FORTINET

WHITE PAPER

フォーティネットが提供する最も柔軟な SASE ソリューション

概要

デジタルイノベーション、クラウドの導入、そして最近のテレワークへの移行により、ネットワークは根本的な変化を遂げました。また、SaaS（Software-as-a-Service）アプリケーションやデータセンターからマルチクラウド環境に移行されたデータなど、クラウドベースのリソースへの依存度が高まっている中、ネットワークアクセスを保護する新しいアプローチの必要性（特に、レガシーネットワークアーキテクチャに内在する「暗黙の信頼」という課題）が明らかになっています。

今日の組織が必要としているのは、場所、デバイス、時間を問わず、ビジネスクリティカルなアプリケーションをはじめとするネットワークとクラウドベースのリソースやデータに、中断なく即時にアクセスできることです。デジタルイノベーションの取り組みによって多くの課題（動的に変化するネットワーク構成や攻撃対象領域の急速な拡大など）が生じていますが、これは多くの従来型セキュリティソリューションが組織やユーザーが必要とするレベルのセキュリティとアクセス制御を提供できなくなっていることを意味します。

「お客様は、WAN のエッジネットワークセキュリティ市場において、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]

SASE（セキュアアクセスサービスエッジ）は、ネットワークセキュリティ機能と WAN 機能を統合する新しい企業戦略です。SASE が目指しているのは、今日の企業の常に変化するセキュアアクセスのニーズをサポートすることであり、これはフォーティネットが長年積極的に開発し推進してきたセキュリティドリブン ネットワーキング戦略と一致します。SASE は、WAN エッジ、クラウドエッジ、データセンター（DC）エッジ、コアエッジ、そして急増するテレワーカーが使用するエンドポイントデバイスなど、あらゆる場所にセキュリティを提供する上で重要な役割を果たします。

SASE の正確な定義とは

他の新しいテクノロジーのカテゴリーと同様に、SASE ソリューションの正確な定義については依然として曖昧な点があります。クラウドベースのサービスなのか、それとも物理的なソリューションも含まれているのでしょうか。SASE ソリューションには、どのようなテクノロジーが関係しているのでしょうか。

SASE はクラウドで提供されるサービスとして分類されるのが一般的ですが、SASE をネットワークへと効果的に統合するには、物理ソリューションとクラウドベースソリューションの組み合わせが必要になる場合があります。たとえば、SASE 接続とネットワークアクセス制御、およびテレワーカー向けのエッジセキュリティデバイスを組み合わせて、物理的な SD-WAN デバイス（特にフルスタックのセキュリティ機能を搭載したデバイス）をサポートしたり、支社に設置されている無線 LAN コントローラや Wi-Fi アクセスポイントなどのテクノロジーと SASE 接続を統合する必要もあります。

したがって、堅牢な SASE ソリューションは、クラウドベースの基本的な保護機能に加えて、ネットワークセグメンテーションや、コンプライアンス要件などをサポートする必要があります。しかし、クラウドベースのセキュリティがこれらの要件に対応するには、トラフィックをクラウドに送信して検査しなければなりません。こういった理由から、フォーティネットは、SASE の導入配備に最適な、クラウドと物理デバイスの両方の統合と展開を可能にする包括的で柔軟なソリューションを提供します。

SASE の目的はセキュアアクセス

SASE の概念を説明するならば、「革新的ネットワーキングソリューションを実現しながらも、その一部として統合型セキュリティを提供できなかった SD-WAN ベンダーによってもたらされたセキュリティの課題を解決しようとする試み」だと言えるでしょう。フォーティネットは、完全統合されたセキュア SD-WAN ソリューションでこの課題を真正面から解決しました。このソリューションは、他のベンダーでは実現できなかった堅牢な統合ネットワークとセキュリティ機能の両方を提供するものです。これらはすべて、私たちが長年お客様に提供してきたセキュリティドリブン ネットワーキングおよびセキュリティ ファブリック プラットフォーム戦略の一環です。

