ゼロトラスト・セキュリティが必要な４つの理由

目次

はじめに

攻撃者の高度化、ランサムウェアグループの急増、テクノロジーの進歩による新たな脆弱性の発生に伴い、企業はますますゼロトラスト・セキュリティ・モデルに注目するようになっています。このアプローチの核心は、以前のセキュリティアプローチの中核を成すユーザー、アプリケーション、デバイスへの暗黙的な信頼を排除することです。実用的な観点からは、ゼロトラスト・セキュリティ・モデルから組織が恩恵を受ける主なシナリオは 4 つあります。企業に対するランサムウェア攻撃、テレワークへの移行、クラウド環境のセキュリティ確保の必要性、次回の監査です。

これらのシナリオは、ランサムウェア攻撃の増加、従業員のハイブリッド勤務（ハイブリッドワークフォース）への移行、クラウドコンピューティングへの移行、セキュリティ監査からの要求の増加といった最近の傾向の結果であり、場所に関係なくアイデンティティを検証し、セキュリティ侵害への対処にあたって予防的な対策を講じるセキュリティアプローチが求められています。ゼロトラストは、データへのアクセスに強力なユーザーアイデンティティを必要とし、攻撃が発生した時点で積極的な緩和策を提供する唯一のアプローチです。

ゼロトラスト戦略の導入は、すでにオーバーワーク状態のセキュリティチームには手に余るように思えるかもしれませんが、必ずしもそうではありません。段階的なアプローチを採用し、迅速に得られる成果に集中することで、従来のセキュリティソリューションに伴う複雑さとリスクを軽減し、セキュリティ体制を改善できます。

ゼロトラストの導入を開始するにあたり、既存のテクノロジーを総入れ替えする必要はありません。まず、最も差し迫ったビジネスニーズに合わせてゼロトラストへの投資計画を立てることから始めることが重要となります。一夜にして進化して古いソリューションをゼロトラストとしてブランディングし直したようなベンダーではなく、信頼の確立されたゼロトラスト・ベンダーを選択してください。ゼロトラスト・セキュリティの複数の要素（ゼロトラスト・ネットワーク・アクセス（ZTNA）、DNS ファイアウォール、マイクロセグメンテーションなど）を単一のプラットフォームで組み合わせることができるベンダーを是非検討してください。ゼロトラストを導入する理由を問わず、ビジネスのアジリティ、コストの最適化、ツールの統合を実現し、業務全体を改善できます。

企業がゼロトラストに移行する理由のトップ 4

ランサムウェア攻撃の増加

ハイブリッドワークフォース

クラウド・コンピューティング・リソースの採用

厳しいコンプライアンス要件

01

ランサムウェア攻撃の増加

ランサムウェアからの保護の強化

ここ数年で、ランサムウェア攻撃は、病院や銀行からパイプライン、その他の重要なインフラまで、世界中の企業を混乱に陥れてきました。現に、**Cybersecurity Ventures** は、ランサムウェアの被害者がこうむる損害額は、2031 年までに年間約 2,650 億米ドルに上ると予測しています。予測では、ランサムウェアの攻撃者は、マルウェアのペイロードと関連した脅迫行為を徐々に洗練させていくにつれ、2 秒に 1 回のペースで（消費者または企業に対する）新たな攻撃を仕掛けてくるだろうとされています。

