KnowBe4
Human error. Conquered.

# Ransomware Hostage Rescue Manual
# ランサムウェア レスキューマニュアル

**ランサムウェア攻撃に備え、復旧するために知っておくべきこと**


2024年度版

目次

# はじめに

ランサムウェアは、サイバー攻撃の中でも最も被害が大きく、経営者やサイバーセキュリティ担当者が最も恐れているものの1つです。ランサムウェアにより、一瞬にして、組織の重要なITインフラがダウンし、数週間から数カ月にわたってすべての業務が完全に停止してしまうかもしれません。一部のデータやシステムは永遠に失われる恐れがあります。完全に復旧するには1年以上かかることもあります。システムがダウンするだけでなく、知的財産や機密データが盗まれて、それらの公開をネタにさらに恐喝される可能性もあります。顧客への影響は、システム的には復旧できても、長期化することも考えられます。

2023年の後半、全世界のランサムウェア攻撃は急増しました。Corvus insuranceの第3四半期レポートによると、第3四半期は前四半期比11%増、リークサイトでは前年同期比95%増となり、特に、政府機関・自治体、公共サービス、法律事務所への攻撃は著しく増加しています。

研究者は、2023年はランサムウェア被害件数が初めて4,000件を超え、2022年の2,670件を一気に上回るものと予想しています。ランサムウェア攻撃の背後にあるClop、AlphV、LockBitなどの犯罪グループは、2023年、よく知られているものですが、さらに多くの新しいグループが登場し、攻撃の規模が拡大しています。

経済的な影響は引き続き甚大です。ランサムウェアは知的財産から従業員情報、財務記録に至るまで、機密データを盗み、それを一般に公開することをネタに永遠に強請り続けようとするので、被害は計り知れません。しかし、システムのダウンタイムによる被害は甚大なものであるとは言え、被害を受けたほぼ全ての組織は最終的には復旧し、ビジネスを回復することができるのです。

ランサムウェアの被害者の多くは、重要なシステムが暗号化されたために数日から数週間にわたって業務を中断しなければならず、数ヶ月に渡ってフル稼働できる状態に戻れない可能性があります。これは業績に深刻な影響を与えます。この例として、米大手日用品メーカーClorox（クロロックス）社へのサイバー攻撃を挙げられます。同社は2023年10月にランサムウェア攻撃を受け、2024年会計年度第1四半期の売上は20%減少し、その損害額は約3億5600万ドル相当と報告されています。クロロックス社を襲った同じグループは、米大手ホテル／カジノ運営エンタテインメントグループであるCaesars Entertainment（シーザーズエンタテインメント）も攻撃しており、同社は盗まれたデータが公開されてしまうことを回避するために1500万ドルの身代金を支払っています。2023年は、これらの攻撃の背後にいるScattered SpiderやAlphVグループは大金を手にした年であったと言えます。これらのランサムウェアグループは、当然ですが、目的を達成するためにソーシャルエンジニアリング攻撃を好んで使っています。

データの暗号化ができなくても、ランサムウェアグループ「Clop」は、2023年初頭から半ばにかけてMOVEitに対するその脆弱性を突く攻撃で盗んだ機密情報を公開するぞ、という単純な脅しで、7500万ドルから1億ドルを稼いだと推測されています。

# ランサムウェアの現状とその地域的な影響

ランサムウェアは全世界の誰もが被害に遭う可能性があり地理的には危険性に差はありません。国際ランサムウェア対策イニシアチブ（International Counter Ransomware Initiative：CRI）などの国際的な組織が各国の政府の協力のもと結成され、協調的な取り締まりを実施していますが、まだその活動は始まったばかりです。ランサムウェア攻撃の被害は、米国からヨーロッパ、アジア太平洋地区へと拡大しています。

**ドイツ**：

ドイツは、CRIのメンバーとして、2023年にサイバー攻撃による損失が2030億ユーロに達したと推定するドイツ連邦政府 情報セキュリティ庁（BSI）のランサムウェア対策活動を支援しています。BSIは、中小企業や地方自治体・自治体のWebサイトが標的になる一方で、Rheinmetall社といった大手企業が攻撃リスクを依然として回避できていないと報じています。

**英国**：

英国の議会委員会は、英国は破滅的なランサムウェア攻撃を受ける危険性が高く、その主な原因は計画性の欠如と投資不足であるという大胆な声明を発表しました。同共同委員会の委員長は、次のような表明を、英国は世界で最もサイバー攻撃を受けている国のひとつであるという不名誉な栄誉を持っているという表明を出しています。これを裏付けるように、2023年には、マンチェスター警察、英国ロイヤルメール、大英図書館がランサムウェアの被害に見舞われています。

**その他のヨーロッパの攻撃**：

ヨーロッパは、主要国以外でも、数々のランサムウェア攻撃が発生しており、ランサムウェアの脅威から安全であるとは決して言えません。2022年後半にはスペインのバルセロナ・ヘルスセンターが攻撃を受け、数千人の患者の検診や数多くの手術に支障をきたす大きな影響を受けています。その直後に、ベルギーのアントワープ市民サービスがランサムウェアによってオフラインにされ、警察組織のデータを含む16年分のデータが攻撃者によって公開されました。また、2023年は、グローバルにオンライントレーディングビジネス展開しているIONグループの攻撃から始まりました。この攻撃では、ヨーロッパと米国でデリバティブ取引を手動処理に切り替えなければならず、取引遅延などの重大な問題を引き起こしました。

**APAC（アジア太平洋地区）**：

2023年には、デンソー（日本）、MSI（台湾）、TSMC（台湾）、名古屋港（日本）、オークランド交通局（ニュージーランド）、ソニー（日本）など大手企業や基幹インフラがランサムウェア攻撃を受け、大きな被害が発生しています。

ランサムウェアによる損害は甚大です。基幹業務の中断、重要なデータの損失に加えて、システム復旧には膨大な時間とコストがかかります。多くの企業や組織がリスク管理には取り組んでいても、被害を受けてから平常状態に戻るレジリエンス管理はできておらず、復旧に想像以上の困難を抱えることになります。これが、ランサムウェアが10年以上にわたってサイバーセキュリティの最重要脅威であり続けている理由です。

しかし、この現状に立ち向かい、ランサムウェア攻撃が成功するリスクを大幅に減らし、復旧時間を短縮するための対策を講じることは、どのような組織においても可能です。適切なランサムウェアインシデント対応計画を作成し、それに従えば、ランサムウェア攻撃が成功するリスクを大幅に低減し、復旧にかかる時間とコストを削減することができます。このホワイトペーパーの目的は、ここにあります。

# ランサムウェアとは何か？

ランサムウェアはさまざまな形態で、さまざまな種類の脅威や被害を引き起こします。最も一般的なものは、重要なデータを暗号化したり、システムへのアクセスをロックするなどして、データの複合とロック解除を条件に身代金を要求するものです。ここでは、ランサムウェア攻撃によって発生する典型的な影響を説明します。

- データやシステムを暗号化し、ロックして、アクセス不可にする
- 機密データを盗み出し、外部へ公開すると脅迫する
- 組織、従業員、顧客のログイン認証情報を盗用する
- サイトやサービスに対するサービス拒否（DoS）攻撃を仕掛ける
- システムを乗っ取り、クリプトマイナーをインストールして実行する
- 侵害された被害者のシステムと従業員情報などを利用して、顧客やビジネスパートナーへの2次攻撃を仕掛ける
- 被害者を世間に晒して、評判を貶める

まず、ランサムウェアグループは暗号化された重要なデータを人質にとって、身代金を払えと脅してきます。この1回目の脅しに応じないと、次に、身代金の支払いを拒めば、データをインターネットに公開すると言って脅迫してきます。データの暗号化と暴露で脅すランサムウェア攻撃は「二重恐喝」と言われます。二重恐喝型は一般化しており、侵害された場合の対処もそれを考慮して計画する必要があります。

ランサムウェア攻撃の80%以上が、データとクレデンシャル（認証情報）の流出をネタに脅す「二重恐喝」を行なっています。

ランサムウェア攻撃者は、最初の段階として、フィッシングメール、パッチが適用されていないプログラム、パスワードの推測／窃盗、侵害されたベンダー、不正なオンライン広告、侵害されたソフトウェアのダウンロードなどの手法を使って、標的のデバイスへ侵入をしようとします。

この最初の段階が成功すると、攻撃者は侵入したデバイス内のファイルへアクセスして、データを暗号化し、アクセス不可にします。そして攻撃者は、画像やWebページをいきなり表示して、データを人質に身代金を要求とともに、次の項で示すような身代金の支払い方法を説明してきます。身代金の支払い期限を1週間以内としていることが多く、この期限を過ぎると、より高額な身代金を要求してきます。さらに「身代金の支払いを拒むようなら、暗号化したデータを外部に公開する」と被害者を追い込んでいきます。2回目の脅迫にも応じなかった場合、攻撃者は窃取したデータの公開へと進んできます。このプロセスについては、「典型的なランサムウェアのプロセス」の項で後述します。

## ビットコインと暗号通貨

身代金の支払いには、必ずビットコイン（略称BTC）などの暗号通貨が使用されます。ビットコインは現在最も人気のある暗号通貨であり、ランサムウェアの恐喝の支払いに必要とされる最も一般的な種類です。しかし、Ethereum、Litecoin、Ripple、Tether、XPR、Dogecoinなど、他の暗号通貨が使われることもあります。

ZcashやMoneroのようなプライバシーの秘匿が強力な暗号通貨は、法的機関による追跡や身代金のブロックが難しくなるため、一部のランサムウェアグループではよく利用されています。

ランサムウェアグループの中には、ギフトカードや送金サービスなど、他の支払い方法を利用するものもありますが、ビットコインや暗号通貨は、現金や従来の支払い方法よりもプライバシーが強力に秘匿されるため、依然として最も多く使われる支払い方法となっています。

暗号通貨はインターネットを通じて世界中どこでも送金できます。適切な場所を探せば誰でも、暗号通貨取引に関連する「デジタル・ウォレット」を確認することができますが、暗号通貨の追跡に長け、非常に大規模なデータベースにアクセスできるオブザーバーが必要です。

特定の暗号通貨取引に対して関係する現実世界の人物やグループに紐づけするために、ウォレットと暗号通貨取引を現実世界のIDに関連付けることは、ほとんどの場合可能ですが、時間とお金が必要です。近年、ランサムウェアギャングは、暗号通貨を少額に分割して他の資金と混ぜる「ミキサー」や「タンブラー」と呼ばれるロンダリング・サービスを利用し、追跡をより困難にしています。このため、暗号通貨はランサムウェアグループにとって理想的な支払い方法となっています。

## TOR（匿名ネットワーク）

ランサムウェアグループは、すべての通信がTOR（「The Onion Router」）を介して行われることを要求することがよくあります。TORは、インターネットトラフィックを匿名化するために開発された仮想ネットワークとそのブラウザーです。TORブラウザーの基幹的な技術「Onion Routing（オニオン・ルーティング）」は、1995年に米国海軍調査研究所（NRL）によって国防高等研究計画局（DARPA）の支援を受けて開発されました。当初の目的は、海軍が情報源との通信を秘匿するためでした。TOR（The Onion Router）の略称は、たまねぎのように幾重にも層を重ねて暗号化を施し、接続経路を匿名化するところから命名したとされています。すべてのトラフィックは発信元で暗号化され、ランダムに選択された「TORノード」の匿名化されたセットを経由して、意図した宛先に到達するまで送信されます。TORネットワークは、発信元から終着先までのトラフィックを他から監視できないように匿名化し、隠蔽する目的で設計されたものです。

