zscaler™

デジタルテクノロジー株式会社

「脱VPN」でハイブリッドワークを！
これを可能にする「Zscaler」

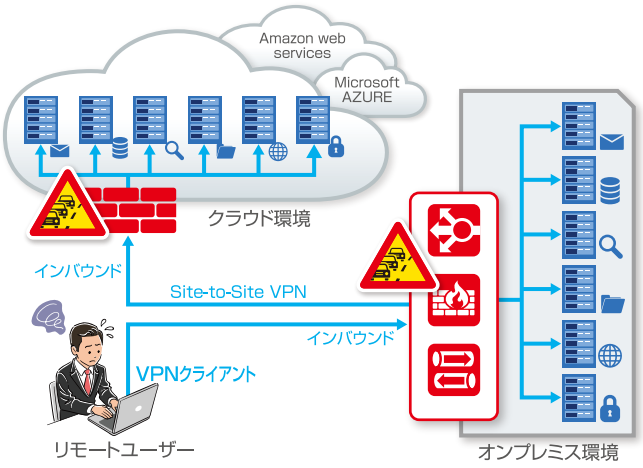
新型コロナウイルス感染症拡大で、日本でも一気に広がったテレワーク。
在宅勤務従業員が社内システムにアクセスするため、
VPNの増強を行った企業も多かったはずです。
またこの数年はSaaSの利用も増えており、その安全性確保のために
社内ネットワークを経由して、SaaSにアクセスする形態も一般的に。
しかしこのようなネットワーク構成は、新たな課題を生み出しています。

課題1

VPN機器への過大な負荷で ユーザーの利用環境が悪化

SaaSを安全に使うため、多くの企業ではSaaSへのアクセスをいったん社内ネットワークで受け、そこで必要な監視・制御を行った上で、SaaSにつなぐという仕組みを採用しています。しかしこの方法では、社内ネットワークに多大な負荷がかかり、社外からのアクセスを引き受けるVPN機器の負荷も増大します。このような機器を今後も継続的に設置・更新し続けるのは、大きな運用コスト負担になります。また社内ネットワークのトラフィックが高止まりしているようでは、ユーザーが快適に使うことも困難です。

- インバウンド通信を許可するセキュリティリスク
- 専用機器の導入コストおよび運用負荷
- プライベートクラウド移行時の対応が複雑

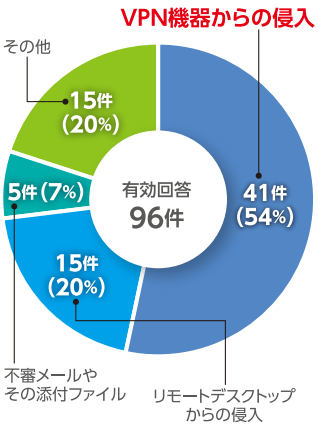


課題2

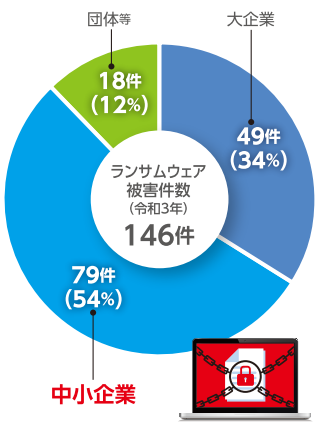
VPN機器の脆弱性が ランサムウェア攻撃の温床に

VPN機器はランサムウェア攻撃の主要な攻撃ポイントにもなっています。警察庁によれば、日本で報告されたランサムウェア被害のうち、54%はVPN機器からの侵入だと指摘されています※。VPN機器の脆弱性は、ネットワーク管理者が意識的に管理しなければなりませんが、中堅・中小企業ではネットワーク技術者が不足しており、このような対応が難しい状況です。しかも日本で報告されたランサムウェア被害のうち、半数以上は中小企業で発生しているのです。

感染経路



ランサムウェア被害の 被害企業・団体等の規模報告件数



注　図中の割合は小数点第一位以下を四捨五入しているため、総計が必ずしも100にはならない。

※ 警察庁「令和3年におけるサイバー空間をめぐる脅威の情勢等について」2022年4月
(https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei.pdf)

