ハイブリッドワークの確保

ネットワークの内外を問わず、あらゆるユーザーのリスクを低減して可視性を向上します

あらゆるユーザー、あらゆるデバイス、あらゆる場所からの接続を保護します

弊社の「どこでも仕事」の将来について：世界的な感染症の蔓延から数年が経って不況が目前に迫った今、ハイブリッドワークは今後も続くと見られています。ITとセキュリティのチームは、リモートであろうとオフィスであろうと、すべてのユーザーとデバイスに一貫した保護と体験を提供しなければなりませんが、従来のロケーション中心のツール（VPNやIPベースのコントロールなど）では、この課題を解決することはできません。

最新のセキュリティで、最新の労働に対応：これを受けて多くの組織がITとセキュリティのアーキテクチャを再考し、分散した労働ニーズに合わせて拡張してZero Trustのベストプラクティスに則ったクラウド配信型のセキュリティを導入しています。

Cloudflareは、あらゆる接続を簡単に保護できるため、ユーザーはデバイスや場所を問わず、ユーザーがアプリケーションやインターネットにアクセスする際に安全性と生産性を維持することができます。

Gartner®社の見解：

2026年までに、75%の労働者が自宅と従来のオフィス拠点を行き来することに時間を消費する生活を続けることになるでしょうが、これはパンデミックがピークとなった2021年の77%からわずかに減少することになります。[1]

境界セキュリティアプライアンスの集合体をベースとしたネットワークセキュリティ設計は、現代のデジタルビジネスとそのハイブリッドデジタルワーカーのダイナミックなニーズである「いつでも、どこでも」に対応するためには不向きです。[2]

ページ別目次

セキュリティを近代化する機会

VPNを使用しない安全なアプリケーションアクセス

ユーザーが分散しているため、VPNなどのオンプレミス・アプライアンスでトラフィックをバックホールするとパフォーマンスが低下し、企業ネットワーク全体に脅威が水平拡散するリスクが生じます。
その代わりに、あらゆるリクエストを可視化し、ユーザーにより近い場所でIDベースのコントロールを行うことで生産性を維持できます。バックホールは不要です。

SaaSセキュリティの効率化

従来の企業ネットワークでは管理しきれなかったSaaSアプリケーションの利用が、これまで以上に増えています。
そのため、企業は、ポリシーへのアクセス設定、データ保護コントロールの適用、シャドーITの軽減、アプリケーションの設定ミスのスキャンなど、SaaSアプリケーションに対するより包括的な可視化とコントロールを必要としています。

インターネット上の脅威からユーザーとデータを保護します

ランサムウェアやフィッシングなど、インターネット上の脅威は常に存在し、その手口はますます巧妙になっています。
アウトバウンドトラフィックにクラウドベースのインスペクションやアイソレーションを採用することで、マルウェアからユーザーを安全に守ることができます。さらに、管理者は、機密データがローカルの非管理対象デバイスに届かないように制御を適用することができます。

成熟した企業におけるハイブリッドワーク

成熟した企業では、ハイブリッドワークのためのセキュリティを安心して近代化することができます

課題：複雑で時代遅れな環境

組織は、オフィスでの働き方のモデルを試行錯誤しています。しかし、このようなハイブリッドシナリオにおいて、一貫した保護とユーザーエクスペリエンスを維持することは困難です。

このような企業は、既存のオンプレミスやレガシーへの投資が重く（多くの場合、複雑な）、より確立されたものである傾向があります。不況の逆風が吹く中、新しいセキュリティプロジェクトを立ち上げるのは、リスクが高すぎて難しいと感じるかもしれません。

機会：近代化への簡便な道

組織は、青天井の予算、高価な「概念実証」、複雑な実装段階、またはデイジーチェーン（数珠つなぎ）サービスを必要とせず、自分たちのペースでデジタル変革を追求する権利があります。

これらの成熟した企業がハイブリッドワークのニーズに対応できるよう、Cloudflareは、Zscalerといった他のZero Trustサービスプロバイダーよりも簡単かつ迅速にデプロイできるよう設計されています。

