# Overview of Threats in Cyberspace

# サイバー空間における脅威の概況 2023

公安調査庁

# はしがき

公安調査庁は、破壊活動防止法及び団体規制法に基づいて、我が国の公共の安全の確保を図ることを任務としており、我が国の情報コミュニティのコアメンバーとして、サイバー攻撃のほか、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、政府の安全で安心な社会を目指す施策の推進に貢献しています。

サイバー空間における脅威が増大する中、その脅威について周知するため、公安調査庁では、2020年、「サイバー攻撃の現状2020」を作成しました。2021年以降は、サイバー空間における脅威をより網羅的に記載した内容とし、名称も「サイバー空間における脅威の概況」に改めて版を重ねてきたところ、今回、2023年版を作成する運びとなりました。

サイバー空間における脅威は、依然として深刻な状況であり、また、偽情報の拡散を含むサイバー空間上での影響工作についても注目が集まるなど、サイバー空間において注視すべき分野は拡大しています。

そうした状況を受け、本冊子においては、2022年におけるサイバー脅威の概況として、非国家主体の活動や偽情報の拡散がもたらす脅威などを取り上げるとともに、宇宙・海洋分野へのサイバー空間の拡大に伴う脅威の増大について特集で示しました。

また、国家等が関与・支援するサイバー攻撃について、その概要や欧米諸国等によるパブリック・アトリビューションをまとめたほか、サイバー攻撃に対する基本的な対処法や最新のサイバーセキュリティの考え方を、「サイバー攻撃の手法と対策」として示しています。

本冊子については、公安調査庁ホームページに掲載しているところ、サイバー空間における脅威について、国民の皆様の理解の一助となりましたら幸いです。

※ 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。

# サイバー空間における脅威の増大

機密情報の窃取、金銭の獲得、業務の妨害などを狙った**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、サイバー空間の現実社会への拡大・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。

さらには、国家主体が、政治的、経済的、軍事的目的を達成するため、**情報窃取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深刻化しています。

## 近年の主なサイバー攻撃等

**2015.12** ウクライナにおける大規模停電事案

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

**2016.11** 米国大統領選挙へのロシアの干渉

米国政府の発表によると、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工作を展開 (→P.8参照)

**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 (→P.12参照)

**2020.12** IT管理ツールの更新プログラムを悪用した攻撃の発覚

米国情報通信企業「SolarWinds」製IT管理ツールの更新プログラムを悪用した攻撃に端を発した大規模サイバー攻撃事案が発生。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 (→P.11参照)

**2021.05** 我が国大手情報通信企業の情報共有ツールを経由した攻撃の発覚

我が国大手情報通信企業が提供する情報共有ツールに対するサイバー攻撃が発覚。後に、同ツールを利用する100以上の組織から個人情報を含むデータが窃取されたことが判明

**2022.02** ウクライナ侵略直前に発生した衛星通信網に対するサイバー攻撃事案

米英政府の発表によると、ロシアは、ウクライナ侵略の直前、ウクライナの指揮管制を混乱させる目的で、米国情報通信企業「Viasat」が運用する衛星通信網を攻撃。ウクライナで数千件、欧州全体で数万件の顧客の通信が停止 (→P.6参照)

KEYWORD **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

# 多様化する非国家主体の活動

**2022年は、国際的な事象に関連して活動する非国家主体によるサイバー攻撃が発生しました。**

ウクライナ侵略を契機に、サイバー空間には、ロシア又はウクライナ支持派の集団・個人が現れ、約200のグループが乱立しているとの報道も見られました。中でも、3月、ロシアを支持し、「Killnet」を名のるハッカー集団は、米国及びその同盟国の政府機関や重要インフラ企業のウェブサイトへのDDoS攻撃を実行したとされるほか、5月には、ウクライナやNATO加盟国をサイバー攻撃の標的として名指ししました。また、9月には、我が国の行政機関、鉄道会社のウェブサイト等において、一時的に閲覧障害が発生しました。「Killnet」は、その一部に関して犯行を自認し、その後も、世界中の組織に対するDDoS攻撃を継続しています。


「Killnet」が投稿した、日本に宣戦布告する動画のスクリーンショット

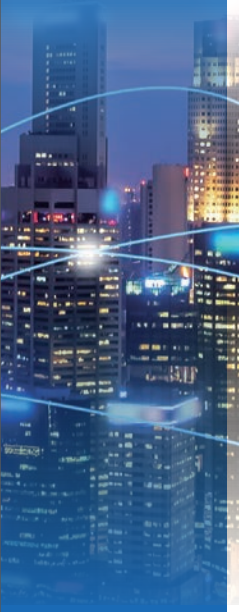
（写真提供：時事）

さらに、国際ハッカー集団「アノニマス」の一部を始め、ロシア政府に対するサイバー攻撃を実行したと主張するグループも見られました。

また、8月、米国のペロシ下院議長の台湾到着直前から、台湾で総統府等の多数のウェブサイトに対するDDoS攻撃が発生したほか、駅やコンビニを始め、各地でTVモニターがハッキングされ、同議長を批判するメッセージが映し出されました。その後、「27Attack」を名のる中国の愛国的ハッカー集団が、総統府等に対するサイバー作戦を実行した旨主張しています。

