SASEの3大メリットとその達成方法

SASE（セキュアアクセスサービスエッジ）を採用すべき理由

最新のデジタルビジネスモデルは、世界中のあらゆる場所から、あらゆるデバイスを利用して接続する従業員や顧客に対して、アプリケーションやサービスへの一貫性あるアクセスを提供することで、エンゲージメントを新たなレベルへと引き上げます。

分散型のユーザやアプリケーションを前提にしたネットワークセキュリティの概念をデジタルの世界にそのまま持ち込むことはできません。ガートナーは、デジタル企業の要件に合わせたネットワークとセキュリティの新しいモデルを開発し、SASE（セキュアアクセスサービスエッジ）を名付けました。

> 「SASE（セキュアアクセスサービスエッジ）は、包括的なWAN機能に包括的なネットワークセキュリティ機能（SWG、CASB、FWaaS、ZTNAなど）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アクセスニーズをサポートする、新しい方法である」**– ガートナー**[1]

メリット
その1

ITコストと複雑さの軽減

データがクラウドアプリケーションとSaaSサービスに広がり、あらゆる場所で働くユーザが増加したことで、従来型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ました。これを解消するため、組織は、サービスを追加してセキュリティギャップを解消することを余儀なくされましたが、セキュリティチームがそのような拡大に追いつくことが困難であることから、導入、管理、運用のコストが大幅に増加することになりました。このようなコストや複雑さの増加にもかかわらず、ネットワークセキュリティモデルのスケーラビリティやアジリティの欠如という問題は解消されず、デジタルの世界に対応できていません。

SASEは、古い概念で今日の問題を解決するのではなく、このようなセキュリティモデルを反転させます。従来のアプローチはアプリケーションの周りに境界を作成しようとするものでしたが、SASEは、アプリケーションにアクセスするユーザなどのエンティティに注目し、セキュリティを可能な限りエンティティに近づけようとするものです。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に基づき、サービスへの接続を動的に許可または却下します。
そして、これらはすべて、SWG、ZTNAなどの以前は分離されていた複数の機能が統合された単一のサービスによって実行されます。

正しい選択

優れたSASE製品で最も重要なコンポーネントは、その基礎となるアーキテクチャです。ガートナーは、SASEによって約束されるメリットを実現するために必要なアーキテクチャについて、具体的に説明しています。最も重要なのは、完全クラウド提供型のセキュリティサービスに必要とされるスケーラビリティを実現するアーキテクチャをゼロから構築する必要があるということです。

つまり、マルチテナンシをサポートし、オンデマンドで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である必要があります。また、ポリシーとポリシーレイヤの従来のネットワーキングの概念からビジネスポリシーベースへの移行を可能にするアーキテクチャである必要があります。そして最後に、統一されたクラウド提供型管理が可能な真の統合プラットフォームをサポートするものでなければなりません。

誤った選択

ガートナーは、クラウドプロバイダインフラストラクチャで動作するVMベース製品を使用する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だと説明しています。
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、スケーラビリティが欠如し、クラウドベンダとユーザがアクセスするアプリケーションの間をヘアピン方式で行き来する必要があるため、安定したユーザエクスペリエンスを提供できません。

このモデルは、ユーザアクセスに基づく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しようとする、シングルテナントのアーキテクチャを活用するものであるため、SASEモデルと呼ぶことが困難な、非常に複雑な導入環境が構築されることになります。さらに、これらのアプローチでは多くの場合、買収によって集約された複数の独立したサービスのオーバーレイUIを寄せ集めた、統合が不完全な複数の製品を利用します。

> 「SASEのポリシー決定/適用機能は、エンドポイントのアイデンティティが置かれるあらゆる場所に必要です。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/エッジ機能を持たないSASE製品には、レイテンシやパフォーマンスの問題が発生し、エンドユーザの不満につながる恐れがあります。」 **– ガートナー**[1]

