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

Overview of Threats in Cyberspace

サイバー空間における脅威の概況

公安調査庁

2024.12

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、団体の規制のための調査等を行い、もって、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、団体の規制のための調査等を行うとともに、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、国内諸団体の動向等、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年に「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、最新版を作成する運びとなりました。

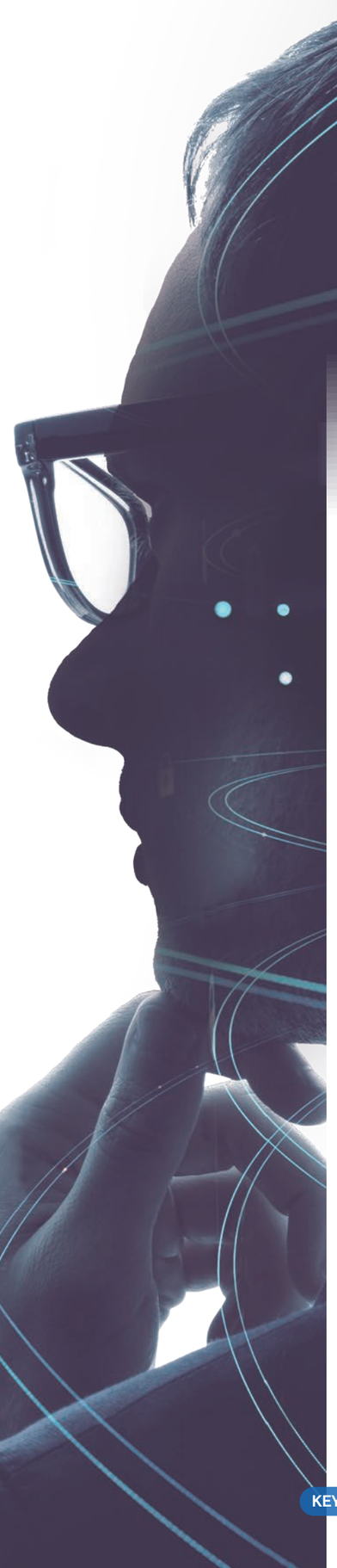
サイバー空間における脅威は、依然として深刻な状況であり、また、生成AIを悪用した偽情報の拡散等、サイバー空間において注視すべき分野は拡大しています。

そうした状況を受け、本冊子においては、サイバー空間をめぐる脅威の概況として、セキュリティ機器やシステムのぜい弱性を狙ったサイバー攻撃の脅威に加え、国内外の各種情勢に応じたサイバー攻撃事例を取り上げるとともに、特集では、生成AIがもたらす脅威について示しました。

また、国家等が関与・支援するサイバー攻撃について、その概要や欧州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、欧米政府等の発表を基にとりまとめ、「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、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、業務の妨害等を狙った**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

2024.08 米国大統領選へのイランの干渉

米国政府の発表によると、イランが、米国大統領選に際し、民主党・共和党候補者両陣営へのハッキングにより窃取した情報を公開するなど、影響工作を展開

2023.11 我が国研究機関に対するサイバー攻撃

我が国研究機関がサイバー攻撃を受け、一部情報が漏えいしていたことが発覚。調査の結果、VPN機器のぜい弱性が悪用されたものであったことが判明

2023.07 我が国港湾施設に対するサイバー攻撃

我が国港湾施設のターミナルシステムに対するサイバー攻撃により、同システムがランサムウェアに感染。数日間にわたり、コンテナの搬入作業等が停止するなどの被害が発生

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

米英政府の発表によると、ロシアが、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

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、企業等に感染被害が発生

2016.11 米国大統領選へのロシアの干渉

米国政府の発表によると、ロシアが、ハッキングで窃取したメール等の公開・拡散、偽情報の流布やSNS上での工作によって、2016年米国大統領選に対する影響工作を展開

2015.12 ウクライナにおける大規模停電

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
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
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