訪台したペロシ米国下院議長と蔡英文総統

（写真提供：Â©Chien Chih－Hung/Taiwan President/Planet Pix via ZUMA Press Wire/共同通信イメージズ）



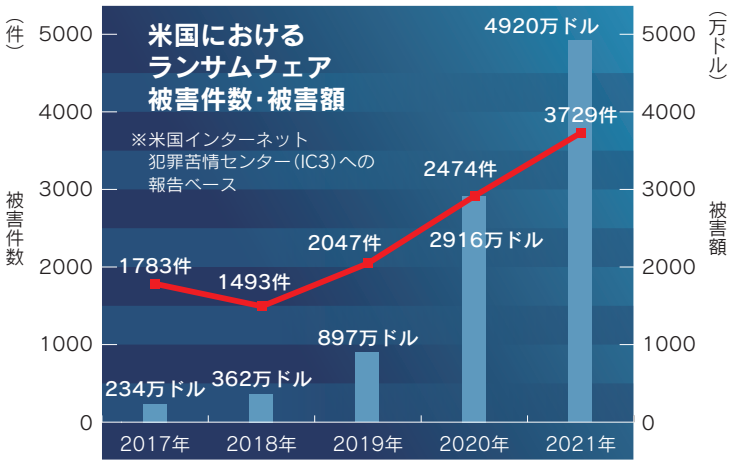


KEYWORD **DDoS攻撃**：多数の端末から多数の処理要求を送りつけ、サーバーをダウンさせるサイバー攻撃

# 我が国内外でランサムウェア攻撃が多数発生

**データを暗号化するなどして使用不能にし、その復元等の対価として金銭を要求するランサムウェア攻撃の脅威は、近年、国内外で拡大を続けているところ、2022年も、関連する被害が相次ぎました。**

我が国大手自動車部品メーカーでは、2月末に取引先で外部からの不正アクセスに起因するシステム障害が発生した影響により、国内工場での生産を一時的に停止する事態となりました。これは、後にランサムウェア攻撃であった可能性が報じられています。



(米国連邦捜査局「IC3 Annual Report」に基づき当庁作成)

このほかにも、2月から3月にかけて、自動車関連企業及びその海外拠点に対するランサムウェア攻撃が複数判明しました。

医療機関に対するランサムウェア攻撃も発生しています。米国の研究では、2016年から2021年にかけて、同国の医療機関に対するランサムウェア攻撃の件数が倍増したことが指摘されています。また、米国連邦捜査局（FBI）も、2021年にランサムウェア攻撃を受けたことが確認された重要インフラ分野のうち、医療・公衆衛生分野における件数が最も多かったと報告しています。

大阪の医療機関のシステム障害で、「調整中」の札が貼られた外来患者用の受付機
(写真提供：時事)

我が国でも、6月に徳島県の医療機関が、ランサムウェア「LockBit 2.0」を用いるサイバー犯罪グループによるサイバー攻撃を受け、電子カルテや院内LANが使用不能となったほか、10月に発生した大阪の医療機関に対するランサムウェア攻撃では、電子カルテシステムの障害の影響により、通常診療の再開に1か月以上を要する被害が発生しました。

こうした状況を受け、ランサムウェア対策に関する国際的な取組も進められています。欧州刑事警察機構（ユーロポール）を中心に、各国の法執行機関や民間セキュリティ企業などが参加するプロジェクト「NO MORE RANSOM」では、ランサムウェアの特定、復号ツールの提供等をウェブサイトを通じて行っています。また、米国が主導し、我が国を含む37か国・機関が参加して11月に開催されたランサムウェア対策に係る国際会議を受け、2023年1月には、オーストラリアを議長国として、脅威情報の共有、不正資金対策、攻撃者の摘発などに関する国際協力の促進を目的とする「国際ランサムウェア対策タスクフォース」が発足しました。

