内外情勢

サイバー空間をめぐる動向

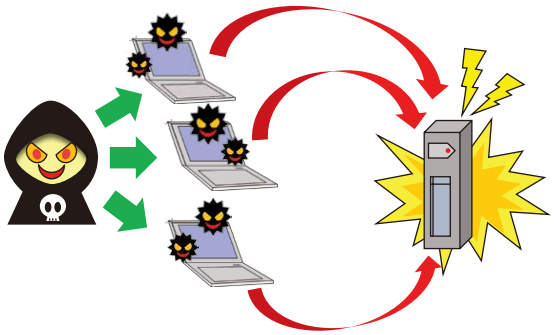
脅威が拡大するサイバー空間上の動向

サイバー攻撃は、我々の生活にとってより一層身近になっている。令和6年（2024年）12月から翌年1月にかけて、我が国の航空事業者・金融機関・通信事業者等に対する「DDoS攻撃」が相次いで発生し、一部サービスが停止したほか、9月から10月にかけて、大手飲料製造企業や大手通信販売企業が、「ランサムウェア攻撃」による被害を受け、物流システム等に深刻な影響が出た。

また、近年、一部の国家支援型サイバー脅威主体が、政治的・経済的・軍事的目的を達成するため、情報窃取にとどまらず、重要インフラの妨害・破壊等を企図したサイバー攻撃を実施しており、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る。

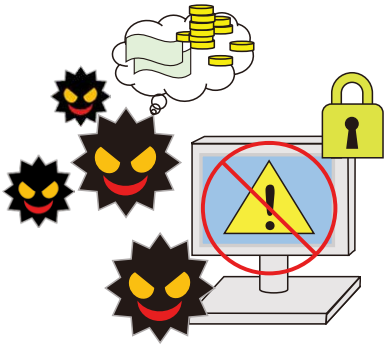
こうしたサイバー攻撃等において、家庭用ルーターが踏み台として悪用される事例が少なからず確認されており、それによって、社会に深刻な被害をもたらしかねないサイバー攻撃の展開が容易になっているだけでなく、その防御も困難になっている（P.34 COLUMN≫1「あなたの家がサイバー攻撃の拠点に？：家庭用ルーターが狙われる」参照）。

【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
(DDoS＝Distributed Denial of Service)



（当庁作成）

【ランサムウェア(Ransomware)】
「身代金」(Ransom)と「ソフトウェア」(Software)を組み合わせた言葉であり、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



（当庁作成）

高度化するサイバー攻撃手法

サイバー攻撃の手法も高度化している。企業や行政機関等の間でサイバー攻撃対策への意識が深まり、セキュリティは一層強化されているが、コンピュータ内に元々入っている正規のツールを悪用し、セキュリティを回避する「ファイルレス攻撃」（P.35 COLUMN≫2「最近のサイバー攻撃の特徴：『ファイルレス攻撃』と認証情報の流出がもたらす新たな脅威」参照）

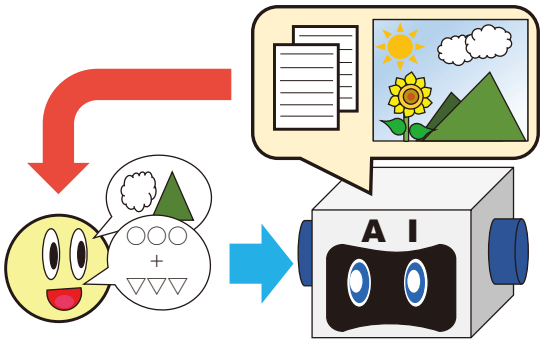
による被害の増加等が確認されている。

また、幅広く普及しつつある生成AIが、サイバー攻撃や偽情報の拡散に悪用される事例も確認されている（P.36 COLUMN≫3「生成AIに潜むリスク：『データポイズニング』の脅威」参照）。ウクライナ政府は、7月、インターネット上のターゲットに侵入後、外部の生成AIと通信して「次に何をすればよいか」を尋ね、その生成AIが回答した手順通りに情報窃取を行うサイバー攻撃を受けたことを公表した。こうしたサイバー攻撃では、侵入時には明確な攻撃プログラムが含まれていないため、従来のウイルス対策ソフト等では検知が難しいとされる。

