citrix™

ホワイトペーパー

セキュアアクセスサービスエッジ（SASE）の概要

今日の要件に応じたネットワークおよびセキュリティアーキテクチャの再考

働き方の進化

働き方は進化しました。企業は、この進化を考慮して将来のインフラストラクチャへの投資、アーキテクチャ、新しいデジタルサービスの提供のタイムラインなどを計画する必要があります。この進化に遅れずについていくことは、業務効率、財務コスト、従業員エンゲージメント、顧客満足度など、ビジネスの成功を測る目に見える指標をプラスにするために不可欠です。

- **クラウド型のアプリケーションとサービスの使用の増加：**ガートナーは、2020年から2022年の間に世界中でSaaSアプリケーションへの支出が34%増加すると推定しています[1]。これらのSaaSアプリケーションは、仕事用と個人用の両方に採用されています。いずれの場合も、これらのアプリケーションに消費者グレードのエクスペリエンス、つまり、アクセスしているアプリケーションや場所を問わない高速アクセスを期待しています。
- **リモートワーカーの増加：**COVID-19により企業と従業員はリモートワークを実際に試さざるを得なくなりました。2020年6月のある調査によると、COVID-19の懸念がなくなった後でも、従業員の72%が少なくとも週に2日はリモートで仕事をしたいと考えています[2]。とはいえ、リモートワーカーは、コラボレーションの難しさが生産性低下の主な理由であるとも述べています。企業の53%は仕事用アプリケーションとデータに関して優れたモバイルエクスペリエンスを提供するための投資を計画中であるのは当然のことです[3]。
- **深刻化するセキュリティ脅威：**386万ドル – これはデータ漏洩が発生した場合の総コストの平均です[4]。ほとんどのデータ漏洩は、人為的エラーやシステムの不具合ではなく、悪意を持って意図的に画策されています。企業がセキュリティのシステムとアーキテクチャを進化させて、悪意のあるアクターから逃げ切ることが大事です。これは、実際の経済的損失を防ぐだけでなく、顧客と従業員の信頼維持にも役立ちます。

ITチームは、リモートワーカーを含むすべてのユーザーがクラウドアプリケーションへの高速で一貫性のあるセキュアなアクセスをサポートできる、ネットワークおよびセキュリティアーキテクチャの基盤を必要としています。残念ながら、現在使用されているハブアンドスポーク型のネットワークおよびセキュリティアーキテクチャは、オンプレミスのアプリケーションおよびブランチオフィスを拠点として、プライベートWANを介して接続された時代に設計されたものでした。ビジネスの成功に具体的な影響を与える可能性のある、より大きなテクノロジートレンドをサポートするには、これらのアーキテクチャ基盤を変える必要があります。

