宇宙サイバーと先端技術研究会　研究報告（Ｎｏ．2）　　2021年3月5日

サイバー安全保障上の脅威：回顧と展望

中曽根康弘世界平和研究所
主任研究員　大澤　淳

サイバー安全保障上の脅威：類型と懸念国

2020 年に入り、我が国の企業を標的に情報窃取を狙ったサイバー攻撃が次々と明らかになった。1 月下旬には、三菱電機とNEC がサイバー攻撃の被害にあい、社内の端末が不正に操作され、外部にデータが送信されていることが判明した[1]。この二社を攻撃したグループは「Tick」(別名 BRONZE BUTLER)と言われるグループで、2006 年以降台湾および日本をターゲットとして様々な攻撃を行っている。この 2 社以外にも、防衛省と取引のある神戸製鋼所とパスコがサイバー攻撃の被害を受けていたことが防衛省から発表されている[2]。トレンドマイクロ社の分析[3]によれば、この攻撃グループは、中国に子会社を持つ日本の企業で、防衛、航空、化学、宇宙（衛星）など高度な技術を保有する会社を標的にしており、2019 年に新たな攻撃ツールを用いて活動を活発化させていた。

インターネットへの依存度に比例して、サイバー攻撃の脅威は増大している。重要インフラに対するサイバー攻撃は、国家の機能を麻痺させ、物理的な武力攻撃と同様の人的・物的損害を引き起こしかねない。サイバー空間では、国家が関与したとみられるサイバー攻撃が、この 10 年で急速に増加し、またその被害も深刻化している。このようなサイバー攻撃の中には、民間の防御では防ぐことができない攻撃も出現している[4]。

サイバー空間では、国家間の対立を背景とした国家が関与する攻撃も増加している。国家が関与するサイバー攻撃が観測されるようになったのは 2005 年ごろまでさかのぼるが、2015

---

[1] NEC「当社の社内サーバへの不正アクセスについて」2020 年 1 月 31 日。
https://jpn.nec.com/press/202001/20200131_01.html.
三菱電機株式会社プレスリリース「不正アクセスによる個人情報と企業機密の流出可能性について」、2020 年 1 月 20 日。https://www.mitsubishielectric.co.jp/news/2020/0120-b.pdf.

[2] 防衛省「防衛関連企業に対する不正アクセス事案について」2020 年 2 月 6 日。
https://www.mod.go.jp/j/press/news/2020/02/06c.pdf.

[3] TrendMicro Research; Joey Chen, Hiroyuki Kakara, and Masaoki Shoji, “Operation ENDTRADE: TICK’s Multi-Stage Backdoors for Attacking Industries and Stealing Classified Data”, Nov. 2019.
https://documents.trendmicro.com/assets/pdf/Operation-ENDTRADE-TICK-s-Multi-Stage-Backdoors-for-Attacking-Industries-and-Stealing-Classified-Data.pdf.

[4] Jun Osawa, “The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?”, Asia-Pacific Review, vol.24, No. 2(2017): 113-131.

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

年ごろまでの国家が関与する攻撃は、政策決定者や防衛産業など特定の企業・組織・個人から機密情報や知的財産を窃取することを目的とした標的型攻撃などの「情報窃取型」サイバー攻撃や、相手国内の混乱の誘発を狙い重要インフラの制御系システムの麻痺ないし破壊を目的とする「機能妨害型」/「機能破壊型」サイバー攻撃が主流であった。

しかし、2015 年ごろから、標的型攻撃の手法を用いて企業のネットワーク内に侵入し、不正な送金を行い、データを人質に身代金を要求する「金銭目的型」サイバー攻撃や、相手国内の情報操作を目的として、偽ニュースの流布、代理主体を用いたサイバー攻撃によるかく乱、サイバー窃取した機密情報の暴露などを行う「情報操作型」サイバー攻撃が新たに見られるようになってきた。

