citrix

ソリューションブリーフ

Citrix Secure Private Accessによるゼロトラストネットワークアクセス

デジタルトランスフォーメーション、クラウドの採用、そして拡大を続けるハイブリッドワーカーにより、セキュリティと接続状況のダイナミクスは根本的に変化しています。その結果、企業はアプリケーションに依存するようになる一方で、かつてないほど多くの従業員がインターネットやさまざまなタイプのデバイス（マネージド型および非マネージド型のもの）を使用して情報をやり取りするようになっています。

このような移行に伴い、サイバーセキュリティ専門家は、事業継続性と優れた従業員エクスペリエンスを確保しながら、セキュリティの維持と拡張に取り組んでいます。同時に、より多くのアプリケーションがクラウドに移行するほど、より多くのワークロードがパブリッククラウドやSaaSを通じて分散されるようになります。その結果、アプリケーションの状況は変化しており、より複雑になりつつあります。

急速に拡大するアタックサーフェス

従来のエンタープライズアーキテクチャとサイロ化されたアプローチは、主にデータセンターセキュリティ、ポイント製品、そして企業ネットワークまたはブランチネットワーク内にある冗長なファイアウォールに依存していました。残念なことに、これらのアプローチは、今日の動的なアプリケーション接続、コンプライアンス、およびセキュリティ上の要件に関しては役に立ちません。パブリッククラウド、マルチクラウド、SaaSへの移行に伴い、機密性の高いデータやビジネスクリティカルなアプリケーションが、データセンターやプライベートクラウドではなく、パブリック/マルチクラウド上により多く存在するようなっています。残念なことに、この結果、複雑な環境では保護と管理がより困難になっています。それは、特に今日のITチームが直面している複雑な問題に対処するために必要となる、専門知識のレベルにおいて顕著です。

ハイブリッドワークモデルの成長とさまざまな種類のデバイスの使用の拡大により、組織におけるアタックサーフェスも拡大しています。企業の管理下にあるデバイスは、リモートアクセスを提供する最も安全な方法です。なぜなら、IT部門はそれらのデバイスを最も厳重に管理できるからです。一方、従業員や請負業者はBYOデバイスを使うことを必要としているかまたは希望しており、これはセキュリティイベントのリスクを高めることになります。

このような複雑さとアタックサーフェスの拡大はすべて、攻撃者にとってチャンスをもたらします。そのため、企業や組織は、セキュリティに対するアプローチを再考すると同時に、従業員がアプリケーションに、あらゆる場所から、いつでも、あらゆるデバイスを通じて、可能な限りシームレスなセキュアアクセスを行えるようにする必要があります。