ぜい弱性を突いたネットワーク貫通型攻撃

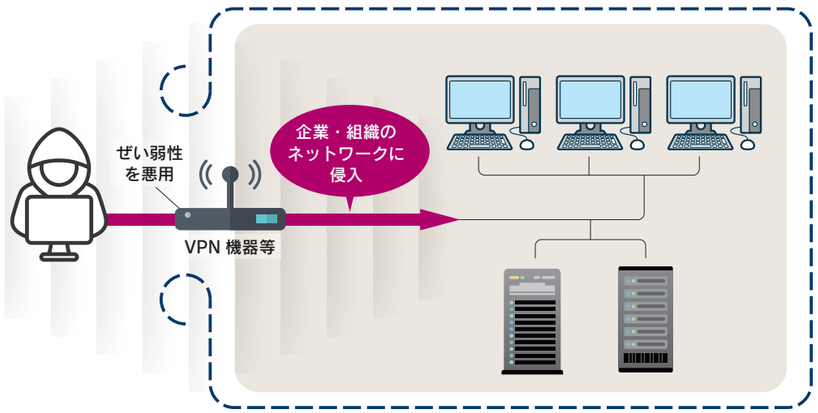
ネットワーク貫通型攻撃とは？

これまで、サイバー攻撃はWebやメール経由で標的企業・組織に侵入する手法が多く確認されていましたが、近年、企業や行政機関等の間でサイバー攻撃対策が意識されるようになり、システムの多層防御や監視体制が徹底され、セキュリティの強化が一層図られるようになりました。その一方で、セキュリティ機器が企業等で広く使用されている状況を逆手に取った“ネットワーク貫通型攻撃”と呼称されるサイバー攻撃が多発しています。

ネットワーク貫通型攻撃とは、インターネットと企業・組織内ネットワークとの境界に設置されるネットワーク機器、セキュリティ製品及びシステム等のぜい弱性を悪用し、攻撃者が直接的に企業・組織内ネットワークに侵入するサイバー攻撃です。攻撃者は、ぜい弱性を悪用することで多層防御や監視体制を容易に回避することが可能となり、標的企業・組織は、侵入を検知できずに不正アクセスを許してしまいます。

攻撃者は、標的ネットワークへの侵入に際して、使用されているネットワーク機器、セキュリティ製品、システム等の種類やぜい弱性の有無等を事前に調べていると指摘されています。また、攻撃者が悪用するぜい弱性には、セキュリティ企業等が未把握のぜい弱性（ゼロデイぜい弱性）もあり、完全に防ぐことは困難であると指摘されています。なお、ゼロデイぜい弱性を悪用する攻撃のように、高度な攻撃には高い技術力に加え、予算や人員等が必要とされることから、国家主体の関与が疑われています。

ネットワーク貫通型攻撃のイメージ



ネットワーク貫通型攻撃の現況

ネットワーク貫通型攻撃が使用されたとみられる事例は近年多数確認されており、ファイブ・アイズ諸国のサイバー関連当局が発出した勧告では、2022年に頻繁に悪用されたぜい弱性の一つとして、VPN機器のぜい弱性が挙げられており、このことは、サイバー攻撃にネットワーク貫通型攻撃が多用されていることを示唆しています（2023年8月）。

近年、我が国においても、このようなネットワーク貫通型攻撃が、サイバー空間における情報窃取の足掛かりとして利用されており、その被害も増加傾向にあります。 2023年11月に発覚した、我が国研究機関に対するサイバー攻撃でも、VPN機器のぜい弱性を起点に内部のサーバー等に侵入されたことが指摘されています。

このような状況を踏まえ、独立行政法人情報処理推進機構（IPA）が、昨今、企業や組織のネットワークとインターネットとの境界に設置されるセキュリティ製品のぜい弱性が狙われ、ネットワーク貫通型攻撃としてAPT（→P.9参照）攻撃に利用されている旨注意を呼び掛けています（2023年8月）。また、IPAは、ネットワーク貫通型攻撃により、他の企業・組織への攻撃における“踏み台”としての機能が仕込まれ、意図せずAPT攻撃に加担してしまうことについても注意を促しています。

また、近年の国家等の関与・支援が疑われるサイバー攻撃でも、ネットワーク貫通型攻撃が使用された事例が複数確認されています。ファイブ・アイズ諸国のサイバー関連当局が、中国サイバー脅威主体「Volt Typhoon」の活動（→P.5参照）について発表した共同勧告では、初期の侵入においてVPN 機器のぜい弱性が悪用された、と指摘しています（2023年5月）。

このほか、豪州通信電子局（ASD）豪州サイバーセキュリティセンター（ACSC）は、中国サイバー脅威主体「APT40」が小規模事業体において使用されているネットワーク機器を乗っ取り、別の攻撃に悪用しているとして、勧告を発表しました（2024年7月）。なお、同勧告には、我が国を始め、米国、英国、カナダ、ニュージーランド、ドイツ、韓国が共同署名しています。

