CHECKLIST

SASE の必須条件

ハイブリッドワーキングに最適なセキュリティサービスをクラウドで提供

近年、新たに必要になったテレワークを可能にするだけでなく、業務でクラウドアプリケーションやクラウド環境への依存度を高めている従業員をサポートするため、組織はマルチエッジネットワーキング戦略を拡大し続けています。しかし、新しいビジネスの要求に対応するために、これらのネットワークが拡張されることで、攻撃対象領域も広がることになります。また、残念ながら、現在使用されている従来型セキュリティソリューションの大半は、クラウドベースのネットワーキングのイノベーションに対応できていません。

その結果、ネットワーク機能とセキュリティ範囲の間でギャップが拡大しています。これによって、セキュリティ侵害を受けやすいポイントが増えるという本質的リスクが生じることに加え、ネットワークにアクセスするために、依然として仮想プライベートネットワーク（VPN）のみを使用する従来型ソリューションに依存しているテレワーカーにとっては、ユーザーエクスペリエンスが低下するという結果につながります。これは、セキュリティ保護やアクセス制御のために、これまで同様にアプリケーショントラフィックがすべてネットワーク経由でバックホールされる必要があることが、一般的な原因となっています。

SASE（Secure Access Service Edge）は、これらの問題に対処するために開発されました。これによって、セキュリティとネットワーキングの戦略の迅速な融合とスケールアウトが可能になります。SASE を使用することで、拡大する動的な新しいネットワークエッジを安全に提供できるだけでなく、オンネットワークとオフネットワークに分散するハイブリッドワーキングの新しい要求に応えることができます。

今日のデジタル市場で成功するためには、このような分散型でパフォーマンス重視の戦略をサポートすることが不可欠です。このため、適切な SASE ベンダーをパートナーに選定できるかどうかで、運用が成功するか、各コンポーネントの連携において苦労するかが決まると言ってよいでしょう。理論上、SASE はどこにいるユーザーにもクラウドへの安全なアクセスを提供します。しかし、すべての SASE ソリューションが、拡張性、セキュリティ、オーケストレーションで等しい機能を提供するわけではありません。そのため、実装を必要とするテクノロジーと、それらを統合システムとして稼働させるために必要な IT スタッフの両面でオーバーヘッドが増大します。

SASE ソリューションに求められる 4 つの条件

上記のような問題を回避するため、SASE ソリューションの導入を検討する際には以下の 4 つの要件をおさえる必要があります。

☑ 統合セキュリティプラットフォームの一部として機能する SASE であること

SASE は、セキュアなクラウドベースの接続を実現するために設計されています。しかし、クラウドだけで成り立っている企業ネットワークはほとんどありません。企業の 93% 以上がマルチクラウド戦略を採用しているにもかかわらず[1]、大多数は依然として物理ネットワークを使用しています。したがって当然のことながら、クラウドのみのセキュリティでは不完全です。データセンターやその他のオンプレミスのリソースは、保護する必要があるのはもちろんですが、さらに、SASE で提供されるものを含め、他の場所で適用されるのと同じセキュリティ製品やサービスを使用し、統一的なセキュリティ戦略の一環としてポリシーの展開とオーケストレーションが行われることを必要とします。このため、SASE のみを提供し、クラウドへのアクセスのセキュリティだけを対象としているベンダーの多くは、全体的な観点からセキュリティ問題に対応する能力に限界があります。このようなサービスではなく、WAN のセキュリティを含む拡張ネットワークに統合された（または、シームレスに延長して展開可能な）SASE サービスを選ぶ必要があります。統一的なセキュリティフレームワークを実現することにより、TCO（総所有コスト）が削減され、SASE の実質的な有用性が高まります。

☑ エンタープライズクラスのセキュリティ

SASE サービスの評価では、そのセキュリティ要素の機能と性能が効果的であることが求められます。つまり、FWaaS（Firewall-as-a-Service）ソリューションがステートフルなプロトコルとプロキシプロトコルの両方をサポートするか、アプリケーションのスピードで SSL インスペクションをサポートするか、テスト / 検証済みのソリューションを完備したスイートとして提供するか（顧客が未検証のテクノロジーを仕方なく使用する状況が起きないか）といった点を検討することによって、企業が必要とする大規模なセキュリティに対応する SASE を選定できます。

