# ゼロトラストの実現に必要なSASEの導入方法を解説

## 今こそ見直しておきたいテレワークのセキュリティ。ゼロトラストの実現に必要なSASEの導入方法を解説!

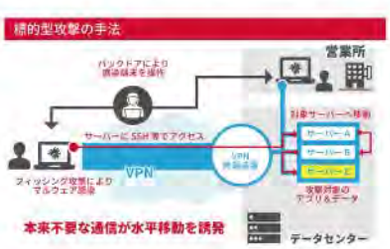
コロナ禍や働き方改革をきっかけにテレワーク時代が到来し、どこでもいつでも、どんなデバイスでも安全に働ける環境の構築が求められている。そこで重要になるのがテレワークに必須のリモートアクセス環境におけるセキュリティだ。とくにコロナ禍ではリモートアクセス環境を狙った攻撃が急増し、多くの企業でセキュリティ向上のため、VPN需要が高まった。しかし昨今ではそのVPNも、脆弱性やネットワーク負荷などの課題が顕在化し、セキュリティの見直しが急務となっている。そうしたなかでゼロトラストやSASEなどの新しい考え方が生まれているが、どのようにリモートアクセス環境を整備していけばいいのだろうか。本稿では、新しいセキュリティ環境をスムーズに導入・運用するアプローチを紹介する。

### 在宅勤務やテレワークの普及で拡がる、セキュリティの「穴」

テレワーク対応や働き方改革に向けた取り組みが進むなか、企業ではこれまで以上にセキュリティに対する意識が高まっている。これにはコロナ禍で多発したセキュリティ事故が大きく影響している。

たとえば、自宅に持ち帰った社用PCを家庭用ネットワークでインターネットにつなぐことで、攻撃者に侵入されやすくなった。以前は社内ネットワークにしか接続しないことを前提として、境界型防御のセキュリティ機能を利用していた。しかし、家庭用ネットワークを使って業務を行う現代ではそうした対策は通用しない。

また、VPNなどのリモートアクセス用機器の脆弱性を悪用され、攻撃を受けるといった被害も相次いでいる。コロナ禍でリモートアクセスが急増したことで、設定が不十分な機器を運用しているケースも増えた。対策が不十分な状況でテレワークの普及が進み、セキュリティの「穴」ができ、そこが狙われて攻撃を受けている格好だ。




そんななか、新しいセキュリティのあり方として注目を集めるようになったものに「ゼロトラスト」がある。ゼロトラストを導入することで、リモートアクセス環境のセキュリティ課題が解消できると期待されている。ただ、ゼロトラストは新しい考え方でもあり、具体的にどのように対応すればよいか悩んでいる企業が多いのも現状だ。

### よくある課題(1)「セキュリティ機能をどのように組み合わせればいいのかわからない」

新しいリモートアクセス環境の整備でまず課題になるのは「セキュリティ機能をどのように組み合わせればいいのかわからない」というものだろう。実際、セキュリティベンダーごとにゼロトラストが示す範囲は異なっていて、どのような機能を実現すればいいかは見えにくくなっている。



# 今こそ見直しておきたいテレワークのセキュリティ。ゼロトラストの実現に必要なSASEの導入方法を解説!

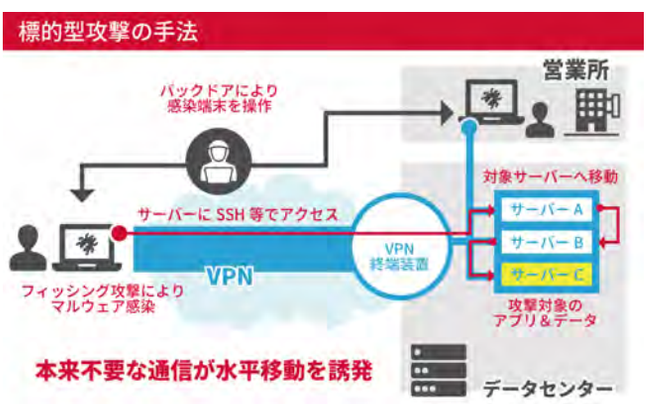
コロナ禍や働き方改革をきっかけにテレワーク時代が到来し、どこでもいつでも、どんなデバイスでも安全に働ける環境の構築が求められている。そこで重要になるのがテレワークに必須のリモートアクセス環境におけるセキュリティだ。とくにコロナ禍ではリモートアクセス環境を狙った攻撃が急増し、多くの企業でセキュリティ向上のため、VPN需要が高まった。しかし昨今ではそのVPNも、脆弱性やネットワーク負荷などの課題が顕在化し、セキュリティの見直しが急務となっている。そうしたなかでゼロトラストやSASEなどの新しい考え方が生まれているが、どのようにリモートアクセス環境を整備していけばいいのだろうか。本稿では、新しいセキュリティ環境をスムーズに導入・運用するアプローチを紹介する。