# 偽情報の拡散がもたらす脅威

**偽情報は、社会不安を利用し、人々の認知、意思決定、行動等に影響を及ぼし、混乱をじゃっ起する可能性があります。**

2022年は、国際的な事象に関連して流布された偽情報に注目が集まりました。

例えば、ロシアによるウクライナ侵略に際して、3月、ロシア外務省報道官が「ウクライナがロシアとの国境付近で生物化学兵器の開発を行っていた証拠を得た」との主張を展開しましたが、米国大統領報道官はこれを否定しました。また、4月には、「ウクライナ人武装勢力の拠点を襲撃した際、米国パスポートを持つ外国人傭兵の遺体が発見された」（4月17日付けロシア紙「コムソモリスカヤ・プラウダ」）との報道もなされましたが、ワシントンポスト紙は、同パスポートの所持者にインタビューを行い、ロシア紙の報道が誤りであると報じました。

また、米国のペロシ下院議長の台湾訪問（8月2～3日）に際して、中国国営メディアCCTVの記者が「中国軍機が台湾海峡を横断」などとブログに投稿し、同メディア等で拡散されましたが、台湾の国防部は同報道を否定する発表をしています（右上図）。


台湾国防部が「中国軍機が台湾海峡を横断」という投稿を「偽情報」と発表

（写真：台湾国防部ウェブサイト https://air.mnd.gov.tw）

加えて、台湾の国防部は、「台湾の桃園国際空港が中国人民解放軍によるミサイル攻撃を受けた」、「中国軍機が台湾軍機を撃墜した」といったSNS投稿は偽情報であるとして、台湾の市民に注意を呼び掛けました（右下図）。

我が国でも、同時期にツイッターで「ペローシ議長搭乗の航空機撃墜」との投稿が確認されましたが、同投稿は、「Yahoo!Japan」のニュースサイトを装ったアカウントによるもので、公式アカウントにそのような投稿はなく、同ニュースサイトは、偽アカウントが発する情報への注意を呼び掛けました。


台湾国防部が「桃園空港は正常に機能中」と発表

（写真：台湾国防部 Facebook https://www.facebook.com/MilitarySpokesman）

特集

# 宇宙・海洋分野に対するサイバー攻撃

**人工衛星の稼働数の増加やその活用の拡大、ナビゲーションシステムやエンジン制御システム等の導入といった海事産業のIT化もあいまって、宇宙・海洋分野にもサイバー空間は拡大を続けており、それに伴い、宇宙・海洋関連のサイバー攻撃も増加傾向にあるとされています。**

宇宙関連では、2022年2月、ロシアによるウクライナ侵略の1時間前に、米国情報通信企業「Viasat」が運用する衛星通信網のネットワークがサイバー攻撃を受け、ウクライナで数千件、欧州全体で数万件の顧客に対する通信サービスが停止し、ドイツでは、数千基の風力タービンの遠隔監視ができなくなりました。

**主な宇宙関連のサイバー攻撃事案**

| 発表時期 | 発生国 | 事案概要 |
|---|---|---|
| 2017年11月 | 米国 | 計測機器メーカー等へのサイバー攻撃により、全地球航法衛星システムの技術を含む営業秘密が窃取 |
| 2020年2月 | 我が国 | 衛星画像を扱う航空測量企業がサイバー攻撃を受け、社内ネットワーク端末への不正アクセスを確認 |
| 2020年9月 | 米国を含む5か国 | イラン革命防衛隊の支援を受けたハッカーが、スピアフィッシングメールによってマルウェアを送付し、衛星関連企業のシステムに侵入 |
| 2021年7月 | 韓国 | 韓国航空宇宙研究院（KARI）が北朝鮮のサイバー脅威主体からサイバー攻撃を受け、情報が流出 |
| 2022年2月 | ウクライナを含む欧州 | 米国情報通信企業「Viasat」が運用する通信衛星「KA-SAT」の地上モデムに対し、DoS攻撃やマルウェア頒布が発生し、衛星通信サービスが停止。欧州では、フランス、ドイツ、チェコのインターネット・サービス・プロバイダがサービスを停止 |

海洋関連では、2019年2月に、米国・ニューヨークなどの港に向かって航行中の船舶のコンピュータシステムがマルウェアに感染し、その機能が大幅に低下するなど、船舶の運用技術システムに対するサイバー攻撃事案が発生しました。

また、2021年には、我が国海運会社が不正アクセスを受け、情報流出の可能性が確認されたほか、2022年には、ドイツ、ベルギー及びオランダの港湾施設が相次いでサイバー攻撃を受け、加えて、インドの港湾でも、ランサムウェアを用いたとみられるサイバー攻撃によって、一部ターミナルの管理システムが停止する事案が発生しました。

サイバー攻撃で内部情報が流出した可能性がある我が国海運会社のデータを販売していると主張するダークウェブ上のサイト

（写真提供：時事）

2023年に入っても、1月初旬、欧州の船舶検査機関「DNV」が運用する船舶管理ソフトウェアのサーバーがランサムウェア攻撃を受けた結果、同ソフトウェアを導入している約1,000隻の船舶に影響が及ぶ事案が発生しました。

