サイバー空間における脅威の概況2021

Overview of Threats in Cyberspace 2021

PSIA 公安調査庁

Public Security Intelligence Agency

はじめに

公安調査庁は、我が国の情報コミュニティのコアメンバーとして、国際テロや周辺国情勢、国内諸団体の動向など、我が国の公共の安全に影響を及ぼし得る国内外の諸動向について情報を収集・分析し、それらを関係機関に適時適切に提供することで、政府の危機管理や安全保障などの重要施策の推進に貢献しています。

我が国を取り巻く内外の情勢は、日々めまぐるしく変化し、特に近年においては、新型コロナウイルス感染症の感染拡大が既存の社会構造や国際秩序の不安定化を引き起こし、我が国の安全保障環境に少なからず影響を与える中で、サイバー空間における脅威の態様にも変化がみられます。

このような情勢を受け、「サイバー空間における脅威の概況2021」として本冊子を作成いたしました。サイバー空間における脅威に関する理解の一助となりましたら幸いです。

※　表紙・裏表紙で使用している写真について

①　提供：Science Photo Library/アフロ

②　提供：Science Photo Library/アフロ

※　が付いた用語は、各ページの下部で「KEYWORD」として説明を記載しています。

写真提供：ピクスタ

サイバー空間における脅威の増大

Growing Threats in Cyberspace

業務の妨害、重要情報の窃取、金銭の獲得などを狙ったサイバー攻撃は、国内外で常態化するとともに、その手口も巧妙化しています。加えて、技術の進展や社会構造の変化により、サイバー空間の社会への拡大・浸透がより一層進む中にあって、サイバー空間における悪意ある主体の活動は、社会・経済の持続的な発展や国民生活の安全・安心に対する深刻な脅威となっています。

さらに、国家が政治的、軍事的目的を達成するため、諜報活動や重要インフラの破壊といったサイバー戦能力を強化しているとみられており、安全保障の観点からも、サイバー攻撃の脅威は重大化しています。

2000.01 我が国官公庁ウェブサイト改ざん事案

科学技術庁（当時）を始めとして、複数の中央省庁などのウェブサイトの改ざん事案が相次いで発生

2010.01 オーロラ作戦（Operation “Aurora”）の発覚

Google社を含む、インターネット、金融、テクノロジー、メディア、化学など、様々な分野の20以上の大企業を標的として、Internet Explorerの脆弱性を利用し、知的財産などを窃取

2010.11 マルウェア「Stuxnet」によるイラン核関連施設攻撃の発覚

イランのウラン濃縮施設の遠心分離機に対するサイバー攻撃が発覚。報道などによると、マルウェア「Stuxnet」が、遠心分離機を秘密裏に誤作動させ、約1,000台を物理的に破壊（→ P5参照）

2016.11 米国大統領選挙へのロシアの干渉

米国政府発表によると、ロシアは、ハッキングで窃取したメールなどの公開・拡散、偽情報の流布やSNS上での工作によって、2016年米国大統領選挙に対する影響力工作を展開（→ P6参照）

2017.05 ランサムウェア「WannaCry」事案

ランサムウェア「WannaCry」が世界中に拡散し、我が国を含む約150か国の政府機関、医療機関、企業などに感染被害が発生

2017.09 米国企業「エクイファクス」からの個人情報窃取の発覚

米国信用情報会社「エクイファクス」が不正アクセスを受け、米国民約1億4,500万人分の個人情報（氏名、生年月日及び社会保障番号）などが窃取されたことが発覚

2020.12 IT管理ツールを利用したサプライチェーン攻撃の発覚

Solar Winds社製IT管理・監視ツール「Orion」の更新プログラムを悪用した大規模なサプライチェーン攻撃事案が発覚。米国サイバーセキュリティ・インフラセキュリティ庁（CISA）は、同ツールの即時利用停止を連邦省庁に指示する緊急指令を発令

2020年のサイバー脅威の概況

Cyber Threats in 2020

1 防衛産業などを狙った攻撃が相次いで発覚

2020年は、我が国で重要情報の窃取を狙ったとみられるサイバー攻撃、とりわけ防衛産業を標的としたサイバー攻撃事案の発覚が相次ぎました。

防衛装備品の調達先である大手電機メーカーA社は、2019年に発生した不正アクセス事案を公表し（2020年1月）、別の大手電機メーカーB社も、同社の防衛事業部門のサーバが2016年以降数年にわたって外部から不正アクセスを受けていたことを公表しました（2020年1月）。

A社の事案については、内部調査の結果、同社の中国拠点のウイルス対策管理サーバが**ゼロデイ攻撃**を受け、侵入が拡大したとされ、防衛省の指定する「注意情報」を含む情報が流出した可能性があることが判明しました（同年2月）。

重要 TITLE **海外拠点に要注意！**

侵入の経路

- **A社**　中国拠点のウイルス対策管理サーバに対するゼロデイ攻撃を利用
- **C社**　シンガポール拠点のサーバへの侵入をきっかけとして、国内サーバに不正アクセス
- **E社**　海外拠点を経由して国内サーバに不正アクセス