Overview of Threats in Cyberspace

懸念される脅威 2

Living Off The Land（環境寄生型）戦術

ファイブ・アイズ諸国のサイバー関連当局によるVolt Typhoonの活動に関する共同勧告では、Volt Typhoonが、米国の重要インフラ関連組織のネットワークに長期間にわたり検知されることなく潜伏していたことに加え、有事における破壊・妨害を目的としていた可能性が指摘されており、注目を集めました。


Joint Cybersecurity Advisory

ACSC

National Cyber Security Centre

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Summary

Volt Typhoonに対する共同勧告
（出典：米国国防総省ホームページ ※1）

Volt Typhoonは、長期間にわたる潜伏を可能とするため、検知を回避する方策を複数用いており、その一つとして、“Living Off The Land戦術”を用いていたと指摘されており、同戦術に対する関心が高まっています。

Living Off The Land戦術とは

Living Off The Land戦術は、環境寄生型戦術とも呼ばれ、標的システムへの侵入後の活動（水平展開、認証情報の窃取、潜伏、標的情報の窃取・破壊等）において、従来の攻撃のように、マルウェア等の不正ツールを使用することなく、標的システム内に既にある正規のツール等を使用します。

標的システム内に既にある正規のツール等を使用することにより、防御側にとっては、そのツールの活動ログを確認するだけでは、その活動が正常なものであるのか、悪意あるものであるのかの判別が難しくなると指摘されています。

なお、同戦術については、Volt Typhoon以外のサイバー脅威主体も用いていることが指摘されており、昨今、我が国でも多大な被害をもたらしているランサムウェア攻撃においても、同戦術が用いられていることが指摘されています。

サイバー攻撃の実行主体は、情報の窃取や破壊、不正な金銭の獲得等、それぞれの目的を達成するため、攻撃の手法をアップデートしており、サイバー空間における脅威動向には引き続き警戒が必要です。

※1 _https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF
（URLは2024年9月時点、次頁以降同）

懸念される脅威 3

AIがもたらすサイバー脅威の増大

近年、LLM（大規模言語モデル）等の生成AIの普及により、その利便性が認知され、幅広い分野でのAI活用が浸透しつつあります。これらAIの技術向上や利用促進により、我々の生活が豊かになることが期待されていますが、一方で、サイバー攻撃や偽情報の拡散といった悪意ある活動に、これら生成AIが利用された事例が次々に確認されています。また、米国政府高官が、北朝鮮を始めとする懸念国等によるサイバー攻撃へのAI活用について言及するなど（2023年10月）、サイバー空間における脅威が増大することが懸念されています。

AIにより高度化・巧妙化するサイバー攻撃

サイバー攻撃へのAIの悪用が指摘されるものとして、初期の侵入プロセスの一つである標的型メールにおける文面作成への生成AIの悪用が挙げられます。

生成AIは、母国語話者としても違和感を覚えない自然な文章が簡単に作成できることから、広く利用されていますが、これを標的型メールにおける文面作成に悪用することで、標的（被害者）が違和感を覚えることなく、マルウェアが仕組まれた添付ファイルを開封してしまうことが懸念されています。

また、マルウェアの作成・改良へのAIの利用も懸念されており、我が国においても、マルウェアの作成に生成AIが悪用されたとみられる事案が確認されています。

このように、AIの悪用によりサイバー攻撃を行うハードルが下がることに加え、AIの更なる発展に伴い、サイバー攻撃がより高度化・巧妙化することが懸念されています。

生成AIを標的とした新たなサイバー攻撃の出現

さらに、上記のような既存のサイバー攻撃だけでなく、生成AIを標的にした、又はその特徴を悪用した新たなサイバー攻撃も懸念されています。

生成AIを標的とする主なサイバー攻撃

データポイズニング攻撃 Data Poisoning Attacks	LLMの学習用データに悪意あるデータ（偽のデータ等）を入れ込むことで、生成AIモデルの正常な稼働を阻害する攻撃
プロンプトインジェクション Prompt Injection	特殊なプロンプト（指示・質問）により、開発段階では想定していない反応を生成AIモデルにさせることで、学習用データに含まれる内部情報等を漏えいさせる攻撃
モデルインバージョン攻撃 Model Inversion Attacks	生成AIモデルにランダムなデータを繰り返し入力するなどして、学習用データに含まれる標的情報を復元・特定する攻撃

