第５章 サイバー情勢

1 情勢

（1） サイバー攻撃情勢

サイバー空間は、地域や年齢、性別を問わず、全国民が参加し、重要な社会経済活動が営まれる公共空間へと変貌を遂げ、金融、航空、鉄道、医療等といった国民生活や社会経済活動を支える基盤となる機能から、警察や防衛といった治安や安全保障に関わる国家機能に至るまで、あらゆる場面で実空間とサイバー空間の融合が進んでいる。

こうした中、国内において、ハクティビストによるものとみられるＤＤｏＳ攻撃により、政府機関や民間事業者等のウェブサイトの閲覧障害が複数発生しているほか、過去には、中国を背景とするサイバー攻撃グループにより、情報窃取を目的としたサイバー攻撃が行われていることが確認されるなど、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いている。

（2） 国際情勢

近年、世界各地で機密情報や知的財産の窃取、重要インフラの機能停止等を企図したとみられるサイバー攻撃が相次いで発生している。こうした攻撃の中には国家の関与が疑われている攻撃も数多く存在し、今後も世界的規模でのサイバー攻撃の発生が懸念される。

① 中国

中国は、軍事関連企業、先端技術保有企業等の情報窃取を目的として、サイバー攻撃を行っているとみられている。

【事例】サイバー攻撃集団「Volt Typhoon」による重要インフラ等を標的とした攻撃

令和６年（2024 年）２月、米国国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁（ＣＩＳＡ）、米国国家安全保障局（ＮＳＡ）、米国連邦捜査局（ＦＢＩ）等は、ファイブアイズ諸国の関係機関と合同で、重要インフラ事業者向けに、中国国家を背景とするサイバー攻撃集団「Volt Typhoon」によるサイバー攻撃に関する注意喚起を実施した。米国の関係機関によると、「Volt Typhoon」による米国の通信、エネルギー、運輸及び水道分野等の重要インフラ事業者への侵害が確認されているほか、有事の際に重要インフラに対するサイバー攻撃を行うため、事前に重要インフラ事業者等のネットワークへのアクセス権限を確保し、複数の重要インフラ事業者におけるＯＴ（Operational Technology）機器に対する侵害を可能としている旨が指摘されている。

【事例】英国の国会議員及び選挙管理委員会を標的としたサイバー攻撃

令和６年（2024 年）３月、英国政府は、英国の国会議員及び選挙管理委員会に対する中国国家を背景とするサイバー攻撃を非難する声明を発表した。英国サイバーセキュリティセンター（ＮＣＳＣ）によると、中国国家を背景とするサイバー攻撃集団「ＡＰＴ 31」が、令和３年（2021 年）に英国国会議員のメールアカウントに対する偵察活動を実行した可能性が極めて高いほか、令和３年（2021 年）から令和４年（2022 年）にかけて、中国国家を背景とするサイバー攻撃集団が、英国選挙管理委員会のシステムを侵害し、メールデータ等を窃取した可能性が高いとしている。

【事例】中国が構築する世界的規模のボットネットの無害化作戦

令和６年（2024 年）９月、米国司法省は、米国を含む世界中の 20 万台以上の機器から構成されるボットネットを無害化するオペレーションを実施したと発表した。米国司法省によると、当該ボットネットは、「Flax Typhoon」として知られている中国企業「Integrity Technology Group」で働く中国国家の支援を受けた攻撃者によってマルウェアに感染させられたＩｏＴ機器等で構成されており、情報窃取等を目的としたサイバー攻撃に用いられたとされている。同月、ＦＢＩ、ＮＳＡ及び米軍サイバー国家任務部隊（ＣＮＭＦ）は、ファイブアイズ諸国の関係機関と合同で、当該ボットネットに関する注意喚起を実施した。

②　ロシア

ロシアは、軍事的及び政治的目的の達成に向けて影響力を行使するため、重要インフラ事業者に被害を与えるサイバー攻撃や、他国の国政選挙に影響を及ぼすためのサイバー攻撃等を行っているとみられている。