「企業の53%は仕事用アプリケーションとデータのモバイルエクスペリエンスを向上させるための投資を計画しています」

クラウド&モバイルファースト時代のアーキテクチャ

従来のアーキテクチャの課題

クラウド&モバイルファースト時代に適したアーキテクチャを実現するために解決する必要のある具体的な課題は以下のとおりです。

- **不十分な従業員のアプリケーションエクスペリエンス：**
  - **アーキテクチャ関連の課題：**ハブアンドスポーク型アーキテクチャでは、セキュリティ上の理由から、トラフィックをデータセンターにバックホールせざるを得ません。このようにトラフィックホップが追加されるとWAN要件が増加するだけでなく、回避可能な遅延が追加され、従業員エクスペリエンスが低下します。
  - **アプライアンス関連の課題：**リモートワーカーがクラウドアプリケーション、特にMicrosoft SharePointなどの暗号化ファイル共有アプリケーションやMicrosoft Teamsなどのビデオ会議アプリケーションを介して作業したり共同作業を行ったりするようになると、基盤インフラストラクチャ（データセンターベースのアプライアンスやWANリンク）の負荷が大幅に増加します。これらのハードウェアアプライアンスには計算能力の制約があり、暗号化されたクラウドアプリケーションからの負荷が増えると、パフォーマンスが低下し、従業員エクスペリエンスに影響を及ぼします。
- **一貫性のないリモートワーカーのセキュリティ：**従業員は、在宅勤務のときでも、ブランチ拠点と同程度のアプリケーションパフォーマンスを期待しています。これを実現するために、従業員はWebおよびSaaSアプリケーションにアクセスするときにVPNクライアントから切断することがよくあります。これを行うと、保護されなくなり、脅威に対して脆弱になります。同様に、BYOデバイスから企業のデータにアクセスする従業員は、リスクを高める可能性があります。実際、CISOとCIOの61%は、リモートワークをする人が増えたために、企業支給以外のデバイスやソフトウェアを使用することによるリスクが高まっていると語っています[5]。したがって、企業は、従業員のアプリケーションエクスペリエンスに影響を与えることなく、場所を問わず、すべてのユーザー、すべてのデバイスを一貫して保護する方法を必要としています。
- **運用の複雑さ：**従来のアーキテクチャには、断片化されたサービスチェーンソリューションで構成されているものがあります。その場合は、他に影響をあたえることなくアーキテクチャを変更することが困難です。また、トラフィックパターンの変化に合わせてアーキテクチャを拡張するには、物理アプライアンスをアップグレードして容量の上限を引き上げる必要が生じることもあります。これには時間がかかり、ITチームが新しいデジタルサービスの提供に集中できなくなってしまいます。

現代のエンタープライズアーキテクチャの主な機能

- **ダイレクトインターネットアクセス：**従業員は、アプリケーションへの直接パスを介してすべてのアプリケーションにアクセスできる必要があります。ただし、この接続は保護が必要です。
- **ユーザーの場所を問わないセキュリティ：**データセンターベースのセキュリティでは、ダイレクトインターネットアクセスは許可されません。したがって、場所に関係なく、従業員とアプリケーション間のパス上のセキュリティを可能にするセキュリティアーキテクチャが必要です。これは、クラウド配信セキュリティサービスでのみ実現可能です。予想どおり、76%の企業がセキュリティをクラウドに移行する計画です[6]。
- **アプリケーションパフォーマンスのためのWANサービス：**ダイレクトインターネットアクセスは、従業員とアプリケーション間のパスを短縮します。しかし、コモディティ接続またはビジネス向けインターネット接続の予測不可能性に起因するアプリケーションパフォーマンスの変動を軽減することはできません。したがって、ダイレクトインターネットアクセス接続でアプリケーションパフォーマンスを確保するには、ソフトウェア定義WAN（SD-WAN）やWANの最適化など、包括的な機能が必要です。
- **シングルパスアーキテクチャ：**典型的なセキュリティスタックのサービスチェーン検査エンジンによる遅延の追加を解消するには、シングルパスアーキテクチャを展開する必要があります。シングルパスアーキテクチャは、複数のポリシーエンジンによる処理のために、トラフィックを1回だけ開いて検査します。たとえば、シングルパスアーキテクチャでは、マルウェア対策エンジンとデータ損失防止エンジンによる分析のために、暗号化されたパケットを1回だけ開いて検査します。
- **統合管理：**ネットワークとセキュリティ全体にわたる管

理プレーンの統合により、プロビジョニング、ポリシーベースの管理、可視性、トラブルシューティングなど、ライフサイクル全体の運用が簡素化されなければなりません。たとえば、IT管理者チームは、ブランチオフィスの場所、セキュリティ拠点、トンネル、ネットワークの使用状況など、ネットワークとセキュリティ全体にわたる完全なエンタープライズアーキテクチャをすべて1つの統合ダッシュボードで包括的に把握する必要があります。これにより、死角がなくなり、アーキテクチャ全体の構成が簡素化され、人的エラーの可能性が最小限に抑えられます。

