

いまさら聞けない

# SASE 入門

SASE導入で企業ネットワークはどう変わる？

いまさら聞けない

# SASE

## 入門

P2 はじめに：

注目の次世代ソリューション「SASE」

P3 SASEはなぜ生まれたのか

P5 SASEの主な構成機能

P7 SASEの導入で企業はどう変わるか

P9 導入・運用ハーダルの高いSASE

P10 SASEのムズカシイを解決：フルマネージドSASE Verona

P11 おわりに

はじめに

## 注目の次世代ソリューション SASE

ネットワークセキュリティの世界は目まぐるしく変化し、常に新しいワードが登場し続けています。その中でも近年、とりわけ注目されているワードが、「SASE」でしょう。

SASE (Secure Access Service Edge) とは、米国の調査会社ガートナー社が2019年に公開した、ゼロトラストを実現する新たなセキュリティのフレームワークです。ネットワーク機能とセキュリティ機能を一つのクラウドサービスとして統合して提供します。

SASEは、企業のネットワーク管理やセキュリティ対策を大きく変革します。しかし、概念的で理解しにくいために、実際にどんな機能があるのか、導入によってどんな効果を得られるのが、具体的なイメージが湧かない方も多いのではないでしょうか。

本書では、SASE誕生の背景から、SASEの機能、SASE導入による企業の変化まで、基礎からわかりやすく解説していきます。