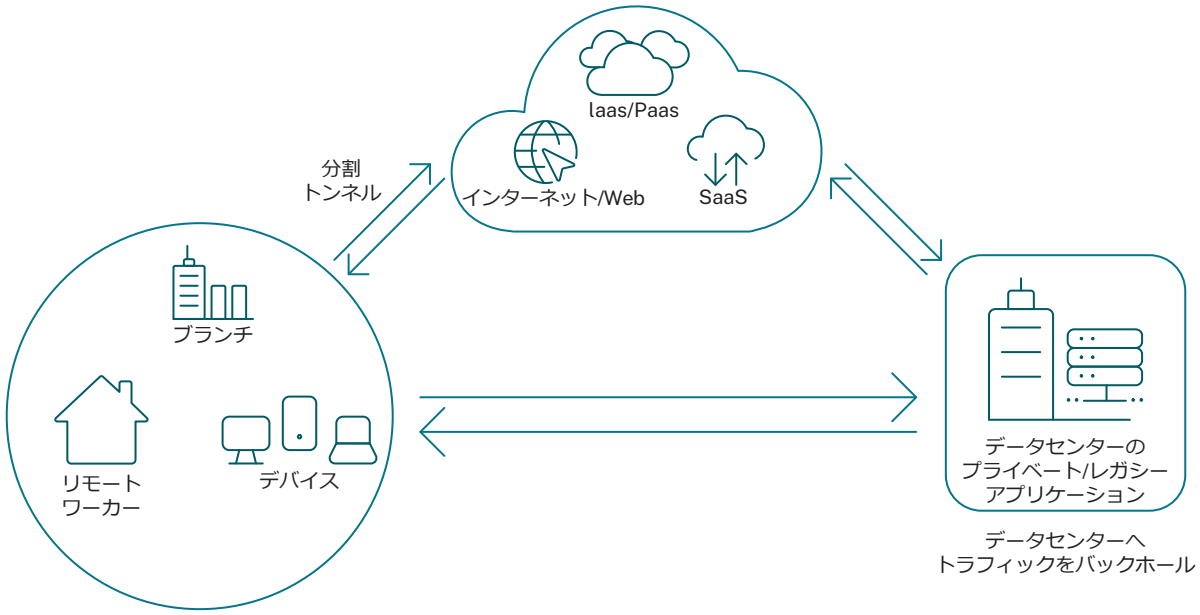


図1：従来のネットワークおよびセキュリティに対するアプローチ

新しいハイブリッドワークモデルと従来のアプローチにおける課題

企業や組織が新しいハイブリッドワークモデルをモダナイズし、それに適応する中で、ユーザー、データ、およびアプリケーションを保護する以前に、それらに関する包括的な可視性と制御を必要としています。クラウドへの移行方法は、組織ごとに異なります。直面する課題は、それぞれが抱えているビジネスアプリケーション、セキュリティとネットワークテクノロジー、接続要件、および埋めるべきギャップにより異なります。

ポイント製品や、セキュリティおよびネットワーキングに対する従来のアプローチに関する一般的な課題としては、次のものが挙げられます。

- **不適切で一貫性のないセキュリティポリシー：**複数のログインや重複するセキュリティポリシーは、安全でない慣行やセキュリティリスクの増加につながる可能性があります。
- **ITコストと複雑さの増大：**複数のベンダーを管理することは、コストが高く、非効率的で、かつ複雑な作業です。
- **巻き添え被害としてのユーザーエクスペリエンスの低下：**エンドユーザーエクスペリエンスの低下、ユーザー受容度の低下、およびシャドーITがもたらされます。

Citrix Secure Private Accessとは？

Secure Private Accessは、シトリックスが提供するより広範なSecure Accessソリューションの一部であり、今日の分散型エンタープライズ環境における課題の概要に対処し、複雑さを軽減するのに役立ちます。

Citrix Secure Private Access

Citrix Secure Private Accessとは、ユーザーID、場所、エンドユーザーデバイスにかかわらず、ゼロトラストアプローチにより常時オンのセキュリティを提供するクラウドベースのZTNAソリューションです。また、同ソリューションは、IT部門が認可したすべてのアプリケーションへのセキュアで高速な接続を保証します。これは、従来のVPNアプローチでよく使われるトラフィックのバックホールを回避することをはじめ、ユーザーやインフラストラクチャを非マネージドデバイス/BYOデバイス経由の不正クラウドサービスとして、すべてのジオロケーションで利用可能であり、ユーザーベースや使用率の増加に応じて自動的なスケーリングが行えるほか、アジリティと常時オンのセキュリティを提供することで、最高のユーザーエクスペリエンスとセキュリティを実現します。これはフルマネージド型のサービスであるため、IT部門は同サービスを利用することで、自社データセンター全体におけるアプライアンス管理に時間を費やすのではなく、より戦略的なイニシアチブに集中できるようになります。

