特集 2

我が国に対するサイバー攻撃

1　我が国への脅威が拡大するサイバー攻撃

我が国企業等を標的としたサイバー攻撃が相次いで発覚

業務の妨害、機密情報の窃取、金銭の獲得など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る。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る。

さらに、国家が政治的、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る。

令和3年（2021年）も、機密情報の窃取を狙ったとみられるサイバー攻撃事案の発覚が相次いだ。

宇宙航空研究開発機構（JAXA）など約200組織に対するサイバー攻撃事案では、平成28年（2016年）9月から平成29年（2017年）4月までの間、合計5回にわたり、偽名で我が国のレンタルサーバを契約したとして、警視庁が当時我が国に滞在していた中国共産党員の男を東京地方検察庁に送致した（4月）。同事案には、中国人民解放軍第61419部隊を背景に持つ中国のサイバー脅威主体「Tick」が関与している可能性が高いと指摘された。また、大手電気機器メーカーは、社内外とインターネット上で情報共有を行うツールに対するサイバー攻撃事案を公表し（5月）、内部調査の結果、100組織以上の個人情報を含むデータが窃取され、同ツールのぜい弱性を悪用したとみられる第三者により、正規のIDとパスワードを用いて外部から不正アクセスが行われたものと判明した（8月）。さらに、令和2年（2020年）12月に公表された大手重工メーカーに対するサイバー攻撃事案は、内部調査の結果、海外拠点経由で国内外の一部サーバに不正アクセスが行われ、情報が流出した可能性が指摘されている（7月）。

これらの事案は、比較的セキュリティが手薄な海外拠点経由で我が国企業を狙った攻撃やゼロデイぜい弱性（未知のぜい弱性）を悪用した攻撃であり、国家が関与・支援したサイバー攻撃の可能性も指摘されている。

国外においても、ゼロデイぜい弱性を悪用したサイバー攻撃事案が発覚した。

米国情報通信企業「Microsoft」の提供するメッセージプラットフォームのゼロデイぜい弱性を悪用したサイバー攻撃について、米国政府は、中国国家安全部と関連を有するサイバー脅威主体が世界中の数万に及ぶコンピュータとネットワークに侵入したと発表した（7月）。

このほか、米国における水道水の有毒化を企図した浄水場に対するサイバー攻撃（2月）や、ニュージーランドにおける金融機関や郵便事業者を標的としたサイバー攻撃（9月）など、重要インフラに対するサイバー攻撃（P.16 COLUMN）も報じられた。

我が国においても、重要な情報やインフラをサイバー攻撃の脅威から守るため、引き続き警戒が必要である。

国家的関与が指摘される事案が継続して発生

米国、英国などは、サイバー攻撃の実行者と所属する国家機関等を特定・公表する取組（パブリック・アトリビューション）を積極的に展開している。こうした取組において、中国、ロシア及び北朝鮮の国家的関与が指摘された事案は以下のとおりである。

■ 中国

中国については、軍や情報機関による大規模なサイバー諜報への関与のほか、当局とサイバー犯罪者がいわば“共生関係”にあることも指摘されている。

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、海南省国家安全庁の職員3人と中国情報通信企業「海南仙盾」に雇われたハッカーの計4人の起訴を発表した（7月）。あわせて、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）、国家安全保障局（NSA）及び連邦捜査局（FBI）は、当該キャンペーンを実行した中国のサイバー脅威主体「APT40」に関する共同勧告を発表した（7月）。我が国外務省も、報道官談話で「APT40」に言及した（7月）ほか、英国、カナダ、豪州、ニュージーランド、欧州連合（EU）及び北大西洋条約機構（NATO）も同主体を非難する声明を発表した（7月）。

