～デジタル変革に取り組む全ての企業様へ～

クラウド導入における運用管理を“もっと”楽にする３つのポイント

エクシオグループ株式会社

〒150-0002東京都渋谷区渋谷3丁目29番20号

クラウドを導入したけれども...

このようなお悩みで、お困りではありませんか？

近年、リモートワークの急増や、デジタルトランスフォーメーション（DX）への対応のため、
多くの企業において、クラウドサービスの利用が進んでいます。
そうした中で、**システム運用管理者の負担は大きくなるばかり**ですね。

ネットワーク遅延

クラウド導入に伴い回線を増速したけれども
ネットワーク遅延が改善されない

セキュリティ不安

セキュリティ脅威の多様化・高度化に
対応しきれていない

管理運用負担

ネットワークが複雑化し
管理運用負担が大きい

なぜ管理者の負担が減らないのか？

原因と対策について探ってみましょう。

それぞれの解決策　▶NEXT

①ネットワーク遅延

①ネットワーク遅延についてのお悩み

【お悩み】クラウド導入に伴い回線を増速したけれども、ネットワーク遅延が改善されない

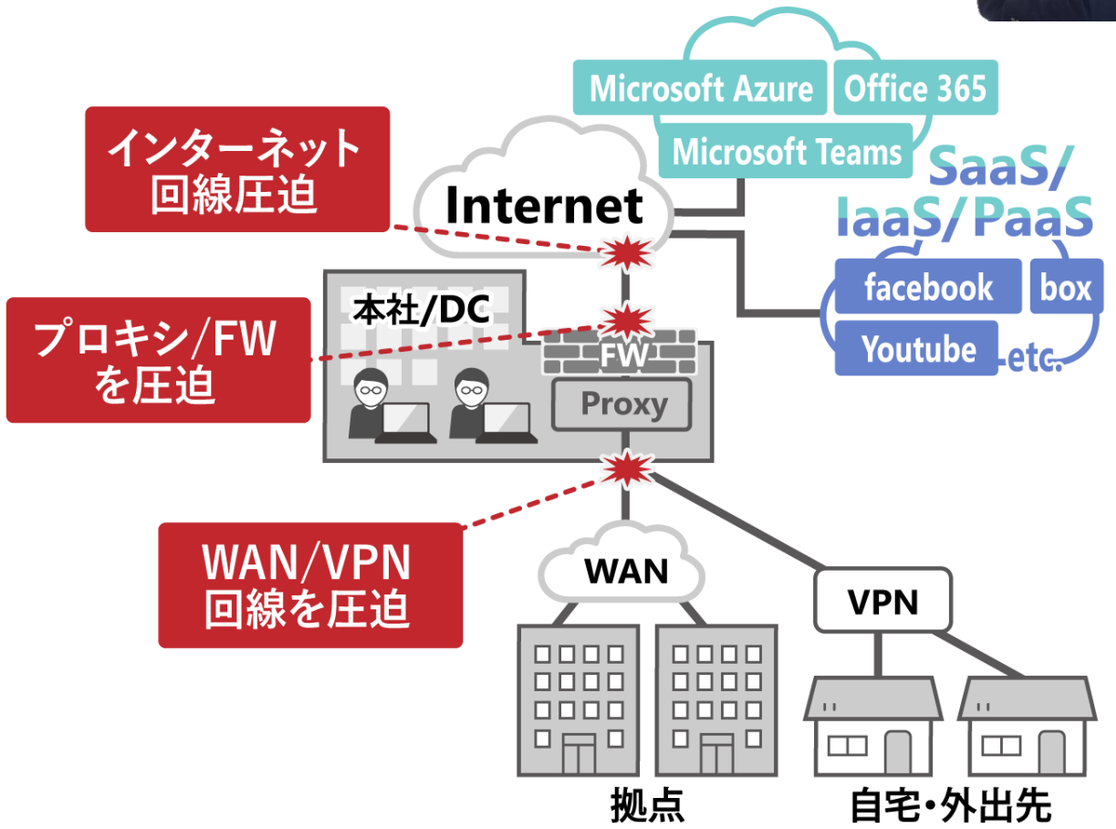