ゼロトラスト戦略が導入されていない場合、ランサムウェアグループによって次のような弱点を突かれる可能性があります。

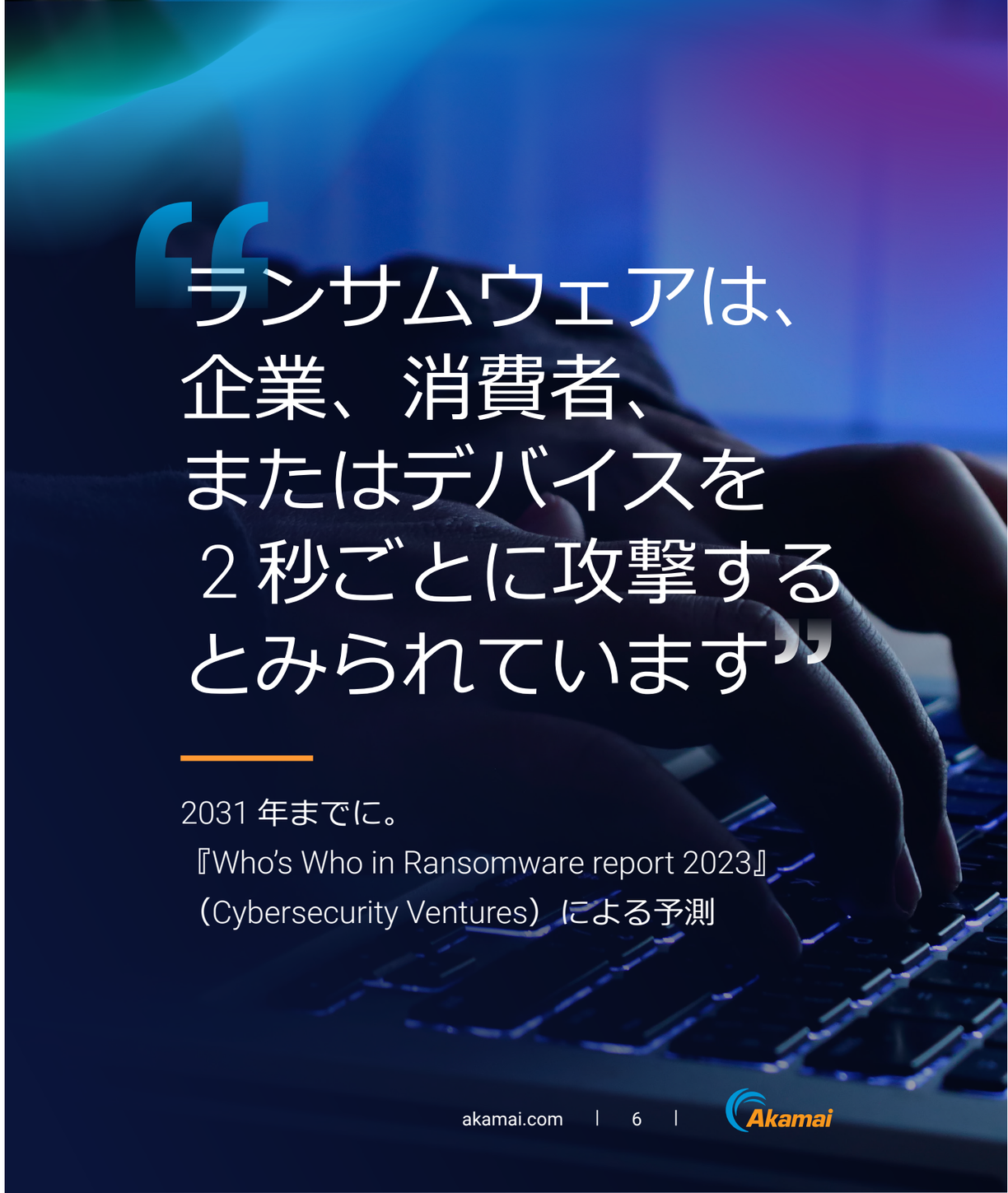
- ユーザー、アプリケーション、およびネットワークに対する暗黙の信頼。ネットワークへの侵入を果たした攻撃者は、暗黙の信頼があることによって、横方向に移動してマルウェアを拡散させることができます。
- 過剰に寛容なアクセスポリシー。マルウェアへの感染と、それによるランサムウェアの注入を可能にします。
- パスワードだけに頼るシステム。認証情報盗用の機会を攻撃者に与えます。

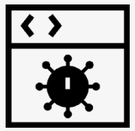
ゼロトラストはどのように役立つのか

ゼロトラスト・アーキテクチャ、アクセス制御ポリシー、マイクロセグメンテーションを導入して使用している企業は、このような攻撃による損害を最小限に抑えることができます。攻撃者は最初にシステムに侵入することが難しくなるだけでなく、拡散力が制限されます。

