ガイド

SASEへの移行を成功させる秘訣

verizon business

目次

複雑なSASE環境への統合に対処する方法

業務を効率化しながらネットワークセキュリティを強化するために、セキュアアクセスサービスエッジ（SASE）を導入する企業が増えています。しかし、SASE環境の導入と統合は複雑なプロセスになる可能性があります。潜在的なリスクとは何でしょうか? また、企業はどのように対処すればいいのでしょうか? ベライゾンの専門家がノウハウを提供します。

サイバー脅威は増加し続けており、攻撃はますます巧妙化しています。ネットワークセキュリティは、これまで以上に強力かつスマートに機能する必要があります。しかし同時に、多くの企業がアプリケーションやデータにアクセスするためにマルチクラウド環境に大きく依存するようになったため、攻撃対象領域が拡大し、課題がさらに深刻化しています。また、リモートワークによる柔軟な勤務形態が、この状況はさらに難しくしています。

こうしたことにより、企業のネットワークセキュリティに対するプレッシャーが高まっているため、多くの企業がSASEを導入しているのも不思議ではありません。

SASEは、定義上、ソフトウェア定義の広域ネットワーク（SD WAN）とセキュアサービスエッジ（SSE）テクノロジーを組み合わせたものです。あらゆる接続形態（セルラー、パブリックインターネットまたはプライベートネットワークなど）にわたる完全に統合された広域ネットワークを、エンドツーエンドのセキュリティスタックと組み合わせて提供します。SASEでは、ネットワークとセキュリティを単一のフレームワークに統合することで、ポリシー管理の簡素化とセキュリティの強化というメリットを実現します。さらに、ゼロトラストアプローチでアクセス管理を強化し、許可されたユーザとデバイスのみがネットワークに接続できるようにします。また、従来のネットワークセキュリティモデルに伴うハードウェアおよび構成管理の制約を排除することで、最新の分散型クラウド環境もサポートします。

SASEを導入すると、企業はより包括的なアプローチに移行して業務を効率化できます。サイバー脅威からの保護を強化し、ハイブリッドで働く従業員にどこからでも安全なアクセスを提供できます。ただし、SASEの導入には課題がないわけではありません。複数のテクノロジーが絡む複雑な統合の管理から新しいビジネスプロセス構築まで、多くの課題を伴う複雑なプロセスになる可能性があります。

