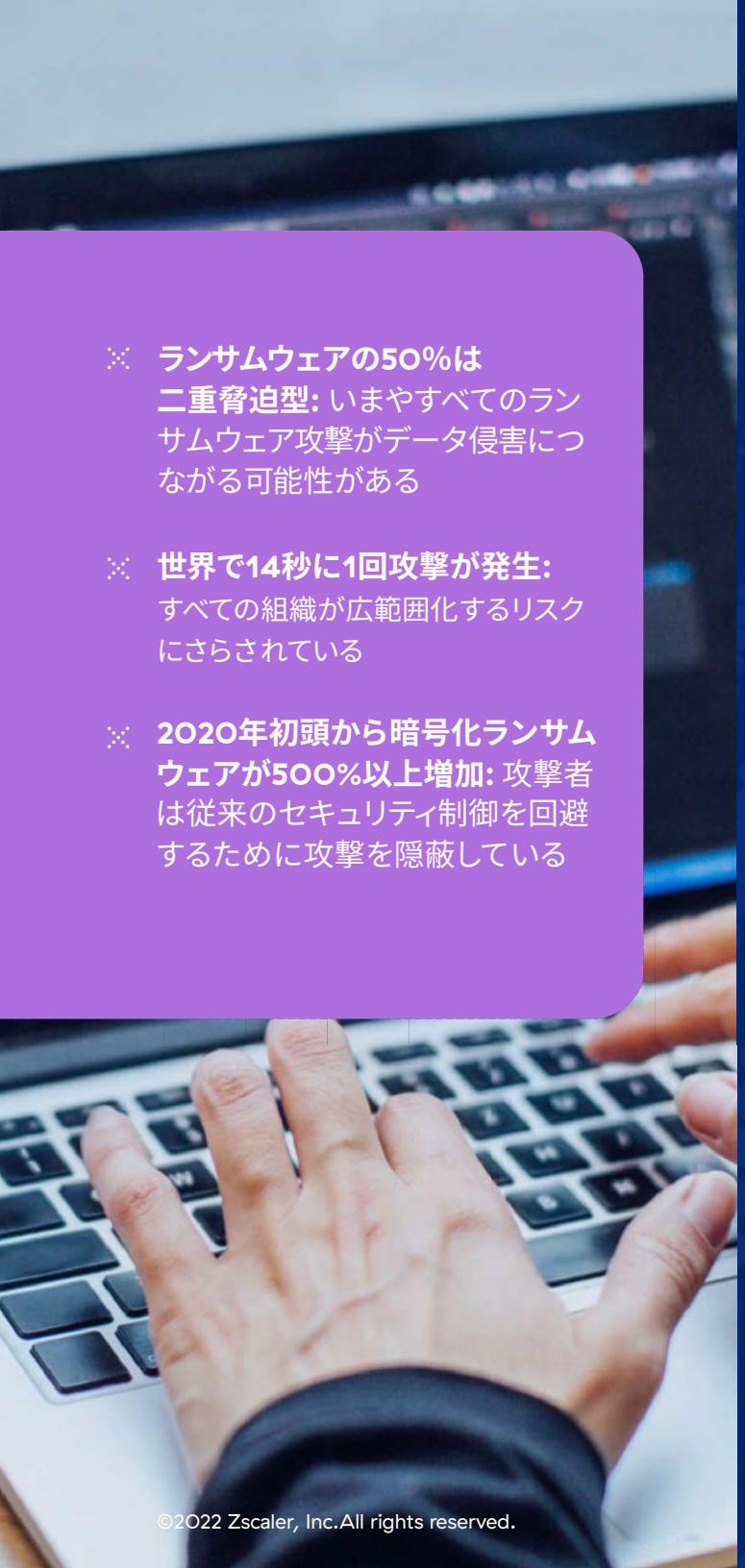
zscaler™

eBook

ゼロトラストアーキテクチャで ランサムウェアを阻止する10の方法



- **ランサムウェアの50%は二重脅迫型:** いまやすべてのランサムウェア攻撃がデータ侵害につながる可能性がある
- **世界で14秒に1回攻撃が発生:** すべての組織が広範囲化するリスクにさらされている
- **2020年初頭から暗号化ランサムウェアが500%以上増加:** 攻撃者は従来のセキュリティ制御を回避するために攻撃を隠蔽している