サイバー空間における
# 不正な活動 1


## 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。諜報活動の一環として、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。

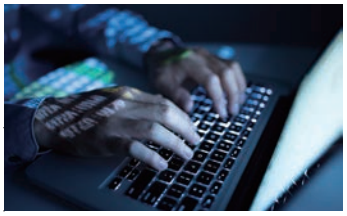
**日本年金機構における個人情報125万件流出事案**（2015年公表）

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

**安全保障への影響を及ぼすおそれのあるデータファイル流出の可能性**（2021年公表）

我が国大手電機メーカーに対するサイバー攻撃（2019年）について、同攻撃により外部に流出した可能性のある防衛関連の情報が記録されているデータファイル約2万件のうち、安全保障への影響を及ぼすおそれのあるデータファイルが59件あったことが判明

サイバー空間における
# 不正な活動 2



## 情報システムの破壊・機能妨害

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、重要インフラの機能停止といった深刻な被害を引き起こす攻撃もあります。

**インドにおける大規模停電事案**（2020年）

インド・ムンバイで大規模な停電が発生し、これにより、鉄道の運行等が停止したほか、病院は非常用電源に切り替える事態に。同国と中国の軍事衝突が発生し、両国の緊張が高まる中での事案であり、米国セキュリティ企業は中国によるサイバー攻撃が原因との報告書を公表

**ウクライナ金融機関等に対するサイバー攻撃事案**（2022年）

米国及び英国は、オンライン決済や銀行アプリの使用にも支障を来したとされるウクライナの金融機関等に対するDDoS攻撃に、ロシアの軍情報機関が関与したと発表

サイバー空間における
## 不正な活動 3
# 不正な金銭獲得

銀行預金、暗号資産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。

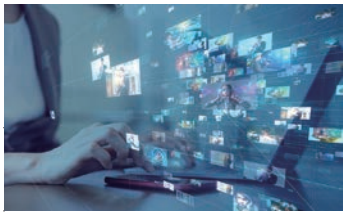
### ハッキングによるATMからの不正出金事案（2018年、2020年公表）

米国政府発表によると、北朝鮮のサイバー脅威主体が、金融機関のシステムへのハッキングを通じて、2015年以降、数十か国に所在するATMから多額の現金を不正に出金

### ブロックチェーンゲームにおける不正送金事案（2022年公表）

ベトナム企業が開発したブロックチェーンゲームが、外部からの不正アクセスを受けた結果、約6億ドル相当の暗号資産が不正に送金

サイバー空間における
## 不正な活動 4
# 影響工作（オンライン上のインフルエンス・オペレーション）



情報の意図的な利用により、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とした活動です。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で流布し、選挙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。

### 2016年米国大統領選挙に対するロシアの干渉（2019年公表）

米国政府発表によると、2016年米国大統領選挙に際し、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

### 2019年英国総選挙に対するロシアの干渉（2020年公表）

英国政府発表によると、2019年英国総選挙に際し、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で拡散。英国政府は、英国のEU離脱が争点とされていた同選挙にロシアの主体が干渉しようとしたことはほぼ間違いないと結論

KEYWORD **クリプトジャッキング**：暗号資産の「マイニング」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

# 脅威主体とアトリビューション

脅威主体（サイバー攻撃者）には、ハクティビスト集団[KEYWORD]、金銭目的の犯罪者、愉快犯、そして国家等が関与・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、国家等が関与・支援する高度なサイバー攻撃集団であり、一般的に次のような特徴があります。

- **重要インフラの破壊、情報操作、諜報活動など、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攻撃を実行**
- **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**

国家等の関与・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脅威主体は、APT（Advanced Persistent Threat：高度で持続的な脅威）と呼ばれています。

## 国家等が関与･支援するサイバー攻撃の概要

| | | |
|---|---|---|
| 中国 | 攻撃主体 | 中心となっているのは人民解放軍（戦略支援部隊）及び国家安全部、これらの組織から委託を受けた企業、サイバー犯罪者等 |
| | 特徴 | 主に「中国製造2025」で重点領域として示された10の重要産業（次世代情報通信技術、航空･宇宙設備、海洋建設機械･ハイテク船舶、省エネ･新エネルギー自動車など）を標的に情報窃取を実行していると指摘 |
| ロシア | 攻撃主体 | ロシア連邦軍参謀本部情報総局（GRU）、対外情報庁（SVR）、連邦保安庁（FSB）、その他（サイバー犯罪者、企業等） |
| | 特徴 | サイバー戦を「情報戦」（Information Warfare）の一環と位置付け<br>● 敵国の内情を把握し、自国の優位性を確保するための情報窃取・操作・暴露<br>● 敵国の軍事、行政、産業システムの破壊、混乱の誘発 |
| 北朝鮮 | 攻撃主体 | 中心となっているのは偵察総局及びその下部組織 |
| | 特徴 | 自国経済の一助とするための外貨獲得、情報窃取、破壊行為等による挑発や報復 |