KEYWORD **LLM**：Large Language Models（大規模言語モデル）。膨大な量のテキストデータを用いて学習され、テキストの生成や要約等、多様な指示・質問に対応可能なプログラム

サイバー空間における
不正な活動

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やスマートフォン等に侵入し、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、安全保障等、多岐にわたる分野が攻撃の標的となっています。

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

我が国大手電機メーカーに対するサイバー攻撃が発生（2019年）。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

日本年金機構における個人情報約125万件流出事案

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（2015年）

情報システムの破壊・機能妨害

情報システムの停止、誤作動等を引き起こすことを目的にした活動です。DDoS攻撃やマルウェア等が用いられ、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。

ウクライナ大手通信事業者に対するサイバー攻撃

ウクライナの大手通信事業者に対するサイバー攻撃により、同事業者が提供するサービスが停止し、市内の空襲警報システムが停止するなどの被害が発生（2023年12月）

ウクライナ金融機関等に対するサイバー攻撃

米国及び英国は、オンライン決済や銀行アプリの使用に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（2022年2月）

不正な金銭獲得

銀行預金、暗号資産等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等の手段が用いられます。

北朝鮮のサイバー脅威主体による暗号資産の窃取

米国連邦捜査局（FBI）は、北朝鮮サイバー脅威主体による暗号資産の窃取事案について度々指摘するとともに警戒を呼びかけており、オンラインカジノサイトから約4,100万ドル相当の暗号資産の窃取について、北朝鮮サイバー脅威主体「Lazarus」によるものと指摘（2023年9月）

ハッキングによるATMからの不正出金

米国政府発表によると、北朝鮮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、少なくとも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（2018、2020年）

AI技術の悪用

近年では、生成AIの普及・発展に伴い、AI技術が悪用される事例が確認されています。中でも、いわゆる“ディープフェイク”動画・音声について、より深刻な影響を及ぼすことが懸念されています。

ロシアによるウクライナ侵略に関する偽情報拡散

ウクライナのゼレンスカ大統領夫人が、訪問先のパリにおいて、米国の支援金で高級車を購入したとの内容のディープフェイクとされる動画が、SNS等に投稿され大量に拡散（2024年7月）。専門家は、ロシアによる影響工作の一環であると指摘

台湾の総統選挙に対する干渉

台湾の総統選挙に際して、蔡英文総統（当時）のイメージを悪化させるようなディープフェイクとされる動画がSNS及び動画プラットフォーム上で幅広く拡散。台湾治安機関関係者は、これらが中国当局によるものと指摘（2024年1月）

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等で勝手に実行させ、第三者が不正に金銭的利益を得る行為
ディープフェイク：AI技術を用いて、現実の映像や音声等を人工的に加工し、実際には行われていない言動をあたかも人々がとったかのように見せかける技術

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、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といった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、諜報活動等、政治的・軍事的な国家目標を達成するため、軍や情報機関等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**

また、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。

加えて、我が国、欧米の政府当局等は、国家等の関与・支援が疑われるサイバー攻撃について、これを抑止するとともに、注意喚起・対策強化の一環として、その実行者と所属する国家機関等を特定・公表するパブリック・アトリビューションを行っています。

国家等が関与・支援するとされ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、国家安全部、これらの組織から委託を受けるなどした企業、サイバー犯罪者等
	特徴	● 他国・地域の政治、安全保障、経済・技術等の戦略的利益に資する情報の窃取 ● 偽情報の拡散等 “認知戦” の展開 ● 有事を見据えた偵察活動等の実施
ロシア	攻撃主体	中心となっているのは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）、これらの組織から委託を受けるなどした企業、サイバー犯罪者等
	特徴	● 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 ● 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	● 核・ミサイル等の大量破壊兵器開発の資金源とも指摘される暗号資産の窃取 ● 政治目標及び軍事目標の達成を目的とした情報窃取 ● サイバー攻撃による報復

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。“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

2024年3月

米国司法省は、中国サイバー脅威主体「APT31」によるサイバー諜報活動等に関与したとして、APT31関係者７人を起訴したと発表

また、英国政府は、選挙管理委員会へのサイバー攻撃等に関与したとして、APT31に関係する企業１社及び関係者２人を制裁の対象に指定した旨発表

米国司法省が起訴した７人
（写真：米国司法省ホームページ ※２）

2023年9月

我が国及び米国政府当局は、中国を背景とするサイバー脅威主体「BlackTech」による情報窃取を目的としたサイバー攻撃に関する合同の注意喚起を発出

2021年7月

米英政府等は、中国サイバー脅威主体「APT40」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、米英政府等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 ※３）