## 在宅勤務やテレワークの普及で拡がる、セキュリティの「穴」

テレワーク対応や働き方改革に向けた取り組みが進むなか、企業ではこれまで以上にセキュリティに対する意識が高まっている。これにはコロナ禍で多発したセキュリティ事故が大きく影響している。

たとえば、自宅に持ち帰った社用PCを家庭用ネットワークでインターネットにつなぐことで、攻撃者に侵入されやすくなった。以前は社内ネットワークにしか接続しないことを前提として、境界型防御のセキュリティ機能を利用していた。しかし、家庭用ネットワークを使って業務を行う現代ではそうした対策は通用しない。

また、VPNなどのリモートアクセス用機器の脆弱性を悪用され、攻撃を受けるといった被害も相次いでいる。コロナ禍でリモートアクセスが急増したことで、設定が不十分な機器を運用しているケースも増えた。対策が不十分な状況でテレワークの普及が進み、セキュリティの「穴」ができ、そこが狙われて攻撃を受けている格好だ。




そんななか、新しいセキュリティのあり方として注目を集めるようになったものに「ゼロトラスト」がある。ゼロトラストを導入することで、リモートアクセス環境のセキュリティ課題が解消できると期待されている。ただ、ゼロトラストは新しい考え方でもあり、具体的にどのように対応すればよいか悩んでいる企業が多いのも現状だ。

## よくある課題(1)「セキュリティ機能をどのように組み合わせればいいのかわからない」

新しいリモートアクセス環境の整備でまず課題になるのは「セキュリティ機能をどのように組み合わせればいいのかわからない」というものだろう。実際、セキュリティベンダーごとにゼロトラストが示す範囲は異なっていて、どのような機能を実現すればいいかは見えにくくなっている。


また、ゼロトラストのほかにも「SASE(Secure Access Service Edge)」という言葉があり、どう使い分けていいかわからないことも多い。たとえば、SASEの説明としては「SD-WAN」「ZTNA」「CASB」「FWaaS」「SWG」などの用語が飛び交い、セキュリティ専門の担当者でも、理解が難しい場合も少なくない。

導入にあたっても、これらのセキュリティ製品をどんな順序でどう実装していけばよいかがわかりにくい点もある。導入する順序を間違えることで機能が二重になったり、一度導入した製品のリプレースが発生したりして、導入コストがかさんでしまうケースもある。

## よくある課題(2)「導入はできても運用が難しい」


2つ目の課題としては「導入はできても運用が難しい」というものが挙げられる。

CASB(クラウドアクセスセキュリティブローカー )、SWG(セキュアWebゲートウェイ)などに対応した機器やサービスを導入するケースで考えてみたい。この場合、すべての拠点を一気に変更することはコストや期間、ビジネスへ与える影響の大きさから難しいことが多く、段階的に移行していくことになる。

そのため、既存のセキュリティと新しい機器やサービスを併用することになり、運用者の手間は以前よりも増えていくことになる。さらに拠点が多ければ多いほど、移行の手間や人材の確保が必要になり、各拠点での運用を安定的に行うための冗長性や可用性の確保も課題だ。また、新しい機器を設置、設定、管理するためのスキルを習得する必要もある。

そのうえ、監視やアラートなどの運用管理も課題になりやすい。ユーザーのアクセス先や利用アプリケーション、脅威などをどのように可視化するかを定義づけ、大量のアラートを捌いていくには、それなりの専門スキルが求められる。

## 新しいリモートアクセス環境を整備するためのポイントとは?

では、新しいリモートアクセス環境を整備するためには何がポイントになるのか。ここでは、製品選定で重要になるポイントを3つに整理して考えてみたい。

**1. 企業全体で統一的なセキュリティレベルを確保できること**

ゼロトラストやSASEという言葉にとらわれすぎると、セキュリティ機能をどう組み合わせればよいかに考えが偏ってしまいやすい。機能を見るのではなく、最初に実現したいセキュリティレベルを全体から見て、リモートアクセス環境を整備していくことが重要だ。