KEYWORD **ハクティビスト集団**：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。「不正にコンピュータシステム等に侵入すること」を意味する「ハック」と、「活動家」を意味する「アクティビスト」を組み合わせた造語

# 1 中国

最近の主な
パブリック・アトリビューション

▼

**2021年7月**

米英政府などは、「APT40」と呼ばれる中国サイバー脅威主体がサイバー空間の安全等を脅かしているとする声明を発表。我が国政府（外務省報道官談話）も、「APT40」は中国政府を背景に持つものである可能性が高いと指摘した上で、米英政府などのアトリビューションを支持

また、米国司法省は、知的財産及び営業秘密の窃取を目的とした世界規模でのサイバー攻撃キャンペーンに関与したとして、コンピュータ詐欺罪及び経済スパイの共謀の容疑で、海南省国家安全庁の職員3人を含む「APT40」関係者計4人の起訴を発表


FBIによるAPT40関係者の手配書
（写真：FBIホームページ https://www.fbi.gov）

**2022年7月**

米国連邦捜査局（FBI）長官と英国保安局（MI5）長官は、中国政府及び中国共産党の脅威について共同会見を実施し、その中で、国家が背景にあるサイバー脅威主体による政府、民間部門への攻撃が観測されており、その活動が大規模かつ洗練されてきている旨指摘。その際、MI5長官は、中国による航空宇宙企業への高度なサイバー攻撃を阻止（5月）したとも言及

MI5のマッカラム長官（左）と
FBIのレイ長官（右）の共同会見
（写真：MI5ホームページ https://www.mi5.gov.uk）

KEYWORD **パブリック・アトリビューション**：政府等が、サイバー攻撃の抑止及び同攻撃への対応を図る一環として、APT集団などの攻撃実行者とその背後にいる国家等の機関を特定した上で、公に当該国を名指しで非難する取組

# 2 ロシア

**最近の主な**
**パブリック・アトリビューション**

▼

**2020年10月**

米英政府は、ロシア連邦軍参謀本部情報総局（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

米国司法省は、GRU所属の６人の起訴を発表

**2021年4月**

米国財務省は、2020年の大統領選挙への介入に関与したとする16組織・16個人のほか、ロシア情報機関のサイバー活動を支援したとするロシア企業６社を制裁対象に指定

また、バイデン大統領は、「SolarWinds」社製品を利用したサプライチェーン攻撃に端を発する大規模サイバー攻撃事案につき、「APT29」（別名「Cozy Bear」）と呼ばれるロシア対外情報庁（SVR）を背景に持つサイバー脅威主体が実行した可能性が高いと非難し、ワシントンに駐在するロシア外交官10人の追放も発表

**2022年3月**

米国コロンビア区連邦裁判所大陪審は、ロシア国防省傘下の研究機関の職員について、2017年５月から同年９月にかけて、外国の石油精製所で使用されていた制御システムにマルウェア「TRITON」を感染させ、精製所の運転を停止させたとして起訴を公表

**2022年5月**

ロシアのウクライナ侵略に先立つ1月13日に実行された、ウクライナ政府機関のウェブサイトの改ざん及び破壊型マルウェア「WhisperGate」の頒布について、英国外務省は、ロシアの軍事情報機関がほぼ確実に関与したものであるとの評価を公表

# 3 北朝鮮

**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」を利用した攻撃について、「Lazarus」（別名「APT38」）と呼ばれる北朝鮮のサイバー脅威主体が実行したと指摘

**2021年2月**

米国司法省は、破壊的サイバー攻撃及びサイバー金融犯罪（金銭及び暗号資産の窃取、ランサムウェアによる恐喝並びに悪意ある暗号資産アプリケーションの開発・配信等）などに関与したとして、北朝鮮偵察総局所属のハッカー３人の起訴を発表

米司法省が起訴した北朝鮮の３被告
（写真：FBIホームページ
https://www.fbi.gov）

**2022年4月**

米国連邦捜査局（FBI）は、ベトナム企業が開発したブロックチェーンゲームのネットワークに対するサイバー攻撃による暗号資産の窃取事案につき、「Lazarus」等と呼称される北朝鮮のサイバー脅威主体が実行したものである旨発表。米国財務省は、当該事案で用いられた北朝鮮の暗号資産ウォレットを制裁リストに追加