サイバー犯罪者やトラフィックを匿名化したい詐欺師たちは、このTORネットワークを使用して、法的機関や政府当局が容易に追跡できないような通信やWebサイトのホスティングを行うことができます。このように、TORは検閲を回避するためのツールであると同時に、匿名トラフィックをより悪質に利用するためのツールでもあります。TOR（および暗号通貨）は匿名化のために非常にうまく作られているため、ランサムウェアグループは発覚を恐れることなく、被害者とやりとりするためにTORを使用することができます。

**TORについての豆知識**:

- .comや.netドメインを使用する代わりに、onionのWebアドレスは.onionで終わります。
- 通常のインターネットブラウザーではTORサイトを閲覧できません。
- TORは元々、米国海軍研究所と国防高等研究計画局（DARPA）によって開発されました。
- TORネットワークやブラウザーは、匿名化によってユーザーの実際の場所や活動を隠すことに長けていますが、完璧ではありません。TORユーザーの場所や活動は、TORネットワークやブラウザーとは関係のない他の方法で発見されることがあります。

## 典型的なランサムウェアのプロセス

通常、侵入に成功したランサムウェアプログラムは、標的である組織に最初にアクセスした後、「コマンド・アンド・コントロール」サーバーに侵入に成功したことを知らせる「dial home（ダイヤル・ホーム）」をします。ランサムウェアは、マルウェア対策製品に検出されないように、日々進化しています。新しい機能や手順を追加するため頻繁に自身をアップデートしています。ランサムウェアプログラムに自動的にプログラムされた手順を実行させたり、新しい指示を与えたりして、被害者の環境に合わせてシステム内を自由に探し回ることを可能にします。

ランサムウェアの攻撃者やグループは、多くの場合、マルウェアやツール、リモート管理プログラム、スクリプトを都度、追加して、被害者の環境をコントロールして状況を監視します。例えば、メールを盗聴して、どのデジタル資産を暗号化すれば、最もダメージが大きくなるかを事前に詳細に調べます。攻撃者は、被害者組織の財務状況まで調査し、支払ってくれそうな身代金の額を決めます。莫大な身代金を要求して一銭も騙し取れない状況を避けるため、被害者が払ってくれそうな金額を要求するのです。ちなみに一般的な身代金要求額は、年間純収入の2%程度だそうです。攻撃者は、認証情報とデータを入手した後、暗号化プログラムを起動し、ファイルやフォルダーを暗号化し、恐喝を開始します。最初の侵入から暗号化、そして恐喝の通知までの時間は、数分から数カ月に要するものまで様々です。ランサムウェアプログラムの多くは、被害者のコンピューターに侵入して、アクセスし、被害者から最大限のデータを盗み出した後に、システム内の複数のコンピューターを暗号化してきます。

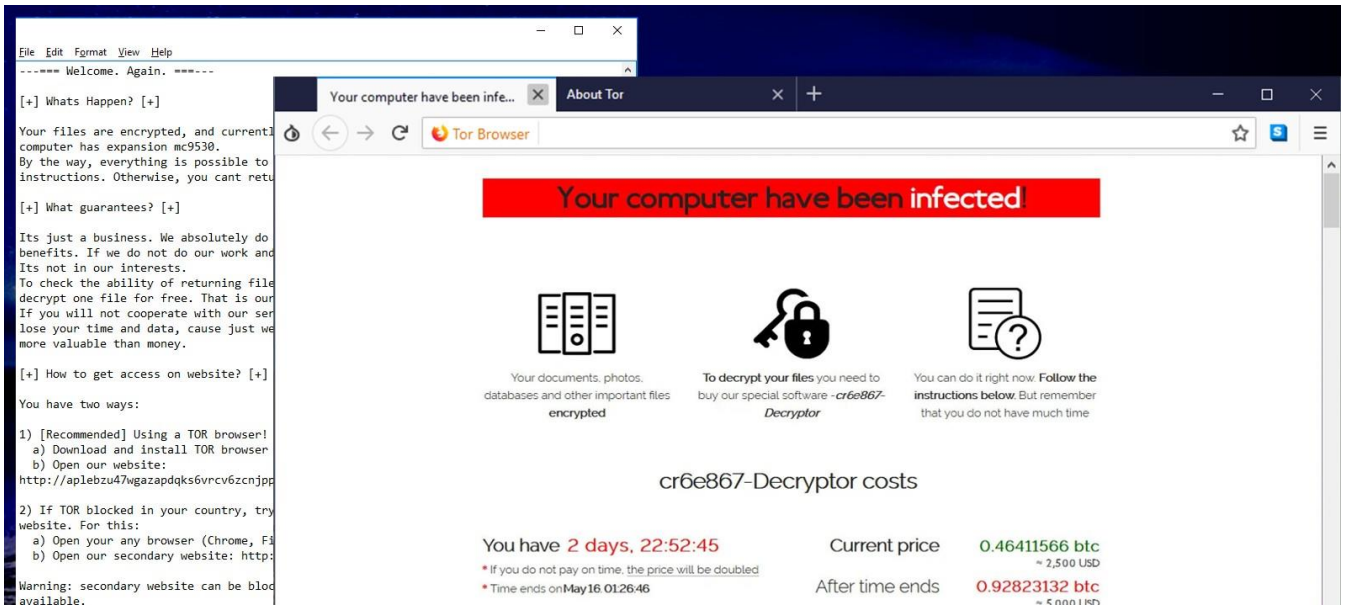
被害者が身代金の支払に応じると、攻撃者は支払われたことを確認した後に、通常、「復号」ソフトウェアと1つ以上の復号キーを被害者に提供してきます。ここから、被害者は復旧の作業に着手することができますが、暗号化されたデータをすべて復号するのは容易ではありません。また、データの暗号化に加えてデータが盗まれていた場合、通常、攻撃者は身代金を受け取ることで、コピーしたデータや認証情報を公開しないことを約束しますが、保証の限りではありません。これらのことを考慮して、身代金の支払いに応じるか、判断することが必要です。

# 感染の形跡：　感染していることに気づけるのか？

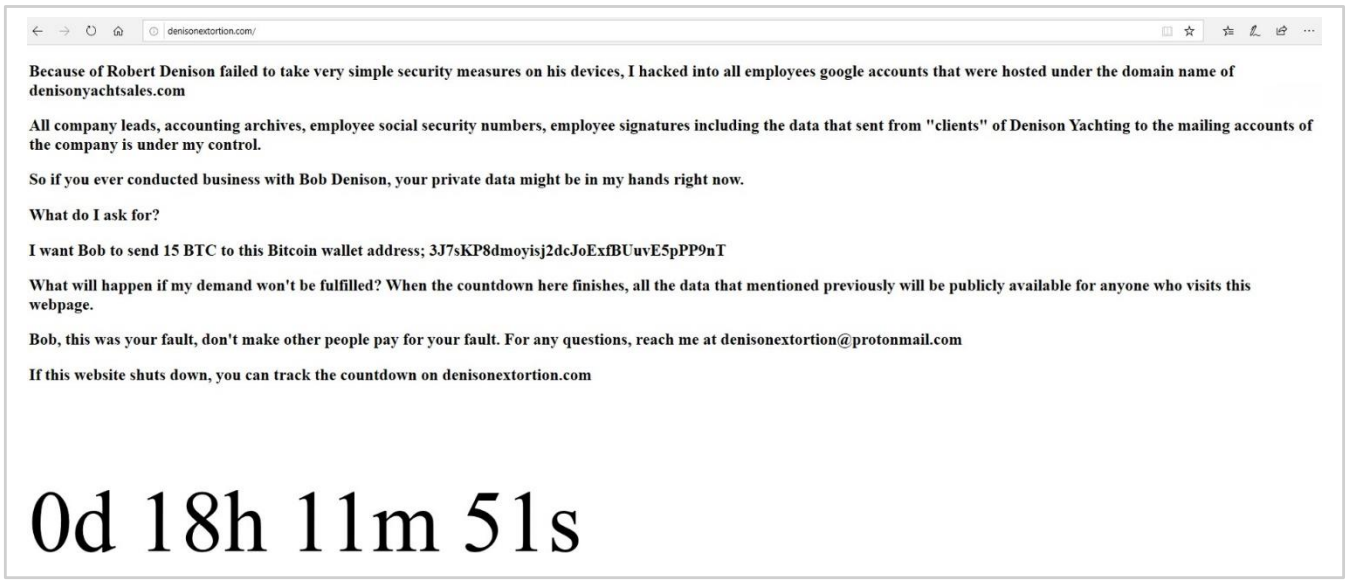
ランサムウェアに感染しているかどうかを知るのは難しいことではありません。以下のようなよく見られる形跡や症状ですぐにわかります。

- 同じネットワーク上の無関係なシステムで、1回または複数回の原因不明の突然の「クラッシュ」が発生する。
- ランサムウェアの「通知」が目に見える形で表示される。
- 突然通常のファイルが開けなくなり、ファイルが壊れている、拡張子が間違っているなどのエラーが発生する。
- ランサムウェアプログラムまたは感染したWebサイトが警告され、身代金が増額されるまでカウントダウンが表示される、またはファイルの暗号を解除できない。
- ランサムウェアプログラムによって警告メッセージウィンドウがポップアップして、ロックされて、閉じることができない。
- すべてのディレクトリーに、HOW TO DECRYPT FILES.TXTやDECRYPT_INSTRUCTIONS.HTMLのような名前のファイルが存在する。

以下は、Sodinokibi ランサムウェアプログラムのランサムウェア画面の例です。




攻撃された顧客のWebサイトにランサムウェアの通知が、カウントダウンとともに表示され、データの漏洩を脅している例です。



# ランサムウェアの根本原因：何が原因で感染したのか？

コンピューターが登場して以来、ほとんどのデバイスと組織への悪意のある侵害の根本原因は、主に次の2つです。

- ソーシャルエンジニアリング
- パッチ未適用のソフトウェア

これは、ランサムウェア攻撃にも当てはまります。この2つ以外にも、この数年間で現れたテクニックやハッキング手法（ブートウイルス、USBキー感染など）はいろいろありますが、ソーシャルエンジニアリングとパッチ未適用のソフトウェアは、30年以上もの間、常に最もよく使われる攻撃手法の1位と2位になっています。