**2. さまざまな拠点をカバーしながら、大規模で高度なサイバー攻撃に耐えられるアベイラビリティを備えること**

サイバー攻撃は、企業規模や業種、地域など関係なく発生する。日本国内はもちろん、世界中のどこに拠点があっても安全にリモートアクセスできるようになることが重要だ。

**3. 簡単に導入、構築でき、運用も事業者や専門組織に任せられること**

マネージドサービスとして、リモートアクセス基盤の管理を外部に任せることで、導入コストや運用負担を低減でき、人手不足にも対応できる。リモートアクセス環境によって推進したい本来の業務管理に集中できるようにすることが重要だ。

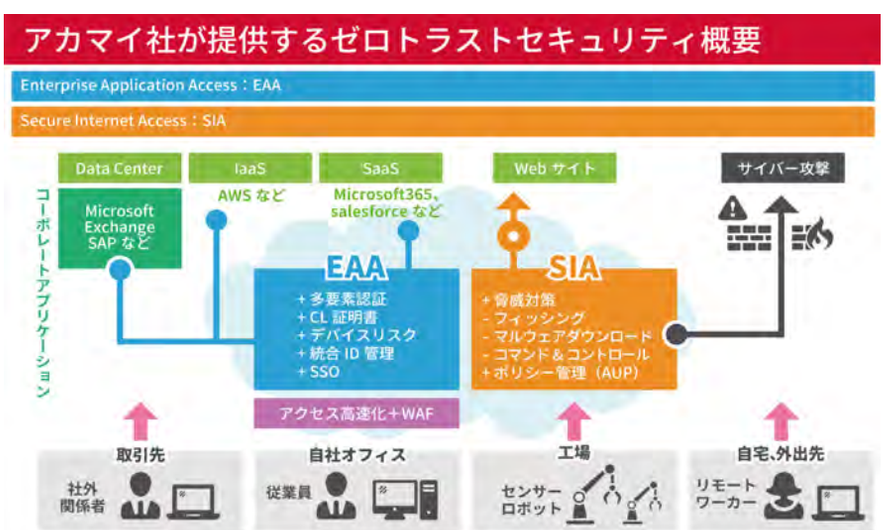
こうした3つのポイントを押さえたリモートアクセス環境として注目できるのが、NTTコミュニケーションズ(以下、NTT Com)が販売を手がける「Akamai Secure Access Service Edge」(以下、Akamai SASE)だ。

## Akamaiが提供するリモートアクセスソリューション

Akamai SASEは、CDN(Content Delivery Network)事業者のパイオニアとして知られるAkamaiの提供するセキュアなリモートアクセスのためのソリューションだ。SASEの名称からわかるように、ゼロトラストやSASEの考え方を実現できるソリューションでもあり、さまざまな機能を包含しながら、新しいセキュリティの考え方やフレームワークを簡単に導入・運用できるクラウドサービスとして提供されている。

最大の特長は、グローバルなクラウド基盤を活用したセキュリティとネットワークの統合サービスであることだ。世界を網羅するAkamaiのデータセンターを活用することで、新たな機器の設置やリプレースは不要だ。企業が管理するユーザー、デバイス、サービスなどすべてのリソースを、パフォーマンスを犠牲にすることなくクラウドベースで効率良く制御できる。基盤の運用管理も任せられるため、運用負荷の低減も可能だ。日本国内にも多数の接続拠点(Point of Presence: PoP)があり、複数のPoPを活用することでアベイラビリティを確保し、安定した安全なリモートアクセスサービスの利用が可能だ。

もう1つの大きな特長は、ゼロトラストやSASEとして求められるさまざまな機能を包括的に活用できることだ。セキュリティ機能は企業のビジネス状況やITシステムの環境により、必要な要素が大きく変わる。環境が変化するなかで必要な機能を随時更新する必要もある。Akamai SASEは柔軟に機能の組み合わせを変えることができるため、環境変化やニーズに応じてアップデートしていくことができる。




さらに、AkamaiのCDNのノウハウを活用できることもポイントだ。IPアドレスのデータベースやDNSのレピュテーション(評価)を確認しながら、DNSと連携した高度なSWGを運用することができる。Akamaiが提供するWebアプリケーションファイアウォール(WAF)サービスと連携させて、アプリやAPIへの攻撃を検知、ブロックすることも可能だ。

