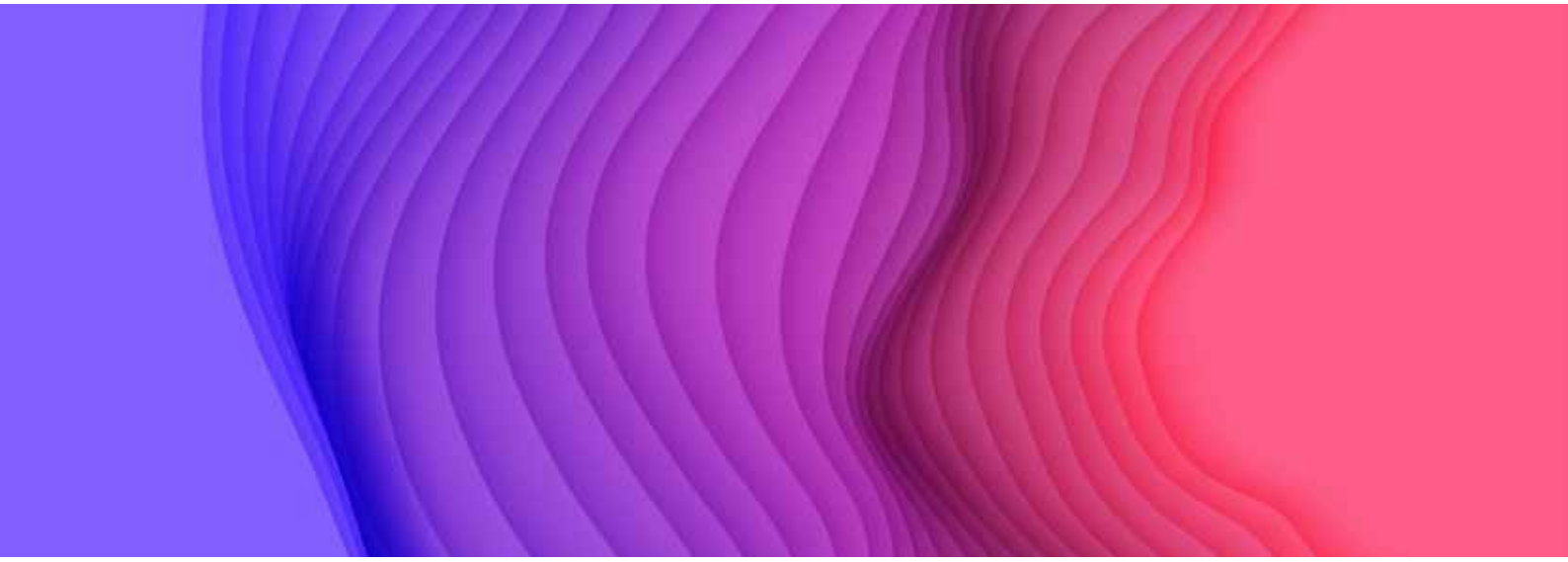
パンフレット

Unified SASEの概要解説ガイド

よりシンプルで高コスト効率のSASEの導入のために

HPE aruba networking



48%

「2023年末までに、ナレッジワーカーの48%がハイブリッド勤務となり、フルリモートワーカーは2019年から27%増加、ハイブリッド勤務のナレッジワーカーは2020年から12%増加して39%に達すると思われる。」[1]これにより、SASEソリューションの需要は高まっています。

46%

「今後12か月の間に、46%の組織がSASEアーキテクチャーを導入するだろう。」[2]

65%

「2025年までに、65%の企業が、個別のSASEコンポーネントを1社、または2社の明示的な提携関係にあるSASEベンダーに集約するだろう。」[3]

[1]『予測分析: ナレッジ従業員、ハイブリッド、フルリモートおよびオンサイトでの勤務形態』、Gartner社、2023年1月

[2] 2023年のPonemon Institute社のレポート

[3]『シングルベンダーSASEのマーケットガイド』、Gartner社、2022年9月

Unified SASEの台頭: よりシンプルで高コスト効率なSASEの導入

昨年一年間で、多くのITリーダーはセキュアアクセスサービスエッジ（SASE）フレームワークを採用し、グローバルな組織全体で高速かつよりセキュアな接続を可能にしてきました。SASEはネットワークおよびセキュリティソリューション機能を単一のクラウドネイティブサービスに集約し、どこからでも一貫性のある接続とセキュリティを可能にするものです。