フォーティネットは、市場で最も幅広い物理およびクラウドベースのセキュリティソリューションを通じて、完全統合型の SASE ソリューションを支援します。それを可能にしているのは、以下の基本的なセキュリティ要素です。

- **万全の機能を備えた SD-WAN ソリューション：**SASE ソリューションの中心である SD-WAN には、動的なパス選択、自律型 WAN 機能、ビジネスアプリケーションの一貫したアプリケーション / ユーザーエクスペリエンスなどが組み込まれている必要があります。

- **物理 NGFW（次世代ファイアウォール）またはクラウドベース FWaaS（Firewall-as-a-Service）：**SASE では、物理およびクラウドベースの導入形態に対応する、フルスタックのセキュリティ機能も不可欠です。たとえば、テレワークを採用している組織では、エッジセキュリティと内部セグメンテーションを組み合わせて、アクセスを制限している企業ネットワークリソースに、ゲストや IoT の脅威がアクセスしないようにする必要があります。また、これにクラウドベースのセキュリティを組み合わせて、オンラインまたはクラウドのリソースへのアクセスを制御します。プロセッサが強化された物理ハードウェアと、拡張性に優れたクラウドネイティブのセキュリティは、大規模でも高いパフォーマンスを発揮するので、最大限の柔軟性とセキュリティが実現します。
- **ゼロトラストネットワークアクセス（ZTNA）：**ユーザーとデバイスを識別し、アプリケーションに対する認証に使用されます。ZTNA は製品というより戦略に近いものであるため、いくつかのテクノロジーが連携して機能します。多要素認証（MFA）は、すべてのユーザーを識別します。ZTNA には、物理的な面ではセキュアな NAC（ネットワークアクセス制御）、アクセスポリシーの適用、およびネットワークリソースへのアクセスを制限する動的なネットワークセグメンテーションとの統合が組み込まれています。クラウドに関して言えば、ZTNA はユーザー間のセキュアな水平通信のためのトラフィックインスペクションを提供するマイクロセグメンテーションや、ネットワーク内部および外部のデバイスに対する常時稼働のセキュリティをサポートしています。物理およびクラウドベースの ZTNA サービスを組み合わせることで、デバイスとユーザーがオンネットであるかオフネットであるかを問わず、セキュアなアクセスとポリシーの適用が保証されます。
- **セキュア Web ゲートウェイ：**インターネットセキュリティやコンプライアンスポリシーの適用、そしてフィルタリングによる悪意のあるインターネットトラフィックの排除を通じて、オンラインのセキュリティに対する脅威からユーザーとデバイスを保護するために使用されます。また、Web アクセスの利用規定を適用し、法規制や業界標準へのコンプライアンスを確保し、データ漏洩を防止することもできます。
- **CASB：**クラウドベースの CASB サービスを使用する組織は、アプリケーションへのアクセス保護やシャドー IT の問題の解決など、SaaS アプリケーションの制御が可能となります。CASB とオンプレミスの DLP を組み合わせて、包括的な情報漏洩対策を確立する必要があります。