↓

国内に比べてセキュリティが手薄になりがちな海外拠点が攻撃の踏み台に

また、防衛関連事業も行う大手通信会社C社は、シンガポール拠点のサーバへの侵入をきっかけとして、国内サーバが不正アクセスを受け、情報が流出した可能性があると公表した（同年5月）ほか、大手重工メーカーD社も、在宅勤務中の職員に対するSNSでの**ソーシャル・エンジニアリング**を発端とする不正アクセス事案を公表しました（同年8月）。さらに、別の大手重工メーカーE社は、本来発生しないはずの海外拠点（タイ）から国内サーバへの接続を発見し、続いて断続的に他の海外拠点（インドネシア、フィリピン、米国）を経由した国内サーバへの不正アクセスが確認されたと公表しました（同年12月）。

1月20日
大手電機メーカーA社は、同社のネットワークに対する不正アクセスにより、個人情報及び企業機密が外部に流出した可能性がある旨を発表

1月31日
大手電機メーカーB社は、同社防衛事業部門の社内サーバの一部に対する不正アクセスを確認した旨を発表

5月28日
大手通信会社C社は、同社サーバへの不正アクセスにより、顧客企業のサービスに関する情報などが流出した可能性がある旨を発表

8月7日
大手重工メーカーD社は、同社グループ企業地方拠点のネットワークが不正アクセスを受けた結果、従業員などの氏名及びメールアドレスのほか、IT関連情報などが流出したと発表

12月28日
大手重工メーカーE社は、海外拠点を経由した国内サーバへの不正アクセスを確認した旨を発表

KEYWORD

ゼロデイ攻撃　：　未知の脆弱性を悪用した攻撃

ソーシャル・エンジニアリング　：　人間の心理・行動の隙を突くことで、情報を窃取し又は特定の行動を取らせる手段

Point

我が国の重要情報を狙うサイバー攻撃の脅威は継続。新型コロナウイルス感染症が拡大する環境下での攻撃傾向の変化や標的型ランサムウェア攻撃の増加も

2 新型コロナウイルスの感染拡大により新たな脅威も

新型コロナウイルス感染症の感染拡大により、サイバー攻撃の状況にも変化がみられます。

例えば、テレワーク環境の急速な整備と歩調を合わせるように、**VPN**などのネットワーク機器の脆弱性を利用した攻撃、ウェブ会議システムの利用に必要なファイルを装った標的型メール攻撃、同会議システムの乗っ取りなどの事案が確認されており、テレワーク環境が新たな攻撃の機会として狙われる傾向がうかがわれます。

また、新型コロナウイルス感染症に関する情報の窃取や、同感染症に関する情報提供を装った標的型攻撃の実行など、攻撃の目的・対象・手段にも影響を与えているとみられます。

重要 TITLE **医療分野が標的に**

米国CISA・英国NCSC共同アラート
（2020年5月5日）

- 新型コロナウイルス感染症への対応に関与する医療機関、製薬会社、研究機関などを標的とする攻撃が活発
- 感染拡大によって、新型コロナウイルス感染症関連の情報収集に対する関心が高まった可能性

↓

新型コロナウイルス感染症の感染拡大下では、引き続き医療分野が標的となる可能性

3 入念に準備されたランサムウェア攻撃が増加

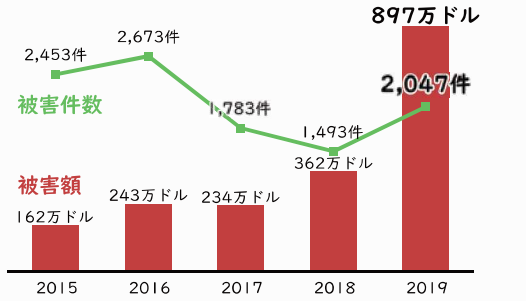
2020年には、**ランサムウェア**を利用した攻撃にも注目が集まりました。

従来のランサムウェア攻撃では、個人・企業を問わず、不特定多数を標的として、攻撃が成功した被害者に金銭を要求する形がとられました。

しかし、最近では、大手企業などを標的として、被害者のシステムに密かに侵入し、事業継続に不可欠なシステムや重要な情報を保存した端末などを特定して、ランサムウェアに感染させる事案が増加しています。また、システムなどを復旧させるための「身の代金」だけでなく、窃取した情報を暴露すると脅迫して金銭を要求する「二重脅迫型」の事案も増加しています。

重要 TITLE **被害額も増大……**

米国におけるランサムウェア被害件数・被害額
※ 米国インターネット犯罪苦情センター（IC3）への報告ベース



（出典：米国連邦捜査局「IC3 Annual Report」）

ランサムウェア攻撃の被害額は増大傾向。今後もますます脅威が高まる可能性

KEYWORD

VPN ： 「Virtual Private Network」の略。インターネットなどの公衆回線上に仮想の専用線を構築するサービス

ランサムウェア ： コンピュータを利用不能にした上で、復旧の見返りに「身の代金」を要求するマルウェア

サイバー空間における不正な活動

Malicious Activities in Cyberspace

情報窃取・サイバー諜報

政府機関や民間企業の情報システム、個人のPCやスマートフォンなどに侵入し、重要な内部情報を窃取したり、相手の動向を秘密裏に監視したりすることを目的にした活動です。政治、経済、外交、安全保障など、多岐にわたる分野が攻撃の標的となっています。