【原因】ボトルネックが解消されていない

データセンターやアプリケーションのクラウド化により、ファイアウォールやプロキシサーバを経由する通信が大量に発生するようになりました。

図のような従来型ネットワーク構成の場合、インターネットへの出口に通信が一極集中するようになります。

また、新型コロナの影響でリモートワークが急増、
VPN回線の逼迫も考えられます。

ボトルネックを見極めた対処をしないと、回線を増速しても増速しても、問題が解決されないという事象に陥ってしまいます。



①ネットワーク遅延についての解決策

【原因】ボトルネックが解消されていない → 解決策を解説

利用状況を見える化

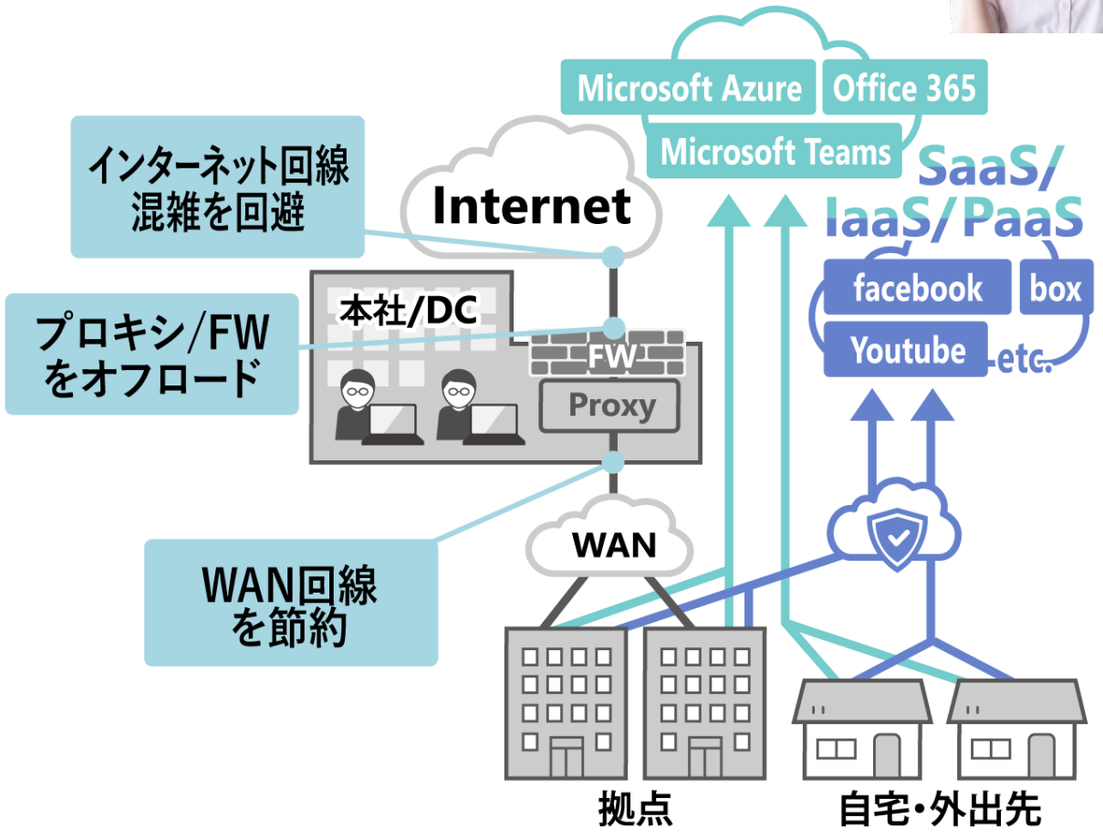
まずは、利用状況を見える化し、根本原因を探りましょう。でも、インターネット回線、プロキシ状況、VPN回線等の様々な回線利用状況を、それぞれ個別に調査管理するのは大変ですよね…。そんな時は、**拠点別/接続先別/アプリケーション別/時間帯別などさまざまな切り口で一元的にトラフィックを可視化**してみましょう。

