zscaler™

eBook

CISO向け 脅威対策ガイド

最も効果的なファイルベースの
脅威対策ソリューションを選択するために

目次

eBook

脅威の最新状況を踏まえたセキュリティの再考

デジタル環境には対応しきれない境界のみのセキュリティ

ハイブリッド ワークやクラウドホスト型のアプリケーションへの移行に伴い、企業のリソースにアクセスする手段が変化し始めています。多くのユーザーがリモート ワークや外出先での生産性を維持するために、管理対象ではないデバイスから公共 Wi-Fi などの安全性の低いネットワークを使用しています。インターネットが新たな企業ネットワークとなりつつあるいま、これまで 1 つだった境界線は数千に拡大し、従来の「城と堀」型のセキュリティアプローチでは、ユーザー、アプリケーション、データを十分に保護できなくなってきています。境界ベースの制御だけに依存し続けると、インターネットへの直接アクセスと使いやすさを優先するあまり、ネットワーク中心の防御が回避されてしまうため、大きなリスクにつながります。

従来のセキュリティ制御を簡単に回避する次世代のサイバー攻撃に対抗するには、境界ではなく、ユーザー、ワークロード、OT/IoT の保護に焦点をあて、セキュリティそのものをユーザーに近づける必要があります。

急速に進むクラウドへの移行を悪用する攻撃者

セキュリティ部門は難題に直面しながらも、従来のセキュリティ制御を現代のモバイルファースト、クラウドファーストの環境に適応させるために最善を尽くしていますが、ここで生じた「溝」こそが、攻撃側を有利な状況に導いています。組織が複数あるネットワーク エッジの保護に奮闘する一方で、マルウェアに対する防御は不十分であることが、Zscaler ThreatLabz の調査結果からも明らかになっています。

- ランサムウェア攻撃は**前年比で 80% 増加** [1]
- 多岐にわたる脅迫手口が出現し、二重脅迫型ランサムウェアは**117% 増加** [1]
- 2021 年のフィッシング攻撃は 2020 年比で **29%増加** [2]
- **85%** の組織が 2021 年にサイバー攻撃の被害に [3]
- 2021 年にランサムウェア攻撃の被害に遭った **63%** が身代金を支払い、この事実がサイバー攻撃の拡大を助長 [3]