デジタルビジネスの最大の脅威はランサムウェア

ランサムウェアは何十年も前から存在していましたが、この2年間で爆発的に氾濫しました。このような攻撃は、かつては個人によって行われていましたが、現在ではネットワーク化されたアフィリエイトの集団がお互いに専門的なスキルやツールキットを売買することによって行っています。これまでの攻撃は焦点が定まらない一時面的なものでしたが、今では標的を絞った多層的な戦術が用いられているため防御が極めて難しく、要求する身代金も非常に高額となっています。**ランサムウェアは、2024年末までに420億ドルの損害をもたらすと予想されています。**[1]

最近のランサムウェアの傾向で最もインパクトがあるのは、データを暗号化するだけでなく、それを公開すると脅す二重脅迫攻撃の出現でしょう。現在、ランサムウェアの攻撃の約50%はデータを流出させる試みを含んでいます。

ランサムウェアの攻撃による被害を最小限に抑えるために組織が採用できる基本的な戦略があります。それが「ゼロトラスト」です。

ゼロトラストとは、セキュリティ侵害が既に発生しているという概念に基づくセキュリティアプローチです。アーキテクチャ、アクセスコントロールポリシー、モニタリングと認証の戦術を導入することで、攻撃による被害額と深刻さを軽減します。

ここでは、ゼロトラストがランサムウェアの防御に役立つ10の方法を紹介します。

[1] *Cybersecurity Ventures*社によると、「グローバル範囲におけるランサムウェアによる被害額は*2031*年までに*2650*億ドルを超える見通しです。」

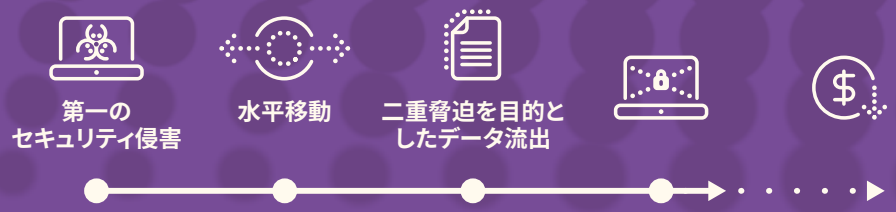
ランサムウェアの攻撃シーケンス

ランサムウェア攻撃が成功するためには、攻撃者が複数の目的を達成しなければなりません。最初にシステムに悪意のあるランサムウェアペイロードを感染させることでお客様の環境に入り込む必要があります。**つまり、攻撃を阻止するための最初のステップは、現在の脆弱性を減らして攻撃対象を最小化するとともに、トラフィックをブロック、制御、インスペクションを可能にする予防的管理になります。**

次に、攻撃者は偵察を実行して盗み出したり暗号化したりする価値の高い資産を探し出します。そのためには、ネットワーク内を水平移動可能である必要があります。**攻撃を阻止し、攻撃者が引き起こす被害を最小限に抑えるための第2のステップは、攻撃者の水平方向への展開能力を制限することです。**

二重脅迫攻撃では、攻撃者は成功の可能性と身代金を増やすため、データを盗み人質にします。**ランサムウェア攻撃から防御する第3のステップは、データ損失防止です。**

ゼロトラストがどのように攻撃チェーン全体の防御を可能にするかご説明しましょう。



#1

ゼロトラストアーキテクチャは、アプリを攻撃者から不可視にすることで攻撃対象領域を最小限に抑えます。

アプリケーション、ユーザー、デバイスのIDがインターネット上でオープンに見つかる状態は、最も貴重な情報資産を公開しているようなものです。これらの資産が可視化されてしまうと、攻撃者はパッチが適用されていないウェブサーバソフトウェアや総当たり攻撃で解読可能な弱いパスワードなどの脆弱性を容易に見つけて悪用することができ、即座にお客様の環境へ侵入するための強力な足がかりを得ることができます。

