CLOUDFLARE

ホワイトペーパー

今後への期待：経済的不確実性の時代に、より良いサイバーセキュリティ体制を構築する方法

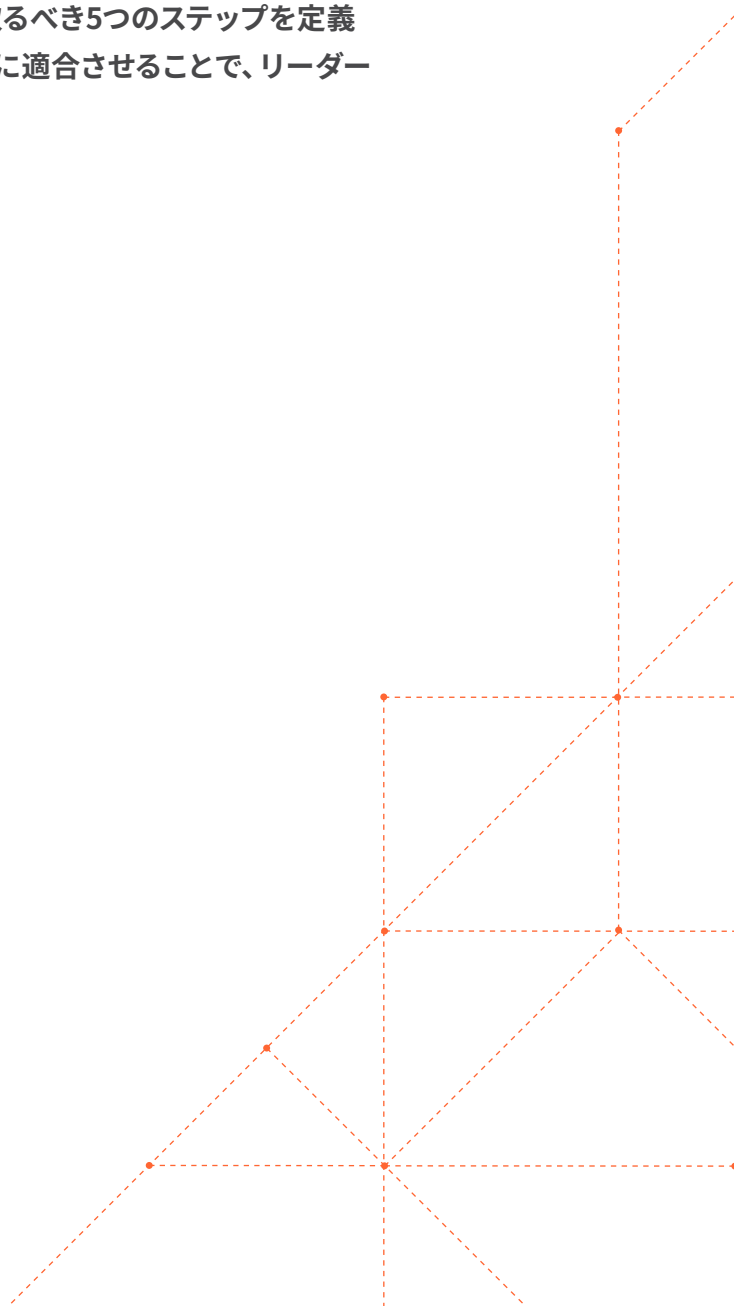
本文

概要

企業は、先行きの不透明感が増す中、経済の不確実性に直面しています。予算の縮小に代表されるこのような不確実性は、CIOや技術リーダーに新たな道筋を見出すようプレッシャーを与えています。

幸いなことに、予算の再調整、効率化のためのプロセスの刷新、リソースの大幅な増加を伴わない計画的な成長の継続など、嵐を乗り切るための戦略を立てたリーダーは、不確実な時代が終わった後も有利な立場に立てることがわかります。

