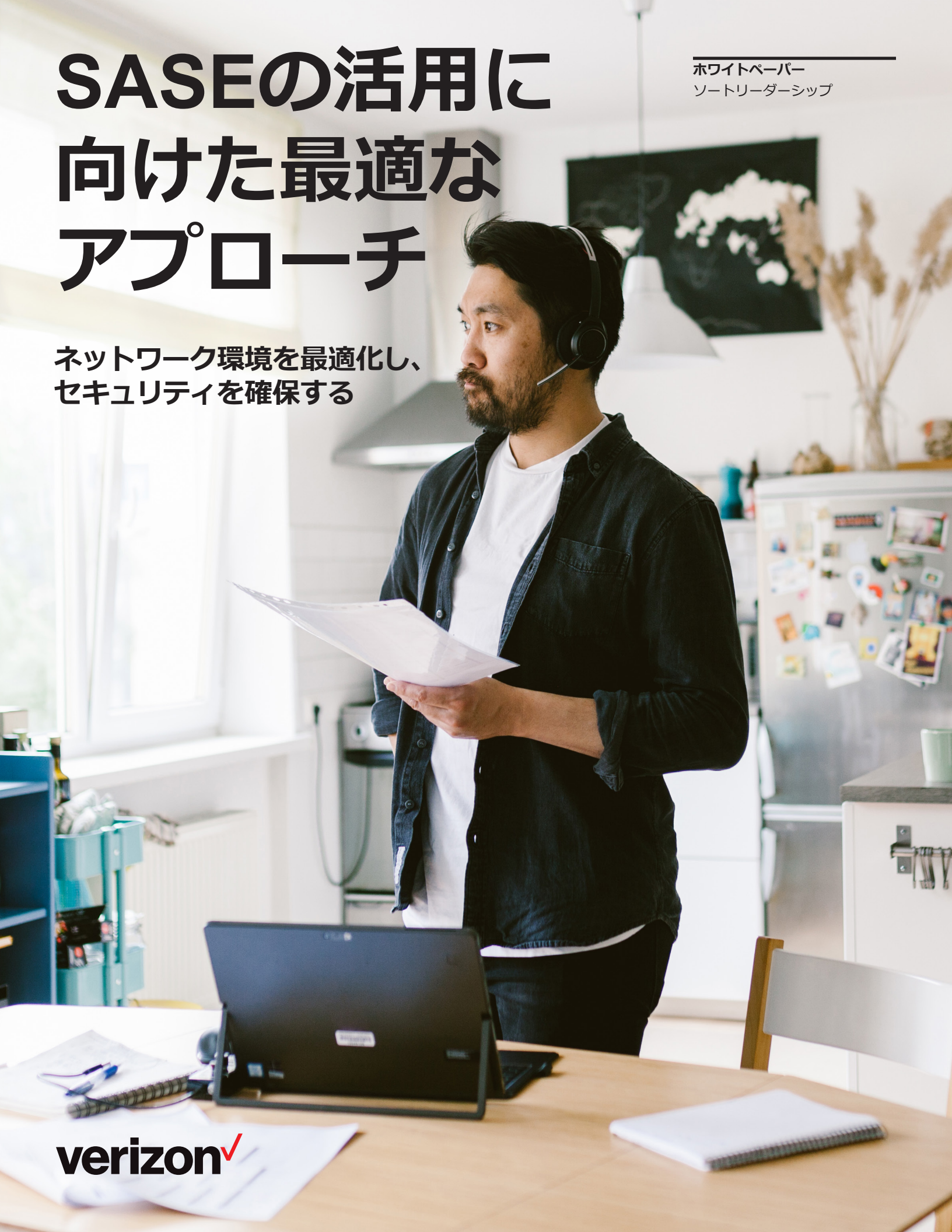
SASEの活用に向けた最適なアプローチ

ネットワーク環境を最適化し、セキュリティを確保する

ホワイトペーパー
ソートリーダーシップ



verizon

はじめに

デジタルトランスフォーメーションによって将来実現すべきことは依然として最優先事項の1つとなっています。その一方で、IT環境が複雑さを増していることを受け、多くの企業のIT部門は、環境の管理とそのセキュリティの維持において大きな課題に直面しているのが現実です。

ネットワークの輻輳を解消したり、潜在的なセキュリティリスクに対処したりする場合、従来型のITアプローチでは、専用のアプライアンスやシステムを増強する手法が用いられます。しかし、エッジアプリケーションが分散したクラウドネイティブの環境では、そのような戦略に同じ効果は期待できません。

しかしご安心ください。現在では、もっと優れたアプローチが存在します。セキュアアクセスサービスエッジ（SASE）の活用です。長たらしい名称であるのは間違いありません。しかし、SASEは、セキュリティとネットワークサービスを統合、パッケージングして提供するまったく新しい手法であり、今日の企業におけるアプリケーションの利用シーン、利用方法に適したソリューションです。

SASEの概要

SASEは、2019年にガートナーが発表したセキュリティに関するクラウドネイティブの新しい概念です。簡単に言えば、SASEは、セキュアゲートウェイやクラウドアクセスセキュリティブローカー（CASB）、ゼロトラストネットワークアクセス（ZTNA）、サービスとしてのファイアウォール（FWaaS）をはじめとするさまざまなネットワークセキュリティサービスをソフトウェア定義のWAN（SD WAN）の機能と統合するネットワークアーキテクチャの1つです。この統合を通じ、クラウドをベースとした統合型のサービスモデルを実現して、デジタルエンタープライズの動的かつセキュアなアクセスのニーズに応えます。

「グローバルネットワークバックボーンを自社で独自に運用し、各種のクラウドサービスに直接接続できるベンダーは高い競争力を有しています。そのようなベンダーが付加的に提供する各種のセキュリティサービスは、バンドルとしても、任意に選択可能なサービスとしても利用できます。そして最も重要な点として、それらのセキュリティサービスは、需要の変化に合わせた利用、スケーリングが可能であり、しかもその一方で、多くのユーザに容易に対応できるのです」
— Mike Fratto、451 Research1