**2022年10月**

国連安保理北朝鮮制裁委員会専門家パネルが、2022年度の中間報告書（9月7日付け）を公表。その中で、北朝鮮のサイバー脅威主体が2022年中に数億米ドル相当の暗号資産を窃取したことや、情報収集を目的としたサイバー活動を継続していることを指摘

### 我が国におけるアトリビューション関連動向

北朝鮮によるサイバー攻撃に関して、2022年10月、我が国金融庁、警察庁及び内閣サイバーセキュリティセンターが、暗号資産取引に関わる個人・事業者に向けた注意喚起を実施。また、同年12月、我が国外務省、財務省及び経済産業省が、北朝鮮のサイバー脅威主体「ラザルス・グループ」（Lazarus Group）を資産凍結等の措置の対象者に追加する旨発表

サイバー 攻撃の手法

# システムの弱点を突いた攻撃

→ 対策の例 はP.15

サイバー攻撃に関する報道では、「ぜい弱性」という言葉がよく使われます。この「ぜい弱性」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、ぜい弱性を修正するため、システムのアップデートに日々取り組んでいます。しかし、ぜい弱性の中には、開発者や提供企業でさえ気付いていないもの（ゼロデイぜい弱性）も存在しており、ぜい弱性の全てを特定し、これらに対処することは、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、主にマルウェアなどを使ってぜい弱性を悪用**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機器のぜい弱性を利用した攻撃

近年、複数のVPN機器のぜい弱性が相次いで報告されており、これを利用して認証情報を窃取・悪用したとみられる攻撃が発生

2021年10月末には、ランサムウェア「LockBit 2.0」を用いるサイバー犯罪グループが、我が国の公立病院を攻撃。電子カルテが暗号化されたほか、院内のシステムがダウン。同攻撃においては、同病院が使用していたVPN機器のぜい弱性が狙われた模様

## 事例 クラウドサービスのぜい弱性

クラウドとは、利用者に対してネットワーク経由でデータ、ソフトウェア、サーバー等を提供するサービスであり、その利便性やテレワークの導入により、情報資産管理手段として企業での利用率が年々上昇。一方、クラウドは、サイバー攻撃による侵入経路の一つとなっており、人為的設定不備によるぜい弱性が内在する場合のほか、暗号資産をマイニングするマルウェアを頒布する攻撃者の主要な標的にも

2022年1月には、南米拠点とされるサイバー犯罪集団「Lapsus$」が、認証サービスをクラウドで提供する米国企業のシステムに、業務委託先を通じて侵入。数百の顧客データが閲覧又は操作された可能性。また、我が国企業でも、2022年5月、クラウドサービスのネットワーク機器が、ぜい弱性を悪用した不正アクセスを受け、情報セキュリティ・システムの設定不備もあいまって、一部の顧客の認証情報が窃取された可能性が指摘。イスラエルのセキュリティ企業によると、2022年における1組織当たりのクラウドサービスに対するサイバー攻撃数は、2021年に比べ約50%増加しており、クラウドサービスに対するサイバー攻撃は、大きな脅威に

クラウドサービスを利用する際には、データセンターの物理的な情報セキュリティ対策、データのバックアップ、OS・ソフトウェア等のぜい弱性対策、不正アクセスの防止、アクセスログの管理、通信の暗号化、ハードウェア機器の障害対策などの情報セキュリティ対策が事業者によって適切に実施されているかを確認することが必要

KEYWORD
**ゼロデイぜい弱性**：存在が公表される前や、修正用プログラムが提供される前の未知のぜい弱性
**VPN**：拠点間の通信を安全に行うため、インターネット上に構築した仮想的な専用回線

サイバー 攻撃の手法

# 人間の心の隙を突いた攻撃

→ 対策の例 はP.16

攻撃者が利用するのは、システムのぜい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。

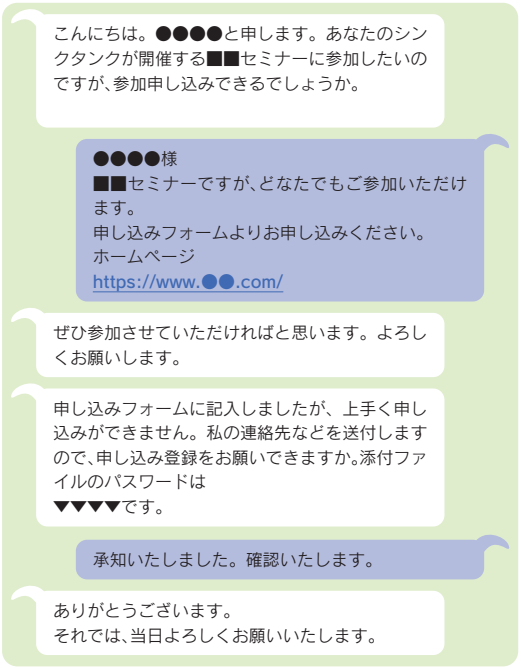
**人間の心理に付け込んだサイバー攻撃**の最たる例が標的型攻撃（スピアフィッシング）です。メール受信者の関心を引くテーマを使用したり、過去に使用されたメール文面を流用したりして、受信者に情報を入力させたり、不正な添付ファイルやURLをクリックさせたりします。

