Digital Security
Progress. Protected.

ランサムウェア対策ガイド

www.eset.com/jp

はじめに

情報セキュリティ業界は、ランサムウェアが企業にとって最大のサイバー脅威になる可能性について以前から警告してきました。しかし、数年前までは身代金の要求額が低く、マルウェアの拡散方法もそれほど効果的ではなかったことから、多くの組織はこれらの警告に注意を払わず、多額の身代金を支払う結果を招きました。

ランサムウェアによる攻撃が数え切れないほど報道される中で、対策を講じないという選択は残されておりません。多くの中小企業（SMB）は、サイバー脅威への備えが不十分であることも少なくありません。企業にとっての脅威は数時間のダウンタイムを引き起こし収益機会の損失をもたらす分散型サービス妨害（DDoS）攻撃から、ランサムウェアなどのマルウェア攻撃まで多岐にわたっており、攻撃による影響を受けた場合、最終的に企業が倒産する恐れもあります。

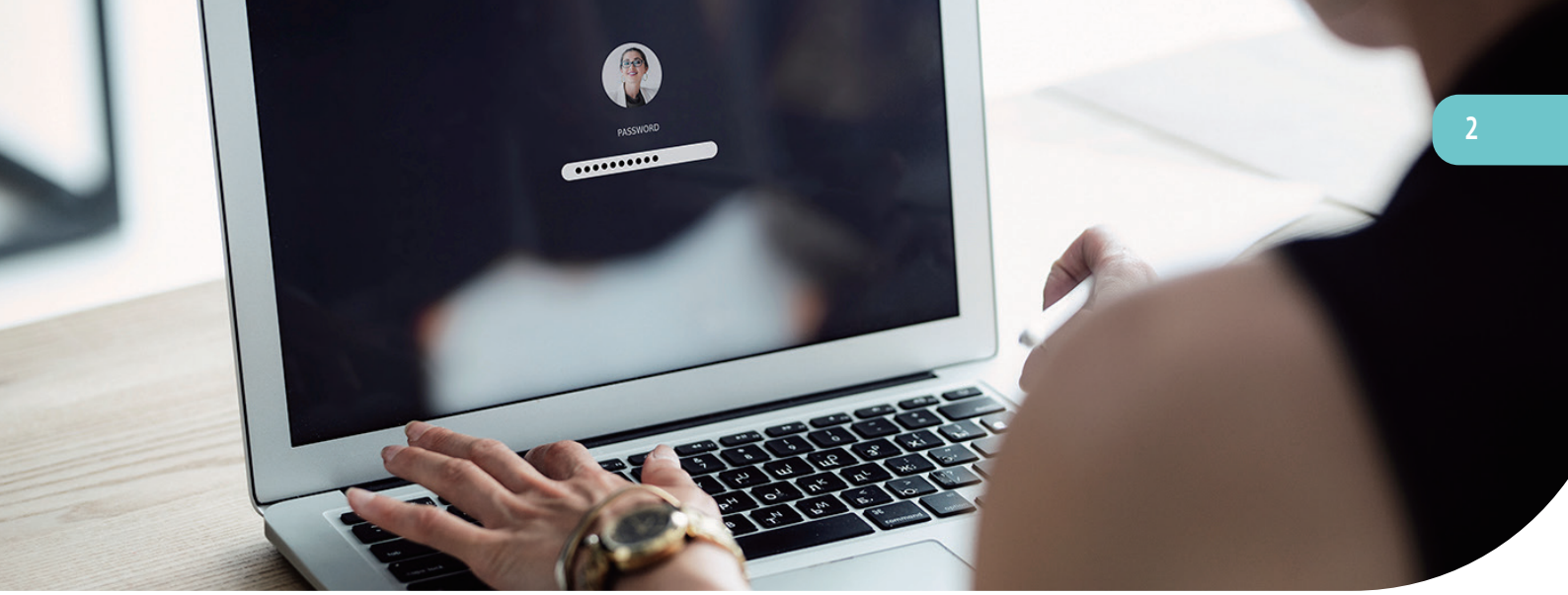
また、近年の仮想通貨の普及により、ランサムウェアの攻撃者は簡単に身代金を受け取ることができるようになりました。サイバー犯罪者は、ビットコインや追跡が困難な仮想通貨で身代金を支払うよう要求することが多くなっています。

本ガイドでは、特に中小企業（SMB）が自社をまもるためにできることをまとめています。

「ランサムウェアインシデントが数え切れないほど報道される中で、対策を講じないという選択は残されておりません。」

01

ランサムウェアとは？



ランサムウェア

ランサムウェア攻撃は、組織が自社のデータにアクセスできない状況を作り出して恐喝する試みです。ランサムウェアはマルウェアの一種であり、コンピュータウイルスやワームなど、さまざまな形態の悪意のあるコードの総称です。

このようなタイプの悪意のあるソフトウェアは、攻撃した対象を恐喝するために使用されます。デバイスへの攻撃が成功すると、マルウェアは画面をブロックしたり、ディスクに保存されているデータを暗号化したりして、被害者に要求する身代金と支払方法の詳細が表示されます。