事例

日本年金機構における個人情報125万件流出事案（2015年公表）

日本年金機構の職員がメールに添付されたマルウェア付きファイルを開封した結果、PC端末が外部から遠隔操作され、加入者の個人情報約125万件が流出

事例

米国連邦人事管理局（OPM）における個人情報流出事案（2015年公表）

米国連邦人事管理局（OPM）がサイバー攻撃を受け、政府職員・契約業者などに関する社会保障番号（SSN）を含む個人情報約2,150万人分が流出。また、関連する別の攻撃によって、政府職員などに関する氏名、生年月日、住所、社会保障番号などの個人情報約420万人分も流出

情報システムの破壊・機能妨害（サイバー破壊活動）

情報システムの停止、誤作動などを引き起こすことを目的にした活動です。**DDoS攻撃**や事前に感染させたマルウェアなどが用いられ、ウェブサイトの改ざんや閲覧障害といった比較的軽微な被害のほか、重要インフラのまひといった深刻な被害を引き起こす攻撃もあり得ます。

事例

「Stuxnet」によるイラン核関連施設攻撃事案（2009～2010年）

報道などによると、イラン・ナタンツに所在するウラン濃縮施設のシステムに、「Stuxnet」（スタックスネット）と呼ばれるマルウェアが侵入し、同施設の遠心分離機を秘密裏に誤作動させ、約1,000台を物理的に破壊。同マルウェアは、インターネットから隔離された制御システムに、可搬記憶媒体を介して侵入した模様

事例

ウクライナにおける大規模停電事案（2015年）

ウクライナの電力会社がサイバー攻撃を受け、制御システムが不正に操作された結果、同国西部で数時間に及ぶ停電が発生し、約22万5,000人に影響

KEYWORD

ＤＤｏＳ攻撃　：　DDoSは「Distributed Denial of Service」の略。サーバの能力を超える多量の情報処理要求を一斉に送り、利用不能にする攻撃手法

Point

一言に「サイバー攻撃」と言っても、その目的や意図は様々。対策を立てる上では、攻撃者が何を狙っているのかを知ることが重要

不正な金銭獲得

銀行預金、暗号資産（仮想通貨）などを不正に獲得することを目的とした活動です。銀行や暗号資産交換所のシステムへの侵入による外部への不正送金、ランサムウェア、**クリプトジャッキング**などの手段が用いられます。

事例

バングラデシュ中央銀行における不正送金事案（2016年）

バングラデシュ中央銀行が標的型メール攻撃を受け、国際銀行間通信協会（SWIFT）システムを通じて米国ニューヨーク連邦準備銀行に不正な送金指図が送信された結果、バングラデシュから他のアジア諸国の口座への不正送金が実行。被害額は約8,100万ドルに上る模様

事例

暗号資産交換所における不正送金事案（2018年）

我が国企業が運営する暗号資産交換所のシステムが、外部からの不正アクセスを受けた結果、約580億円相当の暗号資産が不正に送金

心理戦・影響力工作（オンライン・インフルエンス・オペレーション）

情報の意図的な利用などにより、人々の認知、意思決定、行動などに影響を及ぼすことを目的にした活動です。欧米では、外国政府が窃取した情報や偽情報をオンライン上で流布するなどし、選挙などに際して世論に干渉することについて、民主主義の基盤を脅かす事態であるとの懸念が強まっています。

事例

2016年米国大統領選挙に対するロシアの干渉

米国政府発表によると、ロシアは、①ロシア軍当局者が民主党・クリントン候補陣営のメールなどをハッキングで窃取し、ネット上で公開・拡散する活動、②ロシア政府に近い企業が偽情報の流布やSNS上での工作を行う活動を展開

事例

2019年英国総選挙に対するロシアの干渉

英国政府発表によると、2019年英国総選挙を控え、米英自由貿易協定に関する政府の機密文書が違法に取得され、ソーシャルメディア「Reddit」を通じてオンライン上で拡散。英国政府は、ロシアの主体が同選挙に干渉しようとしたことはほぼ確実と結論

KEYWORD

クリプトジャッキング　：　暗号資産の「マイニング」（取引データの検証作業に必要なコンピュータの処理能力を提供して対価を得ること）を行うプログラムを他人のPCなどで勝手に実行させ、第三者が不正に金銭的利益を得る行為

サイバー空間における脅威主体

Threat Actors in Cyberspace

サイバー攻撃者（脅威主体）には、**ハクティビスト**集団、金銭目的の犯罪者、愉快犯、そして国家が関与・支援するサイバー攻撃集団など、多様な主体が含まれます。特に深刻な脅威として懸念されるのは、国家が関与・支援する高度なサイバー攻撃であり、一般的に次のような特徴があります。

