

サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和6年
7月5日
Vol.113

⚠️ ランサムウェアに感染!? どうする!? ⚠️

ランサムウェアとは、パソコン等の端末やサーバ上の**データを暗号化**等して使用不可にし、それらの**復旧と引き換えに身代金を支払うように脅迫**メッセージを表示するウイルスの総称です。（※二重脅迫「支払わなければデータを公開する」も発生）



Vol. 111
「ランサムウェアに注意!」

以前公開した資料も
参考してください!



- 1 メールから感染させる。
- 2 Webサイトから感染させる。
- 3 脆弱性を悪用し、ネットワークから感染させる。
- 4 公開サーバに不正アクセスして感染させる。

例①: リモートデスクトップ経由による感染。

☞ メンテナンス用に外部からアクセス可能になっていた。
パスワードの総当たり攻撃により不正侵入されたものとみられている。

例②: Webサービスにリバースプロキシサーバを介して接続してADサーバに侵入。

☞ その後繰り返し不正侵入して社内情報を窃取。同サービスの脆弱性を悪用し、ランサムウェアを自動的に配布するバッチファイルを配置。

対策/対応

この時、感染端末の電源は
切らないでください!



侵入経路はVPNや 不審メールから!!

対策は?

- ① OSやソフトウェアは常に最新のバージョンに!!
- ② メール添付ファイルの不用意に開いたり、URLのリンクを開いたりしない!

情報管理規則の徹底や、
委託先等との契約内容も
確認しておきましょう。

万一の時のため、 普段からしておくべき

対策は?

- ① 定期バックアップ
→ オフラインで保存!!
- ② アクセスログなどの各種ログを保存!
- ③ インシデント発生時の対応要領・体制を確立し、職員に周知!!

もし被害に 遭ったら?

- ① **すぐに感染端末をネットワークから隔離しよう!**
- ② **至急セキュリティ担当者に報告を!!**
- ③ **速やかに警察へ通報・相談してください!**

相談窓口 ▶ 愛媛県警察本部サイバー犯罪対策課

TEL 089-934-0110(代)