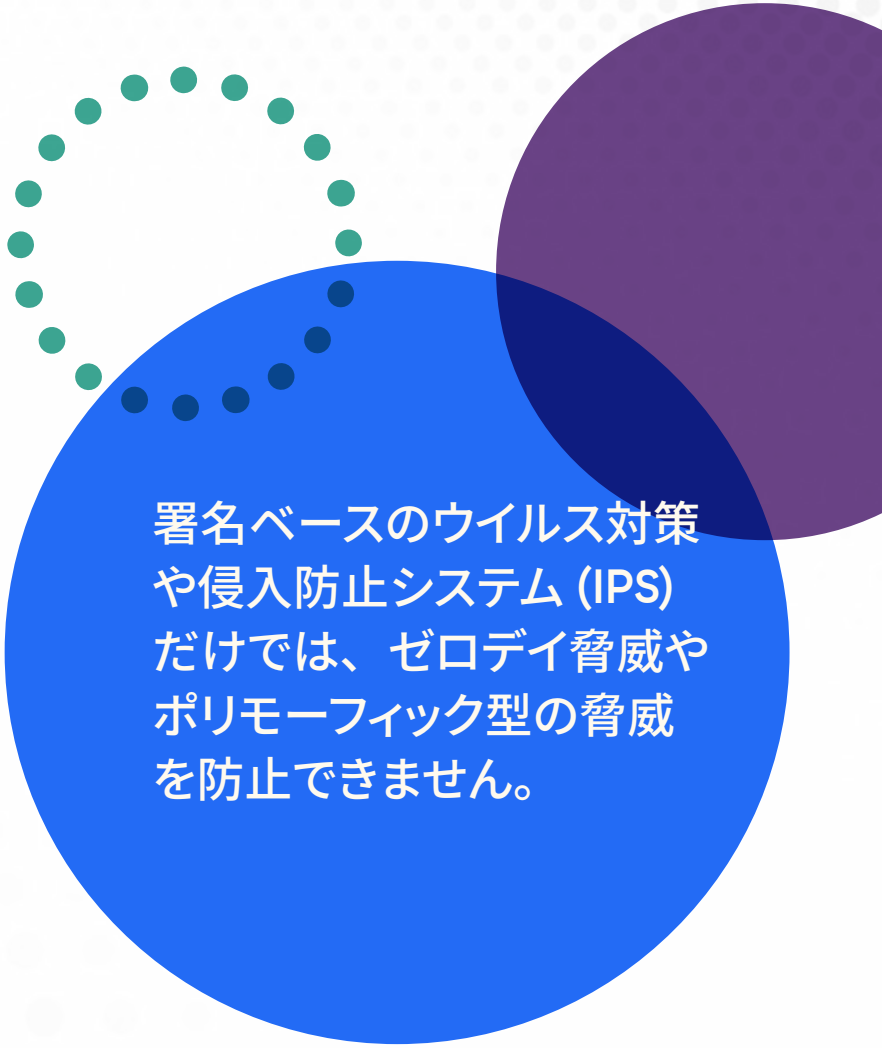
1. https://www.zscaler.jp/resources/industry-reports/2022-threatlabz-ransomware-report.pdf
2. https://www.zscaler.jp/resources/industry-reports/2022-threatlabz-phishing-report.pdf
3. https://cyber-edge.com/cyberthreat-defense-report-2022/

進化が求められるゼロデイマルウェア対策

攻撃者には**スピード**と**拡散**という 2 つの強みがあります。マルウェアの開発者は、防御側が脅威を定義するよりも速く脅威を作成して拡散し、検出を回避するために変形させます。

悪意のある添付ファイルやリンクを使ったフィッシングは、現在も最も一般的な手口です。脅威は暗号化されたトラフィックに潜んでいるため、ファイル転送プロトコルや SSL/TLS を含むすべての Web トラフィックと非 Web トラフィックを検査しない限り、マルウェアがネットワークに侵入したことに気付くことはできません。その結果、攻撃者に機密データが盗み出されたり身代金が要求されたりするのです。

サンドボックスはセキュリティ スタックの重要な機能であり、悪意のあるファイルやコードの実行を防止する手段です。セキュリティの最後の砦としての役割を果たすと同時に、未知の脅威を調査するうえでの最初の検出ポイントとしても機能します。残念ながら、従来のサンドボックス アプライアンスはアウトオブバンド型であるため、SSL 復号や検査のためにはデバイスを追加する必要があります。そして、マルウェアがユーザーまたはデバイスを通過した後に保護が適用されるため、ゼロトラストは実現できません。



クラウド サンドボックスの要件

これまで、攻撃者はクラウド環境で変化していくアーキテクチャーを不正利用することで優位に立ってきました。

ゼロ号患者からの感染を防ぎ、高度な標的型攻撃によるネットワークへのアクセスを阻止するためには、適切なクラウド サンドボックスを選択することが重要です。

次のセクションでは、クラウド サンドボックスを選択する際に考慮すべき具体的な要件を解説しています。

復号と大規模な検査

プライベートな通信や機密情報を安全に保護する暗号化は、その効果の高さからセキュリティのトレンドになりましたが、残念ながら、サイバー犯罪者は悪意のあるペイロードを隠すために暗号化されたトラフィックを利用しています。

新しい手法である、トラフィックの復号と検査はコンピューティング集約型のプロセスとなります。パススルー アーキテクチャーを備えた従来のサンドボックスでは、検査されていないトラフィックの中にマルウェアが紛れ込む場合があります。SSL インスペクション専用の追加デバイスで対応することもできますが、他のアプライアンスと同様に拡張性に欠けるため、コストのかかるデバイスが乱立するだけで、ゼロ号患者の感染によるネットワークへの二次感染を阻止できません。