- 諜報活動、重要インフラの破壊、情報操作など、政治的・軍事的な国家目標を達成するため、軍や情報機関のオペレーションとして実行
- 任務達成のため、コスト度外視で執ような攻撃を継続
- 犯罪者や民間のハッカーを外部の協力者・代理人として使う場合も

米国、英国などは、国家による不正なサイバー活動を抑止するため、攻撃実行者と背後にいる国家機関を特定・公表する取組（パブリック・アトリビューション、詳細はP9参照）をこれまで以上に活発に実施しており、以下のように、中国、ロシア及び北朝鮮の国家的関与を指摘しています。

1 中　国

軍・情報機関によるサイバー攻撃への関与、サイバー犯罪者との“共生関係”を指摘

最近の主なパブリック・アトリビューション

2020年2月

米国司法省は、大手信用情報会社「エクイファクス」へのハッキング（2017年）で、米国民約1億4,500万人分の個人情報などを窃取したとして、**中国人民解放軍「第54研究所」**に所属する4人の起訴を発表

2020年7月

米国司法省は、米国内外の政府機関、民間組織、人権活動家などを標的に、機密情報の窃取を狙ったサイバー攻撃を10年以上にわたり繰り返したとして中国人2人の起訴を発表。同省は、被告人らが**中国国家安全部**とも協力したほか、新型コロナウイルスのワクチン開発に従事する米国企業のネットワークの脆弱性を調査したと指摘

2020年9月

米国司法省は、「APT41」と呼ばれるサイバー主体による、IT企業など世界中の100以上の標的を狙った一連の攻撃に関与したとして、中国人ハッカー5人らの起訴を発表

米国司法省による「APT41」メンバーの起訴発表（写真：代表撮影/ロイター/アフロ）

KEYWORD

ハクティビスト　：　社会的・政治的主張を目的として、サイバー攻撃を行う個人・組織など。ハック（Hack）と活動家（Activist）を組み合わせた造語

Point

国家が関与・支援するサイバー攻撃が特に深刻な脅威。欧米諸国は、攻撃実行者と背後にいる国家機関を特定・公表するパブリック・アトリビューションを積極的に展開

2 ロシア

軍・情報機関によるサイバー攻撃への関与、治安機関とサイバー犯罪者との協力を指摘

最近の主なパブリック・アトリビューション

2019年12月

米国財務省は、ロシア拠点のサイバー犯罪組織「Evil Corp」に対する制裁を発表。同省は、組織指導者と**ロシア連邦保安庁（FSB）**が直接の協力関係にあると指摘

2020年2月

英国、米国、ジョージアなどは、ジョージアでの破壊・混乱を引き起こした大規模サイバー攻撃（2019年10月）を、**ロシア連邦軍参謀本部情報総局（GRU）**によるものと断定し、非難声明を発表

2020年7月

英国、カナダ及び米国は、サイバー主体「APT29」がロシア情報機関の一部であることはほぼ確実とした上で、新型コロナウイルス感染症ワクチンの開発組織に、情報窃取を狙ったとみられるサイバー攻撃を仕掛けていると警告

2020年10月

米英政府は、**ロシアGRU**が平昌冬季五輪の妨害を狙い、北朝鮮による攻撃を装ってサイバー攻撃を実行したと断定し、米国司法省が同機関所属の6人の起訴を発表

米国司法省によるGRU所属の6人の起訴発表（写真：代表撮影/ロイター/アフロ）

3 北朝鮮

サイバー攻撃を用いた不正な金銭獲得・諜報・破壊活動への軍の関与を指摘

最近の主なパブリック・アトリビューション

2020年7月

欧州理事会は、サイバー攻撃に関与した組織・個人に対する初の制裁措置の適用を発表。同発表で、ランサムウェア「WannaCry」について、「APT38」又は「Lazarus」と呼ばれる北朝鮮の主体が実行したと指摘

2020年9月

国連安保理北朝鮮制裁委員会専門家パネルは、中間報告書（同年8月付け）を公表。同報告書は、「Lazarus」と並んで**北朝鮮偵察総局**の傘下にあるサイバー主体「Kimsuky」が、安保理理事国の外交官や同パネル委員に標的型メールを送付し、情報窃取を狙ったサイバー攻撃を実行している模様と指摘

APT集団とアトリビューション

APT Groups and Attribution

サイバー攻撃の中でも、特に国家の関与・支援が想定されるような、洗練された攻撃を特定の標的に対して執ように行うサイバー主体は、APT（Advanced Persistent Threat: 高度で持続的な脅威）集団と呼ばれています。

世界中のセキュリティ企業では、その活動を検知・追跡するため、各APT集団にそれぞれ独自の識別名を付与しています。

一方、サイバー攻撃はその特性上、匿名性・秘匿性が高く、攻撃源は自明ではありません。このため、国家の関与・支援の下で行われた攻撃であっても、加害国が否認しやすいことから、伝統的な軍事的脅威に比べて抑止が難しい状況にあります。

