としまる※ 自己紹介

JCA-NETでコミュニケーションの権利運動に関わる。

https://jca.apc.org

ブログ ne plu kapitalismo / 反監視情報

https://www.alt-movements.org/no_more_capitalism/

https://www.alt-movements.org/no_more_capitalism/hankanshi-info/

※ 以前は「小倉利丸」と名乗っていました。

サイバー攻撃の変遷

- サイバー攻撃は巧妙化・深刻化するとともに、サイバー攻撃関連通信数や被害数は増加傾向にあり、**質・量両面でサイバー攻撃の脅威は増大**している。
- 令和６年中に観測された**サイバー攻撃関連の通信の99%以上が海外から発信**[*1]

*1出典:警察庁資料。令和６年中に警察庁が観測したサイバー攻撃関連の通信（ダークネット向けの攻撃通信を含むパケット）の99.4%が海外のIPアドレスを発信元とするもの。

サイバー攻撃関連通信や被害の量

NICT [*2]が観測したサイバー攻撃関連通信数の推移

*2 国立研究開発法人 情報通信研究機構（National Institute of Information and Communications Technology）の略。
*3 １度に届くデータの塊のこと。センサーがデータを受信した回数と同義。

サイバー攻撃の巧妙化・深刻化

サイバー安全保障に関わる攻撃例

IT系システムの侵害

（暗号化・システム障害、身代金要求）

（例：2021年米コロニアルパイプライン業務停止、2022年大阪急性期・総合医療センターの業務停止、2023年名古屋港業務停止）

＋

有事に備えた重要インフラ等への侵入

（高度な侵入・潜伏能力）

（例：2014年クリミア併合、2022年ウクライナ侵略、2023年VoltTyphoonによるグアム等にある米軍施設や政府機関、重要インフラへの侵害）

＋

機微情報の窃取

（アクセス権限の獲得）

（例：2021~24年JAXAへの侵害、2023年NISCのメール窃取）

https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/setsumei.pdf

左のスライドは2025年内閣官房国家サイバー統括室「サイバー対処能力強化法及び同整備法について」のスライドから。

このスライドに記載されている「サイバー攻撃関連通信や被害の量」という見出しに注目すること。

脅しのテクニック：13秒に1回の攻撃!?

「サイバー攻撃関連通信や被害の量」と見出しをつけ、右側の説明で攻撃例を記載することで、14秒に1回攻撃があり被害になっている、と誤解されるような記述になっている。

自分達では防御できない問題だという印象を与える
「攻撃」=国家安全保障問題=自衛隊や警察などの対応が必要という印象を与える
国家安全保障に関わるから、被害の当事者である企業や通信事業者は協力すべき

