ソリューションの概要

SASE の 3 つのメリットと その効果を最大化する方法

セキュアアクセスサービスエッジ (SASE) がなぜ必要なのか?

現代のデジタル ビジネス モデルは、アプリケーションやサービスへの一貫したグローバル アクセスをあらゆる場所やデバイスから提供することで、顧客、関係者、従業員のエンゲージメントを次のレベルに引き上げています。

ユーザーやアプリケーションが分散する中で、ネットワークセキュリティの概念は今日のデジタル世界ではもはや通用しなくなりつつあります。Gartner はデジタル企業のニーズをサポートするネットワークとセキュリティの新しいモデルである、セキュア アクセス サービス エッジ (SASE) を開発しました。

> 最も重要なのは、SASE のアーキテクチャーです。理想とされるのは、必要に応じてスケールアウトでき、マイクロサービス上に構築されたクラウドネイティブなアーキテクチャーです。遅延を最小限に抑えるには、パケットがメモリーにコピーされ、仮想マシン (VM) から VM へ、あるいはクラウドからクラウドへと渡されることなく処理されてから、転送またはブロックされるようにする必要があります。そして、リスクを考慮して最適化されたポリシーベースの機能をエンドポイントアイデンティティーに提供するために、特定のハードウェアに依存せず、必要なときに必要な場所でインスタンス化されるソフトウェア スタックが求められます」 — **Gartner**[1]

#1 IT コストと複雑さの軽減

クラウド アプリケーションや SaaS サービスにデータが分散し、場所を選ばない働き方が定着しつつある中で、従来のネットワークベースのセキュリティ モデルは限界を迎えようとしています。この問題に対処するために、多くの組織が追加のサービスを導入してセキュリティ ギャップを解消しようとしていますが、これによってセキュリティ部門への負荷が高まり、導入、管理、運用のコストも大幅に増加しています。このように、ネットワーク セキュリティ モデルはコストや複雑さを増大させるばかりか、スケーラビリティーやアジリティーも乏しく、今日のデジタル世界では効果を十分に発揮できなくなっています。

ゼロトラスト SASE は、古い概念で現代の課題を解決するのではなく、セキュリティ モデル自体を変革します。従来のアプローチがアプリケーションの周囲に境界を作成するのに対し、SASE はアプリケーションにアクセスするユーザーなどのエンティティーに重点を置き、セキュリティを可能な限りエンティティーに近づけます。SASE はクラウド サービスとして、組織が定義したビジネス ルールや機関のルールに基づいてサービスへの接続を動的に許可または拒否します。そしてこれらはすべて、SWG や ZTNA などの以前は別々となっていた機能が統合された単一のサービスによって行われます。

求めるべき SASE

優れた SASE 製品の最も重要な要素となるのが、その基盤となるアーキテクチャーです。Gartner は、SASE のメリットを実現するために必要なアーキテクチャーについて具体的に説明しています。最も重要なのは、クラウド提供型のセキュリティ サービスに求められる拡張性を備えたアーキテクチャーをゼロから構築することです。

つまり、マルチテナントに対応し、需要に応じてグローバルかつ動的に拡張できる分散型のアーキテクチャーが必要です。加えて、ポリシーやポリシー レイヤーといった従来のネットワークの概念ではなく、組織のポリシーに基づき、クラウドで一元的に管理できる真の統合プラットフォームをサポートするアーキテクチャーが求められます。

注意が必要な SASE

Gartner は、クラウド プロバイダーのインフラで稼働する VM ベースの製品を使用した、従来型のネットワーク セキュリティ アプローチには注意が必要との見解を示しています。IaaS コンピューティング環境でこれらの VM ベースのアプローチを使用すると、拡張が難しくなり、クラウド ベンダーとユーザーがアクセスするアプリケーションの間にヘアピン通信が発生するため、一貫したユーザー エクスペリエンスを提供できません。