# SASEはなぜ生まれたのか

注目のソリューションSASEは、なぜ生まれたのでしょうか。

背景は主に2つあります。

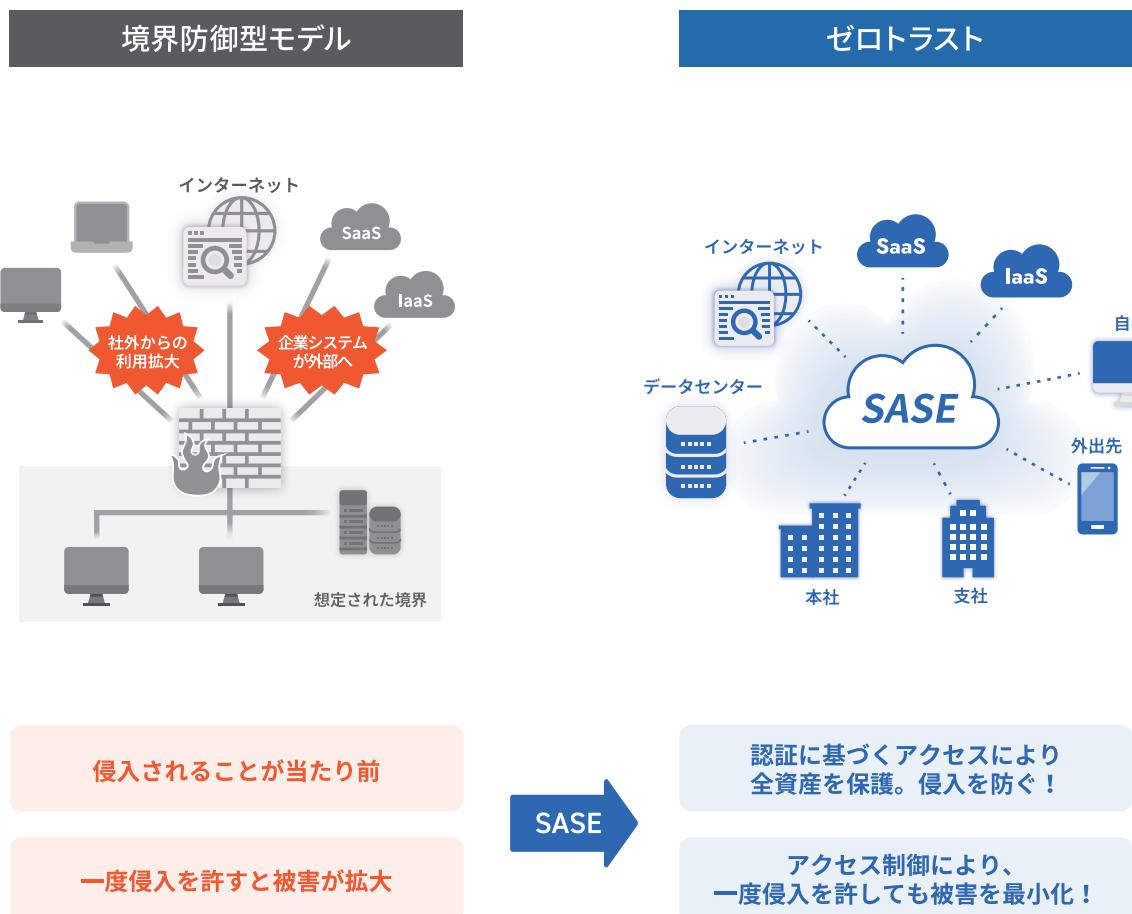
## 1. ゼロトラストの必要性

SASE誕生の一番の理由は、ゼロトラストアーキテクチャへの移行の必要性です。

近年、クラウド利用やテレワークの普及により、情報資産が社外に分散しています。そのため、守るべき資産が社内にあることを前提とし、安全な社内と危険な社外との境界においてセキュリティ対策を実施する「境界防御型」モデルでは、社外の資産にセキュリティを担保できなくなっています。さらに、サイバー攻撃は年々巧妙化しており、攻撃者の侵入を防

ぎきることが不可能です。そのため、社内が安全であることを前提として構築された従来のネットワークセキュリティモデルでは、侵入されたら最後、被害が甚大化してしまいます。

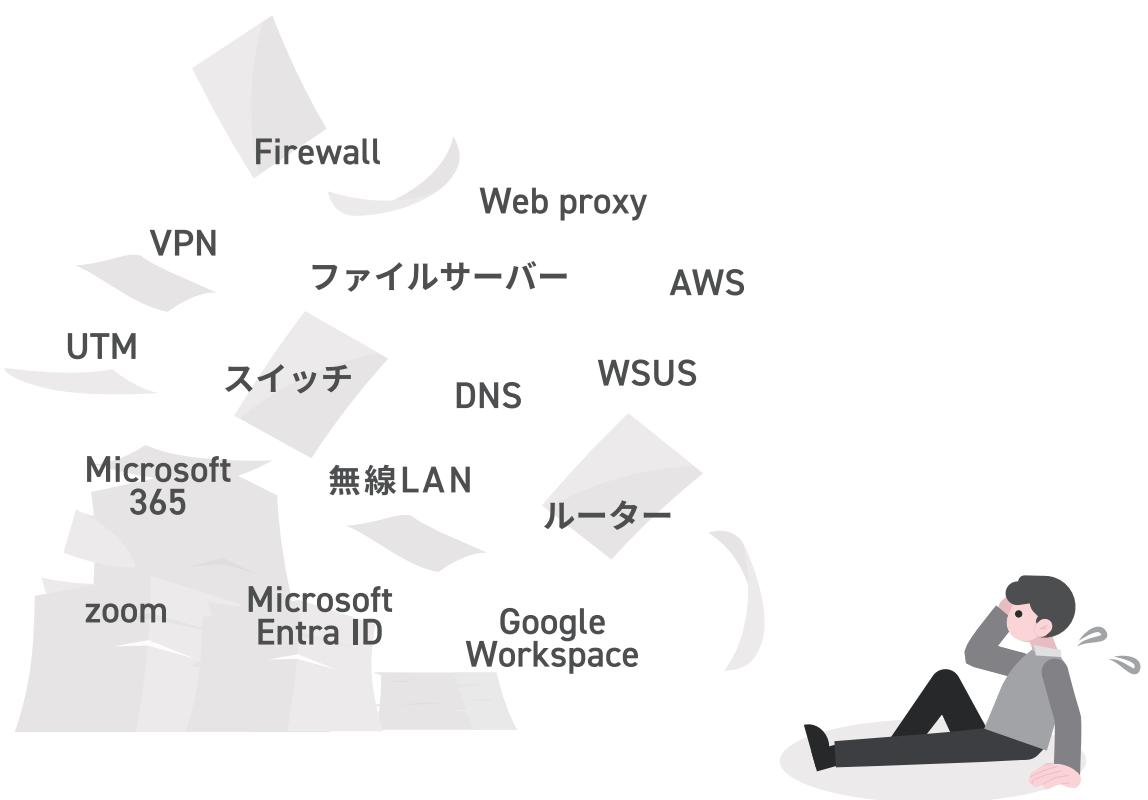
そこで登場したのが、「ゼロトラスト」です。ゼロトラストとは、社内外関係なく全ての通信を信用せず、全デバイス、ユーザ、ネットワークを監視して認証・認可を行い、アクセスを制御するという考え方です。ゼロトラストの概念に則ったセキュリティ対策を実施することで、全資産を保護して攻撃者の侵入を防ぎ、万が一侵入を許した場合も被害を最小限に留めることができます。