従って、サイバーセキュリティ・リスクを最も効率的に軽減するには、まず、ソーシャルエンジニアリング／フィッシングへの対策とパッチ適用に集中することです。

KnowBe4のホワイトペーパー「The Root Causes of Ransomware（ランサムウェアの根本原因）」でデータが示されているように、ソーシャルエンジニアリングと未パッチのソフトウェアは被害者のデバイスやネットワークに侵入するためにランサムウェアグループが最も利用する攻撃手法で、感染原因の大半を占めています。しかし、他の攻撃手法もランサムウェア攻撃で用いられるようになってきており、この実態は、ホワイトペーパー「The Root Causes of Ransomware（ランサムウェアの根本原因）」に示された次のランサムウェア対策ベンダーの調査のサマリー表の通りです。

| レポート名・社名 | ソーシャルエンジニアリング | RDP | 未パッチのソフトウェア | パスワード推測 | 認証情報の盗難 | リモートサーバー攻撃 | サードパーティー | USB | その他 |
|---|---|---|---|---|---|---|---|---|---|
| **Covewareレポート** | 30% | 45% | 18% | - | - | - | - | - | 5% |
| **Statista** | 54% | 20% | - | - | 10% | - | - | - | - |
| **Forbes誌記事** | 第1位 | 第3位 | 第2位 | - | - | - | - | - | - |
| **Dattoレポート** | 54% | 20% | - | 21% | 10% | - | - | - | - |
| **Hiscoxサイバー態勢報告** | 65% | - | 28% | 19% | 39% | - | 34% | - | - |
| **Sophosレポート** | 45% | 9% | - | - | - | 21% | 9% | 7% | 9% |
| **平均値** | 50% | 24% | 23% | 20% | 20% | 21% | 22% | 7% | 7% |

このホワイトペーパーでは、数多くの攻撃手法が、さまざまなベンダーによって異なる分類がなされていますが、3番目ランクインしているパスワード推測が広く使われていることは明らかです。ランサムウェアグループは、以前に盗んだ有効なログインIDとパスワードを使用して被害者のデバイスにログインを試みますが、ログインできなかったとしても、以前盗んだ情報を元に、パスワードなどの認証情報を推測することで侵入に成功します。

この最初のログインをきっかけに侵害をさらに拡げて、最終的には基幹ネットワーク／インフラやサプライチェーンが侵害され、機密情報のロック、業務停止を引き起こします。

**このデータを総括してみると、ランサムウェア攻撃では、次の3つの攻撃手法によって、大半が可能であることが明らかにされています。**

- ソーシャルエンジニアリング
- 未パッチのソフトウェア
- パスワードの推測

## 攻撃手法について、さらに詳しく説明します。

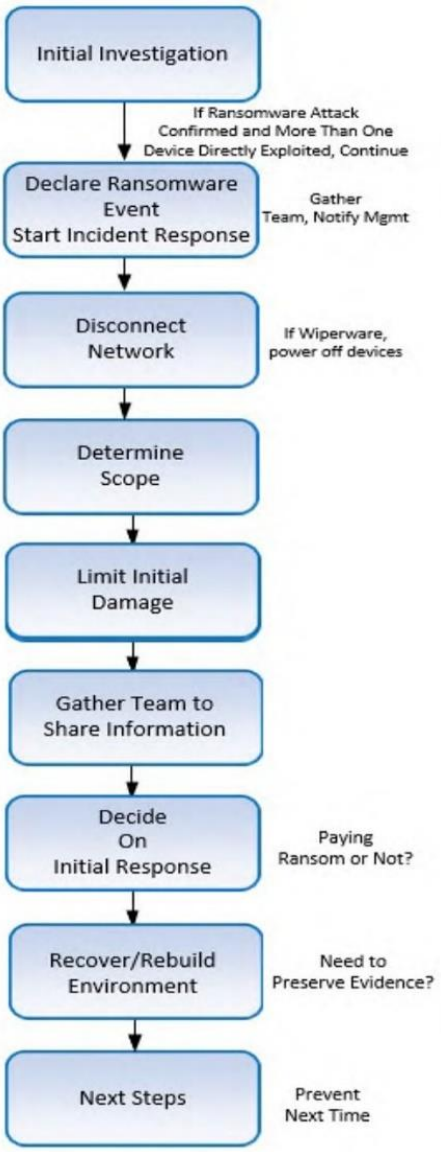
**フィッシングによるソーシャルエンジニアリング**
最も一般的なソーシャルエンジニアリングのシナリオは、無害なファイルを装ったファイルが添付された予期せぬフィッシングメールが届くというものです。ユーザーが真偽を確認せずに添付ファイルを開いたりインストールしたりすると、ランサムウェアに感染してしまいます。これが、ランサムウェア攻撃の根本原因の大半を占めています。

**サイレント・ドライブ・バイ・ダウンロード**
パッチが適用されていないソフトウェアプログラムを使用しているユーザーが、不正なWebサイトまたは侵害されたWebサイトを閲覧すると、マルウェアが勝手にダウンロードされる攻撃手法です。このマルウェアによって未パッチの脆弱性が攻撃された場合、被害者は自分のコンピューターが侵害されたことに気づきません。（画面に変化がなく被害者は攻撃に気づくことはありません。）これは、ラテラルムーブメントのきっかけとなります。

**パッチが適用されていないサーバーまたはサービス**
攻撃者は、被害者のサーバーやネットワーク上のサービスで、パッチが適用されていないソフトウェアプログラムを探し出し、それを悪用して悪意のあるコードを実行させます。パッチを適用すれば、このような侵害を防ぐことができるため脆弱なソフトウェアがないか監視し処置をする日々の作業は重要です。

**フリーソフトウェアベクター**
ソフトウェアの無料版には、高価なゲームやソフトウェアを「クラックしてある」バージョン、無料ゲーム、「改造」ゲーム、アダルトコンテンツなど、さまざまな種類があります。ユーザーの好奇心を煽り、攻撃者はファイアウォールやメールフィルターをすり抜けることができます。

**リモートデスクトッププロトコル（RDP）**
Microsoft Windowsリモート・デスクトップ・プロトコル（RDP）は、Microsoft Windowsコンピューターにリモートでログインし、管理者やユーザーがあたかもそのコンピューターの前に座っているかのようにコンピューターを操作するためによく使用されます。攻撃者は、RDPを実行していてインターネットから丸見えのコンピューターを攻撃し、ネットワーク内へのマルウェア拡散を仕掛けます。RDPは、通常、未パッチの脆弱性やパスワードの推測よって攻撃されます。脆弱なパスワードや有効にされていないアカウントロックアウト保護が狙われます。



# 感染後の処理：感染したらどう対処したらいいの？

ランサムウェアに感染したことがわかったら、直ちに処置を講じる必要があります。感染後の対処について、次の9つのステップを順に説明します。

- ステップ 1：初動調査
- ステップ 2：ランサムウェア攻撃発生の宣言・インシデント対応の開始
- ステップ 3：ネットワークの遮断
- ステップ 4：感染範囲の判定
- ステップ 5：被害の極小化
- ステップ 6：セキュリティチーム・関係者を召集、現状を情報共有
- ステップ 7：対応策の決定
- ステップ 8：原状回復
- ステップ 9：予防措置

## 1 初動調査

ランサムウェア攻撃への対処は、組織内の誰かからの不審なイベントの報告から始まります。セキュリティ担当者が、ランサムウェア感染メッセージが表示されたとかファイルが暗号化されたなどの報告を受けます。そうしたら、まず本当にランサムウェアに感染したのか確認をしてください。

ランサムウェアには、単に感染したと伝えるポップアップメッセージを表示して、デバイスをロックするものがあります。本当はファイルの暗号化はできていないのに“デマ”メッセージを表示するのです。その時、ランダムに暗号化されたファイルが見つかったとしても、それらはかなり以前に別の理由で暗号化されたものである場合もあります。ですから最初に対応する人は、ランサムウェアに感染した！と思い込まされてしまっただけで、本当のランサムウェアの感染でないことを確かめる必要があるのです。

ランサムウェア感染が疑われる場合、本当に感染したことを確認するための主なデータポイントは2つあります。第一に、報告された疑わしいイベント（複数可）に本物の（デマではなく）ランサムウェアが含まれているか？ 2つ目は、2台以上のデバイスが感染しているかどうかです。感染デバイスが1台だけで、他のデバイスには感染がない場合、ランサムウェアではない可能性が高いです。感染したことについて確証を得ていないのであれば、ランサムウェアインシデントを発表するのは早計であり、まずは、初期消火を実施することがポイントとなります。

多くの組織は、ランサムウェアプログラムの拡散またはファイルの暗号化の前に、ランサムウェア攻撃の初期段階で悪意のあるコードを発見しています。それでも、ランサムウェアの形跡を発見した場合は、ランサムウェアが複数のデバイスに拡がっていないかを確かめ、他のデバイスへの拡散を防ぐことが、初動対応として極めて重要です。 しかし、感染デバイスが1台しか確認されていない場合は、ランサムウェア対応チーム全体によるインシデント対応ではなく、セキュリティ担当者による初期消火で初動対応を行い、完全に削除できたか確信が持てない場合は、ランサムウェア対応計画に移行して、複数のデバイスへの感染を監視することです。

2台以上のデバイスが感染していることが確認された場合は、ランサムウェアが組織内のすべてのネットワーク接続デバイスに広がっている可能性を念頭に、完全なランサムウェア対応を進める必要があります。

**注：盗んだ情報を公表しないことを条件に身代金を要求するため、ランサムウェアに分類されますが、単に恐喝するだけのこうした攻撃にはデータの復号やデータ復旧に関する手順は無意味です。それでも、攻撃者との交渉をしたり、攻撃者が残した可能性のあるバックドアを閉じるなどの対策は、侵入経路と手順を理解する上で重要です。恐喝と窃盗のみ目的とする犯罪集団に対応する場合は、これらのことを念頭に置いてください。**

## 2 | ランサムウェア攻撃発生の宣言／インシデント対応の開始

2台以上のデバイスがランサムウェアに感染した場合、ランサムウェア攻撃の発生を公式に発表する必要があります。そして、組織を上げてランサムウェア対応チームに協力する「全員参加」でインシデント対応に臨まなければなりません。すべての上級管理職に、ランサムウェア攻撃の発生と現在判明しているその状況を詳細に報告してください。同時に法務部に連絡し、できるだけ早く主体的に関わってもらうことを依頼してください。また、ランサムウェアインシデント対応チームメンバー全員に、ランサムウェアの侵害と拡散を示す新たな兆候を監視するよう指示してください。関係者全員が、何をチェックし、何を確認し、どのように判定したかを文書化することも忘れてはいけません。ネットワーク上のすべての資産が感染されたという前提のもとに、関係者全員で監視を実行しましょう。データやシステムというデジタル資産がランサムウェア攻撃の影響を受けていないと判断されるか、システムが正式に回復したと宣言されるまで、監視は怠ってはいけません。また、既存のパスワードはすべて漏洩していると考えるべきです。ネットワーク上に侵害されたデバイスが1つでもあれば、そのデバイスがクリーンになって復旧するまでは、ネットワーク全体が信頼されていない状態であると見なすべきです。

**既存のパスワードや保存されているパスワードは、すべて漏洩していると考えるべきです。**

侵害されたネットワークやシステムを隔離して、ユーザー全員が予め合意した代替の通信手段に切り替える必要があります。通常、これはランサムウェア対応チームのコミュニケーションも、緊急時の携帯電話および/または外部メッセージングアプリケーション（Slack、WhatsAppなど）への切り替えを意味します。危険にさらされる可能性のあるシステムを、ランサムウェアのインシデント対応チームが通信に使用することは避けるべきです。ランサムウェアのインシデント対応チームは、経営陣、法務担当者と共に、追って通知があるまで、以降は緊急時の代替通信手段を使用してください。