会社が直面する最も深刻なサイバー脅威の1つがランサムウェアである理由とは？

ここ数年、このようなマルウェアを生み出しているサイバー犯罪者は、標的をさらに限定し、各標的に合わせたアプローチを実行しています。

サイバー犯罪者は、他のランサムウェア開発者によって開発されたランサムウェア技術に使用料を支払い攻撃に利用し、標的から利益を得ています。これは、RaaS（Ransomware as a Service：サービスとしてのランサムウェア）と呼ばれるビジネスモデルであり、ランサムウェア開発者のアフィリエイトを作り出しています。

Ponemon Institute の最新レポートによると、企業に対するランサムウェアの攻撃で最も多かった手法はフィッシングとソーシャルエンジニアリングであり、2 位はなりすましサイト、3 位は悪意のある広告が続いています。

レポートを読む

02

中小企業（SMB）がランサムウェアの標的となっている理由

大企業は中小企業よりも実利の多い標的と見なされる場合もありますが、中小企業はサイバー犯罪者にとって貴重な標的になりつつあります。

往々にして中小企業は、セキュリティ対策のための十分な資金やリソースを持っていないことから、サイバー犯罪者にとっては個人ユーザーよりも貴重な標的であり、大企業よりも攻略しやすい脆弱な存在です。これらの条件が組み合わさっていることから、中小企業は攻撃者にとって「格好の餌食」になっています。

Ponemon　Instituteのレポートでは、中小企業が直面している最大の課題は、サイバーリスク、攻撃、脆弱性に対処するための人材の不足であり、2番目は、予算が限られていることが明らかになりました。また、3番目の課題として、サイバー攻撃から自社を守る方法についての理解が不足していることも挙げられています。

03

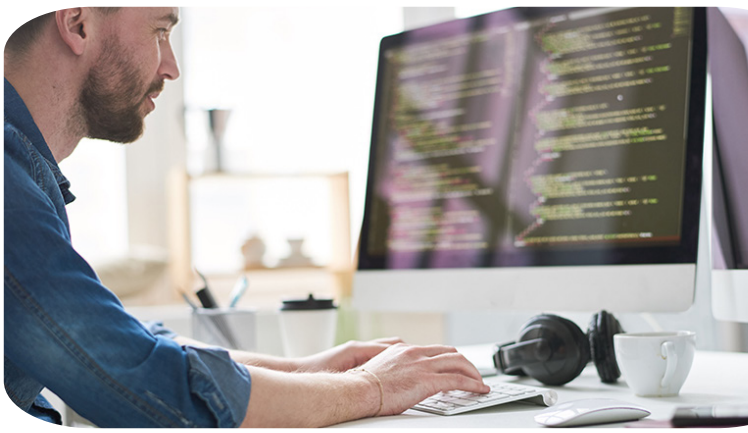
ランサムウェア攻撃を受けた場合のコスト

Dattoのレポートによると、米国でサイバー犯罪者が要求する身代金の平均額は約5,900ドルです。しかし、これは企業が最終的に負担するコストではありません。ダウンタイムによるコストは2019年に要求された身代金の23倍の141,000ドルであり、2018年から2019年にかけて200％以上増加しています。

ランサムウェア攻撃における身代金以外のコストとは？

攻撃の発見、調査、封じ込め、復旧、風評被害、精神的なダメージなど、ランサムウェア攻撃における身代金以外のコストは多岐にわたります。また、失われた情報のコストも計算に入れなければなりません。

ダウンタイムをできる限り最小限に留め、機密ファイルへのアクセスを復元するために、身代金を支払うことを選択する企業もあるかもしれませんが、データを復旧できる保証はありません。ランサムウェアを操るサイバー犯罪者は身代金を増やし続けるかもしれません。また、身代金を支払ったとしても、すべてのデータを復旧できるとは限らず、被害が継続する可能性があります。



04

ランサムウェア攻撃から企業を保護する方法

自社で取り組むことができる4つのステップ

1. 3-2-1のルールに従ってデータをバックアップする

保護するデータについては**3**つのコピーを作成します。

少なくとも**2**種類のストレージメディアにコピーを保存します。プライマリデータを内蔵のハードディスクに保存している場合、バックアップコピーは外付けハードディスク、NASデバイス、またはクラウドに保存します。

最後のコピーは、オフサイトまたはクラウドに保存する必要があります。バックアップコピーの**1**つをオフサイトに保存すればデータのセキュリティを強化できます。また、もう1つのコピーをオンサイトに保存すれば、障害発生時にも迅速かつ簡単にデータを復旧ができます。

2. クラウドサンドボックス機能がプロアクティブな保護を実現

予防は治療に勝るという格言はセキュリティにも通ずるものです。クラウドサンドボックスは、隔離された強力なテスト環境を提供します。この環境で攻撃が疑われるプログラムを実行し、その挙動を自動的に観察、分析、レポートします。

クラウドサンドボックス機能は、社内ネットワークの外部にテスト環境を置くことで、本番環境における実行を防止するプロアクティブな保護を実現します。これにより、ランサムウェアなどのゼロデイ脅威や新しいマルウェアの亜種に対する保護レイヤーを追加してセキュリティを強化できます。

