サイバーセキュリティと データセキュリティの日米協力がなぜ 両国の経済安全保障に不可欠か

松原実穂子
NTT チーフ・サイバーセキュリティ・ストラテジスト

※本稿は、2022 年 11 月 5 日と 6 日に米国メリーランド州アナポリスで開催された NEXT アライアンス会議のワークショップで筆者が行った発表に基づくものである。

1. はじめに：なぜサイバーセキュリティは経済安全保障に不可欠なのか

世界中でデジタル化が進む中、企業や政府の活動をサイバー妨害工作から守り、知的財産をサイバースパイ活動から保護する上で、サイバーセキュリティはますます重要な役割を担っている。情報技術（IT）資産の数は増え続けており、組織が所有する全てのシステムを悪意ある行為から守ることは一層困難になってきてしまった。

だからこそ、サプライチェーンのリスク管理を十分に行うには、サイバーセキュリティとインシデント対応計画が不可欠である。例えば、2021 年 5 月にランサムウェア攻撃被害を受けた米国のコロニアル・パイプライン社 [1]では、5 日もの間、燃料供給を停止せざるを得なくなってしまった [2]。

[1] コロニアル・パイプライン社は、米国東海岸の燃料の 45 パーセントを供給している。参考：David E. Sanger, Clifford Krauss, and Nicole Perlroth, “Cyberattack Forces a Shutdown of a Top U.S. Pipeline,” *The New York Times*, May 8, 2021, https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html.

[2] Derek Brower and Myles McCormick, “Colonial pipeline resumes operations following ransomware attack,” *The Financial Times*, May 13, 2021, https://www.ft.com/content/b6ac99ea-d7c6-49dd-b7d7-1284ce2e85c0.

この事件によって、金銭的動機で行われたサイバー犯罪であっても、重要なサプライヤー１社が攻撃されるだけで、そのサプライチェーンに繋がる全ての企業に影響が及び、経済安全保障や国家安全保障上の危機を引き起こす危険性があることが浮き彫りになった。

コロニアル・パイプライン社の不十分なサイバー防御により、グローバル・サプライチェーンを通じて他の業種や取引先にも被害が及んだ。例えば、燃料不足のせいで補給地が減ったアメリカン航空は、航路の変更を余儀なくされた[3]。さらに、全米で数千箇所ものガソリンスタンドがガソリン不足に陥り、ガソリン価格が高騰している[4]。

本件を受け、日米両政府は、サイバーセキュリティが経済安全保障に不可欠であると公言している。バイデン政権は、コロニアル・パイプライン社が攻撃された直後の 2021 年 5 月中旬に「サイバーインシデントの予防、検知、評価、復旧は国家安全保障と経済安全保障にとって最優先事項且つ不可欠である」と宣言した[5]。日本の高市早苗経済安全保障担当大臣は、2022 年 10 月、「サイバーセキュリティ政策と経済安全保障の一体的な確保に向けた取り組みを進めていく」との日本政府のコミットメントを表明した[6]。

2. 破壊や混乱を招くサイバー攻撃のリスク

経済安全保障に対する主なサイバー脅威には、サイバースパイ活動、公共・民間の重要インフラの混乱や破壊がある。国家の支援を受けた攻撃者やサイバー犯罪者が情報や知的財産を盗むサイバースパイ行為によって、被害者である企業は市場競争力を失い、ブランドや評判が低下してしまいかねない。ランサムウェアや「ワイパー」攻撃は、重要データの暗号化や、IT システムからの重要データの消去によって、被害組織の事業を停止させてしまう。また、ランサムウェアの犯罪者は、不正に得た身代金を次の被害者を狙うための資金に充てている。

2017 年に発生した大事件を受け、ロシアがウクライナだけでなくその支援国に対しても、重要インフラ企業の業務を妨害するようなサイバー攻撃を仕掛けることが懸念されている[7]。2017 年 6 月に「ノットペトヤ」と呼ばれるワイパーを使ったサイバー攻撃がまずウクライナを襲い、その後、被

---

[3] Emma Korynta, “Colonial Pipeline hack impacting some long-haul flights,” *WCNC Charlotte*, updated May 11, 2021, https://www.wcnc.com/article/travel/colonial-pipeline-hack-long-haul-flights/275-6f0b116c-3b54-4975-bd6b-63f2a787f1c5.