中堅・中小企業でもハイブリッドワークが広がりつつある現在、この2つの課題をどのようにして解決すればいいのでしょうか。

有効な解決策は「Zscaler」の活用です。
脱VPNと安全なSaaSアクセスを可能にします。

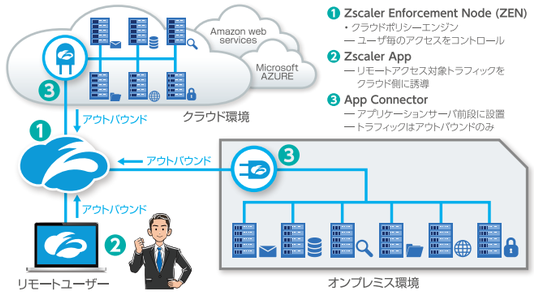
全世界に配置された「Zscaler Zero Trust Exchange」によって、オンプレミスとクラウドの両方をカバーした、多岐にわたるセキュリティ機能を提供。ハイブリッドワークが当たり前の時代における企業システム全体の安全性を、簡単に高めることができます。中堅・中小企業の皆様にまずご活用いただきたいのが、「ZPA」※と「ZIA」※です。

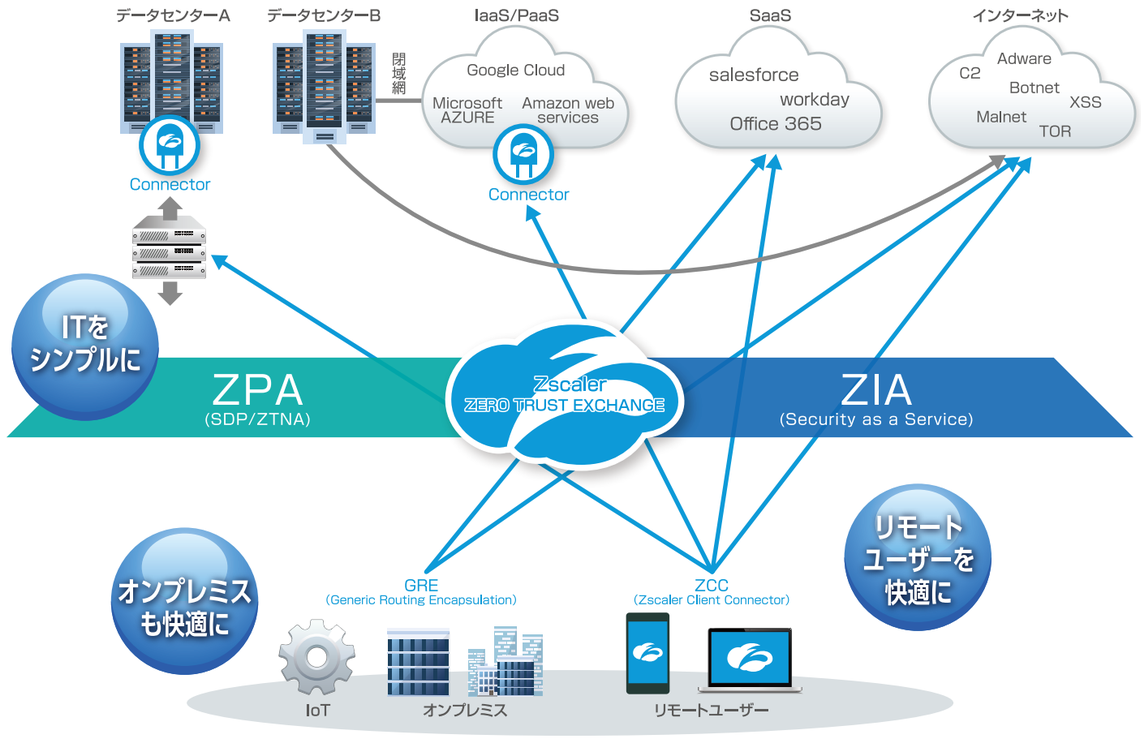
※**ZPA**：Zscaler Private Access　※**ZIA**：Zscaler Internet Access