※2 _https://www.justice.gov/opa/media/1345141/dl?inline
※3 _https://www.fbi.gov/wanted/cyber/apt-40-cyber-espionage-activities

2 ロシア

最近の主な
パブリック・アトリビューション

2024年9月

米国司法省は、ウクライナ侵攻に先立ちウクライナ政府機関等を標的としたサイバー攻撃等に関与したとして、ロシア連邦軍参謀本部情報総局（GRU）職員ら6人を起訴したと発表

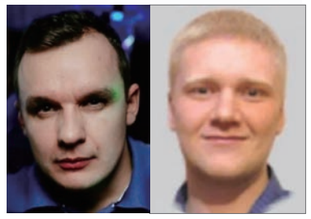
FBIによるGRU職員らの手配書
（写真：FBIホームページ ※4）

2024年6月

EU理事会は、ロシアサイバー脅威主体「Star Blizzard」及び「Armageddon」によるEU及びウクライナを標的としたサイバー攻撃等に関与したとして、ロシア連邦保安庁（FSB）職員を含む6人を制裁の対象に指定した旨発表

2023年12月

米国司法省は、Star Blizzardによる米国政府機関を標的としたサイバー攻撃等に関与したとして、FSB職員ら2人を起訴したと発表



米国司法省が起訴した2人
（写真：FBIホームページ ※5 ※6）

2021年4月

米国財務省は、2020年の米国大統領選への介入に関与したとする16企業・16個人のほか、偽情報を拡散した6つのインターネットメディアを制裁の対象に指定した旨発表

また、バイデン大統領は、上記ロシアの米国大統領選介入への非難に加え、米国企業製ネットワーク管理ソフトウェア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につき、ロシア対外情報庁（SVR）を背景に持つサイバー脅威主体「APT29」が実行した可能性が高いと非難、ワシントンに駐在するロシア外交官10人の追放も発表

※4 _https://www.fbi.gov/wanted/cyber/gru-29155-cyber-actors
※5 _https://www.fbi.gov/wanted/cyber/ruslan-aleksandrovich-peretyatko
※6 _https://www.fbi.gov/wanted/cyber/andrey-stanislavovich-korinets

3 北朝鮮

最近の主な
パブリック・アトリビューション

2024年3月

国連安保理北朝鮮制裁委員会専門家パネルは、2023年最終報告書を公表。その中で、北朝鮮偵察総局傘下のサイバー脅威主体による技術情報の窃取及び不正な金銭獲得を企図したサイバー攻撃が継続していると指摘

2023年9･12月

我が国外務省、財務省及び経済産業省は、国連安保理決議により禁止された活動等に関与したとして、北朝鮮サイバー脅威主体「Andariel」、「Bluenoroff」、「Kimsuky」等を、資産凍結等の措置の対象に追加する旨発表

2023年6月

米韓政府当局は、外交・安全保障・国防等の分野を標的に、サイバー諜報活動を行うKimsukyの活動に関する共同勧告を発表。また、韓国当局はKimsukyを対北朝鮮独自制裁の対象に指定した旨発表