これらのサイバー攻撃を攻撃目的別に分けると表 1 のように整理することができる。

表 1:サイバー攻撃の類型

情報窃取型：	標的型攻撃（ウィルス付きメール、水飲み場攻撃）などにより、特定の政府機関、企業、団体、個人のネットワーク、PC に侵入し、機密情報、営業情報、特許、知的財産などを窃取する攻撃。
機能妨害型：	DDoS 攻撃等の手法により、ネットワークの許容量を超える飽和通信要求によって、サーバー、ネットワークを麻痺させる攻撃。
機能破壊型：	標的型攻撃などにより、特定の政府機関、企業、団体、個人のネットワークに侵入し、システム破壊・改ざんを行う攻撃。ネットワーク内のデータ消去・改ざんを目的とするものと、制御系システムを標的として物理的破壊を目的とするものがある。
金銭目的型：	標的型攻撃、脆弱性利用などにより、特定の政府機関、銀行、企業、個人のネットワークに侵入し、不正な送金を行い、または PC 内のデータを暗号化し、解読に身代金を要求する攻撃。
情報操作型：	代理主体(Proxy)等を用いて真の発信者を隠匿たうえで、SNS 等に偽ニュースを流布させることにより、対象国（主に民主主義国）における世論操作を目的とした攻撃。選挙結果に影響を与えることを企図している攻撃も見られる。
軍事的サイバー攻撃（ハイブリッド型）：	軍事攻撃と一体的に行われる機能妨害・機能破壊を目的とした攻撃。電子戦の一環として C4I を標的とするものと、軍事行動に影響を与える死活的インフラを標的としたものがある。

（著者作成）

現在、ほぼ全ての主要国が「サイバー軍」を創設するなど、サイバー空間で何らかの活動に関わるようになってきているが、その中でも「ロシア、中国、北朝鮮、イラン」の 4 カ国は、既存の国際ルールを逸脱したサイバー攻撃を積極的に行っており、安全保障上の脅威となっている。

米国は 2018 年 9 月に公表した『国家サイバー戦略』において、「ロシア、中国、イラン、北朝鮮」の 4 カ国を、「サイバーという道具を用いて、我々の経済と民主主義を弱体化させ、知的

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

財産を奪い、我々の民主主義のプロセスに争いのタネを蒔いている」敵対国であると明確に認定した[5]。

これらの 4 カ国が関与したと指摘されているサイバー攻撃の特徴を整理すると次の表 2 のようになる。

ロシアが関与するサイバー攻撃の特徴は、①周辺国に対する「機能妨害型」/「機能破壊型」攻撃、②軍事行動にサイバー攻撃を伴う「ハイブリッド戦」、③欧米をはじめとした民主主義国に対する「情報操作型」サイバー攻撃を伴う「情報戦」、である。

中国が関与するサイバー攻撃の特徴は、「情報窃取型」である。相手国の政府や政府機関が持つ「政策情報」の窃取、中国政府の関心事項である「政治情報」の窃取、中国の科学技術の発展に資する「知財情報」の窃取、中国企業をビジネス上有利にする「企業秘密」の窃取を積極的にサイバー空間で行っている。加えて、最近ではアジア地域を中心に、ロシアと同様の「情報操作型」攻撃を伴う「情報戦」を行っているとの指摘もある。

北朝鮮によるサイバー攻撃の特徴は、2015 年ごろまでは、韓国や米国に対する「機能妨害型」／「機能破壊型」サイバー攻撃であったが、直近では、経済制裁による外貨不足を補うため、「金銭目的型」のサイバー攻撃を行なっている。

イランによるサイバー攻撃の特徴は、主に米国やスンニ派の湾岸諸国に向けられた「機能破壊型」である。

表 2:サイバー攻撃の類型と懸念国

情報窃取型：	中国（技術、政策情報）、ロシア（政策情報）
機能妨害型：	ロシア、北朝鮮
機能破壊型：	ロシア、北朝鮮、イラン
金銭目的型：	北朝鮮
情報操作型：	ロシア、中国
軍事的サイバー攻撃（ハイブリッド型）：	ロシア