## 2. ITシステムの運用負荷の増大

また、前述したクラウド化や働き方の多様化、サイバー攻撃の激化は、情報システム部が運用管理しなければならないIT機器・システムの増加を招きました。一方で、IT人材は慢性的に不足しているため、一人一人の情報システム部の業務負

荷が増大しています。万が一、それらの運用管理に手が回らず、脆弱性が放置されてしまっては、せっかく導入したセキュリティ機器から攻撃者の侵入を許してしまう、そんな事態を招きかねません。



こうした近年のネットワークセキュリティの課題を解決し、ゼロトラストを実現しながら運用負荷も軽減するソリューションとして誕生したのが、SASEなのです。

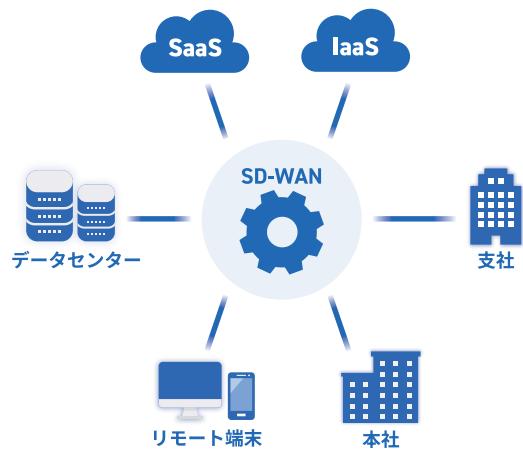
# SASEの主な構成機能

SASEは様々なネットワーク機能・セキュリティ機能の組み合わせで成り立ちます。以下が、SASEの主な5つの構成機能です。

## ネットワーク機能

### 1. SD-WAN (Software-Defined Wide Area Network)

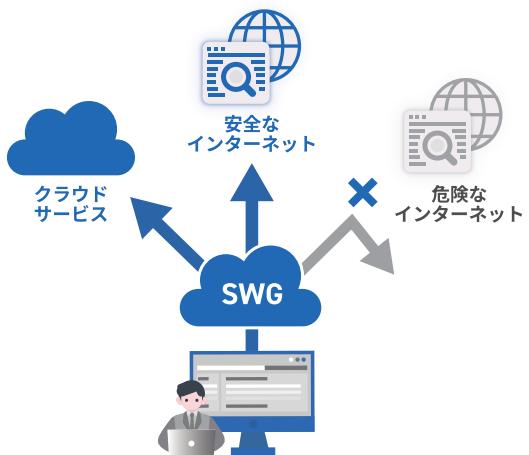
ネットワークをソフトウェアで制御し、柔軟なネットワーク構成やトラフィックコントロールを実現します。拠点間接続やクラウド接続など、WANを一元管理できるようになるため、管理負荷を軽減することができます。また、使用的するアプリケーションや利用用途によって経由する回線を使い分ける「ローカルブレイクアウト」も実装できるため、通信の最適化による通信ひつ迫の解消も図ることができます。