SASEは単なるテクノロジートレンドではありません。このデジタル時代での成長を目指す現代のビジネスにとって、戦略的に不可欠なものです。

しかし、すべてのSASEソリューションが同様に開発されているわけではありません。SASEプロバイダーによっては、完全には統合されていない、もしくは異なる複数ベンダーのPoP間でのルーティングが必要となる、複数のポイントソリューションを提供している場合もあり、レイテンシ、パフォーマンス障害、管理のオーバーヘッドにつながります。

そして、SASEのあらゆるコア機能を緊密に統合された単一プラットフォームから提供するSASEソリューションもあり、強固なセキュリティポスチャ、スタッフの高い作業効率とコスト効率、ユーザーと管理者のエクスペリエンス向上を実現します。

これこそが、Unified SASEであり、SASEへの、よりシンプルで高コスト効率なアプローチと言えます。

このガイドでは、**Unified SASE**について知っておきたいすべての項目について説明しています。

- Unified SASEとは
- 単一ベンダーのSASEが最先端ビジネスにもたらすさまざまなメリット
- HPE Aruba Networkingが提供する強固なUnified SASE
- SASEを今すぐ導入

このガイドをお読みになることで、Unified SASEを導入して、セキュリティの目標をより速く、より効率的に実現する方法を明確に理解することができます。

SASEの導入が拡大している要因

SASEを導入する理由とはそもそも何でしょうか。その答えは簡単に3つにまとめられます。

1. 以前は効果的だったが今はそうではない**セキュリティ**。

2. 以前は管理可能であったが今はそうではない**ネットワーク**。

3. 以前は良好に動作していたが今はそうではない**ソリューション**。

主に境界ベースのセキュアな接続に頼っていた従来のネットワークおよびセキュリティアーキテクチャーは、今や最新のビジネス環境のニーズを満たすものではなくなっています。クラウドサービス、モバイルデバイス、IoT、OT、リモート/ハイブリッド勤務の採用が急速に進んだことで、労働力の分散化と動態化が生じ、その結果いつでも、どこでも、どのデバイスからでも、アプリケーションやデータへのセキュアで信頼性の高いアクセスが必要になりました。

とはいえ、ビジネスニーズが進化する一方で、従来のネットワークセキュリティソリューションを利用し続けることで、組織は接続に関する新たな課題やリスクを抱えることになりました。

- **攻撃対象領域の拡大と複雑さの増加:** 保護すべきユーザー、デバイス、場所、クラウドサービスが増えれば、攻撃の潜在的なエントリーポイントが増え、管理および更新すべきセキュリティツールも増えます。言うまでもなく、各エントリーポイント（ユーザーやデバイス）は企業ネットワークに直接アクセスするため、セキュリティリスクはさらに増加します。
- **ユーザーエクスペリエンスと生産性の低下:** VPNと企業ネットワークにバックホールされるトラフィックが増えるほど、ユーザーはレイテンシ、ジッター、パケットロス、帯域幅制限の増加を感じるようになり、彼らの満足感は言うまでもなく、パフォーマンスと生産性にも影響を与えることになります。
- **運用コストの増大と低効率:** 導入、維持、更新、トラブルシューティングの対象となるネットワークソリューションとセキュリティソリューションが増えるほど、インフラストラクチャ管理と問題解決に費やすリソースと時間が増えます。

こうした課題やリスクに対処するのは非常に難しいと感じるかもしれません。ですが、ネットワーキングとセキュリティのリーダーが連携し、SASEフレームワークを活用することで、こうした課題を解決することが可能です。

SASEとは

セキュアアクセスサービスエッジ（SASE）は2019年に初めて導入されたサイバーセキュリティに関する概念です。SASEは、ネットワーキングとセキュリティ機能を1つのプラットフォームに組み合わせたITフレームワークです。グローバルに分散したワークフォース全体で、すべてのユーザー、デバイス、アプリケーションをセキュアに接続します。

