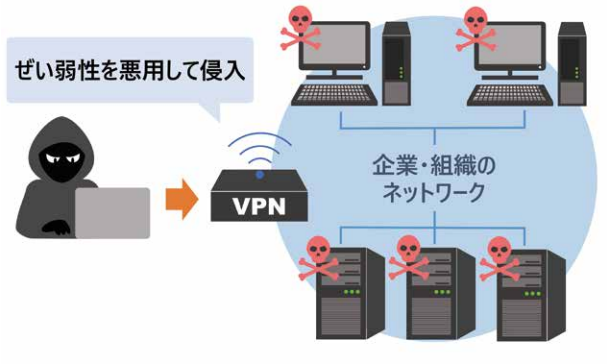
サイバー空間をめぐる動向

被害が拡大する「ネットワーク貫通型攻撃」

近年、拠点間の通信を安全に行うためにインターネットと企業・組織の内部ネットワークとの境界に構築する仮想的な専用回線（VPN）等のセキュリティ機器のぜい弱性を悪用して攻撃者が内部ネットワークに侵入する「ネットワーク貫通型攻撃」による被害が多く伝えられている。

令和6年（2024年）には、米国製VPN機器のぜい弱性を悪用した攻撃が全世界で確認されたことが公表された（1月）。我が国でも、宇宙航空研究機関がVPN機器のぜい弱性を悪用されて複数回にわたる不正アクセスを受け、情報漏えいが発生したことが公表された（7月）。

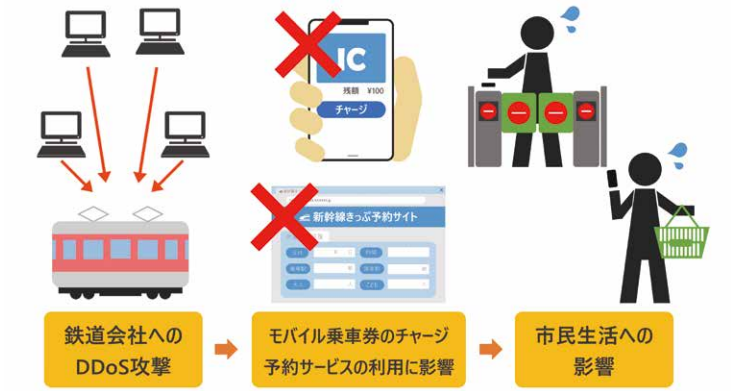


「ネットワーク貫通型攻撃」のイメージ（当庁作成）

我が国重要インフラ等を狙ったサイバー攻撃

令和6年（2024年）に我が国で発生が確認されたサイバー攻撃事案の中には、重要インフラ事業者等を狙い、市民生活・社会活動に影響を及ぼしたものも含まれている。

5月には我が国鉄道会社で発生したシステム障害によりモバイル乗車券やオンライン予約サービスの利用に影響が生じ、12月には我が国航空会社と複数の我が国大手金融機関でシステム障害が相次いで発生したところ、いずれもDDoS攻撃が原因である可能性が指摘された。



DDoS攻撃：インターネット上の多数の機器から特定のネットワークやコンピュータに一斉に接続することで過剰な負荷を掛け、機能不全に追い込む攻撃

鉄道会社へのDDoS攻撃が市民生活に及ぼす影響（当庁作成）

我が国企業に対するランサムウェア攻撃（P.38 COLUMN①「「身代金」を要求するサイバー攻撃：ランサムウェアとは？」）では、全国の自治体・金融機関等から業務委託を受けていた我が国情報処理サービス会社（5月）や我が国大手出版会社（6月）が被害を受け、大量の個人情報が流出する事態を招いた。

国家の関与・支援が疑われるサイバー攻撃

我が国及び欧米政府当局等は、国家の関与・支援が疑われるサイバー攻撃について、その抑止とともに、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。

我が国及び欧米政府当局等が令和6年（2024年）に行った中国・ロシア・北朝鮮に関連する主なパブリック・アトリビューションは、以下のとおりである

■中国

米国司法省は、中国政府機関が支援するサイバー脅威主体「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した（3月）。また、米国、豪州、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」による重要インフラへの脅威を警告する共同勧告を発表した（3月）。このほか、豪州サイバーセキュリティセンターは、中国政府機関が支援するサイバー脅威主体「APT40」の活動への警戒を呼び掛ける共同勧告を発表した（7月）。同勧告には、我が国、米国等を含む8か国が共同署名している。

「APT31」関係者7人についての情報に報奨金を提供する米国国務省のプログラム（米国国務省ウェブサイト<https://rewardsforjustice.net/rewards/apt31-wuhan-xiaoruizhi-science-technology-company-ltd/>）