## セキュリティ機能

### 2. SWG (Secure Web Gateway)

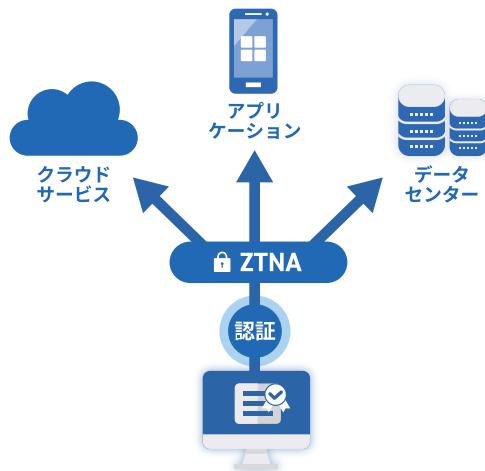
インターネット上に存在するプロキシとして作動する機能です。端末がインターネットへ接続する通信を検証し、悪性のIPアドレスやURLをブロックしてマルウェアや不正サイトから端末を守ります。ユーザーが社内ネットワークにいる場合も、社外ネットワークにいる場合でも、インターネット上の脅威からユーザーを保護することができる他、ローカルブレイクアウトにもセキュリティを実装できるのが、SWGの魅力です。サンドボックスやマルウェア検出などの複数の機能を有しているSWGもあります。



## セキュリティ機能

### 3. ZTNA (Zero Trust Network Access)

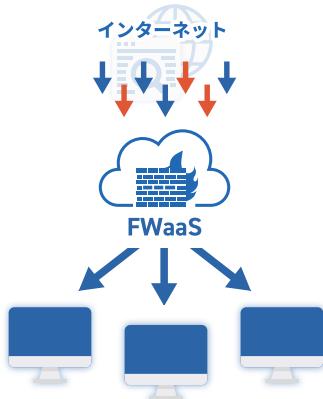
アクセス要求毎に認証を行い、特定のアプリケーションやクラウドサービス、リソースにセキュアなアクセスを提供します。ZTNAを使用すると、アプリケーションやリソースへのアクセスは、ユーザーが ZTNA サービスに対して認証された後に初めて可能になります。あらゆるリソースが認証なしにアクセスされることがないため、ゼロトラストの概念を実装し、攻撃被害の拡大を防ぐこともできます。



## セキュリティ機能

### 4. FWaaS (Firewall as a Service)

従来のファイアウォール機能をクラウドサービスとして提供します。社内と社外の境界ではなく、クラウド上で作動し、悪意あるネットワークトラフィックをフィルタリングするため、社内外関係なく通信を一元的に制御することができます。ディープパケットインスペクションやIPS/IDS機能などの複数の機能を有するFWaaSも存在します。



## セキュリティ機能

### 5. CASB (Cloud Access Security Broker)

ユーザーが利用するクラウドサービスの利用状況を可視化し、一貫したセキュリティポリシーで制御します。シャドーITを可視化し、社内ルールに則したクラウド利用を徹底できます。クラウドの不正利用による情報漏洩を検知したり、マルウェアを検出したりする機能を有するものもあります。