次のセクションでは、そのような状況と市場環境を作り出しているさまざまな要因を見極め、考察を深めます。これらの洞察から、私たちは、セキュリティ体制を損なうことなく、セキュリティ対策を効率化する機会を見出すために、リーダーが取るべき5つのステップを定義しました。ITインフラストラクチャー戦略を新しい経済環境に適合させることで、リーダーは組織を将来にわたって成功に導くことができます。



はじめに

ここ数年、ITリーダーは戦略を練り、実行する中で、次から次へと起こる危機に対処してきました。世界的なパンデミックとその二次的影響、サプライチェーンの不足、東欧での紛争の激化、そして景気後退の可能性に対応しなければならなかったのです。スタンフォード大学で教鞭をとる経済学者ポール・ローマーの言葉を借りれば、「危機を決して無駄にしてはなりません」(出典)。CIOによるリモートワーク支援策は、職場を魅力的なものにするという思いがけない効果をも長期に渡ってもたらすことになるでしょう。同様に現在、経済の見通しの悪化に直面しているリーダーたちが、セキュリティ、ネットワーク、リモートアクセス、ストレージ、開発、インフラについて選択を行うことで、今後の安全で持続可能な成長に向けて、彼らはより強く、より良い立場を築くことができるようになるでしょう。

リモートワークの増加に伴って、ランサムウェアや高度なサイバー脅威が激増し、収益への影響、規模、巧妙さにおいて新たなベンチマークが確立されました（出典）。ネットワーク境界の残骸の消滅と退職者の増加が相まって、セキュリティギャップが生じ、戦略的ITプロジェクトに遅れが出ています。このため、組織は従業員の雇用と維持に関する取り組みだけでなく、システムやマシンへのアクセス制御についても再考を強いられています。パンデミックによりデジタル犯罪が劇的に増加しましたが（出典）、同時に、効果的なサイバーセキュリティの緊急の必要性に対する意識が組織と経営陣に芽生えました。今こそ、組織は安全性、生産性、可用性に優れたハイブリッドワークのインフラを長期にわたって提供するため、より戦略的な対策を講じるべき時です。

ここでは、限られた予算内でビジネスのリスクを軽減し、差し迫る新たな脅威への対応力を高めるためにできる5つのことを紹介します。

1. 既存のセキュリティツールを監査し、重複する機能を発見する

企業は、セキュリティベンダーを統合することによって多くのことを得られます。CISOが望む「特効薬」のようなソリューションとなるツールはありませんが、多くのセキュリティ担当者は、自社が最適な防御を実現できないまま、あまりにも多くのツールに無駄なお金を費やしていると考えている、と述べています。複数のベンダーの複数のツールをサポートすることは、従業員がインフラやデータを保護するのではなく、調達、実装、管理、トラブルシューティング、多数の切断されたシステムのサポートに貴重な時間を費やすことを意味します。実際、2022年6月にRSAカンファレンスで実施された調査では、「回答企業の半数（53%）が、サイバーセキュリティ予算の50%以上を浪費し、いまだに脅威を修正できていないと感じている」ことがわかりました。10%の組織が、サイバーセキュリティの脅威を修復するための効果的なツールが欠如しているとする一方、調査回答者の43%が、脅威の検出と修復における一番の課題は、ツールが多すぎることである」（出典）と述べています。これらのツールのうち、ほんの一握りでもなくすことができれば、従業員の貴重な時間を節約しながら、セキュリティを向上させることができるのです。

また、資本的支出から運用的支出に投資をシフトすることで、短期的なキャッシュフローを即座に改善し、ビジネスの俊敏性を阻害する複数年にわたる資本投資に縛られることを回避できます。簡素化する方法の一つとして、従来のハードウェアへの依存を減らすことが挙げられます。従来の機器からas-a-Serviceソリューションに移行することにより、たとえ予算が減少しても、最優先の取り組みの資金を確保することができます。また、as-a-Serviceモデルを採用することで、ソフトウェアが本来持っている革新的なサイクルの恩恵を受け、レガシーなハードウェアに頻繁にパッチを当てるという避けられない苦痛から解放されます。パッチの適用や技術革新の負担を軽減することで、チームはビジネスを真に差別化する活動に集中することができます。不確実性に直面したとき、戦略的な簡素化と統合は、長期的な成功の実現に役立ちます。