SASEは、IDを中心とした統合型の新たなネットワーク/セキュリティプラットフォームを実現します。この点で、SASEは、セキュリティに対する考え方を戦略的な意味で転換するものであると言えます。グローバルに分散したこのクラウド型プラットフォームでは、リモートオフィスやリモートワーカー、クラウドリソース、IoTデバイスをはじめとする、ネットワークエッジのエンドユーザやデバイスに、安全なネットワーク接続を提供します。このような強固なセキュリティに加え、クラウドを基盤としたSASEのインフラストラクチャでは、リソースがどこにあっても容易に接続できるため、アクセスのパフォーマンスを確実に最適化することが可能です。この結果、ビジネス上のさまざまなメリットが得られ、具体的には、商品の開発や商品の市場投入に要する期間を短縮できるほか、競争上、運用上の課題に、これまでより迅速に対応できるようになります。

こうした一般的な説明とは別に、アナリストのコミュニティやテック業界でしばしば話題に上り、議論されるトピックとなっているのが、SASEの実態の詳細です。ガートナーは、一元的な管理が可能なプラットフォームから提供されるソリューションとしてSASEを位置付けています。しかし一方で、今日の実際の現場では、エンドツーエンドのSASEソリューションには、企業がその目標を達成するのをカスタムのソリューションを通じて支援するために、ベンダー、テクノロジー、サービスを統合することが求められています。

40%

2018年末の時点では、SASEの導入戦略を明示的に策定している企業の割合はわずか1%未満でした。しかし、2024年までにその割合は40%以上になるものと予想されます[2]。

116%

Dell'Oro Groupによれば、「SASE市場の年平均成長率は116%になるものと予想され、その市場価値は2024年までに51億ドルに達する」としています[3]。

1.Mike Fratto、『COVID-19:Secure remote access services in demand as enterprises continue work-from-home strategies』、451 Research、2020年9月10日
2.Neil MacDonald、Lawrence Orans、Joe Skorupa、『The Future of Network Security Is in the Cloud』、2019年8月30日
3. https://www.sdxcentral.com/articles/news/delloro-sase-market-to-hit-5b-by-2024/2020/10/

「SASE」という名称を構成する一字一句が、このソリューション全体における一つひとつの重要なコンポーネントを表現しているのは明らかです。「セキュアアクセス」の意味するところは、セキュリティを実現する手法の再定義であり、それはつまり、ロケーションを中心とする従来のモデルからIDを中心としたモデルへの移行にほかなりません。保護しなければならないのは、エンドユーザが実際に存在するかどうか定かでないロケーションではなく、エンドユーザ自体であることを考えると新たなモデルへの移行は理にかなっています。また、「サービスエッジ」の部分では、必要に応じて利用できるクラウドベースのサービスを重視していることが強調されています。このサービスは、SASEのコアコンポーネントとして重要な役割を果たしており、その背景には、企業がそのコアアプリケーションをクラウドへと移行させている事実があります。

アナリストのコミュニティやテック業界でしばしば話題に上り、議論されるトピックとなっているのが、SASEの実態の詳細です。

SASEが注目される理由

今日のWAN環境では、より強固なセキュリティを求めるニーズが高まっているため、十分な信頼性を備えたソリューションとしてSASEが登場したときには、大きな注目を集めました。このトレンドでは、その原動力となっている数多くの重要な要素があります。新型コロナウイルス感染症によるパンデミックとインターネット上の脅威の拡大のほか、クラウドやエッジへアプリケーションが移行していることや、より動的なアプリケーションの利用の増加などがこれに該当します。さらには、分散アプリケーションの登場によって、パフォーマンス上、セキュリティ上のさまざまな課題も生じています。たとえば、ネットワークのパフォーマンスとセキュリティの最適化の能力と、すばやくスケーリングができる能力を両立しなければならなくなっていることもその一例です。

新型コロナウイルスの感染拡大

2020年に入る前から、リモートワーカーやモバイルワーカーの数は着実に増加していましたが、新型コロナウイルスの感染拡大に伴い、その動きは一気に加速しました。コロナ禍の影響を受けながら仕事をしていくなかで、在宅勤務をはじめとする、なんらかの形態でのリモートワークによる働き方が、当面の間は増加していくものと予想されます。そしてこのような状況から、ビジネスアプリケーションのポートフォリオがクラウドへと移行するのに、さらに拍車がかかっているのです。

セキュリティに対する脅威の増加

クラウドベースのネットワークやサードパーティの提供するネットワーク接続が普及し、グローバル展開やIoTデバイス、リモートワーカーなどのトレンドがますます重視されるようになっています。それに伴いクラウドに移行されるビジネス活動やアプリケーション、データの割合が大きく増加しました。この結果、さまざまな新しいビジネスチャンスが数多く生まれました。一方で、このようなアプリケーションとユーザの分散に伴い、サイバー攻撃を受ける領域が増え、新たな脅威に脅かされるリスクが増大したために、ネットワークを保護することがますます困難になっています。新型コロナウイルスの感染が拡大する中で、リモートワーカーの数は急激に増加しました。そしてこれに起因する脆弱性を特に狙い、ハッカーは攻撃を仕掛けようと企んでいるのです。

仮想化とクラウドへの移行

一般に、ここ数年、企業はデジタルトランスフォーメーションを経験し、ネットワークインフラストラクチャ全体で仮想化を導入し、アプリケーション、データ、ワークロード、これらに付随するトラフィックをクラウドプラットフォームへと移行させてきました。そして、即座に導入、カスタマイズ、最適化のできる動的なアプリケーションの利用が進んでいます。