「76%の企業がセキュリティをクラウドに移行する予定です」

セキュアアクセスサービスエッジ

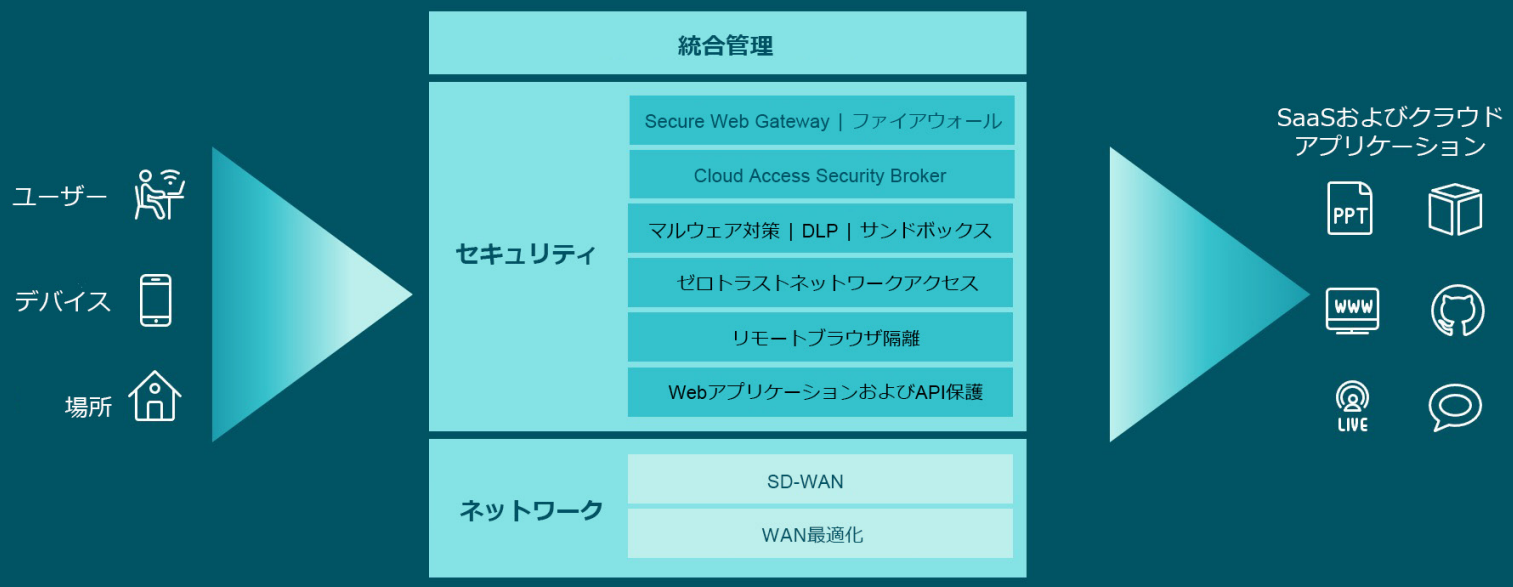
セキュアアクセスサービスエッジ（SASE）は、従来のハブアンドスポーク型アーキテクチャをセキュアなダイレクトインターネットアクセスに置き換えることを目的としています。クラウド配信セキュリティとゼロトラストアクセスおよび包括的なWAN機能の統合により、場所やアプリケーションがホストされている場所を問わず、セキュアで一貫性のある従業員エクスペリエンスが確保されます。

SASEサービスは、従業員のアイデンティティとリアルタイムコンテキストに基づいて適用されます。たとえば、財務部門の幹部は、マーケティング部門のサードパーティの請負業者とは異なるアクセス権を受け取ります。SASEアーキテクチャの主なサービスは次のとおりです。

- **Secure Web Gateway（SWG）**は、Webベースのサイバー脅威からユーザーを保護することを目的としたエンタープライズセキュリティソリューションです。次の機能を提供します。
  - **URLフィルタリング** – 要求されたURLを組織のポリシーによって定義されたフィルタリングデータベースと比較することにより、Webサイトへのアクセスを許可またはブロックします。
  - **マルウェア対策** – 暗号化および非暗号化Webコンテンツを検査し、すべての脅威を特定してブロックします。
  - **アプリケーション制御** – アクセスされているアプリケーションの可視性を提供し、セキュリティと規制準拠を確保するためのきめ細かい制御を可能にします。

