ランサムウェア対策

○　ランサムウェアとは

ランサムウェアは、パソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価（金銭や暗号資産）を要求する不正プログラムです。

○　よくある相談事例

＜相談事例１＞

パソコンの画面が急に制御不能になり「パソコンのファイルを暗号化した。戻すために、ビットコインを支払え。」などという内容の画面が表示された。無視してその画面を閉じたところ、パソコン上のファイルが次々と閲覧できなくなってしまった。

＜相談事例２＞

当社のサーバがウイルスに感染したようで、システムが利用出来なくなった。サーバを確認したところ、内部のファイル名が改ざん、暗号化されており、暗号化を解除するために金銭の支払いを要求された。

また、データの一部が流出しているようで、金銭を支払わなければデータをリークサイト（外部サイト）へ公開すると脅迫された。

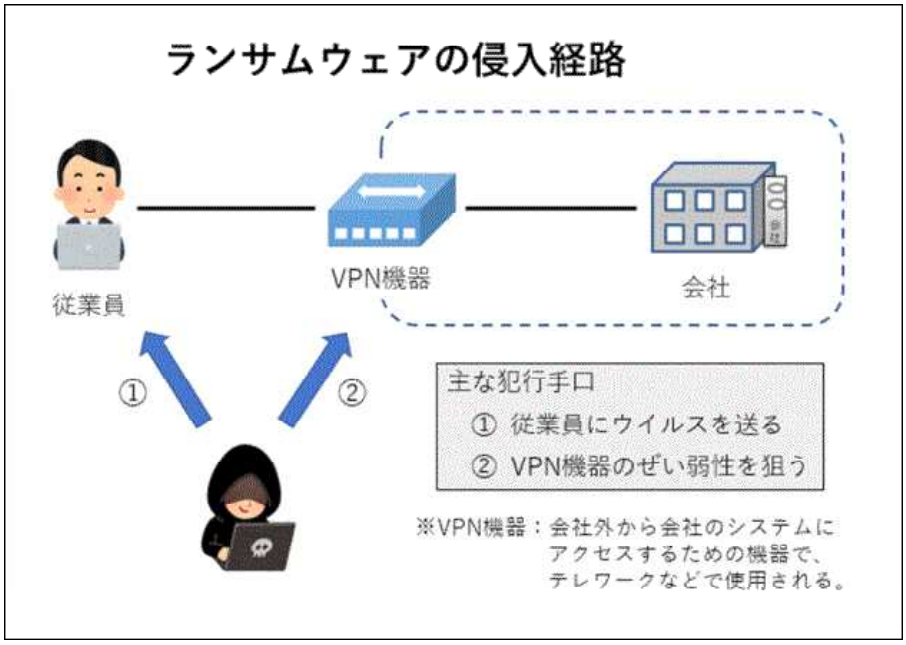
＜相談事例３＞

インターネットを見ていたら、英語で、「パソコンに保存されているファイルを暗号化したので、元に戻したければ１万ドル分の暗号資産（仮想通貨）を支払え。支払わなければ、コンピュータ内に保存されているデータを公開する。」というメッセージが表示された。

○　ランサムウェアの手口

従来のランサムウェアは、不特定多数の利用者を狙って電子メールを送信するといった手口が一般的でしたが、最近では、企業等の VPN 機器をはじめとするネットワーク機器のぜい弱性を狙って侵入する手口が多く確認されています。また、データの暗号化のみならず、データを窃取した上で、「対価を支払わなければデータを公開する」などと要求する二重恐喝（ダブルエクストーション）の手口が多く確認されています。

また、ランサムウェアによる被害のほか、データを暗号化する（ランサムウェアを用いる）ことなくデータを窃取し対価を要求する手口「ノーウェアランサム」による被害も確認されています。