このように、サイバー空間における悪意ある主体の攻撃手法は、日々進化しており、完全な対策を施すことは難しい状況となっている。

【生成AI】

インターネット上の情報を大量に学習し、ユーザーが入力した指示に沿って文章や画像等を自律的に生成できるAI技術



（当庁作成）

軍事行動とサイバー攻撃の統合

近年、世界各地で、軍事的衝突に至る事案が生じており、中には、軍事行動とサイバー攻撃を統合して行う例も見受けられる。ロシアによるウクライナ侵略では、軍事侵攻に先立ち、指揮・命令系統を妨害するための衛星通信設備へのサイバー攻撃が行われ、大規模サイバー攻撃を伴った最初の本格的軍事行動とも指摘されている。侵略が継続される中、ロシアは、ミサイルやドローンによる攻撃の効果を高めるために、ハッキングした監視カメラを用いて、ウクライナの防空システムの偵察や重要インフラの位置の特定を行っているとされる。また、ロシアは、エネルギー需要が高まる冬期に、ウクライナ最大の民間エネルギー企業に対するサイバー攻撃を行うと同時に、同社の火力発電所を砲撃し、住民の被害・混乱を増幅させたとされる。

ロシアによる攻撃を受けるウクライナ（写真提供：ZUMA Press/アフロ）

こうした状況に対し、米国国家情報長官室は、3月、ロシアがサイバー攻撃と軍事行動を統合した経験を蓄積し、有事の際に複合効果を高める潜在力を確実に向上させていると指摘し、懸念をあらわにした。

国家等の関与・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、国家等の関与・支援が疑われるサイバー攻撃について、その抑止に向け、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7年（2025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

発出月	発出国	概要
1月	米国	米国財務省は、米国政府のシステム等に対しサイバー攻撃を行ったとされる、中国の国家支援型サイバー脅威主体「Flax Typhoon」に関与したとして、中国企業に対し、資産凍結等の措置を実施すると発表
1月	米国	米国財務省は、同省のネットワークへの侵入に関与したとして、中国国家安全部関係者1人に対し、また、米国の大手通信企業等にサイバー攻撃を行ったとされる中国の国家支援型サイバー脅威主体「Salt Typhoon」に関与したとして、中国企業に対し、それぞれ、資産凍結等の措置を実施すると発表
3月	米国	米国司法省は、米国政府のシステムに対するサイバー攻撃等に関与したとして、中国公安部職員2人を含む中国企業関係者ら12人を起訴したと発表
8月	米国	米国国家安全保障局（NSA）は、「Salt Typhoon」に関する国際アドバイザリー（「Salt Typhoon」の攻撃手法を技術的に説明した上で、攻撃の検知方法や緩和策を示すもの）を発表。同アドバイザリーには、我が国、豪州等を含む13か国の各政府機関が共同署名

（各種公開情報に基づき当庁作成）

■ロシア

発出月	発出国等	概要
1月	EU	EU理事会は、エストニアに対しサイバー攻撃を行ったとして、ロシア連邦軍参謀本部情報総局（GRU）第29155部隊の部隊員3人を制裁対象者に追加すると発表
4月	フランス	フランス欧州・外務省は、自国の政府機関や民間企業などに被害を及ぼしたとして、GRUと関係を有するサイバー脅威主体「APT28」によるサイバー攻撃を非難する声明を発表
7月	英国	英国外務・開発省は、自国に対するサイバー攻撃に関与したとして、GRU第26165部隊を含むGRU3部隊及びGRU関係者18人に対し、資産凍結や英国への渡航禁止等の制裁を科す対象に指定
9月	米国	米国国務省は、自国の重要インフラ関連組織を狙っ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3人に関する情報に対し、最大1,000万ドルの報奨金を提供すると発表

（各種公開情報に基づき当庁作成）

■北朝鮮

発出月	発出国	概要
1月	日米韓	我が国、米国及び韓国の各政府は、北朝鮮のサイバー脅威主体による暗号資産窃取を目的とした標的型攻撃等への警戒を呼び掛ける共同声明を発表

