

**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
アクセス・無害化措置に関するテーマ別会合 第1回
参考資料（サイバー攻撃の情勢）**

令和6年7月1日

内閣官房

サイバー安全保障体制整備準備室

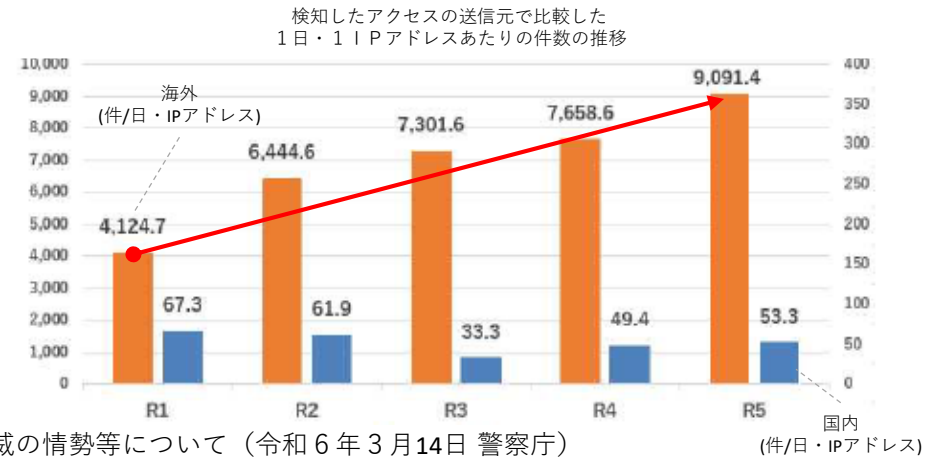
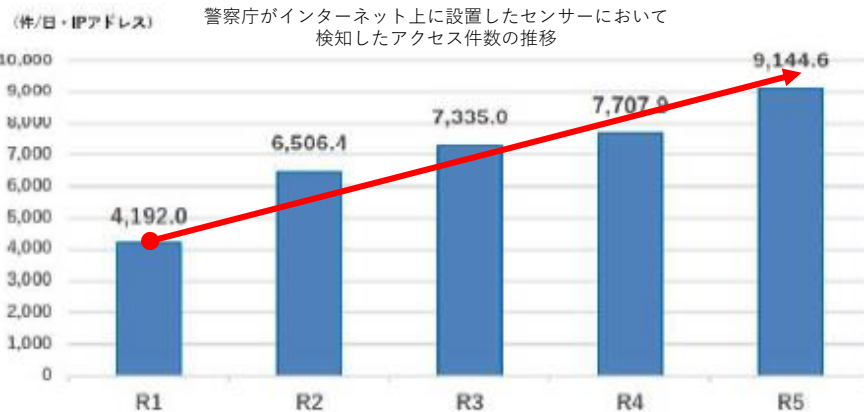
サイバー攻撃の情勢

「年間総観測パケット数の統計（過去10年間）」
（国立研究開発法人情報通信研究機構 NICTER 観測レポート 2023 より）

年	年間総観測パケット数	観測 IP アドレス数	1 IP アドレスあたりの 年間総観測パケット数
2014	約 241.0 億	212,878	115,335
2015	約 631.6 億	270,973	245,540
2016	約 1,440 億	274,872	527,888
2017	約 1,559 億	253,086	578,750
2018	約 2,169 億	273,292	806,877
2019	約 3,756 億	309,769	1,231,331
2020	約 5,705 億	307,985	1,849,817
2021	約 5,180 億	289,946	1,747,685
2022	約 5,226 億	288,042	1,833,012
2023	<u>約 6,197 億</u>	289,686	2,260,132

- ✓ 1 IP アドレス当たりで約226万のパケットが観測（令和5年）され、観測開始以降、最も多い値
✓ サイバー攻撃関連パケットの増加傾向が継続

- 警察庁では、外部に対して何らサービスを提供していないセンサーをインターネット上に設置、送付される通信パケットを収集
➤ 通信パケットを分析し、ぜい弱性を悪用した攻撃、不正プログラムに感染したコンピュータの動向等、インターネット上で発生している各種事象を把握



【出典】令和5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（令和6年3月14日 警察庁）

- ✓ 検知した アクセス件数 は1日・1 IPアドレス当たり9,144.6件（令和5年）、H23以降増加の一途
✓ 検知したアクセスの 大部分の送信元は海外 であり、海外からの脅威への対処が重要

2005年 内閣官房情報セキュリティセンター設置

公開サーバへの攻撃

エストニア・2007年

ウェブサーバ・外向けサービスへの大量送信
SQLインジェクションによる情報漏洩 等

ウェブサイト・
インターネットバンキング等
の停止

2015年 サイバーセキュリティ基本法施行（NISCも改組）



IT系システムの侵害

Wannacry・2017年
コロニアルパイプライン・2021年

情報システム内部への侵入・暗号化
(主に既知の脆弱性を悪用)