こうした状況の中で、米英政府などは、サイバー攻撃の抑止及び対応を図る一環として、APT集団などの攻撃実行者と背後にいる国家機関を特定した上で、公開の場（起訴や制裁を含む）で当該国を名指しで非難する「パブリック・アトリビューション」と呼ばれる取組を強化しています。

欧米政府によって特定・公表されたAPT集団と国家機関のつながり

APT集団の識別名（カッコは別名の例）	関連する国家機関	関与したサイバー攻撃事案、標的の例
APT1 （Comment Panda）	中国人民解放軍 総参謀部第3部（当時） 61398部隊	・原子力メーカーなど在米6組織からの情報窃取（2006～2014年）
APT10 （Stone Panda）	中国国家安全部 天津市国家安全局	・米国企業・政府機関からの技術情報の窃取（2006～2018年頃） ・世界中のIT管理事業者（MSP）への侵入（2014～2018年頃）
APT28 （Fancy Bear）	ロシア連邦軍参謀本部 情報総局（GRU） 第85特務総センター （26165部隊）	・ドイツ連邦議会を狙った情報窃取（2015年） ・米国大統領選挙を狙った情報窃取・暴露（2016年） ・反ドーピング機関を狙った情報窃取・暴露（2016年） ・化学兵器禁止機関（OPCW）Wi-Fi侵入未遂（2018年）
Sandworm （BlackEnergy）	ロシア連邦軍参謀本部 情報総局（GRU） 特殊技術総センター （74455部隊）	・ウクライナ大規模停電（2015年、2016年） ・米国大統領選挙有権者情報の窃取など（2016年） ・ウクライナなどでの破壊型攻撃「NotPetya」（2017年） ・韓国・平昌冬季大会の妨害（2018年） ・ジョージアに対する破壊型攻撃（2019年）
APT29 （Cozy Bear）	ロシアの情報機関 （※）	・米国の政党への侵入（2015年） ・ワクチン開発企業の知的財産窃取（2020年）
Lazarus （APT38）	北朝鮮偵察総局 第3局110号研究所	・ソニーピクチャーズのシステム破壊・情報窃取（2014年） ・バングラデシュ銀行からの約8,100万ドル窃取（2016年） ・ランサムウェア「WannaCry」（2017年） ・世界中のATMからの不正出金（2016年～）

※　エストニア対外情報庁によると、ロシアの対外諜報庁（SVR）及び連邦保安庁（FSB）

（米国政府、英国政府、EU理事会及びエストニア対外情報庁の公表資料に基づいて当庁作成）

オリンピックなどに対するサイバー脅威

Cyber Threats to the Olympics and other major events

オリンピック・パラリンピック競技大会は、サイバー攻撃の脅威にさらされており、特に、英国・ロンドン大会（2012年7～8月）以降、その脅威は顕著となっています。

ロンドン大会では、大会運営に支障を来す被害は生じなかったものの、電力供給システムが攻撃者に狙われていた可能性もあったとされています。また、ブラジル・リオデジャネイロ大会（2016年8月）に際しては、世界ドーピング防止機構（WADA）のデータベースから、各国代表選手の医療情報（治療目的での薬剤使用記録など）が窃取され、インターネット上に暴露される事案が発生しました。さらに、韓国・平昌冬季大会（2018年2月）では、大会運営を支えるITシステムがデータ破壊型マルウェアによる攻撃を受け、開会式開催中に公式ウェブサイト（入場チケット印刷機能を含む）、会場内Wi-Fiサービスなどが一時停止するなどの被害が引き起こされました。

また、サイバー攻撃による大規模停電（2015年、ウクライナ）やニュージーランド証券取引所に対する分散型サービス妨害（DDoS）攻撃（2020年8月）など、重要インフラへのサイバー攻撃の脅威が現実のものとなっています。仮にこうした攻撃が東京2020オリンピック・パラリンピック競技大会の妨害に用いられた場合には、その影響は同大会にとどまらず、国民生活に深刻な影響が及びかねないことから、国家が関与・支援する主体によるものを始め、同大会の妨害を図る勢力によるサイバー攻撃に十分警戒する必要があります。

過去のオリンピック・パラリンピック競技大会をめぐるサイバー攻撃事例

ブラジル・リオデジャネイロ大会（2016年）

2016年9月、WADAのデータベースから窃取された、各国代表選手の医療情報（治療目的での薬剤使用記録など）を、「FANCY BEARS' Hack Team」を名のる者がウェブサイトで暴露

WADAは、ロシアのサイバー主体「APT28」による窃取・暴露であると発表。また、米国司法省は2018年10月、本件について、ロシア連邦軍参謀本部情報総局（GRU）第85特務総センター（26165部隊）によるものと断定し、同部隊員5人を含むGRU要員7人の起訴を発表

