WHITE PAPER

# SASE によるハイブリッドワークのサイバーセキュリティの統一

## ユーザー、デバイス、拠点、アプリケーションを保護する画期的アプローチ

## 概要

企業は、さまざまな場所やデバイスからネットワークリソースにアクセスする WFA（Work From Anywhere：場所に縛られない働き方）の従業員を継続的にサポートし、保護する必要があります。WFA の保護が極めて重要なのは、リモート・ネットワーク・アクセスには複雑性と脆弱性が伴うため、進化し続けるサイバー脅威からの保護を可能にする堅牢なセキュリティソリューションが必要になります。

リモートワークの増加やデジタル脅威の急増に伴い、一貫性のあるポリシーの適用、クラウドリソースへのシームレスなアクセス、一元管理などの課題への対応を可能にする、包括的なセキュリティのアプローチが必要とされるようになりました。SASE（セキュアアクセスサービスエッジ）ソリューションは、ネットワーキングとセキュリティの機能をクラウドネイティブプラットフォームに統合することで、ハイブリッドワーカーのセキュリティを統一する画期的なアプローチを提供します。SASE は、ネットワーク環境に関係なく、ユーザー、デバイス、拠点、アプリケーションを保護します。

**エグゼクティブの 73％が、リモートワークでより重大なセキュリティリスクがもたらされると考えている。[1]**

SASE は、従来のネットワーキングとセキュリティのソリューションとは異なり、クラウドベースの SSE（セキュリティサービスエッジ）とオンプレミス SD-WAN、統合セキュリティサービス、ゼロトラストアクセス、一元的な管理と監視などの多くの機能を提供します。この包括的ソリューションにより、組織は、セキュリティ態勢を強化し、業務効率を向上させ、場所やデバイスに関係なく、すべての従業員の安全で生産的な作業環境をサポートできるようになります。SASE は、リモートワークの導入を支援しつつ、関連するリスクを効果的に減災する、ハイブリッドワークセキュリティの未来を提示する概念です。

## ハイブリッドワークのサイバーセキュリティの複雑さを解消

ハイブリッドワークの拡大により、組織には、オンサイトとオフサイトからネットワークやアプリケーションにアクセスする従業員の保護が求められるようになりました。WFA（場所に縛られない働き方）への移行により、攻撃対象領域が大幅に拡大し、在宅勤務やモバイルワークの従業員が増加したことで、ネットワーク、アプリケーション、リソースのセキュリティが複雑化することになりました。

多数のリモートオフィスや WFA の従業員を抱える組織にとって、セキュリティポリシーの一貫性のある適用を可能にし、ネットワークの場所に関係なく、最適なユーザーエクスペリエンスを従業員に提供するのは、多くの場合に困難です。このような WFA 環境の保護が固有の課題であるのは、これらの変化が、綿密に計画された戦略に沿ってではなく、組織的に発生したものであるためです。

新しいネットワークエッジが急速に拡大し、独立プロジェクトとして実装されることが多い WFA の従業員が新たに加わったことで、多くの脆弱性が表面化し、サイバー犯罪者に次々と悪用されるようになりました。さらには、このトレンドにより、組織におけるユーザー、デバイス、アプリケーションの可視性が低下し、脅威とセキュリティギャップが拡大しています。

SASE アーキテクチャは、大小規模の支社やリモートのユーザーにセキュアアクセスと高パフォーマンスの接続を提供することで、これらの課題の解決を支援します。しかしながら、多くの SASE ソリューションで解決できるのは、一部の問題だけです。SASE ソリューションの多くは、一貫性のあるエンタープライズクラスのセキュリティをハイブリッドワーカーに提供できなかったり、ネットワークエッジに展開された多様な物理 / 仮想のネットワークツールやセキュリティツールとシームレスに統合できなかったりします。結果として、一貫性のあるサイバーセキュリティや最適なユーザーエクスペリエンスを提供することができません。

## SASE によるユーザー、デバイス、拠点の保護の統一

SASE のアプローチは、セキュリティやネットワーキングの多様な機能を単一のクラウドネイティブプラットフォームに統合することで、ネットワークセキュリティのトランスフォーメーションを可能にします。SASE の中核となる理念の 1 つは、場所やネットワーク環境に関係なく、ユーザー、場所、アプリケーションの保護を可能にすることです。

### ユーザーと拠点の保護

SASE により、オフィスあるいはリモートのどちらであっても、ユーザーが一貫した方法で保護されます。SASE はさらに、ユーザーがネットワークリソースにアクセスする、支社 / 拠点や自宅、コーヒーショップ、空港などのリモートのあらゆる場所にセキュリティ保護を拡張します。

### アプリケーションアクセスの保護

今日のデジタル環境では、アプリケーションは、データセンター、パブリッククラウド、SaaS（Software-as-a-Service）プラットフォームなどのさまざまな環境に存在します。SASE により、あらゆるホスティング環境のアプリケーションにアクセスするすべてのユーザーをサイバー脅威やデータ漏洩から保護できるようになります。SASE ソリューションは、CASB（クラウドアクセスセキュリティブローカー）機能、ZTNA（ゼロトラストネットワークアクセス）、SD-WAN のインテリジェントなルーティングとステアリングなどの機能を統合することで、SaaS とレガシーアプリケーションのどちらも包括的に保護します。

