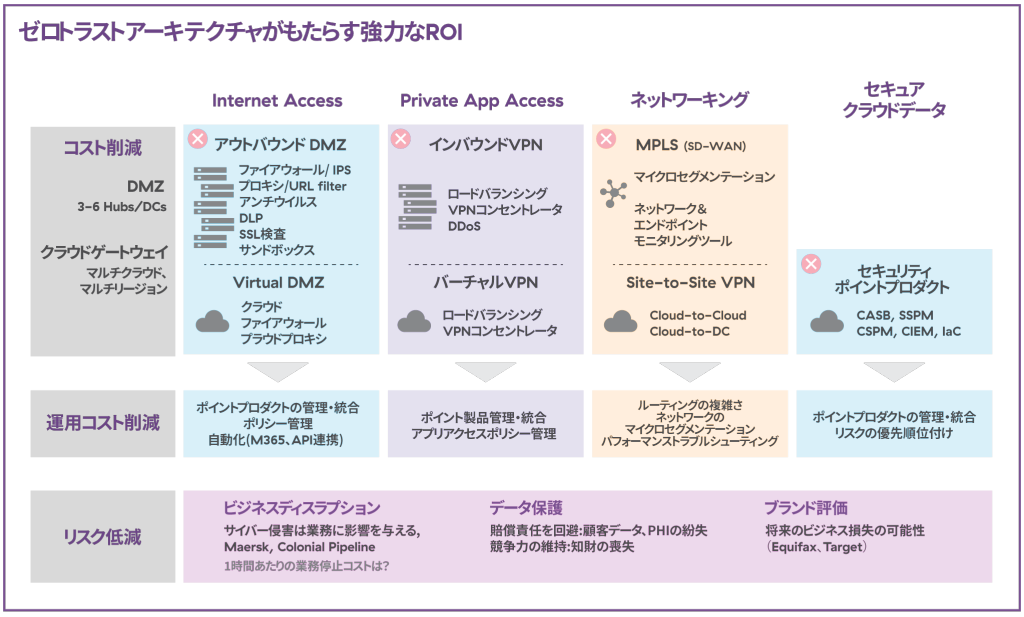
©2022 Zscaler, Inc. All rights reserved.

ゼットスケーラーには、世界6000社以上の顧客との運用実績があり、NPS（ネットプロモータースコア・顧客ロイヤルティや顧客の継続利用意向を測定するための指標）はSaaSサービスの平均値の倍以上の評価を得ている。また1日2400億トラフィックを処理し、毎日70億の脅威検出・ブロックに成功。データセンターは世界に150拠点以上あり、独自のアーキテクチャによりさらなるスケールが可能というキャパシティーと性能を備える。

また、外部の主要なクラウドサービスとの高速回線でのピアリングや機能連携など、パートナーシップも充実している。それぞれの強みを生かし相互補完するエコシステムにより、低コストで柔軟な構成を可能としており、サービス間の連携による自動処理も容易に実現できる。

さらに機密性が非常に高い情報を取り扱うなどでクラウドに接続できない場合に向けて、自社ネットワーク内に「Private Service Edge」を設置することで、クラウドを経由させずに運用可能な構成がとれるなど、導入先の事情やBCP上の必要性に基づく最適な構成も可能にしている。その他、ユーザーのUX改善や非稼働時間を減らすことを可能にする、端末およびアプリケーションの通信状況や稼働状況の常時監視・可視化もできる点に注目すべきだろう。

最後に深谷氏は「セキュリティはビジネスありきで考えるべきもの。ゼットスケーラーはビジネスリスクを低減するばかりでなく、ユーザーの生産性を向上させ、コスト増大を抑えるソリューションを提供しています。セキュリティが事業の足かせになる場面を、私自身がユーザー企業で何度も経験してきました」と明かし、「だからこそ、ゼットスケーラーにはそれを逆転させる可能性を感じています。ゼロトラストクラウドプラットフォームの中でもクラウドネイティブなZero Trust Exchangeは、企業のDX推進にも必ず貢献するものだと思います」と述べた。



ゼロトラストのROI算出要素の一例

zscaler™ | Experience your world, secured.™

Zscalerについて

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタルトランスフォーメーションを加速しています。Zscaler Zero Trust Exchangeは、ユーザ、デバイス、アプリケーションをどこからでも安全に接続させることで、何千人ものお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータセンタに分散されたSASEベースのZero Trust Exchangeは、世界最大のインライン型クラウドセキュリティプラットフォームです。詳細は、**zscaler.jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

©2022 Zscaler, Inc. All rights reserved.
Zscaler™およびzscaler.jp/legal/trademarksに記載されたその他の商標は、米国および/または各国のZscaler, Inc.における (i) 登録商標またはサービスマーク、(ii) 商標またはサービスマークです。その他の商標はすべて、それぞれの所有者に帰属します。

03-4243-6320 Zscaler, Inc.(本社) – 120 Holger Way – San Jose, CA 95134 zscaler.jp