韓国・平昌冬季大会（2018年）

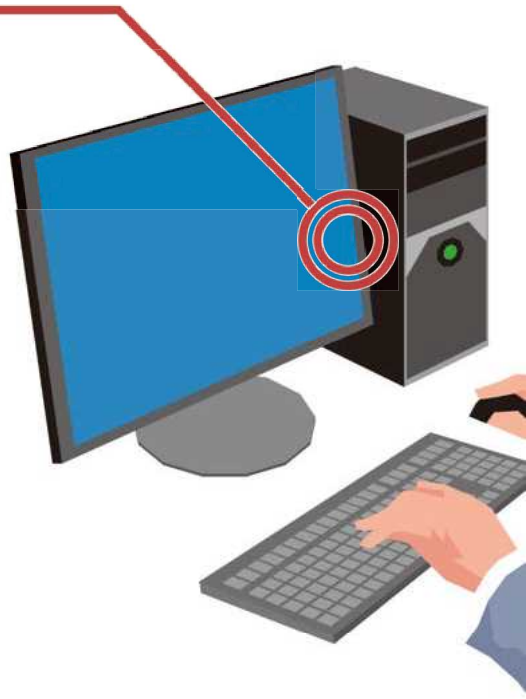
2018年2月、平昌冬季大会の開会式直前、「Olympic Destroyer」と呼称されるマルウェアを用いた破壊型サイバー攻撃によって、大会運営に用いるITシステムに障害が発生。その結果、公式ウェブサイト（入場チケットの印刷機能を含む）、会場でのWi-Fiサービス、プレスセンターにおけるTV及びインターネット通信といったサービスが一時停止

米国司法省は2020年10月、本件について、ロシアGRU特殊技術総センター（74455部隊）が北朝鮮によるサイバー攻撃に見せかけた「偽旗作戦」として実行したものと断定し、その他の攻撃に関する容疑と併せて、同部隊員6人の起訴を発表

サイバー攻撃の手法と対策

TTPs of Cyber Attacks and Responding Measures

システムの弱点を突いた攻撃



サイバー攻撃に関する報道では、「脆弱性」という言葉がよく使われます。この「脆弱性」とは、一言でいえば、コンピュータシステムなどの“欠陥・弱点”のことです。

システムを提供する企業は、脆弱性を修正するためのアップデートに日々取り組んでいます。しかし、脆弱性の中には、開発者や提供企業でさえ気付いていないもの（ゼロデイ脆弱性）も存在するなど、脆弱性の全てを特定して対処することは、事実上不可能です。また、企業がアップデートを提供していても、利用者がアップデートを適用していないケースもあります。

攻撃者は、主にマルウェア（不正プログラム）などを使って脆弱性を悪用することにより、システムに損害を与えたり、不正に操作したりして、攻撃目的の達成を試みています。

事例 VPN機器の脆弱性を利用した攻撃

- 2019年、**複数のVPN製品の脆弱性**が相次いで報告され、直後からその脆弱性を利用して認証情報を窃取・悪用したとみられる攻撃が確認
- この脆弱性については、各機器の製造業者が修正プログラムを提供しているものの、**その後も脆弱性が未修正のVPN製品が狙われる危険性**や、**修正前に窃取された認証情報などが悪用される危険性**が指摘

事例 認証方式の脆弱性を利用した攻撃

- 2019年、バーコード決済サービスの一部アカウントへの不正アクセスにより、サービスの不正利用などの被害が発生
- 被害企業は、別のサイトに対する攻撃などによって不正に入手したID・パスワードのリストを利用して不正アクセスを試みる**「パスワードリスト攻撃」**の可能性が高いと発表。パスワードのみの認証でアクセスを許可するという**認証方式に問題があった可能性**

対策の一例

- 使用しているPC、スマートフォンなどの機器を把握するとともに、修正プログラムを速やかに適用し、最新のバージョンに更新・維持
- 管理者は、認証方法として、**多要素認証**を活用することを検討。利用者も、パスワードを使い回さない、なるべく長い文字数で設定するなど、パスワードを適切に設定・管理
- サイバーセキュリティ関連組織の情報発信をチェックして、攻撃者の最新のTTP・対策を把握

KEYWORD

多要素認証　：　知識情報、所持情報、生体情報の各情報のうち、複数の認証情報を組み合わせた認証方法

ＴＴＰ　：　「Tactics, Techniques and Procedures」の略。攻撃者の戦術・技術・手順といった攻撃手口

Point

攻撃の手法は、日々進化・高度化。最新の脅威や攻撃の手法をよく知るとともに、手洗い・うがいを徹底するように、まずは基本的な対策をきちんと講じることが重要

提供：アフロ

人間の心の隙を突いた攻撃

攻撃者が利用するのは、システムの脆弱性だけではありません。攻撃者は、「ソーシャル・エンジニアリング」を駆使し、システムを利用する人間の心の隙を突き、だましたり誤解させたりすることで、システムへの不正アクセスなどを実現させようとしています。

人間の心理に付け込んだサイバー攻撃の最たる例が**標的型攻撃（スピアフィッシング）**です。メール受信者の関心を惹くテーマを使用したり、過去に使用されたメール文面を流用したりして、受信者に情報を入力させたり、不正な添付ファイルやURLをクリックさせたりします。