■ロシア

EU理事会は、ロシアが支援するサイバー脅威主体「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人を制裁対象に指定したと発表した（6月）。また、米国司法省は、ウクライナ政府関連のシステムに対するサイバー攻撃に関与したとして、ロシア連邦軍参謀本部情報総局（GRU）関係者ら6人を起訴したと発表した（9月）。

■北朝鮮

米国連邦捜査局（FBI）、国家安全保障局（NSA）及び国務省は、北朝鮮軍が支援するサイバー脅威主体「Kimsuky」による標的型メール攻撃への警戒を呼び掛ける共同勧告を発表した（5月）。また、米国、英国及び韓国の各政府当局は、北朝鮮軍が支援するサイバー脅威主体「Andariel」による防衛・宇宙・原子力分野等の情報窃取を目的としたサイバー諜報キャンペーンを警告する共同勧告を発表した（7月）。これに関連し、米国司法省は、「Andariel」に所属する北朝鮮籍のハッカー1人を起訴したと発表した（7月）。このほか、我が国警察庁は、FBI及び米国国防省サイバー犯罪センター（DC3）とともに、北朝鮮軍が支援するサイバー脅威主体「Lazarus」の一部とされる「Trader Traitor」が、我が国の暗号資産関連事業者から約482億円相当の暗号資産を窃取した（5月）ことを特定したと発表した（12月）。

起訴された北朝鮮ハッカーに対するFBIの手配書<https://www.fbi.gov/wanted/cyber/rim-jong-hyok/@@download.pdf>）

中露朝の関与・支援が疑われる主要なサイバー脅威主体

	主体の識別名（別名の例）	関連が疑われる国家機関等	関与したサイバー攻撃事案、標的等
中国	APT1	中国人民解放軍	・原子力メーカー等米国6組織からの情報窃取（2006～2014年）
	APT10	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）
	APT31		・英国国会議員のメールアカウントへの侵入（2021年）、同国選挙管理委員会への侵入（2021～2022年）
	APT40		・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） ・豪州国内組織からユーザー名、パスワード等を窃取（2022年）
	APT41		・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	・各国政府機関等を標的とした大規模なブルートフォース攻撃（2021年）
	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）
	Sandworm（APT44）	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・平昌冬季五輪大会の妨害（2017年）
	Cadet Blizzard		・ウクライナ政府機関等への侵入（2022年～）
北朝鮮	Lazarus（APT38）	朝鮮人民軍総参謀部偵察総局	・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」による攻撃（2017年） ・暗号資産取引所等からの暗号資産窃取（2017年～）
	Kimsuky		・米国等の組織・個人に対する標的型メール攻撃（～2024年）
	Andariel		・米国等の防衛・宇宙・原子力・エンジニアリング分野を狙った情報窃取（2024年）

（欧米政府当局等の発表に基づき当庁作成）

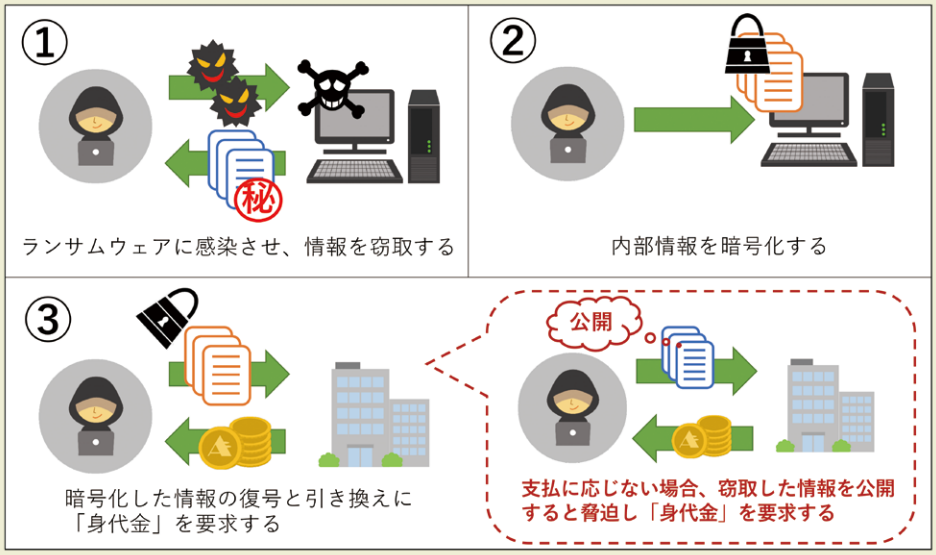
COLUMN ①

「身代金」を要求するサイバー攻撃：ランサムウェアとは？

ランサムウェア（Ransomware）とは、「身代金」（Ransom）と「ソフトウェア」（Software）を組み合わせた言葉で、復旧の見返りとして「身代金」を要求するために、データを暗号化し、コンピュータを利用不能にするマルウェアのことである。