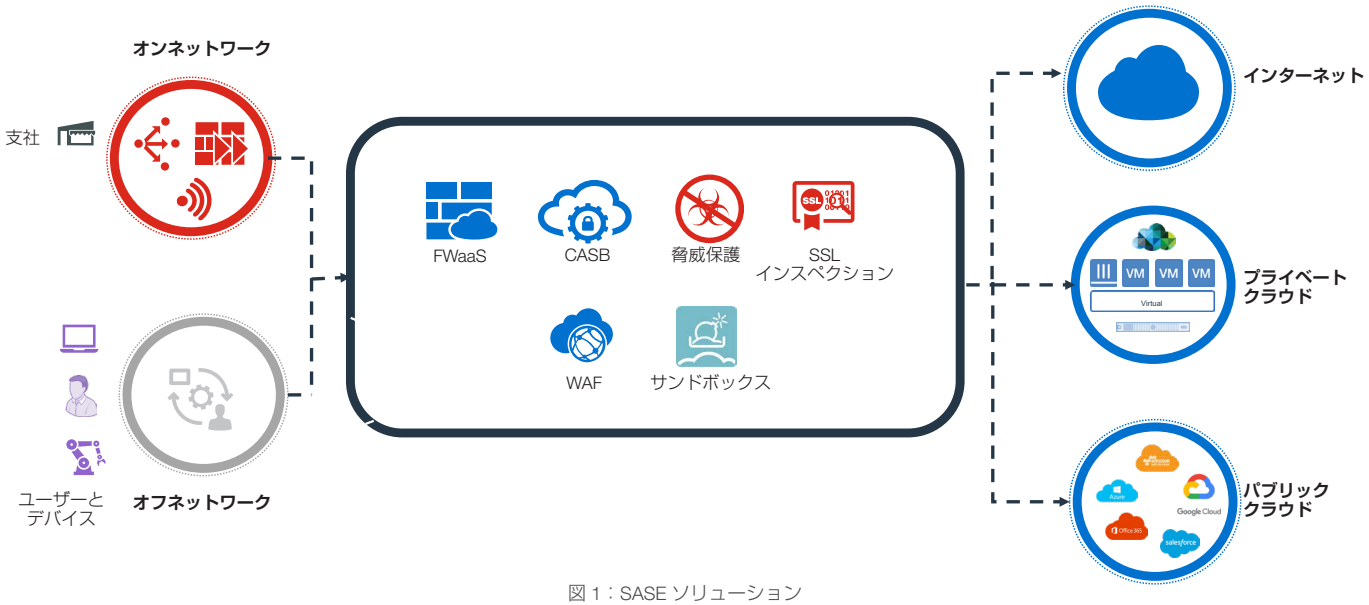

図 1：SASE ソリューション

テクノロジーの追加で SASE を強化

SASE は、デジタルイノベーションを強化し支援するように設計されています。しかし、SASE アプローチを総合的に検討しなかった場合、分離した別のセキュリティソリューションを導入して、その他のセキュリティアーキテクチャとは別に管理しなければならなくなる可能性があります。そのような状況では、ネットワーク全体の可視性と制御の両方が大幅に制限されかねません。そこでフォーティネットは、堅牢な SASE ソリューションに必要な中核的要素に加えて、SASE ソリューションを利用するユーザーとデバイスのセキュリティを拡張し、強化するように設計されたオプションのツールも提供します。これらのツールを使用することで、より大規模なセキュリティ ファブリックにソリューション全体をシームレスに統合できます。

たとえば、エンドポイント保護（EPP）や EDR（Endpoint Detection and Response）テクノロジーなどのエンドポイントセキュリティによって、SASE を利用するデバイス自体のセキュリティが保証されます。高度な仮想プライベートネットワーク（VPN）は、セキュアなデータ転送とトランザクションを提供すると同時に、相互接続する必要があるリモートオフィスやユーザーが数百、数千に及んだ場合に複雑化する環境を管理します。また、セキュアな Wi-Fi コントローラと LAN コントローラを追加することで、ネットワークを出入りするトラフィックは必ず追加の検査レイヤーを通過するようになります。

組織毎にニーズは異なるとはいえ、包括的なネットワーク / セキュリティソリューションがより優れたビジネス成果を提供するのにもかかわらず、SASE の「中核」と見なされるテクノロジーだけを採用することは論理的ではありません。

将来性の高さに反して、不足する適切なベンダー

SASE は、今日の組織が直面するアクセス制御とセキュア WAN の課題に対処するように設計されていますが、完全な SASE ソリューションを提供できるベンダーがほとんどいないという問題があります。たとえば、ツール（特にセキュリティコンポーネント）がテスト済または認定済のベンダーはほとんど存在しません。つまり消費者は、購入を予定しているセキュリティサービスが実環境で保護してくれるかどうかを知る方法がないということです。

