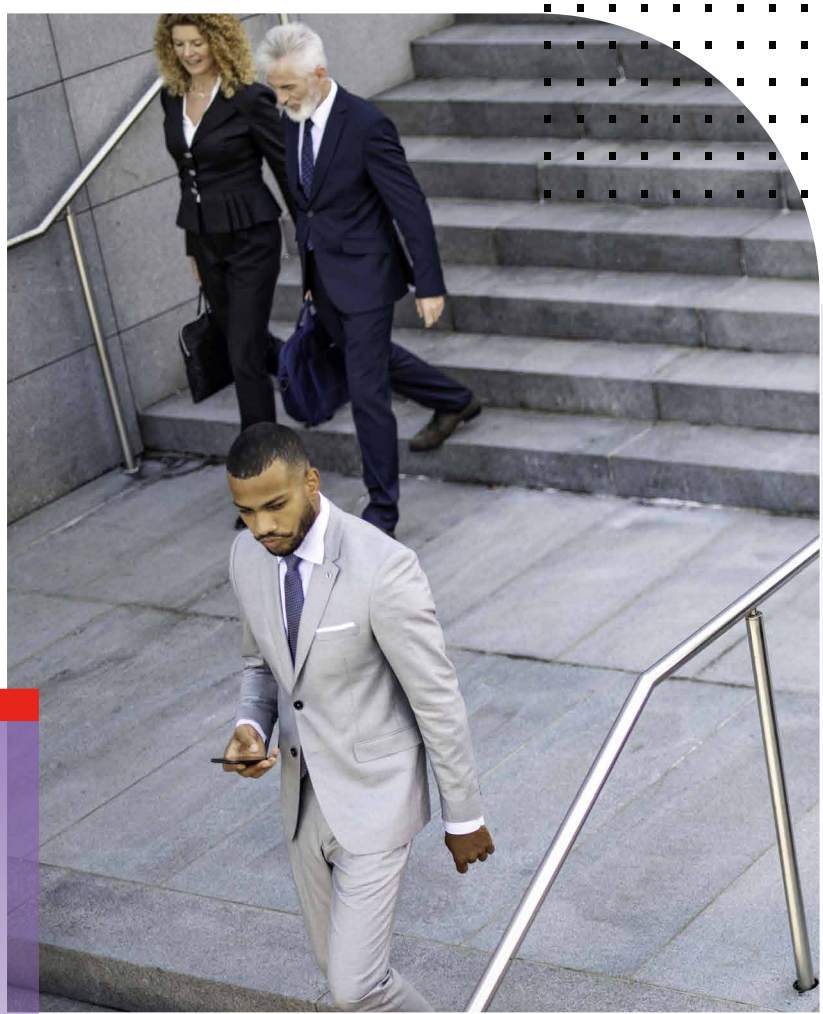
WHITE PAPER

SASE —
ユーザーの場所を問わず、クラウドで提供されるセキュリティをあらゆる場所で実現



概要

事業を運営し、リモートユーザーやモバイルユーザーといった分散したワークフローをサポートするため、企業ネットワークはクラウドベースのアプリケーションへの依存度を高めています。これらのクラウドサービスへのアクセスを求めるユーザーの急増に対応し、さらに従来のコアネットワークからだけでなく、新たに自宅や支社といったリモートのエッジからもアクセスできるようにするため、企業は従来のエンタープライズネットワークを急速に拡張する必要に迫られています。

オンネットワークとオフネットワークのハイブリッドで働く従業員は、多様なデバイスを使用して、さまざまな場所から重要リソースにアクセスします。この新たな働き方によってネットワークが再定義されたために、攻撃対象領域が広がり、その管理と保護がインフラチームの課題となっています。SASE(Secure Access Service Edge)ソリューションは、ネットワーキングとクラウドで提供されるセキュリティサービスを単一の統合パッケージに集約するように設計されています。これによって、すべてのネットワークエッジとリモートユーザーの間で、いつでも、どこでも、柔軟で安全なアクセスが可能になります。