（著者作成）

これらのサイバー懸念国のうち、日本が警戒すべき対象は、中国および北朝鮮であったが、2020 年、懸念対象にロシアが新たに加わった。

中国由来の「情報窃取型」サイバー攻撃を繰り返しているサイバー攻撃グループは、2016 年以降特に日本を対象に攻勢を強めていると分析[6]されており、少なくとも 10 以上の中国関連の攻撃グループが日本を攻撃していると指摘されている。特に防衛、航空・宇宙、ハイテク、

[5] US Department of Defense, “Department of Defense Cyber Strategy 2018 Summary”, Sep. 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[6] FireEye, “APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat”, April 6, 2017. https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html .

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

医薬など先端産業の知財や企業秘密が狙われており、攻撃は 2021 年も継続して行われると予想される。

また、仮想通貨取引所をターゲットとしたサイバー攻撃が日本でも相次いで発覚しており、北朝鮮の「金銭目的型」サイバー攻撃には警戒する必要がある。

さらに、2020 年秋、ロシアが五輪東京大会を標的として「機能妨害型」ないし「機能破壊型」の攻撃を行っていることが明らかになった。後ほどロシアの攻撃については詳述するが、ロシアは高度なサイバー攻撃能力を備えており、東京大会を控え、警戒を強める必要がある。

国家が関与するサイバー脅威の回顧と展望

次に、2020 年の内外のサイバー脅威の回顧を踏まえ、2021 年のサイバー攻撃の脅威をいくつか展望してみたい。

① 新型コロナワクチン開発の情報窃取を狙うサイバー攻撃の増加

COVID-19 の世界的な流行に伴い、欧米をはじめ中露でも新型コロナのワクチン開発が急ピッチで進められている。これらのワクチン開発の情報を狙って、欧米の医薬品メーカーや医療政策を担う当局への情報窃取型のサイバー攻撃が 2020 年は相次いだ。これらの攻撃は、ロシア、中国、北朝鮮によるものとの指摘がなされている[7]。

20 年 7 月 7 日、米国ＦＢＩのレイ長官は、ＦＢＩが捜査中の事案 5000 件のほとんどが中国に関係している、と明らかにした。特に、新型コロナウィルスの研究をしている製薬会社や研究機関に対して、サイバー攻撃が行われている、と指摘している[8]。

7 月 21 日、米国司法省は、記者会見を行い、世界中の企業などを標的にして、知的財産及びビジネス秘密を十年以上にわたりサイバー窃取していたとして、中国国家安全部に関係する二人の中国人、李啸宇(LI Xiaoyu)および董家志(DONG Jiazhi)、を訴追した、と発表した[9]。この中国人ハッカーは、2009 年から 2020 年までの十年以上にわたり、軍事衛星、軍事通信、高出力レーザー、対化学戦兵器などの技術に関する秘密を米国の軍事産業から窃取していたが、直近では新型コロナウィルスのワクチンの開発で先行するモデルナ社に対して情報

---

[7] 米国 CISA Chris Krebs 前長官の CBS news でのインタビュー。CBS News, Transcript: Chris Krebs on "Face the Nation," December 6, 2020. https://www.cbsnews.com/news/transcript-chris-krebs-on-face-the-nation-december-6-2020/.

[8] レイ FBI 長官のハドソン研究所におけるスピーチ。Remarks by Christopher Wray at Hudson Institute, “The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States”, July 7, 2020. https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

[9] US Department of Justice, “Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research”, July 21, 2020. https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion.

