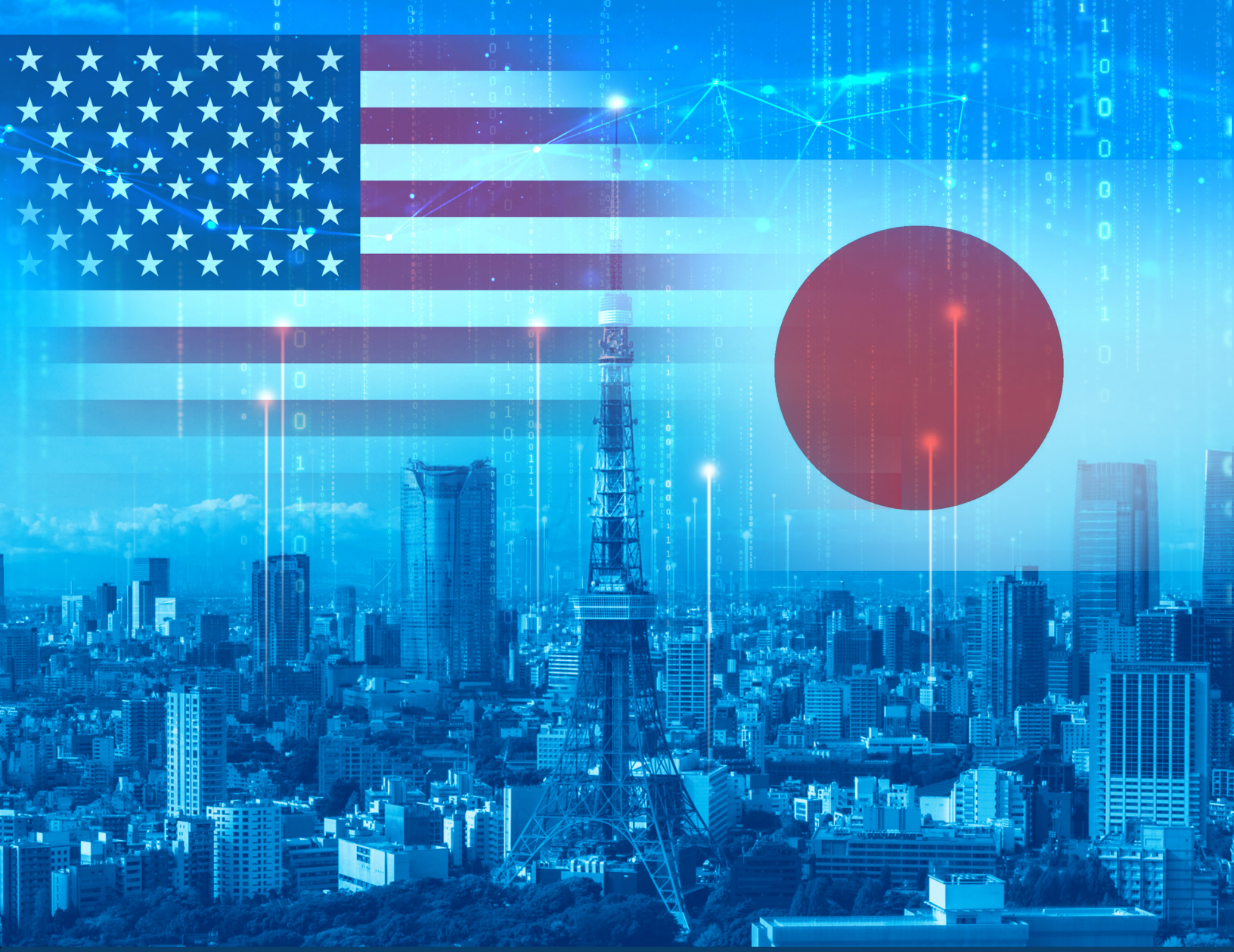

PACIFIC FORUM
INTERNATIONAL

2024年2月

不確実な時代における日米のサイバーセキュリティ推進と強靭化

編集　マーク・ブライアン・マナンタン

エミリー・ゴールドマン｜松原 実穂子｜ベンジャミン・バートレット
アンドリュー・J・ローン｜高澤 美奈

PACIFIC FORUM
INTERNATIONAL

2024年2月

不確実な時代における日米のサイバーセキュリティ推進と強靭化

編集　マーク・ブライアン・マナンタン

エミリー・ゴールドマン｜松原 実穂子｜ベンジャミン・バートレット
アンドリュー・J・ローン｜高澤 美奈

PACIFIC FORUM
INTERNATIONAL

パシフィック・フォーラムについて

パシフィック・フォーラムは、アジア太平洋地域を中心とした外交政策を専門とする研究機関です。1975年に設立され、ホノルルに拠点を置いています。環太平洋地域の幅広い研究機関と協力し、アジアの視点を取り入れながら、プロジェクトで得た知見や提言を世界各国の指導者、政府、一般市民に向けて発信しています。当フォーラムのプログラムは、政治、安全保障、経済、海事、サイバーセキュリティ、重要技術など、既存の課題や新しい課題を取り上げ、厳密な調査、分析、対話を通じて、協調政策を促進しています。

パシフィック・フォーラムは、「日米サイバーフォーラム2023」を支援してくださった在日米国大使館に感謝いたします。また、メーガン・タエナカ、ブルック・ミズノ、ジェスリン・チョン、ブラント・マブニ、ハナ・パク、ムニーク・タン、マシュー・スー、クリスティ・ゴヴェラ、ラミ・キム、クリスタル・プライア、井形彬、山口亮、羽深宏樹、ンゴー・ルオン、カール・ベイカー、デービッド・サントロに心より感謝申し上げます。

なお、本報告書にあるすべての事実、立場、見解は、執筆者個人の責任で発表するものであり、パシフィック・フォーラムやその役員、スタッフ、支援者の見解を反映するものではありません。

パシフィック・フォーラム

ウェブサイト：www.pacforum.org
フェイスブック：Pacific Forum
ツイッター：@PacificForum
インスタグラム：@pacforum
ポッドキャスト：Indo-Pacific Current
メール：pacificforum@pacforum.org

