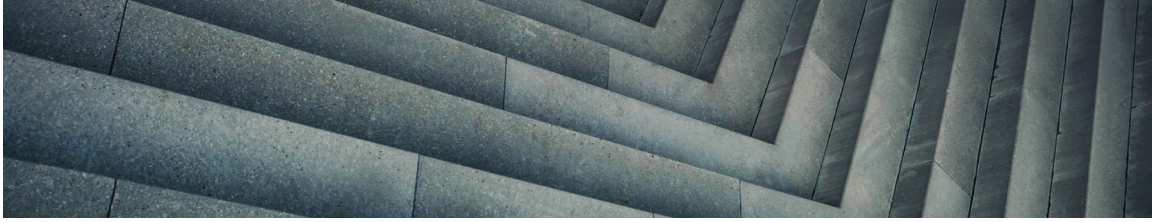
S&P Global
Market Intelligence
Business Impact Brief



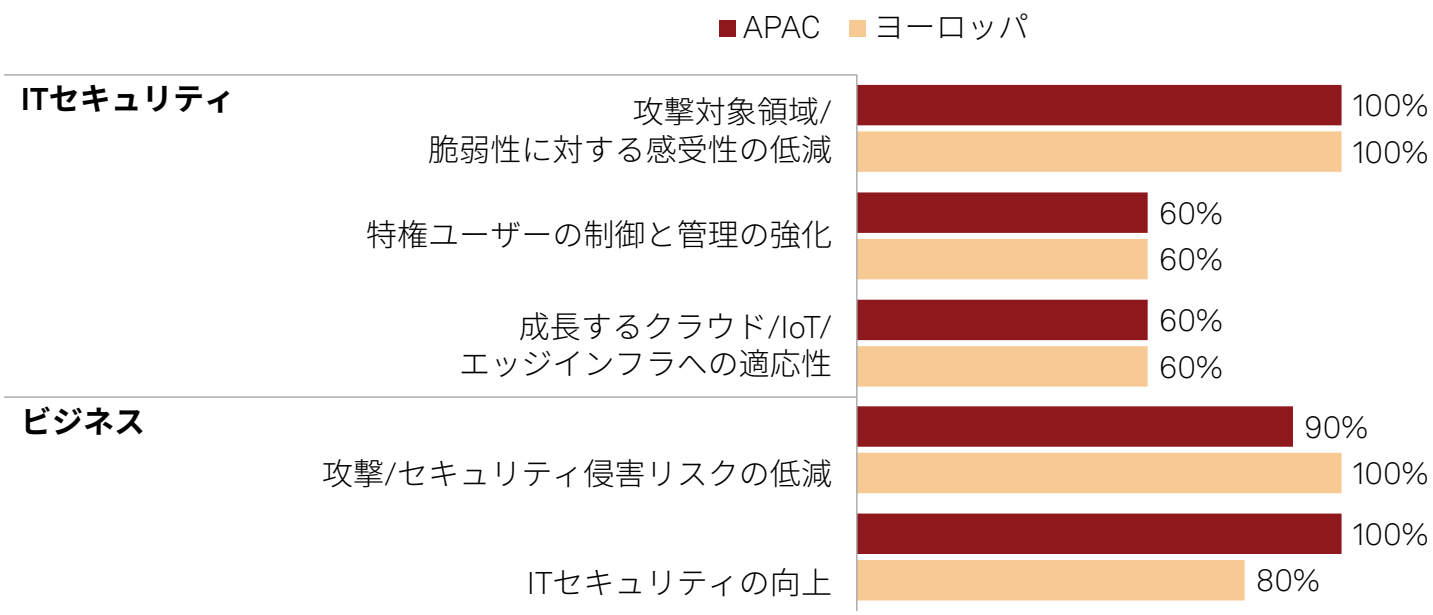
セキュア アクセス サービス エッジがビジネスとITにもたらす主なメリット

見解

デジタル トランスフォーメーション、変化するワークパターン、クラウドベースサービス利用の継続的な増加、エッジ コンピューティングや人工知能などのテクノロジーの出現により、従来の境界ベースのセキュリティモデルには大きな負荷が生じています。ゼロトラスト原則に基づくセキュア アクセス サービス エッジ（SASE）は、安全なウェブゲートウェイ、サービスとしてのファイアウォール、クラウドアクセスセキュリティブローカー、ソフトウェア定義WANなど、クラウドネイティブサービス群として提供される一連の統合リモートアクセスおよびアイデンティティ制御を提供します。SASEは2019年に登場し、すでに20社を超えるベンダーがSASEプラットフォームを提供しており、その採用率は年ごとに高まっています。