SWGは通常、インラインクラウドサービスとして実装され、世界中に分散したPoP（Point of Presence）を介して

ネットワークと包括的なクラウド配信セキュリティを統合管理により集約するSASE

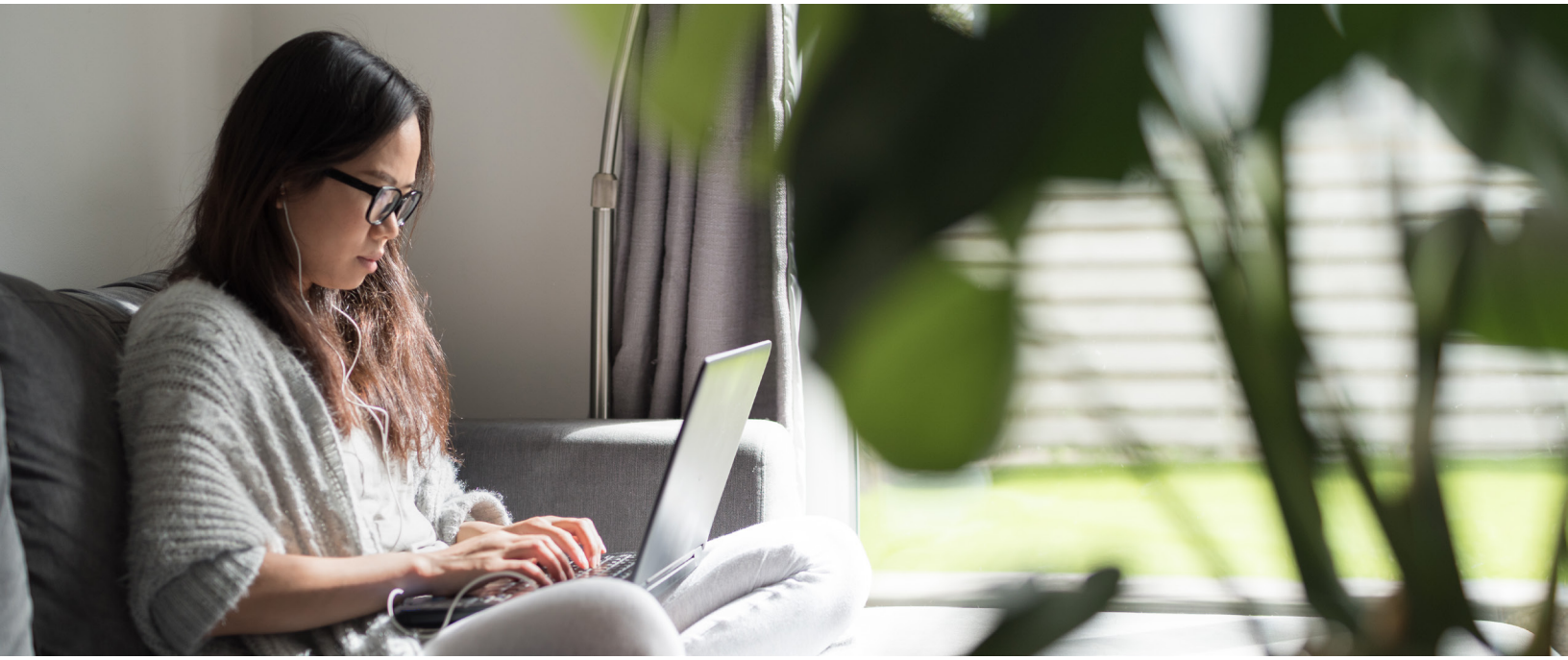


マルチテナントのセキュリティスタックとしてオーケストレーションされます。リモートおよびブランチオフィスのユーザーからのトラフィックは、SWGクラウドに転送され、そこで検査と保護が行われます。