また、メールやウェブサイトを利用する「フィッシング攻撃」のほかにも、音声通信を利用する「ビッシング攻撃」、SMSなどのテキストメッセージを利用する「スミッシング攻撃」など、攻撃者は、様々な形で標的の心の隙を狙っています。

事例 メールを利用した標的型攻撃

- **マルウェア「LODEINFO」**の感染を狙った標的型メール攻撃が我が国で多数確認。「LODEINFO」は、アップデートを頻繁に繰り返し、画面キャプチャ機能やランサムウェア機能を新たに実装するなど、継続的に機能を拡張
- 攻撃メールには、不正な文書ファイルが添付。メールや添付ファイルには、**新型コロナウイルス感染症、外交、安全保障**などに関する内容を装ったものが確認

事例 SNSを利用した標的型攻撃

- 攻撃者は、目的に沿った標的を選定し、標的に接触・攻撃するため、**SNS上の自己紹介・投稿・画像などを検索して情報を収集**するなど、SNSを積極的に利用
- 機密情報の窃取を狙った攻撃では、**大手企業の人事担当者を装った虚偽のSNSアカウント**を利用し、標的とする企業の従業員に虚偽の求人情報を送り付け、マルウェアに感染させた事例も

対策の一例

- 少しでもおかしいと感じたら、届いたメール・SMS・SNSなどのURLや添付ファイルをクリックせず、相手方に送信の事実を確認したり、システム管理者に連絡したりして、慎重に対処
- 住所や電話番号、メールアドレスなどをSNSなどにむやみに投稿せず、趣味や仕事内容、友人関係などについての投稿がソーシャル・エンジニアリングに利用される可能性にも留意
- 不審なメールの検知を可能にする機能の導入など、技術面での適切な対策を実施

KEYWORD

標的型攻撃（スピアフィッシング）　：　標的組織の職員などに対して、同組織の関係者、著名な事業者などに巧妙になりすましたメールなどを送り付け、個人情報を不正に入手するなどする行為

公安調査庁のサイバー関連調査

Cyber-related Intelligence Efforts by Public Security Intelligence Agency

政府機関としての公安調査庁の役割

公安調査庁は、破壊的団体等の調査を行い、規制の必要があると認められる場合には、公安審査委員会に対し、その団体の活動制限や解散指定等の請求を行います。

公安調査庁は、我が国の情報関係機関によって構成される情報コミュニティのコアメンバーとして、官邸や内閣官房を始めとする関係機関に対し、政府の施策決定に資する情報を日々提供しています。

団体規制

- 暴力主義的破壊活動を行う危険性のある団体を調査
- 公安審査委員会に対し、活動の制限や解散指定等を請求
- 観察処分に付された団体に対する規制措置を実施

情報貢献

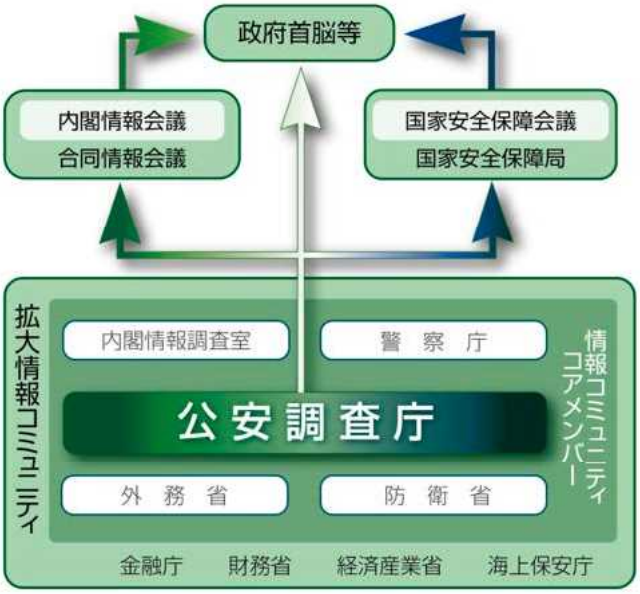
- 我が国の情報コミュニティのコアメンバー
- 関係機関に対し、政府の施策決定に資する情報を提供

サイバー関連調査の推進

公安調査庁は、サイバー空間の状況についても、情報の収集と分析を行った上で、関係機関への適時適切な情報提供を行っています。

サイバーセキュリティ政策における公安調査庁の役割

我が国政府の「サイバーセキュリティ戦略」（2018年7月閣議決定）に基づく最新の年次計画「サイバーセキュリティ2020」では、公安調査庁の役割として、「サイバー関連調査の推進に向け、人的情報収集・分析体制の強化及び関係機関への適時適切な情報提供等、サイバーインテリジェンス対策に資する取組を推進する」などとされています。



公安調査庁からの情報発信・公表資料

Publications from Public Security Intelligence Agency

公安調査庁ホームページ・SNS公式アカウント

公安調査庁ホームページでは、公安調査庁の所管法令、沿革、業務内容などについて紹介しているほか、国内外の諸情勢については、「オウム真理教関連情報」、「世界のテロ等発生状況」、「最近の内外情勢」などの各コンテンツに掲載しています。