SASE 導入の課題

1 既存環境とテクノロジーからの移行

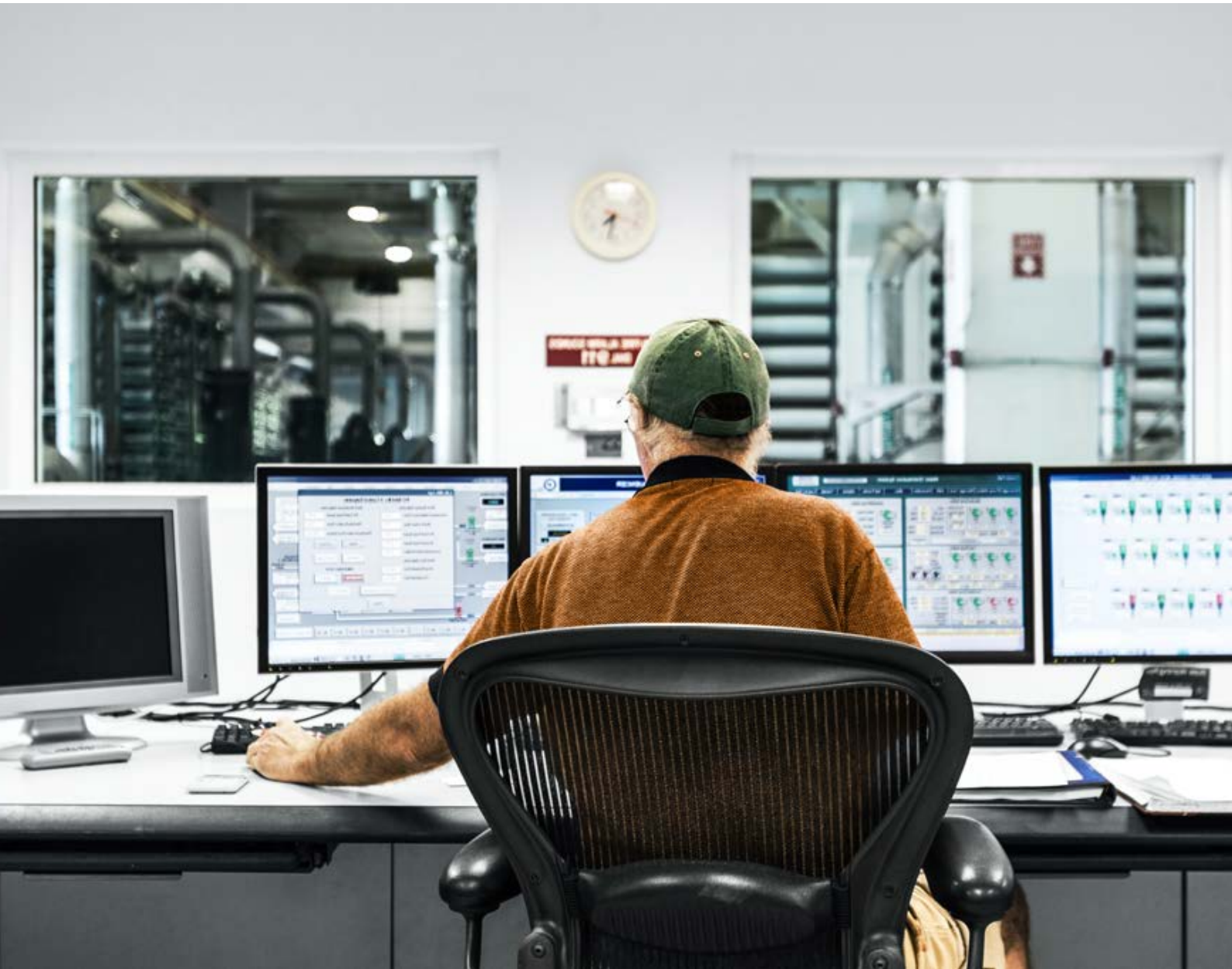
ベライゾンのお客様からよく聞く問い合わせに、SASEの導入を決定するための既存ベンダーとの契約と、テクノロジーのライフサイクルへの対処についての質問があります。IT組織が減価償却サイクルに伴うITインフラの交換を検討し始めると、業務においてテクノロジーに依存している部分がかなり多いため、大規模なテクノロジーのアップグレードがビジネスプロセス、ひいてはユーザに与える影響が浮き彫りになります。したがって、ビジネスとそのユーザへの混乱を最小限に抑えるために、移行またはアップグレードプログラムを慎重に計画することが重要です。

Jeff Patersonは、大規模なグローバル企業をサポートする、ベライゾン英国のソリューションアーキテクトです。「既存のアーキテクチャを、新しいSD WANまたはSASE環境に置き換えるだけでは不十分です。統合の課題は常に存在します。これらのレガシーハイブリッド環境だけでなく、CSP/クラウド環境にもネイティブに統合できる技術的能力が実証されているSSEコンポーネントと組み合わせたSD WANテクノロジーを選択することが、総合的なSASEソリューションへの移行と変革を可能にする鍵となります」とPatersonは指摘します。

2 ネットワーク部門およびセキュリティ部門による調整とベンダー選択

多くの企業は、初めてネットワーク部門とセキュリティ部門を統合して連携させるという課題にも直面します。ネットワークとセキュリティにおけるテクノロジーは、従来からそれぞれの分野で実績ある専門ベンダーがサポートしています。両分野において専門ベンダーであると断言できるのは、ほんのわずかです。SASEが適切なソリューションであることは概念的には誰もが同意していますが、どのベンダーを採用するかについてネットワークとセキュリティ部門の合意を得ることは、一部の組織にとっては課題となっています。どのベンダーを選択するかについて全員の意見を一致させるには、たびたび徹底的な分析と議論のための時間が必要になります。

> 既存のアーキテクチャを、新しいSD WANまたはSASE環境に置き換えるだけでは不十分です。統合の課題は常に存在します。
>
> **Jeff Paterson**
> ベライゾンビジネス、ソリューションアーキテクト



3 何から始めるべきか：複数のテクノロジーを統合する

異なるベンダーのテクノロジーを統合し、シームレスに連携させることは、単一ベンダーのソリューションのようにシームレスに相互運用できるように設計されていない可能性があるため、複雑になることがよくあります。これには、クラウドセキュリティのプロビジョニングとSD WANソリューションへの統合、およびSaaSポリシーの構成が含まれます。単一画面（SPoG）のダッシュボードが必要な場合、さまざまなテクノロジーベンダーからのインサイトを組み合わせる必要があり、実現が非常に困難になる可能性があります。