[4] Clifford Krauss, Niraj Chokshi, and David E. Sanger, “Gas Pipeline Hack Leads to Panic Buying in the Southeast,” *The New York Times*, May 12, 2021, https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html.

[5] White House, “Executive Order on Improving the Nation’s Cybersecurity,” May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[6] 日本経済新聞「高市経済安保相『サイバー政策と経済安保、一体で確保』」2022 年 10 月 3 日（https://www.nikkei.com/article/DGXZQOUC204I20Q2A920C2000000/）。

[7] Michael Hill, “UK organizations, Ukraine's allies warned of potential "massive" cyberattacks by Russia,” *CSO*, September 28, 2022, https://www.csoonline.com/article/3674871/ncsc-chief-warns-uk-organizations-ukraine-s-allies-of-possible-massive-cyberattacks-by-russia.html.

害がドイツや米国を含む少なくとも 65 カ国に及んだ[8]。推定被害総額は、全世界で 100 億ドル以上に上っている[9]。実際、2022 年 2 月にロシアがウクライナに軍事侵攻して以来、少なくとも 7 種類の新しいワイパーが使用されてきた[10]。さらに、2022 年 10 月には、ロシアからウクライナとポーランドの物流・輸送業界に対し、ランサムウェア攻撃が仕掛けられた[11]。マイクロソフトによると、ウクライナに軍事援助や非軍事援助を提供する国や企業を妨害するためのロシアのサイバー攻撃の前兆である可能性があるという[12]。

ワイパー攻撃以外にも、経済活動やイノベーションを阻害するランサムウェア攻撃のリスクも大きい。2022 年第 2 四半期では、ランサムウェア攻撃による平均的なダウンタイムは 24 日間であった[13]。金銭的な被害も深刻である。セキュリティ企業「サイバーリーズン」が最近行った調査では、ランサムウェア攻撃で損失を被ったと回答した組織の 67 パーセントが、損失の合計が 100 万ドルから 1000 万ドルに及んだと明らかにしている[14]。プルーフポイント社による別の調査では、2021 年に 72 パーセントもの米国の組織がランサムウェアに感染し、そのうち 64 パーセントが身代金を支払っていた。日本の組織では 50 パーセントがランサムウェアに感染し、20 パーセントが身代金を支払った[15]。

もう一つ懸念すべきは、グローバル・サプライチェーンを支える上で重要な役割を担う中小企業がランサムウェア攻撃を頻繁に受けている点だ。米国のアレハンドロ・マヨルカス国土安全保障長官は、2021 年 5 月、経営層向けの講演で、ランサムウェア攻撃の被害組織の 50～70 パーセントが中小企業であると警告した[16]。この傾向は日本でも見られる。2021 年、日本企業は他国の企業よりも

---

[8] *NPR*, "'Petya' Ransomware Hits At Least 65 Countries; Microsoft Traces It To Tax Software," June 28, 2017, https://www.npr.org/sections/thetwo-way/2017/06/28/534679950/petya-ransomware-hits-at-least-65-countries-microsoft-traces-it-to-tax-software.

[9] FBI Director Christopher Wray, "FBI Partnering with the Private Sector to Counter the Cyber Threat," Federal Bureau of Investigation, March 22, 2022, https://www.fbi.gov/news/speeches/fbi-partnering-with-private-sector-to-counter-the-cyber-threat-032222.

[10] Kevin Poireault, "NSA Cybersecurity Director's Six Takeaways From the War in Ukraine," *Infosecurity Magazine*, October 19, 2022, https://www.infosecurity-magazine.com/news/nsa-6-takeaways-war-ukraine/.

[11] Microsoft Security Threat Intelligence, "New "Prestige" ransomware impacts organizations in Ukraine and Poland," October 14, 2022, https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.

[12] Clint Watts, "Preparing for a Russian cyber offensive against Ukraine this winter," Microsoft, December 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/.

[13] Coveware, "Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022," July 28, 2022, https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022.

[14] Cybereason, "Ransomware: The True Cost to Business 2022," June 2022, https://www.cybereason.com/ransomware-the-true-cost-to-business-2022, p.8.

