Secure Access Service Edge（SASE）とは

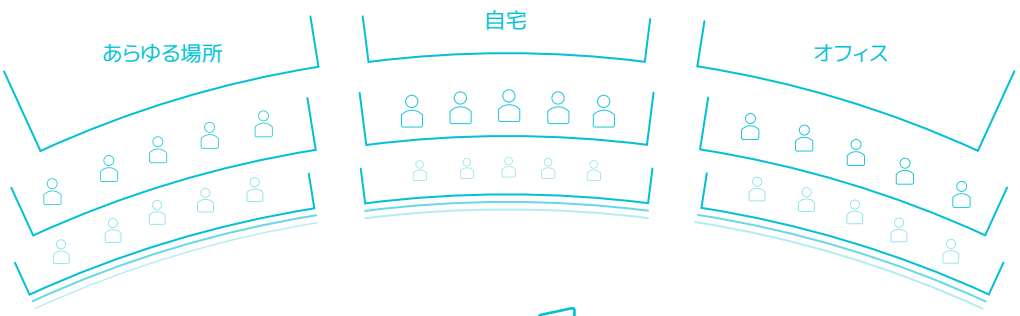
ネットワーク サービスとセキュリティ サービスの結合により、クラウドベースの調和を実現

Secure Access Service Edge（SASE）は、WAN サービスとセキュリティ サービスをクラウドベースのサービス モデルによって統合したソリューションであり、場所を問わずにユーザー、アプリケーション、リソースを接続することができます。

SASE は多くのベンダーやエンドユーザーに支持されており、市場規模は 30 億ドルを超えます。
- Gartner*

聴衆

ユーザーは、あらゆる場所で、あらゆるデバイスからすべての
エンタープライズ アプリケーションに安全に接続する必要があります。



オーケストラ

SASE コンポーネントは、オーケストラの各セクションのように調和し、互いに連携することで
クラウドファーストのアプローチ、アプリケーションの品質保証、
本質的なセキュリティ、シンプルな運用を提供します。

SD-WAN

ソフトウェアベースの WAN（SD-WAN）
基盤となるネットワークからネットワーク サービスを切り離し、基盤となる物理コンポーネントまたはトランスポート コンポーネントから独立してアプリケーショントラフィックを伝送できるようにします。

Secure Access

ゼロトラスト ネットワーク アクセス（ZTNA）
ネットワーク中心のセキュリティから脱却して、「すべてを信頼しない」という原則に基づくアイデンティティベース、ロケーションベース、コンテキストベースの手法を採用し、認可されたリソースへのアクセスのみをオンデマンドで付与します。

Cloud Web Security

セキュア Web ゲートウェイ（SWG）
マルウェアに対する防御を提供するとともに、Web にアクセスするためのポリシーベースの制御を実行します。

Cloud Access Security Broker（CASB）
すべてのエンドポイントを、エンタープライズ クラウドのセキュリティ ポリシーに準拠する状態に維持します。

Data Loss Prevention（DLP）
機密データの損失と誤用、または不正なユーザーによるアクセスを防止するプロセスとツールです。

Remote Browser Isolation（RBI）
Web ブラウジングをユーザーのデバイスではなくリモート サイトで実行することで、マルウェアやウイルスによるデバイスやネットワークへの侵入を防止します。

Cloud Firewall

侵入検知システム（IDS）
ネットワークトラフィックの解析とパケットの検査によって、サイバーセキュリティ上の脅威を検知して報告し、脅威にフラグを付けます。

侵入防止システム（IPS）
ネットワークのパケットを解析して、悪意のあるアクティビティをプロアクティブに報告し侵入を阻止します。

サービスとしてのファイアウォール（FWaaS）
クラウドベースのサービスとして提供され、一元化されたエンタープライズ ポリシーによってネットワークトラフィックを保護します。

パフォーマー

ビジネスにおいて、アプリケーションは舞台上のパフォーマーの役割を果たす存在であり、
聴衆（ユーザー）とのつながりの基礎となります。
アプリケーションがアクセス可能かつセキュアであることは、優れたユーザー体験を実現するうえで必須です。

Web　**SaaS**　**IaaS**　**データセンター**

サービスのクラウドへの移行と従業員の分散化がこれまでにない規模で進んでいる今日のニーズに対応して、SASE コンポーネントを組み合わせて活用することで、ユーザーからアプリケーションまでに至るあらゆる対象を場所にかかわらず保護する、高度に調和したエンタープライズ セキュリティを実現できます。

vmware.com/jp/products/secure-access-service-edge-sase

* 出典：Gartner, Inc.、『Emerging Technologies: Applying SASE' s Architectural Model to Secure Distributed Composite Apps』、Joe Skorupa/Neil MacDonald/Anne Thomas、2020 年 11 月 13 日

ヴイエムウェア株式会社 〒108-0023 東京都港区芝浦 3-1-1 田町ステーションタワー N 18階 www.vmware.com/jp

E:2020/11 J:2021/10