2. ツールだけでなく、データにも焦点を当てる

幹部チームは、パターンや異常をよりよく発見するために、すべてのセキュリティツールセットにおいて、ツールだけでなく、データをよりよく統合することに焦点を移すことを検討するべきです。歴史的に見て、セキュリティチームは、あまりにも多くのデータセットが多くの場所に存在することによる長期的な影響を考慮することなく、時間をかけてツールセットを増やし続けてきました。その結果、相互運用性がほとんどなく、デ ー タが不透明な製品を寄せ集め、ヒューマンエラーの可能性をもたらすことによって、得られるインサイトの精度が低下する結果となります。言うまでもなく、チームは、複数のデータセットを取り出し、それらを統合し、クエリーを実行するために要する時間において、時間だけではなく、リソースも浪費することになります。代わりに、そのようなリソースを、より戦略的なビジネスへの取り組みに集中させることができます。

データセットの手動での結合やCSVのインポート/エクスポートなど、相互運用性の課題を解決するためのクリエイティブな回避策を見つけることができるかもしれませんが、効率性はさておき、セキュリティツールの価値は、これらのシステムが取り入れ、作成し、守備側に利用可能にするデータにこそあると考慮することが重要です。もし、あなたのデータがいたるところに存在し、分類されず、保護されず、慎重に管理されていないとしたら、特にシャドーITの事例で、完全に放置されている可能性のあるデータがある場合、そのようなデータの影響が及ぼす状況の把握に歪みが生じる可能性があります。ツールセットを統合し、セキュリティスタックの相互運用性を綿密に考慮することで、ヒューマンエラーを減らし、データの安全性をより高めることができます。なぜなら、たとえ現在入手可能な最高のツールに投資していたとしても、サイロ化されたデータセットやシャドーデータセットによって、状況の把握がより困難になる場合があるためです。

効率という点では、Zero Trust（「決して信用せず、常に検証する」）の時代において、ツールが増えるということは、チームが仕事を始める前にログイン、認証、システムへのアクセスにさらに時間を費やすことになると考慮することが重要です。従業員が触る必要のあるシステムが少なければ少ないほど、従業員は時間を節約でき、より速く行動することができます。これらのシステム内のデータ、および与えられたタスクを完了するためにどれだけのシステムにアクセスしなければならないかが、最終的に、チームが脅威に対しタイムリーに反応できるかを決定するのではなく、その対応能力を可能にするか妨げるかを決定するのだと考慮することが極めて重要です。

3. イノベーションを最大化し、複雑さを最小化するために、クラウドやas-a-Serviceモデルに注目する。

すべてのビジネスは競争力を維持するためにイノベーションを行う必要がありますが、サイバーセキュリティをビジネスとしていない企業は、最新のCVE、攻撃トレンドに遅れずに付いていくための、時間、予算、リソースがなく、インフラ全体の安全性を保つために必要な重要なパッチを適用していないのです。実現可能であれば、as-a-Serviceモデルを採用することで、リーダーは、技術的負債に関するトレードオフや困難な意思決定を気にすることなく、継続的なイノベーションの恩恵を受けることができるようになります。

また、セキュリティサービスの中には、トラフィック制限を超えた場合に超過料金を請求するものや、帯域幅の料金を請求するものがあることも考慮に入れておく必要があります。自分の組織が月または年単位で支払っている金額をよく見て、自分たちが思っている以上に支払っていないかどうか把握することを検討してみましょう。もしそうなら、この機会に超過料金を請求しない他のソリューションを探し、費用を節約するだけでなく、長期的にもっと予測可能な支出を行うことで、チームが将来に向けてより良い計画を立てることができるようになります。