[15] プルーフポイント「プルーフポイント、フィッシング攻撃の現状を明らかにした年次レポート『2022 State of the Phish』を発表」2022 年 4 月 11 日（https://www.proofpoint.com/jp/newsroom/press-releases/proofpoints-2022-state-phish-report-reveals-email-based-attacks-dominated）。

[16] Doug Olenick, "DHS Secretary: Small Businesses Hard-Hit by Ransomware," BankInfoSecurity, *BankInfoSecurity,* May 6, 2021, https://www.bankinfosecurity.com/dhs-secretary-small-businesses-hard-hit-by-ransomware-a-16529.

ランサムウェア攻撃への防御に成功したが、警察庁によると、2022 年上半期の被害組織の 52 パーセントが中小企業であった [17]。

3. サイバーによる知的財産窃盗のリスク

サイバーによる経済スパイ活動は気付かれにくく、ランサムウェア攻撃よりもはるかに発見が困難な場合もある上、知的財産の窃取によって、市場競争力の喪失や倒産にも至りかねない [18]。知的財産を狙ったサイバースパイ活動の阻止を米国政府が繰り返し呼びかけてきたのはそのためである。バラク・オバマ大統領は、2015 年 9 月の習近平国家主席との首脳会談後、米中両政府が「サイバーによる知的財産の窃取の実施も意図的な支援もしない」旨合意したと発表した [19]。

残念ながら、現在でも本合意は満たされていない。2019 年 10 月に米国家防諜安全保障センターのウィリアム・エバニナ長官（当時）は、サイバーによる経済スパイ活動のせいで、米国経済が年間約 4000 億ドルの損失を被っていると述べた [20]。

さらに、ロシアによるウクライナ侵攻に端を発した地政学的な動きを受け、サイバーによる知財窃取のリスクが高まっている可能性がある。制裁が長引く中、ロシアは輸入できなくなった海外の技術の代わりに知的財産情報を狙う恐れがあるためだ。実際、ロシア産業貿易省は、同国が外国の技術や工場に依存していると 2022 年 9 月に認めている [21]。

プーチン大統領は、2022 年 6 月にロシア対外情報庁（SVR）で演説した際、制裁が課せられている間は特に、ロシアの産業・技術開発への支援が同庁の優先事項の一つであると強調した。この発言を受け、サイバーセキュリティの専門家らは、今後のリスクについて警戒を強めている [22]。

フィンランドの安全保障情報庁 SUPO）も同様の懸念を抱いている。SUPO は 2022 年 9 月、ロシアによるサイバー経済スパイ活動の脅威拡大について警告し、データセキュリティの強化を産業界

---

[17] 警察庁「令和 4 年上半期におけるサイバー空間をめぐる脅威の情勢等について」2022 年 9 月 15 日（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_kami_cyber_jousei.pdf）、p. 2-3。

[18] European Commission and PwC, “Study on the Scale and Impact of Industrial Espionage and Theft of Trade Secrets through Cyber,” December 2018, https://op.europa.eu/en/publication-detail/-/publication/4eae21b2-4547-11e9-a8ed-01aa75ed71a1/language-en, p. 28.

[19] The White House, “Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference,” September 25, 2015, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

[20] Vice, "The Economic Toll of China’s Cyber Espionage,” July 27, 2016, https://video.vice.com/en_us/video/the-economic-toll-of-chinas-cyber-espionage-scene/579780624bfe8ab01eafb1ec.

[21] *Kommersant*, “*Электронику начнут с чистого нуля* [Electronics starts from scratch],” September 13, 2022, https://www.kommersant.ru/doc/5558844.

[22] Kremlin, “*Владимир Путин поздравил сотрудников и ветеранов СВР со столетием нелегальной разведки* [Vladimir Putin congratulated employees and veterans of the Foreign Intelligence Service on the centenary of illegal intelligence],” June 30, 2022, http://kremlin.ru/events/president/news/68790, and Alexander Martin, “Fears grow of Russian spies turning to industrial espionage,” *The Record by Recorded Future*, September 14, 2022, https://therecord.media/fears-grow-of-russian-spies-turning-to-industrial-espionage/.