■ ロシア

ロシアについても、治安機関とサイバー犯罪者との“協力関係”のほか、サイバー攻撃への軍や情報機関の関与が指摘されている。

米国情報通信企業「SolarWinds」製のIT管理ソフトウェアの更新プログラムを悪用した攻撃に端を発した大規模サイバー攻撃事案（令和2年〈2020年〉12月公表）を受け、米国政府は実行主体として、ロシア対外諜報庁（SVR）と関連を有するサイバー脅威主体「APT29」（別名「Cozy Bear」）を名指しした上で、同事案を含むロシアによる悪意あるサイバー活動等への対抗策として、ワシントンD.C.に駐在する10人の外交官の国外追放や、ロシアの6企業に対する制裁を含む大統領令を発出した（4月）。同事案については、米国の大統領令発出に併せて、英国外務省も、SVRの関与があった可能性が高い旨の声明を発表した（4月）。

また、欧州理事会は、「Ghostwriter」と呼ばれる悪意あるサイバー活動にロシア政府が関与しているとして、非難する声明を発表した（9月）。同声明では、「Ghostwriter」は、多数の欧州議会議員、政府関係者等を標的とし、コンピュータシステム等に侵入してデータを窃取した上で、偽情報の流布などを通じて、民主的な制度や手続を弱体化させることを企図しているとして、ロシアに対し、サイバー空間において責任ある国家として行動するよう促した。

■ 北朝鮮

米国司法省は、破壊的サイバー攻撃及びサイバー金融犯罪に関与したとして、北朝鮮偵察総局に属するハッカー3人の起訴を発表した（2月）。

また、国連安保理北朝鮮制裁委員会専門家パネルは、2020年度の報告書（3月公表）で、金融機関及び暗号資産交換業者を標的としたサイバー攻撃によって北朝鮮が獲得した資金は、令和2年（2020年）11月までの約2年間で3億ドル以上に上るほか、窃取した暗号資産を中国所在のブローカーを通じて現金化、資金洗浄していると指摘し、北朝鮮が暗号資産を標的としたサイバー活動を継続しているとの見解を表明した。

COLUMN 重要インフラに対するサイバー攻撃

重要インフラに対するサイバー攻撃は、国民生活の安全・安心に対する深刻な脅威である。

近年、国外では、重要インフラがサイバー攻撃に遭い、実生活に多大な影響を及ぼした事例が相次いでいる。米国では、石油製品パイプライン事業者「コロニアル」に対するランサムウェア（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）攻撃が発生し（5月）、同事業者がパイプラインを5日間操業停止としたことで、パニックによる買いだめが起き、東海岸ではガソリンの売り切れが続出するなど、多大な影響が生じた。本事案については、ロシアのハッカー集団「DarkSide」が関与を認め、社会に影響を与えたとして謝罪した。

その後開催された米露首脳会談では、バイデン大統領がプーチン大統領に対し、攻撃が許されない16分野の重要インフラ（化学、商業施設、通信、重要な製造分野、ダム、防衛産業基盤、緊急サービス〈警察、消防、救急等〉、エネルギー、金融サービス、食品・農業、政府施設、医療・公衆衛生、情報技術、原子炉・核物質・核廃棄物、輸送システム、上下水道）を提示した（6月）。

ガソリンを求める長蛇の車列（写真提供：ⓒRobin Rayne/ZUMA Wire/共同通信イメージズ）


米露首脳会談の様子（写真提供：ⓒWhite House/ZUMA Press Wire Service/ZUMAPRESS.com/共同通信イメージズ）

重要インフラに対するサイバー攻撃事案

年月	発生国	事案概要
平成25年（2013年）3月	韓国	金融機関や放送局で、同時多発的にマルウェア感染によるシステム障害が発生。ATMの利用や一部放送業務に支障
平成27年（2015年）12月	ウクライナ	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
平成29年（2017年）5月	我が国を含む約150か国	我が国を含む世界約150か国で発生した大規模ランサムウェア攻撃により、政府機関や医療機関、金融機関などの端末約30万台が感染
令和2年（2020年）10月	インド	中央給電指令所や港湾施設等に対するサイバー攻撃によりムンバイで大規模停電が発生
令和3年（2021年）5月	米国	米国最大の石油製品パイプライン事業者「コロニアル」がランサムウェア攻撃を受け、5日間操業停止。パニックによる買いだめで東海岸ではガソリンの売り切れが続出