このようなクラウド配信サービスを利用すれば、一連の高価なハードウェアの設置やそれに伴うライフサイクル管理に煩わされることなく、必要に応じて組織を拡大・縮小することも可能です。不確実性の高い時代において、企業は市場環境の変化に俊敏に対応し続ける必要があります。キャッシュフローが懸念される場合は、コストの最小化やゼロ化ができる能力が戦略的優位性となり、なんとか生き延びる企業と市況に関わらず繁栄する企業の差になり得るのです。

4. 従業員体験をレベルアップする

Forbesでは次のように記されていました。「我々の調査では、複雑で多段階のログインプロセスによって労働者はイライラし、時間を浪費し、生産性が妨げられ、仕事に関連する重要なタスクをあきらめてしまうことが分かりました。究極の皮肉として、40%近くの労働者が、負担の大きいログインプロセスのために新しい仕事のセキュリティアプリの設定を先送り、委任、完全にスキップしたことがあると回答しました。これは、お金で買える最も頑丈で、最も高く、最も安全な門で家を守り、レーザー光線を吐くドラゴンで防御し、夜間は無施錠のままにしておくようなものです。」どのツールがどの機能を担っているのかを追跡するのは非効率的で難しいだけでなく、ダッシュボードが多すぎたり、データが置かれる場所が多すぎたりすると、どんな組織にとっても大きなセキュリティリスクと可視性のギャップが生じることになります。サイバーセキュリティの脅威を先取りしたい企業は、クリックやキーストロークの一つ一つが、重要なイベントへの対応から貴重な時間、エネルギー、集中力を奪っていることを考慮しなければなりません。より良い、より合理的な従業員体験を実現するために、経営幹部は、防御側が効果的に仕事をするためにどれだけのツールが必要か、また、防御側が重要なセキュリティイベントに対応するだけでなく、対応にかかる時間を短縮するために何を排除または統合することができるかを厳しく検討することが重要です。

非技術系従業員や守秘義務のない従業員に関しては、リモートワーカーが個人の生産性を高めるために、シャドーITなど次善策に頼る可能性があることも考慮する必要があります。ZeroTrust管理は、特にリモート環境において、より安全な組織を構築するための有望な道筋を提供しますが、すべてのZero Trustアプローチが同じように作られていないことは否定できません。従業員が必要なものにアクセスするのが複雑であればあるほど、セキュリティ管理を遵守するのではなく、セキュリティ管理を回避する方法を見つける可能性が高くなります。リーダーは、セキュリティ製品の有効性だけでなく、使いやすさについても理解する必要があります。

5. ネットワークパフォーマンスを損なわないセキュリティサービスを探す

ツールだけでなく、ツールをどのように構成し、どのように管理するかが、すべての違いを生み出します。パフォーマンス向上に役立つ可能性のある機会を発見するために、現在の構成やカスタマイズの監査をチームに依頼することを検討しましょう。パフォーマンスの向上が不可能な場合は、パフォーマンスのために一から構築されたソリューションを探すことを検討してください。パフォーマンス向上を後から付け足そうとしても、リーダーが達成したいと望む目標を達成することは難しくなります。ネットワークのパフォーマンスに関しては、貧弱なアーキテクチャではアウトコードできないことを念頭に置いておくことが重要です。建物の設計図でも、基礎が出来上がると設計のやり直しが効かなくなるように、ネットワークも究極のパフォーマンスを発揮するためには、一から設計する必要があります。

