ハイブリッドワーカーに最適な SASE ソリューションの選択

目次

概要

社内、自宅、あるいはその中間地点など、従業員の勤務場所に関係なく、重要なアプリケーションやリソースに安全かつ認証に基づいてアクセスできる環境は、現代の大半の組織で常に必要とされています。SASE（セキュアアクセスサービスエッジ）ソリューションは、信頼性と柔軟性に優れたソリューションを提供し、ハイブリッドの WFA（Work From Anywhere：場所に縛られない働き方）モデルへの恒久的な移行を可能にします。SASE ソリューションは、セキュアリモートアクセス、セッション / アプリケーションごとの高度な認証、エンタープライズクラスのセキュリティを、どこからでも利用できる単一のクラウドベースソリューションに結合し、従来の社内勤務で利用されている保護機能やパフォーマンスをリモートワーカーにまで拡張します。

ただし、SASE ソリューションはすべて同じではありません。アプリケーションごとのアクセス、セキュリティ機能、セキュリティの有効性などはソリューションによって大きく異なります。また、ハイブリッドネットワークを使用する組織では、管理すべきテクノロジーがさらに追加されることで、人員が不足している IT 担当者の負担が増える可能性があります。特に、問題の検知やユーザーエクスペリエンスの最適化のために、エンドツーエンドで環境を管理しようとすればなおさらです。自社環境に適した SASE を評価する場合、複数のコアユースケースを調べ、さまざまな重要機能を慎重に検討する必要があります。

現代のハイブリッドワーカーによるサイバーセキュリティへの影響

大多数のビジネスにとって、ハイブリッドワーカーは新しい現実となっています。常に自宅で仕事をしている従業員の割合は、世界各国で昨年から倍増しています[1]。ある調査によると、ビジネスおよび IT リーダーの 83% がハイブリッドワークを今後の事業運営の中心として捉えており、42% はパンデミックの収束後も従業員の半数以上が常時ハイブリッド方式の勤務を続けると見ています[2]。

現代のビジネスにおけるもう一つの実態として、効率性、コスト削減、柔軟性を強化するため、クラウドに移行されるアプリケーションやサービスが増加しています。アプリケーションソフトウェア、インフラストラクチャソフトウェア、ビジネスプロセスサービス、およびシステムインフラストラクチャ市場では、2025 年までに全消費の半分がクラウドに移行するでしょう[3]。

ただし、サイバーセキュリティチームにとっては、こうした事業運営の急激な変化によって新たな問題が生じています。最近の調査によると、セキュリティおよびビジネスリーダーの 80% が、リモートワークが原因で組織はより多くのリスクにさらされていると感じています[4]。それを裏付けるデータもあります。昨年は攻撃総数が 31% 増加しましたが、これはサイバー犯罪者がビジネスネットワークの急激な変化を悪用しようとした結果です[5]。昨年はデータ侵害の成功件数も増加し、過去の年間記録を 23% 上回りました[6]。

このように問題が増加している原因の多くは、現在の課題への対処がまったく考慮されていない旧式または不十分なセキュリティにあります。たとえば、多くの企業は、新型コロナウイルスのパンデミックが発生してから数週間以内に、従来の VPN（仮想プライベートネットワーク）による接続ではリモートワーカーの増加に対応しきれないことに気づきました。VPN では規模に応じた運用が意図されておらず、結果的にセキュリティの問題が発生しました[7]。VPN は多数のリスクも伴います。特に、ネットワーク構成が不完全な場合はなおさらです（コロニアル・パイプラインへの攻撃は、まさにそうした VPN を経由して実行されたものです）[8]。さらには、クラウドへの認識不足やセキュリティの迂回によって、別のセキュリティギャップも生まれてしまいます[9]。

急速に進化する今日のハイブリッドな職場環境を保護するには、SASE ソリューション戦略のように堅牢で目的に応じたセキュリティが求められます。

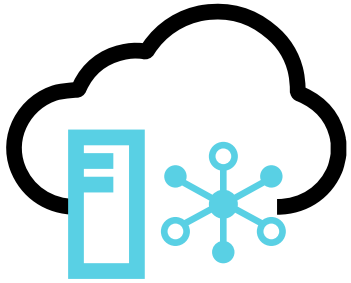
職場環境のハイブリッド化、新しい接続オプション、ビジネスクリティカルアプリケーションのクラウドへの追加配備などにより、あらゆる組織の攻撃対象領域は急拡大しています[10]。