最新のサンドボックス ソリューションを評価する際は、レイテンシーのない無制限の復号と検査をインラインで提供できるベンダーを選ぶことが重要です。

HTTPS を介した脅威は前年比で 314% 以上増加し、その増加率は 2 年連続で 250% を超える結果となっています。[4]

購入時のチェックリスト：

- ☐ SSL トラフィックの復号に追加のハードウェアや仮想マシン (VM) のインストールを必要としない
- ☐ レイテンシーや容量制限なしで以下の種類のファイルを検査、分析できる

EXE	DOC(X)	TAR
DLL	XLX(X)	TGZ
SCR	PPT(X)	GTAR
OCX	APK	RTF
SYS	ZIP	PS1
CLASS	RAR	HTA
JAR	7Z	VBS
PDF	BZ	ZIP ファイル内のスクリプト ファイル
SWF	BZ2	

4. *https://info.zscaler.com/resources-whitepaper-threatlabz-the-state-of-encrypted-attacks-jp*

購入時のチェックリスト：

- ☐ 企業ネットワークの内外を問わず、すべてのユーザーにすぐにポリシーを施行し、同一の保護を提供できる
- ☐ 不審な送信元からのファイルに対する高度な隔離ルールと機能を搭載している
- ☐ ポリシーを一元的に管理できる
- ☐ グレイウェアやアドウェアのファイルをきめ細かく制御できる

一元化されたポリシー管理とルール

クラウド配信型の一元化されたポリシー管理とルールによって、ルールの管理ミスがなくなるだけでなく、各ゲートウェイのサンドボックスを手動で構成する必要もなくなります。**NIST800-207** で概説されているゼロトラストの原則に則した、動的かつ適応性のあるポリシーを備えたソリューションが求められます。ゼロトラストでは、ユーザーの役割や場所、デバイス態勢、リクエストされたデータなどのコンテキストに基づいてアクセスとセキュリティポリシーが確立されるため、攻撃対象領域を最小限に抑えることができます。クラウド型のソリューションには、脅威が特定された時点で、組織内のすべてのユーザーを対象に脅威をブロックするというメリットもあるため、ファイルの事後検証 (例：帯域外の検査や事象発生後の保護の適用など) が不要となり、より同期性の高いセキュリティが実現します。

きめ細かい制御により、組織のリスク許容度やパフォーマンスの期待値に合わせてポリシーを調整することができます。

リスク許容度とパフォーマンスの期待値に合わせたポリシー

クラウド サンドボックスのソリューションは、リスクを制御しながら組織固有のニーズに合ったポリシーを施行する必要があります。最初に組織の状況を確認します。

- **悪意のあるファイルに対する許容度が低い場合：**リスクの回避を重視する組織では、未知または不審なファイルに対して、初回アクションに「隔離」を選択できます。
- **ファイルの隔離に対する許容度が低い場合：**リスク許容度が高く、レイテンシーや中断の回避を重視する組織では、初回アクションに「許可とスキャン」を選択できます。さらに保護を強化するには、ファイルを画像としてレンダリングし、データ漏洩やアクティブな脅威の配信を回避するためにクラウド ブラウザー分離機能との統合を検討します。

組織が抱えるニーズがどのようなものであろうと、ポリシーは単一のプラットフォームからすべてのユーザー、グループ、部門、場所、場所グループに対して簡単に施行できる必要があります。

効率的な分析と脅威インテリジェンス

攻撃者は以前成功した攻撃を再度利用することが多いため、セキュリティ関連コミュニティと保護情報を共有して、脅威を速やかに阻止することが重要です。クラウド サンドボックスはテレメトリー データを取得し、新たに特定された脅威から得たインサイトを脅威フィードやセキュリティ関連コミュニティと共有する重要な役割を果たします。