目次

エグゼクティブ・サマリー

地政学的環境がかつてないほど大きく変わり、破壊的で新しい技術が次々に登場する中、日米は、サイバーセキュリティをめぐるパートナーシップを強化している。本報告書の目的は、そのようなパートナーシップの進化を検証することである。本報告書は、パシフィック・フォーラムが2021年に開催した前回のワークショップ「日米サイバー協力：2020年東京オリンピックを超えて」を踏まえ、3つの分野（サイバー防衛、能力構築、重要技術）における両国のサイバー協力を分析している。

パシフィック・フォーラムの「サイバーセキュリティと重要技術プログラム」は、分野横断的な視点をまとめ、健全で実行可能な政策につながる洞察を提示するため、在日米国大使館と協力し、「日米サイバーフォーラム2023」を開催した。ハワイ州ホノルルで行われたこの非公開イベントでは、政府、産業界、学界の主要な専門家や代表者が集い、以下の政策課題に取り組んだ。第一に、日本における「能動的サイバー防御」の導入と米国のサイバー戦略である「継続的従事（Persistent Engagement）」に関し、どのような機会や課題があるかを見極めること。第二に、情報共有に関する政府と民間部門の信頼関係を確立すること。第三に、サイバー能力の構築において日米間で重複する分野や、両国の取り組みの補完性を評価し、最大限の効果をもたらすリソースをフルに活用すること。最後に、生成人工知能（AI）等によって現在大きく変化している状況に適応することである。

同ワークショップでは、以下の提言がなされた。

サイバー防衛と強靭性

集団的サイバー防衛を推進し強靭化を図るため、継続的従事と能動的サイバー防御の収束を図ったアプローチを構築する。武力紛争のレベルには達しない敵対的サイバー行為やサイバーを利用した行為に対し、機敏な形で協力して対応し、圧力をかけ続けるため、日米の取り組みを拡大する。

サイバー能力開発のための既存の講座等を見直し、現在のサイバー脅威の環境に対応できるように改善する。機密指定をより効果的に行えるようにサニタイジングをするなど、諜報の共有に悪影響を与える摩擦を減らす。

国家と非国家主体との間で、サイバー脅威に対処するための共通の理解とアプローチを確立する。これは、相互の利益と特定の条件下における資源の利用可能性に沿った、明確な戦略ときちんと定義された目標に基づいたものであるべきだ。