単一ベンダーによる SASE アプローチ

あらゆる場所でユーザーに安定した接続とセキュリティを提供するには、ネットワーキングソリューションとセキュリティソリューションをエッジとクラウド内でコンバージする必要があります。最も基本的なレベルの SASE は、複数の NaaS（Networking-as-a-Service）機能と SaaS（Security-as-a-Service）機能を 1 つのソリューションに結合します。異なるベンダーのソリューションを統合しようとしても、このような結合は上手くいきません。しかし、プラットフォームを中心とした単一ベンダーの SASE ソリューションなら、テクノロジーを統合し、ネットワーキングとセキュリティの機能をコンバージして運用効率を向上させることができます。ただし、SASE ソリューションは独立した存在ではありません。安全で信頼できる接続を確保し、場所を問わず必要に応じて優れたユーザーエクスペリエンスを提供するには、大規模なネットワーキング / セキュリティアーキテクチャへのシームレスな統合が可能な SASE ソリューションを見つけることも、組織にとっては重要です。

新たなチャンス到来のときにはいつもそうであるように、緊急のニーズに応えて新市場の一角を占めようとするベンダーが必ず出現します。しかし、そうしたソリューションの多くは期待どおりの効果を上げておらず、なかには未成熟なテクノロジーや不適切な機能に依存しているものもあります。その多くは独立したスタンドアロンソリューションとして動作し、既存のセキュリティテクノロジーや拡大を続けるハイブリッドネットワークと連携していません。組織がシームレスなソリューションを構築し、ソリューションを複雑化するのではなく合理化するのに役立つ製品はほとんどありません。

また、急速に拡大し変化し続けるハイブリッドネットワークを管理する組織では、管理すべきテクノロジーがさらに追加されることで、人員が不足している IT 担当者の負担が増える可能性があります。多数の SASE ベンダーで使用されている手作業による制御やスクリプト、そして不十分な脅威インテリジェンスは、変化の激しい今日の脅威についていくことができないため、組織は脆弱な状態に置かれることになります。



SASE の真の目的は、クラウドソフトウェアとネットワーキングツールのコンバージェンスによって、より適切な方法でサイバーセキュリティテクノロジーを提供することです[11]。

ソリューションの選択：検討事項

重要な機能を評価し、リモートワーカーの保護に最適な SASE ソリューションを選択する場合、7 つの重要な検討事項があります。

1. 単一ベンダーの SASE アプローチ

異なるベンダーのソリューションを統合型 SASE アーキテクチャとして連携させようすると、構築が難しいうえに、保守やトラブルシューティングで多大な時間を要します。単一ベンダーの SASE アプローチでは、ネットワーキングとセキュリティをコンバージし、管理、最適化、およびポリシー適用のすべてを 1 つのインターフェイスで制御することができます。さらに、その単一ベンダーソリューションが分散ネットワークでの相互運用も可能で、クラウドとオンプレミスのデバイス間でシームレスに接続を切り替えることができれば理想的です。これにより、ネットワークのいずれか一方のエッジで接続や制御を終了する代わりに、アクセスおよびセキュリティポリシーによってユーザーとアプリケーションをエンドツーエンドで追跡することが可能になります。ビジネス環境全体でネットワーキングとセキュリティを正しくコンバージすることによってのみ、組織は包括的なゼロトラストアーキテクチャを実装し、一貫したセキュリティと優れたユーザーエクスペリエンスを場所を問わずに提供することができます。

2. 複数のユースケースに対応する統合型エージェント

ユースケースごとに異なるエージェントをオンボーディングしていると、保守業務は瞬く間に複雑かつ高額になってしまいます。効果的な SASE ソリューションは、ZTNA、CASB（クラウドアクセスセキュリティブローカー）、エンドポイント保護など複数のユースケースを単一のエージェントでサポートします。さらには、トラフィックを自動的にリダイレクトし、クラウドベースのセキュリティによってアセットとアプリケーションを保護します。

3. セキュアインターネットアクセス

リモートワークが新たな日常となる中、インターネットに直接アクセスするユーザーによって、組織の攻撃対象領域は大幅に拡大しています。有効なソリューションは、ユーザー（またはアプリケーション）をその所在にかかわらず追跡し、適切な機能を提供して保護できなければなりません。