SASEは2つの「テクノロジーセット」から構成されます。1つはWANエッジサービス（SD-WAN）、もう1つはセキュリティサービスエッジ（ZTNA、SWG、CASB、DEM）であり、これらを組み合わせることで、ネットワークチームもセキュリティチームも同じように、あらゆるユーザー、デバイス、またはサーバーがあらゆる転送方法でどこからでも安全に接続できるようになります。広範なSD-WANファブリックとクラウド配信型SSEを、PoPのグローバルネットワークで活用することで、高速なエッジからクラウドへのアクセスが可能になり、レイテンシが低減し、パフォーマンスが向上します。

SASEの構成要素

統合型のシングルベンダーSASE製品を構築するコアテクノロジーセットは、次の2つです。

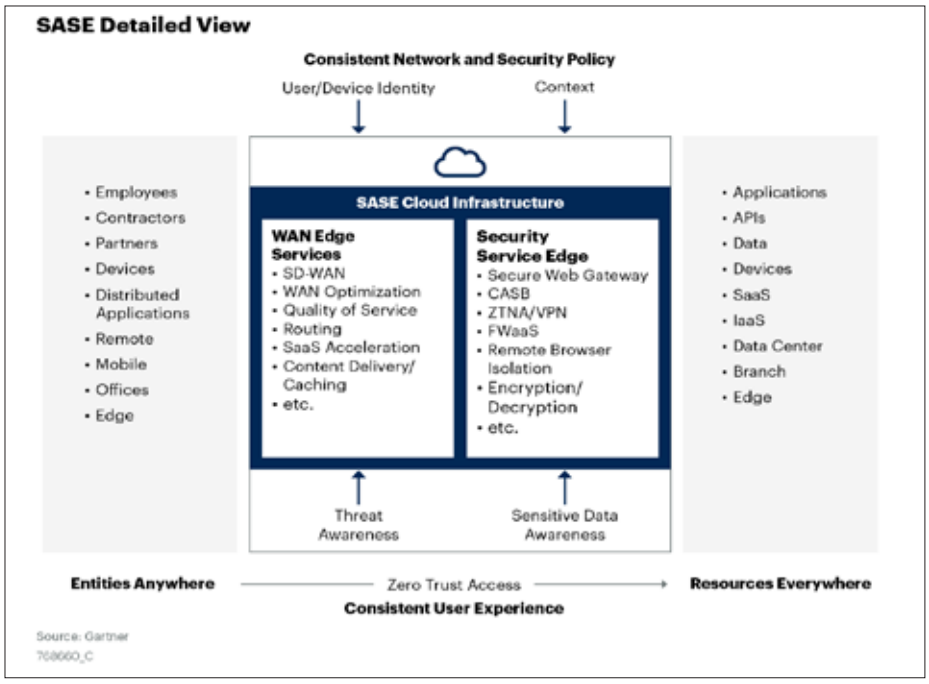


図1. SASE — 詳細情報、シングルベンダーSASEのマーケットガイド[4]

WANエッジサービス（セキュアSD-WAN）

- **セキュリティ:** セキュアSD-WANは次世代ファイアウォール機能を搭載しています。これにはIDS/IPSと粒度の細かいセグメンテーションが含まれており、組織がブランチファイアウォールとセキュアなIoTデバイスを置き換えることができます。さらに、すべての接続はSD-WANファブリックで暗号化されます。
- **マルチクラウドネットワーキング:** SD-WANソリューションの仮想インスタンスをAWS、MS Azure、Google Cloudなどのクラウドサービスプロバイダーに展開し、ブランチオフィスからクラウドへの回復力のある接続を確立できます。またSD-WANは、クラウドへのアプリケーショントラフィックもインテリジェントに制御してデータセンターへのバックホールトラフィックを回避し、トラフィックパターンの変化に動的に適応します。
- **動的パス制御:** SD-WANは、MPLSやブロードバンドインターネット、4G/5G、サテライトリンクなど複数の転送リンクと組み合わせることができます。ネットワーク状況やビジネス目的に合わせて最適なリンクが動的に選択されます。
- **パスコンディショニング:** SD-WANソリューションでは、パスコンディショニングなどの技術も使用して、ブロードバンドインターネットやMPLS接続でよく見られるパケットのドロップや混乱による悪影響を克服します。これにより、インターネットリンク上で専用回線のようなパフォーマンスを実現し、組織はMPLSへの依存を軽減して新しいブランチを迅速に立ち上げることができます。
- **動的パス制御:** この機能は、TCPプロトコルアクセラレーションとデータ重複排除および圧縮アルゴリズムを適用することで、WAN経由のデータ送信を高速化します。
- **一元的なオーケストレーション:** ビジネスおよびセキュリティポリシーは単一のインターフェイスから一元管理されます。これにより、管理者が1つの場所からポリシーの変更と適用を行うことができるため、ネットワーク運用とトラブルシューティングが簡素化されます。