に促した。また、「2022 年国家安全保障概要」の中で、「ロシアは最先端技術を代替的に製造し始めなければならないと感じている」旨指摘した[23]。

4. 第一の政策提言：サイバー脅威に関する情報の共有

上記のサイバー脅威の現状を踏まえ、本稿では、日米両国政府に対し、相互警告メカニズムの構築と合同サイバー演習の実施という 2 点の政策提言を行いたい。第一に、両国は、相互警告メカニズムを確立することで、サイバー脅威に関する機密情報と非機密情報の共有、官民双方へのタイムリーな警告提供を可能にし、組織が強固な防御と強靭性のための措置を講じることができるようにすべきである。

エネルギー省、国土安全保障省、財務省などの米国政府機関は、少なくとも 2021 年秋以降、重要インフラ企業に対する機密と非機密両方のブリーフィングを行ってきた[24]。しかし、機密指定のサイバー脅威情報にアクセスできるのはセキュリティ・クリアランス保有者だけであるため、たとえ熟練したスキルを持っていても、機密指定の警告に基づく重要なサイバー防衛の取り組みに参加できないエンジニアが出てくる可能性がある。

エネルギーや金融等の国際重要インフラ企業では、様々な国籍の社員が働いている。サイバーセキュリティ担当者の中には、米国や日本のセキュリティ・クリアランスを持っていない社員もいるだろう。だからこそ、情報の過度な機密指定を避け、数カ月も何年も時間をかけるのではなく、迅速に手段や情報源に関する情報を機密指定のサイバー脅威情報から削除する、そうした機密指定解除作業を可能にすることが極めて重要である。そうすることは、企業の経営層や現場の担当者が、知的財産をサイバースパイ行為から防御し、重要インフラやサプライチェーンを妨害行為から守るための戦略的・戦術的な決定を下しやすくなるだろう。

それでも、情報の機微性によっては、機密指定にせざるを得ない。重要インフラ企業向けであっても、機密指定のサイバー脅威レポートやブリーフィングでしか伝えられない背景情報もあり、それを見られれば、適切な対策を決められることもあるからだ[25]。

---

[23] SUPO, “National Security Overview 2022,” https://supo.fi/en/national-security-overview, and “Foreign intelligence and influence operations,” https://supo.fi/en/intelligence-and-influence-operations, and “National Security Overview: Russian intelligence changes approach,” September 29, 2022, https://supo.fi/en/-/national-security-overview-russian-intelligence-changes-approach.

[24] The White House, “Press Briefing by Press Secretary Jen Psaki and Deputy NSA for Cyber and Emerging Technologies Anne Neuberger, March 21, 2022,” March 21, 2022, https://www.whitehouse.gov/briefing-room/press-briefings/2022/03/21/press-briefing-by-press-secretary-jen-psaki-and-deputy-nsa-for-cyber-and-emerging-technologies-anne-neuberger-march-21-2022/.

[25] Kevin Poireault, “NSA Cybersecurity Director's Six Takeaways From the War in Ukraine,” *Infosecurity Magazine*, October 19, 2022, https://www.infosecurity-magazine.com/news/nsa-6-takeaways-war-ukraine/.

そのため、日本では、セキュリティ・クリアランス制度を中央省庁の職員や防衛関連企業だけでなく、「その情報を知るべきかどうか（need to know）」と「共有すべきかどうか（need to share）」の原則に基づき、その他の業界関係者にも拡大する必要があると指摘する人々もいる[26]。日本の経済安全保障推進法[27]は今のところ、セキュリティ・クリアランスを扱っていないが、その必要性があることは日本政府も承知している[28]。

日本が強固なセキュリティ・クリアランス制度を確立すれば、米国だけでなく、他の同志国とも機密情報を共有しやすくなるであろう。日本のサプライチェーンが日米以外の国々にも広がっていることを考えると、これは重要なことだ。「クアッド」に参加する日米豪印の首脳は、2022 年 5 月、「政府間及び産業界のパートナーとの間で脅威情報を迅速かつ時宜を得た形で共有」することを目的とした「日米豪印サイバーセキュリティ・パートナーシップ」の開始を合意した[29]。国境を越えて機密情報を共有するには、データセキュリティ対策として、ポスト量子暗号を含む強力な暗号化も必要になるだろう。