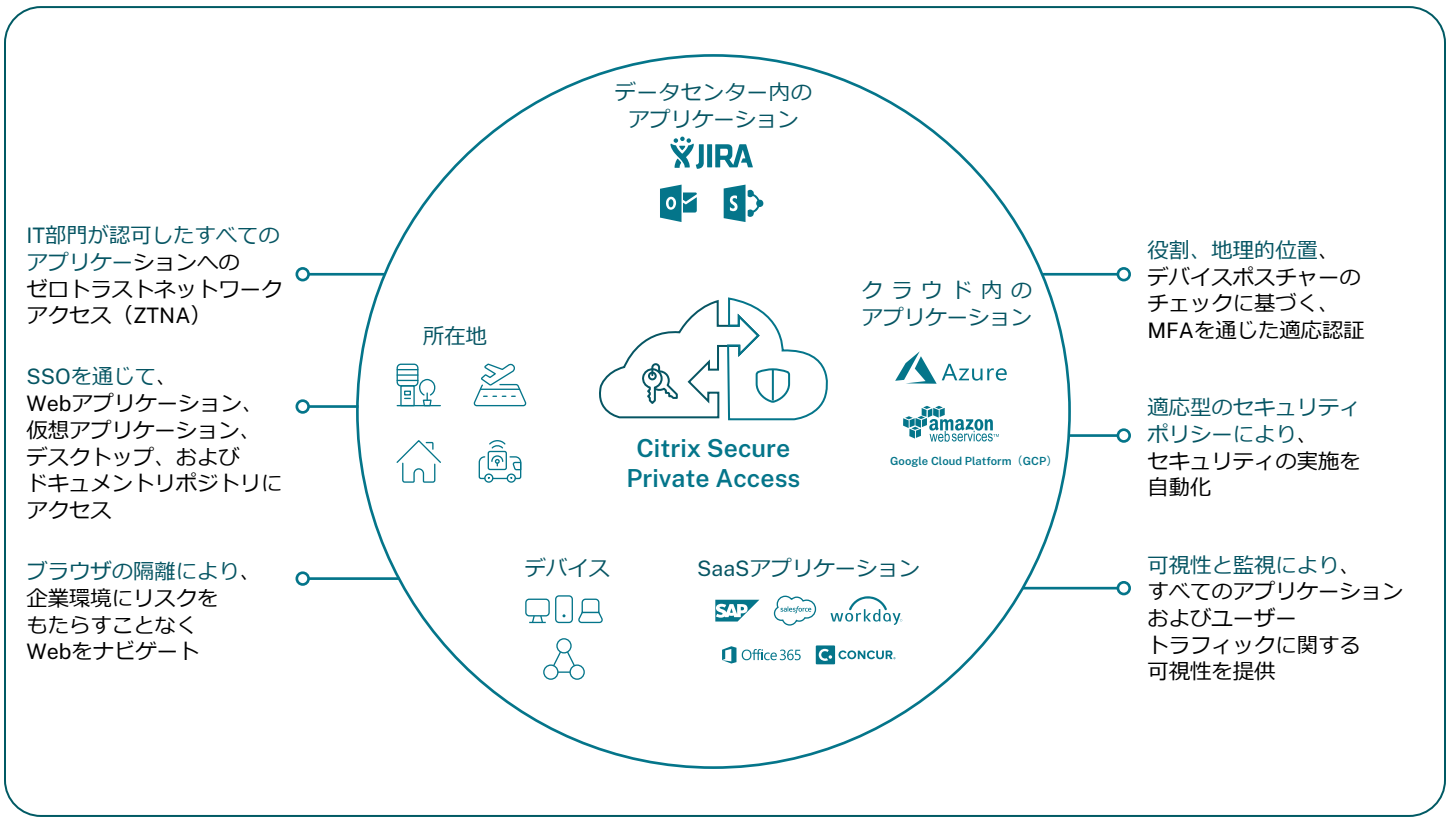
Citrix Secure Private Accessを使用すると、IT部門は、従業員、請負業者、パートナーによる特定アプリケーションへのアクセスを実現できるほか、リモートワーカーによるBYOデバイスを通じたアプリケーションへのセキュアアクセスを実現できるようになります。

適応型のアクセスポリシーに基づいて、BYOデバイス経由のユーザーのセッションを、リモートのブラウザ隔離セッションへと自動的にリダイレクトできます。これにより、悪意あるコンテンツが、BYOデバイス経由でアプリケーションやネットワークに送信されるのを防止できます。また、これにより、企業情報をパーソナルデバイスにダウンロードすることも禁じられます。さらに、Secure Private Accessは、アプリケーション保護ポリシーを提供することで、ユーザーのセッションやWorkspace経由でアクセスされる機密情報が、すべてのキーロガーやスクリーンキャプチャ型のマルウェアから保護されるようにします。

ゼロトラストネットワークアクセス（ZTNA）

ゼロトラストは、「信頼」という従来のセキュリティ原則を拒否します。その代わりに、ゼロトラストは「決して信頼せず、常に検証する」という原則に焦点を当てます。「城と堀（Castle and Moat）」型のアプローチを採用している従来のソリューションは、ログイン時にだけユーザー認証と権利認証を実施することのみに焦点を当てており、ユーザーはいったん認証された時点で基本的に信頼されることになります。このようなアプローチは、多くの不正アクセスを生み出す原因となっており、その結果、デバイスのハッキングや、ユーザーのクレデンシャルの窃取が起こっていました。

ゼロトラストを利用すると、IT部門は、セッション全体を通じてユーザーの行動を継続的に監視して評価し、検出された異常に基づいてセキュリティアクションを自動化できるようになります。