サイバー攻撃を監視する必要⇒実際は私たちのネットでのコミュニケーション
を網羅的に監視することになる。

実際の被害と原因

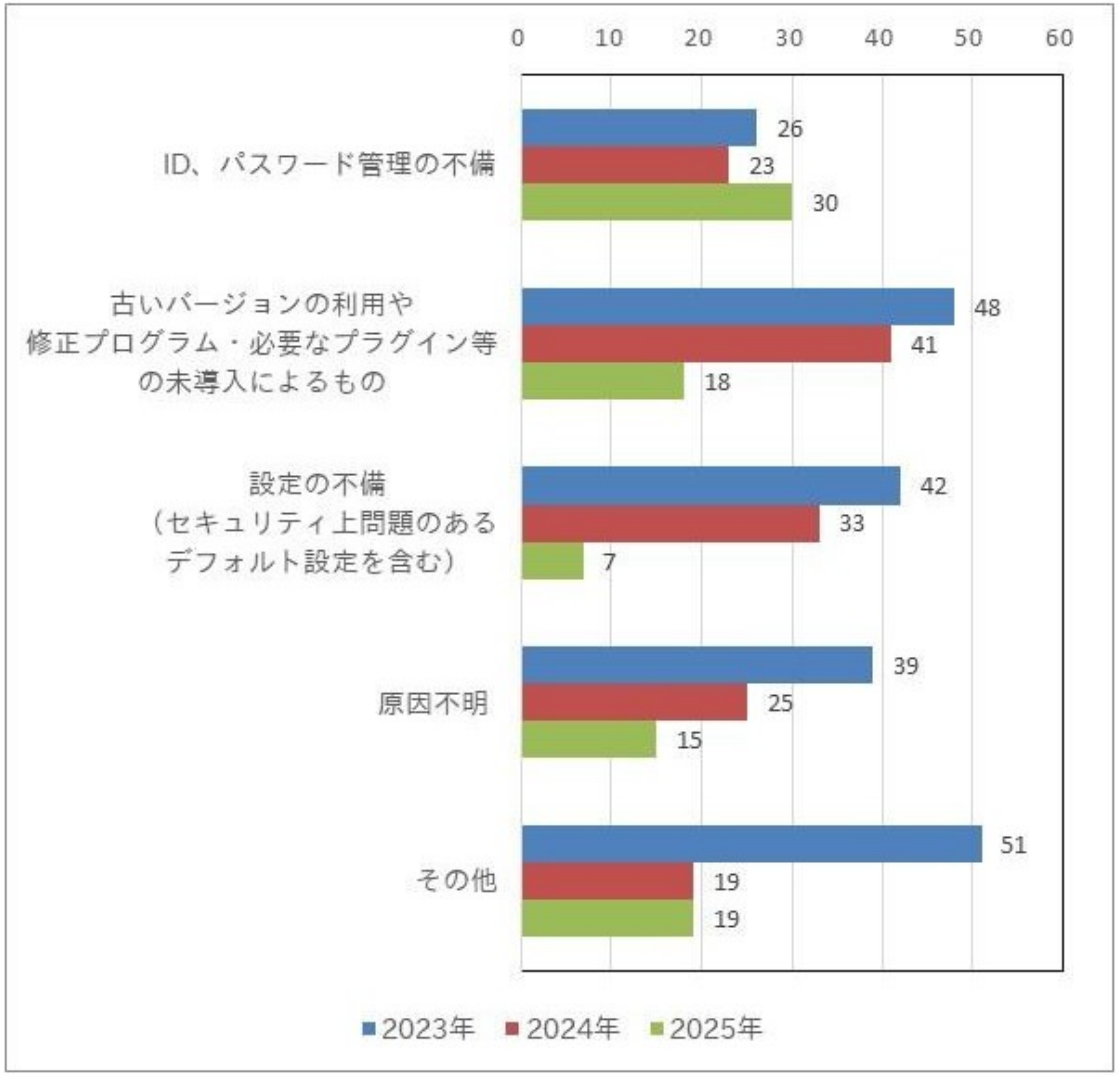


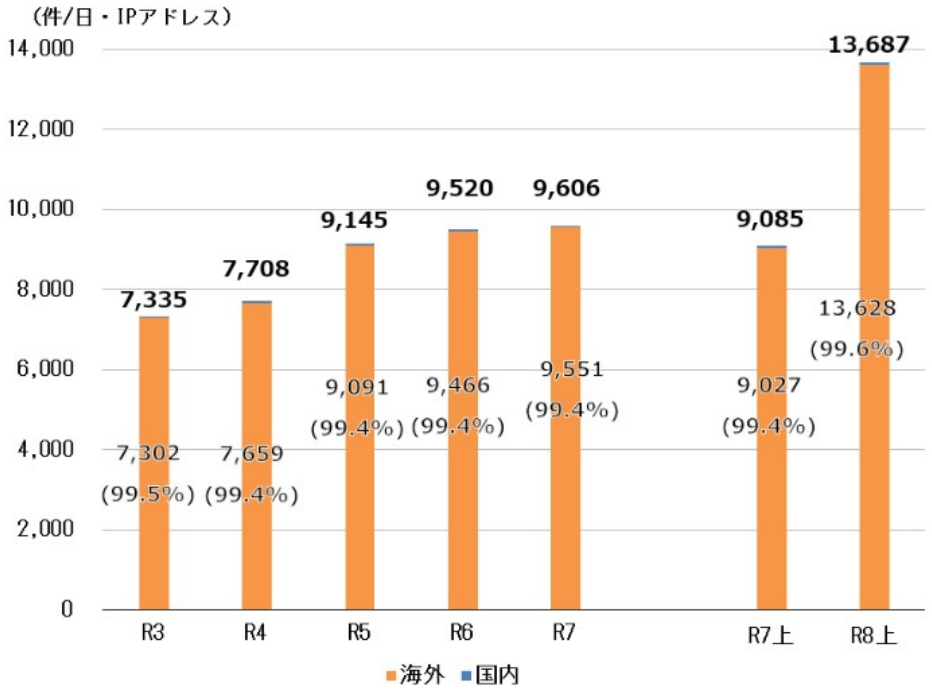
図 2-7：不正アクセス原因別件数の推移（2023 年～2025 年）

上：被害内容別件数
右：原因別件数

被害を被った原因のトップ3は、パスワード設定の不備、適切にシステムのバージョンアップをしていなかった、セキュリティ上必要な対処を怠った、です。これらは自分たちでできること。