（当庁作成）

2　クラウドサービス等を提供する事業者（MSP）を標的としたサイバー攻撃

クラウドサービスやファイル共有サービスなどシステムの運用・保守・管理に係るサービスを提供する事業者は、一般にマネージド・サービス・プロバイダ（MSP）と呼ばれる。MSPは複数の顧客とネットワークやサーバ等のシステムを共有することから、同システムへのサイバー攻撃は、顧客のシステム等への侵入・拡大につながる危険性もある。

国家が関与・支援したとみられるMSPに対するサイバー攻撃

MSPのシステムへの侵入に成功すると、多くの顧客情報の入手や顧客のシステムへの侵入が容易になるという効率の良さから、MSPに対するサイバー攻撃は頻繁に行われており、特に、国家が関与・支援するサイバー脅威主体からは執ように狙われてきた。例えば、中国国家安全部の傘下で活動しているとされるサイバー脅威主体「APT10」は、平成20年（2008年）頃から、世界中のMSPを標的としたサイバー攻撃キャンペーン「クラウドホッパー作戦」を展開してきたとされ、平成30年（2018年）12月、米国司法省は、知的財産や営業秘密の窃取目的で世界中のコンピュータに侵入したとして、「APT10」関係者2人を起訴したと発表した。

MSPに対する攻撃による情報流出事案が発生

我が国でも、MSPに対するサイバー攻撃による情報流出事案が相次いで発生している。

令和2年（2020年）5月、クラウドサービスを提供する我が国のMSPは、当該事業者に対するサイバー攻撃事案を公表し、内部調査の結果、200社近い顧客に影響が出たことが判明した。令和2年（2020年）12月には、MSPに対するサイバー攻撃の結果、大手重工メーカーの子会社が不正アクセスを受けたことを公表した。このほか、社内外とインターネット上で情報を共有するサービスを提供するMSPに対するサイバー攻撃事案では、100組織以上の個人情報を含むデータが窃取されたことが判明している（5月）。

国外では、米国情報通信企業「Kaseya」製品のゼロデイぜい弱性を狙ったランサムウェア攻撃事案が公表され（7月）、同社の製品が多くのMSPに導入されていたことから、最大1,500社に被害が及んだことが判明している。

今後も、様々なサイバー脅威主体によるMSPに対するサイバー攻撃が継続するとみられ、引き続き警戒が必要である。

3　新型コロナワクチンをめぐる情報窃取活動が活発化

欧米等で新型コロナワクチン関連組織に対するサイバー攻撃が発生

新型コロナウイルス感染症が世界中で拡大する中、新型コロナワクチンの開発・製造・輸送を行う組織やワクチン臨床試験機関、許認可機関等に対するサイバー攻撃が欧米等で相次いで発生している。

令和2年（2020年）12月に公表された欧州医薬品庁に対するサイバー攻撃事案では、製薬会社が提出した新型コロナワクチンの承認申請に係る文書などが窃取され、記載内容が加工された上で公開された。同庁に対するサイバー攻撃については、中国やロシアのサイバー脅威主体の関与の可能性が指摘されている。また、複数の米国製薬大手に対するサイバー攻撃について、北朝鮮のサイバー脅威主体の関与が報道されて（2月）おり、新型コロナワクチン関連組織を標的としたサイバー攻撃について、中国、ロシア及び北朝鮮の国家的関与が疑われる事案が相次いで発生している状況が浮き彫りとなった。

4　サイバーセキュリティ意識の向上が喫緊の課題

我が国の新型コロナワクチン関連組織に対しても、不正アクセスやサイバー攻撃の動きがあったと報道されている。

国家が関与･支援するサイバー脅威主体は、国家目標を達成するためにコスト度外視で執ように攻撃を継続する特徴があり、我が国企業や大学等の保有する機微な技術やデータ等を標的としたサイバー攻撃は今後も継続するとみられ、我が国においても、改めてサイバーセキュリティ意識の向上を図る必要がある。