メリット
その2

優れたユーザエクスペリエンスの提供

SASEの主眼がユーザエクスペリエンスに置かれているのには、明確な理由があります。ユーザが企業ネットワークにアクセスしており、アプリケーションはデータセンタに存在し、サーバやインフラストラクチャをITが所有し、管理する手法では、ユーザエクスペリエンスのコントロールや予測は簡単でした。アプリケーションが複数のクラウドに存在するようになった今も、これらのアプリケーションへのアクセス方法は、ネットワークへのVPN接続でセキュリティを確保するという、古いモデルのままです。このモデルは、ユーザをセキュリティに近づけるものであり、優れたユーザエクスペリエンスに必要とされる、セキュリティをユーザに近づけるものではありません。SASEは、セキュリティをユーザに近づけ、ユーザの接続をインターネットエクスチェンジでインテリジェントに管理し、クラウドのアプリケーションやサービスへのダイレクト接続（ピアリング）を最適化することで、最適な帯域幅と低レイテンシを保証する方法を推奨しています。

正しい選択

優れたユーザエクスペリエンスの条件とは、レイテンシが最も少なく、最適な帯域幅が提供されることです。そのための唯一の有効な方法は、アプリケーションに到達するまでのホップ数を少なくし、帯域幅コントロールによって適切な帯域幅が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、さまざまな場所に地理的に分散するインターネットエクスチェンジを活用し、セキュリティスタックを可能な限りユーザに近づけます。そして、これらのエクスチェンジからのアプリケーションへのアクセスには、ダイレクトピアリングを活用して、トラフィックをアプリケーションに最も近い場所へとインテリジェントにルーティングする機能が必要です。

誤った選択

クラウドプロバイダやIaaSで動作するVMを利用するサービスでは、トラフィックのヘアピン方式での通信が発生します。このようなサービスは、SASEのホワイトペーパーにおいてSASEソリューションとして不適格だとされており、回避する必要があります。

その主な理由は、VMベースのアーキテクチャにはスケーラビリティが欠如し、ユーザからの接続をコントロールできず、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コントロールするため、優れたユーザエクスペリエンスを保証できないためです。さらには、これらのアーキテクチャは動的な拡張に対応できず、計画内ダウンタイムなく後で変更できないため、最初に利用条件を計画しておく必要があります。

> 「重要なのは、どのようなSASEアーキテクチャかということであり、理想とされるのは、クラウドネイティブで、必要に応じてスケールアウトできる、マイクロサービスをベースに構築されたアーキテクチャです。レイテンシを最小限にするには、パケットをメモリにコピーし、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、転送/ブロックされるようにする必要があります。さらには、特定のハードウェアに依存しない、インスタント化が可能なソフトウェアスタックであることが重要であり、そのような条件を満たしていれば、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に提供できます。」**– ガートナー**[1]

メリット
その3

リスクの低減

セキュリティとは、リスクの特定と回避に他なりません。クラウドサービスとしての SASEは、ユーザとアプリケーションが広範囲に分散しているという新たな現実を前提に、固有のリスクの課題を解決するように設計されています。サービスの接続から切り離された機能ではなく、プラットフォームのファブリックに組み込まれた機能としてセキュリティを定義することで、ユーザが接続する場所、アクセスするアプリ、使用する暗号化に関係なく、すべての接続をインスペクションして保護します。

正しい選択

リスク軽減の鍵となるのは、ネットワークベースの接続の概念から脱却し、真のゼロトラストネットワークアクセス（ZTNA）に基づいてユーザをアプリケーションに接続するという考え方に移行することです。ZTNA は、認証されたユーザだけが許可されたアプリケーションにアクセスできるようにするもので、複雑な多層型ポリシー定義ではなく、ビジネスベースのポリシーによって許可するか否かを定義します。

SASEプラットフォームによるリスク軽減のもう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をインターネットから隠すことで、DDoS などの攻撃の標的になるのを防ぎます。