5. 第二の政策提言：合同サイバー演習

第二に、日米両国は、政府と重要インフラ企業の関係者を招いて、サイバー演習を実施すべきである。サプライチェーンが攻撃され、複数の重要インフラ業種に混乱が生じた際の対応能力を試すためだ。電力、エネルギー、医療サービス、通信、輸送等の重要インフラ業種は、相互依存関係にある業種にも影響する可能性がある。サプライチェーンへの攻撃によって、2021 年 5 月のコロニアル・パイプラインへのランサムウェア攻撃と同様、国や地域全体にまで連鎖的に影響を及ぼす可能性がある。新たな国家安全保障戦略では、自衛隊の重要インフラ企業に対する情報共有やインシデント対応などの支援が盛り込まれているため[30]、合同サイバー演習が今後必要になってくるであろう。

---

[26] 柿沼 重志「技術流出防止策としてのセキュリティ・クリアランス　～経済安全保障推進法の改正による制度導入に向けて～」『経済のプリズム』217（2022 年 10 月）号、（https://www.sangiin.go.jp/japanese/annai/chousa/keizai_prism/backnumber/r04pdf/202221701.pdf）、p. 1-2。

[27] 経済安全保障推進法の全文はこちら：https://elaws.e-gov.go.jp/document?lawid=504AC0000000043_20230517_000000000000000.

[28] Kyodo News, “Japan's economic security law takes effect amid regional tensions,” August 1, 2022, https://english.kyodonews.net/news/2022/08/18a4fe0f5512-japans-economic-security-law-takes-effect-amid-regional-tensions.html と内閣官房経済安全保障法制準備室「経済安全保障推進法の審議・今後の課題等について」2022 年 7 月 25 日（https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r4_dai1/siryou3.pdf）、p. 2, 5。

[29] 外務省「日米豪印サイバーセキュリティ・パートナーシップ：共同原則」2022 年 5 月 24 日（https://www.mofa.go.jp/mofaj/files/100347973.pdf）、p. 1。

[30] 防衛省「国家安全保障戦略について」2022 年 12 月、https://www.mod.go.jp/j/approach/agenda/guideline/pdf/security_strategy.pdf, p. 22.

日本政府は、官民合同演習を 2 つ行っている。内閣サイバーセキュリティセンター（NISC）は、2006 年から毎年、省庁や重要インフラ企業を招いて合同サイバー演習を開催してきた [31]。最新の 2022 年 12 月の演習では、約 5500 人を招き、ランサムウェア攻撃への対応をシミュレーションした [32]。だが、これまでの演習に防衛省や自衛隊が参加したことはない。同演習が対象としている 14 の重要インフラ業種には防衛が含まれていないためと思われる [33]。

しかし、自衛隊は、エネルギーなど民間の重要インフラに大きく依存しているため、経済安全保障の危機が国家安全保障の危機に発展する可能性もある。重要インフラ企業が操業停止すれば、軍事作戦に悪影響を及ぼし、国家安全保障の能力も低下しかねない。日本政府と産業界は、サイバー演習に防衛省と自衛隊も入れた方が助けとなるであろう。そうすれば、防衛省・自衛隊も他省庁や重要インフラ企業との連絡体制、危機発生時の支援について学べるからだ。

ただ興味深いことに、防衛省・自衛隊は、世界的なサイバー演習「ロックド・シールズ」に日本の他省庁や重要インフラ企業と共にこれまで 2 回参加している。エストニアのタリンにある北大西洋条約機構サイバー防衛協力センター（NATO CCDCOE）は、2010 年から毎年、この合同サイバー演習を開催してきた。様々な重要インフラ業種に混乱をきたす数千回ものサイバー攻撃と並行して偽情報も拡散される中、同志国が如何に対応するかをシミュレーションする。この演習では、戦略的・戦術的意思決定力、技術的なサイバー防御力、法律の理解、コミュニケーションや報告の能力、国際的な官民協力が試される [34]。2022 年 4 月には、32 カ国から 2000 人以上が参加した [35]。

ロックド・シールズでは 2 カ国でチームを組む必要があり、防衛省・自衛隊は、2021 年には米インド太平洋軍、2022 年には英国防省・軍と組んだ。米英政府のいずれも、他省庁や重要インフラ企業を招いていないが、日本は内閣サイバーセキュリティセンター等の他省庁や一部の重要インフラ企業を招待している [36]。これは、防衛省・自衛隊が、国際的な官民連携が強靭性とサプライチェーンのリスク管理のために重要であることを理解し、専門知識の国内外のパートナーとの共有に前向きであることを示している。