影響を受けたであろう第3者や外部組織との連絡は、すべて法務部門が担う必要があります、そのような連絡は「特権的通信」とみなされる可能性が高く、法的な訴訟や調査が発生した場合に他の関係者が知ることが難しくなるためです。侵害されたネットワークおよび資産に関する、以前の外部との通信が盗聴され、攻撃者に知られた可能性があることを想定しておいてください。

ランサムウェアへの対応や復旧に使用する代替の通信手段については、事前に合意しておく必要があります。

## 3 | ネットワークの遮断

現在、ランサムウェアに感染したことが判明しているデバイスが1台のみの場合は、直ちにそのデバイスをネットワークから遮断します（有線および無線の接続が存在する場合はすべて遮断するなど）。複数のデバイスがランサムウェアに感染している場合は、影響を受ける可能性のあるすべてのデバイスのネットワーク機能を無効にします。これには、インターネットアクセスとネットワークの出入口となるネットワークポイントが含まれます。ランサムウェアの拡散や生きている外部からの制御のリスクを低減したい場合は、判明している感染デバイスが1台だったとしても、すべてのデバイスのネットワークアクセスを遮断することを検討してください。

影響を受ける可能性のある全てのデバイスを、個別に、そのネットワーク機能を手動あるいは自動化された方法で無効にしなければならないと思うかもしれませんが、ほとんどの場合、ネットワークの遮断は、デバイスが共有している共有ネットワーク機器（ルーター、スイッチ、VLAN、Wi-Fiルーターなど）を無効にすることで、より簡単に行うことができます。各デバイスのネットワークを個別に無効にすることもできますが、ネットワーク接続が再び許可されたときにネットワークアクセスを再び有効にするには、通常時間がかかり、個別の物理的なアクセスが必要になります。USBや外付けハードドライブなどのストレージデバイスはプラグを抜いてください。

**ネットワークに接続されているデバイスのネットワーク接続を無効にしなければならない場合、可能であれば、その代わりに共有ネットワークデバイスのネットワーク接続を無効に**

デバイス本体の電源を落とさないでください。この時点では、何も消去したり、ファイルやアンチウイルスを「クリーンアップ」したりしないでください。復旧や証拠保全など、後で必要な作業ができなくなってしまう可能性があるため、絶対に電源を落としたりファイルを消したりしないでください。

しかし、このルールには2つの例外があります。まず、ファイル暗号化の初期段階にあるコンピューターを見つけた場合（つまり、ほとんどのファイルが暗号化される前に早期に発見した場合）、または「ワイパーウェア」を発見した場合、影響を受けたデバイスの電源を直ちに落とすことができます（グレースフルシャットダウンではありません）。ワイパーウェアは、身代金を要求し、それが支払われても、復旧させるつもりはなく、単にディスク情報やファイルを消去、破損、暗号化するマルウェアのことです。ランサムウェアよりタチの悪いマルウェアで、これをワイパーウェアと言います。

残念ながら、ランサムウェアとワイパーウェアの違いを早い段階で見分けることは不可能であり、特にワイパーウェアがランサムウェアを装って拡散し、被害が拡大した場合は、防御側が被害の極小化を開始する前にその違いを見分けることは困難です。幸いなことに、ランサムウェアを装うワイパーウェアが発生するケースは極めてまれであるため、以下の点を考慮する必要があります。

ランサムウェアと名乗り同じような振る舞いをするマルウェアは、ランサムウェアであると考えるべきでしょう。しかし、ワイパーウェアの可能性があることは常に頭の片隅に置いておいてください。

## 4 | 感染範囲の判定

このステップでは、インフラストラクチャのどの程度が侵害されているのか、何が暗号化／破壊されているのか、データや認証情報が流出したのかどうかを正確に判断する必要があります。何が感染したかを探す場合、調査担当者は、まずは、通常とは異なる、あるいは説明のつかない新しいプロセス、サービス、デーモンを探し出し、報告する必要があります。暗号化の範囲を確認する場合、調査対象に以下を含めるようにしてください（共有または非共有ドライブやフォルダー）。

- あらゆる種類のネットワークストレージ
- クラウドベースのストレージ（DropBox、Google Drive、Microsoft OneDrive、AWSなど）
- 外付けハードドライブ
- 貴重なファイルの入ったUSBメモリー

上記を点検し、暗号化の形跡がないかチェックしてください。これはいくつかの理由から重要です。第一に、ランサムウェアプログラムの範囲と広がりを把握することです。何が暗号化されたのか？第二に、DropBox、Microsoft OneDrive、Google Driveなどのクラウドストレージ・ソリューションの場合、暗号化されていない直近のバージョンのファイルに戻すことができるかを確認してください。第三に、バックアップシステムを導入している場合、どのファイルがバックアップされていて、どのファイルをリストアする必要があるのか、あるいはまったくバックアップされていないかを把握する必要があります。もし、最悪の場合、身代金の支払いを余儀なくされるにしても、ランサムウェアに暗号化を解除させるためにはドライブを再接続する必要があるので復旧の対象を正確に把握しておきましょう。

感染範囲を特定するもう1つの方法は、ランサムウェアによって作成されたレジストリーやファイルリストを確認し、暗号化されたすべてのファイルをリストアップすることです。ランサムウェアは身代金が払われた時のデータの複合に備えて、どのファイルが暗号化されたかをリストアップしています。多くの場合、このリストはレジストリーエントリーやファイルに保存されています。ランサムウェアの種類によりリストの方法は異なりますが、既知のランサ

ムウェアであればインターネット上に情報があるかもしれませんので調べてみてください。

システム上の暗号化されたファイルをリストアップするために作られた特別なツールもあります。

- 復号ツールへのリンクについては、ランサムウェアに関するナレッジベースをご覧ください。

次に、データやログイン認証情報がコピーされたかどうかを確認してください。コピーされた場合は、どれ位のデータがコピーされたか、またその内容（可能であれば）を確認してください。これは、通常、ランサムウェアプログラムの通知から知ることができます。また、攻撃者がWebサイトやブログに投稿している情報から知ることもできます。ログやデータ漏洩防止（DLP）ツールをチェックして、どのデータが盗まれたか記録されていないか確認してください。盗まれたデータを含む、攻撃者が作成した大きなアーカイブファイル（zip、arcなど）を探してください。攻撃者がデータをコピーする前にステージングに使用した、データを含む大規模な未承認アーカイブファイル（zip、arcなど）を探してください。大量のデータがコピーされる前に ネットワークからコピーされた大量のデータを記録している可能性のあるシステムを調べてください。次に、データを探したり盗んだりするために使用された可能性のあるマルウェア、ツール、スクリプトを探します。また、ランサムウェア攻撃者があなたのデータや認証情報を持っていると言ってきたら、それは間違いありません。ランサムウェア感染に成功した攻撃者が “はったり”をかますことはないのです。

**注：もちろん、ランサムウェア攻撃者がデータや認証情報を盗み出したと言ってきたら、その証拠を見せるよう要求することは可能です。一般にはすぐにサンプルを証拠として見せてきます。まれに、盗まれたファイルがそれほど重要でないこともあります。何が盗まれていて、何が盗まれていないかを、きちんと把握することは、リカバリーを行う上で極めて重要です。**

すべてのデバイスに対して完全なフォレンジック分析を行うか、いくつかのデバイスを（多くのデバイスが含まれる場合は）なサンプルとして抽出して調査をするかしてください。どのような悪意のある活動が行われたかを特定します。ランサムウェア攻撃者は、大抵、ランサムウェアとは別に他の悪意のあるプログラムやスクリプトをインストールしています。本格的なフォレンジック分析が、発生したインシデントの全容を正しく理解するための最良の方法です。フォレンジック分析は専門家に任せ、デバイスの調査をできるだけ妨げないようにしてください。専門家は、専用のフォレンジック分析ツールを使用して、影響を受けたデバイスからストレージデバイスとメモリーのコピーを作成し、悪意のあるものを特定してくれます。

**ランサムウェアの種類とバージョンを特定する方法**

どのランサムウェアプログラムが使われたか正確に把握することが重要です。基本的にランサムウェアには、データや認証情報を暗号化したり盗んだりした後、身代金を期限までに支払うように要求するというパターンがあります。しかし、どのランサムウェアが使われたかを知ることができれば、適切に対処するためのランサムウェア毎に異なる情報を得ることができます。

ランサムウェアには、身代金が高額なものもあれば、支払い方法はビットコインだけでなく、他の方法を提示するものなど様々な種類があります。バグが多く、身代金を支払っても確実に復号できないケースも多々あります。身代金を払えばきちんと複合してくれる実績を残しているランサムウェア攻撃者もいます。ランサムウェアのプログラムとバージョンを知ることは復旧の手助けになります。

ランサムウェアによっては、身代金を支払わなくてもファイルを復号できるツールや複合キーが一般に公開されていることが稀にありますが、それを当てにしてはいけません。結局、あなたが新バージョンのランサムウェアに最初の被害者の1人であるとして、あなたが調べて得た情報を提供すれば、あなたの環境の復旧を支援する専門家や、今後、同じ系統のランサムウェアの被害を受けた人を支援するのに役立ちます。

このステップの結果は、何がどのように影響を受けているかを把握することです。何がどの程度感染しているのか？ また、ランサムウェアの被害は1か所のみで発生しているのか？ それとも複数箇所で発生しているのか？ 何が被害を受けていないのか？ 多くの場合、影響を受けていないものの特定は、被害の範囲や対応方法を決定する上で、何が影響を受けているかを理解することと同じくらい重要です。データや認証情報が流出したかどう

かを判断できますか？ 根本的な感染の最初の原因を特定できますか？

データのバックアップは安全で信頼できますか？ 多くのランサムウェア被害者は、「バックアップがあるから大丈夫」と思い込み、ランサムウェアグループとの最初の交渉を拒否してしまうことがあります。攻撃者は、被害者のバックアップデータを消去または破損することができるもの、バックアップがあるから必ず安全ではない、と覚えておいてください。

したがって、バックアップがあってもそこから復旧が可能か？安全で信頼できるものであるか？必ず確認してください。バックアップデータの安全性が証明されるまでは、安易に復旧作業に取り掛からないようにしましょう。

バックアップデータが安全で信頼できるものであることを確認する手順、バックアップから影響を受けたすべてのデバイスやサービスを確実に復元するのに要する期間を予め試算しておき、レジリエンス管理に役立てましょう。リスク管理も重要ですが、正常時へ復元するためのレジリエンス管理を忘れずに行ってください。

**ランサムウェアはデータや認証情報を窃取することが多く、**
**バックアップからの復元だけではランサムウェア対策として不十分です。**

このステップでは、できるだけ多くの情報を集めることが対策のキーとなります。

## 5 | 被害の極小化

初期被害を抑える方法があれば、まず、それを実行してください（必要な証拠の保全を忘れないように）。ネットワークを無効にし、直接接続されているストレージデバイスのプラグを抜くことは、その一つの方法です。また、もう一つが、暗号化が依然として進行中であるデバイスの電源を落とすことです。多くの被害者は、暗号化が実行されていても、そのデバイスのデータは保存する必要がないと思うと、そのデバイスの電源を切らずに放っておくことがよくあります。しかし、暗号化が進行中と思われるデバイスがあれば、その電源はすぐに落としてください。