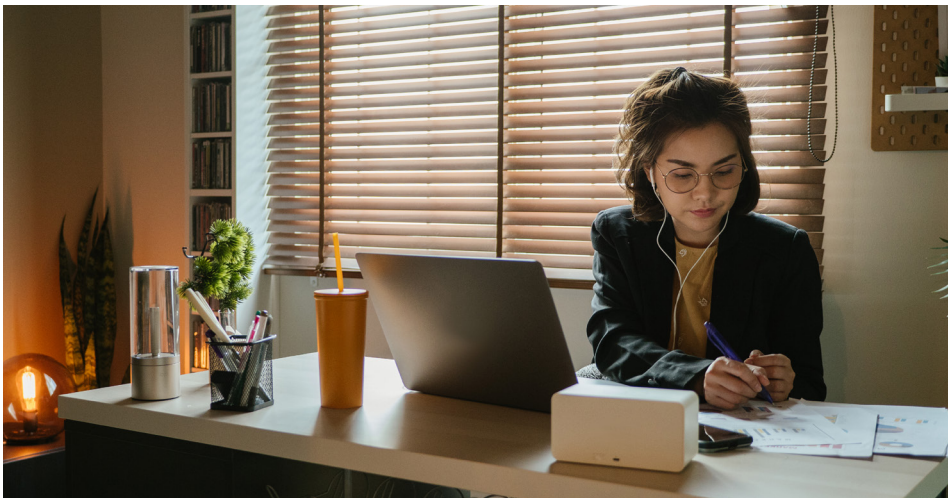
これらのアプリケーションの多くでは、プラットフォームやネットワークにこれまでより負荷がかかり、パフォーマンスやユーザーエクスペリエンスを向上させるために、遅延を減らし、スループットを高めることが求められます。この結果、セキュリティとネットワークの面で、複雑な要素が増え、ストレスが増加しているのです。このようなアプリケーションには、拡張現実（AR）や仮想現実（VR）、IoT、動画画像キャプチャ処理のアプリケーションなどがあります。

ネットワークアプリケーションボックスからの移行

アプライアンスと呼ばれるオンプレミスベースの設備からの移行を計画している企業の数が増加しています。このような固定資産では、大幅な設備投資が必要です。時流に遅れないよう、新たな機能を導入したり、ソフトウェアの更新に対応したりするうえで、高いコストをかけ、ハードウェアの更新を無限に繰り返さねばなりません。

パンデミックの影響により、62%の組織で情報セキュリティインシデントの数が増加しています[4]。

企業は、クラウドコンピューティングや仮想コンピューティングから得られるメリットに慣れ親しむようになるにつれ、クラウドベースのアプリケーションと同じ使いやすさをネットワークベースのアプリケーションにも求めるようになります。一元管理のできるポータル、セルフサービスによる各種機能の起動、包括的な統合セキュリティ/ネットワークソリューションはそのどれもが、急速に期待を集める要素となっています。



4.『451 Research Digital Pulse:CORONAVIRUS FLASH SURVEY OCTOBER 2020』。 https://verizon.northernlight.com/document.php?docid=VK20201016830000071&datasource=VIRNSYND&trans=view&

ベンダーの統合

テクノロジーは、拡張、統合のサイクルを絶えず繰り返すのが常であり、時には、この2つが同時に起こることもあります。新たなテクノロジーが誕生したときに、サイクルの初期の段階では少なくとも一時的に、そのテクノロジーに関して複雑な要素が増えるのが普通です。そして、多くの場合、複数の新規参入業者が生まれます。つまり、組織はこの新しいテクノロジーを利用する場合、まったく異なる多くのベンダーとプロジェクトを進める必要があるのです。しかし、テクノロジーが成熟するにつれて、大規模なベンダー統合が行われるようになります。また、買収や合併を通じてプロバイダーが自社のサービスの完成度を高めようとするのに伴い、企業が関係を持たねばならないベンダーの数は確実に減っていきます。

68%

パンデミックが収束した後の長期戦略を見直していると、68%のシニアエグゼクティブが回答しています[5]。

テクノロジーとベンダーのミスマッチが起こるリスクを抑えられるよう、また、ベンダーとのパートナー関係を築くうえでやみくもなアプローチをしないよう、多くの組織がパートナーにするベンダーの選定をより慎重に進めようとします。そして、組織が求めているのは、セキュリティ、アプリケーション、ネットワーク、言い換えれば、SASEについて幅広い経験を有する数少ない一流のベンダーです。そのようなベンダーなら、求めるサービスをテクノロジーのサイクル全体を通じて間違いなく提供してもらえると、安心できるからです。

複雑さ

組織の今日のIT環境には多数のベンダーと多数のソリューションが存在し、その数は目に見えて拡大する一方であるため、環境の管理は困難を極めます。それは間違いありません。そしてこの問題をさらに複雑にしているのは、社員としてエキスパートを雇用し維持するのが常に困難であるという事実です。このような状況は、企業にとって、複雑さを増す環境に対応したり、あるいは、ベンダーの発するノイズを排除して事実を見極めたりする際にも足かせとなっています。

SASEで実現できること

ネットワークとセキュリティの機能を統合すれば、ネットワークのセキュリティとスケーラビリティを強化しながらネットワークの柔軟性とアプリケーションのパフォーマンスを高めたいとする企業のニーズを満たすことができます。SASEでは、エンドユーザは、どこにいても、どこからアプリケーションやリソースにアクセスしてもそのコネクションを保護する新たな手法を利用できる一方、ビジネスの俊敏性も高められます。

俊敏性の向上

概して、SASEでは、さまざまな手法で俊敏性を強化できます。SASEでは次のことが可能です。

- システムを簡素化でき、統合に関する課題を解決できる
- 安全に短期間でクラウドを導入できる
- ビジネスにおいて、データ、アプリケーション、サービスなどをパートナーと安全かつ容易に共有できる革新的な関係をデジタルで推進できる

SASEやクラウドベースのインフラストラクチャを活用すれば、脅威検知/脅威対策や、セキュアゲートウェイ、次世代のファイアウォールポリシー、Webフィルタリング、サンドボックス、DNSセキュリティなどのセキュリティアプリケーションを必要に応じて簡単に、よりきめ細かいレベルで導入することができます。これらのセキュリティサービスは、エンドユーザに最も近いエッジで提供できます。エンドユーザのロケーションやエンドユーザが利用しているネットワークの形態は問いません。固定回線、モバイルネットワーク、ローミングネットワーク、小規模、大規模のブランチネットワークなどに対応します。