全体的な統合ゼロトラストセキュリティ戦略	IT部門は、ユーザー、アプリケーション、ファイル、エンドポイント全体を通じて、包括的なゼロトラストセキュリティ戦略を実装できるようになります。
IT部門が認可したすべてのアプリケーションへのゼロトラストネットワークアクセス（ZTNA）	VPNは、拡張が難しく、プライバシーに関する懸念があるほか、今日の最新のセキュリティ標準にも適合していません。Citrix Secure Private Accessは、IT部門が認可したあらゆるアプリケーション（Web、SaaS、クライアント/サーバーアプリケーション（TCP）、仮想アプリケーションなど）に対して、ゼロトラストネットワークアクセス（ZTNA）を提供します。これらのアプリケーションは、オンプレミスまたはパブリッククラウドのどちらに導入されている場合であれ、Citrix Workspaceの内部または外部からアクセスされる場合であれ、期待通りのゼロトラスト成果をもたらします。
適応認証、SSO、セキュリティの強化	Citrix Secure Private Accessは、ユーザーセッションの確立前および確立後に、エンドユーザーデバイスをスキャンする機能を提供します。ユーザーロケーションの結果とデバイスポスチャーの評価に基づいて、管理者は、アプリケーションへのユーザーアクセスを認証および承認する方法を定義できます。これらのポリシーにより、管理者は、ユーザーがこのアプリケーション内で実行できるアクションを制御できます。これらのポリシーは、Citrix DaaSのお客様を含む、すべてのアプリケーションに対して実装できます。
統合されたリモートブラウザ隔離テクノロジーを利用することで、BYOデバイスや非マネージドデバイスを通じて、IT部門が認可したアプリケーションへのセキュアアクセスを実現	Citrix Secure Private Accessを使用すると、ユーザーは、エンドユーザーデバイスにエンドポイントエージェントをインストールする必要なしに、BYOデバイスを通じて、IT部門が認可したアプリケーションにアクセスできるようになります。ただし、これは、ユーザーセッションを、ローカルブラウザから、ホステッド型のSecure Browser Serviceへとリダイレクトします。これにより、ユーザーがサンドボックス環境でアプリケーションにアクセスできることを保証し、ユーザーの生産性を維持できます。同時に、これは、インターネットの悪意のあるコンテンツからエンドポイントとネットワークをブラウザ隔離機能で保護し、企業リソースからのエアギャップを作成します。
キーロガーおよびスクリーンキャプチャ型マルウェアからの保護	組織が管理するデバイスは厳密に監視できますが、IT部門は、非マネージドデバイスの健全性に関するインサイトを取得できません。この結果、マルウェア（特にキーロガーやスクリーンショット型マルウェアなど）に感染したデバイスを通じて、攻撃者が機密性の高い企業データを流出させるリスクがもたらされます。 Citrix Secure Private Accessは、制御を強化することで、キーロガーによるユーザークレデンシャルの窃取を防ぐほか、Workspaceアプリ経由でアクセスするアプリケーションの画面ショットがスクリーンキャプチャ型マルウェアにより撮影されるのを防ぎます。

すべてのユーザーとアプリケーションに関するエンドツーエンドの可視性を提供	Citrix Secure Private Accessは、IT部門が認可したすべてのアプリケーションへのすべてのユーザートラフィックに関する、完全なエンドツーエンドの監視と可視性を提供します。すべてのユーザートラフィックを監視するために複数のダッシュボードを備えた複数のアクセスソリューションを使用しているお客様は、Citrix Secure Private Accessを導入することで、たった1つのダッシュボードを通じて、監視を効率化し、サイロ化された複数の環境を1つに統合できるようになります。
潜在的なリスクを検知し、それに対する防御を実施する	Citrix Analytics for Securityは、アプリケーション、デバイス、ネットワークに関するインサイトを提供することで、システム内で検知されたユーザーの行動や異常に基づいてセキュリティ措置の自動化を支援します。これにより、IT部門の手作業を削減し、タイムリーな実施を可能にし、不正な侵害のリスクを軽減できます。

要約

アプリケーションやデータへのアクセスを保護するには、脅威や脆弱性から身を守ること以上に重要なことがあります。従業員が生産性とエンゲージメントを維持するためには、企業や組織は、複数のログインやパスワードのリセットを必要としない、手間のかからないアクセスを確保する必要があります。

これを実現するために、Citrix Secure Accessソリューションは、どこからでも仕事が行える比類のないアプリケーションエクスペリエンスと、クラウドベースの高度な適応型のセキュリティの両方を提供するように設計されています。従来のオンプレミスVPNとは異なり、エンドツーエンドのゼロトラストセキュリティにより、ユーザーは企業ネットワーク全体にアクセスする必要なしに、IT部門が認可したすべてのアプリケーションのみにリモートアクセスが行えるようになります。このようなゼロトラストアプローチにより、企業や組織は、アイデンティティ、ジオロケーション、デバイスの配置などのコンテキストを組み合わせることで、アプリケーションの使用場所と使用方法に基づいてアクセスを許可できるようになります。

一方、より多くの従業員が在宅勤務を行う場合、完全なクラウドベースのセキュリティスタックが特に重要となります。完全なカバレッジと耐障害性を持つよう設計されたグローバルなクラウドサービスソリューションを使用すると、ポリシーと保護を現在の脅威の状況に合わせて自動的に更新できます。

Citrix Secure Private Accessの詳細については、https://www.citrix.com/ja-jp/products/citrix-secure-private-access/ をご覧ください。

お問い合わせ
米国 | 800-424-8749
03-4577-5900

所在地
〒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