特集／サイバーセキュリティ

〈1〉日本と世界のサイバーセキュリティの現状と経済産業省の施策について

経済産業省商務情報政策局サイバーセキュリティ課
橋本　勝国（企画官）

1. 2025 年の日本のサイバー事故ニュース

2025 年は絶え間なくサイバー事故のニュースで持ちきりだったような感覚があります。年初は航空事業者、金融機関、通信事業者等が DDoS 攻撃を受けサービスが一時停止するという話題から始まり、春には証券会社のアカウント乗っ取り被害が多発して連日大きなニュースになりました。秋のアサヒ HD とアスクルのランサムウェアによる出荷停止のニュースがクライマックスだったかと思います。ランサムウェア攻撃によるシステムの停止により製品の出荷が数ヶ月にもわたって停止や制限されるという、国民生活にも直接大きな影響を与える事案であり、日本社会が未だ経験したことのない未知の領域にまでサイバー攻撃が高度化・過激化していると感じた人も多いのではないでしょうか。

2. なぜ日本でサイバー攻撃が急増しているのか

話題が少しそれますがお付き合いください。昨年、秋田県など東北地方や北海道で熊の市街地への出没急増が大きな話題になりました。我々人間から見ると急に熊が市街地に出てきて人間に危害を加えるようになったように見えます。しかし自然現象には必ず原因が存在します。おそらく熊が市街地まででてこざるを得ない理由があるはずです。気候変動による自然環境の変化と餌となる生物の数の変化、天敵がいないことによる個体数の増加など、複数の要因により市街地まででてこないと餌にありつけないような状況に熊たちがおかれていることも想定されます。あるいは人間の住むエリアが単に拡大しているだけかもしれません。真の原因究明については調査がまたれるところです。

閑話休題。日本でサイバー攻撃が増加していることも単なる一時的な現象ではなく、実は明確な原因が存在します。まずは AI の急激な進化があります。今まで海外のサイバー脅威アクターにとって自然な日本語を作成することは非常に難度が高く、つたない表現の怪しい日本語でフィッシングメールを作成するくらいが限界でした。ところが AI の急速な発展により日本語の難度は問題ではなくなり、日本の会社からの本物のメールと見分けがつかないような、巧妙で高度なフィッシングメールが横行しています。またサイバー攻撃自体にも AI が利用され自動化されることで、絨毯爆撃のように手当たり次第色々なシステムに総ざらいの攻撃を行うことが、サイバー脅威アクターにとっては苦も無く実施できるようになってきています。

加えて、紛争などに伴い国家支援の高度サイバー攻撃ツールの開発が隆盛を極めていることが挙げられます。ロシアは侵攻を始める前からウクライナに対して大規模なサイバー攻撃を、今日に至るまで継

続的に実施しています。また中国も台湾へのサイバー攻撃を加速させているという情報もあり、2025年には1日平均263万回のサイバー攻撃があったとする報告書を、台湾の情報機関である国家安全局が発表しています。（なおこれは2023年の123万回、24年の246万回からさらに増えているとされています）これらの攻撃に利用される高度なツールの一部をサイバー脅威アクターが流用することで、世界のサイバー攻撃全体の高度化に拍車がかかっています。

さらにやっかいなことに、ダークウェブ上では攻撃ツールの売買も可能な脅威アクター間のコミュニティができあがっており、ダークウェブにアクセスさえできれば誰でも簡単に攻撃ツールや乗っ取ったサーバへのログイン権利を売買したり、仲間を探すことができます。初期侵入専門、ランサムウェアを使った暗号化と脅迫専門、などの分業制もコミュニティ内で確立されており、初心者でも参入しやすくランサムウェアの脅迫などで手っ取り早く稼げるような「ビジネスモデル」があり参入の障壁が非常に低くなっています。

このような背景から、過去10年間日本へのサイバー攻撃は増加の一途をたどってきました。NICTのレポートによると2015年から2024年の間にサイバー攻撃の年間パケット数は10倍程度に増えています。

（https://www.nict.go.jp/press/2025/02/13-1.html）

このようなサイバー攻撃の高度化・頻度増により、大波のようなサイバー攻撃が海外から日本に押し寄せており、毎年高度化・増加の一途をたどっています。これに対して一部の日本企業のサイバーセキュリティ対策が追いつき切れていない現状があると思われ、サイバー攻撃の激増といった印象につながっているのだと思います。

3. 国内外のサイバー攻撃の現状

いくつか国内外のサイバー攻撃の事案について説明します。中国の関与が疑われる脅威アクターは台湾だけでなく米国や日本への攻撃も実施しています。2019年以降、中国を背景とするグループ「MirrorFace」により執拗に日本の安全保障や先端技術に係る情報窃取を目的とした攻撃キャンペーンが行われており2025年に警察庁などにより注意喚起が行われています。

（https://www.npa.go.jp/bureau/cyber/koho/caution/caution20250108.html）

またこれも中国背景とされるグループ「Salt Typhoon」が、2024年後半に米国の通信事業者のネットワークに侵入して政府関係者の通話記録など安全保障に関する情報の窃取を狙う活動が報告されています。

(https://www.congress.gov/crs-product/IF12798)

さらに「Volt Typhoon」と呼ばれるこれもまた中国を背景としたグループが米国の重要インフラ（電力など）のシステムに忍び込み、有事の際に米国に対しサイバー攻撃を行うためネットワークのアクセス権限を確保する動きがあったという注意喚起が米国政府からなされました。

