22

日本のサイバーセキュリティ政策

松原 実穂子

はじめに

本稿では、日本がサイバーセキュリティに取り組むきっかけとなった2000年のサイバー攻撃被害事件から、2022年のロシアによるウクライナへの軍事侵攻や2023年夏までのランサムウェア攻撃に関連した脅威動向までを対象とする。脅威環境が変化する中、日本がどのような政策や国際協力を進めてきたのか、また今後どのような政策が求められるのかを考察したい。

これまでの経緯

日本政府がサイバーセキュリティに取り組む大きなきっかけとなったのが、2000年1月に発生した科学技術庁や総務省などの官公庁のウェブサイト改ざん事件だ。情報技術（IT）化が進む中、セキュリティ対策とそのための政策作りが急務となり、翌月末の「内閣官房情報セキュリティ対策推進室」（2005年に「内閣官房情報セキュリティセンター」に改組）の設置に繋がった。その後、2011年9月に三菱重工業、IHI、川崎重工業へのサイバー攻撃が相次いで発覚し、サイバーセキュリティへの関心が国内でさらに強まった。

そうした中、2013年9月に東京が2020年の夏季オリンピック・パラリンピックの開催地に選ばれた。世界の注目を集める五輪大会は、これまでにもサイバー攻撃の標的となってきた。五輪大会の成功には、物理空間とサイバー空間双方のセキュリティが不可欠であり、日本でサイバーセキュリティ強化の機運が高まった。日本政府は、2014年11月に成立したサイバーセキュリティ基本法に基づいて内閣官房情報セキュリティセンターを改組し、「内閣サイバーセキュリティセンター（NISC）」を設置した。NISCが担う主な役割は、日本のサイバーセキュリティ政策に関する基本戦略の立案と各省庁との連携、国際連携の窓口機能、重要インフラ防御のための官民連携、サイバー攻撃に関する最新情報の収集などである。その他にも、サイバーセキュリティ政策を担当する中央官庁には、外務省（サイバー外交）、防衛省（安全保障）、警察庁（サイバー犯罪）、総務省（情報通信）、経済産業省（産業全般）、デジタル庁（デジタルトランスフォーメーション）がある。

また、サイバー攻撃は、その被害がサプライチェーンを通じ、業種や国境を越えて広がることもあり得るため、サイバー攻撃の手口や対策に関する情報共有および人材育成支援における国際協力が重要だ。日本の場合、イスラエル、インド、ウクライナ、英国、エストニア、豪州、ドイツ、フランス、米国それぞれとの二国間サイバー協議のほか、欧州連合（EU）などとの多国間協力にも力を入れている。

日本企業が多数進出している東南アジアにおいても安全なビジネス環境の確保は不可欠であり、東南アジア諸国連合（ASEAN）との協力も進められてきた。2009年から政府の局長・審議官クラスを招いた「日・ASEAN情報セキュリティ政策会議」（現「日・ASEANサイバーセキュリティ政策会議」）が年次開催され、重要インフラ防護などについて議論が行われている。2018年には、総務省がタイ・バンコクに「日ASEANサイバーセキュリティ能力構築センター」を設立した。

さらに、2016年5月に行われたG7伊勢志摩サミットでは、主催国である日本が成果文書の一つとして「サイバーに関するG7の原則と行動」を発出し、G7はサイバーセキュリティに関する協力を強化していくことで一致した。加えて、「日米豪印戦略対話（QUAD）」でも、サイバーセキュリティ協力が盛り込まれている。

現状および課題

新型コロナウイルス感染症拡大の中で開催された東京2020オリンピック・パラリンピック大会は、2021年9月に無事終了した。大会運営に関わるシステムやネットワークが2012年のロンドン五輪の倍にあたる4.5億回ものサイバー攻撃にさらされたにもかかわらず、大会運営に影響を及ぼすような被害には至らなかった。これは五輪のサイバー防御史上の快挙である。米メリービル大学のブライアン・ガント助教（サイバーセキュリティが専門）は、東京2020のサイバーセキュリティは、全てのイベントの開催者が手本とすべき模範であると絶賛している。