ユースケースの例ユースケース

通信

状況：100年以上の歴史を持つ年商200億ドル以上のヨーロッパの通信事業者はインターネットのフィルタリングをデプロイし、最近複数のクラウド環境に移行したレガシーアプリへのアクセスを認証するベンダーを1社に絞って探していました。

ソリューション：当社はサービスを統合し、統一プラットフォームを使用して10万人を超える従業員のアプリケーションとインターネットアクセスの両方を保護するためにCloudflareを選択しました。

連邦政府

状況：米国国土安全保障省（DHS）は、連邦政府のオフィス、場所、インフラ全体におけるインターネット脅威対策への投資を主導しています。

ソリューション：DHSは、連邦政府機関全体で使用される、悪意のある危険な宛先へのDNSクエリをフィルタリングする共同ソリューションの開発に、CloudflareとAccenture Federal Servicesを選定しました。

メディアと広告

状況：メディア複合企業（収益100億ドル以上、全世界で10万人以上の従業員）が、身代金要求書を含む社内インフラストラクチャへのサイバー攻撃に直面しています。

ソリューション：Cloudflareは、IDベースのZero Trustルールにより、何百ものWebおよび非Webアプリケーションのセキュリティを確保しています。当社は3ヶ月以内に5万人の従業員を対象に保護を展開し、9ヶ月以内に全従業員に拡大する計画です。

エネルギー

状況：フォーチュン500の天然ガスプロバイダーは、分散したデータセンターと1,500人以上の従業員の両方を対象に、この分野を標的としたサイバー脅威からの保護を強化することを求めていました。

ソリューション：Zscalerを置き換えるためにCloudflareを選択したのは、アプリケーションとインターネットアクセスの保護における信頼性と一貫性の向上、そして長期的にはリモートブラウザ隔離による高度な制御の採用がより容易であることを理由に挙げています。

お客様のご意見

Cloudflareは、私たちのZero Trustのジャーニーにおけるフォースマルチプライヤー（戦力倍増マシン）となります。

John McLeod
National Oilwell Varco社
最高情報セキュリティ責任者

Cloudflareにより、Ziff Mediaグループは複雑なネットワーク設定をすることなく、世界中の従業員にあらゆるデバイスでシームレスかつ安全に社内ツール群を提供することができるようになりました。

Josh Butts
製品・技術担当上級副社長
Ziff Mediaグループ

Cloudflareを使用することで、開発環境におけるVPNやIP許可リストに対する依存を減らすことができます。

Alexandre Papadopoulos、
INSEADサイバーセキュリティ
担当ディレクター

デジタルネイティブのためのリモート中心の労働

デジタルネイティブ向けにはアジャイルセキュリティを優先し、リモートワークの柔軟性をサポートします

課題：クラウドセキュリティの拡張と自動化

多くの組織がリモート中心の採用を実施しています。これらの企業は、オンプレミスのインフラが限られており、安全、迅速、信頼性の高いデジタルサービスを前提としたビジネスモデルを持つ、若くて早いクラウド導入企業であることが多いようです。

どこでも仕事ができる柔軟性は差別化要因になりますが、ユーザーが個人所有のデバイスに依存して移動するため、同様に柔軟なセキュリティツールが必要です。

機会：拡張性に優れたコンポーザブルセキュリティ

デジタルネイティブ企業はレガシーITの廃止が少ないため、当社のインターネットネイティブなアーキテクチャと導入の柔軟性を活用し、セキュリティの近代化に俊敏に対応することができます。

コンポーザブルなサービス、API中心の設計、単一ペインの管理により、セキュリティの導入と適応が容易になります。グローバルネットワークのスピード、スケール、信頼性は、完全なリモートワークのニーズに応えます。

ユースケースの例ユースケース

B2B SaaS

状況：オーストラリアのグラフィックデザインプラットフォームCanva（2021年の評価額は400億ドル）サードパーティユーザーのアクセスを効率化し、VPN導入の手間を省くためにCloudflareを感染症の世界的流行以前にデプロイしていました。