クラウドベースのセキュリティソリューションには、暗号化トンネル（従来の VPN など）を上回る機能が求められます。また、トラフィックを検査し、既知および未知の攻撃を検知して対応するように設計された、エンタープライズクラスのセキュリティソリューションのポートフォリオを提供する必要があります。つまり、優秀な SASE ソリューションは、SWG（セキュア Web ゲートウェイ）機能が組み込まれており、データとアプリケーションを監視して Web ベースの攻撃から保護するほか、URL フィルタリング、DNS セキュリティ、フィッシング対策、アンチウイルス、アンチマルウェア、サンドボックス、ディープ SSL インスペクションなどの機能も備えています。

4. 柔軟なセキュアプライベートアクセス

柔軟な SASE ソリューションは、企業アプリケーションの配置場所がプライベートデータセンターであろうとパブリッククラウドであろうと、それらのアプリケーションへの安全なアクセスを提供します。統合型 ZTNA では、認証されたユーザーに対して、アプリケーションごとに明示的なアクセスが許可され、永続的なトンネルは不要です。ZTNA は ID とコンテキストに基づいてアクセスを許可し、継続的な検証を行うことで、ネットワーク上で誰が何を使用するかを効果的に制御します。SASE ソリューションは SD-WAN および NGFW ソリューションとシームレスに統合され、SASE PoP を通じてインテリジェントなステアリングや動的ルーティング機能を提供します。また、企業アプリケーションへの最短パスを自動的に検出して保護することで、優れたユーザーエクスペリエンスを実現します。これらすべての機能が単一のエージェントによって提供され、ZTNA、トラフィックリダイレクト、CASB、エンドポイント保護などに対応していれば理想的です。

5. セキュア SaaS アクセス

効果的な SASE ソリューションは、アプリケーション、デバイス、ユーザー、ワークロードの配置場所に関係なく、安全なアクセスを提供する必要があります。これは、キャンパス、拠点、自宅、モバイル環境の間を定期的に移動するハイブリッドワーカーにとって不可欠な機能です。SaaS アプリケーションに対する企業の依存度が高まっていることから、クラウドベースの効果的なセキュリティソリューションによってミッションクリティカルなデータも保護し、ユーザーがオンプレミスかオフプレミスかに関係なく、エンタープライズクラスのセキュリティでクラウドベースの情報を安全に保管しなければなりません。さらには、インラインと API ベースの両方の機能をサポートして、デュアルモードの CASB にも対応する必要があります。これにより、クリティカルデータを保護すると同時に、シャドー IT の課題を特定して解決します。以上を踏まえて、組織の SASE ソリューションには、主要な SaaS アプリケーションを可視化する、リスクのあるアプリケーションを通知する、きめ細かいアプリケーション制御によって機密データを保護する、アプリケーションに含まれるマルウェアを管理対象 / 対象外のデバイスで検知しこれに対処する、などの機能が求められます。

6. 柔軟な利用方法とオンボーディングの簡素化

SASE ソリューションを選択する際の検討事項はテクノロジーだけではありません。支払い方法も考慮する必要があります。適切な SASE を使用すれば、組織はビジネスにかかる費用を CapEx（設備投資）モデルから OpEx（運用費）モデルに移行することができます。効率的に移行するには、ソリューションにシンプルなライセンス体系が採用されており、組織が過剰なハードウェアに資本を投下することなく、ビジネスの成長に応じたコストや、セキュリティの利用状況を予測できなければなりません。

継続的なコスト削減が、オンボーディングの簡素化やエンドポイント管理システムの強化につながる可能性もあります。集中管理によって効率的な運用ときめ細かい分析が可能になり、事前生成されたオンデマンドレポートも利用できます。たとえば、ユーザー、エンドポイント、および VPN のイベントに関するログを作成し、効率的なトラブルシューティングを実行できます。

7. シンプルなクラウドベースの管理

クラウドベースの SASE 管理システムは、包括的な可視性、レポート作成、ロギング、および分析機能を提供します。これにより、セキュリティ運用が効率化されるとともに、平均検知時間（MTTD）と平均修復時間（MTTR）が短縮されます。ただし、SASE のセキュリティ要素が、サイロ化したポイントソリューションとして動作していると、セキュリティチームに不要な負担を強いる場合があります。特に、限られた IT 担当者でハイブリッド環境を管理している組織では、その可能性が高くなります。