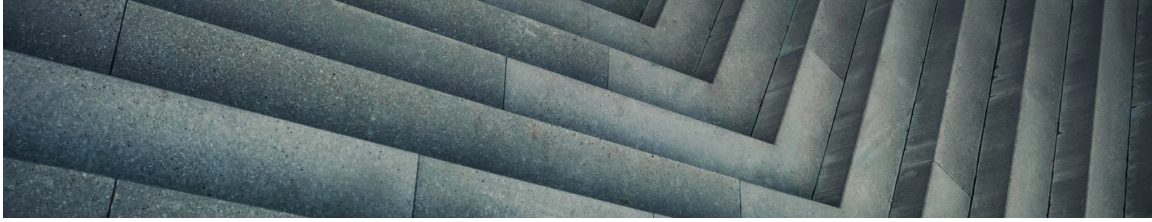
S&Pグローバル・マーケット・インテリジェンスは、2022年後半から2023年前半にかけて、ヨーロッパおよびアジア太平洋（APAC）地域の回答者を対象として、SASEの採用決定に関する主要な意思決定基準、受益領域、導入モデル、障害/得られた教訓に焦点を当てた、SASEカスタム調査プロジェクトを実施しました。本レポートは、20名の仮想エグゼクティブ ディスカッション ボード（APAC=10、ヨーロッパ=10）が回答したSASEのメリット分野上位5つに焦点を当てています。ユーザーへのメリットは重要ですが、この上位ランキングではユーザーへのメリットよりもITセキュリティとビジネス上のメリットを優先しているため、いずれの地域においてもユーザーへのメリットが含まれていません。これは、調査参加者の視点の偏りによるものである可能性があります。参加者は、主にITおよびセキュリティに熟練しており、技術上およびビジネス上の懸念に重点を置いていると考えられます。

SASEのメリットの上位分野



Q. SASEのメリットの上位分野
基準：仮想エグゼクティブ ディスカッション ボードの全回答者（n=20、APAC=10、ヨーロッパ=10）
出典：S&Pグローバル・マーケット・インテリジェンスによるカスタムSASE調査、2023年3月

S&P Global
Market Intelligence
Business Impact Brief



ビジネスインパクト

この調査によると、SASE導入に関与している組織は、すでにこのテクノロジーのメリットを得ているか、または得られるのを期待していることが明らかになっています。当然のことながら、言及された各分野のメリットは重複する傾向にあります。例えば、攻撃対象領域を縮小し、脆弱性に対する感受性を低下させること（ITセキュリティ上のメリットとして挙げられた第1位）は、攻撃やセキュリティ侵害のリスクも低減させることになり、これはビジネスにおけるメリットとして総合ランキングでは第2位となっています。

ITセキュリティ：攻撃対象領域を縮小し、脆弱性に対する感受性を低減 SASEには、攻撃対象領域を縮小し、組織の脆弱性に対する感受性を低減するメリットがあります。これには、従来の境界ベースの制御の代わりにユーザーおよびデバイス/エンティティレベルでアクセスを制限する、高度にスケーラブルなゼロトラストベース、クラウドネイティブなセキュリティ制御から得られるメリットも含まれます。SASEのアイデンティティベースの制御は、アクセスを許可されたエンティティへのアクセスを制限し、攻撃者によるラテラル ムーブメントの抑止に役立ちます。SASEは、マイクロセグメンテーションおよび強制的な信頼性レベルを組み合わせたアイデンティティベースの制御により、安全な通信を保証します。