しかし、SASE のソリューションは、拡張されたネットワークの一部として機能する必要もあります。クラウドのみのソリューションは、組織が直面している課題を部分的にしか解決しません。つまり、より大局的で集約 / 統合されたセキュリティフレームワークの一部として SASE を設計し、提供する必要があります。

「お客様は、ハイブリッドワーキングに最適なセキュリティツールに、シンプルさ、拡張性、柔軟性を兼ね備え、遅延の少ない広範なセキュリティ機能の融合を求めています」[1]

「デジタルトランスフォーメーションをサポートするために、ビジネスの俊敏性を強化してリモートアクセスを保護する必要があり、SASE モデルを採用しました」[2]

SASE の定義

SASE は、ビジネスアプリケーションのクラウドファーストの取り組み、特にオフネットワークでの作業が増えている従業員をサポートするために設計されています。SASE ソリューションは、常に進化し続ける環境におけるビジネス継続性を確保しつつ、分散したネットワークや多様な場所で働く従業員に一貫したセキュリティ機能を提供することによって、デジタルイノベーションを可能にします。その結果として、ビジネス継続性が高まり、クラウドアプリケーションへの一貫した安全なアクセスが可能になり、ユーザーエクスペリエンスが向上します。

SASE は、安全で柔軟な接続を提供するだけではありません。企業が設備投資を抑制し、デジタルイノベーションに伴うセキュリティインフラの複雑さを軽減できるようにも設計されています。また、従来の多くの SD-WAN ソリューションによって生じた接続とセキュリティのギャップを解消するための支援として、WAN とクラウドのエッジに実績のある統合されたセキュリティを提供します。

適切な SASE ソリューションは、インフラの管理者が既存のセキュリティインフラへの投資によって実現した価値を拡張できるようにするため、クラウドでも同じセキュリティソリューションを提供します。そのためには、共通のセキュリティソリューションと、あらゆるエッジに展開可能な拡張性の高いアーキテクチャを中心として、SASE ソリューションを構築する必要があります。これによって、従来の環境の安全を確保するために使用される保護機能をテレワークのユーザーにまで拡張し、ネットワークのシンエッジを保護します。また、クラウドで提供されるアクセス制御は、より大局的なアクセス戦略において一貫性を持ち、統合される必要があります。

人々が働く環境はネットワーク全体に及ぶため、クラウドベースのソリューションだけですべてに対応できることはほとんどありません。一般的に、SASE は「クラウドで提供されるサービス」という観点から説明されます。しかし、SASE が真に効果を発揮するためには、クラウドベースのソリューションと物理ネットワークの統合に依存するネットワーク環境もサポートする必要があります。一貫したシームレスな機能とポリシーの適用をエンドツーエンドで実現するには、SASE のクラウド接続を、ネットワークアクセス制御、無線 LAN コントローラー、支社の Wi-Fi アクセスポイント、そして進化するネットワークエッジに展開される多様なセキュリティツールと組み合わせる必要があります。

つまり、堅牢な SASE ソリューションには、クラウドベースの基本的な保護機能に加えて、ユニバーサルアクセス、ネットワークセグメンテーション、コンプライアンス要件などとの相互運用性が求められます。これらの課題は、クラウドベースのセキュリティソリューションだけで対応できるものではありません。もし実際にクラウドベースのセキュリティソリューションだけで対応するとなると、物理ネットワーク上のトラフィックをすべてクラウドに転送して、インスペクションを実行することが必要になってしまいます。

SASE ソリューションの主な要素

大方のネットワークソリューションは、リモートのユーザー、オフィス、エンドポイントのワークフローに対応するスピードで進化してきました。しかし、ほとんどのセキュリティツールとソリューションはこれに追いついておらず、一貫したセキュリティや、オンプレミスとリモートユーザーの最適なユーザーエクスペリエンスを提供できていません。