また、個人情報を窃取するための手法として、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、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･SNSを利用した標的型攻撃

攻撃者は、事前にSNSを含む様々な手段で情報を収集した上で、大手企業の人事担当者や取引先企業の社員を装い、不信感を持たれないメッセージを送付

実際にあった標的型メールの事例の中には、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のほか、製品購入に向けて取引先企業の社員とメールでやり取りしていた際、何者かが同取引先企業の社員になりすまし、偽の振込先を記載したメールを送付するなど、メールのやり取りを把握していたと思われる事例も確認




攻撃者（左）が、セミナー参加を装い、エラー発生と偽ってマルウェア入りファイルを被害者（右）に送付
（実際に発生した事例を参考に当庁作成）

また、学術関係者やシンクタンク研究員、報道関係者等に対し、実在する組織の社員・職員等を装い、講演・取材の依頼メールや資料等を送付するなどして不正なプログラムを実行させ、情報を窃取しようと試みるサイバー攻撃が近年多数確認されており、警察庁及び内閣サイバーセキュリティセンターにおいても注意喚起。同種事例では、実際に予定されているセミナーへの参加を装い、マルウェア入りのファイルが送信される事案も発生

KEYWORD

**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

**標的型攻撃（スピアフィッシング）**：標的に対して、標的の関係者等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

サイバーセキュリティ 対策の例

# システムに対する攻撃への対策

● **使用しているPC・スマートフォンなど機器の状態やソフトウェア・アプリのバージョンを把握するとともに、速やかに最新版に更新**

**【参考】**

独立行政法人情報処理推進機構（IPA）や米国サイバーセキュリティ・インフラセキュリティ庁（CISA）、米国国立情報標準研究所（NIST）などがぜい弱性情報を公表しています。

- 独立行政法人情報処理推進機構（IPA）
  https://www.ipa.go.jp
- 米国サイバーセキュリティ・インフラセキュリティ庁（CISA）
  https://www.cisa.gov
- 米国国立情報標準研究所（NIST）によるぜい弱性データベース
  https://nvd.nist.gov

● **管理者は多要素認証を導入し、利用者はパスワードを使い回さず、推測困難な長い字数で設定し、適切に管理**

**【参考】**

多要素認証とは、認証の３要素（知識情報、所持情報、生体情報）のうち、２つ以上を組み合わせて認証することで、以下のような具体例があります。

- 知識情報（暗証番号）＋所持情報（電話やSMS、アプリ等によるワンタイムパスワード認証など）
- 知識情報（パスワード）＋生体情報（静脈認証、指紋認証など）

● **サイバーセキュリティ企業などの情報発信をチェックして、攻撃者の最新のTTPを把握し、適切な対策を実施**

## 次世代のセキュリティ製品として注目される「EDR」

近年、APTを始めとする標的型サイバー攻撃の高度化・巧妙化に伴って、ウイルス対策ソフトでは検出できない攻撃が増加しています。また、クラウドサービスの普及やテレワークを含む働き方の多様化もあいまって、組織のネットワークの外側からの通信のみを監視する従来の「境界型セキュリティ」では脅威への十分な対応ができなくなっている状況にあります。

こうした状況への対応策の一つとして導入が進められているセキュリティ製品が「EDR」（Endpoint Detection and Response）です。EDRは、「ゼロトラスト」の考え方に基づき、組織のネットワークのエンドポイント（PCやサーバ、モバイル等）の動作や操作などを監視し、不審な挙動の中から攻撃を検知することから、迅速な初期対応（ネットワークの遮断やプロセスの停止）も可能となるほか、未知のマルウェアに対しても有効であるといった特徴があるとされています。

**KEYWORD**

**TTP**：攻撃者の戦術・技術・手順といった攻撃の手口
**ゼロトラスト**：組織のネットワークの内外を区別せず全ての通信を等しく「信頼できない」とみなし、システムへの侵入を前提として、全ての通信を検知、認証を行うという考え方

サイバーセキュリティ **対策の例**

# 人間の心の隙に対する対策

- **少しでもおかしいと感じたら、メール・SMSなどの添付ファイルやURLをクリックせず、真正な送信者と思われる者に電話などで確認したり、システム担当者に連絡したりして、慎重に対処**