真に安全な SASE ソリューションは、以下のセキュリティ機能およびツールを備えている必要があります。

- **FWaaS（Firewall-as-a-Service）：**SASE のソリューションには、以下のような次世代ファイアウォール（NGFW）が必要です。
  - 高性能な SSL（Secure Sockets Layer）インスペクションと高度な脅威検知機能をクラウド経由で提供する
  - 分散したユーザーのために安全な接続を確立し、維持する
  - ユーザーエクスペリエンスに影響を与えずに、インバウンドとアウトバウンドのトラフィックを分析する
- **DNS（Domain Name System）：**DNS は、悪意のあるドメインを識別して隔離し、悪意のある脅威がネットワークに侵入することを防止します。
- **侵入防止システム（IPS）：**既知の脆弱性を利用しようと試みる悪意のある活動を検出するため、IPS を使用してネットワークを積極的に監視する必要があります。
- **データ漏えい対策（DLP）：**ネットワークとデータの両方の安全性を確保するためには、DLP 機能により、エンドユーザーが重要情報をネットワーク外に持ち出すことを防止する必要があります。
- **セキュア Web ゲートウェイ（SWG）：**SWG ソリューションは、内部および外部のリスクに対して Web アクセスを保護します。また、高性能な SSL インスペクションにより、TLS 1.3 を含む暗号化されたトラフィックに埋め込まれた脅威も自動的にブロックできることが要求されます。
- **ゼロトラストネットワークアクセス（ZTNA）と仮想プライベートネットワーク（VPN）：**エンタープライズクラスのセキュリティを VPN の上に追加し、ZTNA をリモートユーザーにまで拡張する必要があります。これにより、SASE ソリューションが既存の VPN ソリューションと統合できるという本質的なメリットがもたらされ、オフネットワークのリモートユーザーにまでゼロトラストのアプリケーションアクセスが拡張されます。
- **サンドボックス：**クラウドでもアプライアンスでも、サンドボックスを使用することにより、とりわけ未知の脅威に対して重要な保護が提供されます。

☑ 第三者機関により検証された研究とサービス

統一的なセキュリティフレームワークが必要であることに加えて、SASE サービスの価値は、どれだけ優れた脅威インテリジェンスを提供できるかに左右されます。検討対象となる SASE ベンダーは、単なるネットワーキングの経験だけでなく、先進的なセキュリティの研究とイノベーションで実績を持っている必要があります。これにより、SASE ソリューションを介して世界水準のセキュリティを展開 / 利用できるだけでなく、セキュリティを継続的に更新して最新の脅威の手法やテクノロジーに対抗できます。

当然のことながら、TaaS（Technology-as-a-Service）を提供する SASE ベンダーは、脅威のインテリジェンスから保護まで、SASE のサービスや機能について信頼性の高いソリューションの保守とアップグレードを提供する必要があります。それだけではありません。本格的な TaaS には、既知とゼロデイの両方の脅威に対する高度な脅威検知機能が必要です。そのため、SASE の導入を開始する前に、検討中のベンダーが脅威の研究や SASE セキュリティ製品の継続的改善に注力していることを確認する必要があります。

☑ SASE セキュリティが全体的なセキュリティ戦略の一部であること

どの SASE ソリューションでも、セキュリティは基礎となる必須の機能です。すべての要素は、エンタープライズクラスのソリューションとして動作する必要があります。その成果は、第三者機関によるテストと検証、世界最高水準のセキュリティソリューションを提供してきた実績などに表れます。同様に重要なこととして、これらの要素は、シームレスに統合されたセキュリティ戦略の一部として相互運用される必要があります。これは、統一的な SASE ソリューションの一部であると同時に、分散したネットワーク全体を対象に設計された幅広いセキュリティ ファブリックの一部でもあることを意味します。

[1]「10 Key Takeaways From RightScale 2020 State Of The Cloud Report From Flexera,」、Janakiram MSV 著、Forbes、2020 年 5 月 2 日（英語）：
https://www.forbes.com/sites/janakirammsv/2020/05/02/10-key-takeaways-from-rightscale-2020-state-of-the-cloud-report-from-flexera/?sh=1015abc66bcd

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