ソリューション：時を経て、Canvaは成長する従業員全体にZero Trustアプリケーションアクセスポリシーを発表し、さらにインターネットフィルタリングとインスペクションを拡張しました。

Fintechとブロックチェーン

状況：BlockFi – ブロックチェーン技術を活用したシリーズD資産管理プラットフォーム – 管理資産とリモート中心の従業員の増加に対するサイバー脅威に直面し、セキュリティのレベルアップが必要でした。

ソリューション：Cloudflareにより、BlockFiはアプリケーションアクセスのためのIDベースの認証に移行し、時間のかかるIPベースの制御から脱却することができました。

ソーシャルメディア

状況：グローバルソーシャルメディアプラットフォームが内部のアプリケーションアクセスとVPN設定を悪用した侵入事件を起こし、注目を浴びました。

解決策：そこで同社は、13,000人の従業員と契約社員にCloudflare のZero Trust Network Access（ZTNA）のソリューションを採用し、VPN導入を廃止して、リモートアクセスのアプローチを全面的に見直すことにしたのです。

電子商取引

状況：グローバルなeコマースプラットフォーム（収益40億ドル以上、従業員15,000人以上）では、ネットワーク外でインターネットを閲覧し、機密性の高いSaaSアプリケーションにアクセスするリモートユーザーをより確実に保護することを求めていました。

ソリューション：当社は Cloudflare をデプロイし、DNS フィルタリングなどの脅威保護機能を重ねるとともに、SaaS アプリケーションの使用状況の可視化を強化しました。

お客様のご意見

Delivery Hero社では、常にお客様に素晴らしい体験をお届けすることを心がけています。Cloudflareは、社内のチームに対しても同じことをすることができます。世界中に安全な作業環境を提供し、高速で信頼性が高く、プライバシーを尊重したアプリケーションを簡単に構築する方法を提供しています。

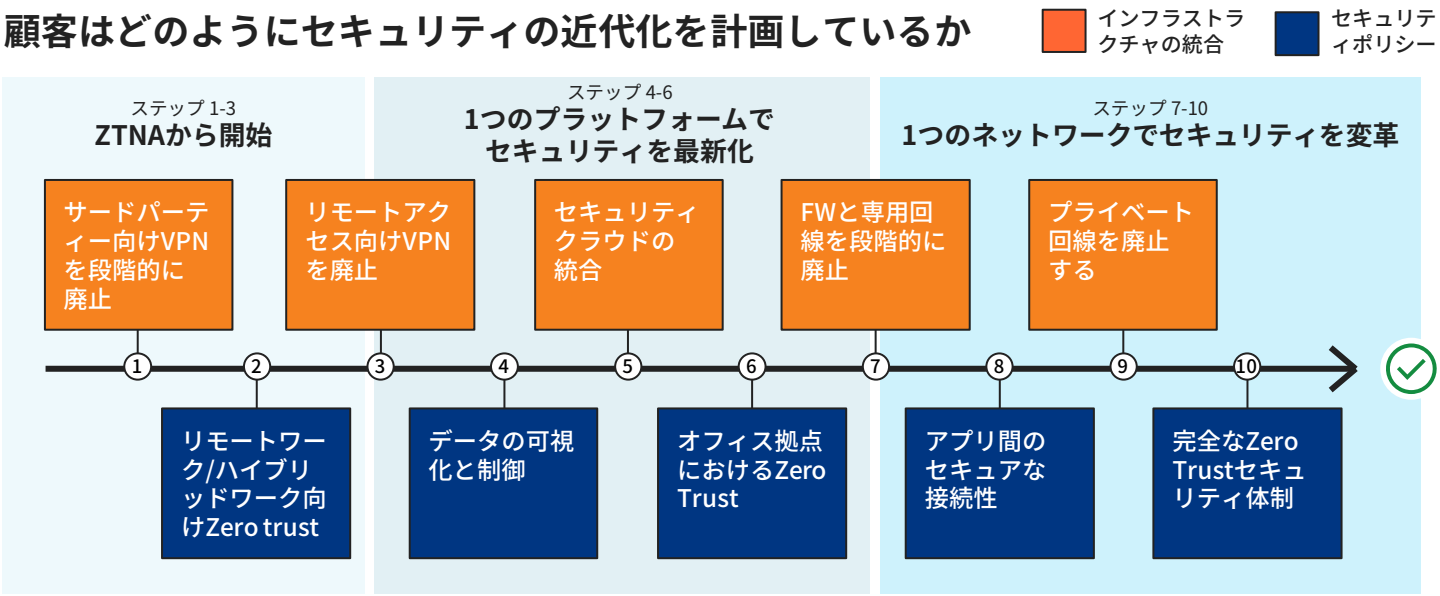
Christina von Hardenberg
Delivery Hero社
最高技術責任者（CTO）