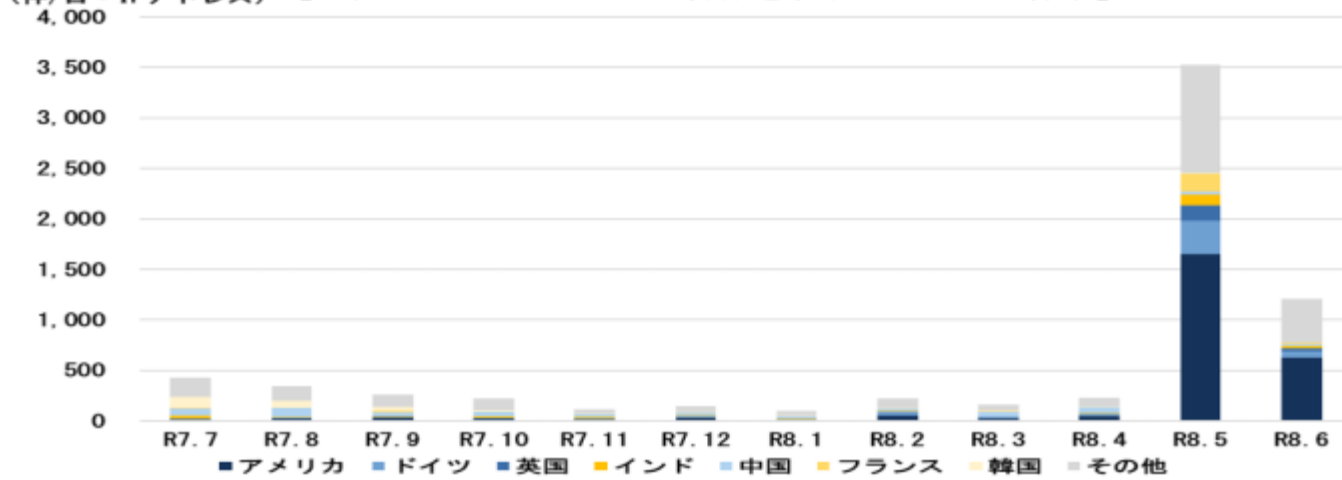
出典：コンピュータウイルス・不正アクセスの届出状況独立行政法人情報処理推進機構 セキュリティセンター2026 年 3 月 30 日

【図表１：警察庁が検知した国内外からの不審なアクセス件数】



また、令和８年５月から、Mirai[2]ボット[3]の特徴を有するアクセスの急増が観測された。Mirai ボットとは、Mirai と呼ばれるマルウェアが感染した家庭用無線ルータやＩｏＴ機器のことで、所有者が認知しないところで、ＤＤｏＳ攻撃等の不正行為に悪用される可能性がある。

【図表３：Mirai ボットの特徴を有するアクセス件数】



上図 2026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」警察庁サイバー警察局
https://www.npa.go.jp/news/release/2026/20260909001.html

- 「不審なアクセス」が本当に「不審」であることをどうやって確認できるのか？⇒玄関のドアをノックする人は不審者とは限らないが、こうした人も含めて「不審者」とみなすような統計操作をしていないかどうか。
- Miraiボット対策は、デフォルトパスワードの変更、最新ファームウェアの導入、機器の電源を入れなおす、です。警察が関与しなければ解決できない問題ではない。⇒自分で「戸締り」をやらない⇒警察がおせっかいする口実を与える。

サイバー安全保障分野での対応能力の向上に向けた有識者会議

有識者会議の提言(2024/11)

保全して、犯罪と犯人を解明することを目的とするものであり、このことを前提に、裁判官は、犯罪の嫌疑、犯罪関連通信が行われる蓋然性等を判断し、傍受すべき通信の手段、内容等を特定して傍受令状を発するものである*。しかしながら、今般実現されるべき**通信情報の利用は、重大なサイバー攻撃による被害を未然に防ぐため、また、被害が生じようとしている場合に即時に対応するため、具体的な攻撃が顕在化する前**、すなわち前提となる犯罪事実がない段階**から行われる必要**がある。したがって、通信情報を取得しようとする時点では、いかなる具体的態様でサイバー攻撃が発生するかを予測することはできず、あらかじめそのサイバー攻撃に関係する通信手段、内容等を特定することは通常は困難であるから、犯罪捜査とは異なる形で通信情報を取得し利用する必要があり、被害の防止と通信の秘密の保護という両方の目的を適切に果たすためには、**これまで我が国では存在しない新たな制度による通信情報の利用が必要**とされると考えられる。

攻撃もない時点からの「通信情報の利用」？

誰の通信情報を利用する？

「誰」をどう選ぶ？

どのような通信情報を攻撃の予兆とみなす？

網羅的に通信情報を収集し、必要に応じて利用する。「必要」はそのときどきの状況や政策によって変化する。今日のゴミは明日の宝。
通信情報の収集には通信事業者の協力が必須。
収集の規模はコンピュータ・システムの収集と処理能力に依存する。

参考資料(JCA-NETセミナーから)

スマホとサイバー戦争

スライド

https://archive.org/details/20260422-toshimaru

動画

https://archive.org/details/2026-04-24-10-44-38

サイバースパイとサイバー攻撃――スパイ機関創設批判

スライド

https://archive.org/details/20260327_20260328

動画

https://archive.org/details/20260327cyberwar

サイバーセキュリティ戦略批判

スライド

https://archive.org/details/20251219-tosimaru

動画

https://archive.org/details/2025-12-20-18-01-20

サイバースパイとサイバー攻撃――スパイ機関創設批判

スライド

https://archive.org/details/20260327_20260328

動画

https://archive.org/details/20260327cyberwar

もうちょっと詳しく知りたい場合は、『サイバースパイ・サイバー攻撃法案批判』をお読みください。
https://dararevo.wordpress.com/wp-content/uploads/2025/04/honbun_indexari.pdf