脱VPNを可能にする ZPA

ZPAは、社外からオンプレミスシステムへのリモート接続を、セキュアかつ快適にするサービスです。リモートユーザーからのアクセスをまずZscalerのクラウドサービス「ZEN」※へと誘導し、ここでセキュリティポリシーに従ってユーザー毎のアクセスをコントロール。ここからオンプレミスシステムとSaaSに対して、直接トラフィックを引き渡します。SaaSへのアクセスの際にオンプレミスシステムを経由する必要がないため、オンプレミスへのトラフィック集中を回避可能。アプリケーションの前段には「App Connector」を設置しZENと暗号化通信を行うため、VPN機器も不要になります。

※**ZEN**：Zscaler Enforcement Node

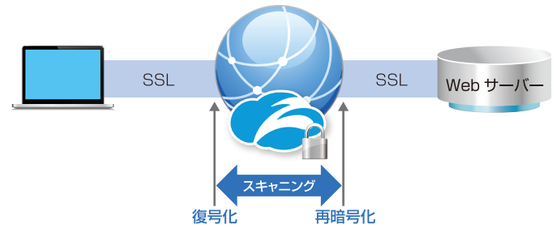




インターネット接続の安全性を極限まで高める ZIA

ZIAは、ユーザーがインターネットに接続する際に、高い安全性を提供できるクラウドプロキシーです。SSMA™と呼ばれる独自の並列スキャン技術により、インターネット上でやり取りされるデータを高速に処理して、セキュリティ上のリスクを排除。数多くのクラウドサービスと直接接続しているため、これを低遅延で行えます。HTTPSで保護された通信も、クラウド上で処理をすることにより高速に処理が可能。見えない攻撃も、見逃すことなく検出できます。

※**SSMA™**：Single Scan Multiple Analysis



ZPAを活用することで、以下のことが可能になります

ユーザーと利用アプリケーションの可視化

アプリケーションにアクセスしたユーザーの情報、アクセス先のアプリケーションやノードの情報、セッションの開始・終了時間、適用されたポリシーの情報など、アクセス情報をきめ細かくログに記録。これをドリルダウンしていくことで、詳細情報まで可視化できます。

アプリケーションアクセスの常時監視と詳細な制御

ユーザーからアプリケーションへのアクセスは常に監視されており、ユーザー /グループごとにアクセス先を詳細にコントロール。有効かつ認証されたユーザーだけが、アプリケーションにアクセスできることを保証します。

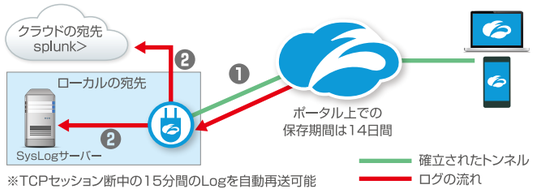
ZPAによるラテラルムーブメント※の抑制

多くのマルウェアはいったんシステムに侵入した後、ラテラルムーブメントによって感染を拡大します。しかしZPAは、暗号化された通信でユーザーとアプリケーションを接続することで、感染の拡大を抑制できます。

※**ラテラルムーブメント**：感染したマルウェアが、システム内の他の領域にも感染を拡大すること。

ログのリアルタイム転送

ZPAは詳細なアクセスログをクラウド上に残すだけではなく、そのデータをリアルタイムにオンプレミスにストリーミングすることが可能です。必要なのは受信可能なTCPポートを用意するだけ。社内のsyslogサーバーなどでログを分析できます。