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

窃取型サイバー攻撃を行なっていた。

同じ 7 月、英国政府はロシアの情報機関のサイバー攻撃グループ A P T29 が、新型コロナウィルスのワクチン開発の情報収集のために、サイバー攻撃を行っていると非難した[10]。

11 月には、新型コロナワクチン開発を手掛けている英国のアストラゼネカ社に標的型サイバー攻撃が行われたとロイター通信が報道している。侵入の手口は標的型攻撃で、ヘッドハンティングを装って、マルウェアが含まれた求職情報がアストラゼネカ社の社員に送付されていた。攻撃の手口から、北朝鮮が関与していると分析されている[11]。

2020 年 12 月には、EU の欧州医薬品庁（EMA）が、サイバー攻撃を受けたと発表した[12]。EMA では、米国 Pfizer 社とドイツの BioNTech 社が共同で開発する新型コロナウィルスワクチンの審査中で、両社は自社のコロナワクチンに関する情報が不正にアクセスされたと発表している[13]。

米国でも 12 月、IBM と国土安全保障省が、米国内のワクチン供給に関わる組織を標的とした攻撃が行われている、と警告した[14]。IBM によれば、攻撃者は、米国以外に、ドイツ、イタリア、韓国、台湾、韓国などのワクチン供給団体にも攻撃を行っており、国家が関与する攻撃と指摘されている。

米国と英国では、20 年 12 月から新型コロナワクチンの接種が始まったが、ワクチンの有効性に関わる研究や副反応などワクチンの安全性に関わる科学的調査はこれから本格化する。日本でも 2021 年にはワクチンの接種が本格化するが、それに伴って、有効性や安全性に関わる研究調査の情報が、サイバー攻撃によって狙われる危険性がある。

② 金銭を狙う身代金要求（ランサムウェア）型サイバー攻撃の流行

身代金要求型のサイバー攻撃は、2019 年ごろから攻撃手口が大幅に変化し、それに伴って被害が大きくなっている。I P A の分析[15]によれば、その攻撃の手口は、①諜報機関が採用

---

[10] UK National Cyber Security Center, “Advisory: APT29 targets COVID-19 vaccine development”, July 16, 2020. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf.

[11] Jack Stubbs, “Exclusive: Suspected North Korean hackers targeted COVID vaccine maker AstraZeneca – sources”, *Reuters,* November 27, 2020. https://www.reuters.com/article/us-healthcare-coronavirus-astrazeneca-no-idUSKBN2871A2.

[12] European Medicines Agency, “Cyberattack on the European Medicines Agency”, December 9, 2020. https://www.ema.europa.eu/en/news/cyberattack-european-medicines-agency.

[13] BioNTech and Pfizer, “Statement on EMA Cyberattack”, December 9, 2020. https://pfe-pfizercom-d8-prod.s3.amazonaws.com/2020-12/Statement_on_EMA_Cyberattack.pdf?EV8kRKMugLPz4HJfLksbRNvzgLwXubxS.

[14] Claire Zaboeva and Melissa Frydrych, “IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain”, *SecurityIntelligence,* December 3, 2020. https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/?_ga=2.111133260.892692677.1613380397-1607664142.1613380397.

[15] 独立行政法人情報処理推進機構（IPA）セキュリティセンター「事業継続を脅かす新たなランサムウェア攻撃について～人手によるランサムウェア攻撃」と「二重の脅迫」～」2020 年 8 月 20 日。hhttps://www.ipa.go.jp/files/000084974.pdf。

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

していた標的型攻撃の手法を導入し、標的とした企業・組織を調べ上げた上で、当該企業・組織のネットワークに秘密裏に侵入を図る「標的型ランサム」、②暗号化したデータの復旧のための身代金に加えて、支払わなければデータを公開すると脅かす「二重脅迫」、を特徴としている。

すでに米国では、医療機関を中心に多数の被害が発生しており、一部の地方自治体では、医療サービスがストップした事例がある他、世界中で被害が広がっており、アルゼンチンでは配電事業者やインターネットプロバイダーが攻撃され、インフラサービスが止まるなどの被害が生じている。今後日本でも、身代金要求型の攻撃によって、国民生活に不可欠な企業や組織がＩＴシステムの停止に追い込まれ、重大な影響が発生する恐れが高まっている。