【事例】世界的規模で様々な分野を標的としたサイバー攻撃

令和６年（2024 年）２月、ＮＣＳＣは、ファイブアイズ諸国の関係機関と合同で、ロシア対外情報庁（ＳＶＲ）を背景とするサイバー攻撃集団「ＡＰＴ 29」によるサイバー攻撃に関する注意喚起を実施した。これまで確認されていた政府、シンクタンク、医療及びエネルギー分野に加えて、航空、教育、法執行機関、地方議会、国会、政府の財務部門、軍事組織等にまで「ＡＰＴ 29」の標的が拡大しているほか、攻撃手口として、新たにクラウドサービスを標的としているとされている。また、同年 10 月、ＦＢＩ、ＮＳＡ、ＣＮＭＦ及びＮＣＳＣは、「ＡＰＴ 29」によるサイバー攻撃が世界規模の脅威をもたらしているとして、攻撃手口や必要な対策に関する注意喚起を実施した。

【事例】ドイツの政党等を標的としたサイバー攻撃

令和６年（2024 年）５月、ドイツ政府は、ＥＵや北大西洋条約機構（ＮＡＴＯ）等の支持の下、ロシア軍参謀本部情報総局（ＧＲＵ）を背景とするサイバー攻撃集団「ＡＰＴ 28」によるドイツ社会民主党執行委員会に対するサイバー攻撃を非難する声明を発表した。「ＡＰＴ 28」は、Microsoft Outlook のぜい弱性を悪用し、多数のメールアカウントを侵害しており、その標的には、ドイツやウクライナ等の政府機関や物流、防衛、航空宇宙、ＩＴ分野の企業が含まれているとされている。

【事例】世界中の重要インフラを標的としたサイバー攻撃

令和６年（2024 年）９月、ＦＢＩ、ＣＩＳＡ、ＮＳＡ等は、ファイブアイズ諸国を含む諸外国の関係機関と合同で、ＧＲＵ第 161 特殊訓練センター（29155 部隊）によるサイバー攻撃に関する注意喚起を実施した。29155 部隊は、ＮＡＴＯ加盟国、ＥＵ、中央アメリカ及びアジアの政府機関、金融、運輸、エネルギー、医療分野等を標的として、遅くとも令和２年（2020 年）から情報窃取等を目的とした活動を行ってきたとされている。

③　北朝鮮

北朝鮮は、政治目標の達成や外貨獲得を目的として、様々な形でサイバー攻撃を行っているとみられている。

【事例】サイバー攻撃集団「Lazarus」による暗号資産関係事業者を標的とした攻撃

令和４年（2022 年）10 月、北朝鮮当局の下部組織とされる「Lazarus」と呼称されるサイバー攻撃集団が、数年来、日本国内の暗号資産関係事業者を標的としたサイバー攻撃を行っていると強く推察される状況にあることが、日本の関係都道府県警察やサイバー特別捜査隊の捜査等によって判明したことから、警察庁は、金融庁及び内閣サイバーセキュリティセンター（ＮＩＳＣ）と連名で注意喚起を実施した。

【事例】サイバー攻撃による外貨の獲得

令和６年（2024 年）３月、国連安全保障理事会北朝鮮制裁委員会の専門家パネルより、最終報告書が公表された。平成 29 年（2017 年）から令和５年（2023 年）までにかけて発生した北朝鮮の関与が疑われる暗号資産関連企業に対するサイバー攻撃事案 58 件（被害額約 30 億米ドル相当）を調査した結果、北朝鮮が獲得した外貨の約半分はサイバー攻撃によるものであり、北朝鮮では、こうした外貨を大量破壊兵器計画に使用しているとされている。