ランサムウェア攻撃の手法は、以前は、不特定多数の標的にランサムウェアをメールで送信する「ばらまき型」が一般的とされた。しかし、近年は、テレワーク等で普及したVPN機器等のぜい弱性を悪用して標的の内部ネットワークに侵入し、ランサムウェアに感染させる「標的型」が主流となっている。

また、データを元に戻すための「身代金」を要求するにとどまらず、データを盗み取った上でコンピュータ内のデータを暗号化し、「身代金」要求を拒否すればデータを外部に公開すると脅迫する「二重脅迫」（ダブルエクストーション）も増加しているとされる。6月に発生した我が国大手出版会社に対するランサムウェア攻撃でも「二重脅迫」の手口が使われた。なお、「身代金」は匿名性の高い暗号資産での支払を要求される場合が多い。



「二重脅迫」の手口を使用したランサムウェア攻撃のイメージ（当庁作成）

近年、攻撃に必要なランサムウェアの開発やネットワークへの不正侵入に必要な認証情報の収集といった作業を「サービス」として提供する「RaaS」（Ransomware as a Service）という手口が拡散しているとされる。また、最近では、我が国で生成AIを利用してランサムウェアを作成した男性が5月に逮捕され、10月に懲役3年、執行猶予4年の有罪判決を受けた。「RaaS」や生成AIは、必ずしも高度なスキルを保有していなくてもランサムウェア攻撃を比較的容易に実施できるようにするものであり、ランサムウェア攻撃による被害拡大の一因となっている。

企業・組織の内部ネットワークがランサムウェアに感染すると業務継続が困難になり、金銭的損失のみならず、情報漏えい等によって社会的信用を喪失する事態を招きかねないため、被害低減・予防のために適切な対策を講じることが推奨されている。

ランサムウェア攻撃への被害防止対策
VPN機器等のぜい弱性を塞ぐ
認証情報を適切に管理する
アクセス権等の権限を最小化する
ウイルス対策ソフト等を導入する
電子メール等を警戒する
ネットワークを監視する
データ等のバックアップを取得する

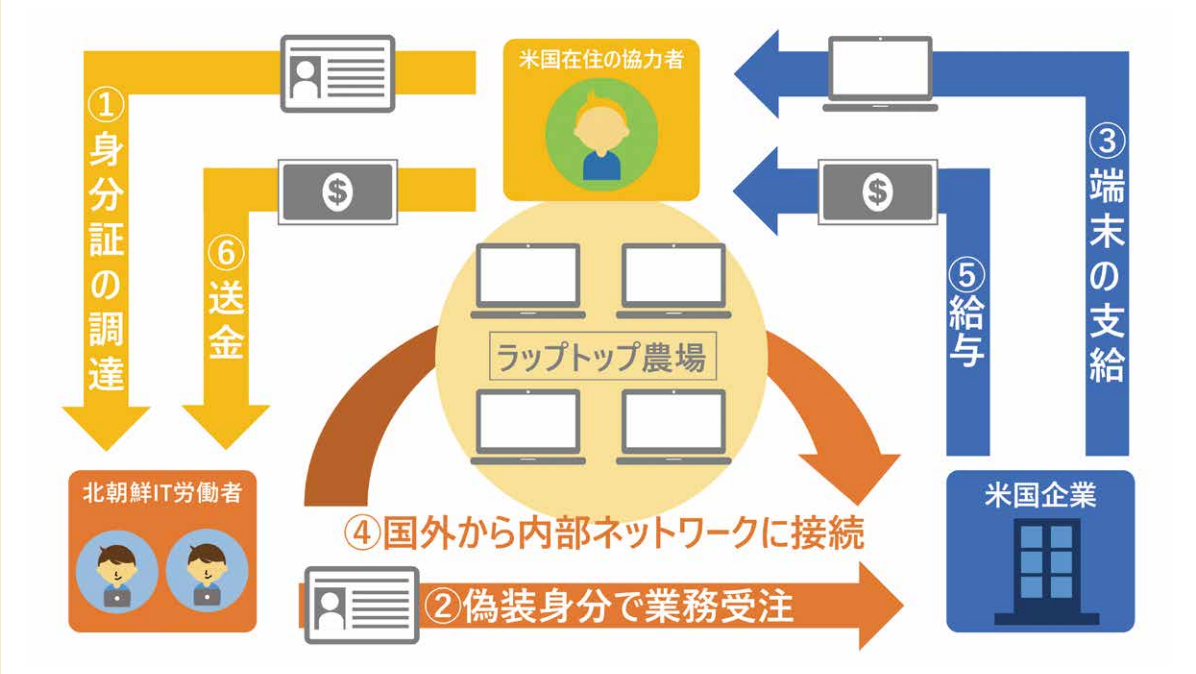
（警察庁ウェブサイト「ランサムウェア被害防止対策」<https://www.npa.go.jp/bureau/cyber/countermeasures/ransom.html>に基づき当庁作成）