また、パンデミック中のサプライチェーンに関する課題を受け、日本では2022年5月に経済安全保障推進法が成立した。同法の柱である重要物資の安定的な供給の確保、基幹インフラ役務の安定的な提供の確保、先端的な重要技術の開発支援のいずれも、サイバーセキュリティ無くしては成立しない。そのため、同法は日本のサイバーセキュリティ強化にとって重要な意味を持つ。

さらに、2021年9月に日本政府が出した「サイバーセキュリティ戦略」では、サイバー攻撃への抑止力を高めるため、「政治・経済・技術・法律・外交その他の取り得る全ての有効な手段と能力を活用し、断固たる対応をとる」ことが盛り込まれた。これは、翌2022年12月に出された国家安全保障戦略への導入で注目された「能動的サイバー防御」の先鞭とも言うべき表現である。能動的サイバー防御によって、武力攻撃に至らないサイバー攻撃であっても、「国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合」、防衛省・自衛隊を含む日本政府が未然排除や被害の拡大防止のための措置を取れるようになる。

それは、「武力攻撃に至らない」サイバー攻撃でも大きな被害を出し得るからだ。2021年5月の米コロニアル・パイプライン社へのランサムウェア攻撃は、金銭目的のサイバー犯罪が重要インフラ企業1社のみに対して行われたとしても、サプライチェーンを通じて被害が拡大し、国家安全保障上の危機に繋がり得ることを証明した。日本においても、2023年7月の名古屋港へのランサムウェア攻撃では、貨物の積み下ろし作業が約2日間中断し、自動車業界やアパレル業界などの業務に多大な影響を及ぼした。だからこそ、「能動的サイバー防御」を実現し、官民が連携して重要インフラを守れるようにすることが一層重要である。

おわりに

2022年2月に始まったロシアによるウクライナへの軍事侵攻では、妨害型および諜報目的のサイバー攻撃がウクライナに対して続いている。戦争が長期化する中、日本を含む支援国はウクライナへの軍事・

人道支援を妨害するためのサイバー攻撃についても、注意を払う必要がある。

現在、ITなくしては経済も安全保障も成り立たない。サイバーセキュリティは経済安全保障と国家安全保障の要である。しかも、サプライチェーンを通じて国境を越えたサイバー攻撃被害が拡大し得るからこそ、国内外の官民連携が欠かせない。今こそ日本は一丸となって、重要インフラの防御と情報共有の拡大に取り組まなければならない。

参考文献

日本電信電話株式会社（2021）「東京2020オリンピック・パラリンピック競技大会におけるNTTの貢献～通信サービスwith サイバーセキュリティの観点から～」、https://group.ntt/jp/newsrelease/2021/10/21/211021a.html

Brian Gant (2021), “The Tokyo Olympics are a cybersecurity success story,” *Security Magazine*, https://www.securitymagazine.com/articles/95880-the-tokyo-olympics-are-a-cybersecurity-success-story

Microsoft Threat Intelligence (2022), “New “Prestige” ransomware impacts organizations in Ukraine and Poland,” https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/

Tonya Riley (2022), “Iranian hackers planned attack on Boston Children’s Hospital last summer, FBI director says,” *CyberScoop*, https://cyberscoop.com/iran-hospital-wray-fbi-boston-children/

松原 実穂子（まつばら・みほこ）
NTTチーフ・サイバーセキュリティ・ストラテジスト

早稲田大学卒業後、防衛省にて勤務。ジョンズ・ホプキンス大学高等国際問題研究大学院で修士号取得（フルブライト奨学生）。修了後パシフィック・フォーラムCSIS、日立システムズ、インテル、パロアルトネットワークスのアジア太平洋地域拠点における公共担当の最高セキュリティ責任者兼副社長を歴任。現在はNTTのチーフ・サイバーセキュリティ・ストラテジスト。近著に『ウクライナのサイバー戦争』（新潮社、サイバーセキュリティアワード受賞）。