資料５－４

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
通信情報の利用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とこれまでの政府の取組）

令和６年６月19日

内閣官房

サイバー安全保障体制整備準備室

背景：サイバー攻撃の情勢

- 国立研究開発法人情報通信研究機構（ＮＩＣＴ）では、到達可能かつ未使用のＩＰアドレス宛に届くパケットを観測
- パケットを分析することにより、インターネット上で発生しているサイバー攻撃の兆候や傾向を把握

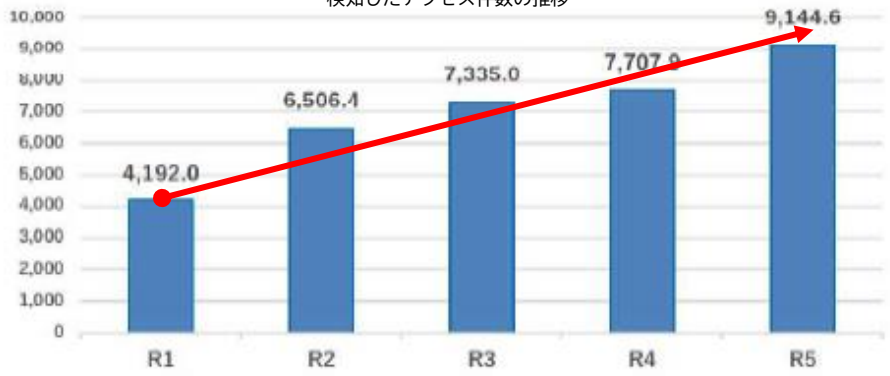
「年間総観測パケット数の統計（過去10年間）」
（国立研究開発法人情報通信研究機構 NICTER 観測レポート 2023 より）

年	年間総合観測パケット数	観測ＩＰアドレス数	１ＩＰアドレス当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	**約6,197億**	**289,686**	**2,260,132**

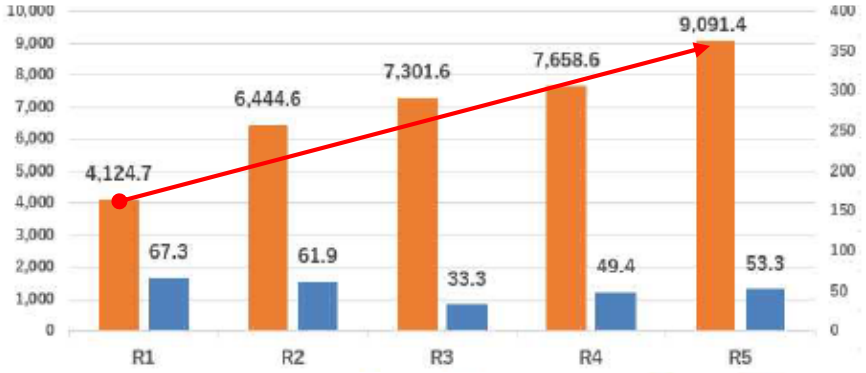
✓１ＩＰアドレス当たりで約226万のパケットが観測（令和５年）され、**観測開始以降、最も多い値**
✓**サイバー攻撃関連パケットの増加傾向が継続**

- 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

警察庁がインターネット上に設置したセンサーにおいて検知したアクセス件数の推移



検知したアクセスの送信元で比較した１日・１ＩＰアドレスあたりの件数の推移



【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・１ＩＰ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**

サイバー攻撃の情勢の変遷：重大化・深刻化

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

最近の国内事例（サイバー攻撃の重大化・深刻化）

国内事例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**メールデータ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

国内事例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

国内事例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

最近の国外事例（サイバー攻撃の重大化・深刻化）

国外事例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**

国外事例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

国外事例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**

これまでの政府の取組の例　①サイバーセキュリティ基本法の概要（令和３年改正後）

第Ⅰ章　総則

■目的（第1条）

⇒　以下の３つの大目的に寄与することを規定

①　経済社会の活力の向上及び持続的発展

②　国民が安全で安心して暮らせる社会の実現

③　国際社会の平和及び安全の確保並びに我が国の安全保障

■定義（第2条）

■基本理念（第3条）

■関係者の責務等（第4条～第9条）

⇒①国、②地方公共団体、③重要社会基盤事業者（重要インフラ事業者）、④サイバー関連事業者、⑤教育研究機関
等の責務等について規定

※なお、国民については、責務ではなく、努力とされている。

第Ⅱ章　サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒　次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③　重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒　その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章　基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■サイバーセキュリティ協議会（第17条）