○　感染が疑われたら・感染が確認されたら

(1) 感染したパソコン等をネットワークから隔離する

ランサムウェアの感染拡大を防止するため、感染したパソコンの LAN ケーブルを抜くなどして、ランサムウェアに感染したパソコンをネットワークから隔離してください。

感染原因等の調査に必要なログ等が消失する場合もあるので、**パソコンやネットワーク機器等の電源を落とさないでください。**

(2) 警察に通報・相談する

ランサムウェアの被害に遭った場合は、最寄りの警察署又はサイバー犯罪相談窓口（Tel：088-875-3110）に通報・相談してください。

警察署案内（https://police.pref.kochi.lg.jp/police-docs/2024012200010/）

(3) 感染原因等を調査する

被害の拡大防止・再発防止のため、ランサムウェアの感染原因等を調査してください。

他のマルウェアやハッキングツール等の影響を受けている可能性があるため、ランサムウェアの感染が確認されていないパソコンやサーバも含めて調査することを推奨します。

なお、調査に当たっては、感染したパソコンをはじめとした各種機器のログが必要となりますので、ログはバックアップデータと同様に適切に保管することを推奨します。

(4) VPN 機器等のぜい弱性を塞ぐ

利用しているネットワーク機器やパソコンの OS 等の更新ファイルを適用して、ぜい弱性を塞いでください。VPN 機器等のネットワーク機器のぜい弱性が悪用され、ネットワークに侵入された事例も多数確認されています。

(5)パスワードを変更する

攻撃者からアクセスされた可能性があるパソコン、サーバ、ネットワーク機器等のパスワードを速やかに変更してください。

（ぜい弱性対策を実施したにもかかわらず、パスワードの変更を怠ったために、ネットワークに侵入された事例も確認されています。）

(6)暗号化されたファイルを復号する

一部のランサムウェアについては、「No More Ransom」プロジェクトのウェブサイトで復号ツールが公開されています。復号ツールを利用することにより、暗号化されたファイルを復号できる場合がありますが、次の点に注意してください。

- 一部のランサムウェアにしか復号ツールが対応していないこと
- 復号ツールが利用できるランサムウェアとして紹介されていた場合であっても、バージョン等の違いにより、復号ツールが使えない場合があること

○　被害防止対策

ランサムウェアの被害に遭わないために、被害防止対策や被害軽減対策等について見直しを行うとともに、社員に対して適切なセキュリティ教育を行うなど、総合的な対策強化を図ってください。

(1)VPN 機器等のぜい弱性を塞ぐ

ネットワークへの侵入のために VPN 機器等のネットワーク機器のぜい弱性が悪用される事例が多数確認されています。また、OS やソフトウェアにぜい弱性が残っている状態では、電子メールの添付ファイルの実行やウェブサイトの閲覧により、マルウェアに感染する可能性があります。

利用している VPN 機器や OS 等の更新ファイル等を適用して、ぜい弱性を残さないようにしてください。

(2)認証情報を適切に管理する

利用している VPN 機器等のネットワーク機器やリモート・デスクトップ・サービスの認証パスワードがぜい弱であったためにネットワークに侵入され、ランサムウェアによる被害が生じる事例が確認されています。

パスワードが初期設定のままであったり、よく使用されているもの（「password」、「user0123」、「12345678」等）に設定されていないか確認し、そのような設定になっている場合は、大文字・小文字・数字・記号の組合せにより文字数が多く、推測されにくい文字列を設定するとともに、他のサービス等で使用していないものを設定し直すなど認証情報を適切に管理してください。

また、２要素認証等による強固な認証手段の導入や、IP アドレス等によるアクセス制限と組み合わせるなどといった対策も積極的に実施してください。

なお、パスワードが外部へ流出した可能性がある場合には、速やかにパスワードを変

更してください。

⑶ アクセス権等の権限を最小化する

いったんネットワークに侵入されると、ネットワーク内の複数のパソコンでデータが暗号化されるなど、被害の範囲が拡大することとなります。ネットワーク管理者はユーザに割り当てる権限やアクセス可能な範囲を必要最小限にしてください。例えば、一般ユーザに管理者権限を割り当てないようにしてください。