ボトルネックの解決

次にこのようなお悩みの場合は、インターネットへの出口やVPNがボトルネックとなっているため、従来の社内イントラに集約していたネットワーク構成から、直接インターネット接続するようWANを最適化します。

例えば、**信頼性のあるOffice365等の通信は各拠点から専用線を通さずに直接インターネット経由で接続し、機密性の高いデータには、従来通りデータセンタ経由で接続し**、セキュリティ水準を保ったまま、回線のコスト・パフォーマンスを上げます。これらの作業を、**現地に赴くことなく遠隔で対応**できたらとても“楽”になりますね。

それが**SD-WAN**です。 SD-WANについてはスライド14をご参照ください。



②セキュリティ不安

②セキュリティ不安を感じる原因

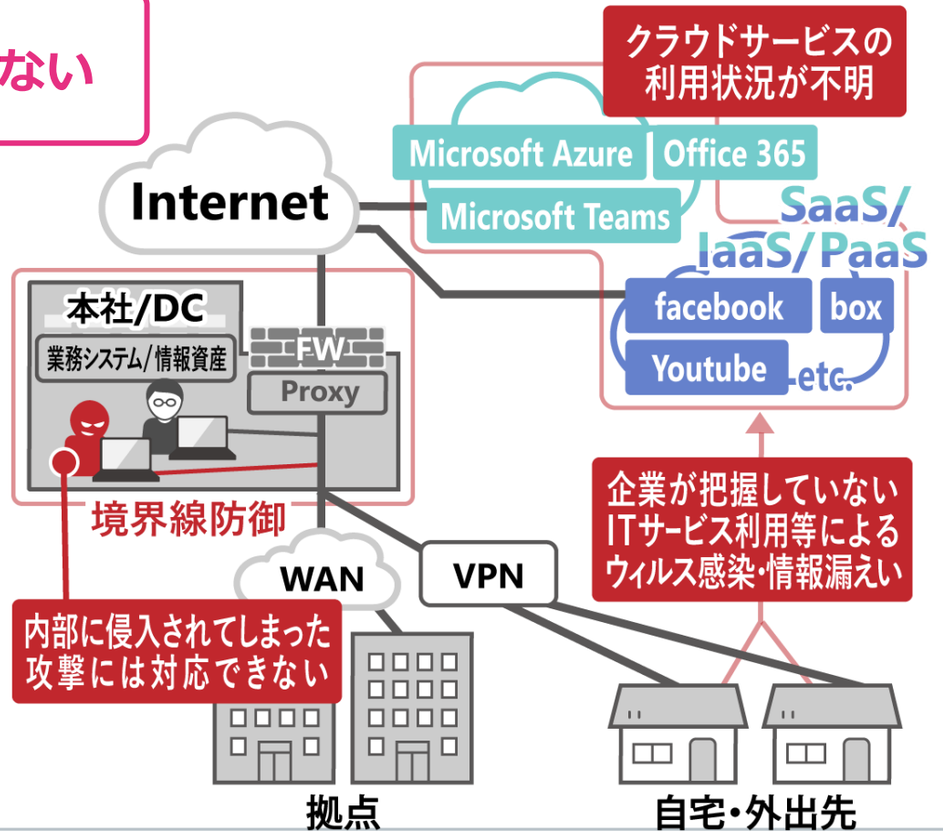
【お悩み】セキュリティ脅威の多様化・高度化に対応しきれていない

【原因】多様化する働き方に対応した仕組みが実装できていない

これまでは社内イントラ内で利用されているパソコンを意識し、
社外からの接続に対して悪意を防御する「境界線防御」を
すればよかったのですが、攻撃手法の高度化や内部不正により、
境界線を防御するだけでは守り切れないのが実状となっています。

