ランサムウェアによる被害に遭わないために

ランサムウェア（Ransomware）とはコンピュータウイルスの一種で、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語です。「身代金要求型不正プログラム」とも呼ばれ、このウイルスに PC やサーバ、スマートフォンなどが感染すると、データが暗号化されたり、画面をロックされて端末が利用できなくなったりします。また、暗号化の解除を条件に金銭を要求されたり、情報を盗まれたうえにデータを暴露すると脅迫され、金銭の支払いの有無にかかわらず、データが暴露されてしまったケースが近年発生しており、特に組織を狙ったランサムウェアの攻撃が増加しています。

○ 感染経路

- メールから感染
  - メール本文中に表示された URL にアクセスすることで感染
  - メールの添付ファイルを開くことで感染
- ウェブサイトから感染
  - 偽サイトや細工された広告を閲覧することで感染
  - ウェブサイトからダウンロードしたファイルを開くことで感染
- OS の脆弱性を悪用され感染
  - 攻撃者が OS の脆弱性を悪用しウイルスを実行、その後、攻撃ツール等を利用しネットワークを通じて次々と感染
- 不正アクセスにより感染
  - 攻撃者が管理用のリモートデスクトップ（※あるパソコンに他のパソコンの画面を表示させて遠隔操作することができる仕組み）等でサーバに不正アクセス、その後、サーバ上でウイルスを実行

図 2-1 WannaCryptor に感染させられた端末の画面

（出典　IPA 独立行政法人情報処理推進機構）

対策

- **ウイルス対策の徹底**
  OS、アプリケーション及びウイルス対策ソフトは、アップデートにより、最新の状態を保つ。
- **データのバックアップ**
  定期的にクラウドサービス（※ユーザーがインターネット等のネットワークを通じてPCやスマートフォンから利用できるサービス）や外部メディア等にバックアップを行う。可能であれば複数のバックアップを行う。
- **不審なメールのリンクやファイルは不用意に開かない**
  メールのアドレスや本文を確認した上で、必要な場合のみ添付ファイルを開くようにし、素性が不明な者からのメールのリンクやファイルは不用意に開かない。
- **端末が感染した場合はネットワークから隔離**
  被害拡大防止のため、パソコンのLANケーブルを抜く、Wi-Fiの接続を切るなど、ネットワークから隔離する。
- **ウイルス駆除・データ復元**
  セキュリティソフトでウイルスを駆除した後に、バックアップデータからデータを復元する。
  ※ ランサムウェアの種類によっては、復号ツールで復旧できる場合もあります。
  ※ 復号ツールで復旧できない場合も、セキュリティ会社に依頼することで復旧できる場合があります。

岩手県警察本部サイバー犯罪対策課の公式ツイッターは QR コードから！！サイバー空間を悪用した犯罪の手口やサイバー犯罪の被害に遭わないための情報をお知らせしています。

@Iwate_cyber

岩手県警察本部生活安全部サイバー犯罪対策課

令和3年5月1日発行