⇒本部長及びその委嘱を受けた国務大臣は、サイバーセキュリティ協議会を組織

⇒協議会に、重要インフラ事業者、サイバー関連事業者等を構成員として加えることが可能

■犯罪の取締り及び被害の拡大の防止（第18条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第19条）

■産業の振興及び国際競争力の強化（第２０条）

■研究開発の推進等（第22条）

■人材の確保等（第22条）

■教育及び学習の振興、普及啓発等（第23条）

■国際協力の推進等（第24条）

第Ⅳ章　サイバーセキュリティ戦略本部

■設置（第25条）

■所掌事務等（第26条）

⇒サイバーセキュリティ戦略案の作成、国の行政機関、独立行政法人・指定法人に対する監査・原因究明調査、事象発生時の国内外の関係者との連絡調整等の実施

■組織等（第27条～第30条）

⇒内閣官房長官を本部長として、副本部長（国務大臣）、国家公安委員会委員長、デジタル大臣、総務大臣、外務大臣、経済産業大臣、防衛大臣、総理が指定する国務大臣、有識者本部員で構成

■事務の委託（第31条）

⇒独立行政法人・指定法人に対する監査・原因究明調査の事務の一部をIPAその他政令で定める法人に委託（秘密保持義務を規定）

⇒事象発生時の国内外の関係者との連絡調整の事務の一部を政令で定める法人に委託（秘密保持義務を規定）

■資料提供等（第32条～第37条）

第Ⅴ章　罰則

■罰則（第38条）

⇒協議会の事務に従事する者又は従事していた者及び戦略本部からの事務の委託を受けた者が秘密保持義務に反した場合。1年以下の懲役又は50万円以下の罰金

これまでの政府の取組の例　②サイバーセキュリティ政策の推進体制

内 閣　内閣総理大臣

国家安全保障会議（NSC）

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 ｻｲﾊﾞｰｾｷｭﾘﾃｨ基本法により設置）※

本部長　内閣官房長官

副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣

閣僚本部員
- 国家公安委員会委員長
- 総務大臣
- 経済産業大臣
- デジタル大臣
- 外務大臣
- 防衛大臣
- 国務大臣のうちから、内閣総理大臣が指定する者

有識者本部員

上沼 紫野	弁護士（虎ノ門南法律事務所）
遠藤 信博	日本電気(株)特別顧問
後藤 厚宏	情報セキュリティ大学院大学学長
酒井 啓亘	早稲田大学法学学術院教授
櫻井 敬子	学習院大学法学部教授
田中 孝司	KDDI(株)代表取締役会長
土屋 大洋	慶應義塾大学大学院教授
松原　実穂子	日本電信電話(株)ﾁｰﾌ･ｻｲﾊﾞｰｾｷｭﾘﾃｨ･ｽﾄﾗﾃｼﾞｽﾄ
村井 純	慶應義塾大学教授

※ 構成員は、令和６年４月現在。

緊密連携

デジタル庁

連携

サイバーセキュリティ協議会

官民の多様な主体が相互に連携した、より早期の段階での、サイバーセキュリティの確保に資する情報の迅速な共有等

（事務局）

内閣官房 内閣サイバーセキュリティセンター（NISC）（2015.1.9 内閣官房組織令により設置）

〔各省のサイバーセキュリティ施策の統一性保持のための総合調整〕

内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）

副センター長（内閣審議官）

協力

＜重要インフラ所管省庁＞

〔所管重要インフラ事業におけるサイバーセキュリティの確保〕

- 金融庁（金融機関）
- 総務省（地方公共団体、情報通信）
- 厚生労働省（医療）
- 経済産業省（電力、ガス、化学、クレジット、石油）
- 国土交通省（鉄道、航空、物流、空港、港湾、水道）

＜その他関係省庁＞

文部科学省（セキュリティ教育）等

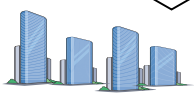
協力

閣僚本部員６省庁

〔各省の所掌に基づくサイバーセキュリティ施策の実施〕

- 警察庁（ｻｲﾊﾞｰ犯罪取締り）
- デジタル庁（ﾃﾞｼﾞﾀﾙ社会形成）
- 総務省（通信・ﾈｯﾄﾜｰｸ政策）
- 外務省（外交・安全保障）
- 経済産業省（情報政策）
- 防衛省（国の防衛）