AI を活用したマルウェア対策エンジン

クラウド配信のサンドボックスは、計算負荷の高い AI/ML モデルを管理して、より優れた保護機能を提供します。

無害なファイルは再スキャンの対象外にし、高度な AI/ML を使用して未知の脅威や不審な脅威をインラインで効率的に特定、隔離、防止するサンドボックスが求められます。これには以下が含まれます。

- **迅速なファイル判定：**無害なファイルは即座にルーティングし、不審なファイルや未知のファイルを分析することで、手作業の負荷を軽減します。
- **ゼロデイ対策：**追加作業なしで未知の脅威を隔離することで、環境内におけるゼロデイ脅威の拡大を防止します。

脅威インテリジェンスを活用した SOC ワークフロー

アナリストは 1 つの脅威の調査に何時間も費やすケースがあります。悪意のあるペイロードの行動に関するインサイトや脅威インテリジェンスを共有することで、このような負担を軽減し、調査と対応をスピードアップさせるクラウド サンドボックスが求められます。脅威フィードが既存のセキュリティ ツールと統合できることも重要です。具体的には、報告された URL の最新のコンテキスト、抽出された侵害指標 (IoC)、MITRE ATT&CK® などのサイバーセキュリティ フレームワークに沿った戦術、技術、手順 (TTP) が含まれます。

購入時のチェックリスト：

- ☐ 分析プロセスと緊密に統合された ML/AI 機能がある
- ☐ ML/AI を活用して悪質な可能性があるファイルを保持して分析し、迅速に判定する AI ベースの隔離機能がある
- ☐ 場所を問わず、ユーザーやネットワーク間で共有される日常的な脅威にプロアクティブに対応できる
- ☐ プラットフォームを通じてフォレンジック データやファイル判定を共有する機能がある
- ☐ 脅威フィードを既存のセキュリティ ツールと統合できる

脅威スコアを提供するだけでなく、使用される回避技術を概説するサンドボックスを選択してください。この技術の例を以下に示します。

- サンドボックスでの検出を回避するためにコードの実行を遅らせる
- ネットワークを通過するトラフィックをキャプチャーして表示する
- リモート接続を許可するためにポートを開放する
- より価値の高いターゲットを見つけるために水平移動を試みる
- リモート コントロールを許可しようとする

レポート

レポート機能のあるセキュリティ ソリューションは、レポートの実用性が高いほど有益です。クラウド サンドボックスのレポートには、以下が求められます。

- 悪意のある攻撃のライフサイクル全体が含まれる
- シンプルな操作性で簡単に使える
- 概要を簡単に把握できる
- アプリケーション プログラミング インターフェイス (API) を介して利用でき、既存のログと関連付けられる
- コンプライアンス レポートもサポートする大規模なプラットフォームの一部である

MITRE ATT&CK フレームワークを活用して SOC を強化

レポート機能を評価する際は、**MITRE ATT&CK のフレームワーク**にマッピングできるサンドボックス インテリジェンスを検討します。この機能により、SOC チームは提供された分析情報を適用してセキュリティ スタックの他の部分で戦術的な防御を構築できます。このように、サンドボックスはセキュリティ運用ワークフローにおいて欠かすことができません。

フレームワークの成熟度に応じて、レポート機能は以下のような目的で使用できます。

- 提供された分類情報を使用してラベル付けの負担を軽減する
- エンドポイントでの検知と対応 (EDR) ソリューションを回避する可能性のあるステルス技術を確認する
- 他の各種制御と比較対照する
- 闇雲にすべての戦術や手法を阻止するのではなく、自社をターゲットにしている最も一般的な TTP に焦点をあてる
- リバース エンジニアリング レポートを作成する

