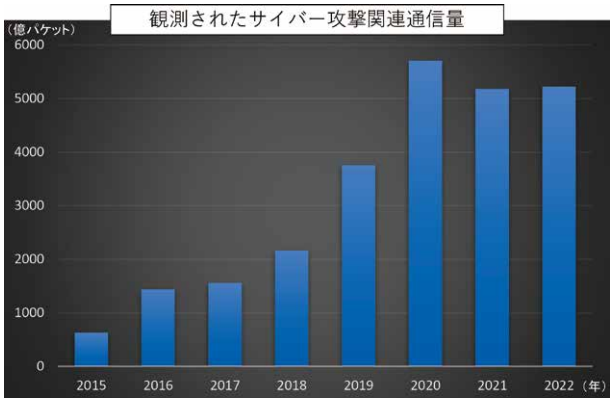
内外情勢

サイバー空間をめぐる動向

国家安全保障への脅威が拡大するサイバー攻撃

機密情報の窃取、金銭の不正な獲得、業務の妨害などを目的としたサイバー攻撃は、国内外で常態化するとともに、その手口も巧妙化している。また、最近では生成AIを悪用したサイバー攻撃への懸念も指摘されている（P.35 COLUMN①「生成AIがもたらす信頼の危機」）。

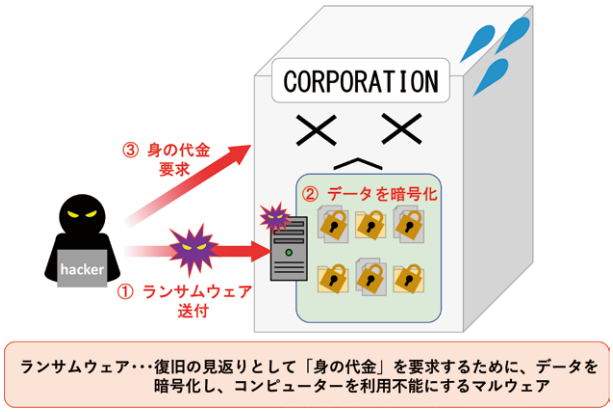
こうしたサイバー攻撃の手口の巧妙化は、安全保障の観点でも重大な脅威となっている。取り分け、懸念国のサイバー戦能力強化は、機密情報や技術の窃取、重要インフラの破壊、偽情報拡散による世論操作など、我が国に深刻な影響を及ぼすおそれがある。



国立研究開発法人情報通信研究機構（NICT）公表の「NICTER観測レポート2022」に基づき当庁作成

■深刻な影響を引き起こしかねない重要インフラ等へのサイバー攻撃

令和5年（2023年）に、各国で発生が確認されたサイバー攻撃事案の中には、市民生活や社会活動に深刻な影響を引き起こしかねない、重要インフラ等を標的としたものも確認されている。我が国においても、名古屋港のターミナルシステムが、ランサムウェア感染に起因するシステム障害により、数日間にわたり荷役作業への影響を受けた（7月）。



ランサムウェア攻撃のイメージ

■国際的なイベント等に反応したサイバー攻撃

このほか、国際社会の耳目を集めるような国際会議等のイベントに反応した、非国家主体によるサイバー攻撃も各国で引き続き確認されており、我が国においても、G7広島サミット（5月）、東京電力福島第一原子力発電所のALPS処理水の海洋放出（8月）に際し、ウェブサイトの閲覧障害等の事象が見受けられたところ、非国家主体のものとみられるSNSアカウントが我が国の政府機関や企業等に対するサイバー攻撃を実行した旨の投稿を行った。

国家の関与・支援が疑われるサイバー攻撃

欧米政府当局等は、国家の関与・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る。

欧米政府当局等による近年の主なパブリック・アトリビューション

	APTの識別名 （カッコは別名の例）	関連が疑われる国家機関 ※欧米政府当局等が公表したものに準拠	関与したサイバー攻撃事案、標的の例
中国	APT1 (Comment Panda)	中国人民解放軍	・原子力メーカーなど在米6組織からの情報窃取（2006-2014年）
中国	APT10 (Stone Panda)	中国国家安全部	・米国の企業・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（2006-2018年頃）
中国	APT40 (Leviathan)	中国国家安全部	・米国等の企業・政府機関等からの技術情報の窃取（2011-2018年） ・台湾政府機関への侵入（2018年）
中国	APT41 (Wicked Panda)	中国国家安全部	・米国等世界中の100社以上への侵入に関与（2014-2020年）
ロシア	APT28 (Fancy Bear)	ロシア連邦軍参謀本部情報総局	・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）
ロシア	APT29 (Cozy Bear)	ロシア対外諜報庁	・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） ・米国企業製ネットワーク管理ソフトウェアへの攻撃（2020年）
ロシア	Sandworm (BlackEnergy)	ロシア連邦軍参謀本部情報総局	・ウクライナ大規模停電（2015、2016年） ・米国大統領選挙有権者情報の窃取等（2016年） ・韓国・平昌冬季大会の妨害（2018年）
北朝鮮	Lazarus (APT38)	北朝鮮偵察総局	・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）