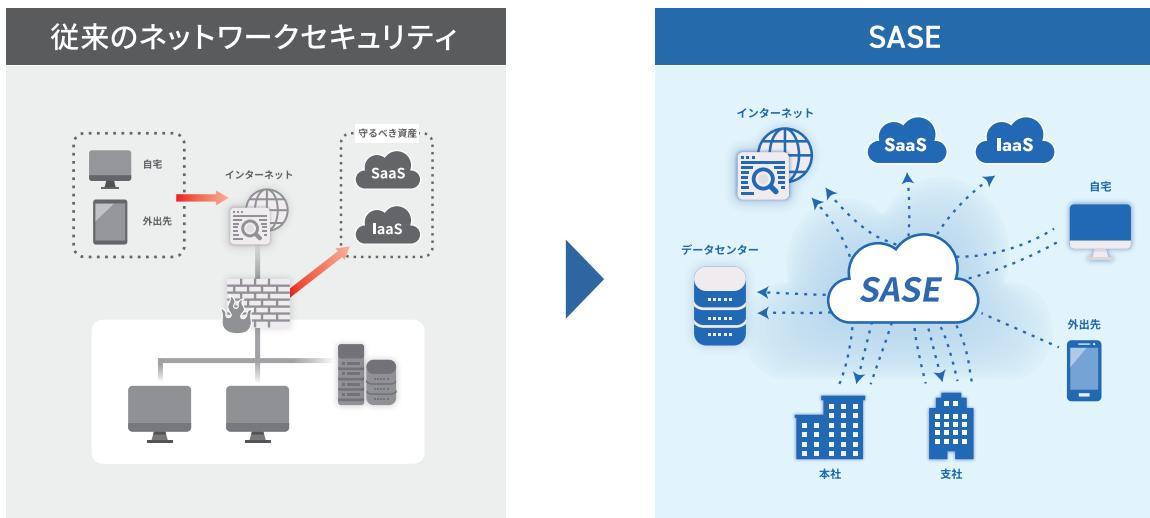


# SASEの導入で企業はどう変わるのか

ここからは、SASEを中心としたアーキテクチャへ移行することで得られる4大メリットを紹介します。

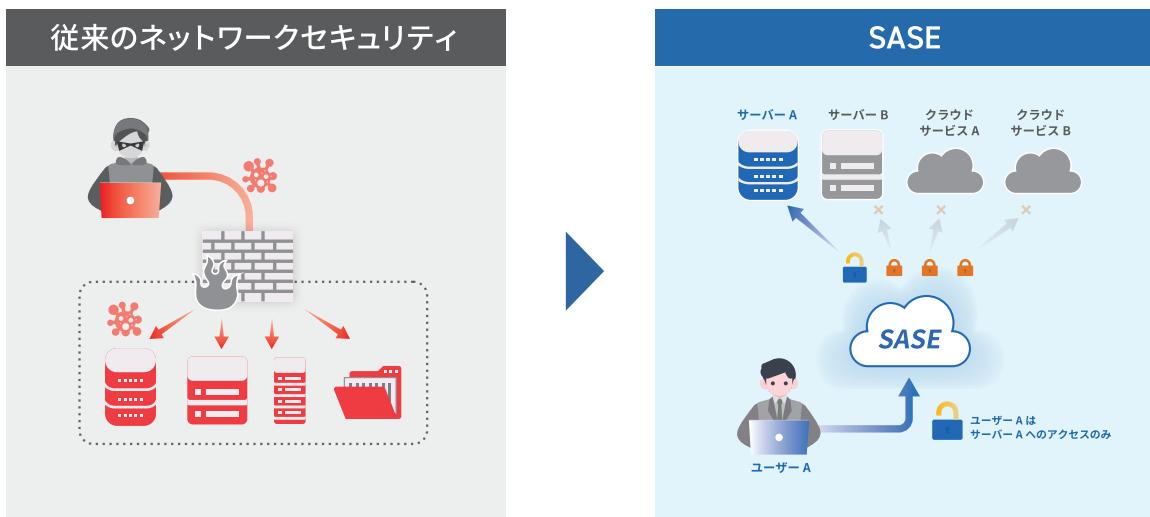
## 1. 包括的なネットワークセキュリティにより攻撃の侵入を防ぐ

SASEひとつであらゆる経路、あらゆる通信プロトコルを保護し、包括的なネットワークセキュリティを提供します。リモートワークからのアクセスや、クラウドサービスへのアクセスなど、アクセス元、アクセス先を問わないセキュアなアクセスを実現するため、セキュリティが脆弱な通信経路がなくなり、攻撃者の侵入を防ぐことができます。