Akamai はどのようにランサムウェアのキルチェーンを断ち切るのか

ランサムウェア攻撃には、通常、初期感染、ラテラルムーブメント（横方向の移動）、データ窃取と暗号化が含まれます。ゼロトラストを導入した企業は、各手順が実行されるたびに、あるいは実行される前でさえ対処することができます。





初期感染

Akamai Guardicore Platform は、最初のエントリーポイントを超えて攻撃が拡散するのを防ぎます。Akamai MFA は、ユーザーが認証情報を盗まれたり悪用されたりしないように保護します。

ラテラルムーブメント

Akamai Guardicore Platform は伝搬経路を減らし、ラテラルムーブメントを防止します。Akamai Guardicore Access は、悪用したいアプリケーションを感染させようとする攻撃者の動きを制限します。Akamai Hunt は、検知回避能力の高い高度な脅威をネットワーク内で検知して緩和します。

データ窃取と暗号化

Akamai Guardicore Platform は、重要なアプリケーションへのアクセスを制限し、侵害されたネットワーク内の機微な情報に攻撃者がアクセスできないようにします。Akamai Secure Internet Access Enterprise は、フィッシングサイトやコマンド & コントロールサイトへのリクエストをブロックします。そして、Akamai Hunt は異常なふるまいを検知し、攻撃者が貴重なデータを暗号化して身代金を要求することを防ぎます。

02

ハイブリッドワークフォース

新しいハイブリッドワークフォースのセキュリティ確保

ファイアウォールや VPN などの旧式のセキュリティツールを使用している企業では、コロナ禍をきっかけに発展・拡大した新しいハイブリッドワークフォースのセキュリティを確保することが困難です。リモートアクセス VPN が最初に導入された 30 年ほど前は、状況がまったく異なりました。インターネットは初期段階にあり、アプリケーションはデータセンターで実行されていました。また、リモートロケーションから接続するユーザーははるかに少数でした。VPN を使用してユーザー認証を継続し、ネットワーク全体にアクセスできるようにすると、アタックサーフェスが拡大し、レガシー VPN に伴う多くのゼロデイ脆弱性の悪用が可能になります。必要な認証情報を持つユーザーは誰でも企業 VPN にログオンできます。内部に入ると、ユーザーはネットワーク内を横方向に移動して、VPN で保護されるべきリソースにアクセスできるようになります。

ゼロトラストはどのように役立つのか

最小権限アクセスの原則に基づくゼロトラストは、どのようなユーザーやアプリケーションも本質的には信頼すべきでないことを前提としています。ゼロトラスト・ネットワーク・アクセス（ZTNA）は、VPN とはまったく異なるアプローチで、テレワーカーのアクセスのセキュリティを確保します。ユーザーは、ネットワーク全体をリスクにさらすことなく、必要なアプリケーションとデータのみに直接接続します。これにより、機微な情報やリソースへのアクセスが過度に許容された悪性のユーザーが横方向に移動することを防止します。違反が発生した場合でも、効果的なゼロトラスト・マイクロセグメンテーション・ソリューションであれば内部ネットワークをセグメント化できるため、侵害が広がってネットワークの他の部分にダメージを与えることはありません。**Gartner** によると、2025 年までには、新規導入されるリモートアクセスの 70% 以上が VPN サービスではなく主に ZTNA で行われるようになります。この割合は、2021 年末時点では 10% 未満でした。

Akamai はハイブリッドワークとテレワークをどのように促進するのか

Akamai の包括的なゼロトラスト・プラットフォームは、ハイブリッドワークフォースのニーズを満たします。メリットは次のとおりです。

リスクの軽減

Akamai は、適切なユーザーを適切なアプリケーションに直接接続し、アタックサーフェスを縮小し、ラテラルムーブメント（横方向の移動）を制限します。

ユーザー体験が向上

リモートユーザーは、アプリケーション、デバイス、ロケーションにかかわらずリソースにアクセスできるため、VPN に接続したり接続を解除したりする必要はなくなります。

アジリティの向上

Akamai のソリューションはサービスとして使用されるため、企業はハードウェアを展開する必要がなく、需要の増加に合わせて拡張する必要もありません。そのため、コストと複雑さが軽減されます。

