

サイバーセキュリティだより

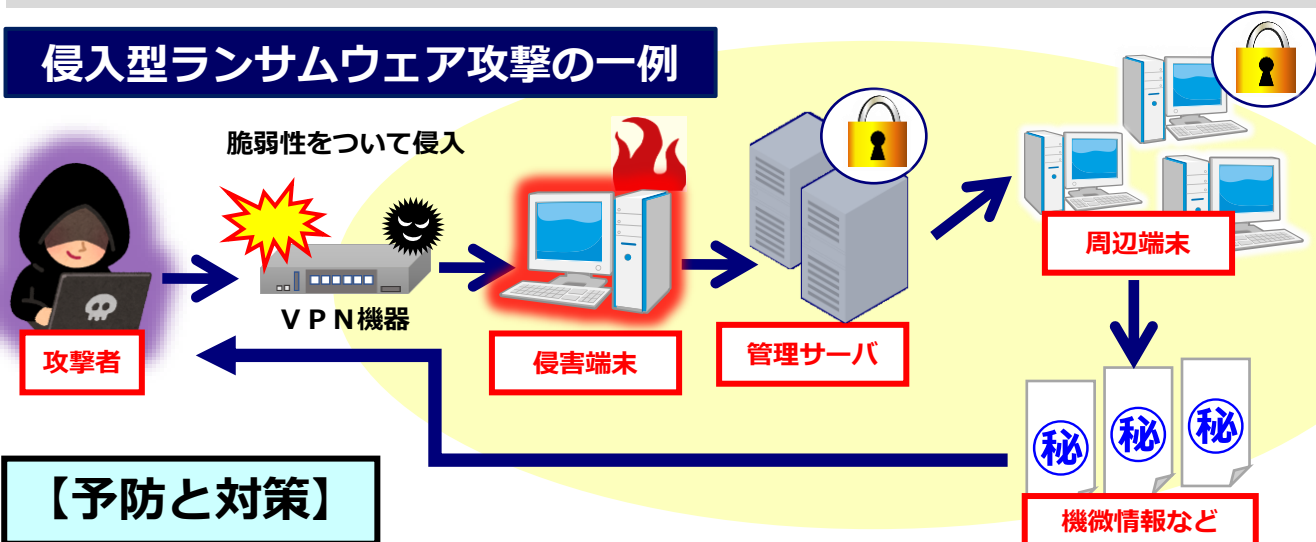
発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和6年
6月3日
Vol.111

!! ランサムウェアに注意!!

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）

侵入型ランサムウェア攻撃の一例



【予防と対策】

企業・組織のネットワークへの侵入対策

リモートデスクトップサービスの認証を突破されたり、VPN装置のアップデートが行われておらず、侵入された等の事例が多くあります。

VPN機器等の脆弱性を塞ぐ・認証情報を適切に管理する・アクセス権等の権限を最小化する・ウイルス対策ソフト等を導入する等の対策を執りましょう！

データ・システムのバックアップ

ネットワークサーバにバックアップサーバが接続されていると、バックアップサーバも被害に遭う可能性があります。

ファイルは定期的にバックアップし、バックアップに使用する装置・媒体はバックアップ時のみ対象機器と接続するようにしましょう。

★一部のランサムウェアについては、復号ツールが「No More Ransom(※)」のWebサイトに公開されており、暗号化されたデータを復号できる場合があります。

※「No More Ransom」は、ランサムウェアの被害低減を目指す国際的なプロジェクトです。



もしも感染したら、まずは何をすれば...!?

初動対応 ●**侵害を受けたシステム(端末)を切り離す**
●推測される侵入経路を調査・特定
(状況整理、影響範囲調査などを含む)

●**警察への通報**

侵害拡大防止 ●社内対応体制確保
●侵害を受けたシステムやアカウントの対応 等

～★侵害の進行段階に応じた対応が必要になります!～

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)