- **Cloud Access Security Brokers（CASB）**は、承認済みおよび未承認のSaaSアプリケーションへのアクセスの監視、保護、および管理を支援します。CASBの機能は次の4つの柱を中心に構築されています。
  - **可視性** – ユーザーが使用している未承認のシャドーITアプリケーションを含むすべてのアプリケーションを一元表示します。
  - **データセキュリティ** – 機密データの不正アクセスと漏洩を軽減します。
  - **脅威対策** – インラインプロキシアーキテクチャ、ネイティブまたは統合型脅威フィード、動作分析を活用し、マルウェアや危殆化されたユーザーを特定して被害をくい止めます。
  - **規制準拠** – 可視性とレポートが業界の規制とデータレジデンシー（保管場所）ポリシーが順守されていることを示します。
- **ゼロトラストネットワークアクセス（ZTNA）**は、許可されたユーザーと承認済みアプリケーションの間に「ジャストインタイム」かつ「ジャストイナフ」のアクセスを提供することにより、「過度の信頼」を排除することを目的としています。特定のIPアドレスを持つユーザーが企業ネットワーク全体にアクセスできるようにする従来のVPNソリューションとは異なり、ZTNAは、正確で適応性のある、アイデンティティ認識とコンテキスト認識によるアクセスを可能にします。ZTNAソリューションの主な特長は次のとおりです。
  - **アイデンティティ認識** - ユーザーのアイデンティティに基づいてアクセスが許可されます。通常、ZTNAソリューションにはアイデンティティ情報用としてMicrosoft Azure Active Directoryなどのアイデンティティプロバイダーが統合されています。
  - **コンテキスト認識** - ZTNAソリューションは、ユーザーのアイデンティティ、アクセスの要求元の場所とデバイス、時刻、要求されている特定のアプリケーションの機密性、セキュリティ監視サービスからの情報に基づくリアルタイムのリスク計算など、リアルタイムのコンテキストパラメーターを考慮します。アクセスレベルは適応型です。つまり、これらのパラメータが変わると、アクセスの許可/制限/拒否も変わります。
  - アプリケーションレベルのアクセス - 許可されたユーザーに、基盤ネットワークではなく、特定のアプリケーションへのアクセスが許可されます。これにより、企業のネットワークにマルウェアが内部拡散する可能性を抑えます。
  - **インターネットからは見えないアプリケーション** - ユーザーとアプリケーション間のデータ転送はZTNAアーキテクチャ内の「ブローカー」によってサポートされ、アプリケーションのIPアドレスをインターネットに公開する必要がありません。その結果、アプリケーションは、DDoSまたは同様の攻撃を仕掛けようとする悪意のあるアクターから隠されたままになります。

ZTNAソリューションは、企業の攻撃対象領域を最小限に抑えることでユーザーとアプリケーションの両方を保護します。ユーザーはVPNにログインする必要がなく、VPNスタックを介してバックホールする必要がなくなるため、ユーザーエクスペリエンスが向上します。つまり、ZTNAソリューションは、データセンターに必要なVPNスタックをクラウド配信サービスに置き換えることで、企業のセキュリティアーキテクチャを簡素化し、運用のアジリティと効率を高めます。

- **Firewall-as-a-Service** – ファイアウォールは、信頼できるセキュアなトラフィックのみ通過を許可する双方向（クラウド入出力）制御を提供することにより、企業ネットワークとインターネット間のゲートキーパーまたはフィルターとして機能します。通常、ファイアウォールは、侵入検知/防止、マルウェア対策、ログ、レポートなどの機能を提供します。さらに、最新のファイアウォールのほとんどは、サンドボックス化、ジオロケーション、およびシグネチャレス（異常ベース）脅威検出も提供します。その一部を説明します。
  - **マルウェア対策** – 暗号化および非暗号化Webコンテンツを検査し、すべての脅威を特定してブロックします。
  - **侵入防止/検知システム（IPS/IDS）** – IPS/IDSはトラフィックを検査し、既知の脅威シグネチャと比較して悪意のあるファイルを識別します。IDSは、マルウェ



