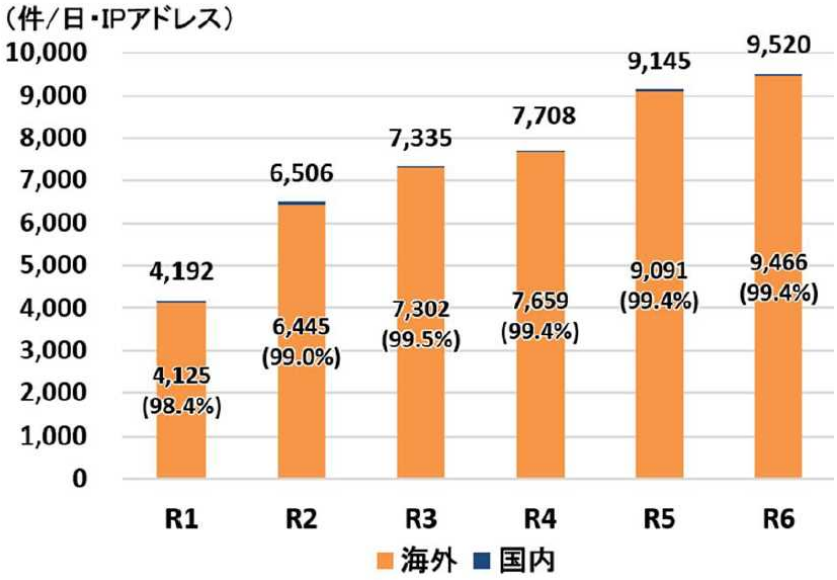
# 令和６年における
# サイバー空間をめぐる脅威の情勢等について（抜粋）

## 高度な技術を悪用したサイバー攻撃
### ～ぜい弱性探索行為等不審なアクセス件数の増加～

サイバー攻撃の準備として、攻撃者は攻撃対象を事前に探索する場合があるところ、令和６年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**※1の不審なアクセス件数は１日・１IPアドレス当たり9520.2件と平成23年以降、増加の一途をたどっており、(前年比4.1%増)その大部分が海外を送信元とするアクセスで占められている。

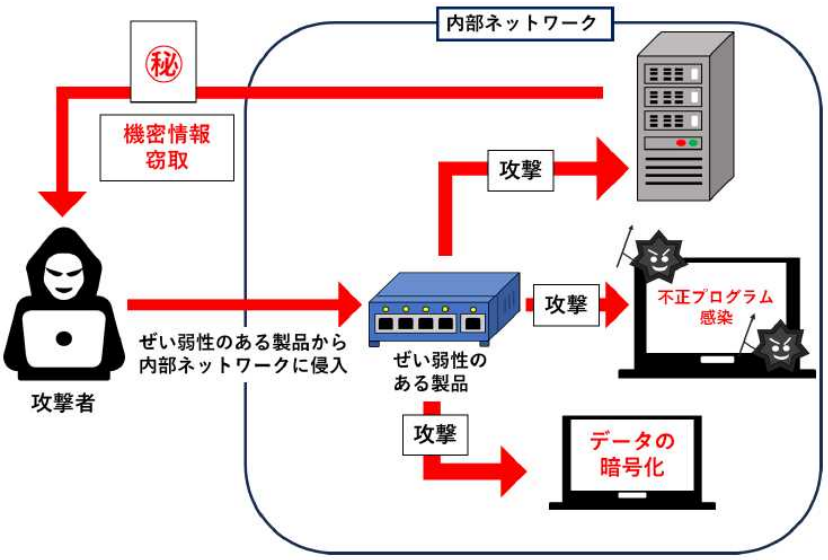
※１「ぜい弱性探索行為等」とは、システムの中で攻撃可能な部分を探すことで、サイバー攻撃の前段階に行われるもの。