ITセキュリティ：特権ユーザーの制御と管理の強化 特権アクセス管理は、今日の多くの組織にとって重要な関心事です。特権ユーザーは、非常に広範囲なアクセス権を持つため、彼らの認証情報で組織データにアクセスし、その高い信用レベルを使用して攻撃の拡大を狙う者が、それらのアイデンティティを頻繁に標的にするとしても驚くには値しません。SASEの優れた利点の一つは、その合理的かつ一元化されたロールベースのアクセス制御 （RBAC）です。RBACとゼロトラスト ネットワーク アクセスを組み合わせることで、特権ユーザーは自分のロールに必要な特定のリソースにのみアクセスできるようにし、特権資格情報を利用したセキュリティ侵害による潜在的な損害を抑制することができます。SASEは「ジャストインタイム」アクセスにも対応しており、重要なリソースへの一時的な時間制限付きアクセスを提供します。

ITセキュリティ：成長するクラウド/IoT/エッジインフラへの適応性 SASEのアーキテクチャは、サービスエッジでセキュリティポリシーを適用するように設計されているため、クラウド、IoT、およびエッジのユースケースに適しています。また、クラウド、IoT、エッジデバイス、データセンター、オフィス間の安全なトンネルを通じてクラウドからエッジへの安全な接続性を確保するとともに、ネットワーク遅延の低減によりリモートデバイスの接続性を向上させます。SASEには、デバイス認証、暗号化、ポリシーベースのアクセス制御などのIoTセキュリティ機能が組み込まれており、IoTデバイスとデータにおける高いセキュリティを実現します。

ビジネス：攻撃/セキュリティ侵害のリスクの低減 ビジネスの観点から見ると、攻撃やセキュリティ侵害のリスクは高く、かつその修復には多額の費用がかかります。ビジネスリーダーは、当然のことながらリスクの低減と回避に関心を寄せており、今日のほとんどの組織では取締役会レベルの懸念事項です。ほとんどの調査参加者によれば、意思決定者はSASEがデジタル トランスフォーメーション プロジェクトの成功に役立つことを明確に理解しており、導入前にSASEの堅固なビジネスケースを構築する必要はないということでした。

ビジネス：ITセキュリティの向上 SASEのクラウドネイティブ アーキテクチャにより、従来のオンプレミス アプローチと比較して、より高いレベルのスケーラビリティとレジリエンスを実現できます。従来のツールと比較してより迅速なセキュリティ アップデートと脅威インテリジェンスの適用と更新が可能であるため、プラットフォームの全体的なセキュリティと分析の最新性が向上します。SASEの一元化されたアーキテクチャは、従来のアプローチよりも管理がシンプルでかつ合理化されており、必要なデバイスと人員が少なくて済み、管理を簡素化しながらも攻撃対象領域を縮小させることができます。

今後の展望

今後、SASEが普及することは明らかです。クラウドネイティブのセキュリティ管理とゼロトラスト ネットワーク アーキテクチャのサポートおよびセキュリティとネットワークドメイン全体で一元化されたポリシー管理と相まって、全体的なリスクの低減とネットワーク管理の簡素化が実現し、エッジへのポリシー適用を促進すると同時に、スケーラビリティとレジリエンスは強化されます。クラウド、エッジ、IoTに依存する、ますます複雑化する今日のIT資産を考慮すると、SASEは正しい方向に向けた重要な一歩であると言えるでしょう。

verizon

この調査は、企業が不要な雑多な情報を排除しつつ、良い点と悪い点の両方を含めた真実を把握するために行われました。また、企業が直面する課題とSASEによって得られるメリットを理解することで、提供されるサービスを進化させることができます。弊社のネットワークセキュリティを専門とする経験豊富なコンサルタントは、戦略的アプローチおよび目標とするオペレーションモデルの特定、継続的なプロアクティブマネジメントの提供など、SASE導入プロセス全体を通してお客様をサポートします。SASE導入のリスクを低減し、より大きなメリットをより迅速に実現できるよう支援いたします。

EMEA whitepaper　APAC whitepaper