また、先に述べたように、働き方はリモートワーク
＋クラウド活用へとシフトしています。

企業のデバイス・ユーザ・システムが社外に存在するようになり、
IT部門では全てのクラウド利用状況を管理しきれない状態に
なっています。



②セキュリティ不安についての解決策

【原因】多様化する働き方に対応した仕組みが実装できていない → 解決策を解説

リモートアクセス手段を変更

まずは、これまでの境界線防御ではなく、全ての通信は信頼できないものととらえ、**社内外の区別なく情報資産へのアクセスに対して、アクセス要求がある度に認証**を行うようリモートアクセス手段を変更します。（ZTNA※1）

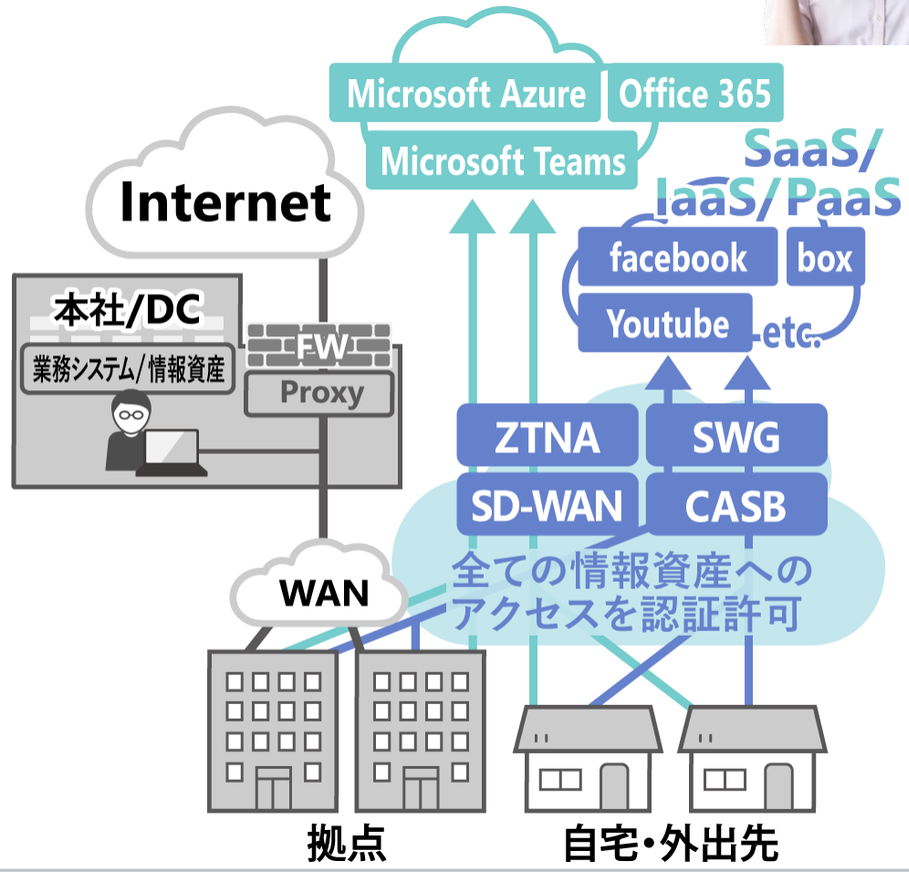
そうすることで、社外からのアクセスだけでなく、内部に侵入されてしまった悪意に対しても防御を行うことができます。

リモートワーク＋クラウド活用に対応したセキュリティ対策

また、クラウド利用へのセキュリティ対策には、**クラウドサービスへのログイン状況やデータのアップ／ダウンロードなどの状況を可視化・分析し、通信のブロックやアラート通知などの制御**を行うようにします。（CASB※2）