（各種公開情報に基づき当庁作成）

なお、中国・ロシア・北朝鮮の関与・支援が疑われるサイバー脅威主体には、主に以下のようなものがある。

	主体の識別名（別名の例）	関連が疑われる機関	関与したサイバー攻撃事案、標的等
中国	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	中国国家安全部	・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）
	Flax Typhoon	不明	・米国の重要インフラ等へのサイバー攻撃（2022、2023年）
	Salt Typhoon	不明	・複数の米国大手通信事業者への侵入（2024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（総当たり）攻撃（2021年）
	APT29 （Cozy Bear）	ロシア対外諜報庁	・米国の政党のシステムへの侵入（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	ロシア連邦軍参謀本部情報総局	・ウクライナ政府機関等のシステムへの侵入
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
	Kimsuky	朝鮮人民軍総参謀部偵察総局	・米国等の組織・個人に対する標的型メール攻撃
	Andariel	朝鮮人民軍総参謀部偵察総局	・米国等の防衛・宇宙・原子力・製造分野を狙った情報窃取（2024年）

（各種公開情報に基づき当庁作成）

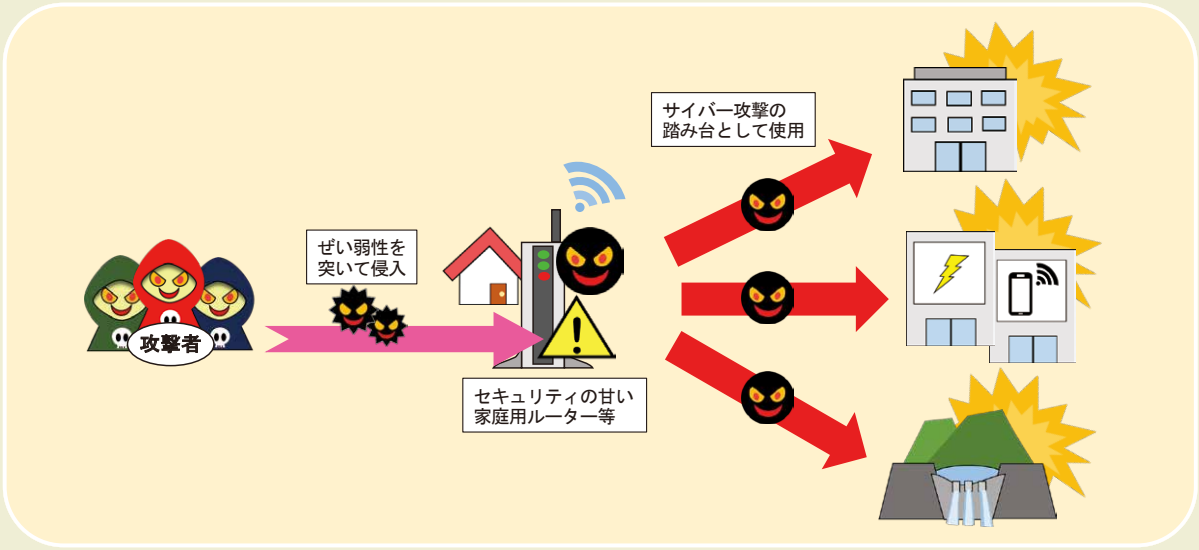
COLUMN » 1

あなたの家がサイバー攻撃の拠点に？：家庭用ルーターが狙われる

インターネットが広く普及し、我々の生活に欠かせないものとなった今、家庭用ルーターは、多くの家庭で用いられるようになった。また、最近では、単なる通信の接続にとどまらず、スマートデバイスやIoT機器を支える家庭内インフラとしての役割も担っており、その重要性はより高まっている。

その一方で、家庭用ルーターがサイバー攻撃に悪用される事例も度々確認されている。国家等の関与・支援が疑われるサイバー攻撃において、家庭用ルーターが悪用されたことも指摘されており、各国の政府機関が警告を発している。

令和5年（2023年）5月、「ファイブ・アイズ」（注）諸国の政府当局等が、中国のサイバー脅威主体「Volt Typhoon」の活動について発表した共同勧告では、米国の重要インフラ関連組織のネットワークが「Volt Typhoon」に侵入されていたことが明らかにされ、注目を集めたが、この侵入の“中継地点”として、家庭用ルーターが悪用されたことが指摘されている。「Volt Typhoon」は、家庭用ルーター等のぜい弱性を突いて侵入し、これを踏み台とすることで、不審な通信と検知されることを避け、重要インフラ関連組織への攻撃の事実自体を察知させないために使用していたとされる。