サイバー脅威に関する日米間の諜報共有を強化する。具体的には、文脈の理解に重要な機密情報や機微な情報であるものの、機密解除やサニタイズが不可能なものも処理できるように、相互運用可能なセキュリティ・クリアランス制度を創設する。

ランサムウェアに関する日米の法執行機関の協力を強化し、悪意ある行為者の責任を追求してその活動を阻止する。実用的な諜報共有を向上させ、商業部門において事業継続性が確保されドミノ効果が抑制されるよう支援する。

サイバー能力

サイバー能力構築に向けて日米が連携を強化できるよう、事務局を設置する。米国のサイバーセキュリティ・インフラストラクチャーセキュリティ庁（CISA）と日本の内閣サイバーセキュリティセンターから人材を派遣することで、官僚的な縦割りを緩和し、取り組みの内容を明確にする。

デジタル・インフラ整備支援における日米の比較優位を活用し、国際的な技術標準を推進することで、東南アジアと太平洋地域における新興経済国間の相互運用性を向上させる。

ASEAN・米国サイバー対話とASEAN・米国首脳会議を通じて、サイバー能力構築に向けた米国と東南アジアの協力を制度化する。継続的従事とハント・フォワード作戦の実施という作戦論理に沿った形で米国のサイバー外交の関与を再考する。

生成AI

生成AIに関する日米の二国間協力はこれまで安全保障に焦点を当ててきたが、それを拡大し、経済や社会といった側面を含め、幅広い分野における影響を検討する。

政策や技術の取り組みを早急に主導し、生成AIの開発ライフサイクル全体にわたって、さまざまな部門やプレイヤーが責任ある形でAIに携わるよう整備する。

広島AIプロセスを踏まえ、政策の一貫性と規制の相互運用性を引き続き重視した形で、AIに関するグローバル・ガバナンスの基礎を築く。また、これに関連して、ユネスコとOECDの基礎的枠組みを参考にして有用な洞察を得る。

既存のサイバー机上演習やシミュレーションに加え、強化学習を活用し、サイバー訓練環境に自律型サイバー防御を適用・拡大する。

生成AIの利点を防衛に活用しつつも、そのリスクと脆弱性にも留意し、実用的でバランスの取れたアプローチに努める。

序論

マーク・ブライアン・マナンタン

日本は、長年繰り返し要請されてきた、サイバー防衛の強化についに取り組んでいる。2022年12月に日本政府は、国家防衛戦略、防衛力整備計画とともに国家安全保障戦略を改定し、能動的サイバー防御を導入することを示した。このことは大きな注目を集めている。日本政府がサイバー防衛に先制的な姿勢を示しつつあることは、検証に値する様々なことを示唆している。

中国、ロシア、北朝鮮の国家主導のハッキング集団によるサイバー脅威は増大している。過去10年間、日本は、その脅威にどう立ち向かうべきかという大きなジレンマを抱えてきた。日本は能力が遅れていることから、サイバー攻撃に対応できず、しばしば厳しい世論や評価の対象となってきた。また、平和主義の憲法による制限に縛られる中で、変化する戦略環境に適した高度なサイバー戦略を進めることに苦労してきた。

日本の戦略は主に中国を中心に考えられてきたが、ロシアによるウクライナへのいわれのない侵攻により、国家安全保障戦略の改定が早まった。能動的サイバー防御に方向転換したことにより、自衛隊は、国家安全保障上の問題を引き起こす可能性のある重大なサイバー攻撃を事前に防ぐことができる。そのサイバー攻撃が武力攻撃とみなされなくても、自衛隊は、想定される被害の拡大を防がなければならない。日本の能動的サイバー防御には、情報共有やインシデント対応に関する官民連携の強化が求められる。重要なインフラを守る上でこれは特に重要

であろう。情報戦に対する日本のサイバー態勢を最新のものにしていく必要がある、という認識も高まっている。

国家安全保障戦略を通じて自衛隊のサイバー防衛力を欧米諸国と同レベルに引き上げようとしていることからも見られるように、日本の目標は、より効果的にサイバー攻撃を監視し、どこから来たのかを突き止め、対抗措置を発動させることである。日本が能動的サイバー防御に向けて動き始めたことは、今後日米がサイバーセキュリティ協力を強化できる可能性を示している。日米同盟がマルチドメイン環境における適応・運用能力を向上する上で、この変化は欠かせない。