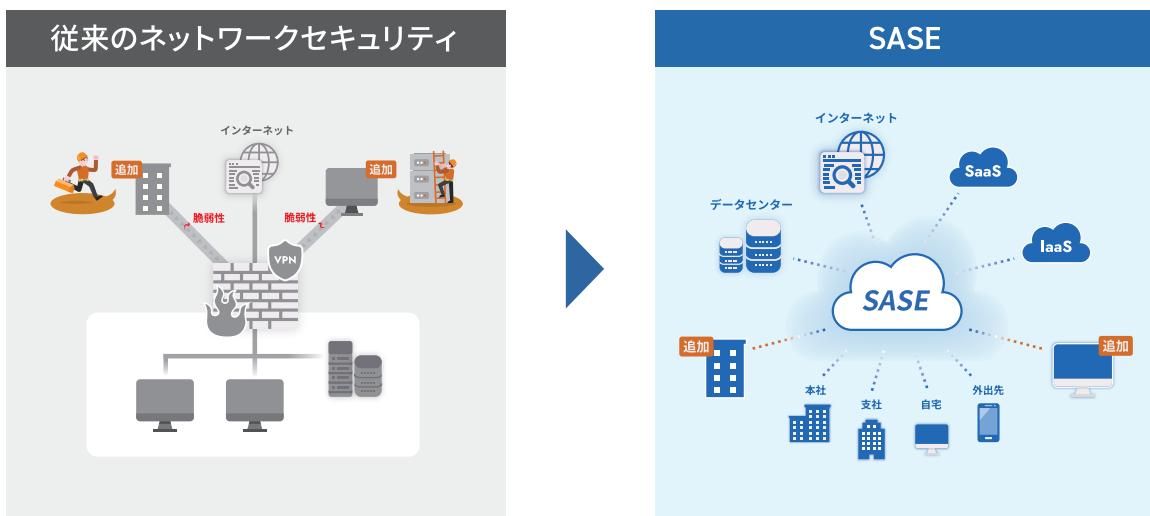
## 2. 社内トラフィックの管理・監視により被害の拡大を防ぐ

SASEにより、社内トラフィックを含めたすべてのネットワークアクセスを管理できるようになります。ネットワーク内の通信を細かく制御するマイクロセグメンテーションを実装できるため、万が一攻撃者の侵入を許しても全システムの侵害を防ぎ、被害の拡大を防止します。