03

クラウド・コンピューティング・リソースの採用

クラウド移行の簡易化

企業は、柔軟性とアジリティを確保し、インフラを最新化するために、アプリケーションをクラウドに移行しています。しかし、このようなクラウド環境ではアタックサーフェスが拡大し、新たなセキュリティ要件も生じます。さまざまなクラウド環境とオンプレミス環境間の統合により、アプリケーションが壊れ、セキュリティが危険にさらされる可能性があります。企業が従来のネットワーク構成（VPN やファイアウォール）を使用してアプリケーションをクラウドに移行しようとすると、横方向の脅威、不十分なスケーラビリティ、高いコストなどのリスクの増大に直面することがよくあります。移行が完了した後も、アセットは安全である必要があり、ユーザーはロール権限に基づいて認証されなければなりません。クラウドインフラのユーザーは、通常、オンプレミス環境よりもリソース、サービス、および管理権限へのアクセス権が強いため、追加のリスクや中断の可能性が生じます。

ゼロトラストはどのように役立つのか

ゼロトラスト戦略はクラウドへの移行を促進します。ゼロトラストは、脆弱性をもたらす可能性のある多くのクラウドベースのアプリケーション、特にサードパーティ製アプリケーションに内在する潜在的な信頼を排除します。ゼロトラスト・ソリューションを利用すれば、企業はより強力な保護機能を備えたクラウドベースのアプリケーションをより簡単に展開できます。ゼロトラストをクラウドに展開する利点には、次のようなものがあります。

- ☑ 資産とリスクに対する可視性が向上
- ☑ ゼロトラスト・セグメンテーションとクラウドリソースへの最小権限アクセスにより、アタックサーフェスを縮小
- ☑ 最新化されたネットワークインフラにより、スピードとアジリティを確保
- ☑ IT 運用コストを削減し、複雑性を軽減

Akamai はどのようにクラウド移行を改善するのか

Akamai のゼロトラスト・ソリューションは、アセットとそれぞれのポリシーを自動的に移行するのに役立ちます。ダウンタイムもビジネスの中断もありません。Akamai は次のことを実現します。

より優れた可視性

アプリケーションの依存関係をより深く理解することで、効果的なクラウド・セグメンテーション・ポリシーを作成して、アタックサーフェスを縮小し、リスクを最小限に抑えることができます。

ゼロトラスト・ネットワーク・アクセス（ZTNA）

ユーザーは、強力な認証に基づいて、アクセスを許可されたアプリにのみ接続できます。

脅威ハンティング

Akamai の脅威ハンター専任チームは、クラウド環境全体で異常な攻撃のふるまいを継続的に検索し、Akamai のお客様にネットワークに対するリスクを通知します。

04

厳しいコンプライアンス要件

コンプライアンスのシンプル化とリスクの軽減

セキュリティ管理者はコンプライアンス要件を満たしているからといって真の安全な企業であるとは限らないことを知っていますが、セキュリティ監査は依然として経営陣にとって最優先事項です。経営陣は、監査に失敗するとビジネスの大きな中断が発生し、収益に影響が及ぶ可能性があることを認識しています。コンプライアンス評価は、セキュリティチームにとって最も時間とリソースを消費する活動の一つです。さらに、デジタル環境への移行とテレワークの普及により、コンプライアンスはさらに困難になっています。通常、企業は、Payment Card Industry Data Security Standard（PCI DSS）、Health Insurance Portability and Accountability Act（HIPAA、医療保険の携行性と責任に関する法律）、Society for Worldwide Interbank Financial Telecommunication（SWIFT、国際銀行間通信協会）などのコンプライアンス基準を満たすために、環境を隔離し、規制対象資産をリングフェンスする必要があります。

また、リモートユーザー、企業のオンプレミスユーザー、パートナー、サプライヤーなどに対応する必要があり、企業の環境の境界を定義することはほぼ不可能です。アクセス制御は監査を成功させるための主な決定要因であり、セキュリティチームは監査準備の際に次の質問に対処する必要があります。

- 機微な情報へのアクセスを許可されたユーザーのみに制限するためにはどうすればよいですか？
- 監査環境を詳しく調べるためにはどうすればよいですか？
- 監査プロセスをシンプル化し、秩序あるものにするためにはどうすればよいですか？