ITインフラストラクチャの簡素化

セキュリティスタックの統合プロジェクトを実施する場合は、SASEベースのモデルを第一に検討すべきです。このモデルなら、利用するセキュリティ製品の数が無秩序に増えるのを抑えられ、定型業務でありながら不可欠なメンテナンスやアップデート作業など、関連する管理作業のオーバーヘッドを削減できるので、ITインフラストラクチャが簡素化されます。通常、このようなメンテナンスやアップデートの作業は、たびたびスキルが不足しがちだったり、あまりにも多くの業務を抱えているIT部門の負担になっています。ベンダーを任意に選択できるようになり、最終的にSASE環境の一元管理が可能になれば、さまざまなメリットがあるのは明らかです。

ネットワーク機能とセキュリティ機能の統合

SASEでは、アプリケーションを意識したルーティングやファイアウォールをはじめとする多数のネットワーク機能とセキュリティ機能を統合することもできます。SD WANネットワークやクラウドサービスはもはや珍しいものではありませんが、クラウド型のセキュリティ機能とアプリケーションの登場によって、これら機能の統合の必要性に注目が集まるようになっています。クラウドの単一の制御ポイントからセキュリティ機能とアプリケーションを管理できれば、数多くのメリットが得られます。たとえば、アクセスのパフォーマンスを最適化したり、運用を簡素化したり、セキュリティポスチャを強化したりすることが可能になります。

「拡張性、柔軟性に優れた低レイテンシーのシンプルな環境と、幅広く展開できるセキュリティを顧客が求めるようになったために、WANエッジとネットワークセキュリティの市場の統合が避けられなくなっています」[6] ーガートナー

パフォーマンスの向上

SASEでは、クラウドインフラストラクチャのあらゆる利点を利用できるだけでなく、グローバルのSD WANサービスや組み込みの最適化機能を通じてネットワークのパフォーマンスを強化することも可能です。さらには、ハイブリッドのネットワークとクラウドのセキュリティサービスの統合によって、エンドユーザのセッションに近い所でデータの検査ができるようになり、パブリッククラウドのトラフィックにデータセンターを経由するよう強制する必要がなくなります。この結果、レイテンシーを抑制でき、アプリケーションのパフォーマンスを高められます。

優れたセキュリティ

かつてネットワークの境界は、脅威からの攻撃を防ぐ場所として機能していましたが、今日の分散ネットワーク環境では、そのような効果はもはや期待できません。SASEでは、WANセグメントやVPNセグメントの境界を重視するセキュリティアプローチだけに依存する代わりに、IDとアプリケーションに応じてアクセスのセキュリティをきめ細かく判断できます。

コストの削減

クラウドをベースとする単一の仮想プラットフォームにアプリケーションを移行させれば、ハードウェアのポイント製品に依存する必要がなくなるため、拡張性と俊敏性を強化しながら、設備投資を削減でき、必要なITリソースを抑えられます。利用するベンダーを1つに集約することで管理とソリューションの統合がシンプルになり、購買や契約の交渉さえも簡素化されます。

5.『働き方の未来』、ベライゾン https://enterprise.verizon.com/resources/ja/reports/future-of-work-reimagining-business-as-usual.pdf
6. ガートナー、『Market Trends:How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge』、2019年

SASEを正しく活用する：4つの重要な要素

SASEを正しく活用するのは容易ではありません。いくつもの大きな課題があります。1つには、SASEが絶えず進化を続けている注目のテクノロジーである点が挙げられます。しかし、SASEを構成する主要な要素は少なくとも過去10年間にわたり、なんらかのかたちで存在してきました。このことを忘れてはなりません。たとえば、ベライゾンは、SASEを構成するITソリューションを、20年以上にわたって提供し続けています。

このようなソリューションにおいて、ベライゾンは広範な経験を積んでいるため、SASEに関して他に類のない価値の高い知見を有しています。SASEのアプローチをネットワークサービスとセキュリティサービスに適用する場合、どのような課題があるのか、また、適用によってどのような可能性を期待できるのか、詳しく理解しているのです。SASEを正しく活用するために適切な対応が必要な注目すべきポイントが主に4つあると、現場での経験からベライゾンは考えています。

1.テクノロジー間の連携

SASEは、1つであるゆる課題に対応できる万能のソリューションではありません。つまり、組織固有の任意の課題を効果的に解決できる環境を構築するには、さまざまなテクノロジーを問題なく使いこなせなければなりません。

ネットワーク

SASEを導入しようとしている企業には、物理レベル（プライベートIPやMPLS）から仮想レベル（SDNレイヤー）に至る領域のさまざまなネットワークテクノロジーを統合する能力が求められます。もちろん、ここで目指しているのは、トラフィックルーティングの機能や優先順位付けの機能、帯域の最適化機能を備える完全に統合されたSD WAN機能の構築にほかなりません。さらにそのような組織なら、SD WANに加え、WANの最適化やルーティングをはじめとするサービスとしてのネットワーク機能も導入することが可能です。

アプリケーション

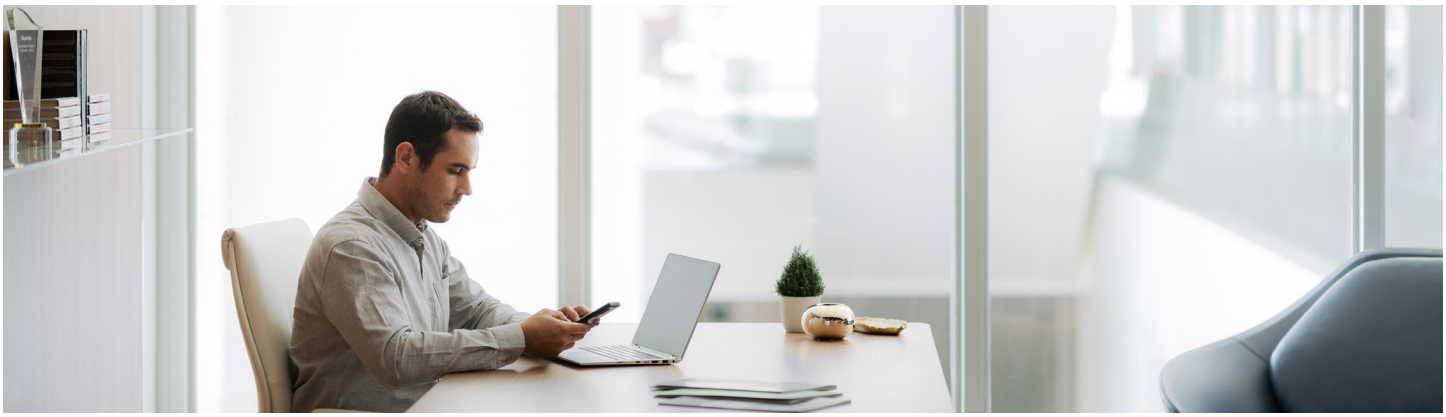
場所を問わずにユーザやモノをクラウドのあらゆるアプリケーションと安全につなぐことがSASEの目的であるため、ZTNAやセキュアWebゲートウェイ（SWG）、CASB、FWaaSなどのセキュリティソリューションを組み合わせることが必要になります。