アが検出されたときにアラートを作成する監視/記録ツールです。IPSは、これをさらに一歩進め、潜在的に悪意のあるトラフィックを自動的にブロックします。

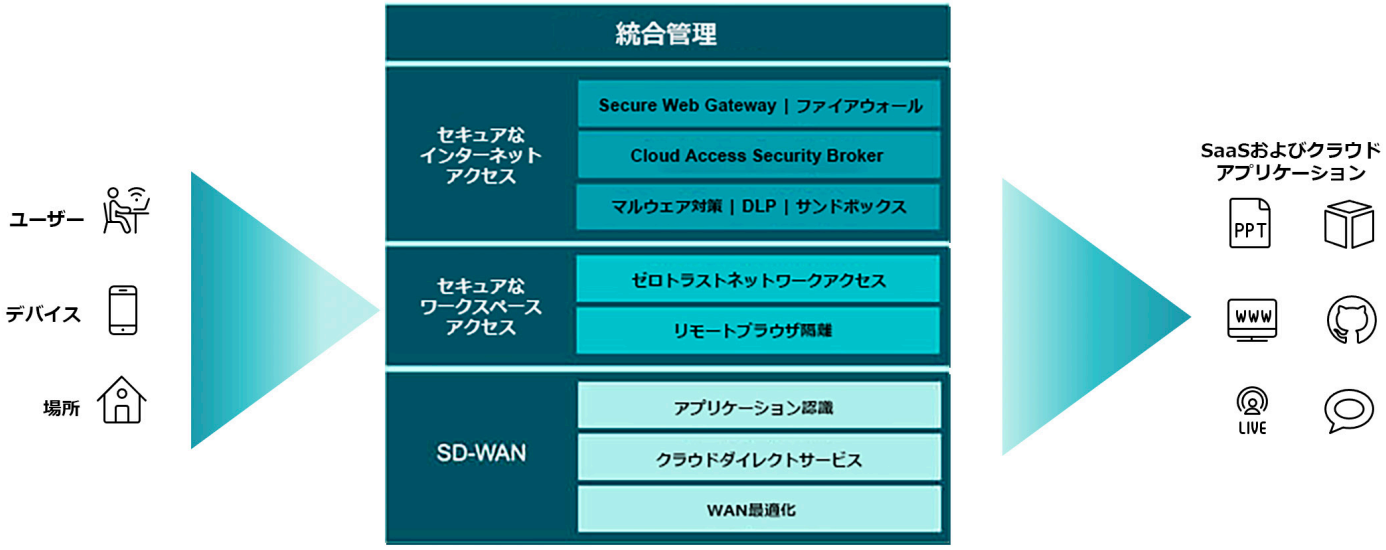
- **シグネチャレス/異常ベースの脅威検出** - 異常ベースの検出では、ファイルの動作または潜在的な動作（ファイル内のコードの検査による）を典型的なベースライン動作と比較します。たとえば、新しくダウンロードされたファイルがセキュリティ制御を無効化しようとしている場合、そのファイルは隔離される可能性があります。
- **ネットワークサンドボックス** – 疑わしいファイルがサンドボックスに送信され、隔離された環境で実行されます。悪意のあるファイルであることが判明した場合は、ファイルに関する情報がファイアウォールに送信され、ファイルがブロックされます。
- **ジオロケーション** – 特定の範囲のIPアドレスを特定の地理に割り当て、その割り当てに基づいてアクセスを許可/制限/ブロックします。

ファイアウォールは、企業のブランチ拠点、データセンター、およびクラウドインスタンスを脅威から保護するために使用されます。より堅牢で包括的な脅威管理「プラットフォーム」を作り上げるため、他のセキュリティおよびSecOps（分析）ソリューションと統合される場合があります。

- **SD-WAN：**ソフトウェア定義WANソリューションは、分散している企業の拠点からクラウドおよびオンプレミスのアプリケーションへの低遅延で復元力のある接続を提供すると同時に、従来のルーターベースのネットワークソリューションを使用して最新のネットワークを管理するときの複雑さを解消します。SD-WAN機能には、以下のように包括的なWANエッジ機能が含まれます。

  - **パス選択** – 管理者が定義したポリシーとリアルタイムWANヘルス（パケット損失、ジッター、遅延など）に基づく、トラフィックの識別と動的ステアリング。パス選択機能は、ネットワークパフォーマンスの変化に関係なく、ユーザーが一貫したアプリケーションエクスペリエンスを確実に受け取ることを支援します。
  - **ルーティング** – ブランチ拠点のルーターに代わる機能（BGP、OSPF、マルチトポロジをサポート）。
  - **ネイティブセキュリティ** – IPS/IDS、シグネチャおよびヒューリスティックベースのマルウェア対策、Webフィルタリングなど、ブランチグレードのセキュリティ機能。さらに、SD-WANソリューションにより、ブランチ拠点とクラウド（IaaS/PaaS）インスタンス間のVPNトンネルのセットアップが簡素化されること