暗号化・システム障害
身代金要求



有事に備えた重要インフラ等への侵入

イラン核施設・原子力発電所へ
の攻撃・2010年
ウクライナ・2015年/2022年等
Volt Typhoon・2023年

最深部・制御系システムに至る高度な侵入能力
(ゼロデイ脆弱性の積極活用など)
高度な潜伏能力
(Living-off-the-Landなど)

インフラ機能停止

近年の国内事例

【事例①】

- 令和5年(2023年)8月、内閣サイバーセキュリティセンター(NISC)の電子メール関連システムに対し、不正通信があり、個人情報を含むメールアドレスの一部が外部に漏えいした可能性があることが判明したことを公表
- 本事案においては、メーカーにおいて確認できていなかった電子メール関連システムに係る機器の脆弱性を原因とするものであると考えられ、同様の事案は国外においても確認

【事例②】

- 令和3年4月、警視庁公安部は、中国共産党員の男(30代)が、住所、氏名等の情報を偽って日本のレンタルサーバの契約に必要な会員登録を行った事実から、私電磁的記録不正作出罪・同供用罪で検挙
- 捜査を通じ、不正に契約したレンタルサーバが宇宙航空研究開発機構(JAXA)等に対するサイバー攻撃に悪用されたことを把握、また、攻撃の実態解明の過程で、同一の攻撃者が関与している可能性が高いサイバー攻撃が約200の国内企業等に対して実行されたことを把握
- 一連のサイバー攻撃は、日本製ソフトウェアのぜい弱性が悪用されたゼロデイ攻撃と判明するとともに、これらのサイバー攻撃がTickと呼ばれるサイバー攻撃集団によって実行されたものであり、このTickの背景組織として山東(さんとう)省青島(チンタオ)市を拠点とする中国人民解放軍第61419部隊が関与している可能性が高いと結論付け

【事例③】

- 中国を背景とするサイバー攻撃グループ「BlackTech」(ブラックテック)は、2010年頃から日本を含む東アジアと米国の政府、産業、技術、メディア、エレクトロニクス及び電気通信分野を標的とし、情報窃取を目的としたサイバー攻撃を実施
- BlackTechは、インターネットに接続されたネットワーク機器に対し、ソフトウェアの脆弱性を狙うほか、ネットワークの設定の不十分さ、サポートの切れた機器・ソフトウェアなど、様々な脆弱な点をサイバー攻撃することにより侵入
- BlackTechは、侵害拠点を構築後、侵害活動を拡大させるため、信頼された内部のルーターを通じて、本社や別の拠点のネットワークへ侵入を拡大

近年の国外事例

【事例①】

- 2024年5月、独・内務省は、ロシア軍参謀本部情報総局 (GRU) を背景とするAPT28による、ドイツ社会民主党 (SPD) 等に対するサイバー攻撃について公表
- 攻撃キャンペーンの対象となったのは、SPDのほか、防衛、IT、物流、航空宇宙等の分野であり、Microsoft Outlook の未知の脆弱性を用いて電子メールアカウントを侵害

【事例②】

- 2024年3月、英国政府は、中国を背景とする組織やAPT31による、2つの悪意のあるサイバー攻撃キャンペーンについて公表
- 2021年から2022年にかけて、中国を背景とする組織が英国選挙管理委員会のシステムを侵害した可能性が高く、また、このキャンペーンとは別に、2021年、侵害に成功したものはなかったものの、APT31が英国国会議員に対する偵察活動を実施

【事例③】

- マイクロソフト社は、中国を背景とした主体であるVolt Typhoonが、2021年半ばから、グアム等の米軍施設を含む米国の重要インフラに対する侵入を繰り返してきたと発表
- Volt Typhoonの侵入の標的は、グアムを中心に米国の通信、製造、公共事業、輸送、建設、政府機関、教育機関等、多岐にわたっていたことを指摘
- 同社は、Volt Typhoonの一連の活動の目的が、将来の米国とアジア地域における紛争が生起した際における米国の通信インフラの阻害にある可能性があると評価

【攻撃の特徴】長期間の潜伏に必要な 高度な検知回避能力

- ✓ ネットワーク機器の脆弱性を突いて侵入。ゼロデイ脆弱性も悪用
- ✓ マルウェアを使わず、正規ユーザになりすまし、正規ツールを駆使 (Living off the Land)
- ✓ 侵入痕跡となるログの消去 等

- 
- ✓ サイバー攻撃による 実空間への影響が重大化・深刻化
 - ✓ サイバー攻撃に用いられる 手法の高度化・巧妙化が進展