Webトラヒックに対しても、**社内外のユーザ問わずプロキシチェック**を行うようにします。（SWG※3）

複数のクラウドサービスを併用している今、これらを1つずつ設定制御するのはかなり大変ですよね…。次からは、そんなお悩みについてみていきましょう。



※1 Zero Trust Network Access ※2 Cloud Access Security Broker ※3 Secure Web Gatway

③管理運用負担

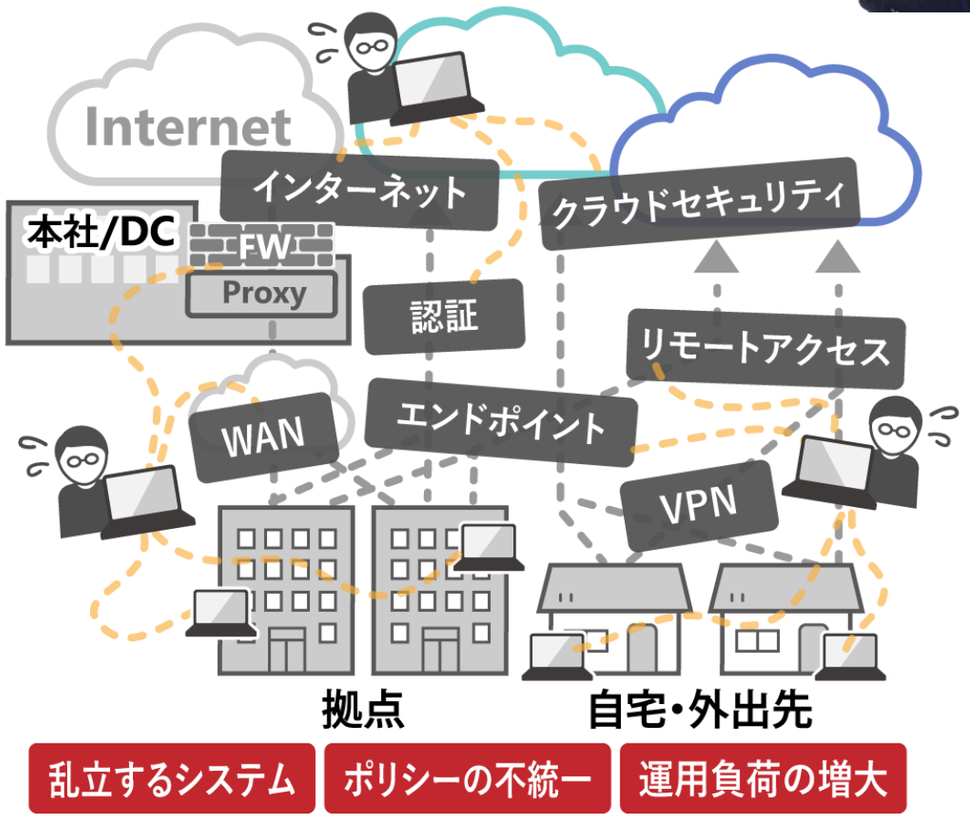
③管理運用負担を感じる原因

【お悩み】ネットワークが複雑化し、管理運用負担が大きい…

【原因】つぎはぎネットワークでバラバラ管理

従来型のネットワーク構成では、セキュリティ対策、クラウド利用、リモートワーク…等、それぞれの課題に対してそれぞれの対応を行ってきました。そのため、ネットワークはつぎはぎで複雑化、管理運用もそれぞれに対して個別に行うことになり、NW利用状況の把握や、ポリシーの設定にも大変な稼働がかかってしまいます。