COLUMN ②

隠れた脅威：リモートワーカーに紛れ込む北朝鮮IT労働者

コロナ禍を経てリモートワークが広く普及する中、北朝鮮IT労働者が国籍や氏名・経歴を偽ったり、実在の人物になりすましたりして、フリーランスのリモートワーカーとしてIT企業等から業務を受注し、ソフトウェアやシステムの開発に従事して報酬を得ている状況が把握され、各国が警戒を強めている。

米国で摘発された事案では、米国在住の協力者が、偽造身分証等を北朝鮮IT労働者のために調達したり、業務受注先の企業から支給された業務用ラップトップPCを集約して協力者の自宅に多数設置し（「ラップトップ農場」）、北朝鮮IT労働者が国外から企業の内部ネットワークに接続できるよう支援したりするほか、協力者が企業の給与を代理で受け取って北朝鮮IT労働者に送金したりするスキームが形成されていたという。



米国内の協力者が北朝鮮IT労働者の活動を支援するスキームのイメージ（米国司法省発表に基づき当庁作成）

我が国でも、3月、北朝鮮IT労働者が日本人になりすまして、我が国企業を対象とした業務受発注のためのオンラインプラットフォームを利用し、報酬を得ている疑いがあるとして、警察庁等が注意喚起を行った。過去に我が国で摘発された複数の事案では、北朝鮮IT労働者の活動を支援する我が国在住の協力者の存在も指摘されている。

北朝鮮IT労働者が獲得した報酬は、核・ミサイル開発の資金源となるおそれがあり、業務委託であっても北朝鮮労働者に報酬を支払った場合は国連安保理決議に基づく制裁に違反する可能性がある。また、北朝鮮IT労働者が業務で関与した企業の内部ネットワークにアクセスして情報窃取するなどの悪意あるサイバー活動に関与している可能性も指摘されている。

北朝鮮IT労働者の代表的な手口
国籍や身分を偽るなどしてプラットフォームへのアカウント登録等を行う
プラットフォーム等で、ウェブページ、アプリケーション、ソフトウェアの製作等の業務を幅広く募集している
VPNやリモートデスクトップ等を用いて、外国から作業を行っていることを秘匿している場合がある
不自然な日本語を用いるなど日本語が堪能ではなく、そのためテレビ会議形式の打合せに応じない
プラットフォームを通さず業務を受発注することを提案する
一般的な相場より安価な報酬で業務を募集している
複数人でアカウントを運用している兆候がみられる
暗号資産での支払を提案する

（警察庁等「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3月26日付け＞に基づき当庁作成）

COLUMN ③

国家主体等の関与が指摘される「ニュースサイト」を利用した偽情報等の拡散

近年、インターネット上では、あたかも報道機関が運営しているかのような体裁の「ニュースサイト」が数多く確認されている。こうした「ニュースサイト」の中には、国家主体等の関与や、特定国の主張に沿った記事の掲載が指摘されているものも存在する。

ロシアについては、フランス政府が、多数のウェブサイトによるネットワーク「Portal Kombat」が親露プロパガンダを展開している旨指摘する報告書を発表した（2月）ほか、米国司法省が、キリエンコ・ロシア大統領府第一副長官主導の下、米国主要メディアを模倣したウェブサイトが作成され、これを通じた米国世論を誘導する試みが確認されたとして、32のドメイン名を凍結する旨発表する（9月）など、欧米政府等がロシアの関与が疑われる情報工作を暴露・非難する動きが広がっている。なお、ロシア政府の関与の有無は断定できないものの、ロシアの主張に沿う報道等を日本語で転載する「ニュースサイト」の設立も複数確認されている。

中国に関しては、カナダの研究機関が発表した報告書（2月）で、中国企業が、我が国を含む30か国の現地メディアを装った123以上の「ニュースサイト」を運営している旨指摘されている。これらの「ニュースサイト」は、当該国現地メディアからの転載記事等に紛れ込ませる形で、中国国営メディアの記事や偽情報を含む親中国的な記事を拡散しているとされている。

こうした「ニュースサイト」は、文章の一部に簡体字が用いられるなど、一見して不審なものもあるが、中には、レイアウトが既存報道機関のサイトに酷似し、非常に紛らわしいものもある。こうした疑わしい「ニュースサイト」には、アクセスしないことが大切である。

米国司法省が凍結対象と発表した主なドメイン名
washingtonpost.pm
fox-news.top
fox-news.in
lemonade.ltd
spiegel.agency

（FBIによる宣誓供述書を基に当庁作成）

「ニュースサイト」の「銀座新聞」トップページ（写真提供：時事）