実際に、6 月には自動車大手のホンダが標的型手法による身代金要求型のサイバー攻撃を受け、国内外 11 工場で操業を停止した[16]。11 月には、大手ゲーム開発会社のカプコンがサイバー攻撃を受け、顧客や社員、取引先の情報など 36 万件が流出した可能性があると発表された[17]。この攻撃は身代金要求型のサイバー攻撃で、社内のコンピュータシステムのデータを暗号化して凍結し、データを復元したければ身代金を払えと要求、さらに、払わなければサイバー攻撃によって窃取した情報を外部に漏らす、と脅すものであった。この攻撃者は「Ragnar Locker」と自称する集団で、企業のＩＴシステムを請け負うマネージド・サービス・プロバイダー（ＭＳＢ）の管理ソフト経由で当該企業のネットワークに侵入の足掛かりを構築していた。

Virus Total に上がった検体を分析したセキュリティ企業[18]によると、「Ragnar Locker」が使用したマルウェアは、セキュリティ企業が解析を試みるのを防ぐコンパイルがなされており、感染したコンピュータが旧ソ連邦圏の国の所在地登録がなされている場合には、発症させないなどの作り込みがなされている。

「Ragnar Locker」の被害は、カプコン以外に複数の企業に広がっていると見られ、米国のＦＢＩは 11 月に「Ragnar Locker」に関する警告を発表した。同発表によれば、ＦＢＩが初めて「Ragnar Locker」による身代金要求型攻撃を検知したのは 20 年 4 月で、すでに、クラウドサービス、通信、建設、旅行、ソフトウェアなど複数の事業者が攻撃されたと分析している。

日本では、まだ身代金要求型の攻撃の被害は、一部企業にとどまっているとの見方が主流であるが、欧米では、医療機関や大学、地方自治体が身代金要求型攻撃の標的となり、国民生活に大きな支障が生じ始めている。カプコンの事例は、非常に嫌な前兆であり、2021 年は身代金要求型攻撃が日本国内でも流行することが想定され、これによって生じる重要インフラや国民生活に密着したサービスへの影響が懸念される。

---

[16] Joe Tidy, “Honda's global operations hit by cyber-attack”, *BBC News,* June 9, 2020. https://www.bbc.com/news/technology-52982427.

[17] 株式会社カプコン　プレスリリース「不正アクセスによる情報流出に関するお知らせとお詫び」2020 年 11 月 16 日。https://www.capcom.co.jp/ir/news/html/201116.html。

[18] 吉川孝志，菅原圭「企業名を名指しで脅迫する「Ragnar Locker」ランサムウェアの解析」三井物産セキュアディレクション 2020 年 11 月 11 日 https://www.mbsd.jp/research/20201111/ragnar-locker/。

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

③ 民主主義プロセスを狙う情報操作型サイバー攻撃への懸念

2020 年は 4 年に一度の米国大統領選挙の年であり、4 年前の 2016 年の選挙では、ロシアによる大規模な介入があったことから、世界中のセキュリティ研究者が固唾を飲んで見守った。9 月には、マイクロソフト社が、中国とロシア、イランのハッカー集団から米大統領候補者の陣営を狙うサイバー攻撃が行われたと発表[19]し、また 10 月には、ラトクリフ国家情報長官が、ロシアとイランによるサイバーでの干渉の試みが見られたとは警告を発した[20]。しかし、結果的には大規模なサイバー攻撃は見られず、大統領選挙後、米国国土安全保障省のサイバーセキュリティー・インフラセキュリティー庁（CISA）は、サイバー攻撃が全米 50 州の投票・開票に影響を与えることはなかった、と結論づけている[21]。

また、20 年 1 月に行われた台湾の総統選挙でも、当初中国からのサイバー介入が警戒されていたが、結果的に大きな混乱はなく、選挙は終了した。

しかしながら、20 年 8 月にノルウェー議会で大規模なサイバー攻撃が発生し、同国の情報機関が、サイバー攻撃がロシア軍の情報機関 GRU に所属する APT28（Fancy Bear）によって行われたと指摘している[22]ように、散発的ではあるが、2020 年も情報操作型のサイバー攻撃に関する報道がなされており、2021 年は日本では総選挙が行われる年でもあり、注意しておく必要がある。