さらにクラウド過渡期である場合は、オンプレ＆クラウドのハイブリット状態による二重管理も発生してしまいます。



③管理運用負担についての解決策

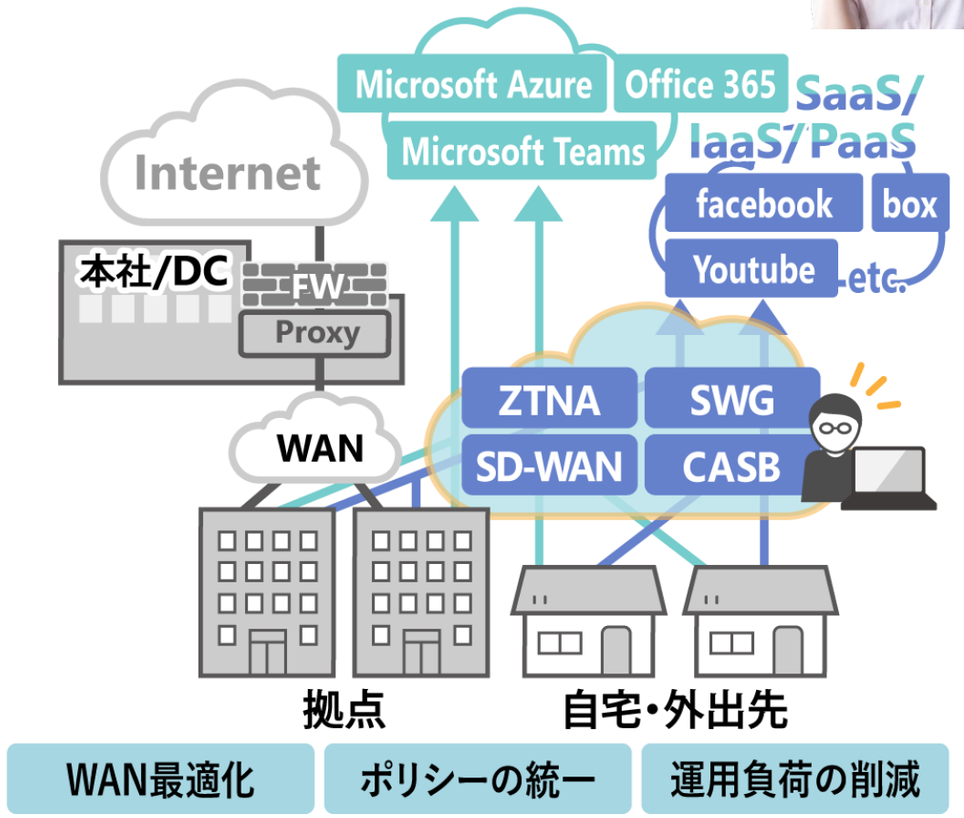
【原因】つぎはぎネットワークでバラバラ管理 → 解決策を解説

個別の設定管理をやめる

これまでのように、アプリケーション毎に異なるセキュリティポリシーを適用させることをやめてみませんか？
デバイス・エッジ毎に設定管理するのをやめてみませんか？

そのためには、すべてのアプリケーションをデータセンタからクラウド上に集約してからエッジに提供するというアプローチをします。これにより**デバイスやエッジの数が増えても、一貫したセキュリティポリシーを適用させることができます**。ポリシーや設定項目に変更があれば、クラウド側でのみコンテキストを変更すればよく、アプリケーションやデバイスごとに設定する必要はなくなるのです。