### 統合型のセキュリティプラットフォーム

SASE の中核である統合型のセキュリティプラットフォームは、NGFW（次世代ファイアウォール）、SWG（セキュア Web ゲートウェイ）、ZTNA、セキュア SD-WAN などのさまざまなセキュリティサービスのシームレスな統合を可能にします。この統合型のアプローチにより、組織は、セキュリティポリシーと多くのエージェントを統合し、導入と管理を簡素化し、セキュリティのサイロと死角を解消することで、攻撃対象領域を縮小することができます。

### 拡張性と柔軟性

SASE ソリューションは、現代の企業の進化するニーズに合わせた動的な拡張を想定して設計されています。SASE プラットフォームは、小規模の支社 / 拠点あるいは世界中に分散する従業員のどちらをサポートする場合であっても、変化するビジネス要件に適応する拡張性と柔軟性を提供します。これにより、あらゆる規模、あらゆる業種、あらゆる地域の組織が、一貫性のあるセキュリティ態勢を維持できます。

**リモートワークへの移行と同時に、フィッシング、スミッシング、ランサムウェアなどのサイバーセキュリティの脅威が急増した。従業員が 500 人以下の組織のデータ侵害の平均コストは 331 万ドルであり、データ侵害あたりの最終的なコストがすぐに判明することはない。[2]**

### ユーザーエクスペリエンスの最適化

セキュア SD-WAN でオンプレミス WAN を強化し、保護することで、接続、オペレーション、アプリケーションアクセスが改善されます。このトランスフォーメーションにより、あらゆるユーザーエクスペリエンスが大幅に改善されます。セキュア SD-WAN と SSE の統合により、アプリケーションがインテリジェントかつ動的に適切なリンクにステアリングされるため、ビジネスの生産性とユーザーエクスペリエンスの品質が保証され、リモートユーザーが優れたユーザーエクスペリエンスで安全かつ効率的に企業アプリケーションにアクセスできるようになります。

## SASE ソリューションの主な要素

ほとんどのネットワークソリューションが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できるスピードで進化してきたのに対し、ほとんどのセキュリティツールとソリューションはそのスピード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。

従業員がさまざまな場所やデバイスからアプリケーションに安全にアクセスする必要がある、今日の進化し続ける WFA 環境において、VPN では必要とされるセキュリティと柔軟性を提供することはできません。リモートアクセスとハイブリッドワークセキュリティの新しいソリューションとして登場した SASE は、セキュリティの包括的アプローチを提供します。

効率的な SASE ソリューションは、NGFW、SWG、ZTNA、CASB、RBI（リモートブラウザ隔離）、DLP（データ漏洩対策）、エンドツーエンドの DEM（デジタルエクスペリエンスモニタリング）などの複数のセキュリティ機能と SD-WAN を単一の統合プラットフォームに統合します。この統一されたクラウドネイティブアーキテクチャにより、ネットワークインフラストラクチャ全体でのセキュリティスタックの統合、管理の簡素化、ユーザーエクスペリエンスの最適化、一貫性のあるセキュリティが実現し、可視性が向上します。さらには、社内や SaaS のアプリケーションやインターネットへのセキュアアクセスを可能にし、あらゆるタイプの脅威からの完全な保護を可能にします。

SASE ソリューションは、ゼロトラストセキュリティモデルと単一の統一されたエージェントを採用する必要があり、ネットワークリソースへのアクセスを厳格に認証して承認し、継続的な検証をするメカニズムも必要です。組織は、ゼロトラストアプローチを採用することで、ネットワークインフラストラクチャ内のインサイダーの脅威、不正アクセス、ラテラルムーブメントのリスクを低減できます。

SASE ソリューションは、AI を活用した包括的な脅威インテリジェンスフィードと分析の内蔵により、高度な脅威をリアルタイムで特定

して減災します。機械学習、振る舞い分析、脅威インテリジェンスの共有を活用することで、マルウェア、ランサムウェア、フィッシング、ゼロデイエクスプロイトなどのさまざまなサイバー脅威からのプロアクティブな防御が可能になります。

SASE ベンダーは、組織の SASE への移行を支援し、組織のアーキテクチャやニーズに常に適応できるソリューションを提供する必要があります。そのため、SASE は、SD-WAN を利用する大規模の支社 / 拠点から LAN 接続のみの小規模の拠点、さらには世界中のリモートの拠点までのあらゆる場所のすべてのユーザーを保護し、一貫性のあるユーザーエクスペリエンスとセキュリティを提供する必要があります。

## 終わりに

SASE は、単にハイブリッドワーカーの直近のセキュリティの問題を解決するだけではなく、拡張性、柔軟性、俊敏性を提供することで、現代の企業の進化するニーズに対応します。SASE は、セキュリティポリシーの統合、導入の簡素化、可視性の向上により、IT チームのセキュリティ態勢を強化し、安全で生産性の高い作業環境をサポートします。

ハイブリッドワークセキュリティの未来を体現する SASE は、ネットワークインフラを保護し、WFA の従業員を強力にサポートし、デジタル時代の複雑さの問題に自信を持って対処するための統合プラットフォームを提供します。

[1]「Remote Work Statistics and Trends In 2024」、Kathryn Haan、Forbes、2023 年 6 月 12 日（英語）：
https://www.forbes.com/advisor/business/remote-work-statistics/

[2]「Zero Trust Security in the Age of Remote Work」、i4DM、2023 年 9 月 23 日（英語）：
https://www.linkedin.com/pulse/zero-trust-security-age-remote-work-i4dm/

**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