また、インターネットに公開しているサーバや機器が乗っ取られた場合に備えて、当該サーバ等からアクセス可能な範囲を限定してください。

⑷ ウイルス対策ソフト等を導入する

他のマルウェアやハッキングツール等を使ってネットワークに侵入し、データを窃取した後にランサムウェアによりファイルを暗号化する手口も確認されています。

ウイルス対策ソフトを導入し、定義ファイルを更新して最新の状態に保つことで、マルウェアやハッキングツール等を利用されるリスクを低減することができます。

⑸ 電子メール等を警戒する

受信者の関心を引くような内容や不安を煽る内容のメールを用いて添付ファイルを開かせる（実行させる）又はリンク先のウェブサイトにアクセスさせるように仕向けて、ランサムウェアをはじめとしたマルウェアに感染させる手口が確認されています。

知人や企業等からの電子メールと思えるものであっても､送信元が詐称されていたり、本文からは不正なメールと見抜けなかったりすることもあります。添付ファイル付きのメールやリンク付きのメールについては、送信元への確認を行うなど、その真偽を確かめ、不用意に電子メールの添付ファイルを開いたり、リンク先にアクセスしたりしないでください。

⑹ ネットワークを監視する

ランサムウェアを含めたマルウェア等に感染したパソコンでは、外部のサーバーとの間で不審な通信を行う場合があります。ネットワークに侵入されてしまった場合にネットワーク内の不審な挙動を検知し感染拡大や外部からの侵入の範囲拡大を阻止するため、EDR[*1]（Endpoint Detection and Response）の導入も検討してください。

また、侵入経路の特定のため、ネットワーク機器のログ等をはじめとする各種ログを保存してください。ログ等は、ランサムウェアにより暗号化される事例も多数確認されているため、オフラインで保存してください。

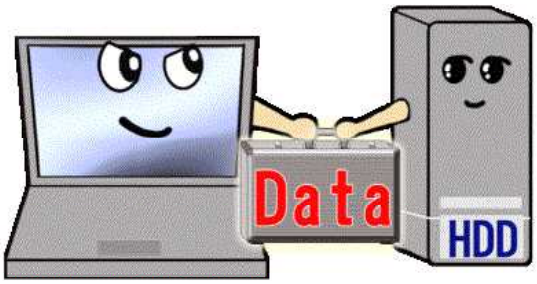
---

*1 EDR：ネットワーク上の機器を監視し、不審な挙動を検知した際に管理者に通知する機器やサービス

(7)データ等のバックアップを取得する

ランサムウェアにより、バックアップデータやログも暗号化されてしまう事例が確認されています。不測の事態に備えて、バックアップやログはなるべくこまめに取得し、ネットワークから切り離してオフラインで保存してください。

また、日頃からバックアップデータによるシステムの復旧手順を確認してください。



○　復号ツールについて

ランサムウェアによって暗号化されたファイルを復号するためには、感染したランサムウェアの種別を特定する必要があります。ランサムウェアを特定するために、ランサムノート（身代金を要求するドキュメント等）や暗号化されたファイルの拡張子を確認してください。確認した情報を基に、ランサムウェアに対応する復号ツールが「No More Ransom」プロジェクトのウェブサイトで公開されているか確認してください。

なお、「No More Ransom」プロジェクトのウェブサイトで公開されている復号ツールの使用方法については、JC3 のウェブサイトを参考にしてください。

- 「No More Ransom」プロジェクトの概要（外部サイト）
  （https://www.npa.go.jp/bureau/cyber/pdf/NO_MORE_RANSOM1.pdf）
- 「No More Ransom」プロジェクト（外部サイト）
  （https://www.nomoreransom.org/ja/index.html）

○　参考リンク

- **一般財団法人日本サイバー犯罪対策センター（ＪＣ３）**
  「ランサムウェア対策について」（外部サイト）
  （https://www.jc3.or.jp/threats/topics/article-375.html）
- **独立行政法人情報処理推進機構（IPA）**
  「ランサムウェア対策特設ページ」（外部サイト）
  （https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html）
  「情報セキュリティ・ポータルサイト「ここからセキュリティ！」（外部サイト）
  （https://www.ipa.go.jp/security/kokokara/）