エッジコンピューティング

エッジコンピューティングもSASEの重要な構成要素の1つです。エッジコンピューティングの機能には、コンテンツ配信ネットワークやマルチアクセスエッジコンピューティング（MEC）、IoTゲートウェイなどがあります。そして、これらの複雑な分散システム全体を対象としてセキュリティを管理することが不可欠です。そのためには、エッジコンピューティングのどのような点がSASEのモデルに適しているのかを詳しく理解している必要があります。

デバイス

モバイルデバイスやモバイルアプリケーションの数が飛躍的に増加し、それらがネットワークエッジにおいて占める割合が大きくなってきています。これらのデバイスとオペレーティングシステムがネットワークと接続する方法やネットワークとやり取りをする方法を効果的に管理することが企業には求められるとともに、接続ややり取りのセキュリティを完全に確保することが求められるようになります。



2.オーケストレーション

SASEでは、さまざまなテクノロジーコンポーネントを統合する方法がきわめて重要になります。

サービスの切り替え

サービスの切り替え機能は、サービスデリバリー環境の自動化と最適化を担う役割を果たしているため、SASEにおける重要なコンポーネントの1つになっています。仮想ネットワークでこの機能を利用する場合、コネクテッドサービスの展開と運用を自動化するために、オーケストレーションツールやオーケストレーションシステムの使用に関する専門知識が必要です。

最適化

現状では、単一のエンティティだけでエンドツーエンドの完全なSASEソリューションを提供することはできません。そのため、個々の組織が求めるソリューションを実現するには、複数のテクノロジーや製品を組み合わせることが必要になってきます。新規のテクノロジーコンポーネントとすでに展開済みのテクノロジーコンポーネントのそれぞれが最大限にその能力を発揮できるように各コンポーネントを最適化することが今後重要になります。

パフォーマンスのテスト

SASEの特徴である多機能の複合環境を念頭に置くと、システムが適切に統合されていて期待通りのパフォーマンスを発揮しているのをテストできる能力が不可欠になります。そのためには、適切な手順と最も効果的な構成で機能が展開されているかどうかを確認できるよう、統合、パフォーマンス、負荷に関するテストを実施する適切なツールが必要です。

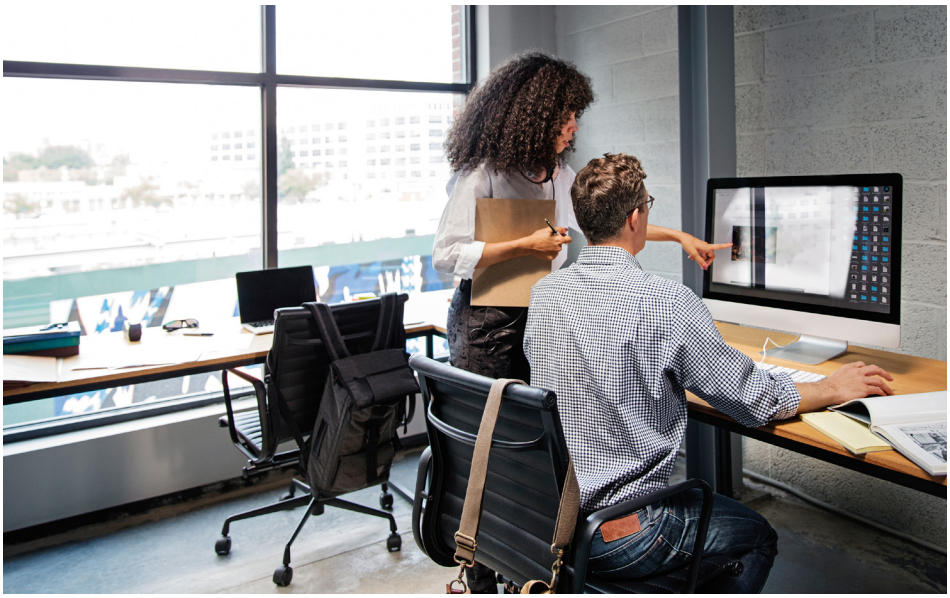
3.組織を横断した運用

過去10年にわたり企業のネットワークチームとセキュリティチームが連携を強めているのは事実ですが、まだ、ほとんどの場合、両者は独立したグループとして組織されています。SASEはその性質上、従来は分離されていたネットワークとセキュリティという2つのサービスコンポーネントを統合するので、本番環境におけるセキュリティとネットワークの管理方法を再考する必要があります。ネットワークと情報通信のテクノロジーの融合に伴い1990年代に見られたこれらの運用の統合と同様に、SASEでも、セキュリティとネットワークの管理を組織上の観点から統合しなければなりません。

SASEでは依然として大きな進化が進んでいるため、CIOとCISOのグループは、企業インフラストラクチャの運用サポートにおける個々の役割を再度検討する必要があります。変化は組織全体に浸透します。そして最終的には、企業のSASE戦略を連携して実行しなければならないネットワークアーキテクトやセキュリティアーキテクト、アプリケーションアーキテクトなどに影響を与えるので、適切な管理体制を準備することが不可欠です。