（欧米政府当局等の発表に基づき当庁作成）

〈APTとは〉

APT･･･Advanced Persistent Threat（高度で持続的な脅威）

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攻撃主体について、APT集団と呼称。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

令和5年（2023年）における、欧米政府当局等による主なパブリック・アトリビューションは、以下のとおり。

■中国

米国の重要インフラ分野を標的としたサイバー攻撃に対し、米国、オーストラリア、カナダ、ニュージーランド及び英国の各政府当局は、中国が支援するサイバー脅威主体「Volt Typhoon」の活動に関する共同勧告を発表した(5月)。また、米国の国家安全保障局(NSA)、連邦捜査局(FBI)及びサイバーセキュリティ・インフラセキュリティ庁(CISA)は、我が国の警察庁及び内閣サイバーセキュリティセンター(NISC)と共同で、中国と関連を有するサイバー脅威主体「BlackTech」によるルータのぜい弱性等を悪用したサイバー攻撃について、注意喚起を行った(9月)。

「Volt Typhoon」の活動に関する共同勧告(米国国防省ウェブサイト〈https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_PRC_State_Sponsored_Cyber_Living_off_the_Land_v1.1.PDF〉)

■ロシア

英国国家サイバーセキュリティセンター(NCSC)、米国NSA、米国CISA及び米国FBIは、米国政府機関のほか、欧州及びウクライナで被害を及ぼした、ロシアの軍情報機関と関連を有するサイバー脅威主体「APT28」によるサイバー攻撃に関する共同勧告を発表した(4月)。また、米国司法省は、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、ロシア連邦保安庁(FSB)職員ら2人を起訴したと発表した(12月)。

起訴されたFSB職員に対するFBIによる手配書(FBIウェブサイト〈https://www.fbi.gov/wanted/cyber/ruslan-aleksandrovich-peretyatko/@@download.pdf〉)

■北朝鮮

米国財務省は、北朝鮮のサイバー攻撃及び身分を偽ったIT技術者の違法な活動を通じて、核・ミサイル開発の資金獲得(P.36 COLUMN②「狙われる暗号資産」)に関与したとして、サイバー部隊要員の訓練機関や偵察総局の傘下組織を含む団体・個人を制裁対象に指定した(5月、11月)。また、我が国においても、政府は、北朝鮮に関連する国連安全保障理事会決議により禁止された活動等に関与する北朝鮮のサイバー脅威主体を含む団体・個人に対し、資産凍結等の措置を実施する旨の発表を行った(9月、12月)。

制裁対象指定に係るプレスリリース(米国財務省ウェブサイト〈https://home.treasury.gov/news/press-releases/jy1498〉)

COLUMN ①

生成AIがもたらす信頼の危機

米国のOpenAI社が、令和4年(2022年)11月にチャット形式でテキストを生成するAI「ChatGPT」を公開したことを契機に、生成AI技術への関心が世界的に高まっている。テキスト、画像、動画など多岐にわたる用途の生成AI技術が急速に発展しており、我が国においても「ChatGPT」を始めとした生成AIの利便性が認知され、幅広く普及しつつある。その一方で、SNS上で生成AIを用いた偽画像・偽動画が拡散されるなど、生成AIによってもたらされる負の側面が課題になりつつある。

こうした点に関連して、生成AIを用いたツールやサービスが、国家が関与・支援するサイバー脅威主体、犯罪グループなどによって、偽情報の拡散や標的型攻撃の文面作成、マルウェアの作成などサイバー攻撃に悪用されている可能性も指摘されている。

主な生成AIサービス・製品（当庁作成）

生成AIの悪用リスクに関する各国等の認識

「一般大衆の認識を形成し、信頼を毀損するため、AIを活用したツールや技術を用いて**偽情報を拡散**することで政治的目的を達成しようとする国家が増加している。」
英国政府通信本部（GCHQ）「Ethics of AI: Pioneering a New National Security （令和3年〈2021年〉2月）」

「ChatGPTの機能は、フィッシングメールによる詐欺などの犯罪活動に加えて、**テロリズム、プロパガンダ、偽情報の分野**においても悪用される可能性がある。」
欧州刑事警察機構（ユーロポール）「ChatGPT-the impact of Large Language Models on Law Enforcement（4月）」