ウクライナ戦争、そして中国との戦略的競争により、米国のサイバー脅威環境は激変している。これに対処するため、米国政府は国防総省の「2023年サイバー戦略」とバイデン政権の「国家サイバーセキュリティ戦略」という2つの重要な文書を発表した。米国の2023年サイバー戦略は、悪意ある行為を阻止・弱体化させることを目指す、「前方防衛（Defend Forward）」と継続的従事の概念に沿っている。また、これまで同様、スピード、敏捷性、行動を重視し、迅速かつ継続的な形でその「キャンペーン」を進めることに重きを置いている。同戦略は、日本のような同盟国やパートナー国のサイバー能力を高めることの重要性について述べているが、それが米国のサイバー外交とどう関わっていくのかについてはほとんど説明していない。

米国の国家サイバーセキュリティ戦略の下で、バイデン政権は、重要インフラのサイバーセキュリティ保護を保証する責任を、個人、組織、地方自治体から、主に民間部門に移した。これまでは自主規制であったが、コロニアル・パイプラインへの攻撃をはじめとするサイバー事件から学んだ教訓をもとに、同政権は、サイバーセキュリティに関する規則を義務化し始めている。つまり、民間企業は、サイバーセキュリティへの投資を増やし、経済的利益と国家安全保障上の利益の両方を優先させることが求められている。

しかし、すべての主要な戦略や政策同様、成功したかどうかの真の指標はその発表ではなく、実施にかかっている。能動的サイバー防御をはじめとする概念の運用や、国家サイバー戦略に基づく規制ガイドラインの普及・遵守には、適切な政府資源の動員やインセンティブが必要となる。政府、産業界、学界、市民社会の主要なステークホルダーから成る、信頼できるネットワークや拠点に基づく効果的な協力があってこそ成功できる。政府と民間部門の間の信頼は、官民パートナーシップの中核であり、協力と遵守を保証する基本的な要素である。

サイバーセキュリティは分野横断的な課題である。そのため、日米のサイバー政策と戦略における最近の進展が、両国のサイバー外交とどのように関係しているかを見極めることが重要である。また、中国やロシアとの地政学的な競争が激化していることから、特に情報戦における、生成AIの破壊的な影響も喫緊の課題である。

本報告書は、日米サイバー協力に関する主な最新情報だけでなく、日米同盟内外で現在議論されているサイバー政策や技術政策に役立つ情報も提供することを目指している。最大の目標は、サイバー技術と重要技術に関する日米の最近の動向をどのように運用化できるかを深く掘り下げることである。本報告書から得られる洞察は、日米サイバーセキュリティ協力を複雑にしている無数の具体的な問題をより深く理解し、それらがインド太平洋地域にどのように影響するのかを把握するのに役立つだろう。

日米サイバーフォーラム

前回行われたワークショップ「日米サイバー協力：2020年東京オリンピックを超えて」の成果を踏まえ、パシフィック・フォーラムは、在日米国大使館の支援の下、ハワイ州ホノルルで「日米サイバーフォーラム2023」を開催した。「サイバー防衛」、「サイバー外交」、「重要技術」の3つのテーマに沿って行われたこの非

公開イベントでは、専門家や実務家が一堂に会し、中国の技術的影響力の増大、インド太平洋地域における安全保障の劣化、生成AIの破壊的影響の中で、日米のサイバー戦略・政策がいかに大きく変化しているかを議論した。複数のステークホルダーがいることを踏まえ、この戦略的ワークショップは、以下の目的を掲げて行われた：

「能動的サイバー防御」や「継続的従事」といった、漠然としがちな概念を解き明かし、それらが実際何を意味するのかを具体的な形で明らかにする。

様々な能力開発の取り組みのどこに重複や補完性があるのかを特定することで、資源配分を最適化し、政策でサイバーを取り上げ続けるようにする。

民間部門から詳細な洞察を得ることで、当初から活動に参画してもらい、できれば強固な信頼を得た上で、オープンで透明性があり生産的な形で連携する。

日米サイバーセキュリティ協力における生成AIの機会と課題を評価する。

同ワークショップで得られた主な知見を次ページ以降で概説する。本報告書には、同ワークショップで話し合われたサイバーセキュリティと生成AIの重要課題をさらに詳しく分析した、5つのポリシーブリーフも含まれる。各ポリシーブリーフとも、政策立案者による検討に値する、実行可能な政策提言を提示している。