【１日・１IP アドレス当たりのアクセス件数の推移】




### 【ぜい弱性を放置することの危険性】

攻撃者は、**ぜい弱性があるネットワーク機器を攻撃の足掛かりとして、内部ネットワークに侵入**し、サイバー攻撃を行うため、そのぜい弱性を放置することなく、平素から**ぜい弱性情報やアップデートに関する情報を確認**し、対処することが必要である。




### ～ぜい弱性が悪用された事例～

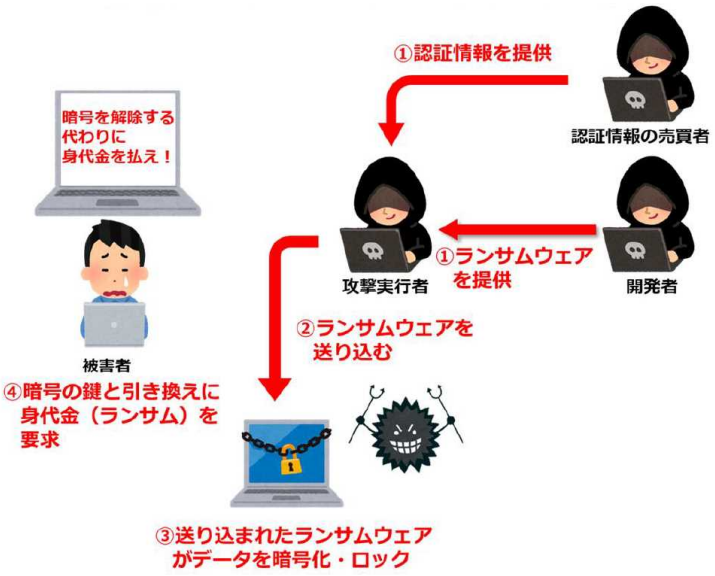
令和６年７月、国内の宇宙航空分野の研究開発機構は、**VPN装置のぜい弱性を起点とする不正アクセス**により、侵害を受けた端末、サーバ及びクラウド上で管理していた情報の一部が漏えいしたことを発表した。

# 犯罪組織等によるサイバー攻撃
## ～ランサムウェアによる攻撃～

ランサムウェア被害件数を組織規模別に令和５年と比較すると、大企業の被害件数が減少する一方、**中小企業の被害件数は37％増加**した。これは、RaaS※2による攻撃実行者の裾野の広がりが、対策が比較的手薄な中小企業の被害増加につながっていると考えられる。

※2「RaaS」とは、Ransomware as a Serviceの略でランサムウェアによる攻撃をサービスとして提供・実行するビジネスモデル

【ランサムウェア攻撃の流れ】




## ～ランサムウェアに関する事例～

令和６年６月、出版大手企業は、同社のサーバがランサムウェアを含む大規模な攻撃を受けたと発表した。同社は、**この攻撃により25万人分を超える個人情報や企業情報が漏えい**したことが確認されたこと及び同年度決算において、**調査・復旧費用等として20億円を超える損失を計上**する見込みであることを発表した。

# 被害の未然防止・拡大防止に向けた取組
## ～国際連携を通じた情報発信～

● 令和６年12月、警察庁は米国連邦捜査局(FBI)及び米国国防省サイバー犯罪センター(DC3)とともに、**北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」**が暗号資産関連事業者から暗号資産を窃取したことを特定し、合同で文書を発出した。

● 令和７年１月、警察庁は**「MirrorFace」**と呼称されるサイバー攻撃グループが、国内の組織、事業者及び個人に対して、マルウェアを添付したメールの送信や、ソフトウェアのぜい弱性を悪用した標的ネットワーク内へ侵入により、情報窃取を目的としたサイバー攻撃を行っていることを確認した。

さらにこれらの攻撃が**中国の関与が疑われる組織的なサイバー攻撃活動であると評価**し、同グループの手口や未然防止対策等に関する注意喚起を実施した。

出典：警察庁ホームページ「令和６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」
https://www.npa.go.jp/publications/statistics/cyversecurity/data/R6/R06_cyber_jousei.pdf

長崎県警察