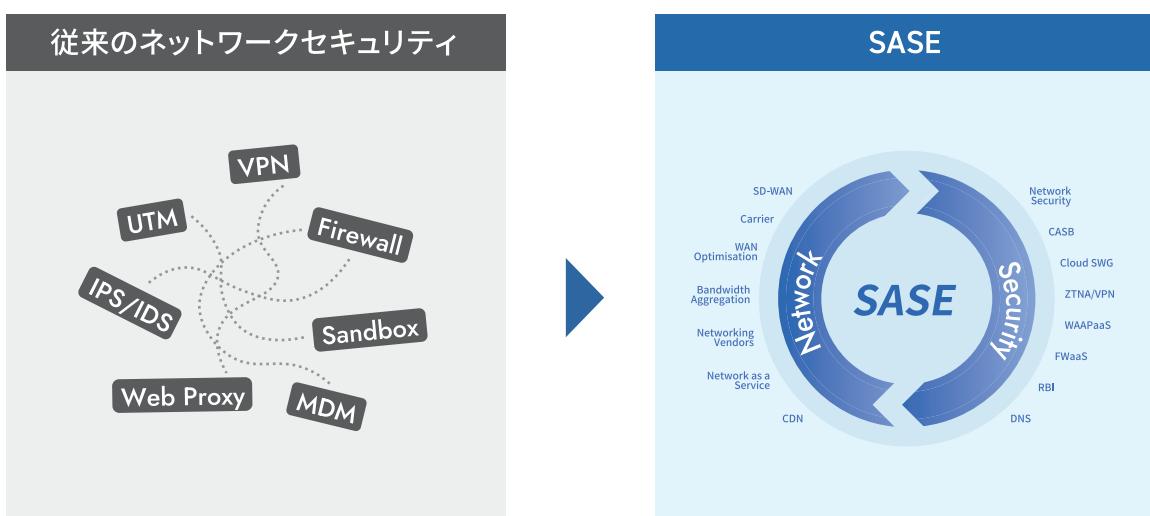
### 3. ネットワークアーキテクチャの拡張に柔軟に対応

SASEはあらゆる機能がクラウド上で提供されるため、拡張が容易です。テレワーク・クラウドサービスの導入や拠点の追加などの変化に、ネットワーク構成の大幅な変更なく柔軟に対応し、すべての通信・リソースが高いセキュリティレベルを保つことができます。



### 4. ネットワークセキュリティの統合管理により運用負荷を軽減

SASEによってあらゆるネットワーク機能・セキュリティ機能を一つのクラウドサービスとして包括管理できるようになります。そのため、ネットワークセキュリティの運用が効率化し、運用が行き届くようになります。



# 導入・運用ハードルの高いSASE

このような移行メリットがあるSASEですが、実は、導入・運用が難しいという問題があります。特に、人的・金銭的リソースに制限の多い中堅・中小企業にとってはハードルが高く、SASEの登場から約4年が経過した今でも、なかなか移行が進んでいないのが実情です。ここでは、よく耳にするSASE導入・運用の課題を3つ紹介します。

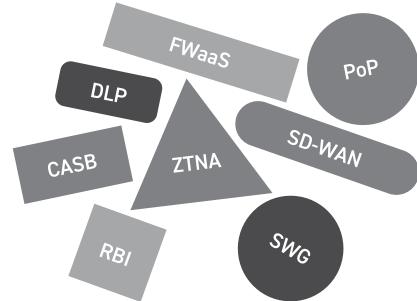
## 1. 導入に専門知識が必要

多くのSASEは、グローバル展開する大企業向けの構成となっており、企業のネットワーク構成全体の変更を必要とします。よって、導入に半年以上の時間を要し、導入には長期の大規模プロジェクトを遂行できる高度なIT人材が必要です。



## 2. 機能が多く使いこなせない

SASEの機能は多岐に渡るため、各機能のポリシー設定・変更などの運用・管理が煩雑になってしまう場合があります。また、それらの運用・管理に手が回らなかったり、必要以上の高機能であったりして、せっかく導入したSASEを使いこなせない恐れもあります。