企業は、ネットワーク部門とセキュリティ部門の根本的に異なる要件にも対応する必要があるのです。たとえば、セキュリティ部門は、イベントや脅威にリアルタイムで対応できるように、セキュリティポリシーの構成へのフルアクセスを必要とすることがよくあります。これとは対照的に、ネットワーク部門はSD WANポリシー設定へのアクセスを制限するだけでよい可能性があり、不注意による致命的な変更を実行することなく、セルフサービスによる自律的な作業を行なえばよいのです。

では、企業はどのようにこれらの課題を乗り越え、ビジネス目標を満たすSASEの実装を成功させることができるのでしょうか?

成功のための計画を立てる

統合を慎重に計画し、各段階で何が関与し、各要素の責任者が誰であるかを把握することが重要です。完璧な最終形を実現するための明確な指針となるロードマップを作成し、全員の認識が一致していることを確認します。「目標を明確に定義してください」とJeff Patersonは言います。「あるいは、選んだパートナーに助けを求め、協力して全体的な目標について合意してください。そして、重要なのは、これを文書化して、すべての関係者の合意と承認を得ることです。

> 協力して全体的な目標について合意してください。そして、重要なのは、これを文書化して、すべての関係者の合意と承認を得ることです。

Jeff Paterson
ベライゾンビジネス、ソリューションアーキテクト

適切なタイミングで適切な人材を関与させる

SASEの統合は、多くの流動的要素と多くの人が関与する複雑なプロセスです。すべての関係者にプロジェクトについて説明し、成功に向けて全力を尽くすことが重要です。全員が同じ認識を共有していなければ、「ネットワーク部門とセキュリティ部門の間で連携が取れず、ベンダーを選択する際に断片的なアプローチが取られ、SD WANおよびSSEコンポーネントのアーキテクチャと設計がサイロ化してしまう可能性があります」と、ベライゾンビジネス、Tier 2デザインオーソリティーチームでSASEのテクニカルリーダーを務めるアソシエイトフェローのFyllon Papadopoulosは指摘しています。

これらのコンポーネントの統合が後回しにされた場合、結果としてSASEソリューションに課題をもたらす可能性があります。「ベンダーの選択によっては、SD WANエンドポイントでのSSEトンネルのプロビジョニングが自動化をサポートしない可能性があり、その結果、構成のオーバーヘッドが大幅に増加する可能性があります」とFyllon Papadopoulosは話します。「あるいは、トンネルのヘルスチェックや、SD WANとSSEコンポーネント間のAPIが不足しているためにトンネルが自動的にフェイルオーバーされず、手動による介入が必要になる可能性もあります。

もしくは、特定のクラスのアプリケーションに実装したいセキュリティ検査には、構成が複雑なSD WANポリシーが必要になる場合もあります」

この問題を回避するには、ネットワーク部門とセキュリティ部門がプロジェクトの初期段階から緊密に連携して次のことを行うことが重要です。

- ベンダーの選択と相互運用性について調整する
- 全体的なアーキテクチャと設計が意図どおりに機能することを確認する
- 一元化と統合の経済性を十分に活かす
- テクノロジーが特定のユースケースをサポートしていることを確認する

プロジェクトの規模について合意する

特定のビジネスニーズ、予算、現在の設定に応じて、どのような実装が適切かを決定する必要があります。過剰な出費やニーズを満たさないものの実装を避けるために、最初に確立することが重要です。Jeff Patersonは次のように述べています。「組織の機能を実現する重要なアプリケーションに焦点を当てるのか、それとも、作業が時間、労力、支出の増加を伴い、簡単に数百、数千のアプリケーションに及ぶ可能性がある全社的なすべてのアプリケーションに拡大するのでしょうか？」最初に適切な計画を立てることで、より効果的で合理的な実装が可能になるのです。

> 組織の機能を実現する重要なアプリケーションに焦点を当てるのか、それとも、作業が時間、労力、支出の増加を伴い、簡単に数百、数千のアプリケーションに及ぶ可能性がある全社的なすべてのアプリケーションに拡大するのでしょうか？
>
> **Jeff Paterson**
> ベライゾンビジネス、ソリューションアーキテクト