Zscaler Private Access™のようなソリューションを活用することで、ユーザーがアプリケーションに接続する代わりに、アプリケーションがユーザーに接続することが可能になります。 このようなインサイド・アウト型の接続では、すべてのアプリケーションがプライベートに保たれるため攻撃者から見えません。このアプローチを環境内のすべてのデバイスとアプリケーションに拡大することで、攻撃者が偵察活動を行うことはほぼ不可能になります。

#2

ゼロトラストアーキテクチャは、暗号化されたものを含むすべてのトラフィックを徹底的に検査します。

今日のインターネットトラフィックの大部分は暗号化技術を利用していますが、悪意のあるトラフィックも例外ではありません。現在、インターネットトラフィックの90%以上が暗号化されており、ランサムウェアの暗号化率は2020年初頭から500%以上上昇しています。セキュリティチームは、もはやSSL暗号化されたトラフィックはすべて安全だと短絡的に考えることができなくなりました。

しかし今日では暗号化の有無にかかわらず、すべてのトラフィックを検査することが強固な防御戦略の不可欠な要素となっています。次世代ファイアウォールやその他の境界ベースの防御に依存するアーキテクチャでは、もはや対応しきれない状況 です。最先端のオンプレミスセキュリティツールでさえ、生産性を低下させるパフォーマンスボトルネックをもたらすことなくSSL暗号化されたトラフィックを全て検査することは不可能です。SSL暗号化されたマルウェアの大規模な検知を目的に構築されたクラウド上の専用プロキシベースアーキテクチャが、すべてのトラフィックを保護し、死角を解消します。

#3

ゼロトラスト戦略には、未知のランサムウェアが危害を及ぼす前に検知するコントロール機能が含まれています。

カスタムメイドのマルウェアを利用するランサムウェア攻撃が増えています。こうした脅威を有効に防御するために、新たな脅威を検知してブロックする能力が必要です。クラウドネイティブのサンドボックスとAIを活用した検知機能によって、ユーザーに配信されたり実行が許可されたりする前にファイルを隔離して完全に分析することで、行動分析に基づいて未知のランサムウェアヴァリアントを発見できます。

Zscalerクラウドサンドボックスのようなソリューションでは、ユーザー、グループ、およびコンテンツタイプに基づいてポリシーを定義することで隔離措置をきめ細かくコントロールできます。このソリューションはZero Trust Exchange™の一部ですので、グローバルコミュニティから提供される判定ファイルをほぼリアルタイムで入手でき、マルウェアの検知精度を最大限に高めると同時にユーザーへの影響を最小化することができます。

#4

ゼロトラストは、アクセスコントロールポリシーを簡素化し、可視性や効率化を強化します。

マイクロセグメンテーションは、ゼロトラストの中核をなすコンセプトです。アプリケーションとリソースへのアクセスを制限することで、攻撃者が一か所を侵害しても他に損害を与えられないようにするものです。従来のネットワークベースのマイクロセグメンテーションアプローチでは、ファイアウォールはネットワークアドレスを調べることでルールを適用していました。同種アプローチでは、アプリケーションの移行やネットワークの進化に応じてポリシーを再定義し、更新する必要がありました。オンプレミスのデータセンターにおいてさえこうした方法は極めて困難でしたが、日々進化するクラウド環境では管理が手に負えなくなるぐらい複雑化し ています。

プロキシアーキテクチャは、マイクロセグメンテーションの実装に伴う複雑さを大幅に軽減するとともに、ワークロードにより強固な保護を提供します。ポリシーや許可はリソースIDに基 づいて管理されるため、ネットワークインフラストラクチャに依存せず、ネットワークのアーキテクチャがどれだけ動的に、またビジネス要件がどれだけ急速に変化しても、自動的に適応し ます。アドレスベースのルールを大量に用意するかわりに、IDベースのポリシーを少数用意するだけでセグメントの保護が可能となり、管理も簡素化します。