重要インフラ事業者等



政府機関（各府省庁）

企業

個人

これまでの政府の取組の例　③関係法令における重要インフラの位置付け

重要インフラの定義

法第３条及び第12条第２項第３号

重要社会基盤事業者　**国民生活及び経済活動の基盤**であって、その**機能が停止し、又は低下**した場合に国民生活又は経済活動に**多大な影響を及ぼす**おそれが生ずるものに関する事業を行う者

重要社会基盤事業者等　**重要社会基盤事業者**及びその**組織する団体**並びに**地方公共団体**

重要インフラの責務

（地方公共団体の責務）

第５条　地方公共団体は、基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。

（重要社会基盤事業者の責務）

第６条　重要社会基盤事業者は、基本理念にのっとり、その**サービスを安定的かつ適切に提供**するため、サイバーセキュリティの重要性に関する関心と理解を深め、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力する**よう努めるものとする。

（参考）重要インフラ以外の事業者の責務

（サイバー関連事業者その他の事業者の責務）

第７条　サイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者をいう。以下同じ。）その他の事業者は、基本理念にのっとり、その事業活動に関し、**自主的かつ積極的にサイバーセキュリティの確保に努める**とともに、国又は地方公共団体が実施するサイバーセキュリティに関する**施策に協力する**よう努めるものとする。

（国民の努力）

第９条　国民は、基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に必要な注意を払うよう努めるものとする。

施　策

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）

第14条　**国は**、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の**自主的な取組の促進**その他の**必要な施策**を**講ずるものとする**。

「重要インフラのサイバーセキュリティに係る行動計画」の概要

官民連携による重要インフラ防護の推進

- 任務保証の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現
- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進

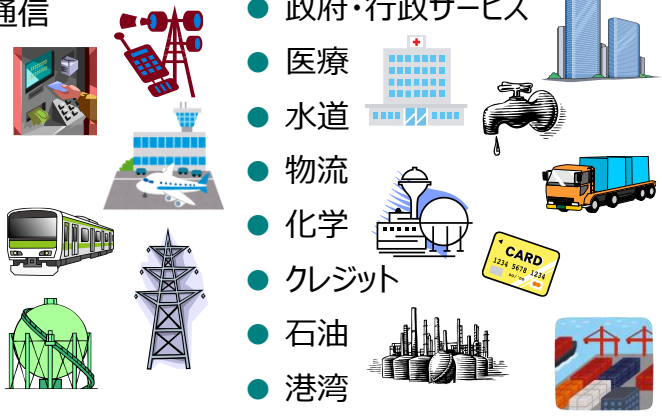
NISCによる総合調整

重要インフラ所管省庁

- 金融庁
  [金融]
- 総務省
  [情報通信、行政]
- 厚生労働省
  [医療]
- 経済産業省
  [電力、ガス、化学、クレジット、石油]
- 国土交通省
  [航空、空港、鉄道、水道、物流、港湾]

重要インフラ(全１５分野)

- 情報通信
- 金融
- 航空
- 空港
- 鉄道
- 電力
- ガス
- 政府・行政サービス
- 医療
- 水道
- 物流
- 化学
- クレジット
- 石油
- 港湾



関係機関等

- サイバーセキュリティ関係省庁
  [総務省、経済産業省等]
- 事案対処省庁
  [警察庁、防衛省等]
- 防災関係府省庁
  [内閣府、各省庁等]
- サイバーセキュリティ関係機関
  [NICT、IPA、JPCERT/CC等]
- サイバー空間関連事業者
  [サプライチェーン等に関わるベンダー等]

「重要インフラのサイバーセキュリティに係る行動計画」における主な取組

障害対応体制の強化

経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進

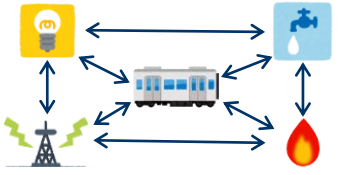
安全基準等の整備及び浸透

重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進

情報共有体制の強化

官民間や分野内外間における情報共有体制の更なる強化

リスクマネジメントの活用



自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用

防護基盤の強化

分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