SASEモデルは、ユーザ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によって実現し、このアーキテクチャによって、すべてのトラフィックの復号化とインスペクションが可能になり、完全な可視性が提供されます。そして最後に、エントリとアプリケーションの間で全データコンテキストが交換されるように SASEアーキテクチャを構築することで、すべての接続がコンプライアンスとデータガバナンスの要件を確実に満足できます。

誤った選択

従来の境界セキュリティへのアプローチでは、パケットストリームに注目し、それらのストリームのインスペクション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、境界ベースのセキュリティにおいては有効でしたが、SASEベースの導入で直面した新たな課題によって、その有効性が完全に失われることになりました。

最大の問題は、サービスとして動作するファイアウォールアーキテクチャで可能なのは脅威の事後判断であるため、発見前に脅威が標的に到達できるということです。理由は簡単で、送信前にデータを手に入れ、結果の判断ができないためです。このような制約によって、セッションの復号化とデータ保護が極めて困難になり、プロキシの場合と同様、これらの機能もストリームを取得して再構成する必要があるからです。

ファイアウォールサービスでは、復号化、インスペクション、再構成の機能には、サービスから切り離された個別のプロセスが必要であるため、ポリシーが複雑になり、レイテンシが発生し、パフォーマンスが低下し、結果として、実装しても機能が大幅に制限されてしまうことも少なくありません。また、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が必要です。ストリームベースのファイアウォールには、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知られてしまい、結果として標的型攻撃の攻撃対象領域となるというリスクもあります。

> 「SASEの多くの機能は、プロキシモデルが使用してデータパスにアクセスし、アクセスを保護します。従来型のインラインネットワーク/エンタープライズファイアウォールのベンダには、分散型のスケーラブルなインラインプロキシの構築に必要な専門知識がないため、SASEを採用する側がコストの上昇やパフォーマンスの低下といったリスクを負うことになります。」**–ガートナー**[1]

ゼットスケーラーのSASEへのアプローチ

Zscaler Cloud Security Platformは、優れたパフォーマンスとスケーラビリティを実現するためにゼロから構築されたSASEサービスです。グローバルな分散型プラットフォームであるため、ユーザは常に短いホップでアプリケーションにアクセスでき、世界中の主要インターネットエクスチェンジの数百のパートナーとのピアリングによって、ユーザのパフォーマンスと信頼性を最適化します。

ゼットスケーラーは創業から10年以上にわたり、SASEと同じ原理のもとにプラットフォームを構築してきました。現在、Forbes Global 2000に名を連ねる400以上の組織が、ゼットスケーラーを採用して、デジタル時代への新たな一歩を踏み出しています。

ゼットスケーラーが構築した、優れたスケーラビリティを備えた実績あるアーキテクチャにより、ピーク時には最大80億件のトランザクションが処理され、120,000のユニークセキュリティアップデートが毎日実行されています。

ゼットスケーラーのSASEアーキテクチャを世界中の150箇所のデータセンタに展開することで、接続する場所に関係なく、高速かつ安全なローカル接続をユーザに提供しています。

詳細はこちら

SASEの詳細については
zscaler.jp/gartner-secure-access-service-edge-saseをご確認いただき、ガートナーによるネットワークセキュリティの未来像についての予測も併せてご覧ください。

ゼットスケーラーのSASEへのアプローチの詳細については、
zscaler.com/products/secure-access-service-edgeを参照してください。

1. ガートナー、「ネットワークセキュリティの未来はクラウドにある」、2019年8月30日、Lawrence Orans、Joe Skorupa、Neil MacDonald共著

ゼットスケーラーについて

ゼットスケーラーは、モバイル対応、クラウドファーストの環境へのセキュアトランスフォーメーションを可能にします。ゼットスケーラーは、デバイス、場所、あるいはネットワークの区別なく、ユーザをアプリケーションやクラウドサービスに接続し、それと同時に、包括的セキュリティと高速のユーザエクスペリエンスを提供します。高価で複雑なゲートウェイアプライアンスは、もう必要ありません。

zscaler™