滋賀県警察

サイバーセキュリティ滋賀

サイバー犯罪からあなたを守るセキュリティ情報をお届けします。

R８年度 No.23

ランサムハウス

RansomHouseを知っていますか？？

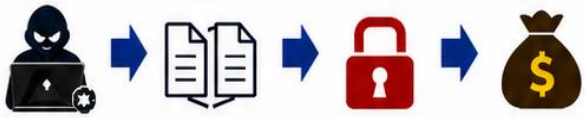
データを人質に脅迫！

日本企業も狙われる、分業化したランサムウェア犯罪

ランサムウェアは、パソコンやサーバーに侵入し、組織の重要なデータを**盗み出し、暗号化して**使えなくしたうえで、**身代金を要求する犯罪**です。

・データを元に戻してほしかったら、
・情報を公開されたくなかったら。
「身代金を払え」

攻撃の流れ（イメージ）



脆弱性の悪用やID・パスワードの窃取などで侵入

重要なデータを盗み出す

データを暗号化し、業務を停止させる

盗んだ情報の公開をちらつかせ、身代金を要求する

RansomHouseとは？

- 世界中の企業や団体を標的とするランサムウェアグループです。
- 2025年以降、日本企業への攻撃も確認されています。
- 盗んだ情報の公開をちらつかせる「二重の脅迫（ダブルエクストーション）」を行います。
- RaaS（Ransomware as a Service）として活動しています。

※攻撃された企業名は公表されていません。

RansomHouseだけではありません

ほかにも存在するランサムウェアグループ

Qilin（キリン）

RaaSとして活動する大規模グループのひとつ。世界中の組織を標的に。

The Gentlemen（ザ・ジェントルメン）

二重の脅迫を行うことで知られるRaaSグループ。さまざまな業種を攻撃。

Akira（アキラ）

2023年に登場したRaaSグループ。中小企業も標的に。

LockBit（ロックビット）

世界的に有名なRaaSグループ。過去に多くの被害事例が報告されている。

グループ名が変わったり、別のグループで活動することもあります。
常に新しい手口で狙ってきます。

今すぐできる対策

1. VPN・OS・ソフトウェアを最新の状態にする — 脆弱性を放置しない
2. 管理者権限を最小限にする — 必要な人だけ付与
3. 多要素認証（MFA）を利用する — ID・PWだけでは防げない
4. バックアップを取り、復元できるか確認する — 定期的に復元テストを！
5. 不審なログインや通信を早期に検知する — 監視・アラートを活用

被害にあったときは？

1. ネットワークから隔離する — LANケーブルを抜く・Wi-Fiを切る
2. むやみに電源を切らない — 調査に必要な情報が失われる場合があります
3. すぐに報告・相談する — 情報システム担当・保守事業者・警察などへ連絡する

「おかしい」と思ったら、自分だけで解決しようとしない。

早めの対応が、被害の拡大を防ぎます！

最新の手口や対策情報はこちらから

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）