「ディープフェイクやChatGPTのようなAI技術が成熟し、SNSのチャンネルが多様化している現状において、中国共産党は関連技術を用いて**認知戦**を行う可能性がある。」
台湾国家安全局蔡明彦局長「台湾立法院外交国防委員会 中共複合式威脅對我國家安全之影響（4月）」

「サイバー犯罪者や敵対的な外国政府は既にAIを悪用しており、生成AIは**ディープフェイクや悪性コードの作成**を容易にし、脅威主体のサイバー攻撃能力を強化するツールとなる。」
米国連邦捜査局（FBI）レイ長官「Mandiant/mWISE 2023 Cybersecurity Conference（9月）」

（各国等の発表に基づき当庁作成）

ロシアのウクライナ侵略に際し、ゼレンスキー大統領が自国民に降伏を呼び掛ける「ディープフェイク」(注)動画が作成され、SNSで拡散された(令和4年〈2022年〉3月)ものの、同動画の作成主体は明らかになっていない。その一方で、ウクライナ国防省情報総局(GUR)は、以前から、ロシアが情報戦の一環としてディープフェイクを用いた動画を拡散する可能性について警告していた(令和4年〈2022年〉3月)。このように対象国の混乱を企図したとみられる偽情報の作成にAIが用いられる事例が指摘されている。

生成AI技術の進展に伴い、悪意ある主体による偽情報の作成・拡散やサイバー攻撃手法の精緻化・巧妙化が更に促進されるとみられ、国民生活の安全・安心に対して深刻な脅威をもたらすことが懸念される。

ゼレンスキー大統領の顔が合成されたディープフェイク動画（写真提供：AFP＝時事）

(注) 機械学習や深層学習を含むAI技術を用いて、本物又は真実であるかのように誤って表示し、人々が発言又は行動していない言動を行っているかのような描写をすることを特徴とする、操作又は合成された音声、画像又は動画コンテンツを指す。

COLUMN ②

狙われる暗号資産

平成20年(2008年)に「サトシ・ナカモト」を名のる人物が公表した論文をきっかけに最初の暗号資産(仮想通貨)となるビットコインが誕生して以来、様々な暗号資産が考案・運用され、現在流通する暗号資産は数千種とも数万種とも言われている。

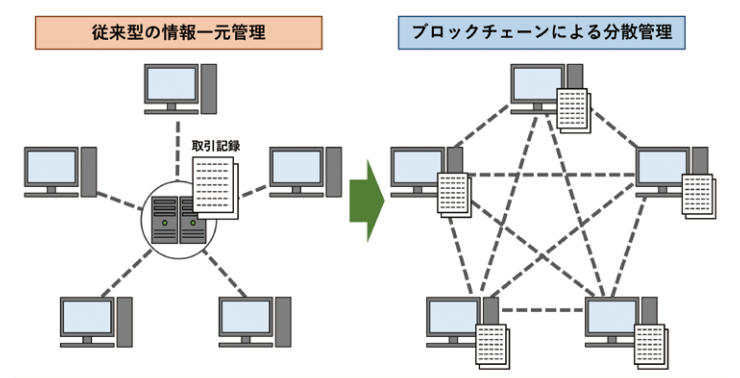
暗号資産とは、インターネット上でやり取りできる財産的価値である。「ブロックチェーン」と呼ばれる技術などを用いて記録され、国家や中央銀行が発行する法定通貨とは異なり、価値の保障や裏付けとなる資産がないものの、代金の決済などに使用でき、かつ、「取引所」などと呼ばれる暗号資産交換業者を通じて法定通貨と相互に交換することも可能である。

暗号資産の普及とともに投機目的の資金が集中し、取引価格が急上昇した平成29年(2017年)は、「仮想通貨元年」とも言われ、我が国でも、暗号資産等を通じて巨額の財産を築き、「億り人」などと呼ばれる人々が出現した。

一方で、ハッキングによる暗号資産の窃取被害も問題となっている。我が国では、平成26年(2014年)以降、数十億円から数百億円相当の暗号資産が窃取される事案が複数確認されているところ、令和元年(2019年)には、交換業者における暗号資産の管理方法を見直す法改正も行われた。

暗号資産に関しては、サイバー犯罪者のみならず、国連などの制裁下にある北朝鮮も、核・ミサイル開発資金を含む外貨獲得の手段として早期から着目していたとされ、令和5年(2023年)も、北朝鮮との関連が疑われる暗号資産の窃取事案が相次いでいる(P.23 特集2「増大する北朝鮮弾道ミサイルの脅威」及び右下表参照)。