購入前に確認すべき項目

ここでは、購入前に確認が必要な項目とその理由を紹介します。

- **そのソリューションは、場所に関係なく、すべてのユーザーとそのデバイスに対応していますか?**
  ユーザーは、外出先や自分のデバイスだけでなく、セキュリティで保護されていないネットワークから企業のリソースにアクセスすることがあります。業務に必要なすべてのデバイスを保護することが重要です。[5]

- **そのソリューションはインラインで動作しますか?テスト アクセス ポイント (TAP) モードで動作しますか?**インラインで動作するソリューションは、ファイアウォールなどのサードパーティーのデバイスを介して新しいルールを作成することなく、脅威を特定して直接ブロックできます。

- **そのサンドボックスは、HTTP、HTTPS、FTP、FTP over HTTP のすべてのプロトコルでトラフィックを検査しますか?また、制限はありますか?**
  ステルス性のマルウェアを検知するには、トラフィックの検査が不可欠です。クラウド配信のサンドボックスはレイテンシーなしですべてのトラフィックを検査します。

- **ゼロトラスト要件を含む関連法規に準拠していますか?**
  コンプライアンス規制によっては、サンドボックスの処理方法やファイルの保持およびプライバシーに関する厳しい要件が課せられる場合があります。こういった要件を満たすためには、メモリー内でのみ動作し、分析時に識別可能な情報だけを抽出するソリューションが有効です。また、そのソリューションが NIST 800-207 グローバル標準で規定されているゼロトラストの原則に準拠し、その原則を攻撃対象領域を減らしてデータを保護するための指針として使用しているかどうかも重要です。

- **そのサンドボックスは他のセキュリティ モジュールと連携していますか?**
  1 つの製品で高度な標的型攻撃 (APT) から完全に保護できるわけではなく、脅威の防止、軽減、検出、対応といった多層アプローチが必要になります。サンドボックスは重要な層の 1 つであるため、他のソリューションやモジュールと問題なく連携できる必要があります。

- **そのソリューションはベンダーが提供するサンドボックスまたは EDR サンドボックスを補完しますか?**
  組織に壊滅的なダメージを与える可能性のあるマルウェアのキルチェーンを断絶するために、補完的なソリューションと多層保護が真の多層防御戦略には必要です。これは、エコシステム内のどこかでエラーが発生した場合も、別の層で対応できることを意味します。攻撃を阻止するためにエンドポイント、ネットワーク、およびポリシー制御が連携して機能する必要があります。

5. https://image-us.samsung.com/SamsungUS/samsungbusiness/short-form/maximizing-mobile-value-2022/Maximizing_Mobile_Value_2022-Final.pdf