4.ノウハウ

SASEのプロジェクトでは、ネットワーク、SD WAN、仮想アプリケーション、セキュリティ、デバイスに関する広範な専門知識を有していることが成功の前提条件になります。たとえば、企業には、MPLSなどのネットワークプロトコルからクラウドアーキテクチャ、セキュリティアーキテクチャに至る内容について精通するさまざまなスキルを有したITエキスパートが求められます。しかし、この特別なスキルセットを社内の人材に期待できない場合は、代わりにパートナーを探してサポートを求めることが不可欠です。その場合、パートナーには、これらの多様なテクノロジーをその細かな差異に至るまで詳しく理解していることと、それらのテクノロジーのどのような点がSASEのモデルに適しているのかを熟知していることが求められます。

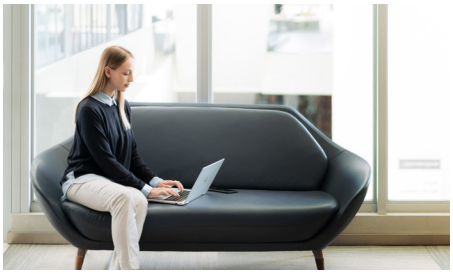


業界をリードする、ベライゾンのSASEアプローチ

ベライゾンは、10年以上にわたり、SASE仕様のサービスやテクノロジーに投資し、これらを提供してきました。多様な専門領域をカバーするベライゾンのアプローチは、主要なパートナーとの協業で補完しながら、さまざまなロケーションに分散しているさまざまなユーザ、データ、エンドポイントをあらゆるアプリケーションやサービスと安全につなぐうえで役立ちます。

ベライゾンのSASEは、ネットワーク業界やセキュリティ業界で認知されているリーダー企業のベンダーが提供する実績のある製品を統合するので、私たちは「最適な組み合わせ」のソリューションと表現しています。これらのベンダーのソリューションは、機能面、検証面、市場での存在感、イノベーションの観点で理想的なもので提供されるテクノロジーやサービスはベライゾンのものと統合されます。

組織が適切なネットワーク、SD WANポリシー、クラウドセキュリティプロバイダーを選択できるよう、また、これらのコンポーネントすべてを完全に管理された統合サービスとして利用できるよう、ベライゾンはこの最適な組み合わせのアプローチを通じてサポートします。



主要なテクノロジーの分野を牽引

業界が認めるリーダーシップ

ネットワークとセキュリティの分野に関して高い専門知識と技術を保有していると、ベライゾンは評価を受け続けており、業界のアナリストから認知されています。ガートナーのMagic Quadrant for Network Services, Global7では14年連続、Magic Quadrant for Managed Security Services, Worldwideでは7年連続でリーダーの評価を獲得[8]しています。また、ここ3年間は、通信事業者としては唯一、Magic Quadrant for Network Services, GlobalとMagic Quadrant for Managed Security Services, Worldwideの両方でリーダーに選出されています。

また、ベライゾンの発行しているデータ漏洩/侵害調査報告書は過去10年間にわたり、進化を続けるサイバーセキュリティ上の脅威の動向を定量的に分析し、評価するための頼りになるリソースとして地位を高めてきました。そして、あらゆる業界のセキュリティプロフェッショナル、ビジネスリーダー、組織から信頼され続けています。

エッジコンピューティング

アプリケーションが企業のデータセンターからクラウドやエッジへと移行するのに伴い、分散ネットワーク全体でデータのセキュリティの要件を満たすための役割が、SASEに求められるようになっています。ベライゾンのAdvanced SASEソリューションは、エッジとクラウドの両方で、さらには、企業のデータセンターでも、アプリケーションのセキュリティを効果的に確保できます。つまり、ネットワークの周辺でデータを処理したり、移動したり、エンドツーエンドでデータを保護したりできるよう、セキュリティをネットワークに統合するのです。

仮想ネットワークサービス

市場をリードするベライゾンの仮想ネットワークサービス（VNS）製品は、オーケストレーションされ完全に管理された拡張性の高いプラットフォームです。このプラットフォームでは、物理ネットワークをオンデマンドの仮想ネットワークに変換するので、ルーティング機能やSD WAN、WANの最適化をはじめとする主要な仮想サービスを通じ、コスト面と俊敏性の面でソフトウェア定義のネットワーク（SDN）からメリットを得られます。

モノのインターネット（IoT）

IoTの分野に関して高い専門知識と技術を保有していると、ベライゾンは業界のアナリストから認知されてきました。ガートナー発行の2020年版『Magic Quadrant for Managed IoT Connectivity Services, Worldwide』レポートにおいて、リーダーの評価を獲得しました[9]。また、ベライゾンの革新的な5G、MEC、およびIoTのプロフェッショナルサービスでは、達成が難しいとされる目標も画期的なソリューションの迅速な構築を通じてクリアできるよう、企業をサポートしています。

デバイスの管理

今日の企業では、ネットワークアプリケーションや仮想的なものを含んだネットワークデバイスの数が急激に増加しており、SASEの実装に際し、これらのアプリケーションやデバイスの統合と管理が不可欠になっています。ベライゾンの先進の管理ソリューションは、ネットワークにつながるデバイスやサービスの管理、追跡、制御において、IT管理者をサポートします。

7.ガートナー、『Magic Quadrant for Network Services, Global』。2020年2月20日公開。アナリスト:Neil Rickard、Bjarne Munch、Danellie Young。Magic Quadrant for Network Services, Global 2015～2020でリーダーの評価を獲得。Magic Quadrant for Global Network Service Providers 2011～2014でリーダーの評価を獲得。Verizon Businessとして、Magic Quadrant for Global Network Service Providers 2007、2009～2010でリーダーの評価を獲得。Verizon Businessとして、Magic Quadrant for Managed and Professional Network Service Providers, North America 2008でリーダーの評価を獲得。
8.ガートナー、『Magic Quadrant for Managed Security Services』。2019年5月2日公開。アナリスト:Toby Bussa、Kelly M. Kavanagh、Sid Deshpande、Pete Shoard。
9.ガートナー、『Magic Quadrant for Managed IoT Connectivity Services, Worldwide』。2019年12月12日公開。アナリスト:Pablo Arriandiaga、Eric Goodness、Leif-Olof Wallin、Jonathan Davenport。