このモデルでは、ユーザー アクセスに基づく SASE モデルでネットワークベースのアクセスポリシーを使用する、シングル テナントのアーキテクチャーに依存することになるため、SASE モデルとは呼び難い、非常に複雑な導入環境が構築されます。さらに、これらのアプローチは完全には統合されておらず、買収を通じて追加されることが多い個々のサービスのオーバーレイ UI によってつなぎ合わされる複数の製品に基づいている場合がほとんどです。

> SASE (セキュア アクセス サービス エッジ) は、WAN の広範な機能と包括的なネットワーク セキュリティ機能 (SWG、CASB、FWaaS、ZTNA など) とを組み合わせることで、デジタル企業の常に変化するセキュアなアクセスのニーズをサポートします」 — **Gartner**[1]

#2 優れたユーザー エクスペリエンスの提供

SASE がユーザー エクスペリエンスに重点を置くのには、明確な理由があります。ユーザーがネットワークに接続し、アプリケーションがデータ センターに存在し、そして IT 部門がサーバーやインフラを所有して管理していた時代は、簡単にユーザーエクスペリエンスを制御し、予測することができました。しかし、アプリケーションがクラウドに移行した現在も依然として、これらのアプリケーションにアクセスする際は VPN でネットワークに接続してセキュリティを確保するという、古い手法が使われています。このモデルはセキュリティをユーザーに近づけるのではなく、ユーザーをセキュリティに近づけて優れたユーザー エクスペリエンスを提供しようとしますが、これに対しゼロトラスト SASE は、ユーザーの近くでセキュリティを施行します。そして、ユーザーの接続をインターネット エクスチェンジで効率的に管理し、クラウドのアプリケーションやサービスへの直接接続 (ピアリング) を最適化することで、最適な帯域幅と低遅延を確保します。

求めるべき SASE

優れたユーザー エクスペリエンスを提供するには、遅延の少ない、最適化された帯域幅が不可欠です。これを効果的に行う唯一の方法は、アプリケーションに到達するまでのホップ数を減らし、帯域幅コントロールによって適切な帯域幅を割り当てられるようにすることです。

適切なアプローチでは、さまざまな場所に分散するインターネット エクスチェンジを活用して、セキュリティ スタックを可能な限りユーザーに近づけます。そして、これらのエクスチェンジからアプリケーションにアクセスするには、ダイレクトピアリングを通じてトラフィックをアプリケーションに最も近い場所へと効率的にルーティングする機能が必要です。

注意が必要な SASE

クラウド プロバイダーや IaaS で稼働する VM をベースとしたサービスでは、トラフィックのヘアピンが発生します。このようなサービスは SASE に関する記述おいて、適格な SASE ソリューションとみなされていないため、回避する必要があります。

これは主に、VM ベースのアーキテクチャーは拡張性が乏しく、ユーザーからの接続を制御するのではなく、アプリケーションのコンピューティング環境から接続を制御するため、優れたユーザーエクスペリエンスを確保できないためです。また、これらのサービスは動的に拡張できず、予定外のダウンタイムを発生させる可能性のある変更を後から追加できないため、最初に利用条件を計画しておく必要があります。

> ポリシーを決定し、施行する SASE の機能は、エンドポイントのアイデンティティーが配置されるすべての場所に必要です ... IaaS のインターネット バックボーン機能のみを使用し、ローカルの POP やエッジ機能を持たない SASE 製品は遅延やパフォーマンスの問題を発生させ、結果としてエンドユーザーの不満を招く恐れがあります」 — **Gartner**[1]

#3 リスクの低減

セキュリティとは、リスクを特定し、回避することです。クラウド サービスとしてのゼロトラスト SASE は、ユーザーとアプリケーションが広範囲に分散した新たな時代の課題を解消するために生まれました。セキュリティをサービスの接続から切り離された機能ではなく、アーキテクチャーの構造自体に組み込まれた機能として定義することで、ユーザーが接続する場所やアクセスするアプリ、また、使用される暗号化に関係なく、すべての接続が検査されたうえで保護されます。