④ 情報窃取型サイバー攻撃は高水準で継続

冒頭で紹介したサイバー攻撃グループ「Tick」による三菱電機や NEC への標的型攻撃に見られるように、日本企業が持つ知的財産や特許を狙った情報窃取型のサイバー攻撃は、2020 年中も頻発しており、2021 年も高水準で推移すると思われる。

20 年 2 月には、上記の三菱電機に加えて、神戸製鋼所と測量大手のパスコがサイバー攻撃を受けていたと防衛省が発表した[23]。三菱電機同様、防衛情報を狙った情報窃取型の攻撃と分析されている。

直近の攻撃の傾向として、日本企業の海外支店や子会社が侵入の足掛かりとされるケース

---

[19] Tom Burt, “New cyberattacks targeting U.S. elections”, Microsoft On the Issues, September 10, 2020. https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/.

[20] US DNI Press Release, “DNI JOHN RATCLIFFE’S REMARKS AT PRESS CONFERENCE ON ELECTION SECURITY”, October 22, 2020. https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2020/item/2162-dni-john-ratcliffe-s-remarks-at-press-conference-on-election-security.

[21] US CISA, “JOINT STATEMENT FROM ELECTIONS INFRASTRUCTURE GOVERNMENT COORDINATING COUNCIL & THE ELECTION INFRASTRUCTURE SECTOR COORDINATING EXECUTIVE COMMITTEES”, November 12, 2020. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election.

[22] “Norway blames Russia for cyber-attack on parliament”, *BBC News*, October 13, 2020. https://www.bbc.com/news/world-europe-54518106.

[23] 防衛省, Ibid. 2020 年 2 月 6 日。

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

が目立つ。本国のネットワークに比べて、海外支店や子会社のセキュリティは一般的にかなり甘く、にもかかわらず本国のネットワークに接続しているため、サイバー攻撃者はこのセキュリティの弱点を突いて攻撃してくる。テレワークが世界中で主流となるなかで、企業の情報システムのクラウド化も進んでおり、企業が契約するクラウドサービスをターゲットとしたサイバー攻撃も増加しつつある。20 年 5 月にＮＴＴコミュニケーションズは、同社がサイバー攻撃を受け、自衛隊の通信情報を含む顧客情報が流出したと発表した[24]が、このＮＴＴコムのケースでも、同社のクラウドサービスで使用していた海外のサーバーが攻撃の侵入口となっていた。同様の手口は、20 年 11 月三菱電機でも生じている。同社は契約するクラウドサービスが不正アクセスを受け、国内の取引先の取引口座に関する情報が流出したと発表した[25]。

2021 年の東京大会をターゲットとしたリスクの増大

2021 年に開催予定の東京大会もまた、サイバー攻撃に晒されていることが、2020 年の秋に明らかになっている。

この 10 年の五輪へのサイバー攻撃を振り返ると、2012 年ロンドン五輪では、電力システムへのサイバー攻撃が予告され、開会式直前に電力システムが手動へ切替られたが、それ以外にも大会期間中には公式 Web への悪意のある接続要求や大規模な DDoS 攻撃への対応に追われた。次の 2016 年リオデジャネイロ五輪でも、Web 配信をターゲットとした大規模な DDoS 攻撃への対処が必要になったほか、観戦者からの金銭窃取を目的としたサイバー犯罪や大会関係者の個人情報を狙ったサイバー攻撃も発生した。

2018 年冬の韓国平昌五輪では、大会運営のシステムがサイバー攻撃さらされ、その結果、開会式直前に大会運営システムが停止し、チケットの発券システムなど一部のサービスが使用不能となったとの報道がなされた。当初その手口から北朝鮮が関与する攻撃グループによる犯行が疑われたが、平昌五輪の攻撃の背後にロシアの関与があったことが、英国および米国政府によって認定されている。

