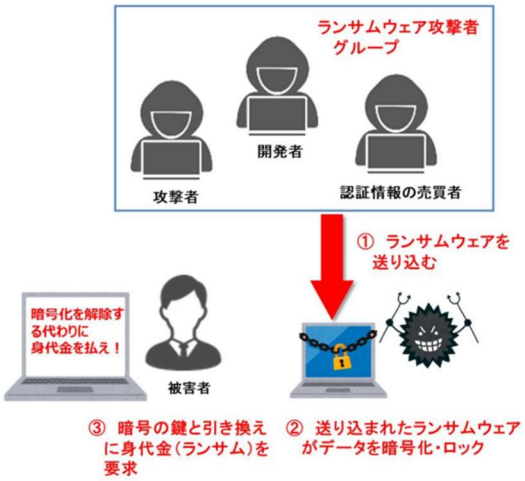
ランサムウェアにご注意を！！

ランサムウェアとは

ランサムウェアとは、端末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（金銭又は暗号資産）を要求する不正プログラムである。近年は、データを窃取した上、「対価を支払わなければ当該データを公開する」などと対価を要求する二重恐喝が被害の多くを占め、実際に事業者の財務情報や個人情報等が、ダークウェブ上のリークサイトに掲載される事例が多数確認されている。また、ランサムウェアで暗号化することなく、データを窃取した上で機密情報等の公開を予告して対価を要求する手口も発生している。

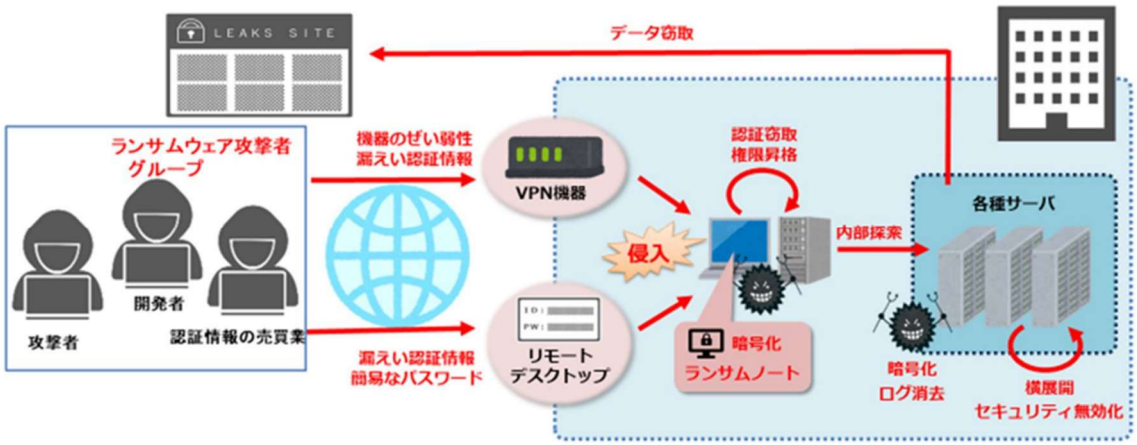
【ランサムウェア攻撃の概要】



ランサムウェアの手口

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あったが、近年では、企業等のVPN（Virtual Private Network）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る。攻撃者は、未修正のぜい弱性、漏えいした認証情報や簡易なパスワード、設定不備等を悪用して組織のネットワークへ侵入する。そして、より広い領域にアクセスするために管理者権限の奪取やセキュリティ無効化を試みながら、ネットワーク内部を探索して重要データやバックアップを物色する。一通り内部探索を終えると、データをクラウドストレージ等へアップロードして窃取した後、ランサムウェアを起動して暗号化を実行する。復旧を妨害するため、バックアップも一緒に暗号化される場合が多い。最後に、「脅迫状（ランサムノート）」をデスクトップ等に保管して攻撃者側への連絡と身代金の支払を要求し、ログや使用したツール等の痕跡を消去して攻撃を終了する。

【ランサムウェア攻撃の流れのイメージ】



※警察庁「令和7年における サイバー空間をめぐる脅威の情勢等について」より

予防と対策

・VPN機器等のぜい弱性を防ぐ（アップデート等）
・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
・電子メール等を警戒する
・ネットワークを監視する
・データ等のバックアップを取得する

被害発生時は
警察へ通報・相談を！

本件問い合わせ先
千葉県警察本部生活安全部
サイバー犯罪対策課対策係
電話番号　043-201-0110