2021年2月

米国司法省は、破壊的サイバー攻撃、不正な金銭獲得を企図したサイバー攻撃等に関与したとして、3人の起訴を発表

米国司法省が起訴した3人
（写真：米国司法省ホームページ ※7）

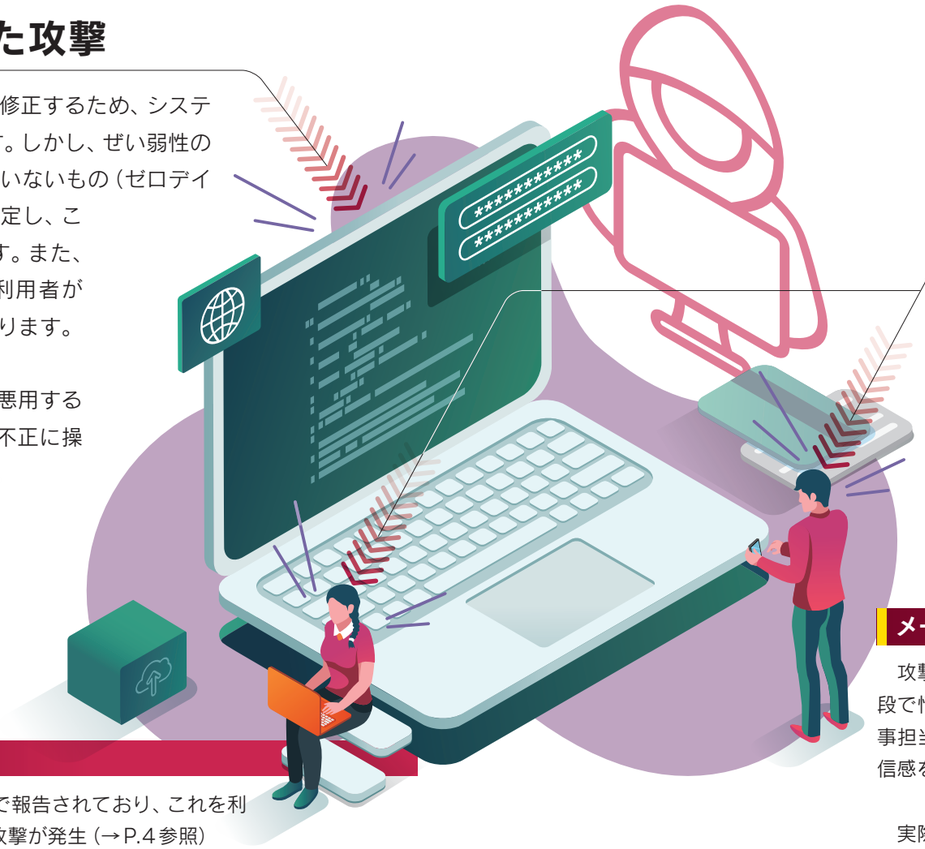
※7 _https://www.justice.gov/opa/press-release/file/1367701/dl

サイバー攻撃の手法

システムの弱点を突いた攻撃

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、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。

サイバー攻撃の実行主体は、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、目的の達成を試みています。



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（→P.4参照）

各機器の製造企業は、修正プログラムを提供しているものの、利用者が同修正プログラムを適用するまでの僅かな間に攻撃される事案も発生

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普及が進んでいる一方、サイバー攻撃の標的となる事案も発生

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等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

サイバー攻撃の手法

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などして、システムへの不正アクセス等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です。標的の関係者になりすます、標的の関心を引くテーマを使用する、過去に使用されたメール文面を流用するなどの手段で、標的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。

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攻撃の事例の中には、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ことが窺える事例も確認

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、近年、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例（右図参照）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

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・スマートフォン等の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）等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）及び一般社団法人JPCERTコーディネーションセンターによるぜい弱性データベース「JVN iPedia」
  https://www.jvndb.jvn.jp
- 独立行政法人情報処理推進機構（IPA）
  https://www.ipa.go.jp
- 一般社団法人JPCERTコーディネーションセンター
  https://www.jpcert.or.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

また、上述の「JVN iPedia」では、登録されたぜい弱性情報の効率的な収集等の機能を提供する「MyJVN」を公開しています。
https://jvndb.jvn.jp/apis/myjvn/

- **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、アプリ等によるワンタイムパスワード認証等）
- 知識情報（パスワード）＋生体情報（静脈認証、指紋認証等）

- **サイバーセキュリティ企業等の情報発信をチェックして、攻撃者の最新のTTPs[KEYWORD]を把握し、適切な対策を実施**

進化するセキュリティ ～“EDR”から“XDR”へ～

近年、サイバー攻撃の高度化・巧妙化に伴い、検知困難な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外部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の概念が”EDR”（Endpoint Detection and Response）とその拡張版ともいえる”XDR”（Extended Detection and Response）です。これらは両者ともに”ゼロトラスト”[KEYWORD]というサイバーセキュリティの基本的な概念に則ったもので、EDRは、組織のネットワークのエンドポイント（PCやサーバー、モバイル等）の動作や操作等を監視しながら、不審な挙動の中から攻撃を検知し、迅速な初期対応（ネットワークの遮断やプロセスの停止）を行うことを目的としたものです。他方、XDRは、エンドポイントだけでなく、ネットワーク、クラウド、電子メール等の複数のセキュリティデータを収集し、相互に関連付けることで、多岐にわたるサイバー攻撃を検知することを目的としています。