**漏洩したパスワードの変更**
被害を抑えるために行うべきもう1つのことは、攻撃者がアクセス可能なサービスのうち、侵害された可能性のあるもので利用される全てのログインパスワードの変更です。SaaSが一般化している現在、多くのサービスは、インターネットベースのシステム上で実行されているため、無効にすることはできません。例えば、パブリックなクラウドベースのサービスなどです。ランサムウェアの被害に遭った場合、最初の感染から発覚までに使用されたすべてのパスワードが漏洩したと考えるべきでしょう。当該システムのパスワード、従業員のパスワード、侵害された環境からアクセス可能な顧客向けポータル上の顧客のパスワードなど、感染デバイスとネットワークで使用されたすべてのログイン認証情報がその全てが漏洩した可能性があります。

漏洩した可能性のあるすべてのパスワードの一覧を作成し、できるだけ早くすべてを変更するための作業を調整する必要があります。今後の「パスワード再設定日」を決めて、関係者との調整とアクションプランを立てましょう。漏洩した可能性のあるパスワードをすべて変更しておかないと、再び侵害されるリスクが高まります。

直接侵害されたデバイスやネットワークに保存されているパスワードのうちで、一旦無効化され、ネットワーク通信の遮断によって隔離されているものについては、パスワードのリセットは、感染デバイスやサービスが回復するまで待つしかありませんが、漏洩したパスワードは、他のものを推測する手がかりになりますので、それらにより影響を受ける可能性のあるすべてのデバイス、ネットワークのパスワードは変更してください。

## 6 | セキュリティチーム・関係者を召集、現状を情報共有

いよいよ、把握できたランサムウェアの影響範囲について協議するチームを収集する時です。事前に合意してお

いた代替の通信手段を使用するか、安全な物理的会議スペースを使用して、何が影響を受け、何が影響を受けなかったのか？何が暗号化されたのか？データや認証情報は流出しましたか？ランサムウェアプログラムはどのようにして最初に環境に侵入したのか？をセキュリティチームと関係者全員で情報共有してくだい。

**注：被害組織の中には、普段使っているビデオ会議システムや電話会議システムへのアクセスも侵害されて、攻撃者に復旧計画を盗聴されてしまったところもあります。事前に合意しておいた代替の通信手段を使用することは、極めて重要です。**

この段階に入ると、外部のコンサルティング会社から関係者などが加わり、情報共有とともに情報管理が重要になります。内部関係者として、上級管理職、法務担当者に加えて、マーケティング／広報担当者も加わってきます。内部統制という観点から、外部へ発信・共有できる情報とできない情報を細かく規定する必要があります。許可されていない情報を共有しないこと、公開情報は事前に作られたインシデント対応計画の規定内に留めることを周知徹底する必要があります。

このステップの目標は、これまでに知り得たことをすべて共有し、影響と範囲について全員が共通理解を持ち、次のステップをどうするかを全員が把握することです。各チームメンバーは、情報に誤りがある、あるいは不完全不明瞭であると思った場合に躊躇せず発言し、他のメンバーに公平な立場で意見できるようにしておきましょう。

インシデント対応チーム内の各メンバーの理解が異なっている、一部のメンバーに情報が集中することは珍しくありません。メンバー全員で共通の理解を持ち、透明性を確保することは重要です。

このステップで最も重要なことは、経営幹部や法務担当者が、ステップ2のインシデント発生の宣言に加えて、業界規制団体、法執行機関、米国ではサイバーセキュリティ・インフラストラクチャ・セキュリティ・エージェンシー（CISA）などの外部団体に詳細を報告するかどうかを決定することです。CISA は、サイバーセキュリティの防衛と復旧を調整する米国の最高国家機関です。多くの国に同様のサイバーセキュリティ機関があります。米国では、CISA はすべてのランサムウェア被害者が CISA、FBI、またはシークレット・サービス（範囲が該当する場合）に連絡し、ランサムウェアイベントの開示と支援を受けることを推奨しています。そうすることで、有益な情報、アドバイス、追加の法的保護を得ることができます。日本においては、警視庁のサイバー犯罪相談窓口へ連絡してください。また、このようなサイバーセキュリティインシデントをカバーする保険会社に加入している場合は、保険会社に連絡する必要があります。外部の関係者に連絡を取るかどうかは、経営陣と法務チームによって決定され、法務チームの責任下に行われるべきです。

## 7 | 対応策の決定

攻撃の初期情報と影響範囲が判明したら、次は犯罪者への対応を選択しなければなりません。暗号化されて、データがアクセス不可になった場合も、さらにデータが盗まれ悪用されるかもしれない場合でも結局、選択肢は2つです。

- 身代金を支払う
- 身代金を払わない

身代金を支払うかどうかの判断は、必ず上級管理職と法務担当者を巻き込んで、決定してください。身代金を支払わないと判断した場合は、直ちに復旧作業に取り掛かってください。

身代金を支払うことを決めた場合は、恥や罪悪感を持たずに、この決定を臆せずに進めてください。犯罪者は、身代金を支払わないという選択をできないように追い込みます。ランサムウェアの被害者の約40%が身代金を支払っていると推定されていますが、ランサムウェア攻撃への対策が進むにつれ、身代金を支払う被害者の割合は徐々に減少しています。多くの被害組織が身代金を支払うのは、通常の業務に戻るため、または流出したデータや認証情報がさらに悪用されるのを防ぐために、それが最も迅速でコストのかからない方法と判断したからです。

多くの被害者は、バックアップが最初に信じていたほど安全でも、効果的でもないことに気づきます。


保険を適用できる場合は、往々にして、全体的なダウンタイムと調査、復旧コストを削減するために、身代金の支払いに同意することがほとんどです。

身代金を支払うことを決定した場合、誰が身代金の交渉役となるのか（社内の関係者か、社外の関係者か）、いくらなら支払うか（要求額全額ではない場合）、支払いに必要と思われる暗号通貨にアクセスする方法を決定する必要があるか（これについては後述します）を決める必要があります。

被害者の組織（または保険会社）が身代金を支払うことにしたとしても、犯罪者の要求した通りの額を支払いたくはないでしょう。ランサムウェア攻撃者は、当初は想像以上に高額な身代金を要求しますが、交渉すれば要求額を引き下げることがあります。最初の要求額の半額まで下げるケースも珍しくありません。

また、ランサムウェア攻撃者との身代金交渉は慎重に行なってください。攻撃者を怒らせたり侮辱されたと思われたりすると、さらに高額な身代金を要求することも珍しくありません。

いずれにせよ、身代金を支払う前に、必ず攻撃者に、確実にデータを復号できるという証拠を提出させてください。複合プログラムやキーの仕組みや受け渡し方法などを事前に確認してください。

復号プログラムやその複合手順は、攻撃者の説明通りに動作しないこともありますから事前確認は入念に行なってください。

**身代金の支払いは違法か？**

身代金を支払うことが最善と判断したとして、支払う前に、それが違法でないことを確認する必要があります。特に米国では、米国財務省の外国資産管理局（OFAC）は、2020年10月1日付けでランサムウェアの身代金支払いについての勧告を出しています。この勧告によって、少なくとも、米国の法律に従う義務がある企業は、OFACの制裁対象組織リストにある犯罪グループに身代金を支払うと、法的責任を問われます。

OFACの制裁対象リストに掲載されている主なランサムウェア開発者／組織は以下の通りです。

初期のランサムウェアプログラムであるCryptolockerの開発者であるEvgeniy Mikhailovich Bogachev、悪質なサイバー活動への物質的支援を提供し、SamSamランサムウェアの収益を流すために使用された2つのデジタ

ル通貨アドレスを特定した2人のイラン人、WannaCryランサムウェアの背後にある北朝鮮のLazarus Group、および2つのランサムウェアサブグループであるBluenoroffとAndariel、など、OFACリストに掲載されている制裁対象者または組織に身代金を支払うと、たとえ被害者がOFACの制裁対象リストにランサムウェアグループが掲載されていることを知らなかったとしても、民事上の罰金や処罰を受けることになります。

法的リスクを最小限に抑えるため、身代金を支払う場合は、まず必ず関連する法規制に詳しい弁護士に相談してください。身代金の支払いを追跡し、相手のランサムウェアグループがOFACの制裁対象リストに載っているかどうかを知らせてくれるサービスに相談することもできます。このようなサービスを提供している暗号通貨追跡会社には、ChainalysisやEllipticなどがあります。

身代金を支払うことが合法かどうかを判断することを手助けしてくれる公的なサービスもあります。CISA、FBI、または関連する管轄の法執行機関からの協力を得ることは決して損にはなりません。しかし、その場合でも最終的な判断は弁護士に依頼してください。

# 8 | 原状回復：修復か、再構築か？

身代金を支払うかどうかにかかわらず、影響を受けたシステムや情報を修復（REPAIR）または再構築（REBUILD）するかどうかを決定する必要があります。大規模な暗号化が発生しなかったとしても、侵害された可能性のあるシステムの再構築や修復は検討しなければなりません。

## 修復だけを実施

多くの被害者は、金銭、資源、時間上の制限があるため、感染デバイスやサービスを、できるだけ早く復旧させるため、最低限のことしかできません。マルウェアや悪意のある改変をすべて削除し、漏洩パスワードをすべて変更し、影響を受けたシステムを（多くの場合、暗号化されたファイルを復号することによって）動作可能な状態に復元し、とにかく早く復旧して稼働させることに全力を尽くしてしまうことでしょう。

しかし、このことは、攻撃者の再侵入（または他の将来の攻撃者の侵入）をより簡単に許してしまうような悪意のある何かが見落とされてしまうリスクを高めてしまうのです。

## すべてを再構築

最も安全な（そして通常は最も高価な）選択肢は、通常、ネットワーク内のすべてのデバイスとサービスを完全に一から作り直し再構築（および/または切り替え）することです。真新しいログイン認証情報を使用して、既存の脆弱性が存在しないことを確実にすることです。ダウンタイム中に、過去に存在した可能性のある脆弱性やエラーを根本から見直し、インフラを再構築する被害者もいます。新しいソフトウェアプログラム、既存プログラムのアップデートバージョン、新しいセキュリティ防御プログラム、MFA（以前に使用されていなかった場合）を追加することもあります。侵害された旧インフラとは全く異なるかたちで刷新されることもあります。

## 証拠の保全

被害者は、法的な対応を考慮し、ランサムウェア攻撃の証拠保全を可能な限り行わなければなりません。そのため、修復や再構築などのすべてのアクションは、他のデバイス（つまり、侵害を受けた以外の別のデバイスまたはシステム）で行われます。被害者は、現在影響を受けているデバイスまたはシステムの完全なバックアップ（ミラーコピー）を作成し、他の同様なデバイスまたはシステムへリストアしてから、新しいデバイスから修復またはリカバリーの作業を行なってください。これによって、古いデバイスやシステムは隔離され、影響を受けないように保つことができます。また、リカバリーの前にフォレンジックコピー（メモリーおよびストレージ領域）を作成することも大切です。証拠保全について懸念があれば上級管理職と法務担当者に連絡して、修復か再構築かを相談の上判断するようにしましょう。