適切なノウハウと豊富な管理の経験

ベライゾンは、複数の専門分野にまたがるノウハウを提供でき、SASEで必要になる主要なテクノロジーの分野において、他社を凌駕する豊富な経験を有しています。

このことは、あらゆる規模の組織がクラウド、ネットワーク、セキュリティの幅広いテクノロジーを購入している今日のビジネスの世界において、きわめて重要な意味を持ちます。これらのシステムやテクノロジーは融合し始めていますが、そのようなタイプの複雑な環境を統合、管理する準備が整っている組織の数はごくわずかです。

このようなテクノロジーのすべてに対応できるシニアネットワークエンジニアとシニアセキュリティエンジニアが、ベライゾンには豊富に在籍しています。これらのエンジニアは、SASEで必要となる主要なテクノロジーのすべてをオーケストレーション、最適化、管理するうえで求められるノウハウとナレッジを保有しています。

ベライゾンの提供するマネージドサービスは、SASEの導入と運用を簡素化できるほか、組織のセキュリティを維持する際の懸念事項と作業を減らします。

SASEを正しく導入するうえで理解しておくべき要素が数多く存在します。いくつか例を挙げれば、運用環境やパフォーマンス要件、セキュリティプロファイルなどがこれに該当します。

ベライゾンは、ネットワークサービスとセキュリティサービスの分野におけるリーダーです。そのため、ベライゾンは、専門的な知恵を結集し、他では見つけることの難しい高いレベルのノウハウとサービスを企業に提供することができるます。ベライゾンでは、実績のある最高のサービスを、最適な組み合わせのソリューションとして統合しています。これにより、SASEを簡素化するほか、企業の負荷を軽減し、懸念事項を減らします。

ベライゾンは、お客様の企業がそれぞれのニーズに最も適した手法でSASEを見出し、導入できるようサポートします。

現在、SASE製品を市場に投入している企業の多くは、テクノロジーハードウェアプロバイダーであり、マネージドサービスプロバイダーは見当たりません。当然のことながら、これらの企業が売り込みを図っているのは、1つですべてのニーズを満たそうとする特定のソリューションです。自身で提供しているケースと、他のテクノロジープロバイダーから供給を受けている場合があります。

このアプローチの問題点は、SASEの場合、現実には包括的なテクノロジーソリューションは存在しないと言うことです。必要なのは、企業の固有の課題や目的に応じて複数のソリューションを統合することです。多くの場合、SASEを適切に利用するためには、テクノロジーの最善の組み合わせを実現でき、スタックのすべてを単一の管理プラットフォームで管理できるプロバイダーをパートナーにすることが企業には求められます。ベライゾンは、これに対応できる特別なポジションに位置しています。

SASEの可能性を最大限に引き出すためには、オーケストレーションと最適化が不可欠ですが、ベライゾンはこれらの領域において豊富な経験を有しています。

今日のIT環境は規模が拡大し複雑化しているため、多くの企業では、自社のネットワークプラットフォームを管理するのがますます困難になっており、そのセキュリティの維持については言うに及びません。

たとえば、SD WANは洗練されたサービスですが、その可能性を最大限に引き出すには、組織における実際の各種アプリケーションに合わせて調整を加える必要があります。そしてそのためには、一般的なアプリケーションや企業固有のアプリケーションに関する知識が必要になります。どのアプリケーションが重要であり、それらのアプリケーションの利用ではどのようなビジネス上の目標があるのかを理解することも求められます。

ベライゾンには、複数の組織の状態を可視化したことによって蓄積してきたインサイトがあります。このインサイトを活用して環境をオーケストレーションおよび最適化し、ソリューションの可能性を最大限に引き出すことができます。

ベライゾンのソリューションでは、単一のサポート窓口を提供するほか、ソリューション全体を可視化したレポートも利用できます。

現在、SASEについて語っているベンダーのほとんどは、コアのSASEセキュリティエレメントだけに言及しており、コネクティビティは無視しているか、重要でないと見なしています。実際には、これら2つを分けて考えることはできません。ベライゾンのソリューションでは、ネットワークプラットフォームとセキュリティコンポーネントの両方を1つにまとめて提供できるため、異なるコネクティビティ手法すべてを対象として、ネットワークのパフォーマンスとセキュリティを直感的に把握することが可能です。

適切なオプション

ベライゾンは、検証され実績のあるアプローチを通じてSASEソリューションをバンドルしています。これにより、簡素化、最適化を実現し、組織に最適なかたちでオーケストレーションを実施しています。

ベライゾンによる、SASEにおける最適な組み合わせのアプローチで特に大きなメリットの1つは、高いパフォーマンスと柔軟性、強固なセキュリティが単一のマネージドサービスの下で実現される点にあります。このような形態により、SASEへのパスが簡素化され、個々のコンポーネントの管理において、企業の負担となりうる懸念事項が解消されます。

ベライゾンが、オーケストレーション、テスト、最適化を実施したSASEソリューションでは、より広い範囲を対象とする可視性とレポート機能を提供し、高い管理性を実現しています。さらに最も重要な点として、組織の分散環境全体でセキュリティを確保できます。スタック全体で高い可視性を実現でき、ネットワークとセキュリティの両方を管理、最適化できる単一のプロバイダーからソリューションの提供を受けるのが、SASEにおける最適なアプローチであると、ベライゾンは自身の経験から確信しています。