#5

ゼロトラストアーキテクチャは、すべての場所のユーザとデバイスを保護します。

2020年に発生した新型コロナウイルス感染症の影響であらゆる業界がリモートワークに切り替える必要性に迫られた際、多くの組織は仮想プライベートネットワーク（VPN）やリモートデスクトッププロトコル（RDP）を利用して、従業員が自宅から企業のネットワークやリソースに接続できる環境を用意しました。しかし残念なことに、ランサムウェア攻撃者はすぐさまこうした動きに目を付け、RDPやVPNを利用した新しい波状攻撃を繰り出しました。実際に、米国東部の燃料供給の半分近くを停止させたことで有名になったコロニアル・パイプライン社への攻撃では、VPNを悪用するものでした。

リモートユーザーのセキュリティを確保するゼロトラストベースのアプローチでは、ユーザーの所在地に関わらず、すべての接続が同じように保護されます。軽量のエンドポイントエージェントであるZscaler Client Connectorをすべてのリモートユーザーのデバイスに追加することで、Zscaler Zero Trust Exchangeで提供されるすべてのセキュリティ、ポリシー執行、そしてアクセスコントロールを利用できるようになります。さらに、Zscalerは世界中に150のデータセンターを設置しているため、ユーザーは常に最寄りのデータセンターを経由した高速接続を利用でき、VPNレイテンシーを回避できます。

#6

真のゼロトラストアーキテクチャでは、攻撃者がネットワーク上を水平移動することは不可能です。

悪意のあるトラフィックを企業ネットワークから排除するのに、従来のファイアウォールベースのネットワークセグメンテーションに依存し続けているセキュリティチームはいまだに数多く存在します。このような戦略は実装や管理が複雑であるだけでなく、結果的に社内リソースを危険にさらし続けてしまっています。攻撃者はアプリケーションやファイアウォール内への侵入に成功すると環境全体を水平移動することもできるため、他の方法 で保護された場合よりも多くのデータを暗号化して盗み出すことができます。

真のゼロトラストアプローチは、ネットワークを危険にさらすことなく、ユーザーが必要と するアプリケーションに1対1のセグメントで直接接続させます。セキュリティチームは、社内ネットワークやサブネットからのトラフィックを信頼するのではなく、プロキシアーキテク チャを使用してユーザを継続的に認証しながらアプリケーションに直接接続させることで、 今日の企業が直面する最大のデジタルリスクを排除できます。そして何より、プロキシは ユーザー、デバイス、アプリケーションのロケーションを問わず機能するため、オンプレミ スでもオフプレミスでも安全な接続を提供します。

#7

ゼロトラストアーキテクチャは、攻撃者によるワークロードの悪用を防止します。

ゼロトラストアーキテクチャでは、相互通信を試みているワークロードのIDに応じてセキュリティポリシーを執行します。これらのIDは常に検証されており、未認証のワークロードによる他者との通信はブロックされます。すなわち、悪意のあるリモートコマンドやコントロールサーバー、社内ホスト、ユーザー、アプリケーション、データとのやり取りを許しません。

Zscaler Zero Trust Exchangeのようなプラットフォームは、お客様のリソースにアクセスする際、発信元を問わずあらゆるトラフィックがすべての企業ポリシーを遵守することを自動的に保証します。対象リソースが社内、社外、あるいはサードパーティのSaaSであるかを問わず、ポリシーを完全に統一された形で適用します。このネットワークに対するマイクロセグメンテーションのアプローチは、複層ポリシーを適用するよりもはるかにシンプルかつより効果的です。