段階的なアプローチを検討する

実装には万能な方法は存在しないため、企業は特定のニーズに合わせて導入方法を構築する必要があります。しかし、大企業の場合、ネットワークとセキュリティを一度に移行することは、一般的に過剰な労力を必要とするため、事業継続にとってリスクが高いと考えられています。「顧客の事業規模が大きく、レガシーアプリケーションが多数ある場合、段階的なアプローチを採用する傾向があります」と、ベライゾン、セキュリティソリューションアーキテクトのMike Hannanは言います。「私たちは、範囲を重要なアプリケーションに限定することに重点を置いており、そこで概念実証、小規模なテストから大規模なテストへ、そして完全な本番環境へと移行します」

> 顧客の事業規模が大きく、レガシーアプリケーションが多数ある場合、段階的なアプローチを採用する傾向があります。

Mike Hannan
ベライゾンビジネス、セキュリティソリューション
アーキテクト

時間枠を現実的に考える

養子縁組の方法が一つではないのと同様に、ネットワークとセキュリティの統合にかかる時間の長さにも決まったものはありません。「ネットワークとセキュリティの移行を検討している場合、それは一度に取り組むにはかなり大きな課題です」とMike Hannanは言います。「専門的で経験豊富なパートナーだけでなく、多くの社内リソースも必要になる可能性があります」そのため、プロジェクトの規模、達成すべき目標、限られた時間内に達成できる成果について現実的に考えることが重要です。「段階的なアプローチで、より達成しやすくなります」とHannanは続けます。「おそらく最初にリモートアクセスに取り組み、次に拠点通信に移行することで、ゼロトラストの決定を下せるように可視性を高めることになります」

> ネットワークとセキュリティの移行を検討している場合、それは一度に取り組むにはかなり大きな課題です。
>
> **Mike Hannan**
> ベライゾンビジネス、セキュリティソリューション
> アーキテクト

適切なパートナーを見つける

SASEの導入は非常に複雑になる可能性があるため、経験豊富なパートナーと協力する必要があります。「どの地域にお住まいでも、複雑でありながら安全なネットワークの設計、実装、運用する経験と実績のあるプロバイダーを選択し、協力して作業を進めてください」とJeff Patersonは言います。

このような重要なITの変革には、さまざまな大企業におけるネットワークやセキュリティインフラの変革をサポートしてきた経験を持ち、SASE環境においてお客様に必要なものを明確にし、それを展開し、将来にわたってサポートできるパートナーからのガイダンスやサポートが必要になるはずです。「ビジネスの基盤となる安全に“つながった”ネットワークを提供してきた実績のあるプロバイダーと提携することが不可欠です。そうすれば、SASEの初期実装と既存環境との統合の両方がスムーズに行われ、サービスの継続的な管理と運用が運用チームによって十分に理解されているという確信が得られます」とJeff Patersonは強調します。

> ビジネスの基盤となる安全に“つながった”ネットワークを提供してきた実績のあるプロバイダーと提携することが不可欠です。
>
> **Jeff Paterson**
> ベライゾンビジネス、セキュリティソリューション アーキテクト

ベライゾンに相談する

ベライゾンは、お客様がSASE導入のどの段階であってもサポートできます。ネットワークの設計、既存IT資産のスムーズな引き継ぎ、安全なネットワークの変革と管理において20年以上の経験を持っています。ベライゾンの経験豊富なチームは、数多くのベンダーおよび業界の認定を取得しています。そのため、ビジネスニーズと最適なテクノロジーを組み合わせることに長けています。また、ベライゾンはデジタルネイティブで自動化された共同管理および完全管理の安全なネットワークソリューションを提供するために、ネットワークオペレーションセンター（NOC）とセキュリティオペレーションセンター（SOC）への継続的な投資を行っています。

ベライゾンが、お客様のSASE統合を成功させるための計画と管理をどのようにサポートできるかについては、Verizon.com/business/en-gbをご覧ください。ベライゾンのセキュリティおよびSASEソリューションの詳細情報の取得には、こちらからメールをご登録ください。

関連情報

SASE Management

組織全体のセキュリティを合理化。SASE Managementは、ネットワークとクラウドのセキュリティを統合し、エッジ、オフィス、クラウドにおいて人、データ、デバイスの連携を可能にします。

詳細はこちら >

パートナー

エコシステム全体で業界最高水準のプロバイダーと連携し、シームレスで優れたソリューションを提供することで、組織のパフォーマンス向上と価値の迅速な実現をサポートします。

詳細はこちら >

Digital Enablement Platform

APIをベライゾンと統合し、Digital Enablement Platformを通じてインベントリ、インシデント、変更管理を効率化します。

ビデオを視聴する >