これは、高度に専門化したサイバーセキュリティ分野においても深刻な問題として受け止められています。この分野のベンダーは、自社ソリューションが業界の期待に応えられない場合、第三者機関によるテストと検証をオプトアウトすることがあります。ベンダーが提供する SASE ソリューションのセキュリティエクスペリエンスが最低限のレベルであるにもかかわらず、今日話題のマーケティング用語である「SASE」を利用しようとした場合、この問題は一層深刻化することになります。

フォーティネットの優位性

フォーティネットには、SASE 戦略に関する質問がしばしば寄せられます。SASE が効果的に機能するには、そのすべてのコンポーネント（接続性、ネットワーク、セキュリティの構成要素）が統合された 1 つのシステムとして連携する必要があります。これは、フォーティネットにとって目新しい話ではありません。というのも、フォーティネットは統合されたセキュリティプラットフォームとセキュリティ ファブリックのアーキテクチャを構築し、その一部として長年にわたり核となる SASE 要件（およびその他多くの要件）に応えてきました。これにより、セキュリティドリブン ネットワーキングのアプローチの一環としてネットワーキングとセキュリティ機能の真の融合が実現し、保護機能を損なうことなくデジタルイノベーションが短期間で加速します。SASE の実装を検討しているフォーティネットのお客様の多くは、（微調整は必要ですが）セキュリティ ファブリックのおかげですでに SASE ソリューションが導入済みであることに気付いています。

SASE は大きな問題の解決に尽力しています。しかし、これはフォーティネットが過去に対処したのと同じ種類の問題です。

- フォーティネットは、セキュリティを SD-WAN に完全統合した最初の大手セキュリティベンダーです。これは、フォーティネットが長年にわたるセキュリティとネットワーキングの経験を単一の統合ソリューションへと集約することによって実現したものです。
- さらにフォーティネットは、ネットワーキングとセキュリティ機能を加速させ、最も要求の厳しい今日のネットワーク環境で必要とされるレベルのパフォーマンスを提供するように設計された、世界初の SD-WAN プロセッサを開発しました。
- フォーティネットは、自社のセキュリティツールが現在業界で最も多くのテストや検証を実施され、認定を受けたソリューションであることに誇りを持っています。

これは、お客様が必要とする種類の SASE ソリューションを提供することが、すでにネットワークとセキュリティに対するフォーティネットのアプローチの一部となっていることを意味します。また、幅広い高度な接続性とセキュリティテクノロジーでソリューションをカスタマイズできるため、要件の変化に応じて SASE ソリューションを適応させることができます。フォーティネット セキュリティ ファブリックは、オンプレミスかクラウドかに関係なく、導入する他のソリューションとの統合と接続が可能です。そして、これらの要素はすべて、フォーティネットの一元管理システムから管理が可能であるため、SASE 環境を含むネットワーク全体で広範な可視化ときめ細かい制御が保証されます。

フォーティネットは、ネットワーク全体で場所を問わず（WAN やクラウドエッジだけでなく、DC エッジ、コアネットワークエッジ、エンドポイントエッジにも同様に）一貫したセキュリティを提供し、シームレスな接続、可視化、および制御を可能にする完全な SASE ソリューションを提供できる独自の地位を確立しています。

フォーティネットは、今日 SASE を取り巻く市場が活況を呈していることを大変嬉しく思います。この状況は、フォーティネット セキュリティ ファブリックのアプローチの正当性を立証するものであり、長年のフォーティネットの主張が改めて確認されることになったと言えます。クラウド接続とデジタルイノベーションの時代を迎えた今、ネットワークとセキュリティは融合する必要があります。サイロ化された時代遅れのアーキテクチャに戻ることはできません。SASE の時代、そしてその先に向けて設計されているソリューション、それがフォーティネットです。

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

フォーティネットジャパン株式会社

〒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

WP-SASE-Solution-202009-R1