こうした被害の拡大を受けて、最近では、各国の法執行機関がブロックチェーン分析企業などと協力し、窃取された暗号資産を回収する取組も進められている。



ブロックチェーンの概念図(総務省「ICTによるイノベーションと新たなエコノミー形成に関する調査研究」及び経済産業省「ブロックチェーン技術を活用したシステムの評価軸Ver.1.0」に基づき当庁作成)

ビットコイン（BTC）	・ 最も代表的な暗号資産であり、時価総額（令和5年11月時点）も他の暗号資産を圧倒する。 ・ 流通性の高さから、決済手段としても広く用いられる一方、ランサムウェアグループが、身の代金支払の手段として指定することもある。 ・ 北朝鮮関係者も、窃取した暗号資産をビットコインに交換した上で現金化していたとされる。
イーサリアム（ETH）	・ ビットコインに次ぐ時価総額（令和5年11月時点）を有するアルトコイン（ビットコイン以外の暗号資産の総称）の代表格。 ・ スマートコントラクト（プログラムを通じて契約内容を自動で実行する仕組み）の基盤として、DeFi（分散型金融：金融機関等の管理者による仲介を要しない金融サービス）など、ブロックチェーンを利用した新興のサービスに用いられる。
テザー（USDT）	・ 代表的なステーブルコイン（法定通貨や貴金属などと価値が連動するよう設計された暗号資産）。 ・ 発行元のテザー社が発行額と同額の米ドルを準備金として保有することにより、米ドルと価値を連動（1ドル＝1USDT）させているとされる。
USDコイン（USDC）	・ テザーと同様、米ドルと価値が連動するよう設計されたステーブルコイン。

米国財務省による制裁対象となった北朝鮮関係者が保有していたとされる暗号資産4種(なお、犯罪者が資金洗浄その他の不正行為に用いる手段として、ビットコインに代わってDeFiやステーブルコインが利用される割合が高まっているとの指摘もある)(図中の画像提供：igapy/PIXTA(ピクスタ))

時期	被害企業等	被害金額（窃取時点）
2022年3月	ベトナムのブロックチェーンゲーム企業	約6億2,000万ドル相当
2022年7月	米国の暗号資産事業者が提供する暗号資産移転サービス	約1億ドル相当
2023年6月	エストニアの暗号資産ウォレット事業者	約1億ドル相当
2023年7月	セントビンセント・グレナディーンの暗号資産決済事業者	約6,000万ドル相当
2023年7月	エストニアの暗号資産決済事業者	約3,700万ドル相当
2023年9月	オーストラリアのオンライン暗号資産カジノ	約4,100万ドル相当

FBIが北朝鮮の関与を指摘した最近の暗号資産窃取事案(FBI発表に基づき当庁作成)

COLUMN ③

ホリデーシーズンのサイバーリスク

クリスマスや年末年始など、人々の行動が普段と異なる時期は、サイバー攻撃に注意する必要がある。例えば、北朝鮮のサイバー脅威主体が、他国の外交官に対し、年末の挨拶を装った標的型メールを送ったとされるセキュリティ企業の報告もあるが、標的となるのは、外交官のような特別な立場の人物に限らない。誰もが、季節の挨拶やシーズンセールの広告を装ったメールでマルウェアに感染したり、文中のリンクから偽のウェブサイトに誘導してIDとパスワード等の認証情報等を窃取されたりするおそれがある。

クリスマスや年末年始に限らず、長期休暇の時期は、企業も格好の標的となる。システム管理者が長期不在となることで、トラブルが発生した場合の対応が遅れたり、休暇後に溜まった大量のメールを確認する際に誤って標的型メールの添付ファイルやURLをクリックしてマルウェア感染させてしまったりと、普段とは異なる環境下ゆえに思わぬ被害が生じるおそれがある。

季節の挨拶を装った標的型メール（複数事例に基づき当庁作成）

長期休暇前	長期休暇中	長期休暇明け
✓ 機器やデータの社外持ち出しルールを確認・遵守 ✓ 使用しない機器は電源をOFF	✓ 持ち出した機器やデータは厳重に管理	✓ 長期休暇中に公開された修正プログラムがないか確認 → 必要な修正プログラムを適用 ✓ メールチェックやウェブサイトの閲覧前に、セキュリティソフトの定義ファイル（※）を更新 ✓ 持ち出した機器等のマルウェアチェック ✓ 溜まったメールをチェックする際は、不審なメールに注意

※定義ファイル（パターンファイル）…セキュリティソフトがマルウェアを検出する際に使われるデータベースの一種

（独立行政法人情報処理推進機構（IPA）「長期休暇における情報セキュリティ対策」に基づき当庁作成）