KBCS だより
令和7年 No.6

令和7年上半期のサイバー情勢について

警察庁は本年９月、サイバー空間の脅威の情勢を示す指標、事例等を紹介する広報資料「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」を公表しました。

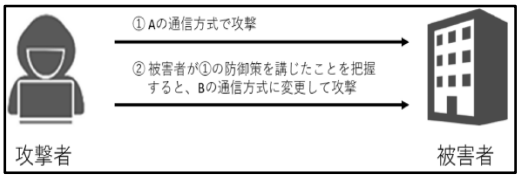
■高度な技術を悪用したサイバー攻撃の脅威情勢

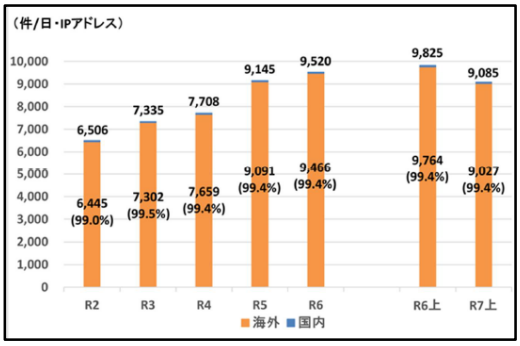
○　政府機関や金融機関等の重要インフラ事業者等におけるDDoS 攻撃とみられる被害や、情報窃取を目的としたサイバー攻撃等が相次ぎ発生

- 金融機関等に対するDDoS 攻撃被害とみられるウェブサイトの閲覧障害（令和６年12 月下旬から令和７年１月上旬）
- 保険大手企業に対するランサムウェア攻撃事案（２月）
- 研究開発機関に対する情報窃取目的とみられるサイバー攻撃（３月）
- 大手システム事業者に対する情報窃取目的とみられるサイバー攻撃（４月）
- 電力事業者に対する情報窃取目的とみられるサイバー攻撃（４月）
- 国際総合物流企業に対するランサムウェア攻撃（４月）
- 政府機関等に対するDDoS 攻撃による被害とみられるウェブサイトの閲覧障害（６月）

○　令和７年上半期に警察庁が設置したセンサーにおいて検知したぜい弱性探索行為等の不審なアクセス件数は、１日・１IP アドレス当たり9,085.4件（前年比7.5%減）と、引き続き高水準で推移（その大部分が海外を送信元とするアクセス）

〈年末年始にかけての重要インフラ事業者等に対するDDoS 攻撃の手口】〉





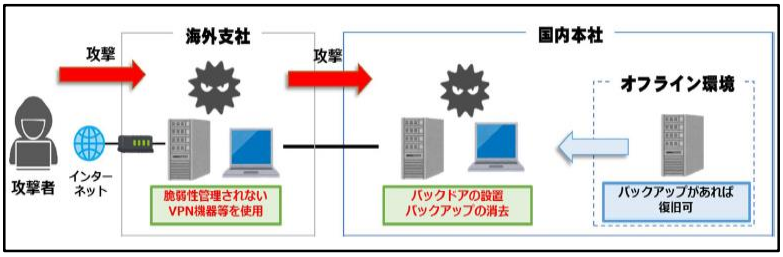
■ランサムウェア被害の概要と被害件数

○　令和７年上半期におけるランサムウェアの被害報告件数は116 件であり、半期の件数として令和4 年下半期と並び最多（右図参照）

○　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、77件で約3分の2 を占めて件数・割合ともに過去最多

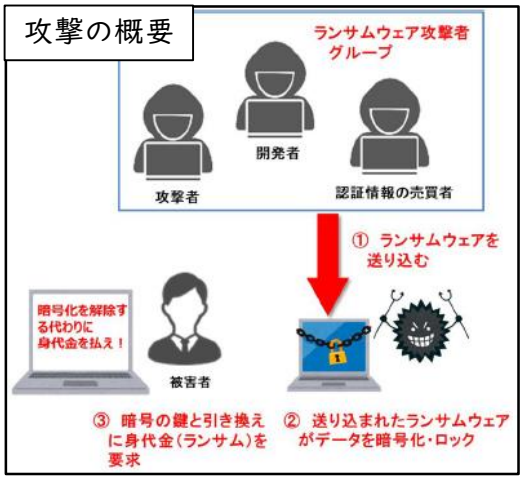
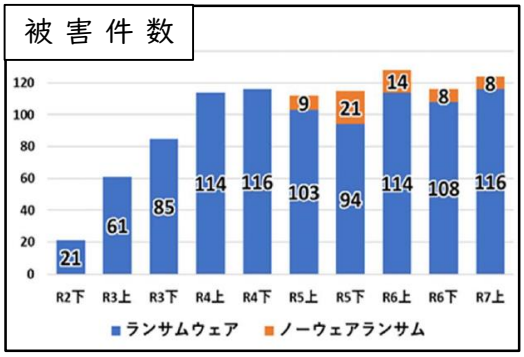
○　令和６年と比較して、ランサムウェアの被害による調査・復旧費用が高額化しており、1,000 万円以上を要した組織の割合は、50%から59%に増加

〈海外支社等の機器から侵入され、国内の本社が被害に遭う事例〉



☑ログは被害企業が侵入の実態調査やバックアップからの復旧対応を行う際に必要です。ログが保存されていない場合、適切な対策を講じることができず、バックアップからの復旧対応にも支障を及ぼすおそれがあります。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、サイバー攻撃を想定した業務継続計画（BCP）の策定といった対策をしましょう。

攻撃の概要



被害件数