公安調査庁公式TwitterやYouTube公安調査庁公式チャンネル「PSIAchannel」では、公安調査庁の施策や取組、お知らせしたい情報などを発信していますので、ホームページと併せてご覧ください。

Website

公安調査庁ホームページ
http://www.moj.go.jp/psia/

Twitter

「公安調査庁@MOJ_PSIA」

YouTube

「PSIAchannel」

内外情勢の回顧と展望

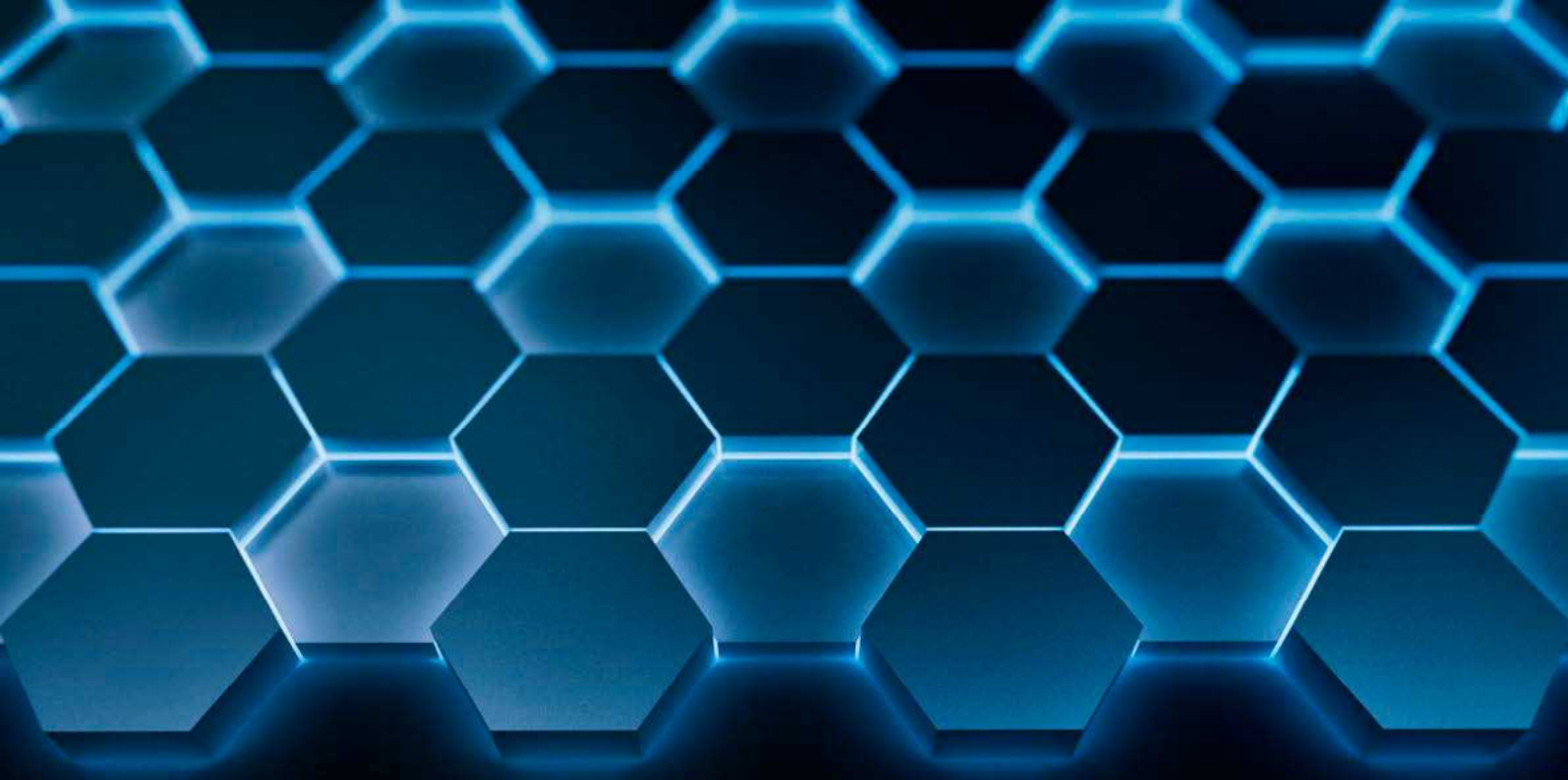
毎年1月、その前年の公共の安全に関わる国内外の諸情勢を「内外情勢の回顧と展望」に取りまとめて、発刊しています。

最新版及び過去の「内外情勢の回顧と展望」は、公安調査庁ホームページでもご覧いただけます。

国際テロリズム要覧

平成5年以降、世界のテロリズムの動向について取りまとめた「国際テロリズム要覧」を発刊しています。

また、公安調査庁ホームページには「国際テロリズム要覧」2020年版を国民の皆様に広く知っていただくことを目指し、同要覧をわかりやすく再編集して掲載しております。



情報の力で、国民を守る。

公安調査庁