(https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)

私も驚いたのは2026年1月の米国によるベネズエラ大統領逮捕の際に首都カラカスの電力を米国がサイバー攻撃によって停電させたという報道です。トランプ大統領自身も「我々の特定の技術でカラカスに大停電を発生させた」と述べています。

(https://www.nikkei.com/article/DGXZQOCD207AQ0Q6A120C2000000/)

日本国内の実被害が大きかった事例としては、昨年のアサヒHD、アスクルのランサムウェア事案はもちろん、2024年には(株)KADOKAWAもランサムウェア攻撃をうけ、ニコニコ動画などのWebサービスが長期間停止、また北朝鮮を背景としたグループ「TraderTraitor」がDMM Bitcoinのシステムへ取引先経由で侵入し約500億円相当の暗号資産を窃取しました。DMM Bitcoinは結果として廃業まで追い込まれる事態となりました。

これらの事例を見ると下記のような共通のトレンドが浮かび上がってきます。

①国家を背景としたグループによる安全保障にかかわる情報の窃取
②電力や通信事業者など国民の生活に直結する重要インフラへの忍び込みと攻撃
③取引先経由の侵入
④サービスの停止と甚大な被害額

4. 世界各国のサイバーセキュリティ施策のトレンド

このような情勢も踏まえ、世界各国のサイバーセキュリティ施策のトレンドも上記のような脅威に対応できるよう変化してきています。

欧米ではIT製品が設計段階から安全に設計されユーザが特別な設定を施さなくても購入したままの状態で安全に使えるようにしなければならないという「セキュア・バイ・デザイン」の概念が浸透しつつあり、EUでは2024年12月に制定されたサイバーレジリエンス法によりデジタル製品の製造者にセキュリティを考慮した設計を義務付けました。2027年12月に同法の運用が開始される予定となっています。英国では消費者向けIoT製品に一定のセキュリティ基準を義務付けたPSTI法が2024年4月に施行されました。米国でもサイバー・トラスト・マークというルータや無線IoT製品に対するセキュリティのラベリング制度が準備中となっています。これらのセキュリティ面が一定程度担保された機器が流通することで社会全体でのサイバー防御力が上がり、ワクチン接種人口増加がはしかなどの感染症流行を低下させるように、サイバー攻撃を一定程度防いでくれることが期待されます。

また国民生活に直結する重要インフラ事業者（電気、ガス、水道、通信事業者など）についてはサイバー攻撃の成功が国民生活と経済を直撃するため、重要インフラ事業者のサイバーセキュリティ基準を強化しサイバーインシデントが発生した際の政府への報告を義務付ける動きが加速しています。米国では重要インフラ事業者に対して重大なサイバーインシデントの認知後72時間以内の政府への報告、ランサムウェアの身代金支払い後24時間以内に米CISAへの報告が義務付けられる法律が2022年3月に成立し、運用開始に向けて詳細が検討されています。EUではもともとNIS指令という重要インフラ事業者にサイバーインシデント報告を義務付ける仕組みがありましたが、2016年に対象セクターが拡大され、サイバーインシデント認知後24時間以内にEU当局へ報告という形で規制が強化されました。自国の国民生活と経済を守るために重要インフラ事業者のサイバーセキュリティ対策の高度化は必須となりつつあります。

さらに企業のサイバーセキュリティ対策水準を整備・可視化する動きがあります。英国では全ての企業に対し一般的なサイバー攻撃への防御策を提供することを目的としたサイバー・エッセンシャルズという認証制度が制定されました。英国政府や公的機関が調達においてこの認証制度を必須としています。オーストラリアにおいてもすべての企業を対象としたエッセンシャル・エイトという類似制度があります。また米国防省はより厳しいセキュリティを求めるべくCMMC（サイバーセキュリティ成熟度モデル認証）という独自基準を策定し、調達に適用しています。調達にこういった基準を組み込むことで自組織だけでなくサプライチェーン全体でサイバーセキュリティ防御力を高めることができます。

5. 日本国の状況

世界的なサイバー攻撃の激化・高度化の波の中、日本では2025年5月にサイバー対処能力強化法および同整備法が成立し、2026年度の施行が予定されています。この法律の目的としては官民の情報共有の強化、政府による通信情報の分析と攻撃兆候の早期検知、必要時の攻撃サーバ無害化措置といった能動的サイバー防御の制度基盤を構築することです。基幹インフラ事業者によるサイバーインシデントの報告義務および情報共有・対策のための協議会の設置が明言されています。また攻撃兆候の早期検知のため国が通信事業者から国内のサイバー通信情報を取得し分析する法的な根拠が与えられています。自衛隊や警察による重大なサイバー被害を防止するため攻撃サーバへのアクセス・無害化措置も一定の条件下にて可能となりました。

また同法律の成立の2ヶ月後にサイバーセキュリティ戦略本部（NISC）が国家サイバー統括室（NCO）へ改組されました。従来のNISCは民間企業に対する権限不足や重大サイバー攻撃への直接対処能力において課題がありましたが、同法の成立とともにNCOにはより大きな権限が与えられています。欧米並みのサイバー対処能力の実現のため、NCOは今後民間からのサイバーインシデント報告、情報共有のための協議会制度、警察庁・防衛省などの国内組織の連携総括など、まさに国のサイバーセキュリティの司令塔としての役割が期待されています。経済産