クラウドに配置された SASE コンポーネントとオンプレミスのセキュリティソリューションがシームレスに連携すれば、統合機能はさらに強化され、一貫したポリシーをオーケストレーションして適用することができます。

信頼できる Work From Anywhere（場所に縛られない働き方）

米国の労働人口の約 50% が長期にわたって自宅勤務を続けていることを受けて[12]、ハイブリッドワーカーの保護という課題は近いうちに、セキュリティチームが常に向き合わなければならない現実となりそうです。コアユースケースの解決に必要な機能を適切な SASE ソリューションに正しく実装すれば、分散した従業員に安全で信頼できるアクセスを提供するとともに、エンタープライズクラスのクラウドベースセキュリティでリモート接続を強化することができます。さらに、厳選されたソリューションによって、組織は重要な業務に専念すると同時に、複雑な統合を手作業で管理する必要性を排除し、進化し続けるエンドツーエンドのハイブリッド IT 環境で一貫したセキュリティ態勢を構築することできます。

[1] 「Securing the hybrid workforce」、Security Magazine、2022 年 1 月 7 日（英語）：
https://www.securitymagazine.com/articles/96855-securing-the-hybrid-workforce

[2] 「83% of IT leaders believe the hybrid workforce is here to stay」、Tech Republic、2021 年 11 月 3 日（英語）：
https://www.techrepublic.com/article/83-of-it-leaders-believe-the-hybrid-workforce-is-here-to-stay/

[3] 「What is cloud computing? Everything you need to know about the cloud explained」、ZD Net、2022 年 2 月 25 日（英語）：
https://www.zdnet.com/article/what-is-cloud-computing-everything-you-need-to-know-about-the-cloud/

[4] 「Corporate attack surface exploding as a result of remote work」、Help Net Security、2021 年 9 月 27 日（英語）：
https://www.helpnetsecurity.com/2021/09/27/corporate-attack-surface/

[5] 「Cybersecurity Still A Challenge, And Improving Resiliency Is Essential」、Forbes、2021 年 12 月 15 日（英語）：
https://www.forbes.com/sites/steveculp/2021/12/15/cybersecurity-still-a-challenge-and-improving-resiliency-is-essential/?sh=3800c54c276c

[6] 「Identity Theft Resource Center's 2021 Annual Data Breach Report Sets New Record for Number of Compromises」、ITRC、2022 年 1 月 24 日（英語）：
https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

[7] 「Hybrid workforce model needs long-term security roadmap」、Tech Target、2021 年 6 月 25 日（英語）：
https://www.techtarget.com/searchsecurity/opinion/Hybrid-workforce-model-needs-long-term-security-roadmap

[8] 「The Cybersecurity Challenges Of Working From Anywhere」、Forbes、2022 年 3 月 2 日（英語）：
https://www.forbes.com/sites/adigaskell/2022/03/02/the-cybersecurity-challenges-of-working-from-anywhere/?sh=1131b8d614cc

[9] 「Misconfigurations: Still the Biggest Threat to Cloud Security」、Network Computing、2021 年 8 月 25 日（英語）：
https://www.networkcomputing.com/cloud-infrastructure/misconfigurations-still-biggest-threat-cloud-security

[10] 「2022 年の予測：拡大する攻撃対象領域を標的にする脅威」、Fortinet、2022 年 1 月 24 日：
https://www.fortinet.com/jp/blog/threat-research/security-predictions-for-2022-tomorrows-threats-will-target-the-expanding-attack-surface

[11] 「What's Driving The SASE Boom」、Forbes、2021 年 11 月 11 日（英語）：
https://www.forbes.com/search/?q=What%E2%80%99s%20Driving%20The%20SASE%20Boom&sh=5efde110279f

[12] 「83% of IT leaders believe the hybrid workforce is here to stay」、Tech Republic、2021 年 11 月 3 日（英語）：
https://www.techrepublic.com/article/83-of-it-leaders-believe-the-hybrid-workforce-is-here-to-stay/

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

EB-SASE-WFH-era-202211-R1