データを処理し、ソースに最も近いところで処理するグローバルエッジネットワークの力を活用することで、組織は現在と将来の両方で戦略的優位性を得ることができます。MITテクノロジーレビューによると、「大量のデータを処理すると、パフォーマンスの問題につながることがあります。これに対し、多くの企業がエッジコンピューティングに注目しています。エッジコンピューティングは、プライバシーとセキュリティの要件を維持しながら、ソースに近いところでデータを処理し、高速でリアルタイムの分析と応答を可能にします」（出典）。将来のアーキテクチャを前提としたソリューションを戦略的に選択することで、プライバシーとセキュリティという重要な要素を犠牲にすることなく、より優れたネットワークパフォーマンスという戦略的優位性をチームに与えることができるようになります。

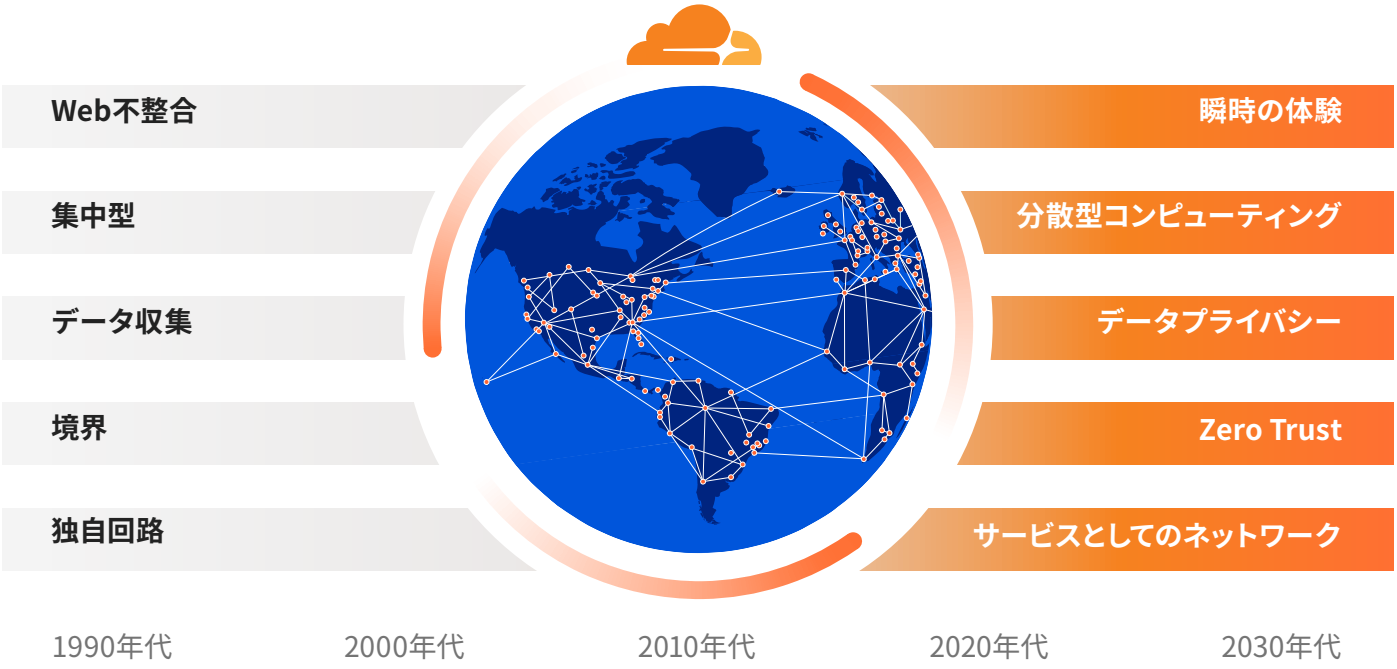
要約すると、不確実な時代に、より良いサイバーセキュリティ体制を構築するために行うことができる手順は次のとおりです。

