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、政府機関、金融機関等の重要インフラ事業者等におけるＤＤｏＳ攻撃とみられる被害や情報窃取を目的としたサイバー攻撃、国家を背景とする暗号資産獲得を目的としたサイバー攻撃事案等が相次ぎ発生するなど、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「MirrorFace」による情報窃取を目的とした攻撃

令和７年（2025 年）１月、警察庁及び内閣サイバーセキュリティセンターは、2019 年頃から日本国内の組織、事業者及び個人に対するサイバー攻撃キャンペーンが、「MirrorFace」（別名：EarthKasha）と呼称されるサイバー攻撃グループによって実行されたと評価し、連名で注意喚起を発出した。攻撃対象、手口、攻撃インフラ等を分析した結果、「MirrorFace」による攻撃キャンペーンは、主に我が国の安全保障や先端技術に係る情報窃取を目的とした中国の関与が疑われる組織的なサイバー攻撃であると評価している。

【事例】サイバー攻撃集団「Salt Typhoon」による情報窃取を目的とした攻撃

令和７年（2025 年）１月、米国財務省外国資産管理局（ＯＦＡＣ）は、中国四川省を拠点とするセキュリティ企業「四川聚信和网络科技有限公司（四川聚信）」に対する制裁を発表した。四川聚信は、中国国家安全部（ＭＳＳ）と強いつながりがあり、サイバー攻撃グループ「Salt Typhoon」の活動に直接関与しているとされている。「Salt Typhoon」の一連の攻撃は、米国の国家安全保障、外交政策等に係る情報窃取を目的とした組織的なサイバー攻撃であると評価されている。

【事例】サイバー攻撃集団「ＡＰＴ 27」による情報窃取を目的とした攻撃

令和７年（2025 年）３月、米国司法省は、世界的なコンピュータ侵入キャンペーンに関与したとして、中国公安部２名、安洵信息技術有限公司（i-Soon）従業員８名及び「ＡＰＴ 27」（別名：Silk Typhoon、UNC5221）構成員２名を訴追したと発表した。これらのアクターは、中国公安部（ＭＰＳ）及びＭＳＳの指示や独自の判断に基づき、米国を拠点とする中国の批判者及び反体制派、米国内の大規模な宗教組織、アジアの外務省、並びに米国の連邦政府及び州政府等を標的としたサイバー攻撃を実施し、窃取したデータの対価としてＭＰＳ及びＭＳＳから多額の金銭を受け取っていたとされている。

同日、米国財務省は、訴追された「ＡＰＴ 27」構成員及び同人が設立した上海黒英信息技術有限公司（Shanghai Heiying 社）を制裁対象に指定することを発表した。

【事例】サイバー攻撃を支援する民間企業

令和７年（2025 年）12 月、英国政府は、英国及び同盟国に対するサイバー攻撃を実行したとして中国を拠点とする安洵信息技術有限公司（i-Soon）及び北京永信至诚科技有限公司（Integrity Tech）を公表し制裁を行った。制裁対象となった企業は、世界中で 80 以上の政府機関及び民間企業を標的としたサイバー攻撃を実施したほか、他者の悪意あるサイバー活動を支援したとされている。英国国家サイバーセキュリティセンター（ＮＣＳＣ）は、これらの民間企業が中国のサイバー攻撃を支援したと評価している。

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】フランスへのサイバー攻撃

令和７年（2025 年）４月、フランス外務省は、ロシア軍参謀本部情報総局（ＧＲＵ）に属するハッカー集団「ＡＰＴ 28」が 2021 年以降にフランスの省庁や防衛関連企業、シンクタンク、2024 年パリオリンピック関連組織等に対してサイバー攻撃を行ったとする声明を発表した。これらの攻撃は、情報窃取やシステム侵害を目的とした国家主導の行為であり、フランスは国際法違反として強く非難した。声明は、フランス国家情報システム庁（ＡＮＳＳＩ）の技術的分析に基づいており、「ＡＰＴ 28」の活動がフランスのＩＴインフラに深刻な脅威を与えたとしている。