管理者の運用負担を最小限に抑え、パフォーマンスの低下を起こさずにサービスの提供が可能になります。



解決方法の共通点「SASE」

SASEという考え方

ここまで見てきた解決方法は、全て SASE という考え方に基づいています

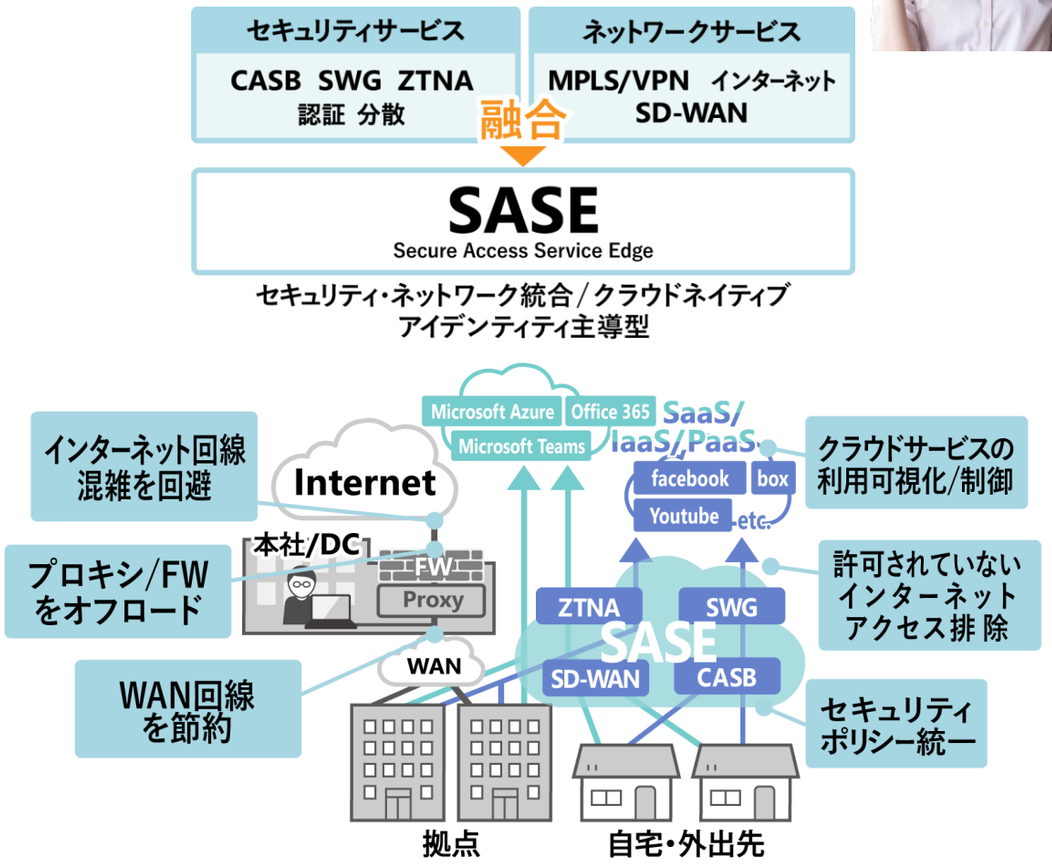
SASE とは

SASEはSecure Access Service Edgeの略で、2019年にガートナーが提唱したネットワークセキュリティモデルです。

IT環境におけるセキュリティ機能とネットワーク機能を1つのクラウドサービスに統合させるという、新たなセキュリティフレームワークです。

SASEは概念上、SD-WANとネットワークセキュリティサービス（SWG、ZTNA、CASBなど）を統合したものになります。

SASEを取り入れると、リモートワーク＋クラウド活用という新しい働き方に対しての運用管理のお悩みをまるっと解決することができるのです。



SD-WANとは？

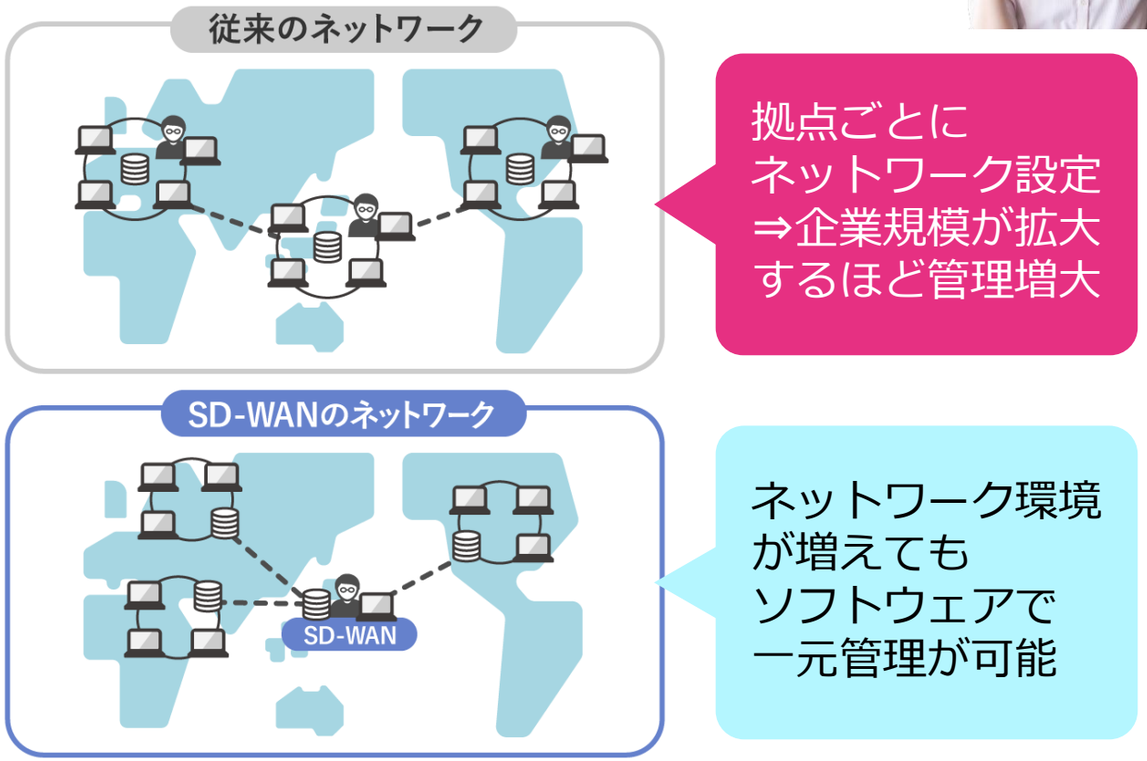
SASE について、もう少し詳しく見てみましょう

SD-WANとは

これまでの企業内ネットワークでは、拠点ごとにネットワークを設定していたため、拠点間の情報共有には、セキュリティを担保した専用回線の利用と、拠点間同士の経路制御や様々な設定が必要になります。その結果、企業規模が拡大すればするほど、IT管理者に多大な負荷がかかることになってしまいます。

それを解決するのが**SD-WAN**です。

ネットワーク上に仮想的な別のネットワークを構築することで、国内外の拠点を問わず、様々な形態のネットワーク環境や端末設定を、ソフトウェア上で一元管理することが可能になります。



SD-WANの主な機能

- 制御設定の一元管理
- WANの最適化
- アプリケーションベースの経路制御
- 拠点のゼロタッチ導入

まとめ

まとめ

クラウド導入における運用管理を
“もっと”楽にする**３つのポイント**

①ネットワーク遅延

WANの
- 見える化
- 最適化
- 集中管理

を同時に実施
（SD-WAN）

②セキュリティ不安

- アクセス毎認証
- クラウド監視

でセキュリティ強化
(ZTNA、CASB、SWG等)

③管理運用負担

- ネットワークと
  セキュリティの融合

で一元管理
(SASE)

無料相談のご案内

最適なネットワーク環境を実現されたい方

『無料相談』 をぜひご活用ください

ネットワークついてのお困り、疑問など、ご気軽にご相談ください。

弊社のネットワークの専門チームが、お悩みをお伺いします。

お申し込みはこちらから

Engineering for Fusion

社会を繋ぐエンジニアリングをすべての未来へ

EXEO