まず、エミリー・ゴールドマン博士は、米国のサイバー戦略である「継続的従事」の概念と実践を深く掘り下げている。継続的従事が何であり、何でないかを解明した上で、日本の「能動的サイバー防御」とどのように組み合わせれば、継続性を通じた日米の集団的強靭性を向上させられるかを評価している。また、運用上の整合性を測るため、能力構築の強化も推奨している。

松原実穂子氏は、ゴールドマン博士が呼びかけている集団的強靭性をさらに分析している。ランサムウェア、重要インフラ保護、サイバー脅威インテリジェンスなど、サイバーセキュリティ協力におけるニッチ分野がどのように実践され、拡大しつつあるのかについて説明する。また、ウクライナ戦争が提示している教訓をもとに、台湾有事が起きた場合にサイバー脅威インテリジェンスにおける相互運用性を向上させることの重要性を強調する。そして、日米間で相互運用可能なセキュリティ・クリアランス制度を設けることで、情報共有をさらに強化することのメリットについても解説している。

ベンジャミン・バートレット博士は、サイバー外交とサイバー防衛の概念を融合させ、サイバー外交における米国の取り組みを活性化させるための新たな視点を紹介する。これは新戦略「継続的従事」にも似ている。同博士は、サイバー外交のツールを改善しようとしている米国の政策立案者に対し、日本との協議や調整を行うよう促している。サイバー能力を構築するためのインド太平洋地域における取り組みは、日本の方が制度化されているからである。このようなアプローチは、日米両国がより効果的に資源を投入し、能力を構築するための相互補完性を培う助けとなるだろう。

アンドリュー・ローン氏は、サイバーセキュリティにおける今の生成AIブームを取り上げ、リスクの過大評価や誤った認識について、専門家や政策立案者に注意を促している。また、偽情報、マルウェア生成、ハッキングを含め、大規模言語モデルを使った活動に関して詳細な議論を展開している。AIは確かにサイバー脅威の規模と範囲を拡大するだろうが、サイバー防衛と強靭性も高めるだろう。同氏は、技術の上で日米のサイバー防衛を向上する方法として、強化学習を提案している。

高澤美奈氏は、生成AIに対する規制を分析し、AIに関するガードレールを整備することの緊急性を強調している。イノベーションがもたらす急速な変化に対し、規制は遅れがちである。そのような中、日米両国は率先して、AIのベストプラクティスを生成AI開発のライフサイクル全体に適用しなければならない。高澤

氏は、インド太平洋地域や多国間における議論の舵取りをし、AIガバナンスに関する多国間の既存の取り組みを補完することを日米両国に促している。

このワークショップで得られた重要な知見とポリシーブリーフが有益な洞察を提供し、実務的な協力を促すことができれば理想的である。日米関係は依然強固だが、両政府は今岐路に立たされている。日米の政策立案者は、地政学的な競争とグローバルな情報通信技術企業の影響力が増大する現代において、日米同盟のあるべき姿を再考することが求められている。

「自由で開かれたインド太平洋」の実現という約束を果たす圧力が高まっている。そのような中、日米両国は、限りある資源を最大限に活用し、互いの比較優位を活用するため、戦略的な形で同地域における取り組みを調整すべきである。インド太平洋、特に東南アジアにおける日本の持続的な取り組みから米国が学べることは多い。同地域で最も信頼できるパートナーだと考えられている日本は、中国の影響力と主張の高まりを緩和することができるだろう。日本は器用な外交術を使い、一貫した経済投資を行い、東南アジアで能力開発に取り組んでいる。それを受け、米国も、同地域における安全保障および経済のパートナーとして自国のイメージを再活性化するため、今後の対応を再考できるだろう。

多少の進展があったとはいえ、今こそ日米両政府は、これまでの経路から脱却すべきである。数十年にわたって同じ道を辿ってきたことは、官僚主義的な惰性ももたらしたかもしれない。強靭性を中心としたサイバー協力を行うには、サイバー防衛、サイバー外交、重要技術開発に対し、包括的でバランスの取れたアプローチが必要である。これにより、地政学的または技術的要因によって引き起こされる可能性のある体系的なリスクに対し、調整・適応する能力を強化・改善することができる。また、政策立案者は、官民の主要なステークホルダーの間の信頼関係とパートナーシップの構築に取り組むとともに、それを継続的に評価・調整しなければならない。日米両国はサイバーセキュリティ協力へのアプローチを改善し続けている。そのような中、本報告書で提示された政策提言は、明確な目標に基づいて具体的な成果を実現できるよう、日米同盟をより強靭なものにすると思われる。