シトリックスのSASE統合アプローチ



シトリックスのSASEへのアプローチは、いつでも、どこでも、どのデバイスでも、アプリケーションへのセキュアで信頼性の高いアクセスを実現する機能を統合します。

もあります。

- **ゼロタッチプロビジョニング** – この機能により、ブランチのSD-WANアプライアンスのプロビジョニングと初期構成を中央のITチームがリモートで実行できます。これにより、SD-WANアプライアンスをブランチ拠点に出荷して1つ以上のWAN回線に接続するだけで、現場で複雑な構成を行う必要がなくなります。SD-WANアプライアンスは、SD-WANコントロールプレーンから構成をダウンロードし、他のSD-WAN対応のブランチ拠点およびクラウドとのトンネルのセットアップを自動的に開始します。

SD-WANと統合された上記のセキュリティ機能により、企業はネットワークおよびセキュリティアーキテクチャを変革し、クラウド、モビリティ、および拡大する多様なユーザーの需要を満たすことができます。

アイデンティティ認識型ゼロトラストアクセス：

シトリックスは、包括的なクラウド配信セキュリティスタックをSD-WANおよびゼロトラストアクセスと統合する完全統合型SASEソリューションを提供し、セキュアに、あらゆるアプリケーション、あらゆる場所、あらゆるデバイスで、最高のエクスペリエンスをユーザーに提供します。

- **包括的クラウド配信セキュリティ：**Citrix Secure Internet Access（SIA）は、包括的なクラウド配信セキュリティサービスを提供します。これには、Secure Web Gateway、Next Generation Firewall、Cloud Access Security Broker、10以上の脅威エンジンによるマルウェアインテリジェンス、データ損失防止、サンドボックス化、AIによる分析などが含まれます。100か所以上のPoP（Point of Presence）にグローバルに分散して各PoPが一貫してすべてのサービスを提供するSIAは、場所を問わず、完全なセキュリティスタックでユーザーを保護します。

Citrix Secure Internet Accessは、包括的なクラウド配信セキュリティサービスを提供します。

- **アイデンティティ認識型ゼロトラストアクセス：**Citrix Secure Workspace Accessは、あらゆるデバイスで従業員エクスペリエンスを合理化するように設計されたデジタルワークスペースで、企業が承認したすべてのアプリケーションへのアイデンティティ認識型ゼロトラストアクセスを提供します。組み込みのリモートブラウザ分離は、ブラウザベースの攻撃からエンドポイントと企業ネットワークを保護します。Webサイトのデータはユーザーのデバイスに直接転送されないため、エクスペリエンスはセキュアです。
- **SD-WANによる高速なアプリケーションエクスペリエンス：**Citrix SD-WANは、SaaS、クラウド、仮想アプリケーションのパフォーマンスを向上させるセキュアで柔軟性の高い自動接続を提供する、次世代のWANエッジソリューションです。WANリンク間のフェイルオーバーが1秒未満でトラフィックをパケットレベルで優先順位付けする機能やデュアルエンドQoSなどにより、ネットワークの可用性に関係なく、一貫して高速のアプリケーションパフォーマンスが保証されます。
- **詳細なフォレンジックと簡単な検索：**モバイルユーザーを含むすべてのユーザーおよびユーザー行動（ドメイン名だけでなくHTTPSトラフィックの完全なURL情報を含みます）の詳細なログにより、比類のない詳細な可視性が提供されます。AIを活用したレポートエンジンは、レポートとアラートのための最重要情報を抽出します。組み込みのレポートに加えて、ログをリアルタイムでSIEMソリューションにエクスポートすることもできます。
- **統合管理：**シトリックスは、SD-WANとSIAの全体で緊密な統合、自動化、および一元管理を提供し、初期設定から継続的な管理およびトラブルシューティングまで、ライフサイクル全体の運用を簡素化します。
    - Citrix SD-WANの拠点とCitrix SIA間の「デュアルレジリエント」（耐障害性に優れた冗長構成）の自動接続
    - SD-WAN対応の拠点、SIA PoP、および接続トンネルにわたるアーキテクチャ全体の単一表示
    - SIA、クラウドプロバイダー、およびその他のWANリンク全体のトラフィックステアリングと帯域幅の割り当ての、ビジネスニーズに応じたきめ細かな制御
    - ネットワークおよびセキュリティアーキテクチャ全体でレポートを統合することにより死角を解消