修復または再構築のいずれを選択したとしても、システム環境を全面復旧し、安全に業務を行えるようにするためにやるべきことは山のようにあります。まずは、ビジネスインパクト分析（BIA）を行って、どのサービスをどのような順序で復旧させるべきかを決定しましょう。これによって、全面復旧までの時間を短縮して、全体的な損害を減らすことができます。どちらを選択しても、外部の業者による全面復旧までの支援はほぼ不可欠です。

## インフラの再建

ほとんどの場合、どのアプリケーションとサービスを最初にリストアする必要があるかを特定した後、基盤となるすべてのサポートインフラ（IPアドレス管理、DHCP、DNS、Active Directory、セキュリティサービス、ツールなど）を、まずクリーンな状態にリストアする必要があります。ほとんどのアプリケーションにおいて、この既知のクリーンなサポートインフラが確保されているかが、アプリケーションをリストアする前に必要条件となります。アプリケーションの中には、外部のクラウドや侵害されたインフラとは別系統に構築されているものもあります。このようなアプリケーションをオンラインに復帰するのは、比較的簡単です。その他のアプリケーションは、原状復帰するのに、少なくとも数日から数週間のサポートインフラでの作業が必要になります。

複合的な選択肢もあります。一部は修復して、修復できないシステムやサービスは再構築することになります。しかし、修復は安価で短期間でできますが、再攻撃や将来の攻撃に対するリスクが残存する可能性が高いことに注意しなければなりません。このようなリスクを考えて、適切な方法を選んでください。

## 暗号化されてしまったファイルのバックアップ

身代金を支払い、ランサムウェア攻撃者から複合プログラムや復号キーが送られてきたとしても、いきなりオリジナルの暗号化されたファイルの複合を行わないでください。複合に失敗しファイルが破損して永遠に失われてしまう可能性があります。必ず暗号化されてしまったファイルのバックアップを取っておいてください。復元の作業は、暗号化されたファイルのバックアップを取った上で、コピーで行うということを忘れないようにしてください。

身代金を支払わない場合でも、暗号化されたファイルのバックアップを取っておくことをお勧めします。その理由は、たまたま暗号化キーが発見されて、公開されたりする可能性があるからです。ランサムウェアの開発者が良心の呵責や恐怖に駆られ、感染ユーザーのファイルをすべて復号したことはこれまでも数多くあるのです。つまり、望みは薄いかもしれませんが、このような運よくリカバリーできるかも知れません。また、ランサムウェアによっては、暗号化されたファイルの復号を可能にするツールが公開されることもあります。

## 身代金の交渉と支払い

身代金の支払いに関して最もよく聞かれる質問は、「お金を払ったら、これらの犯罪者は本当にファイルを復号する手助けをしてくれるのか？」というものです。この答えは少し複雑です。端的な答えはイエスで、ほとんどの場合、ファイルを復号する方法を提供してくれます（ランサムウェアのグループによって異なりますが）。結局のところ、攻撃者はお金が欲しいので、支払いを容易にするために迅速かつ的確なカスタマーサービスと技術サポートを提供します。

攻撃者はランサムウェアをビジネスとして行っています。ですから、被害者からお金を騙し取るだけで、ファイルを復号しないということがネットに公開されれば、その攻撃者(組織)にはお金を払っても無駄だと思われて“ビジネス”に悪影響が出ます。変な言い方ですが、攻撃者は被害者から確実に身代金を巻き上げる“ビジネス”を拡大する上で重要なのは、被害者が支払った時に、確実にファイルを復号してあげることなのです。

なお、このホワイトペーパーでは、身代金の支払いにビットコインで行われることを想定しています。ビットコインを入手し、適切な支払いを行うための手順を説明します。

## 身代金の支払い方法を見付ける

通常、ランサムウェアの画面の右側に手順へのリンクがあります。また、DECRYPT_INSTRUCTIONS.TXTの

ような名前のファイルが添付されるケースもあります。身代金の支払いは、この手順に従って、実行してください。あなたが感染したランサムウェアのバージョンに関わらず、支払い方法には3つの情報が記載されています。

- 支払額
- 支払い方法
- 身代金支払いまでの残り時間（カウントダウンタイマー）

上記の情報を入手したら、次は身代金の支払い方法を確認してください。

## ビットコインを入手する

最初のステップは、ビットコインを購入できるビットコイン取引所に口座を開設することです。これは他の日であれば簡単なことですが、身代金の支払い期限が迫っている可能性があるため、少し複雑になります。つまり、ビットコインを素早く入手できる取引所を見つける必要があります。万が一に備えてランサムウェアに感染する前に調べておきましょう。

- ビットコインの入手方法については、ランサムウェアに関するナレッジベース（英文）をご覧ください。

**注**：暗号通貨がビットコインでない場合は、ビットコインという単語を扱う暗号通貨に置き換えてください。

アカウントを作成すると、ウォレットアドレスが作成されます。これは、ビットコインを購入する相手に提供する必要があるアドレスです。ビットコインの実際の購入は、支払い方法が異なります。銀行口座とのリンクを求めるビットコイン取引所もありますが、通常、そのような取引所では取引間の待ち時間が長くなるため（新規口座の場合、最大4日間）、それらの取引が決済されるのを待つ時間がないかもしれません。http://www.LocalBitcoins.com のようなビットコインブローカーサイトを使用すると、現地の販売者と接続し、支払いタイプでフィルタリングすることができます。ビットコインを最速で入手するという点では、これが最善の策かもしれません。

お勧めとしては、価格の変動や取引手数料を考慮し、必要なビットコインよりも少し多めに（数ドル程度）購入することをお勧めします。

## TORブラウザーをインストールする (オプション)

TORブラウザーが何なのかご存じない方は、冒頭のTORとは何か、どのように機能するのかを説明したセクションをお読みください。機能的には、通常のWebサイトを閲覧するのと同じですが、若干の違いがあります。ちなみにTORブラウザーをダウンロードするには、http://www.torproject.orgのダウンロードボタンをクリックしてください。他のWebサイトからTORブラウザーをダウンロードしないでください。

TORブラウザーをインストールして開いてみると、見た目は他のブラウザーとほとんど変わりません。これにより、TORネットワーク上でホストされているサイトにナビゲートできるようになります。ランサムウェアの作成者は、TORネットワーク内の極めて一時的な場所にサイトをホストしていることが多く、支払い指示の中で支持されるそのサイトに移動するためにTORブラウザーを使用せざるを得ないことがあります。

通常、復号の指示やメイン画面で表示されるTORのWebサイトの「アドレス」は下記のように見慣れないものだと予め覚えておいてください。

**TOR Webサイトのアドレス例**

kprrj4jalkparf4p.onion/rqla7yulv7filqlrycpqrkrl.onion

## 身代金を支払う

ビットコインウォレットにビットコインがあり、復号プロセスが機能することを確認できたら、要求されたビットコイン額をランサムウェア攻撃者のウォレットに送金しましょう。通常、身代金の支払いには以下の情報の1つ以上が必要になります:

- 特定のランサムウェアの支払い情報を閲覧するためのWebアドレス(TORアドレスの可能性があります)
- ビットコインの送金に使用する攻撃者のビットコインウォレットID
- ランサムウェアによっては、ビットコインを攻撃者のウォレットに送金する際に生成される取引IDまたは「ハッシュ」ID

多くの種類のランサムウェアでは、身代金を支払うために特別に作成されたTORネットワーク上のページにアクセスする必要があります。TORブラウザーにサイトのWebアドレスを入力します。通常、サイトの指示に従って、ビットコインを送信する必要があるウォレットIDを見つけることができます。ウォレットIDは通常、数字と文字の長い文字列で、ランサムウェアの支払い指示または支払い説明画面のどこかに記載されています。

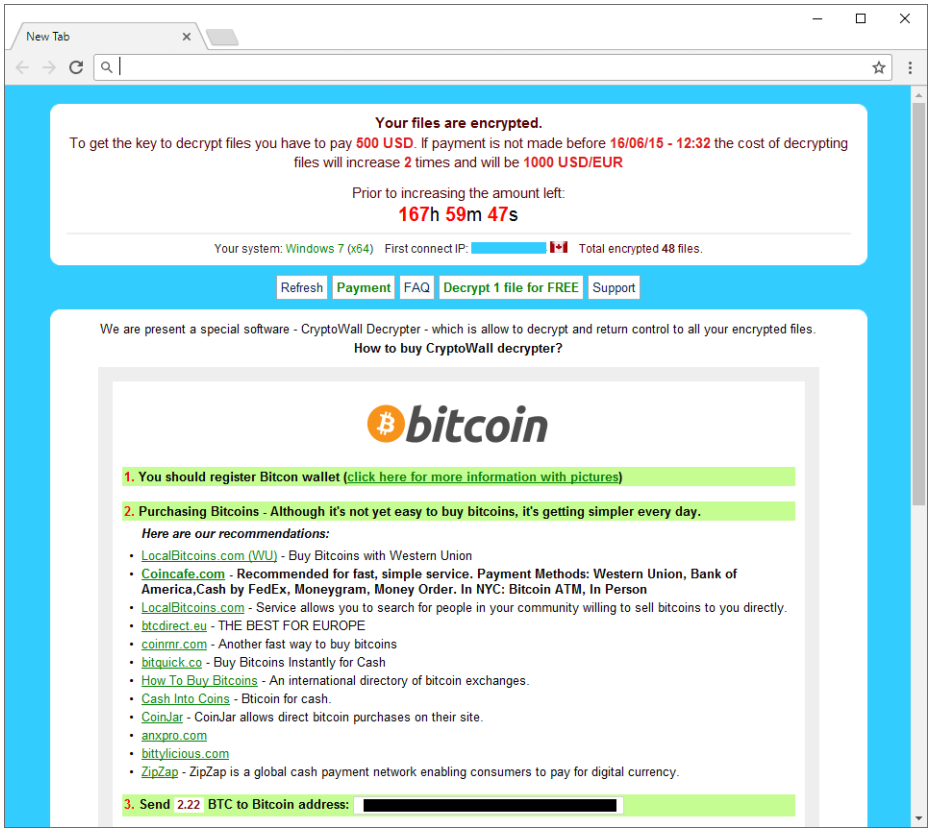
**ビットコインウォレットの文字列の例**:

19eXu88pqN30ejLxfei4S1alqbr23pP4bd

注:ランサムウェアのWebサイトにアクセスするとそこからカウントダウンが始まるので、準備ができるまで無闇にアクセスしないでください。攻撃者に追い立てられないようにするために注意してください。

ビットコイン取引所で自分のアカウントにログインし、ビットコインを攻撃者のウォレットに送金すると(これには20～40分ほど時間がかかる場合があります)、通常は取引確認ハッシュが発行されます。多くの場合、ビットコインを送信するだけで、攻撃者はファイルの復号キーを提供します。ランサムウェアのタイプによっては、取引ハッシュIDを攻撃者に提供する必要があります。ランサムウェアには通常、取引ハッシュIDを入力または貼り付けるフィールドがあります。