求めるべき SASE

リスクを軽減するには、ネットワークベースの接続から脱却し、真のゼロトラスト ネットワークアクセス (ZTNA) に基づいてユーザーをアプリケーションに接続させることが重要です。ZTNA は、アプリケーションにアクセスできるユーザーを制限し、複雑な多層ポリシーではなく、組織のポリシーでアクセスの許可または拒否を定義します。

SASE プラットフォームでリスクを削減するもう 1 つの方法は、攻撃対象領域を排除することです。SASE は、企業ネットワークと送信元のアイデンティティーをインターネットから隠し、DDoS 攻撃などの標的にならないようにします。

SASE モデルは、ユーザーとアプリケーションの間のすべての通信を処理するプロキシベースのアーキテクチャーを通じて提供され、このアーキテクチャーがすべてのトラフィックを復号して検査し、完全な可視性を実現します。また、SASE アーキテクチャーは、エンティティーとアプリケーション間で交換されるすべてのデータ コンテキストを使用して構築されており、あらゆる接続がコンプライアンスとデータ ガバナンスの要件に準拠するようにします。

注意が必要な SASE

境界型セキュリティへの従来のアプローチでは、パケット ストリームを調べ、それらのストリームの検査に基づいてリスクを判断する、ファイアウォールベースのモデルが使用されていました。このモデルは、境界型セキュリティにおいては有効でしたが、SASE ベースの導入環境ではその効力を十分に発揮できません。

最大の問題は、サービスとして実行されるファイアウォール アーキテクチャーは侵害の発生後にしか脅威を検知できず、脅威が送信先に到達できてしまうという点です。その理由は非常にシンプルで、送信前にデータを保持し、その結果を判断できないためです。このような制限によって、セッションの復号とデータ保護が極めて困難になりますが、これは、これらの機能もプロキシと同様に、ストリームを保持して再構築する必要があるためです。

ファイアウォール サービスで復号、検査、再構築を行うには、サービスから切り離された個別のプロセスが必要になり、ポリシーが複雑になるだけでなく、遅延やパフォーマンスの問題が発生します。また、実装しても限られた機能しか使えない場合もあるのが実状です。SASE には、すべてのコンテンツを同時に処理できるシングルパスのアーキテクチャーが必要です。ストリームベースのファイアウォール製品は、ホスト ネットワークの送信元 IP アドレスを潜在的な攻撃者に公開するため、結果として攻撃対象領域が拡大し、標的型攻撃の標的にされるリスクが生じます。

Zscaler が提供する SASE ソリューション

Zscaler の AI を活用したクラウド セキュリティ プラットフォームは、パフォーマンスとスケーラビリティーのためにゼロから構築された SASE サービスです。グローバルに分散したプラットフォームを提供する Zscaler は、ユーザーと接続先のアプリケーションとの間の最短パスを常に確保し、世界中の主要なインターネット エクスチェンジの何百ものパートナーとのピアリングを通じてユーザー、ワークロード、ビジネス パートナー、拠点に最適なパフォーマンスと信頼性を提供します。

Zscaler Zero Trust SASE は、業界で最も実績ある SSE プラットフォーム上に構築され、SD-WAN への新たなアプローチを提供します。現在、Forbes Global 2000 の 30% 以上が Zscaler を採用して、デジタル時代への安全な第一歩を踏み出しています。

Zscaler は市場に参入して以来、そのスケーラブルなアーキテクチャーの価値を証明し続けており、現在は 1 日あたり 3,600 億以上のトランザクションを処理し、そこから得られた 500 兆以上のシグナルで AI/ML を活用したクラウド効果を強化しています。

Zscaler Zero Trust SASE アーキテクチャーは世界中の 150 か所以上のデータ センターで提供され、ユーザーの接続場所に関係なく、高速で安全なローカル接続を確保します。

Zscaler の SASE ソリューションの詳細については、こちらをご覧ください：
https://www.zscaler.jp/capabilities/secure-access-service-edge

[1] Gartner、The Future of Network Security Is in the Cloud、Lawrence Orans、Joe Skorupa、Neil MacDonald

zscaler™ | Experience your world, secured.™

Zscaler について
Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.jp