家庭用ルーターを悪用したサイバー攻撃のイメージ（当庁作成）

同勧告によると、この攻撃において悪用されたのは、メーカーによるサポートが終了しているなど、セキュリティの甘い家庭用ルーター等であったとされている。

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、家庭用ルーター等が悪用されることへの対策として、主に以下の対策を推奨している。

	対策
1	初期設定のパスワードは使用せず、推測されにくい強固なパスワードを設定する。
2	使用していない、不要な機能については無効化する。
3	製造元が提供する最新のファームウェア（機器に内蔵されているプログラム）を適用し、ぜい弱性を修正する。

国家等の関与・支援が疑われるサイバー攻撃を防ぐため、また、自身の家庭用ルーターが攻撃に悪用されることを防ぐため、家庭用ルーターも、“サイバーセキュリティの最前線”であることを、改めて認識していただきたい。

（注）米国、英国、豪州、カナダ及びニュージーランドによる情報共有の枠組み

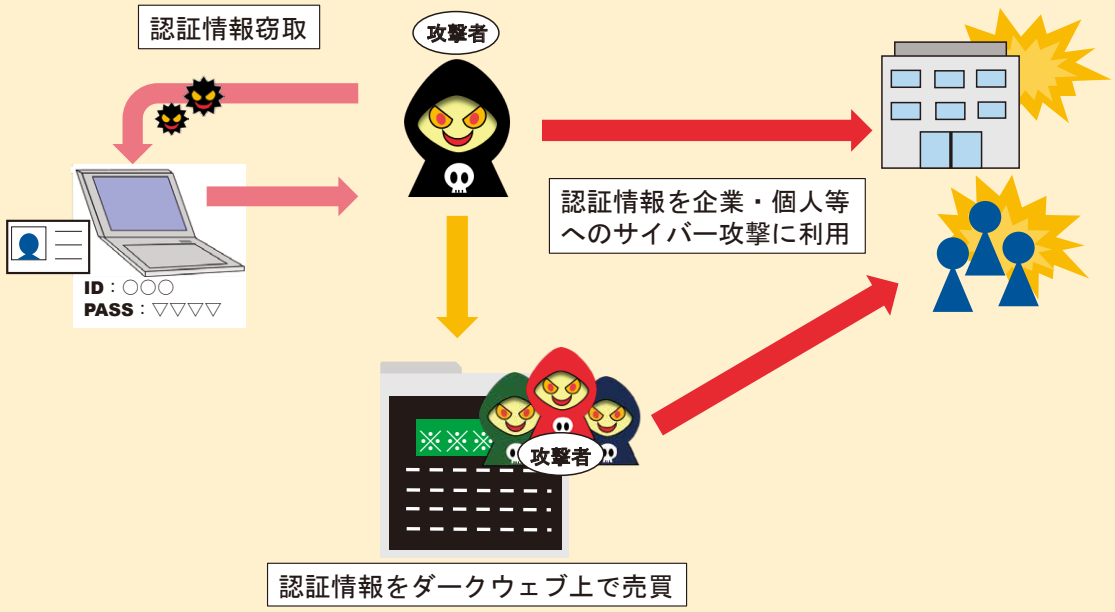
COLUMN » 2

最近のサイバー攻撃の特徴：「ファイルレス攻撃」と認証情報の流出がもたらす新たな脅威

欧米のサイバー当局は、近年のサイバー攻撃について、「ファイル」に依存する従来のマルウェアを使用した攻撃に加え、「ファイルレス攻撃」と呼ばれる手法による攻撃が確認されるようになったと指摘している。従来のマルウェアを使用した攻撃は、情報窃取や遠隔操作等、悪意のある挙動を実行させる悪性ファイルをコンピューターの記憶装置上に作成・保存するため、攻撃の痕跡が残りやすく、セキュリティ製品で検知することも比較的容易であった。一方、「ファイルレス攻撃」は、従来のマルウェアを使用した攻撃と異なり、悪性ファイルを記憶装置上に作成・保存せず、標的のシステムやコンピューター内に元々入っている正規のツールを悪用して攻撃を実行する。そのため、「ファイルレス攻撃」は、悪性ファイルを探してブロックするという従来のセキュリティ対策のみでは、防御することが困難となっている。