たとえば、仮想プライベートネットワーク（VPN）のみのソリューションは、最低限の保護しか提供しません。このため、侵害されたユーザーやデバイスがネットワークにアクセスした場合に、攻撃者やマルウェアによるラテラルムーブメント（水平移動）が起きるリスクが残ります。侵害された可能性のあるユーザーがクラウドベースのアプリケーションに直接アクセスしようとする場合にも、この問題の深刻さは変わりません。残念ながら、企業におけるセキュリティのステークホルダーにとっては、分散したネットワークのセキュリティのために、まとまりのない分散したツールを寄せ集めて使用しなければならない状況が課題となっています。そのような場合に使用されるのは、ネットワークから完全に隔離され、また相互に連携することのないツールであることが珍しくありません。急速なデジタルイノベーションに伴ってベンダーやソリューションが乱立し、その状況はポイントセキュリティ製品のサイロ化に如実に現れています。このために、管理と制御がさらに複雑化します。

一般的な企業では、分散環境で平均 45 のセキュリティソリューションを展開しています。[3]

このように分散したばらばらなソリューションを管理し、関連付けることは、すでに多大なタスクを担っているセキュリティチームにとっては非常に重い負担となります。そのため、オンネットワークとオフネットワークのハイブリッドで働く従業員に統一されたセキュリティポリシーを適用することが、ほとんど不可能になっています。企業が競争力を維持しつつ、進化する脅威に対応するためには、すべてのエンドポイントを、一貫性のある統合されたセキュリティとネットワーキングのポリシーにより保護し、管理する必要があります。そのようなポリシーは、場所を問わずネットワークユーザーすべてに適用できるものでなければなりません。

適格なベンダーはごく少数

オフネットワークのリモートユーザーや、シンエッジのオンネットワークユーザーに対し、一貫したセキュリティが提供されていない場合には、セキュリティの課題が生じます。SASE は、この課題を解決するという概念の下に設計されています。SASE は、オンプレミスかリモートを問わず、分散した動的なネットワークの制御とセキュリティのニーズに対応することを目的としています。しかし、企業が実際に必要とするレベルのセキュリティと WAN の統合を提供するように設計された、包括的ソリューションを提供する能力を有する SASE ベンダーはごくわずかです。

たとえば、SASE のみのベンダーを使用して包括的セキュリティ戦略を策定しようとしても、複数のセキュリティベンダーが提供する個別のツールを継ぎ接ぎしたソリューションになりがちです。さらに悪いことに、多くの場合に、既存のネットワークに展開されているツールとは異なるものになってしまいます。このようなアプローチは、コストがかかるだけでなく、SASE で中核となる「展開や管理を簡素化しながら場所を問わず一貫したセキュリティを提供する」という意図を打ち消すものです。

SASE ソリューションはクラウド経由で提供されるものですが、このような課題を回避するには、既存の WAN セキュリティ機能の延長線上で機能することが求められます。WAN エッジで展開されるセキュリティソリューションは、実績があり、認定され、企業の他のセキュリティフレームワークとネイティブに相互運用するように設計されていることが必要となります。この条件を満たさない SASE は、ハイブリッドに働く今日の従業員が直面している課題に十分に対応できません。アクセスを可能にするものの、ユーザーとサービスを孤立させ、ネットワーク全体の可視性と制御を妨げることになるからです。

[1] 「The Future of Network Security Is in the Cloud」、Frank Marsala 著、Gartner、2019 年 9 月 13 日（英語）：https://www.gartner.com/en/documents/3957375

[2] 「The SASE Model: What's Driving Adoption?」、Geetha Nandikotkur 著、Data Breach Today、2020 年 8 月 31 日（英語）：https://www.databreachtoday.co.uk/sase-model-whats-driving-adoption-a-14919

[3] 「The more cybersecurity tools an enterprise deploys, the less effective their defense is」、Charlie Osborne 著、ZDNet、2020 年 6 月 30 日（英語）：https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