**【参考】**

活動が再開したと報道されるマルウェア「Emotet」は、アドレス帳やメールの送受信履歴などといった情報を抜き取った上、これらの情報を用いて、取引先や顧客に対し、正規の送信者として「Emotet」に感染したメールを送付するため、受信者が送信者情報などを信頼して添付ファイルを開けてしまう危険性が高まります。

また、過去にやり取りした内容などを使用した標的型メール攻撃も行われており、メールの真偽を見分けることが難しくなっています。

以下の点について、より注意を払うことで、不審なファイルの実行やURLのクリックを未然に防止できる可能性が高まります。

- メールの表題が自身に関係のあるものであっても、メールの送信者については未知の者ではないか。
- メールがフリーメールアドレスから送付されていないか。
- メール本文に、不自然な日本語や日本語で使わない漢字が含まれていないか。
- 添付ファイルが実行形式ファイル（exeなど）であったり、日本であまり使われない圧縮形式（rarなど）であったりといった不審な点がないか。

- **住所や電話番号、メールアドレスなどをSNS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（→P.14参照）に利用される可能性にも留意**

- **不審メールの検知を可能にするソフトウェア・アプリの導入など、技術面での適切な対策を実施**

## 「悪意あるリンクをクリックしない」では不十分!?

心の隙を突く攻撃に対して、個人的なレベルでは、不審なメール等の添付ファイルやURLをクリックしないということが求められるのはもちろんですが、英国国家サイバーセキュリティセンター（NCSC）が公表したブログ記事では、組織におけるサイバー攻撃対策として、そうした注意を呼び掛けるだけでは不十分だと指摘されています。

記事によれば、業務上、見慣れないドメインのリンクをクリックしなければならない場面は多い一方、システムに侵入するにはたった一人だますのに成功すればよいという攻撃者にとって有利な状況において、組織をサイバー攻撃から守るには、左ページで解説したような技術面での適切な対策が必要だと指摘されています。ただし、個人への啓発・トレーニングも無意味というわけではなく、万一悪意あるリンクをクリックしてしまった場合にも、叱責やペナルティを恐れることなく、セキュリティ担当者への迅速な報告など、早期の事案対処が可能となるような組織文化や職場環境を構築することも重要だとされています。

## 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。

また、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、政府の施策推進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等を調査
- ❖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

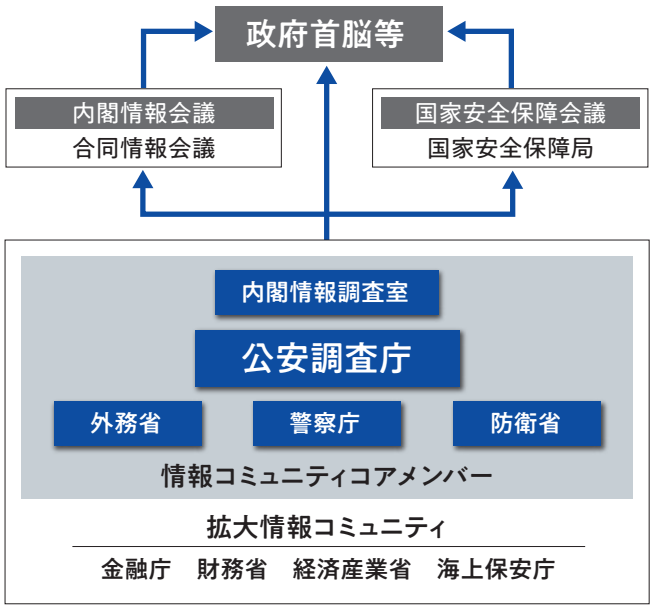
- ❖我が国の情報コミュニティのコアメンバーとして、関係機関に対し、政府の施策に資する情報を提供


## 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」（2021年9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2022」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

## 公安調査庁ホームページ

https://www.moj.go.jp/psia/

公安調査庁のホームページでは、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、「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」など国内外の情勢に関する各種情報を発信しています。


## 公安調査庁SNS公式アカウント

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。

### Twitter

「公安調査庁@MOJ_PSIA」


### YouTube

「PSIAchannel」


## 内外情勢の回顧と展望

毎年1月付けで、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、公表しています。

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」を国民の皆様に広く知ってもらうことを目指し、同要覧の最新版を分かりやすく再編集して掲載しています。


## 経済安全保障パンフレット

経済安全保障の観点から留意すべき現状等についてまとめていますので、社内・学内の研修等にご活用ください。

公安調査庁ホームページにも、経済安全保障特集ページを設けていますので、併せてご覧ください。

情報の力で、国民を守る。

PSIA 公安調査庁
PUBLIC SECURITY INTELLIGENCE AGENCY

# Overview of Threats in Cyberspace 2023