【事例】西側諸国の物流企業とテクノロジー企業を標的としたサイバー攻撃

令和７年（2025 年）５月、米国サイバーセキュリティ・社会基盤安全保障庁（ＣＩＳＡ）、米国国家安全保障局（ＮＳＡ）、米国連邦捜査局（ＦＢＩ）、西側諸国当局等は、ＧＲＵによる西側諸国の物流企業やテクノロジー企業を標的とするサイバー攻撃に関し、共同サイバーセキュリティアドバイザリー（ＣＳＡ）を発出した。同アドバイザリーによれば、物流企業やテクノロジー企業を標的とした攻撃では、以前に公開された戦術、技術、手順（ＴＴＰ）が組み合わせて使用されており、また、ウクライナや隣接するＮＡＴＯ諸国のＩＰカメラを大規模に標的とする攻撃とも関連している可能性が高いとしている。

【事例】マイクロソフトの認証情報を窃取するサイバー攻撃

令和７年（2025 年）７月、英国外務省は、欧州各国を標的としたサイバー攻撃に関与したとして、ＧＲＵの３部隊 (26165、29155、74455) 及びＧＲＵの幹部職員を含む関係者 18 人に対する制裁を発表した。同日、ＮＣＳＣは、ＧＲＵ 26165 部隊に属するサイバー攻撃集団「ＡＰＴ 28」が、Microsoft 社のサービスにおける被害者のメールアカウントへのアクセスを可能とする認証情報を窃取するためマルウェア「AUTHENTIC ANTICS」を使用していたことを明らかにした。林官房長官（当時）は 22 日の記者会見で、悪意あるサイバー活動を明らかにするための英国政府の取組を支持すると述べた。

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】北朝鮮ＩＴ労働者による外貨獲得

令和６年（2024 年）12 月、米国司法省は、経済制裁違反、電信詐欺、マネー・ローンダリング、身分盗用等の長期にわたる共謀により、14 人の北朝鮮人を起訴したと公表した。彼らは、ＩＴ労働者として米国企業や非営利団体で身元を偽装して雇用され、雇用による収入に加えて、企業の機密情報を窃取し雇用主を恐喝することで収入を補い、2017 年４月から 2023 年３月までの６年間に少なくとも 8,800 万ドルを不正に稼いだとされている。

北朝鮮ＩＴ労働者が手口を一層巧妙化させ、世界的に活動を拡大している現状を踏まえ、令和７年（2025 年）８月には、警察庁、外務省、財務省及び経済産業省は、「北朝鮮ＩＴ労働者に関する企業等に対する注意喚起」（令和６年（2024 年）３月公表）を更新するとともに、米国及び韓国と共に、「北朝鮮ＩＴ労働者に関する共同声明」を発出した。

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

令和７年 (2025 年) ２月、ＦＢＩは、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が暗号通貨取引所 Bybit から約 15 億ドル相当の暗号資産を盗んだことを公表した。「TraderTraitor」は急速に活動を進めており、盗まれた資産の一部をビットコインやその他の暗号資産に変換し、複数のブロックチェーン上の何千ものアドレスに分散しているとされている。また、「TraderTraitor」は、北朝鮮当局の下部組織とされる「Lazarus Group」の一部とされており、手法の特徴として、同時に同じ会社の複数の従業員に対して実施される、標的型ソーシャルエンジニアリングが挙げられる。

(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７年には、政府機関や金融機関等の重要インフラ事業者等におけるＤＤｏＳ攻撃とみられる被害や情報窃取を目的としたサイバー攻撃等が相次ぎ発生した。

【事例】情報窃取を企図した不正アクセス事案

○　令和７年３月、研究開発機関は、リモートアクセス機器に対するゼロデイ攻撃による不正アクセスを受け、個人情報が漏えいした可能性があることを発表した。

○　同年４月、システム事業者は、同社のサービスを提供するサーバ等が不正アクセスを受け、顧客情報等が漏えいした可能性があると発表した。同月、同社は顧客情報等の漏えいが確認されたほか、その原因が第三者製のソフトウェアのぜい弱性を悪用されたことによるものであったと発表した。

○　同年４月、電力事業者は、社内のネットワークへの接続機器の一部が不正アクセスを受け、個人情報等が漏えいした可能性があると発表した。

○　同年６月、機器製造業者は、自社で管理するサーバに不正アクセスを受け、個人情報等が漏洩した可能性があると発表した。

○　同年７月、情報通信事業者は、ネットワーク機器へのゼロデイ攻撃を原因とする不正アクセスを受け、個人情報等が漏洩した可能性があると公表した。

【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６年 12 月下旬から令和７年１月上旬にかけて、交通機関や金融機関等において、ＤＤｏＳ攻撃による被害とみられるウェブサイトの閲覧障害や各種アプリケーションへのアクセス障害が複数発生した。