1. **既存のセキュリティツールを監査し、重複する機能を発見する**
   - 重複するツールを統合する
   - 設備投資（CapEx）から運用コスト（OpEx）へ投資をシフトする
2. **ツールだけでなく、データにも焦点を当てる**
   - ツールの相互運用性によって、より良い、より正確なデータセットにつながる
   - より正確なデータセットとレポート作成は、ビジネスゴールの達成に不可欠な優れた知見へとつながる
3. **イノベーションを最大化し、複雑さを最小化するために、クラウドやas-a-Serviceモデルに注目する**
   - サイバーセキュリティをビジネスとしていない場合、パッチ適用、保守、アップグレードをas-a-Serviceに移行することで得られるものが多い
   - クラウドとas-a-Serviceモデルは、変動する経済環境の中で機敏に行動するために必要な柔軟性を提供してくれる
4. **従業員体験をレベルアップする**
   - 多くのツールを多くの場所に置くことは、セキュリティの盲点や従業員のフラストレーションを生むため、統合や簡素化することで、従業員体験を最適化することができる
   - 従業員が使いやすいように最適化することで、従業員の定着率を高め、シャドーITに頼って仕事を終わらせようとすることを阻止できる
5. **現在のサイバーセキュリティスタックに隠れたコストとパフォーマンス向上の機会を探す**
   - 既存のツールを監査することで、パフォーマンスを最適化する機会を見出すことができる
   - お客様がいる場所に最も近くグローバル規模で構築されたツールを採用することで、組織は、より優れた、安全な顧客体験を提供することが可能となる

Cloudflareのサービス

Cloudflareは、2008年経済危機の余波が残る2010年に、オンプレミスのインフラストラクチャからクラウドへの移行を先導すべく設立されました。より良いインターネットの構築を支援するという大胆な目標を掲げて、Cloudflareのプラットフォームを構築したのです。Cloudflareの製品スイートは、ハードウェアの追加もソフトウェアのインストールもコードの変更も一切行わずに、インターネットに接続されたあらゆるものを保護し、高速化します。

Cloudflare上のインターネットプロパティは、すべてのWebトラフィックがCloudflareのインテリジェントなグローバルネットワーク経由でルーティングされています。しかも、このネットワークはリクエストを受け取るたびにスマートになります。Cloudflareは、お客様がよりスマートに働き、より優れた構築を行い、より速く実行し、安全・確実に成長できるよう支援します。現在、Cloudflareは数百万ものインターネットプロパティを保護し、高速化しています。