クラウドサンドボックスは、オンプレミスのサンドボックスにはない、以下のようないくつもの利点を提供します。

1. 社内と社外のスタッフの保護
クラウドサンドボックスは従業員が社内にいても社外にいても利用できます。クラウドコンピューティングリソースを利用するESET　LiveGuard Advancedは、すべてのプロセスを5分程度で完了します。また、悪意のある脅威が検出されると、会社全体が自動的に保護されます。

2. メンテナンスコストの削減
オンプレミスのサンドボックスは定期的にメンテナンスおよびアップデートする必要があります。クラウドサンドボックスでは、ITリソースを解放でき、別の重要な業務に割り当てることが可能ます。

3. ビジネスに合わせた拡張性
ビジネスが拡大し、多くのデバイスが使用される場合でも、ランサムウェアやゼロデイ攻撃からすべてのデバイスを保護でき簡単に利用できるソリューションとして、そのニーズに対応できます。

3. データの暗号化

また、データを外部に流出させて脅迫する、二重脅迫型ランサムウェア攻撃と呼ばれる攻撃も増加しています。通常、サイバー犯罪者は、機密データのコピーを自分の環境に取り込んでから、被害者のサーバー上にあるデータを暗号化して、アクセスをブロックします。二重脅迫型ランサムウェア攻撃は、身代金が支払われない場合、窃取したデータを暴露し、販売やオークションにかけるという脅威にさらします。

暗号化だけではランサムウェアの攻撃を防ぐことはできませんが、機密データの外部への流出を防ぐために暗号化は非常に重要な対策です。ここでは、暗号化ソリューションを選択する前に確認すべき3つの重要な項目について説明します。

Q1 **オンサイトやオフサイトのデバイスによってリスクは異なるか？**
多くの中小企業では、ノートパソコンが物理的なITインフラの中核です。リモートとオフィスワークが混在している場合、オフィスから離れることが多く、盗難に遭う可能性が高くなります。リモートユーザーの課題にも対応できるかどうか、ソリューションの機能を必ずテストしてください。

Q2 **ソリューションは優れた設計になっているか？**
セキュリティポリシー、暗号鍵、機能、エンドポイント暗号化の動作をリモートで迅速に変更できれば、デフォルトのポリシーをより強力かつ厳格にできます。また、必要なときに必要な場所で例外を適用し、簡単にロールバックできることも重要です。

Q3 **ソリューションは柔軟性があり簡単に利用できるか？**
エンドポイント暗号化技術の導入を成功に導くのは、柔軟性と使いやすさです。したがって、使用するソリューションが実際に簡単に導入できるかどうかを確認する必要があります。セットアップに時間がかかりすぎたり、操作のために追加のツールが必要だったりすると、IT管理者の頭痛の種になるだけでなく、新たなセキュリティリスクも生じます。

4. 簡単に復旧できるか？

多くの組織にとって、災害ディザスタリカバリーを全社的に実施することは容易ではありません。しかし、組織図から特定の部署や部門を無作為に選んで災害ディザスタリカバリーを行うことはより現実的な方法です。この方法では、必ずと言っていいほど変更すべき点が見つかります。攻撃を受けている最中ではなく、すぐに対応しなければならないというプレッシャーもなく、これらの改善点を発見できれば、現在の対策を効果的なものにするために役立ちます。

バックアップが復元されるまでは、バックアップが成功したかどうかはわかりません。定期的に復元テストを実行しましょう。可能な場合には、別のコンピュータにバックアップを復元し、会社の貴重なデータを利用できることを確認してください。バックアップをテストするのに最適なタイミングは、緊急事態でバックアップがすぐに必要になる前であることを覚えておいてください。

万が一、ランサムウェア攻撃によって企業データが暗号化されてしまった場合、No More Ransomで利用可能な復号化ツールがあるかどうかを確認してください。

ESETソリューションはランサムウェアなど高度なサイバー脅威に対応し業界最高レベルの保護を実現

ESETの包括的なソリューションは、ヨーロッパで開発・提供されている多層構造のデジタルセキュリティテクノロジーで、お客様のビジネスのセキュリティ要件を満たすことができます。また、セキュリティやサポートに一切妥協することなく、さらなるコスト削減を実現します。

ESET PROTECT Advanced は、
ヨーロッパで開発されている保護製品です。

詳細を見る

ESET PROTECT Advancedの特長

- ランサムウェア攻撃からの保護
- 標的型およびファイルレス攻撃からの保護
- ゼロデイの脅威の防止
- クラウドサンドボックス（ESET LiveGuard Advanced）による高度な脅威からの保護
- ESET Full Disk Encryptionによる個人情報保護法の遵守
- クラウドベースまたはオンプレミスのセキュリティ管理コンソールを利用可能
- 軽量で高速な最適化されたシステムパフォーマンス
- 容易な導入と運用

**ESET PROTECTセキュリティ管理コンソールは
ブラウザで無料デモをお試しいただけます**

欧州のデジタルセキュリティの中核を担うESET

Digital Security
Progress. Protected.