○　令和７年３月から４月にかけて、政府要人の個人ウェブサイトにおいて、ＤＤｏＳ攻撃による被害とみられる閲覧障害が複数発生した。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。

○　同年６月、政府機関、自治体、民間事業者等が運営するウェブサイトにおいてＤＤｏＳ攻撃による被害とみられる閲覧障害が複数発生した。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。

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 8,800（令和７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行っている。

▲サイバーテロ対策協議会の様子（滋賀）

（2）　サイバー攻撃の捜査・実態解明等に関する取組

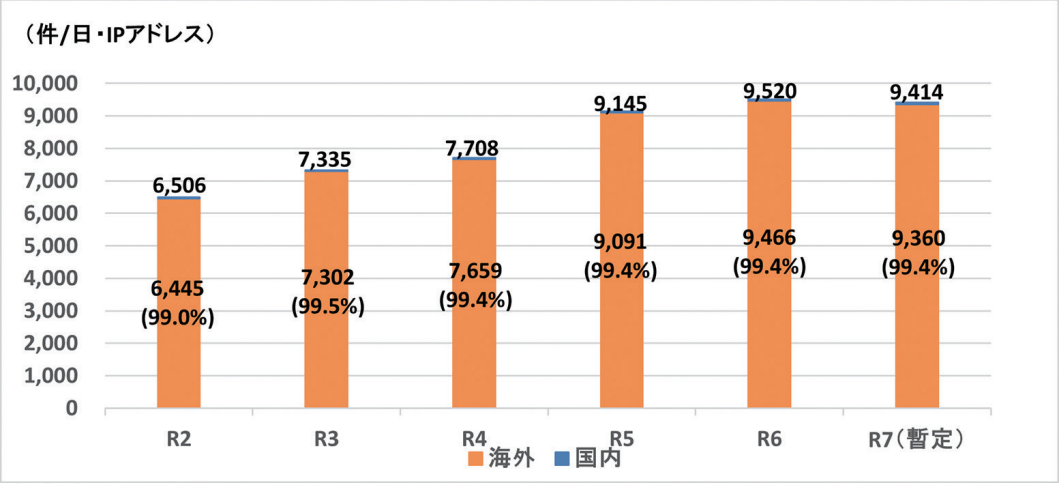
①　サイバー攻撃の捜査・実態解明

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７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２年～令和７年）



②　豪州主導国際文書「最新の防御可能なアーキテクチャのための基礎」への共同署名

令和７年 10 月、警察庁及び国家サイバー統括室（ＮＣＯ）は、豪州、ドイツ、カナダ、ニュージーランド、韓国及びチェコの関係機関とともに、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「最新の防御可能なアーキテクチャのための基礎」（“Foundations for modern defensible architecture”）の共同署名に加わり、サイバー脅威に対応したシステムの構築、維持、更新、強化のために役に立つアプローチを提供する文書を公表した。

▲豪州主導国際文書「最新の防御可能なアーキテクチャのための基礎」（抜粋）

③　パブリック・アトリビューション

令和６年 12 月、警察庁、ＦＢＩ及び米国国防省サイバー犯罪センター（ＤＣ３）は、令和６年５月、北朝鮮を背景とするサイバー攻撃グループ「TraderTraitor」が、我が国の暗号資産関係事業者から約 482 億円相当の暗号資産を窃取したことを特定し、合同で公表した。

令和７年８月、警察庁及びＮＣＯは、米国、オーストラリア、カナダ、ニュージーランド、英国、チェコ、フィンランド、ドイツ、イタリア、オランダ、ポーランド及びスペインの関係機関とともに、中国を背景とするサイバー攻撃グループ「Salt Typhoon」によるサイバー攻撃に関する国際アドバイザリー「Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System」の共同署名に加わり、パブリック･アトリビューションとして、本件アドバイザリーを公表した。

▲北朝鮮を背景とするサイバー攻撃グループ
TraderTraitor による暗号資産関連事業者を標的とした
サイバー攻撃について

▲中国を背景とするサイバー攻撃グループ
「Salt Typhoon」によるサイバー攻撃に関する
国際アドバイザリー（冒頭抜粋）