制御

包括的な接続性、セキュリティ、コンピューティングを提供しつつ、ポリシーはお客様がコントロールできるようにした統合グローバルネットワークです。

Flexibility

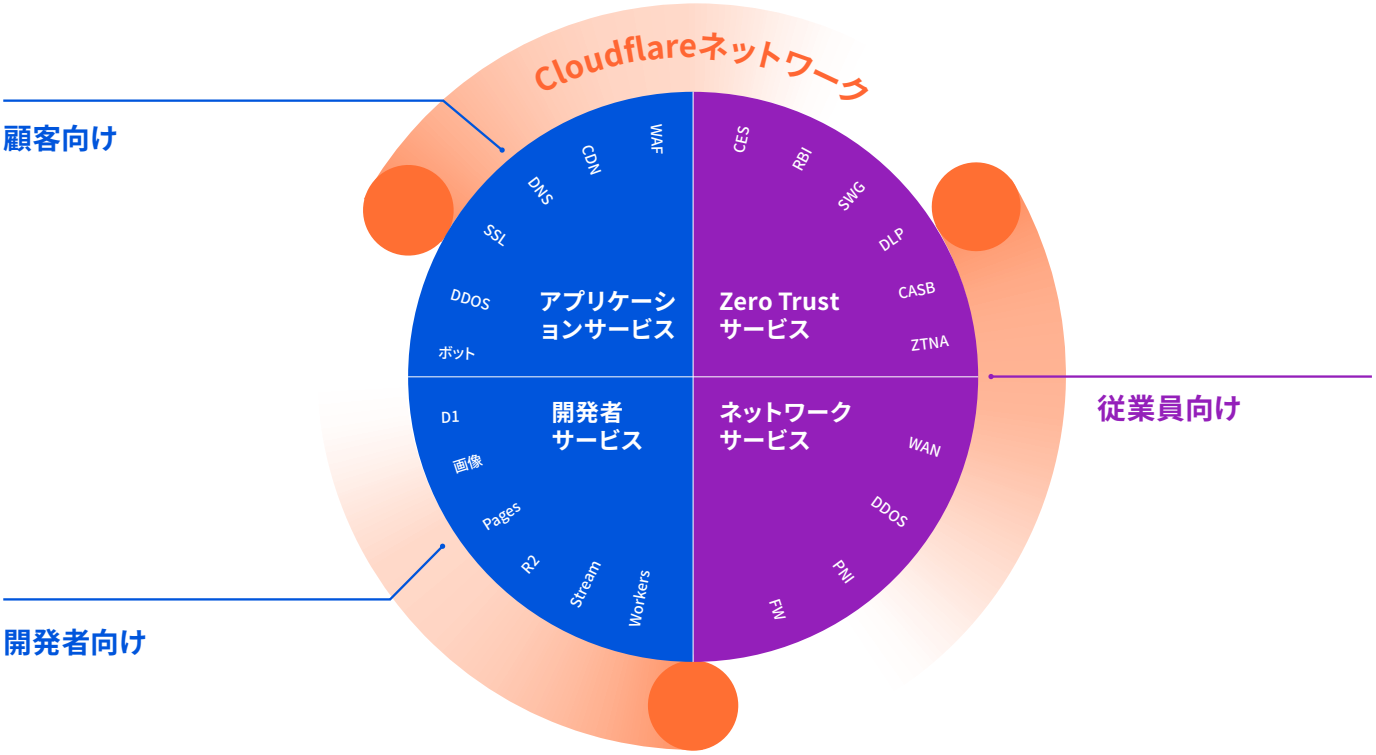
クラウドネイティブなサービスですので、先行資本投資は必要ありません。ビジネスの変動に合わせて使用量を簡単に増減できます。

予測可能性

予測可能な請求 – 際限のないエグレス費など、想定外の費用は一切かかりません。来年にならなければ届かないハードウェアに今資本投資する必要はありません。

Cloudflareのグローバルネットワークは、インターネットに接続するものすべての安全性、プライバシー、信頼性を高め、高速化します。

- Webサイト、API、インターネットアプリケーションの**安全を確保**
- 企業ネットワーク、従業員、デバイスを**保護**
- ネットワークエッジで実行するコードを**記述**して**デプロイ**