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等の添付ファイルやURLをクリックせず、攻撃者が装っているメール等の相手方本人に電話等で確認したり、システム担当者に連絡したりして、慎重に対処**

【参考】

近年では、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されています。加えて、2024年夏頃から、過去に確認されていたマルウェア「ANEL」が再び確認されるなど、攻撃手法の変化も見受けられます。これらマルウェアは、メールに添付されたWordファイルやExcelファイルの開封のほか、メールに記載されているリンクのクリックを通じて感染し、標的の個人情報等を窃取します。また、メールは、実在する組織の人物名やイベント名が記載されているなど、高い説得力を有しており、個人のフリーメールアドレス宛てにもメールが送付されていると言われているほか、文面もより巧妙になってきているとの指摘もあり、メールの真偽を見分けることが難しくなっています。

なお、個人や組織を対象とし、国内外の情勢に連動した情報窃取を展開しているとの指摘もあります。

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で使われない漢字やフォント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等）であるといった不審な点がないか

- **住所や電話番号、メールアドレス等をSNSにむやみに投稿せず、趣味や仕事内容、友人関係等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**
- **不審メールの検知を可能にするソフトウェア・アプリの導入等、技術面での適切な対策を実施**

サイバー攻撃をめぐる「AI vs AI」

近年、AIの普及・発展に伴い、サイバー攻撃が高度化・巧妙化することが懸念されています（→P.6参照）。特に、上記の不自然な日本語や日本で使われない漢字やフォントについては、AIの使用により、人がその不審性を認識できなくなることも予想されます。

他方で、サイバーセキュリティへのAIの活用も進んでいます。ネットワークやシステムの監視及び攻撃の検知への活用が進められており、人がその不審性を認識できない攻撃について、早期に検知することが期待されているほか、マルウェア解析への活用等も進められており、AIによるサイバーセキュリティの発展も期待されています。

AIの普及・発展は、今後のサイバー空間における脅威及びセキュリティの両面において、重要な要素であると評価されており、注目されます。

KEYWORD

TTPs：Tactics,Techniques and Procedures。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

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。

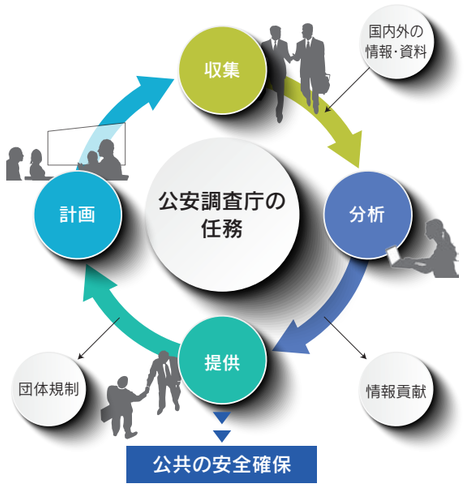
また、公安調査庁は、我が国の情報関係機関によって構成される情報コミュニティのコアメンバーとして、官邸や内閣官房を始めとする関係機関に対し、政府の施策に資する情報を日々提供しています。

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

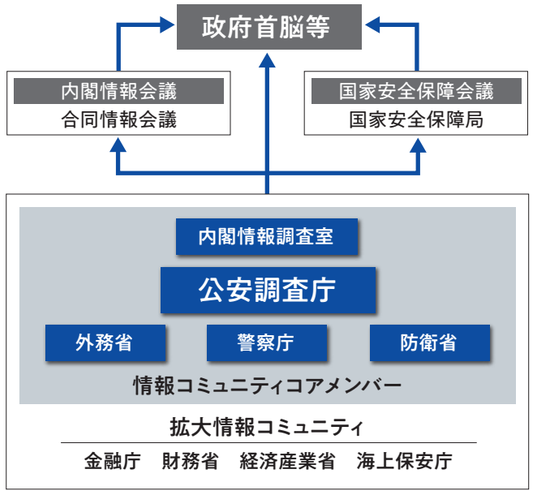


サイバー関連調査の推進

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 2024」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・分析の強化及び関係機関への情報提供等、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、業務内容等について紹介しているほか、国内外の諸情勢に関して、「オウム真理教特集ページ」、「世界のテロ等発生状況」、「最近の内外情勢」等の各コンテンツを掲載しています。

公安調査庁SNS公式アカウント

公安調査庁公式X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等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。

X

「公安調査庁@MOJ_PSIA」

YouTube

「PSIAchannel」