[4] 『シングルベンダーSASEのマーケットガイド』、Gartner社、2022年9月

セキュリティサービスエッジ（SSE）

ゼロトラストネットワークアクセス（ZTNA）| プライベートアプリケーションへのセキュアなアクセス

- ZTNAテクノロジーは、ホストされている場所やユーザーの所在地に関係なく、プライベートアプリケーションやリソースへのきめ細かなIDベースのゼロトラストアクセスを提供します。最新のZTNAソリューションを使用すると、チームは従業員やサードパーティユーザーのリモートアクセスVPNを完全に排除でき、基盤ネットワークへのアクセスを増加させることなく特定の許可されたプライベートアプリケーションへのアクセスを許可することで、攻撃対象領域を大幅に削減できます。

セキュアなWebゲートウェイ（SWG）| インターネットへのセキュアなアクセス

- SWGは、Webフィルタリング、SSL検査、マルウェア検出と保護などの機能により、高度な攻撃から分散型ビジネスを保護します。SWGは、認可ユーザーの高速でセキュアなインターネットリソースへのアクセスを確保しながらビジネスを損害から守ります。

クラウドアクセスセキュリティブローカー（CASB）| SaaSアプリケーションへのセキュアなアクセス

- ITチームは、クラウドサービスの使用をCASBで特定、管理、制御できます。CASBサービスは、ユーザーとクラウドベースのSaaSアプリケーション間の接続を媒介し、データフローを規制し、データロスを防ぎ、シャドーITを明らかにして、機密データの保護を確保します。

デジタルエクスペリエンスモニタリング（DEM）| デジタルエクスペリエンスと生産性の向上

- DEMは、強化されたインラインの可視性と解析をデバイス、アプリケーション、ネットワークのインタラクション、エクスペリエンス、パフォーマンスに提供します。DEMは、迅速なトラブルシューティングとエクスペリエンスに関する問題の的確な診断により、ITチームが時間を有効活用できるようにします。

Unified SASEとは

Unified SASEは、SD-WANとSSEの2つのテクノロジーセットを1つのベンダーソリューションに組み込み、ビジネスを一層簡単にし、運用効率を高め、コスト節減を実現できるようにします。また統合型アプローチでは、アジリティの向上と迅速な導入も可能になるため、価値実現時間が短縮されます。Gartner社は、「2025年までに、SD-WAN関連の新規購入の50%で単一ベンダーSASEオファリングの機能が選択される。これは2022年度から10%の増加となる」と、予想しています[5]。

単一ベンダーのSASEが最先端ビジネスにもたらすさまざまなメリット

Unified SASEは、SASEによる多くのメリットを組織にもたらし、導入もより簡単かつ高コスト効率になります。具体的には、次のようなメリットを提供します。

- **セキュリティポスチャの統合と改善:** Unified SASEは、すべてのトラフィックおよびロケーションにわたり汎用セキュリティポリシーや一元的なアクセス制御を適用することで、攻撃対象領域を縮小し、脅威検出と応答時間を改善します。
- **ネットワーキングチームとセキュリティチームの効率改善:** 単一ベンダーによるSASEを導入することで、両ソリューションが統合されるだけでなく、ネットワーキング機能とセキュリティ機能の統合により、チーム間の障壁の緩和、複雑さとコストの最小化、部門横断的な連携と実装の最適化を図ることができます。ネットワークとセキュリティの運用は、可視性、構成、監視、トラブルシューティングの一元管理システムの提供によって効率化されます。
- **より優れたユーザーエクスペリエンスと管理者エクスペリエンスの実現:** Unified SASEの最速のアクセスパスを経由するトラフィックの自動ルーティングと、データセンターへのバックホールトラフィックの防止により、アプリケーションへの高パフォーマンスで低レイテンシの接続をユーザーに保証できます。エンドユーザーには最適なアクセスエクスペリエンスが可能になり、管理者は簡単ながらきめ細かなアクセス制御を汎用ゼロトラストポリシーで適用できます。
- **コストの削減と柔軟性の向上:** SASEでは、複数のポイントソリューションとハードウェアアプライアンスが不要になるため、資本支出（CAPEX）と運用支出（OPEX）が削減されます。Unified SASEは高い拡張性も備えており、変化するビジネスニーズにすばやく適応し、地理的に分散した組織に複数のPoPを提供します。