**CryptoWallランサムウェアの支払い画面の例**




## ファイルの暗号化を解除する

ビットコインを支払った後、攻撃者が入金を確認するまで（最大数時間）待つ必要があるでしょう。攻撃者が入金を確認したら、攻撃者はファイル復号用のキーを含むプログラムなど実行ファイルにアクセスできるようにしてきます。

**重要：この段階になったら、感染時に接続されていたすべての外付けドライブ、USBデバイス、ネットワークストレージを接続しアクティブにしておいてください。そうでないと、復号プログラムが対象ファイルを見つけられなくなってしまいます。共有フォルダーが感染時と同じパスになっていること、など複合対象へのアクセスができるようにしておきましょう。その他、外付けハードドライブやUSBデバイスも感染した時と同じパスになっていることを確認しておいてください。**

身代金を支払って復号キーやプログラムを入手しても、感染前の状態に復元できないファイルが発生することがあります。完全に復号されたとしても、異なる時期に暗号化されたために、ファイル間の同期が取れないことがあります。復旧プロセスには成功と失敗がつきものです。すべてのファイルを取り戻し、追加作業なしでランサムウェアによる暗号化以前と同じようにシステムが動作できる被害者は稀です。それでも、ファイルを復号できた被害者のほとんどは、身代金を支払わなかった場合に比べて、やるべき作業は大幅に少なくて済みます。もちろん、的確なバックアップを保有して、サイバー攻撃への備えを的確に実施している被害者は、身代金の支払いを拒否しても、タイムリーにファイルを復元して、現状復旧することが可能です。

# 9 予防措置：今後のサイバー犯罪の防止

ランサムウェアに限らず、サイバー攻撃からネットワークやシステムを守ることは、今や個人にとっても企業にとっ

ても、当然のことです。このステップは極めて重要です。ネットワークやシステムが攻撃されたのであれば、少なくとも犯した過ちから学び、予防措置は早急に講じてください。このような問題を二度と起こさないために、積極的な対策を実施することは必須です。今こそ、対策を総点検する時です。今やるべき行動計画を次に示します。

- **継続的なセキュリティ意識向上トレーニングを実施する**

  セキュリティ意識向上トレーニングはランサムウェア攻撃の根本原因の第1位であるソーシャルエンジニアリングへの対策として最も効果的です。フィッシング攻撃演習と組み合わせ実施することで、従業員のフィッシングメールへの防御が劇的に向上します。ランサムウェア攻撃がダウンタイムを引き起こす前に脅威を認識できるようにすることが極めて重要です。

- **多層防御を導入するだけでなく運用を改善し続ける**

  メールセキュリティやWebセキュリティ、EDR、新しいスタイルのセキュリティ意識向上トレーニングなどで多層防御を実現することはもちろんですが、問題を可視化して改善を続ける、運用を向上させることはさらに重要です。IT部門、一般従業員を含む人が運用の鍵だということを忘れないでください。

- **パッチのリリースから2週間以内に、すべてのパッチを適用する**

  未パッチのソフトウェアは、ランサムウェア攻撃の根本原因の第2位です。

- **攻撃対象領域の管理を徹底する**

  併せて、外部から攻撃可能なシステムの可視化と状態管理、サプライチェーンや人という攻撃対象領域の特定と管理を継続して行なってください。タブレットなどマルウェアの実行がほぼ不可能なデバイスに切り替え攻撃対象を削減したり、フィッシング演習で人的ファイアウォールを構築したりすれば、攻撃者の意欲を削ぐことにつながります。

- **適切なバックアップ/リストアソフトウェアを導入する**

  すべてのデバイスおよびシステムでバックアップを定期的に取り、リストア機能を定期的にテストしてください。

## セキュリティ意識向上トレーニング

ほとんどのランサムウェア攻撃は、不注意な従業員の1回のミスから始まっています。従業員の心理的な隙や低い警戒心が、安全上、最も脆弱な箇所になってしまうことを理解しておいてください。多くのITプロフェッショナルが証言しているように、フィッシングメールに含まれる怪しいポイントを事前に知っているだけで、従業員による悪意のあるリンクやソフトウェアを見抜く能力に大きな違いが生まれます。攻撃者やマルウェアの作成者が従業員を騙す手口は常に変化しているため、ITやメールセキュリティの基本だけでなく、常に変化する攻撃の手口や脅威についても、従業員に最新の情報を提供することが重要です。

しかし、「会計事務所」の給与振込担当者から給与計算スプレッドシートを送ってきたらどうでしょう？特に第4四半期給与明細.zipのような添付ファイルであればなおさらです。また、人事部は1日に20通の履歴書を受け取るかもしれませんが、インシデントを引き起こすために必要な悪意のある履歴書は1通あれば十分です。

攻撃者は、このような従業員の心の隙を狙う「ソーシャルエンジニアリング」を使って従業員を騙してサイバー攻撃を仕掛けてくるケースが増えています。KnowBe4のセキュリティ意識向上トレーニングと模擬フィッシング演習の組み合わせは、フィッシングメール内の怪しいポイントだけでなく、ソフトウェアベースの脅威・攻撃手法や物理的なセキュリティトレーニングまでもカバーしています。従業員セキュリティトレーニングは、基幹ネットワークを安全に守るために不可欠なものになってきています。

## 模擬フィッシング演習

セキュリティ意識向上トレーニングは第一次防衛ラインを強化する上で大きな効果を発揮しますが、セキュリティ

意識向上トレーニングに模擬フィッシング演習を組み合わせることで、従業員が常に高いセキュリティ意識を持たせることにつながります。

KnowBe4の模擬フィッシングキャンペーンでは、完全にランダム化され、完全にカスタマイズ可能な模擬フィッシング演習をお客様の環境内の任意の従業員に送信することができます。従業員一人ひとりがこのような攻撃を常に警戒することが重要です。結果として、すべての従業員が受信ボックスへ送られてくるすべてのメールに注意を払うようになります。人の心理を操るソーシャルエンジニアリングには、「セキュリティ防御技術」だけに頼ることはできません！ 模擬演習を通して、注意すべき怪しいポイントを学習することができます。模擬フィッシングメールを誤ってクリックしたら、どうなるかを模擬体験するで、怪しいメールを見極める能力は飛躍的に高まります。

模擬演習のもう1つの利点は、今起きている脅威に対する予防接種となることです。例えば、ランサムウェア攻撃者が実際に使用しているマルウェア付きメールやフィッシングメールを捉え、それを演習用メールとして使うことで従業員がどのように反応するかを事前に把握することができます。これにより組織内の脆弱な人をタイムリーに見つけて、その時点で世の中に発生している脅威について従業員一人ひとりに合わせて教育することができます。KnowBe4は、ランサムウェア攻撃の最新情報と、実際に起きているフィッシング攻撃のメールを訓練メールテンプレートに変換して提供しています。これによって、現実の攻撃に引っかかりやすい従業員をチェックすることを可能にしています。

## 要約

以下の4つのことを徹底するだけで、ランサムウェア攻撃だけでなく、様々なサイバー犯罪によるリスクを大幅に軽減することができます。

- ソーシャルエンジニアリングへの対策：セキュリティ意識向上トレーニングと模擬フィッシング攻撃演習
- ソフトウェアのパッチ
- 攻撃対象の管理
- 強固な認証

この他にも、コンピューターやネットワークを防御するために導入すべき緩和策は数多くあります。しかし、ほとんどの場合、これらの重要な4つの緩和策に十分に集中することができなかったことが、ほとんどのサイバー攻撃やランサムウェアが成功した要因です。

本書はランサムウェアへの対応計画に盛り込むべき一連の手順をまとめたものですが、的確な情報が提供されていることを心から願っています。貴社がランサムウェアの被害に遭うことがないことを祈りますが、万が一被害に遭われた場合に、本マニュアルをお読みいただければ、今後の対策、復旧、予防の方法を確認する一助となると考えております。

RESOURCES

KnowBe4

# Ransomware Attack Response Checklist
# ランサムウェア攻撃に対応するためのチェックリスト

**ステップ1： 調査初動**

- [ ] a. ランサムウェア攻撃なのかを判定する。
- [ ] b. 2つ以上のデバイスが攻撃されたのかを判定する。

全て該当すれば、ステップ2へ。

**ステップ2：ランサムウェア攻撃発生の宣言・インシデント対応の開始**

- [ ] a. ランサムウェア攻撃の発生を表明する。
- [ ] b. 事前に決めた代替のコミュニケーション手段を利用することを開始する。
- [ ] c. チームメンバー、上層部、法務部門へ連絡する。

**ステップ3：ネットワークの遮断**

- [ ] a. 即座にネットワーク接続を無効化する。
- [ ] b. データを消してしまうワイパー型のマルウェアが疑われる場合、即座にデバイスの電源を落とす。

**ステップ4：感染範囲の判定**

以下への影響を確認。

- [ ] a. 共有デバイス
- [ ] b. クラウドベースのストレージ： DropBox、Googleドライブ、OneDriveなど
- [ ] c. ネットワークストレージデバイス
- [ ] d. 外部ハードデバイス
- [ ] e. USBストレージデバイス (USBメモリー、メモリースティック、接続スマホ／カメラ)
- [ ] f. 他のコンピューターの共有フォルダー

**個人情報やログイン認証情報が盗難にあっていないかを特定する**

- [ ] a. ログ情報およびDLP（Data Loss Prevention）ソフトをチェックして形跡していないかを確認する。
- [ ] b. データをコピーするためにステージングファイルとして使用された可能性のある機密データを含む異常に大きなアーカイブファイル（zip、arcなど）がないか確認する。
- [ ] c. データの検索やコピーに使用された可能性のあるマルウェア、ツール、スクリプトを見付ける。
- [ ] d. ランサムウェアによるデータ盗難の確実な形跡である、個人データや認証情報を盗み出したことを告げる攻撃者からの通知。

RESOURCES

**ランサムウェアの感染経路を特定する**

- [ ] a. ランサムウェアの感染経路／タイプは何か？　例えば、Ryuk、Dharma、SamSamなど

## ステップ5：被害の極小化

- [ ] a. 検出された被害を最小限にとどめるて被害を可能な限り軽減する。

## ステップ6：セキュリティチーム・関係者を召集、現状を情報共有

- [ ] a. ここでの目的は被害の範囲や程度など、すべての情報をセキュリティ担当者および関係者間で共有し、正しく理解してもらうこと。

## ステップ7：対応策の決定

- [ ] a. 身代金を支払う、または支払わないか？
- [ ] b. 修復または再構築？
- [ ] c. 外部のセキュリティスペシャリストを依頼するか？
- [ ] d. 法的機関、関係政府機関へ連絡したか。