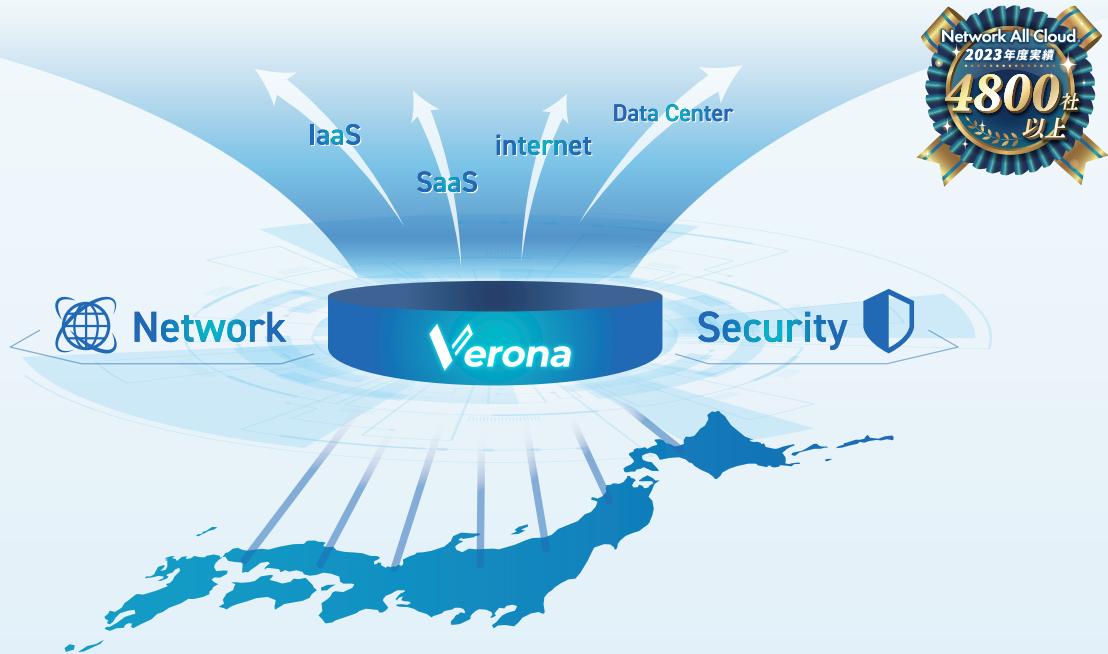
## 3. 導入費用・ランニングコストが高額

SASEは前述の通り大規模な移行作業を伴うため、移行にかかるSI費用が1,000万円を超える場合も多々あります。また、複雑なライセンス体系であらゆるコンポーネントごとに課金され、ランニングコストが高額となることも。



# SASEのムズカシイを解決 フルマネージドSASE Verona

そこで紹介するのが、フルマネージドSASE Veronaです。Veronaなら、前述のSASEの課題を取り除き、誰でも手軽に次世代ネットワークセキュリティを実現することができます。



## Veronaのポイント

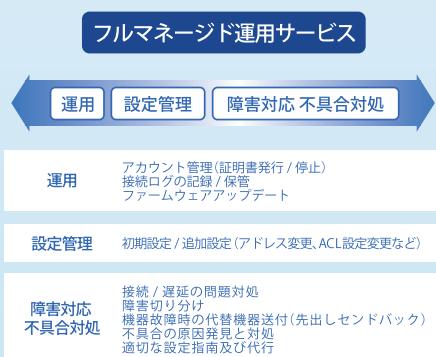
### 1. カンタン導入

導入に必要な作業は、ヒアリングシートの記入だけ。専門知識不要で、最短2週間でSASEを導入できます。



### 2. 運用負荷“ゼロ”

障害対応や設定変更など、日々の運用・管理をセキュリティのプロが代行。負荷なくSASEを運用できます。



### 3. オールインクルーシブ

サービス費用に全ての費用がインクルード。高額なSI費用を含めた様々な費用が不要で、大幅なコスト減を実現。



# おわりに

本書では、注目の次世代ソリューション、SASEについて、誕生の背景や機能、導入による効果まで、基礎からわかりやすく解説してきました。

SASEは、複数のセキュリティ・ネットワーク機能を一つにまとめた、画期的なソリューションです。強固なセキュリティ対策を施せるだけではなく、運用・管理負荷を軽減できるというメリットもあります。

激化するサイバー攻撃。クラウド利用やテレワークへのセキュリティ対応の遅延や、運用管理が複雑化している状況では、セキュリティの大きなリスクが潜んでいます。ま

だ大丈夫、と思っているうちに被害が起きてしまっては取り返しがつきません。早めにSASE導入することで、信頼性と企業価値向上にもつながります。

とはいっても、SASE導入の検討には、ネットワークの見直しなどに時間がかかる企業様も多いことでしょう。網屋は、3700社以上のお客様のネットワークセキュリティを提案・構築・運用してきたノウハウを基に、SASE移行相談や導入コンサルティングも実施しております。まずはお気軽にご相談ください。

## フルマネージドSASE Verona

詳しい製品概要資料はこちら ↗

### お問い合わせ先

株式会社網屋 ネットワークセキュリティ事業部



お電話でのご相談

**03-6822-9995**



メールでのご相談

**infra-sales@amiya.co.jp**

開発元

**AMIYA** 株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町11F  
TEL : 03-6822-9996 (ダイヤルイン) FAX : 03-6822-9998

<https://www.amiya.co.jp/>

Veronaは網屋の登録商標です。  
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。  
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。

販売元