#8

ゼロトラストには、攻撃者を撃退する積極的な戦略が含まれています。

最近のランサムウェア攻撃者は、第一段階の防止策を迂回する能力を持った手ごわい相手です。したがって、ゼロトラストの重要な一側面は被害が発生する前に攻撃を発見し隔離する戦略を採用することです。偽装機能を統合した世界唯一のゼロトラストプラットフォームであるZscaler Deception™は高度な偽装戦術を用いて、攻撃者の戦略がどれほど高度でターゲットに特化したものであっても、おびき寄せ、検知した上で遮断します。

このプロアクティブな防御アプローチでは、偽のエンドポイント、ディレクトリ、データベース、ファイル、ユーザパスなどのデコイ（おとり）をお客様のIT環境に配置します。これらのデコイは価値の高い生産資産を模していますが、実際のユーザには非表示になっています。それらの目的は、敵対者が接触したときにお客様のセキュリティチームに警告することです。デコイには正規のトラフィックがないため警告の精度が極めて高く、他の検知システムのノイズを上回る脅威や侵害の確かな証拠を提供します。これによってセキュリティチームが優位に 立ち、敵対者のプレイブックを混乱させ被害を軽減できます。

#9

ゼロトラストアーキテクチャは、データ損失を防ぐ総合的な保護を提供します。

二重脅迫ランサムウェアの攻撃戦略がますます一般化していることから、すべてのランサムウェア攻撃をデータ侵害とみなす必要があります。お客様の機密データの流出や公開を防ぐ対策は、ランサムウェア攻撃に伴う最も深刻な被害の発生を低減する上で大きな役割を果たします。

クラウドアクセスセキュリティブローカー（CASB）ソリューションを使用すると、クラウドアプリケーションに対してきめ細かな制御を適用でき、SaaSプラットフォーム内の保存データを保護し、偶発的なオーバーシェアリングや悪意ある侵入を防止できます。お客様のクラウドアプリケーションの可視性を向上し、脆弱性や設定上の不備、そして「シャドーIT」と呼ばれる未許可のクラウドアプリの使用を容易に発見できることも大きなメリットです。情報漏洩防止（DLP）機能を使えばデータ流出を自動的にブロックすることが可能となり、二重脅迫による脅威を抑制できます。

#10

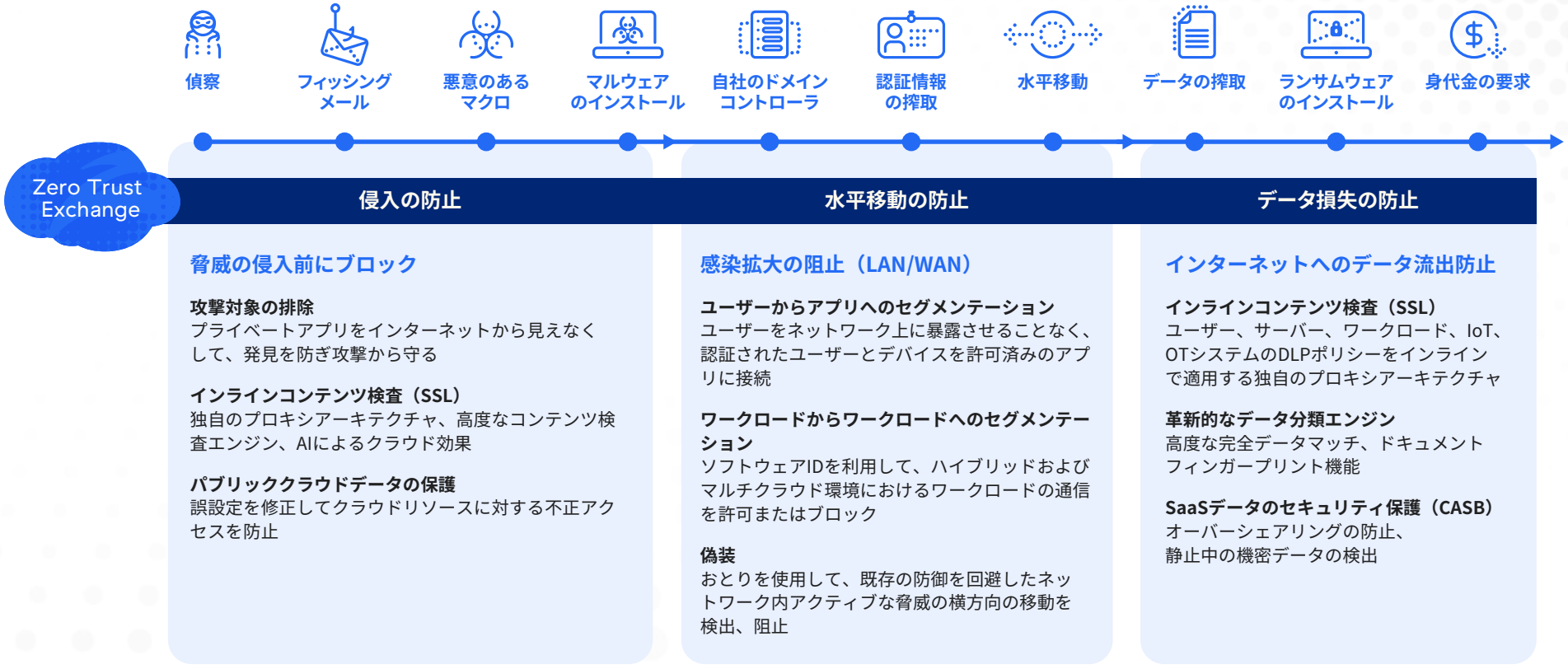
ゼロトラストアーキテクチャは、すべてのアウトバウンドトラフィックに完全なインライン検査を実施し、データ盗取を阻止します。