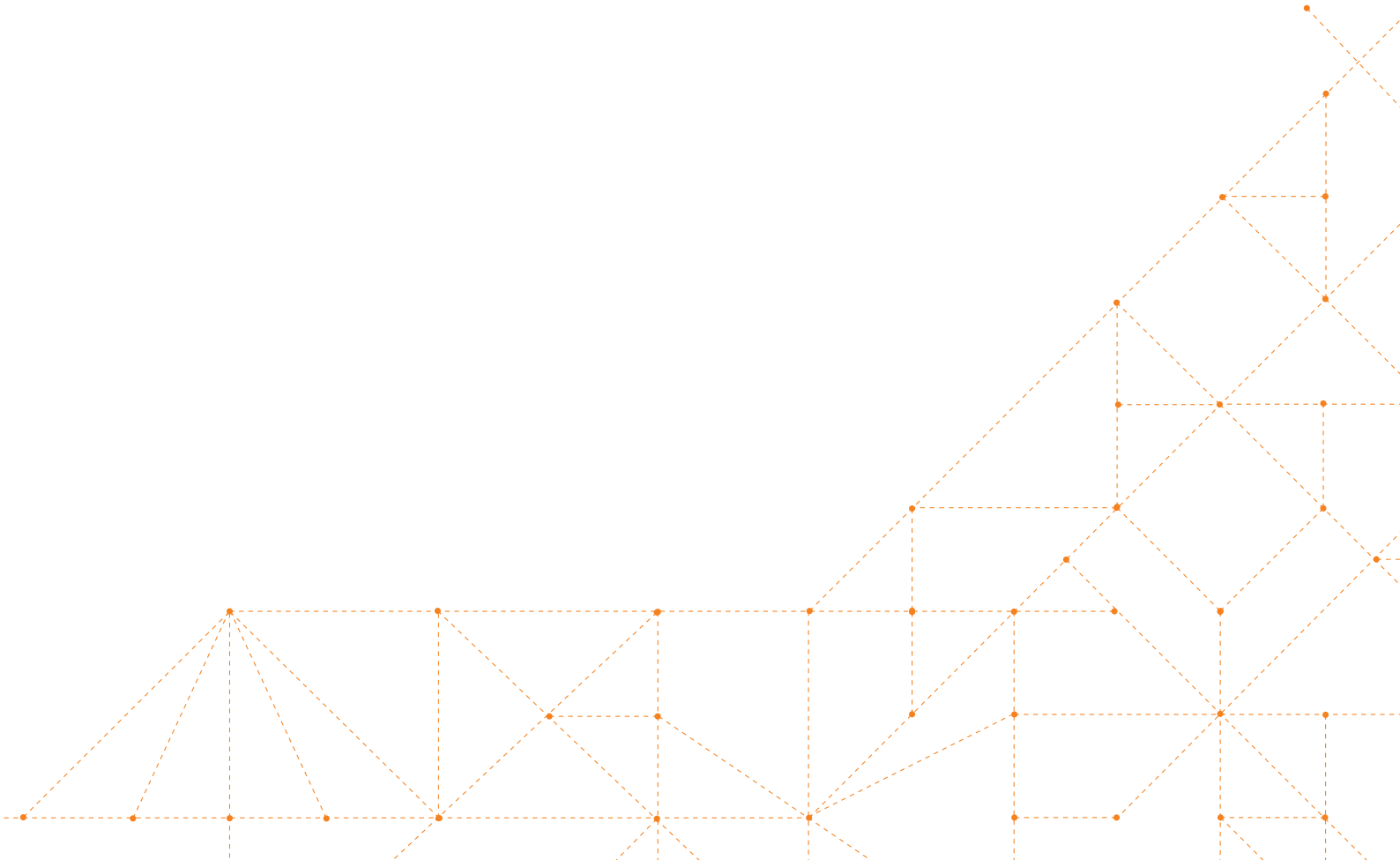


Cloudflareのプラットフォーム

Cloudflare（クラウドフレア）について

Cloudflareはオンプレミスのインフラストラクチャをクラウドへ移行する作業を促進するために2010年に設立されました。Cloudflareでは、より良いインターネットの構築を支援するという会社の使命を十分に理解したうえで、まったくのゼロからプラットフォームを作りました。Cloudflareの製品スイートは、ハードウェアの追加、ソフトウェアのインストール、コードの変更を要することなく、インターネット上のあらゆるオンラインアプリケーションを保護し、高速化します。Cloudflareで稼働するインターネットプロパティであれば、すべてのWebトラフィックがCloudflareのインテリジェントなグローバルネットワーク経由でルーティングされます。しかも、Cloudflareネットワークはリクエストごとにスマートになります。Cloudflareはお客様がよりスマートに働き、製品を改善し、実行速度を上げ、安全に成長できるよう支援しています。現在、Cloudflareは数百万ものインターネットプロパティを保護し、高速化しています。

詳細については、こちらをご覧ください：www.cloudflare.com



CLOUDFLARE

enterprise@cloudflare.com | www.cloudflare.com

REV:BDES-4327.2023MAR10