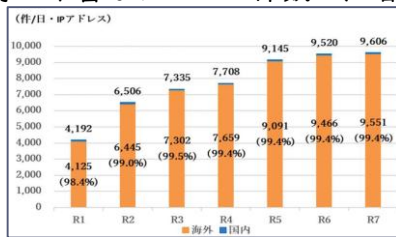


令和7年におけるサイバー情勢について

警察庁は本年3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。

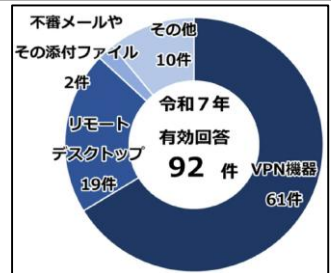
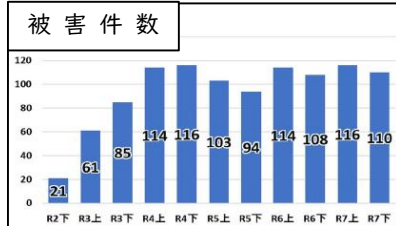
■ 高度な技術を悪用したサイバー攻撃の脅威情勢

- 令和7年において、国家を背景とするサイバー攻撃グループ（APT 攻撃グループ）の関与が疑われるものが複数存在、特に情報窃取を目的としているとみられるサイバー攻撃が確認
- 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、増加の一途をたどり、その大部分の送信元が海外（右図参照）
- 【令和7年における主なサイバー攻撃事例】
 - ・ 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）
 - ・ 機器製造業者に対する情報窃取目的とみられるサイバー攻撃（6月）
 - ・ 情報通信事業者に対する情報窃取目的とみられるサイバー攻撃（7月/11月）
 - ・ 教育機関に対する情報窃取目的とみられるサイバー攻撃（12月）



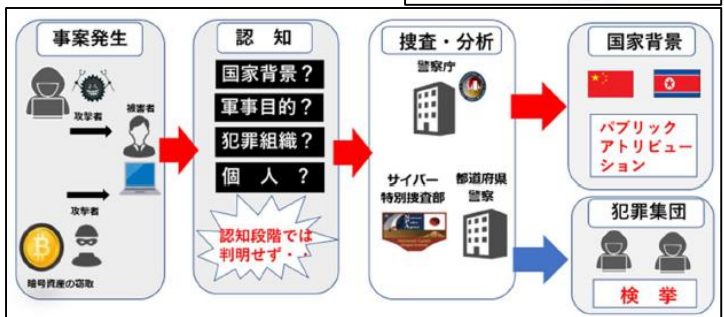
■ ランサムウェア被害の概要と被害件数

- 令和7年におけるランサムウェアの被害報告件数は **226件**
 - ・ 保険大手企業の自社サーバに対するランサムウェア攻撃（2月）
 - ・ 国際総合物流企業の自社サーバに対するランサムウェア攻撃（4月）
 - ・ 飲料メーカー大手の自社サーバに対するランサムウェア攻撃（9月）
 - ・ 通販大手の自社のサーバに対するランサムウェア攻撃（10月）
- 被害企業について、組織の規模別で見ると、前年と同様に **中小企業が約6割**。業種別では、製造業が約4割を占め、続いて卸売・小売業、サービス業、情報通信業が上位
- ランサムウェア被害に関する調査費用、復旧費用は高額化。**復旧に総額1,000万円以上**を要した組織の割合は**全体の5割超**、復旧に要した期間については、1か月未満で復旧した組織の割合は全体の5割強
- **侵入経路はVPN（Virtual Private Network）機器が6割以上**



■ 国家安全保障における警察の果たす役割等

- サイバー攻撃は、その性質上、事案発生時点では、その攻撃主体や目的等を即座に判断できるものではないため、**全てのサイバー事案が安全保障に直結する事案である可能性も見据え**ながら、捜査権を有する警察が事案の捜査を行うとともに、実態解明を推進。
- 【パブリック・アトリビューション】
令和7年8月、警察庁及び国家サイバー統括室(NCO)は、米国、オーストラリア、ニュージーランド等と共に、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリーの共同署名を行い、パブリック・アトリビューションとして、本件アドバイザリーを公表。
- 【能動的サイバー防御（ACD）】



令和7年5月、第217回国会において、サイバー対処能力強化法及び同整備法が成立。強化法及び整備法は、「官民連携の強化」、「通信情報の利用」及び「攻撃者のサーバ等へのアクセス・無害化措置」の3つを取組の柱としており、警察関係では、整備法により、警察官職務執行法の一部が改正され、サイバー攻撃による重大な危害を防止するための警察によるアクセス・無害化措置を可能とする規定が新たに制定。同規定は、令和8年10月1日に施行される予定。

異常を検知すれば、警察へ速報をお願いします

京都府警察本部モノづくりプリアーブ事務局 075-451-9111