2020 年 10 月 19 日、英国政府は、ロシアが 2018 年の平昌五輪をサイバー攻撃したことを初めて公式に確認し、ロシア軍の情報機関である GRU（74455 部隊/GTsDT)の攻撃者が北朝鮮や中国のハッカーを偽装（偽旗作戦）した上で、開会式をターゲットとして攻撃を行い、コンピュータとネットワークを使用不能した、と発表した[26]。

英国政府による同日の発表では、GRU が、2020 年東京大会を標的としたサイバー攻撃を実施したことも明らかにされた。英国政府の分析によれば、攻撃対象は、五輪組織委、スポン

---

[24] NTT コミュニケーションズ「当社への不正アクセスによる情報流出の可能性について」2020 年 5 月 28 日。https://www.ntt.com/content/dam/nttcom/hq/jp/about-us/press-releases/pdf/2020/0528.pdf。

[25] 三菱電機株式会社「不正アクセスによる情報流出について」2020 年 11 月 20 日。https://www.mitsubishielectric.co.jp/news/2020/1120.pdf。

[26] GOV.UK, “UK exposes series of Russian cyber attacks against Olympic and Paralympic Games”, October 19, 2020. https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games.

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

サー企業、大会運営を支える企業と多岐にわたっているとのことである。英国政府の発表を受ける形で、英国のラーブ外相は、「GRU の行為は、不誠実で見境がない。最も強い言葉で非難する」と述べている。

英国政府の発表と時を同じくして、米国司法省も、世界規模の破壊的マルウェアの拡散とサイバー空間の騒乱の容疑で、GRU の要員 6 名を訴追したと発表している[27]。司法訴追は、ピッツバーグ連邦大陪審によって行われ、GRU の 74455 部隊に所属するロシア国籍の要員 6 名を起訴したが、容疑者たちは、2015 年および 16 年のウクライナ電力システムへの攻撃、2017 年のフランス大統領選挙への攻撃、2017 年に欧州を中心に世界中に拡散した NotPetya を使用した攻撃、2018 年の平昌五輪への攻撃、2018 年の化学兵器関連機関と英国国防科学研究所への攻撃、2019 年のジョージアへの攻撃など、ロシアの戦略的利益に沿ったサイバー攻撃に関与した、とされている。

ピッツバーグ連邦陪審院の訴追状[28]は、ロシアのサイバー攻撃者の平昌五輪への攻撃の様子を詳細に記述している。それによれば、攻撃が始まったきっかけは、平昌五輪の 2 ヶ月前になされた国際オリンピック委員会による決定で、この決定で IOC は、ドーピングを理由に平昌五輪にロシアの選手団の参加を認めないとした。この決定の 2 週間後、ロシアのサイバー攻撃者は、平昌五輪委員会に IT サポートを行う企業 2 社への侵入を開始している。

攻撃の技術的手口は、訴追状の記述からある程度推察が可能である。攻撃者は公開情報を丹念に調べた上で、IT サポート企業の社員の ID およびパスワードを推定し、これらを用いて侵入の足がかりを築いた、とされている。攻撃者たちは、平昌五輪が始まる 1 ヶ月前には、五輪の IT サポートを行う企業のドメイン管理者の権限を入手し、この企業のネットワーク内の 16,000 もの PC やサーバーにおいて、内部のファイルにアクセスする権限を収集している。

その結果、攻撃者たちは、本来秘匿されているはずの五輪の運営に関わるファイルへのアクセスが可能となった。このサポート企業は、韓国の組織委員会からの委託を受け、五輪に関わる IT ネットワークを構築していたが、ロシアの攻撃者たちは、そのネットワークに関わる情報を全て取得していたと分析されている。攻撃者はネットワーク構成を把握した上で、事前に入手していたアクセス権限を用いて、五輪の運営に使われている IT ネットワークの内部に機能破壊型のマルウェア（Olympic Destroyer）を配置していったとされる。そして五輪の開会式の 2 月 9 日に、トリガーとなる最後のマルウェアのコンポーネントがアップロードされた。