悪意ある攻撃者がSSL暗号化された受信トラフィックにマルウェアを隠せば、同様に暗号化戦略を悪用して企業の重要な機密データを流出させているという事実を隠蔽することができます。SSL暗号化されたトラフィックをインスペクションする能力は、データ損失を防ぎ、ゼロデイのデータ流出の脆弱性を識別するために不可欠です。

Zscaler Zero Trust Exchangeのようなゼロトラストアーキテクチャベースのソリューションは、お客様の環境内のすべての接続がインバウンドかアウトバウンドかを問わず個別に検証され、保護されることを保証します。クラウドネイティブのプロキシアーキテクチャでは、パフォーマンスに影響を与えたり過剰なコストをかけたりすることなく、完全な大規模のSSLインスペクションの実行が可能です。これにより、ランサムウェアの攻撃者が壊滅的な二重脅迫攻撃を行うために悪用してきたセキュリティギャップが排除されます。

ランサムウェアからの保護にゼロトラストを活用する

Zscaler Zero Trust Exchangeは、サイバー犯罪者が攻撃を成功させるシーケンスの全段階を対象に最も総合的な防御を提供します。
Zscalerが提供するゼロトラストを活用した保護の詳細は、こちらをご覧ください。



最新の攻撃から身を守るには
最新のセキュリティが必要です

業界で最も包括的なランサムウェア対策を活用して、
ビジネスを保護してください。

詳細はこちら

zscaler™ | Experience your world, secured.™

Zscalerについて
Zscaler（NASDAQ: ZS）は、デジタルトランスフォーメーションを加速させ、俊敏性、効率性、耐障害性、安全性の向上を可能にします。Zscaler Zero Trust Exchangeは、あらゆる場所のユーザー、デバイス、アプリケーションを安全に接続することで、サイバー攻撃やデーター損失から何千ものお客様を保護しています。SASEベースのゼロトラストエクスチェンジは、世界中の150以上のデーターセンターに分散する、世界最大のインラインクラウドセキュリティプラットフォームです。詳細は、**zscaler.jp**をご覧いただくか、Twitter（**@zscaler**）をフォローしてください。

03-4243-6320 Zscaler, Inc.(本社) – 120 Holger Way – San Jose, CA 95134 zscaler.jp