Zscaler Cloud Sandbox と高度な脅威対策

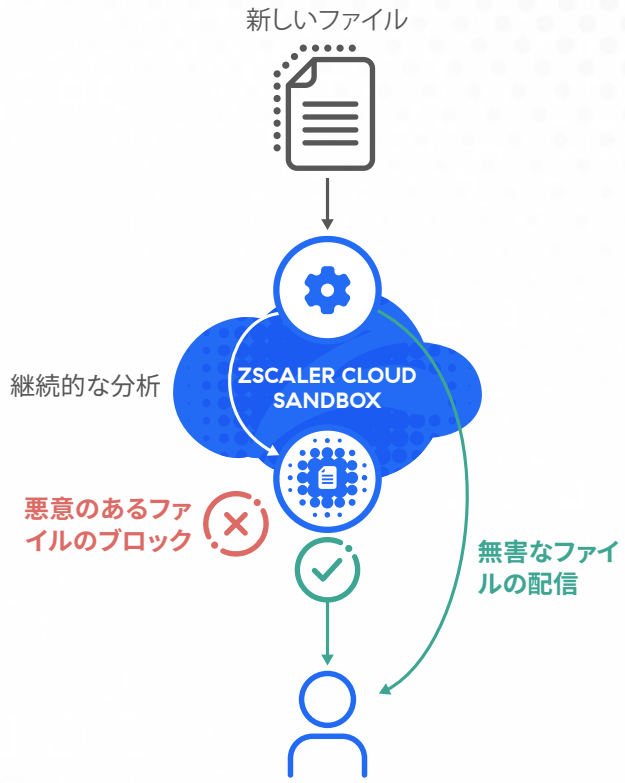
真のクラウドネイティブなインライン型サンドボックスとは

組織が拡大する攻撃対象領域に立ち向かう一方で、攻撃側が従来のセキュリティ スタックに生じた「溝」を悪用している現状は、真のクラウドネイティブなインライン型サンドボックスを導入する絶好のタイミングと言えます。Zscaler Cloud Sandbox は、最新の脅威を捕捉して阻止することを目的として構築されており、すべての場所、すべてのユーザーにゼロデイ マルウェア対策を提供します。

クラウドネイティブでプロキシーベースのアーキテクチャー上に構築された Zscaler Cloud Sandbox は、未知の脅威や不審なファイルをインラインで自動的に検出、防止して、効果的に隔離する、世界初の AI 活用型マルウェア対策エンジンです。SSL/TLS を含む Web およびファイル転送プロトコル (FTP) に対する無制限でレイテンシーのない検査により、クラウド サンドボックスは詳細かつ動的な分析をリアルタイムで実行します。そして、未知のファイルが悪意のあるファイルのダウンロードとしてユーザーの元に届かないようにします。

AIを活用した検疫による未知のマルウェアの阻止

無害なファイルの即時配信、ゼロ号患者の防御、
きめ細かなポリシー制御でのインライン保護



複雑性とコストの削減

- 導入が簡単で、ハードウェアやソフトウェアの管理が不要
- 必要のないポイント製品を除去
- MPLS または VPN を介したインターネット トラフィックのバックホールを排除

すべてのユーザーと場所に対する迅速な保護の適用

- 単一かつ一元化されたコンソールでグローバル ポリシーを定義
- ポリシー変更があった際は速やかに施行
- 脅威が特定された時点で、組織内のすべてのユーザーを対象に脅威をブロック

隠れた脅威の検知

- AI 活用型の隔離で既知および新たな脅威からのゼロ号患者による感染を阻止
- 分析のためにファイルをアップロード (ファイル チェック ポータル)

統合プラットフォームサービス

- ウイルス対策、ハッシュ ブロックリスト、YARA マルウェア分類ルール、自動 JA3 フィンガープリント検出、ML/AI モデルを使用して、既知の悪質な脅威をすべて事前にフィルタリング
- コレクティブ インテリジェンス フレームワーク (CIF) のフィードにより、Zscaler の顧客全体の数十億に上るトランザクションを活用した独自の脅威フィードに加えて、60 以上の脅威フィードとも統合可能
- クラウド サンドボックスを EDR ソリューションで階層化することで、セキュリティ効果を高め、初期アクセス、実行、標的型攻撃を低減

ESG 経済検証の研究で、Zscaler Zero Trust Exchange はセキュリティ アプライアンスを 90% 削減することがわかっています。[6]

- 静的、動的、二次的分析 (コード分析や二次的ペイロード分析を含む)
- 無制限でレイテンシーのない SSL インスペクション
- インバウンドおよびアウトバウンド トラフィックの保護
- ユーザー、発生元、回避戦術などを含む豊富なフォレンジックでセキュリティの調査と対応を強化

Zscaler Cloud Sandbox は、Zscaler Internet Access に完全に統合された機能であり、Zscaler Zero Trust Exchange の一部でもあります。

詳細はこちら：
zscaler.jp/technology/cloud-sandbox

6. https://info.zscaler.com/resources-industry-report-esg-economic-validation-jp

zscaler™ | Experience your world, secured.™

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SASE ベースの Zero Trust Exchange は、世界最大のインライン型クラウド 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 で **@zscaler** をフォローしてください。

+1 408.533.0288

Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134

zscaler.jp