五輪関係のネットワークは、開会式直後に、大会組織委員会の認証サーバーや端末などが破壊され、一時的に五輪運営に関わるシステム（出入場管理、宿泊管理、物品管理、試合日程管理など）が停止した。軍、警察、情報機関の技術者で構成された韓国の緊急対応チームの夜を徹した復旧作業によって、大規模な機能停止は防がれたものの、チケットの発券シス

---

[27] US Department of Justice, “Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace”, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[28] United States District Court Western District of Pennsylvania, October 15, 2020. https://www.justice.gov/opa/press-release/file/1328521/download.

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021

テムの停止、会場内の WIFI の停止、プレスセンターのネットワークの停止などの被害が表面化した。

ロシアの攻撃者の意図はどこにあったのだろうか。平昌五輪へのサイバー攻撃で使用されたマルウェアはデータ消去型であったこともあり、GRU の攻撃意図がオリンピックの運営の妨害にある、と英国の国家サイバーセキュリティセンター(NCSC)は分析している[29]。

ドーピング問題で国家として五輪への参加が認めらないことについて、ロシアが国の名誉の問題として憤っているであろうことは想像にかたくないが、この問題はそれだけにとどまらない。冷戦終焉後、ロシアと欧米との間には安全保障上の緊張関係があり、ＮＡＴＯとＥＵの東方拡大、ウクライナやジョージアにおける親欧米政権の成立など、ロシアは自国の安全保障が脅かされているとの認識を抱いている。そのため、ドーピング問題も欧米諸国によるロシアへの嫌がらせとの被害者意識を募らせており、自国のプライドをかけて、開催を妨害する目的で、サイバー攻撃を行っていると考えられる。残念ながら、東京大会もドーピング問題でロシアの参加が認められていない以上、ロシアの攻撃の標的となるのは避けられないと思われる。

東京大回におけるサイバーセキュリティについて、日本では、内閣官房サイバーセキュリティセンター(NISC)および大会組織委員会が中心となって、1)重要サービス事業者を対象としたリスクマネジメントの促進、2)サイバー脅威・事案情報の共有体制の整備による対処態勢の強化、を行なっている。従来の大会で問題となったような大規模な DDoS 攻撃や金銭目的のサイバー犯罪に対しては一定の対応体制が整っている。しかしながら、今回明らかになったロシアの攻撃者による五輪大会へのサイバー攻撃では、五輪のＩＴシステム構築を担う企業に執拗に攻撃を行い、五輪関連のネットワークにアクセスする正規の権限(ＩＤとパスワード)を用いて、ネットワーク内部への侵入を行なっていた。英国政府の発表では、ロシアの攻撃者は東京大会の委員会とスポンサー企業、支援企業への攻撃に着手しているとしており、すでにネットワークに侵入されている可能性が否定できない。

過去にロシアが関与したサイバー攻撃使われたマルウェアは、技術的にも完成度が高く、被害が顕在化する前に発見される可能性は低い。また、一度マルウェアが発症すると、コンピュータのデータや起動に必要なブートレコードを破壊するなどその烈度も非常に高い。2021 年の東京大会に向けて、組織委員会のみならず、関連するサポート企業は、自社と五輪関連のネットワークについて、侵入されていることを前提に、認証方法の変更やシステム内部の振る舞い検知など、サイバーセキュリティを点検し直す必要があろう。

[29] UK NCSC, “UK and partners condemn GRU cyber attacks against Olympic and Paralympic Games”, October 19, 2020. https://www.ncsc.gov.uk/news/uk-and-partners-condemn-gru-cyber-attacks-against-olympic-an-paralympic-games.

本稿での考えや意見は著者個人のもので、所属する団体のものではありません
© Nakasone Peace Institute 2021