また、最近、欧米のサイバー当局等は、ユーザーIDやパスワードといった認証情報が、通常の検索エンジンでは見つけることができない、いわゆるダークウェブ上に漏えい、売買されていることを深刻なリスクとして警告している。

加えて、サイバー攻撃者が、ダークウェブ上で入手した認証情報を悪用し、容易かつセキュリティ製品に検知されないようにサイバー攻撃を実行することが可能となっているという指摘もある。



認証情報を悪用したサイバー攻撃のイメージ（当庁作成）

これらの状況に対し、豪州通信情報局（ASD）豪州サイバーセキュリティセンター（ACSC）は、各国のサイバー当局等とともに、「ファイルレス攻撃」等への対策として、正規のツールも含め、使用するシステムやコンピューターの動作を監視し、不自然な挙動を検知する機能の導入を検討することを推奨している。また、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、認証情報を悪用した攻撃に対する防御策として、SMS認証や顔認証等の多要素認証の使用といったセキュリティ対策を実施することを推奨している。

COLUMN » 3

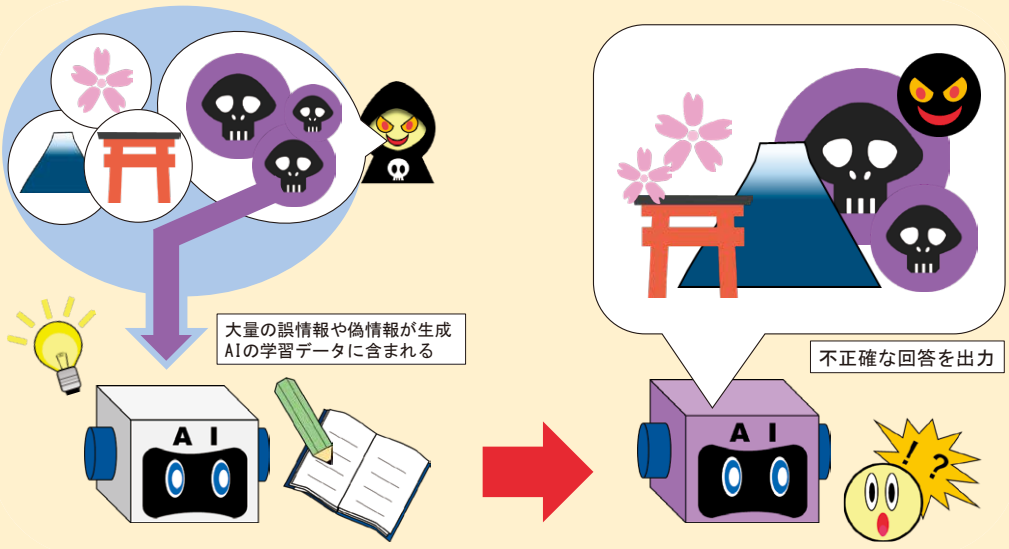
生成AIに潜むリスク：「データポイズニング」の脅威

検索エンジンに生成AIが搭載されるなど、これまでAIをほとんど利用する機会がなかった人々の間でも、AIの存在が身近なものになりつつある。一方、急速に発展・普及した生成AIはその性質上、さまざまなリスクを内包している。その一つが、「データポイズニング」である。

「データポイズニング」とは、開発・運用段階でインターネット上のデータを大量に学習する生成AIの仕組みを悪用し、開発者の意図に反して不正確な、偏った、あるいは悪意のある結果を出力させることを目的として、攻撃者が学習用データの中に、意図的に誤ったデータを混入させることを指す。

令和5年（2023年）9月に経済協力開発機構（OECD）が公表した報告書では、生成AIが、誤情報や偽情報を生成し、拡散するリスクを指摘している。

上記のOECDを始め、様々な政府機関等が生成AIに内包されるリスクについて言及している。利用する我々も、そうしたリスクについて認識し、生成AIの回答をうのみにしないなどの注意が必要であろう。



生成AIに関する「データポイズニング」のイメージ（当庁作成）