【事例】防衛、航空宇宙、原子力等の分野を標的としたサイバー攻撃

令和６年（2024 年）７月、ＦＢＩ等は、韓国及び英国の関係機関と合同で、平壌等に拠点を置く北朝鮮偵察総局第３局傘下のサイバー攻撃集団「Andariel」によるサイバー攻撃に関する注意喚起を実施した。「Andariel」は、米国、英国、韓国のほか、日本やインドを含む世界各国の防衛、航空宇宙、原子力等の産業分野を標的とし、北朝鮮政府の軍事・原子力施策を発展させる目的で機密情報等を窃取したとされている。

（3） 国内の被害情勢

近年、国内において、先端技術や機密情報の窃取を目的として行われるサイバーエスピオナージ事案等が多発している。

令和６年には、民間事業者や研究開発機関等に対する情報窃取を企図した不正アクセス事案や、重要インフラ等の機能に障害を発生させ、社会経済活動に影響を及ぼしたサイバー攻撃事案が発生した。このほか、政府機関や自治体、民間企業等が運営するウェブサイトの閲覧障害が発生するなどのサイバー攻撃事案が発生している。

【事例】情報窃取を企図した不正アクセス事案

○　令和６年３月、大手システム事業者は、業務上使用する複数のコンピュータが不正プログラムに感染し、個人情報や顧客情報を含むファイルが不正に持ち出せる状況になっていたと発表した。

○　同年３月、半導体関連機器事業者は、同社のサーバ等が第三者による不正アクセスを受けた可能性があると発表した。

○　同年７月、国内の宇宙航空分野の研究開発機関は、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洩したことを発表した。

○　同年７月、エネルギー関連事業者は、外部からの不正アクセスにより、業務委託元から提供を受けている個人情報等が流出した可能性があることが判明したと発表した。

【事例】重要インフラの機能に影響を及ぼしたサイバー攻撃事案

令和６年５月、大手鉄道事業者は、インターネット上の乗車券等の予約サービスを提供するウェブサイト、スマートフォンのＩＣ乗車券サービスを提供するアプリケーション等に接続しづらい状況となっていることを発表した。

【事例】ＤＤｏＳ攻撃による被害とみられるウェブサイトの閲覧障害

○　令和５年 12 月から令和６年４月にかけて、ＤＮＳ権威サーバを狙ったランダムサブドメイン攻撃によるとみられるウェブサイトの閲覧障害が断続的に発生した。

○　令和６年２月、同年７月及び同年 10 月、政府機関、自治体、民間事業者等が運営する複数のウェブサイトにおいて閲覧障害が発生した。同じ頃、ＳＮＳ上に、ハクティビストのものと思われる複数のアカウントから、それらの犯行をほのめかす投稿が確認された。

2　官民連携の推進及び実態解明

（1）　官民連携の推進

①　サイバーテロ対策協議会

警察では、各都道府県警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等とで構成するサイバーテロ対策協議会を全ての都道府県に設置し、サイバー攻撃の脅威や情報セキュリティに関する情報提供、民間の有識者による講演、参加事業者間の意見交換や情報共有等を行っているほか、サイバー攻撃の発生を想定した共同対処訓練等を行っている。

▲サイバーテロ対策協議会における共同対処訓練の様子（秋田）

②　サイバーインテリジェンス情報共有ネットワーク

警察では、情報窃取の標的となるおそれの高い先端技術を有する全国約 8,700（令和６年 12 月現在）の事業者等との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行うサイバーインテリジェンス情報共有ネットワークを構築している。このネットワークを通じて事業者等から提供された情報を集約し、これらの事業者等から提供された情報及びその他の情報を総合的に分析するとともに、事業者等に対し、分析結果に基づく注意喚起を実施している。