Cloudflareは、急速に拡大するリモートワークのセキュリティを確保するために不可欠な存在です。アプリケーションへのアクセスにZero Trust を採用したことで、管理者は、従来のツールでは得られなかった可視性ときめ細かな制御を実現することができました。

Marccio Alcaide
Facily社
ITセキュリティ責任者

事例的ハイブリッド業務のロードマップ

顧客はどのようにセキュリティの近代化を計画しているか



セキュリティ近代化のロードマップ

上記のロードマップは、ハイブリッドワークに適応するためにセキュリティを近代化する際に、組織が取るべきアプローチの一例です。このロードマップには、2つの重要な目標があります。

1) **上段（オレンジ色）**：接続とセキュリティのインフラストラクチャを、ポイント製品やハードウェアから、1つのクラウドネイティブのプラットフォームに統合すること。
2) **下段（青色）**：ユーザーとリソースの間にZero Trustセキュリティを採用するための可視性と制御を、あらゆるデバイス、あらゆる場所で実現することです。

フェーズ1〜5：アプリとインターネットアクセスの確保

多くの場合、ハイブリッドワークに対応するためには、まず労働と企業リソースをどのように結びつけるかを近代化する必要があります。

フェーズ 1：多くの場合、最初のステップはVPNトラフィックのオフロードを開始し、契約社員、開発者、パートナー、新しく買収したチームなどの特定のユーザー向けにインターネットネイティブなコントロールに移行することです。Cloudflareはエンドポイントにソフトウェアをデプロイすることなく、ブラウザ経由でアクセスできるセルフホストアプリのセキュリティを特に簡単に確保します。

フェーズ 2：この最新のツールは、役割、MFAとハードキーの要件、アイデンティティとデバイスの配置に基づいてアプリごとのポリシーの構築に必要な可視性を提供します。

フェーズ 3：このアプローチに自信をつけるとチームはVPNを完全に廃止して、Web以外のプライベートネットワークやレガシーネットワークをZero Trustで保護する方向へと進んでいきます。

フェーズ 4：その後、シャドーITの軽減、テナントの管理、データ流出の防止など、SaaSアプリケーションの可視性と制御の改善に焦点が移行します。

フェーズ 5：内部アプリケーションとSaaSアプリケーションを単一のプラットフォームで管理するようになったため、企業は、外部へのインターネットアクセスの制御を拡張し、DNSフィルタやSecure Web Gatewayといった脅威から保護するツールを統合することを検討しています。

フェーズ 6〜10：接続性をクラウドに移行

ロードマップの残りのフェーズはほとんどの組織で計画中ですが、その願望は、すべてのネットワーク接続とセキュリティを1つの統一されたクラウドネットワークに移行することです。

フェーズ 6：この時点で、組織は一貫したZero Trustを本社、支店、データセンター、サテライトオフィスなどのあらゆるネットワークロケーションに拡張し、ハイブリッドワークのサポートを求めます。

フェーズ 7：オフィスのトラフィックがセキュリティのためにCloudflareに送られることが多くなると、企業は従来のオンプレミスのファイアウォールやその他のプライベートネットワークアプライアンスを段階的に廃止することができるようになります。