## ステップ8：原状回復

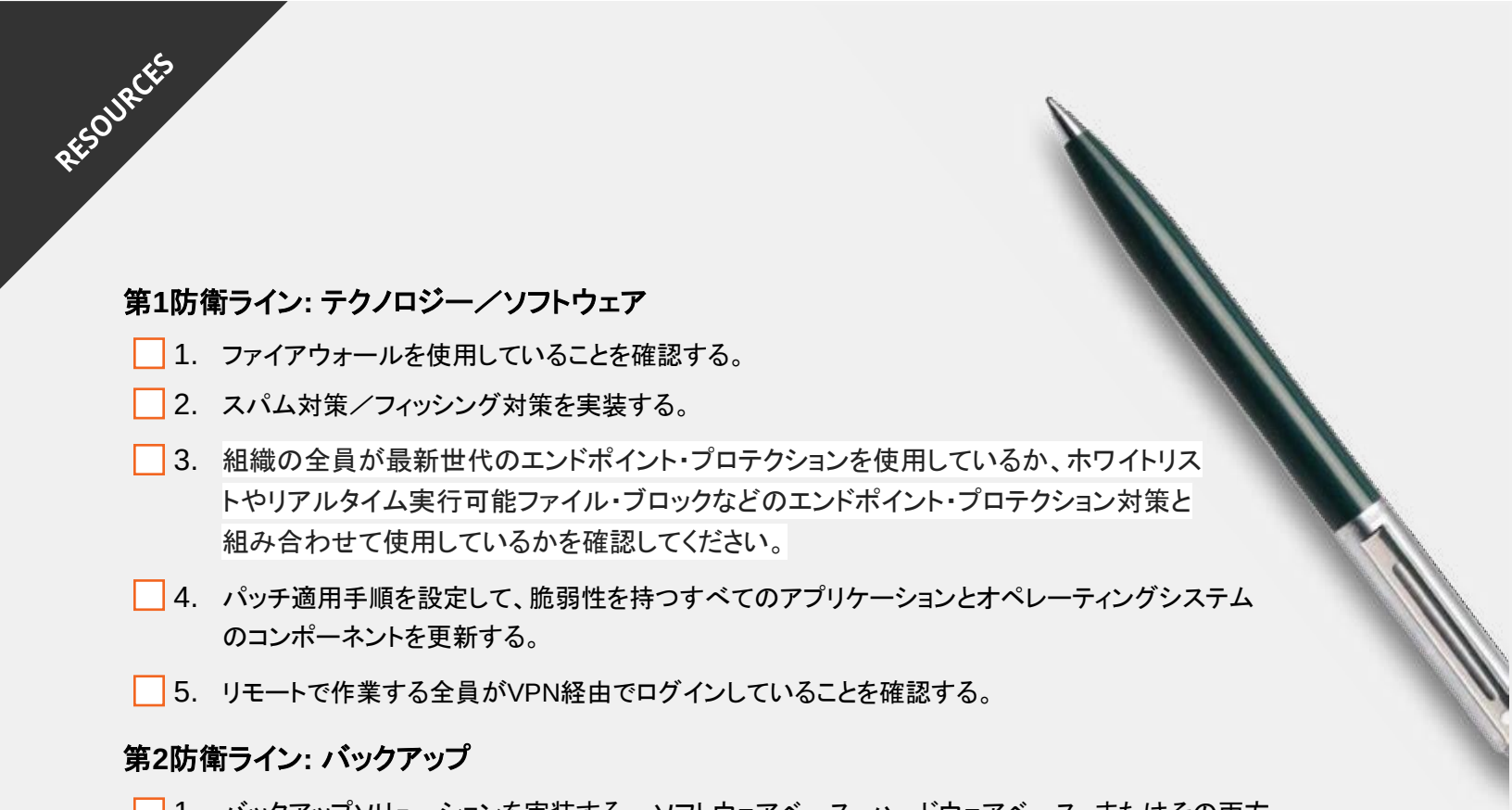
- [ ] a. 修復のみ、または修復と再構築？
- [ ] b. 証拠保全は必要か？
- [ ] c. ビジネスインパクト分析により、どのデバイスやシステムを復旧させるか、また、いつ実施するかを決定する。
- [ ] d. まずは、基幹インフラ／基幹システムの原状回復を実施する。

## ステップ9：予防措置

再発防止策。

- [ ] a. セキュリティ意識向上トレーニング／フィッシング攻撃演習など、ソーシャルエンジニアリング攻撃対策を実行する。
- [ ] b. 更新プログラムを必ずインストールする。
- [ ] c. 可能な限り、多要素認証（MFA）を実装する。
- [ ] d. アプリケーション毎に強力な異なるパスワードを設定する。
- [ ] e. ウイルス対策ソフト／ EDR（Endpoint Detection & Response）ソフトを利用する。
- [ ] f. スパム対策／フィッシング対策ソフトを利用する。
- [ ] g. DLP（Data Loss Prevention）ソフトを利用する。
- [ ] h. 定期的にバックアップを取り、テストする。

RESOURCES



## 第1防衛ライン: テクノロジー／ソフトウェア

- [ ] 1. ファイアウォールを使用していることを確認する。
- [ ] 2. スパム対策／フィッシング対策を実装する。
- [ ] 3. 組織の全員が最新世代のエンドポイント・プロテクションを使用しているか、ホワイトリストやリアルタイム実行可能ファイル・ブロックなどのエンドポイント・プロテクション対策と組み合わせて使用しているかを確認してください。
- [ ] 4. パッチ適用手順を設定して、脆弱性を持つすべてのアプリケーションとオペレーティングシステムのコンポーネントを更新する。
- [ ] 5. リモートで作業する全員がVPN経由でログインしていることを確認する。

## 第2防衛ライン: バックアップ

- [ ] 1. バックアップソリューションを実装する - ソフトウェアベース、ハードウェアベース、またはその両方。
- [ ] 2. モバイル/USBストレージを含む、アクセス・保存が必要なすべてのデータがバックアップされていることを確認する。
- [ ] 3. バックアップによる冗長化によって、データの機密性・完全性 ・可用性が確保されていることを確認する。
- [ ] 4. バックアップ/リストア手順のリカバリー機能を定期的にテストする。物理バックアップのデータ完全性とオンライン/ソフトウェアベースバックアップのデータリカバリーの容易性を、少なくとも過去3～4ヶ月間テストする。サイバー攻撃者は、数ヶ月間ネットワークに潜伏して、バックアップに違法アクセスすることがある。

## 第3防衛ライン：個人情報データ／ログイン認証情報盗難対策

- [ ] 1. DLP（Data Loss Prevention）ツールを利用する。
- [ ] 2. ファイル・フォルダー・データベースへのアクセス権限を限定する。
- [ ] 3. システムログを有効化して、データの移動をトラッキングする。
- [ ] 4. ネットワークトラフィック分析により、コンピューターやネットワーク上での異常なデータ移動を監視する。
- [ ] 5. データを暗号化し、不正コピーを防止する。

## 第4防衛ライン：「人」による防御 - ヒューマンファイアウォール

- [ ] 1 新しいスタイルのセキュリティ意識向上トレーニングを実施して、マルウェアなど悪意あるアプリのダウンロードや実行を防ぐために何を注意すべきかをユーザーに教育する。
- [ ] 2 5%～10%の悪意あるメールがメールフィルターをすり抜けている。セキュリティ意識向上トレーニングと並行して、少なくとも毎月1回、フィッシング攻撃演習を実践する。

## その他の関連情報

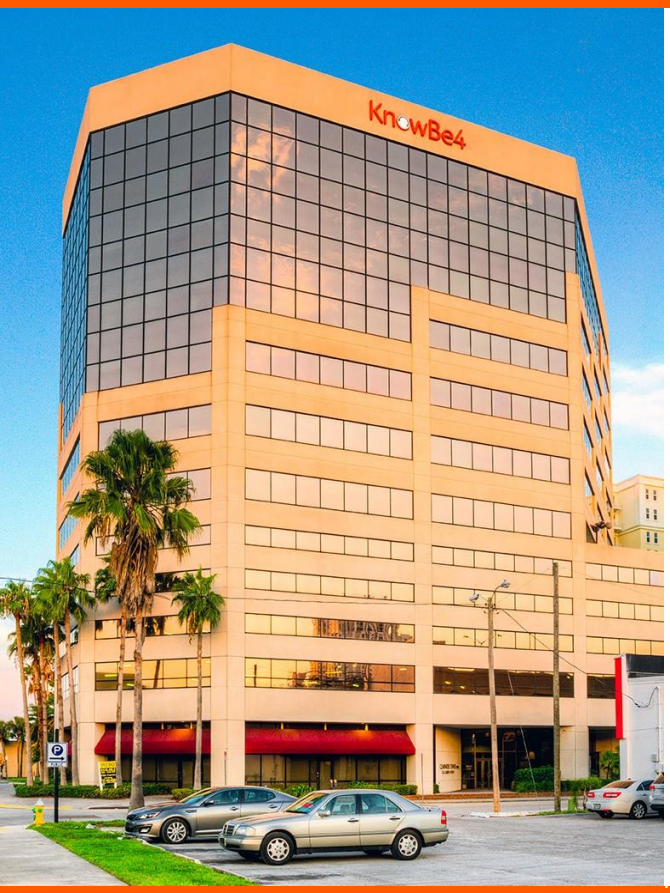
**フィッシングセキュリティテスト**
あなたの企業や組織の従業員の何パーセントがフィッシング攻撃に引っかかるかをスコア化することができます。.

**セキュリティプログラムビルダー**
あなたの企業や組織のためにカスタマイズされたセキュリティ意識向上プログラムの作成を自動化します。

**Phish Alertボタン**
あなたの企業や組織の従業員がフィッシング攻撃の報告をワンクリックで行うことができます。

**無償Email Exposure Checkツール**
あなたの企業や組織の従業員のメールアドレスが、どれくらいインターネット上で公開されているかをチェックできます。

**無償なりすましドメインテスト**
ハッカーがあなたの企業や組織のドメインのメールアドレスを偽装できるかをチェックできます。




## ＜KnowBe4について＞

KnowBe4は、セキュリティ意識向上トレーニングとフィッシングシミュレーション・分析を組み合わせた世界最大の統合型プラットフォームです。セキュリティの人的要素への抜本的な対策の欠如に気づき、KnowBe4は「人」を狙うセキュリティ脅威から個人、組織、団体を防御することを支援するため設立されました。

KnowBe4プログラムは、偽装攻撃によるベースラインテスティング、クラウドベースのインタラクティブなトレーニング、継続的なアセスメントを組み合わせた統合型のアプローチです。ここには、フィッシング、ビッシング、スミッシングといった多彩な偽装攻撃を通しての本番さながらのフィッシング体験とトレーニングがあります。セキュリティ第一のマインドセットを形成し、組織全体のセキュリティカルチャーを醸成します。

2020年7月現在、金融機関、製造業、エネルギー産業、医療機関、官公庁、生損保などで、3万3千社を超える企業や団体がKnowBe4を採用して、防御 の最終ラインとして「人」による防御壁を構築して、日々求められるセキュリティ上の的確な意志決定を可能にしています。

**詳しくは、www.KnowBe4.jp**をアクセスしてください。

KnowBe4
Human error. Conquered.

KnowBe4 Japan 合同会社　〒100-6510 東京都千代田区丸の内1－5－1
新丸の内ビルディング10F EGG 内
Tel: 03-4586-4540 | www.KnowBe4.com／www.KnowBe4.jp |