[5]『シングルベンダーSASEのマーケットガイド』、Gartner社、2022年9月

Unified SASEの導入を開始する方法

単一ベンダーのSASEソリューションの導入は困難に思われますが、実際はそのようなことはありません。適切なパートナーがいて明確なロードマップがあれば、組織は既存の業務を中断したりパフォーマンスを損なったりせずに、スムーズかつ安全にSASEに移行できます。

SASEの導入を成功させるには、次の5つの基本的なステップを実行します。

- **ステップ1: SASEの目標と要件を決める。**ビジネス目標、ユースケース、SASE要件を特定します。現在のネットワークとセキュリティアーキテクチャーを評価します。ギャップ、課題、既存のリソースを発見します。
- **ステップ2: 単一ベンダーのSASEプロバイダーを選択する。**機能、カバレッジ、パフォーマンス、スケーラビリティ、信頼性、サポート、価格に基づいて異なるプロバイダーを比較します。統合され、一元型で、柔軟性があり、使いやすい、優れた設計の単一ベンダーのSASEソリューションを探します。
- **ステップ3: SASE戦略を設計、開発する。**プロバイダーと協働し、ベストプラクティスに基づいてネットワークトポロジ、セキュリティポリシー、ユーザーグループ、アプリケーションプロファイル、および接続オプションを定義します。これは、ビジネスが最大の成功を実現できるよう、SASEプロバイダーと連携して行うプロセスです。
- **ステップ4: 段階的アプローチでSASE導入を開始する。**一元管理コンソールを通じてエージェント、コネクター、SD-WANデバイス、またはプライベートPoPなどの必要なコンポーネントを導入します。ユーザー、デバイス、拠点、アプリケーションをSASEソリューションに移行します。これは段階的に、または一括で行います。SASEは、既存のソリューションと併用できます。そのため、導入はチームのニーズに合わせて迅速に行うことも、ゆっくり行うこともできます。
- **ステップ5: SASEを最大限活用する。**導入を継続する中で、プロバイダーが提供するツールやダッシュボードを使用して可視性、有益な情報、フィードバックを獲得してSASEソリューションをさらに最適化します。投資を最大限活用し、SASEでさらにビジネスに利益をもたらせる、新しいユースケースと機能を発見します。

HPE Aruba Networkingが提供する強固なUnified SASE

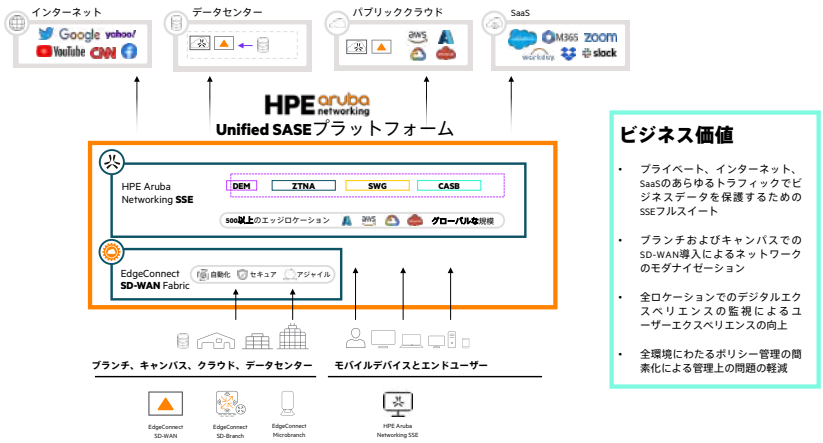


図3. HPE Aruba NetworkingのUnified SASEプラットフォーム

セキュアで信頼性の高いビジネスへのアクセスをどこでも実現できる強力な単一ベンダーのSASEソリューションをお探しの場合、HPE Aruba Networking SASEがその答えかもしれません。業界をリードするSD-WANと受賞歴のあるSSEを備えたHPE Aruba Networkingは、今日の分散型で動的な企業向けに設計されたSASEへの包括的で統一されたアプローチを提供します。