---

[31] 内閣サイバーセキュリティセンター「分野横断的演習について」2018 年 10 月 29 日（https://www.nisc.go.jp/pdf/council/cs/ciip/dai16/16shiryou06.pdf）、p. 1。

[32] 内閣サイバーセキュリティセンター「重要インフラ 14 分野を対象に障害対応体制の検証のためのサイバー演習を実施～2022 年度「分野横断的演習」～」 2022 年 12 月 12 日、https://www.nisc.go.jp/pdf/policy/infra/NISC_enshu_20221209.pdf

[33] 内閣サイバーセキュリティセンター「重要インフラグループ」（https://www.nisc.go.jp/policy/group/infra/index.html）、2022 年 10 月 23 日閲覧。現時点での日本の重要インフラ所管省庁は、金融庁（金融）、総務省（情報通信、地方公共団体）、厚生労働省（医療、水道）、経済産業省 （電力、ガス、化学、クレジット、石油）及び国土交通省（航空、空港、鉄道、物流）である。

[34] CCD COE, “Locked Shields,” Accessed October 24, 2022, https://ccdcoe.org/exercises/locked-shields/.

[35] CCD COE, “Over 2000 Cyber Experts from 32 nations at the Locked Shields Exercise,” Accessed October 24, 2022, https://ccdcoe.org/news/2022/over-2000-cyber-experts-from-32-nations-at-the-locked-shields-exercise/.

[36] 防衛省「ＮＡＴＯサイバー防衛協力センターによるサイバー防衛演習『ロックド・シールズ２０２１』への参加について」2021 年 4 月 13 日（https://www.mod.go.jp/j/press/news/2021/04/13b.pdf）と「ＮＡＴＯサイバー防衛協力センターによるサイバー防衛演習『ロックド・シールズ２０２２』への参加について」2022 年 4 月 19 日（https://www.mod.go.jp/j/press/news/2022/04/19e.html）。

日本は既に、重要インフラの相互依存の問題に取り組む合同演習の開催や参加の経験を積んできた。今こそ日本は、米国やクアッドなど同志国の官民関係者と共に、率先して国際的な合同サイバー演習を創設すべきである。日本の重要インフラ企業がセキュリティ・クリアランス保有者を配置するようになれば、こうしたサイバー演習が、機密指定の知見を共有する場にもなり、より幅広くサイバー防衛に役立つであろう。

6. まとめ

知的財産の窃取、ワイパーやランサムウェア攻撃によるサイバー妨害行為は、日米の経済安全保障に暗い影を落としている。産業界の強靭性を確保し、グローバル・サプライチェーンを守るには、サイバー脅威に関する情報を政府間で共有するだけでは不十分である。重要インフラ企業も含めて情報共有やサイバー演習を行うと共に、政府や民間企業が収集したサイバー脅威に関する実用的な情報に一部の社員は着実にアクセスできるようにしなければならない。

日本は、強固なサプライチェーンのリスク管理とサイバー防御のため、国内外の官民連携を深化・拡大させようとしており、経済安全保障推進法やロックド・シールズ演習などの重要な取り組みを始めている。日本は経済安全保障において正しい方向に進んでおり、今後は、米国や他の同志国と協力し、急速に変化し続けるサイバー脅威に対応するため、取り組みを加速させる必要がある。

＊松原実穂子氏は個人的な立場で本稿を執筆した。その見解および解釈は、あくまでも筆者個人のものである。

日米 NEXT 同盟イニシアティブは、日米間で外交・安全保障・技術政策分野を横断する新たな協力関係を構築するため、幅広い分野の政策・技術専門家（政府内外）を招待し、二国間対話、ネットワーキング、共同提言の策定を行うフォーラムです。日本財団の支援を受けて笹川平和財団米国が設立した本プログラムの目的は、日米共通の利益により大きく貢献し、ますます複雑でダイナミックになる地政学的環境における新たな課題に備えられるよう、日米同盟を強化することです。2021 年に設立された本イニシアチブは、重複する課題も多い二つのトピック（1）外交・安全保障政策、2）技術とイノベーションの連結）に取り組んでいます。米国笹川平和財団のシニアディレクターであるジェームズ・ショフが本イニシアチブを主導しています。
