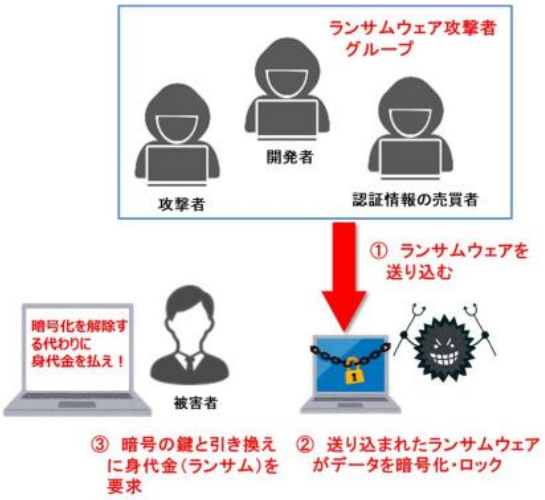
サイバー攻撃対策通信

令和７年10月10日
令和７年度第６号
栃木県警察本部
警備部警備第一課
（サイバー対策センター）

令和７年上半期における脅威の情勢

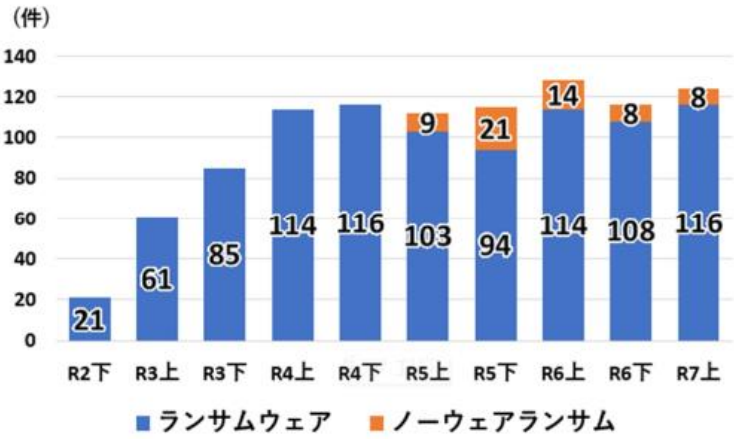
ランサムウェア攻撃の流れと被害報告件数

【ランサムウェア攻撃の流れ】



●企業・団体等における被害の報告件数の推移

※　ノーウェアランサム：暗号化することなくデータを窃取した上で、対価を要求する手口。令和５年上半期から集計。



攻撃の態様としては、ランサムウェアの開発・運営を行う者が、攻撃の実行者にランサムウェア等を提供し、その見返りとして身代金の一部を受け取るもの（RaaS：Ransomware as a Service）も確認されている。

業種別報告件数・復旧期間と費用

●被害企業・団体等の規模別／業種別報告件数

●復旧等に要した期間／調査費用の総額／復旧期間と費用の関係性

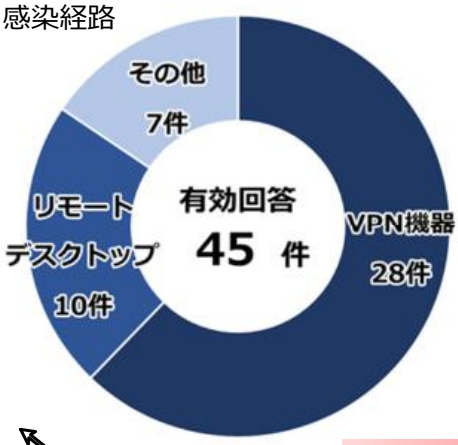
組織規模別のランサムウェア被害件数は、前年と同様に中小企業が狙われる状況が継続しており、被害件数の約 3 分の 2 を占めて件数・割合ともに過去最多となった。

栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER

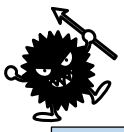
感染経路と手口別件数

ランサムウェア被害にあった企業・団体等へのアンケート調査の回答結果

●感染経路



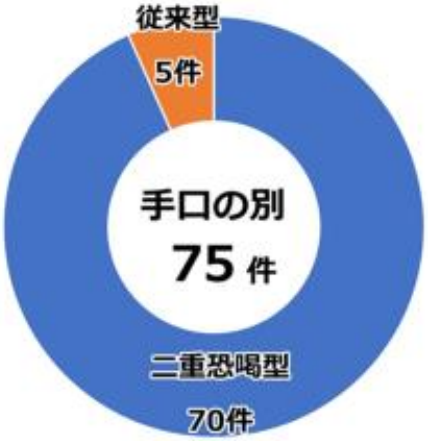
感染の原因は、当該機器の ID・パスワード等が非常に安易であったことや、不必要なアカウントが適切に管理されずに存在していたことなどが挙げられる。



サイバー特別捜査部による分析

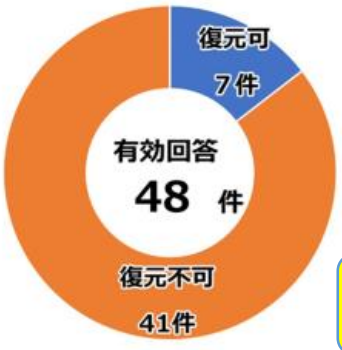
近年は、データを窃取したうえ、「対価を支払わなければ当該データを公開する」などと対価を要求する**二重恐喝**の被害も多くみられる。

●手口別報告件数

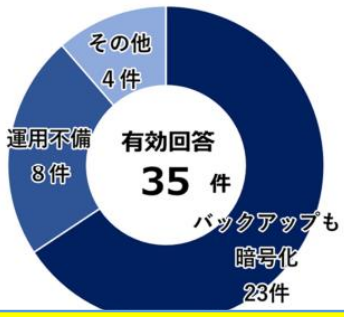


バックアップの取得・復元結果

●バックアップの取得状況／バックアップからの復元結果



●バックアップから復元できなかった理由



日頃からのログの取得・保管やバックアップのオフライン環境での保管といった対策が求められる。

ランサムウェアグループは身代金を得るために日々策を講じている。

【例】

- **土日が休業日の企業を狙う場合に、金曜日の営業終了後にシステムに侵入して月曜日の朝までに暗号化を実行する。**
- **被害企業に侵入口を閉じられた場合でも再侵入できるように、遠隔操作可能なソフトウェアをバックドアとして設置する。**
- **侵入時の痕跡を消したり、復旧作業をさせないために、被害企業のログやバックアップを消去する。**

出典：警察庁「令和７年上半期におけるサイバー空間をめぐる脅威の情勢等について」

栃木県警察サイバー対策センター
TOCHIGI POLICE
CYBERCRIME CONTROL CENTER