SASEアーキテクチャ実装のメリット

SASEアーキテクチャは、モバイル/リモートワーカーによるクラウドアプリケーションへの高速で信頼性の高いセキュアなアクセスを可能にすると同時に、ITのアジリティを向上させることを目的として設計されました。ネットワークとセキュリティ全体の統合管理、シングルパスアーキテクチャ設計、強力なSD-WAN機能など、提供される機能の微妙な相違に注意を払うことを前提とすると、SASEの導入により次のメリットを実現できます。

- **ユーザーエクスペリエンス、コラボレーション、エンゲージメントの向上** – ダイレクトインターネットアクセスにより、バックホール接続による遅延が解消されます。ただし、インターネットのパフォーマンスが変動しても一貫したパフォーマンスを確保するには、SASEソリューションのSD-WANおよびWAN最適化機能が必要です。シングルパスアーキテクチャにより、検査/ポリシーエンジン自体によって不要な遅延が追加されることはありません。
- **従業員の場所に関係なくセキュリティを向上** – 承認済みのアプリケーションには、アイデンティティ認識型ゼロトラストアクセスが可能です。これにより、攻撃対象領域が減少し、企業ネットワーク内部でのマルウェアのラテラルムーブメント（拡散）を防ぎます。Webおよび未承認のアプリケーションの場合は、包括的なクラウド配信セキュリティにより、ユーザーの場所に関係なく、一貫したセキュリティ体制を保証します。
- **運用の簡素化とITのアジリティの向上** – SASEアーキテクチャは、ネットワークとセキュリティ全体でのベンダーの統合に有効です。単一ベンダーのソリューションは、緊密な統合と統合管理により、導入、構成、レポート、およびサポートサービスを簡素化します。SASEアーキテクチャではセキュリティをクラウドに移行する必要があるため、全体的なハードウェアフットプリントが削減され、アーキテクチャの弾力性と規模が向上します。

始めましょう

他の先進的技術と同様に、一部の企業が他社に先駆けてSASEアーキテクチャを採用するものと予想されます。従来のハブアンドスポーク型アーキテクチャの交換、レガ

シーVPN技術の交換、アプリケーションのクラウドへの移行、リモートワーカーの一貫したセキュリティ、従業員エンゲージメント向上の必要性は、話し合いのきっかけとなり得るもののほんの一部です。

ネットワークおよびセキュリティアーキテクチャを再検討して設計を見直すことができれば、早期導入者にとって大きなアドバンテージとなり、業務効率、財務コスト、従業員エンゲージメント、顧客満足度など、ビジネスの成功を測る指標にプラスの影響をもたらすことになります。この変革を実現するため、企業はテクノロジーパートナーを賢明に選択する必要があります。

シトリックスは、ネットワークとセキュリティ全体にわたり、緊密な統合、自動化、一元管理により、すべてのSASEサービスを統合します。40万社以上の組織から信頼を得、より良い働き方を生み出しているシトリックスは、ネットワークとセキュリティの変革を加速するお手伝いをいたします。

詳細は、**https://www.citrix.com/ja-jp/products/citrix-secure-internet-access/**をご覧ください。

出典：

1 Based on Citrix's own calculations. Gartner Press Release, Gartner Forecasts Worldwide Public Cloud Revenue to Grow 6.3% in 2020, 23 July 2020. https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

2 PwC's US Remote Work Survey, June 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

3 PwC's US Remote Work Survey, June 2020, https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html

4 Cost of a Data Breach Report 2020, IBM, https://www.ibm.com/security/data-breach

5 PwC's Workforce Pulse Survey, https://www.pwc.com/us/en/library/covid-19/workforce-pulse-survey.html

6 PwC's Global Digital Trust Insights 2021, https://www.pwc.com/us/en/services/consulting/cybersecurity/library/global-digital-trust-insights/cyber-defense-technology.html

お問い合わせ
TEL：03-4577-5900

〒100-0013
東京都千代田区霞ヶ関3-2-1 霞ヶ関コモンゲート西館23F

©2020 Citrix Systems, Inc. All rights reserved. Citrix、Citrixロゴおよびその他のマークは、Citrix Systems, Inc. および／またはその一つもしくは複数の子会社の商標であり、米国の特許商標庁および他の国において登録されている場合があります。その他の社名、商品名はそれぞれの所有者の登録商標または商標です。