ゼロトラストはどのように役立つのか

幸いなことに、ゼロトラスト・アプローチは、これらのすべての質問に対処するのに役立ちます。ゼロトラストの 2 つの主要な柱である、明示的に検証する能力と最小権限アクセスをサポートする能力により、コンプライアンスのプロセスが大幅にシンプル化されます。企業は、規制対象の資産をデータセンターやクラウド内の他のトラフィックから分離し、場所を問わず、アイデンティティに基づいてアクセスを許可できます。強化された可視性は、規制された環境の内外での流れを把握し、範囲内の内容を特定するのに役立ちます。これにより、監査の複雑さとコストが大幅に削減され、監査担当者の作業が容易になります。

Akamai はどのようにコンプライアンスを促進するのか

Akamai の包括的なゼロトラスト・ポートフォリオにより、PCI DSS、HIPAA、国際標準化機構（ISO）、サーベインス・オクスレー法（SOX）といったあらゆるフレームワークの監査に対応できます。Akamai Enterprise Application Access は、機微な個人情報への第三者によるアクセスを制御し、一般データ保護規則（GDPR）の要件を満たします。Akamai Guardicore Segmentation は、PCI DSS に基づく規制対象資産の理解を向上させ、クリアリングハウス機能を分離して HIPAA に対応し、インターネットアクセスを制限し、重要なシステムを分離して SWIFT 規制に対応します。Akamai MFA は、ヘルスケアシステムのパスワードを取得した攻撃者から HIPAA 患者情報を保護し、認証情報の侵害を防止することで、SWIFT コンプライアンスを強化します。

グローバルな銀行が 2 週間で SWIFT コンプライアンスを達成

外部の規制当局は、あるグローバル規模の銀行（Akamai のお客様）に、重要なアプリケーションをすべてリングフェンスし、金融機関間の安全な送金に関する SWIFT の要件を満たすことを求めました。通常、このようなアプリケーションでは、ベアメタルサーバーや仮想サーバーなど、さまざまな場所に 100 台以上のサーバーを導入する必要があります。平均すると、その規模の銀行では、このプロセスの計画と実行には 8〜12 か月の時間がかかります。なぜなら、複数の拠点にまたがるセグメントに対してバーチャル・ローカル・エリア・ネットワーク（VLAN）を構築する必要があるためです。SWIFT アプリケーションの依存関係を把握し、ルールセットが正しく、何も壊れていないことを確認することが、タイムラインに追加されることになります。一方、このプロジェクトでは、新しいファイアウォール機器の購入も必要になります。また、SWIFT アプリケーションは銀行業務にとって不可欠であるため、銀行はダウンタイムを許容できませんでした。全体として、セグメンテーションプロジェクトには多くの人々の多大な努力が必要でした。しかし、Akamai を利用したため、たった 1 人のセキュリティエンジニアが約 2 週間でプロセス全体を完了することができました。ネットワークの変更は不要で、銀行はアプリケーションの変更やダウンタイムを回避できました。

コンプライアンスのシンプル化と促進

グローバル規模の銀行

- SWIFT アプリケーションのリングフェンスが必要
- ベアメタル、VMware、および OpenStack サーバーを備えた複雑な環境

従来のセグメンテーション

- 複雑なインフラ全体でセグメントを定義するのが困難
- アプリケーションや依存関係の可視性がない
- ダウンタイムが必要
  期間：8 ～ 12 か月
  スタッフ：少なくとも 5 人

Akamai Guardicore Segmentation

- SWIFT アプリケーションのマッピングを数時間で完了
- セグメンテーションポリシーを自動で提案して微調整
- 新しいハードウェアやファイアウォールの購入と展開は不要
- ダウンタイムなし
  期間：2 週間
  人員：アーキテクト 1 人

Akamai ゼロトラスト・ポートフォリオでビジネスニーズに対応する方法をご確認ください

詳細はこちら

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、**akamai.com** および **akamai.com/blog** をご覧いただくか、**X**（旧 Twitter）と **LinkedIn** で Akamai Technologies をフォローしてください。公開日：2024 年 9 月。