フェーズ 8：これらの高度なユースケースは、ハイブリッドマルチクラウド環境におけるアプリ間接続の確保に重点を置いており、ネットワークインフラストラクチャチームは**フェーズ 9**で通信会社のMPLS契約を終了する準備を整えられるようになります。

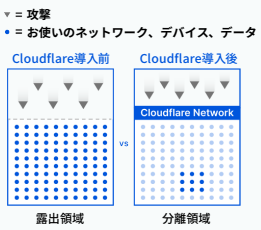
フェーズ 10：近代化が真の意味で終わることはありませんが、Zero Trustがすべてのユーザー、デバイス、データ、アプリケーション、環境に普及することが望まれています。

ビジネスとセキュリティの成果

Zero Trustが御社のビジネスの時間とコストを削減する5つの方法

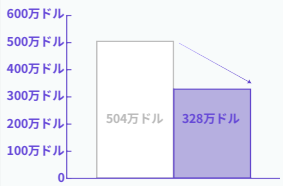
攻撃表面削減

91%↓



BREACH攻撃コスト削減

35%↓

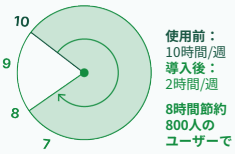


従業員オンボーディング高速化

60%↑

ITチケット負担削減

80%↓



ユーザーレイテンシー削減

39%↓

その他、事業の推進力となるもの

職場の生産性を飛躍的に改善

管理者向け

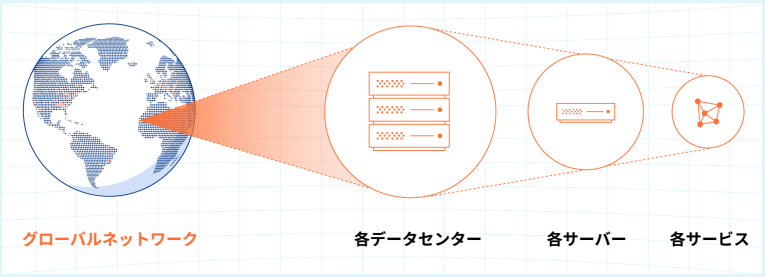
- ■アプリケーションとインターネットアクセスにまたがるポリシーを設定するための単一の管理インターフェイスによる設定の簡素化
- ■IDプロバイダー、エンドポイント保護、クラウドプロバイダー、ネットワークオンランプとの統合をすべて同じ管理インターフェイスから設定可能

エンドユーザー向け

- ■ストレスフリーの認証とネイティブなブラウジング体験、使い勝手の良いセキュリティ

従来型サービスのコスト削減

- ■仮想プライベートネットワーク（VPN）アプライアンスを交換または増強し、代わりにZero Trust Network Access（ZTNA）を採用
- ■オンプレミスの Web プロキシやファイアウォールからクラウドネイティブの L3〜L7 セキュリティサービスへの移行
- ■リモートブラウザーアイソレーション（RBI）で仮想デスクトップインフラストラクチャからユースケースを開放
- ■従来のセキュアなメールゲートウェイを近代的なクラウドメールセキュリティに置き換える



一貫した速度と規模で、リモートまたはオフィスのすべてのユーザーを保護

セキュリティ、パフォーマンス、信頼性を実現するすべての機能は、現在275都市に広がるネットワーク上のすべてのCloudflareデータセンターのすべてのサーバーで実行されるように設計されています。

Zero Trustのロードマップを加速させる

今すぐ試す　お問い合わせ

03-4510-1893 | enterprise@cloudflare.com | www.cloudflare.com

REV: PMM-2022JJUL

[1] *ハイブリッドワークをサポートするTop Network Practices*、Gartner社、Karen Brown、Andrew Lerner、Mike Toussaint、2022年4月8日
[2] *2022年度SASE Convergenceに向けた戦略的ロードマップ*、Gartner社、Neil MacDonald、Andrew Lerner、John Watts 2022年6月24日