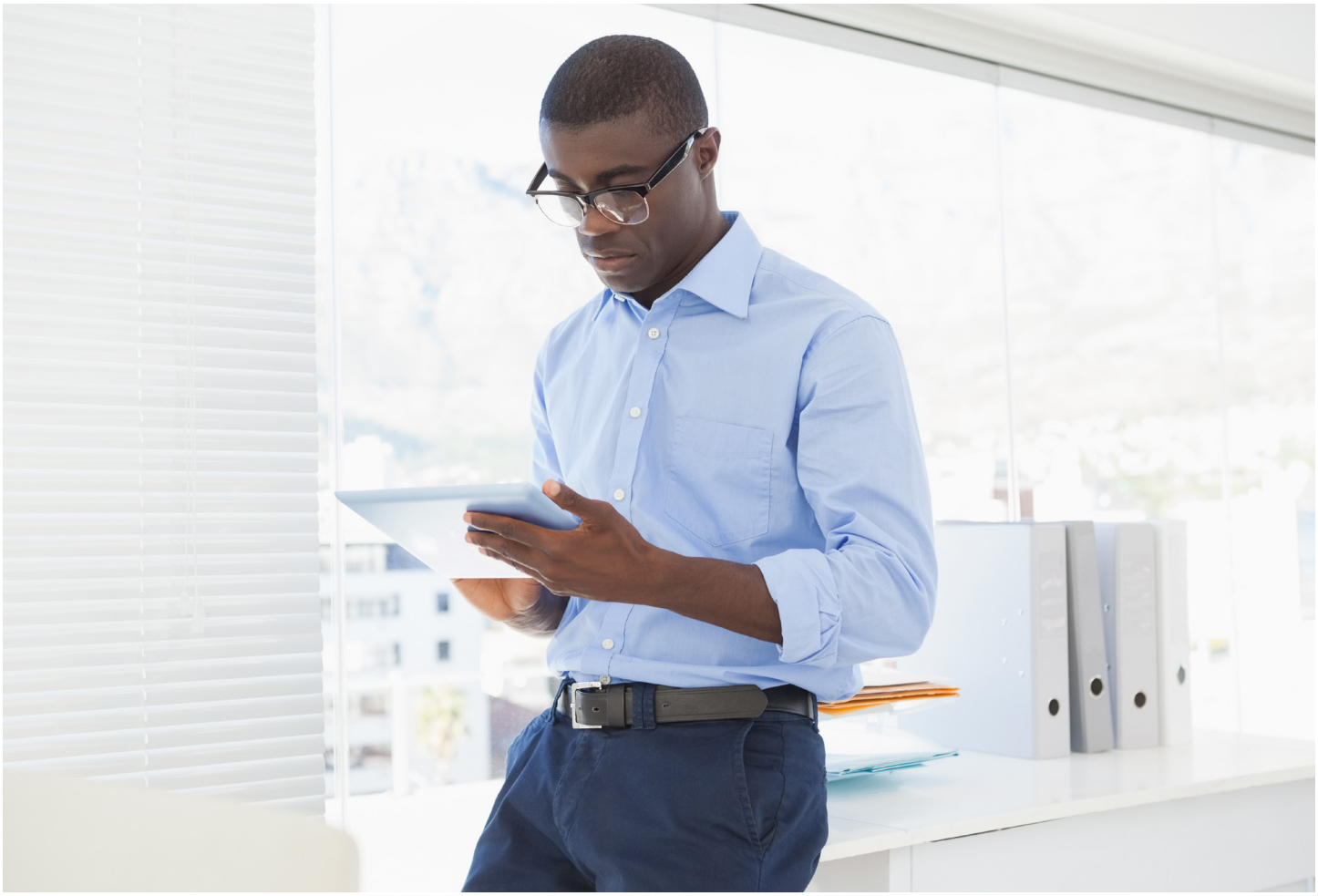
また、ベライゾンでは、さまざまな構成とポイントソリューションを活用して、柔軟な環境を実現しています。

すでにいくつかのサービスが組み込まれているブラウンフィールド環境や特定のベンダーに関して特殊な要件を持つ企業に対しては、業界をリードする複数のポイントソリューションを提供してギャップを解消し、完全なSASEソリューションを実現します。ベライゾンは、単一のプロバイダーによるソリューションを選択できる一方、異なるベンダーの異なるソリューションをシームレスに統合できるオーケストレーションと管理のノウハウも有しています。

適切なマインド

ベライゾンでは、SASEのサービスのサポートをより完全なものとするために、運用面での変更をすでに導入しつつあります。具体的には、SASEによって推進されるネットワークとセキュリティの広範な統合に対応できるよう、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）を統合する取り組みがあります。

また、SASEのようなテクノロジーを導入する場合、サービスレベルアグリーメント（SLA）を用意することが不可欠であるとベライゾンは認識しており、そのため、SASE環境のために作成した新たなSLAを導入しています。



将来に向けた道筋を整える

今ほどネットワークとセキュリティの統合が求められたことも、タイミングとして最適なときも、これまでにはありませんでした。当然のことながら、ネットワークとセキュリティに対する従来のアプローチはSASEによって駆逐されます。しかし、それによってITプロフェッショナルには、ネットワークアーキテクチャとセキュリティアーキテクチャの設計手法を抜本的に刷新する機会が生まれます。

SASEの短期的な効果としては、ネットワークとセキュリティを統合した環境全体でのセキュリティの強化とパフォーマンスおよび柔軟性の向上が期待できます。一方でこのような短期レベルの効果により、ビジネスのデジタルトランスフォーメーションやクラウドネイティブなコンピューティング、エッジコンピューティングなどに関する広範かつ継続的な取り組みも推進され、企業の将来像が再定義されます。

SASEを構成するネットワーク機能とセキュリティ機能の複雑さを理解しているパートナーからは、特定のニーズを満たす適切な機能を選択、実装する際に有用なサポートが受けられます。このようなパートナーと連携することが重要です。SASEの分野に新規参入した一部の企業の主張とは異なり、ネットワークとコネクティビティがSASEにおいて果たす役割は重要です。テクノロジースイート全体でSASEが機能するようにするためには、ネットワークとコネクティビティについて理解し、その両者をセキュリティソリューションと連携させなければなりません。

ベライゾンは、ネットワークとコネクティビティについて熟知しており、それらのノウハウを保有しています。ネットワーク、SD WAN、セキュリティ、デバイスに関する蓄積されたナレッジと、これらの分野におけるリーダーとしての実績、市場をリードする自社とパートナーのソリューションにより、ベライゾンでは、最適な組み合わせによる統合サービスとしてSASEを提供することが可能です。

Verizon Advanced SASEの詳細については、ベライゾンのビジネスアカウントマネージャーにお問い合わせいただくか、こちらからお問い合わせください。