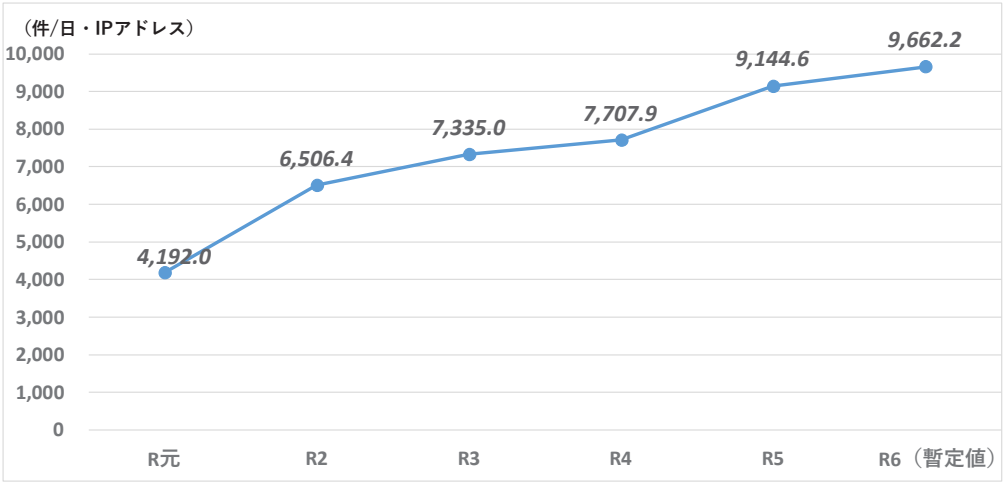
（2）　サイバー攻撃の捜査・実態解明等に関する取組

①　サイバー攻撃の捜査・実態解明

警察では、違法行為に対する捜査を推進するとともに、サイバー攻撃を受けたコンピュータやサイバー攻撃に使用された不正プログラムを解析し、その結果や犯罪捜査の過程で得た情報等を総合的に分析するなどして、攻撃者及び手口に関する実態解明を進めている。また、ＩＣＰＯを通じるなどして、外国捜査機関との間で国際捜査協力を積極的に推進している。

そのほか、警察では、インターネット上で発生している各種事象の把握を目的として、インターネット上にセンサーを設置し、攻撃者が攻撃対象を探索する場合等に不特定多数のＩＰアドレスに対して無差別に送信される通信パケットを観測・分析している。

令和６年中、一つのセンサー当たり約 9.1 秒に１回という高い頻度で世界中から不審なアクセスが行われていることを観測した。



インターネット上に設置したセンサーに対する１日当たりの不審なアクセス件数の推移（令和元年～令和６年）

②　豪州主導のＡＰＴ 40 に関する国際アドバイザリーへの共同署名

中国政府を背景とするサイバー攻撃グループといわれているＡＰＴ 40 は、北米、欧州、豪州等を標的としており、我が国の企業も攻撃の標的になっていたことが確認されている。

令和６年７月、警察庁及びＮＩＳＣは、米国、英国、カナダ、ニュージーランド、ドイツ及び韓国の関係機関と共に、豪州通信電子局豪州サイバーセキュリティセンターが作成した、ＡＰＴ 40 による過去の攻撃事例に基づく攻撃手法、攻撃の検知や緩和策が示された国際アドバイザリー「APT40 Advisory PRC MSS tradecraft in action」の共同署名に加わり、本件アドバイザリーを公表した。

▲豪州主導のＡＰＴ 40 に関する国際アドバイザリー（抜粋）

③　豪州主導国際文書「ＯＴサイバーセキュリティの原則」への共同署名

令和６年 10 月、警察庁及びＮＩＳＣは、米国、英国、カナダ、ニュージーランド、ドイツ、オランダ及び韓国の関係機関と共に、豪州通信情報局（ＡＳＤ）豪州サイバーセキュリティセンター（ＡＣＳＣ）が策定した文書「ＯＴサイバーセキュリティの原則」（Principles of operational technology cyber security ）の共同署名に加わり、重要インフラ事業者がＯＴ環境の設計、実装及び管理に係る意思決定を行うことを支援する６つの原則を示した文書を公表した。

▲豪州主導国際文書「ＯＴサイバーセキュリティの原則」（抜粋）