ネットワーキングとセキュリティソリューション間の統合に対する需要が高まる中、HPE Aruba Networkingは、ITチームがビジネスの接続を統合、簡素化、保護するために役立ちます。HPE Aruba Networkingを使用すると、ITチームは、データセンターを介してデータをルーティングするのではなく、HPE Aruba Networking EdgeConnect SD-WANを使用して、ネットワークエッジのアプリケーションにWANおよびクラウドのセキュリティ制御を直接提供できます。また、SSEにより、キャンパス、ブランチ、自宅、外出先など、どこで接続しても、すべての人やデバイスにゼロトラストのセキュリティ制御を確実に適用できます。

SASEを今すぐ導入

「今後12か月の間に、46%の組織がSASEアーキテクチャーを導入するだろう。」

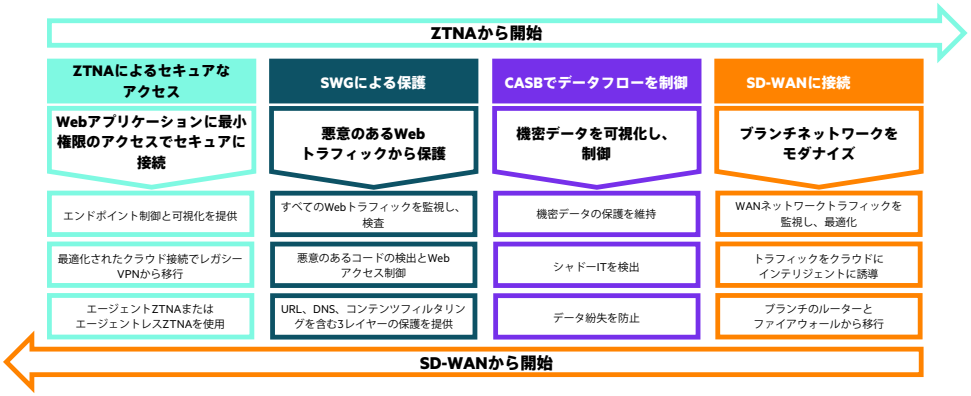
– 2023年のPonemon Institute社レポート[4]

SASEは単なる一時的なテクノロジートレンドではありません。このデジタル時代での成長を目指す現代のビジネスにとって、戦略的な必須事項です。SASEを導入することで、組織はネットワーク制御に重点をおいたネットワークおよびセキュリティのアーキテクチャーの課題やリスクを克服し、セキュリティポスチャ、ユーザーエクスペリエンス、運用効率の向上とコスト節減を実現することができます。

そして、目標と要件を満たす単一ベンダーのSASEプロバイダーが提供するUnified SASEなら、より早くそれを達成することができます。

Unified SASEがお客様の組織にぴったりだと思われる場合に、最後に残る問題があります。それは、実装をどこから開始すればよいのかという点です。組織が辿る最も一般的な道筋には2つあります。

[4] 2023年のPonemon Institute社のレポート



道筋1: SSEから開始（具体的にはZTNA）

「SSE導入レポート2023」によると、67%の企業がSASEの導入をSSEテクノロジーから始めようと考えています。これに該当する場合は、VPNをHPE Aruba Networking ZTNAに置き換えて、データセンター、クラウド、または両者の間に存在するプライベートアプリケーションへのゼロトラストアクセスを検討してください。

HPE Aruba Networking SSEの詳細はこちら

道筋2: SD-WANから開始

SASEの導入をSD-WANから始めます。HPE Aruba Networking EdgeConnectで単一のSD-WANを確立し、セキュアなエッジポートフォリオ（小規模オフィス/ホームオフィス、ブランチ、キャンパス、またはWAN）を完成させます。

HPE Aruba Networking EdgeConnectの詳細はこちら

専門家とのチャット: arubanetworks.com/company/contact-us/contact-us-form

最適な導入検討を。
HPEのプリセールススペシャリストに
お問い合わせください。

お問い合わせ

BR_UnifiedSASE_RVK_081023 a00133570jpn