※TCPセッション断中の15分間のLogを自動再送可能

ZIAは以下の機能を提供しています

URL/コンテンツフィルタリング

ユーザーがアクセスしようとしているURLやコンテンツの安全性を評価し、危険だと判断されるものをフィルタリング。マルウェア感染のリスクを回避します。

クラウドサンドボックス

マルウェアか否か判断できない不明なファイルは、クラウド上のサンドボックスで分析します。これによって未知のマルウェアの被害も防止できます。

トラフィックの帯域制御

ビジネスニーズに合わせ、アプリケーション毎の通信帯域を制御できます。これによってより快適な利用が可能になります。

インライン型アンチマルウェア

インターネット側から送られてきたコンテンツの内容をリアルタイムでスキャニングし、ウィルスやスパイウェアがユーザー端末に到達しないようにします。

クラウドファイアウォール/IPS※

ファイアウォールやIPSの機能をクラウドで提供。リアルタイムで詳細な可視化と制御を行います。　※**IPS**：Intrusion Prevention System。不正侵入防止システム。

情報漏洩の防止

セキュリティポリシーに従い、ファイルタイプ別にアップロード/ダウンロードの制御が行なえます。また機械学習を活用した、コンテンツ内容をスキャンした上での制御も可能です。

デジタルテクノロジーが 脱VPNのために「Zscaler」をおすすめする理由

このようにZPAとZIAを活用することで、脱VPNが可能になります。これに加えてZscalerには、次のような特長があります。

グローバルでの高いサービス実績

Zscalerは2008年からサービスを展開しており、現在では1日あたり2,100億トランザクションを処理しています。展開しているデータセンター数は、6大陸で150カ所以上。これだけの規模でサービスを提供している企業は他にありません。また可用性・安定性もSLAにもとづいて定義されており、サービス停止や遅延が発生した場合の対応についても明確化されています。

※**SLA**：Service Level Agreement。サービス提供者と顧客との間で結ばれる、可用性などのサービスレベルに関する合意や契約。

監視が容易で運用負荷も軽減可能

Zscalerを活用することで、どのユーザーがどのアプリケーションにアクセスしているか、リアルタイムのトラフィックがどのような状況なのかなど、システムの利用状況を監視・可視化しやすくなります。これによって運用負荷が軽減され、「一人情シス」になりがちな中堅・中小企業でも、セキュリティの確保が容易になります。

Zscalerのセキュリティサービス

Zscaler
統合された4つのサービスを提供

ZPA
Zscaler Private Access

VPNを伴わない
リモートアクセスオフィスから
データセンターまでの
ゼロトラスト

安全な企業アプリへのアクセス
ユーザーから企業アプリまで

ZIA
Zscaler Internet Access

サイバー脅威の検出
データ保護(DLP/CASB)
ローカルブレイクアウト
(O365/SD-WAN)

安全なインターネットアクセス
ユーザーからインターネット

ユーザー体感の可視化
ユーザーからアプリまでの
通信品質

ユーザー、アプリ、場所に紐づく
DXスコアでユーザーの体感を
定常的に監視・可視化

ZDX
Zscaler Digital Experience

アプリとワークロードの保護
アプリ間の通信

アプリケーションの
マイクロセグメンテーション
設定ミスや規約違反の
自動修正(CSPM)

ZCP
Zscaler Cloud Protection

グローバル展開 :150 data centers(SASE)
AI / ML Powered | PolicyNow™ | NanoLog™ | Extensible

Zscalerの導入・活用は デジタルテクノロジーにご相談ください。

デジタルテクノロジーは、脱VPN・脱リモートデスクトップをはじめとしたテレワーク見直しや、ハイブリッドクラウドの構築・運用などをお手伝いします。これらソリューションの検討段階におけるコンサルティングから、初期導入に必要な各種作業、運用フェーズにおける監視・設定に至るまでを一貫して支援。またハイブリッドクラウドの運用や、オンプレミスからクラウドへの移行などをご支援する「D-Cloud」サービスもご用意しています。Zscalerの導入・活用はもちろんのこと、DXやIT運用にかかわるお悩みは、ぜひデジタルテクノロジーにご相談ください。

デジタルテクノロジー株式会社

https://www.dtc.co.jp/

[東京] 〒104-0032 東京都中央区八丁堀 2-23-1 エンパイヤビル
MAIL：sales@dtc.co.jp

[大阪] 〒530-0001 大阪市北区梅田1-13-1
大阪梅田ツインタワーズ・サウス 15F
MAIL：osaka@dtc.co.jp

2024.02