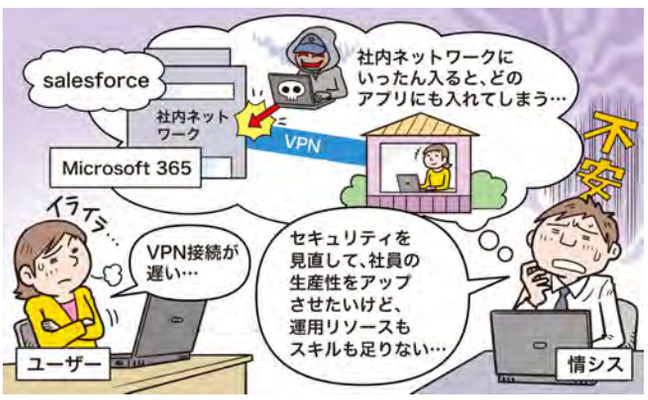
## NTT Comが顧客に寄り添ってリモートアクセス環境の整備をサポート

導入にあたって、NTT Comによる強力なサポートが得られることも大きな強みだ。「どのようにセキュリティ機能を組み合わせればいいかわからない」「運用負担が大きい」といった課題もNTT Comのコンサルタントやエンジニアが顧客に寄り添って解決してくれる。

NTT Comは、Akamaiパートナーとして約20年の実績を持っている。数十名規模のAkamai有資格者を擁するAkamai最上位パートナーで、「Akamai Partner of the Year」を日本で唯一受賞している。企業が抱えるさまざまなセキュリティ課題を理解し、24時間365日サポート体制で解決策を提示していく。

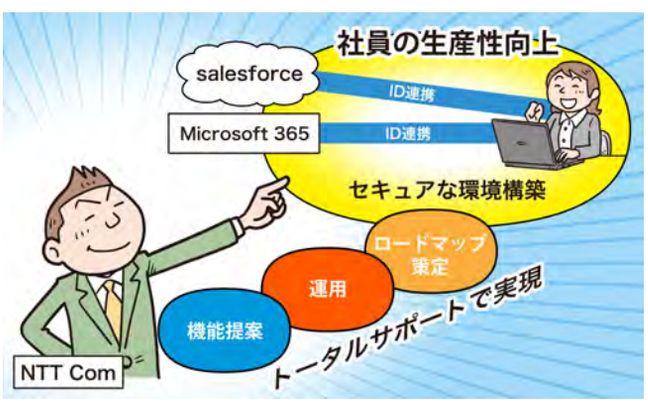
# NTT ComのAkamai SASE導入実績

## 導入前の課題




VPNを活用してリモートアクセス環境を構築していたが、社内ネットワークにアクセスすると、すべてのアプリ、ファイルサーバーにアクセスできてしまうことから、セキュリティに懸念を抱いていた。また、いったん社内ネットワークを経由することでインターネット回線が逼迫し、ユーザーから苦情も出ていた。

## 解決策




必要なセキュリティ機能の提案から、運用管理、その後のロードマップ策定などをNTT Comがサポートし、Akamai SASEを導入。社内ネットワークを経由することなく、ID認証でアプリを使用できるセキュアなリモートアクセス環境を構築した。さらに回線逼迫も解消し、社員の生産性向上や働き方改革の実現に貢献した。

さまざまなデバイスでいつどこからでも安全に働ける環境構築が求められるテレワーク時代が到来し、企業の環境に応じて必要なセキュリティを安定的に運用していくことは、ビジネスを継続していくうえで必要不可欠だ。リモートアクセス環境の整備はもちろん、Webアプリケーションの保護やネットワークの高度化まで実現が可能なAkamai SASEは企業にとってビジネスを支える大きな力となるはずだ。


Akamai SASEに関するお問い合わせ

NTTコミュニケーションズ株式会社

**法人のお客さまお問い合わせ窓口［ドコモビジネスコンタクトセンター］**

携帯OK **0120-003300** 受付時間 9:00～17:00

※携帯電話からもご利用になれます。土・日・祝日・年末年始は休業とさせていただきます。

サイト www.ntt.com/business/services/network/cdn/cdn.html

お問い合わせメールアドレス cdn-sales@ntt.com




A1207092 2022.10