主な知見

「能動的サイバー防御」と「継続的従事」の運用化

「能動的サイバー防御」や「継続的従事」の運用化には、活発な情報共有が必要である。脆弱性に付け込んだりサイバー攻撃を仕掛けたりする敵の能力を理解する上で、これは特に重要である。しかし、脅威の状況を包括的に理解するには、民間部門の賛同が必須である。それがなければうまくいかない。民間部門は、グローバルな形でデータにアクセスできるため、脅威の検知と情報共有に欠かせない存在である。

「前方防衛」は、敵を混乱、阻止、または抑制することを意味する。その根底にあるのは、自らの防御を続けることは戦略的損失に等しいという考えである。サイバー空間における戦略的損失は累積され、長期にわたれば、物理的な通常戦争における損失と同程度の被害につながる可能性がある。したがって、攻撃された後のインシデント対応に加え、敵の行動を積極的に暴き、それに対抗することも、サイバー空間を通じて安全を確保するための総合的なアプローチの一部でなければならない。

「継続的従事」の規模と範囲に関する法的な問題は未解決である。民間部門においては特にそうであろう。米国政府は、サイバー攻撃を特定の事件ではなく、長期にわたって累積する損害をもたらす、悪意ある継続的な活動パターンとして捉えるべきである。今起きている被害や危険を示す明確な事例があれば、政府は動くことができるが、常に国際法に従わなければならない。

同様に、日本は平和主義憲法が通信の機密性とプライバシー保護を保証しているため、「能動的サイバー防御」は法的な障壁に直面している。また、攻撃的サイバー能力を導入する権限が自衛隊に与えられたとしても、政治や法律、そして規範上の課題を乗り越えなければ運用はできないだろう。

サイバー領域における主権に関するコンセンサスの欠如は、米国の同盟国やパートナー国の間で依然根本的な課題である。その結果、サイバーセキュリティ協力の運用が限られてしまっている。主権に関する明確で一貫性のある方針が宣言されなければ、脅威ハンティングや脅威インテリジェンスの共有といったサイバーの共同任務の遂行は制限されたままとなろう。

主権や国際法に関する根本的な課題が残るとはいえ、日米両国は、実務的な形でサイバー協力を改善することができる。官民間で互いの組織文化、方法論、資源制約、リスク要因を理解することが重要な出発点となる。より緊密な連携の達成に向けたベースラインを確立することで、同盟国やパートナー国の間の信頼と運用効率を高め、摩擦を減らすことができるだろう。

マルチドメイン作戦への転換が進む中、サイバー能力の付加価値を特定するためには、ベースラインの設定が非常に重要となる。そのすり合わせによって、より円滑にリアルタイムで脅威情報を共有し、脅威ハンティングを行うことができるようになる。大きな影響力をもたらす紛争が朝鮮半島、東シナ海、南シナ海、台湾で発生した場合、これは特に有益となるだろう。

国際サイバー外交における相乗効果の実現

サイバー外交における米国の実績にはむらがある。東南アジアや太平洋島嶼国に対する米国政府の取り組みを見ればこれは明らかである。対テロ戦争で20年間中東に気を取られていた米国は、中国の影響力拡大もあり、再び東南アジアに注目している。米国のサイバー能力構築は勢いを増してきているが、ま

だ正式な制度化に至っていない。ファイブ・アイズ以外の同盟国を米国が信頼していないことも、サイバー協力、特に情報共有の妨げとなっている。

東南アジアにおけるサイバー能力構築に向けた日本の取り組みは、米国と比較すると、より高度とは言えないまでも、より持続的である。2023年に日本ASEAN友好協力50周年を記念した際も、共同のサイバー能力構築が最優先事項として掲げられた。東南アジア諸国は、中国に対する日本のアプローチに賛同している。日本は、強硬な反中感情を前面に押し出すのではなく、限られた資源を活用した上で、公共財の提供、投資、能力構築を通じて、東南アジアの信頼と信用を獲得してきた。

東南アジアにおける日米の主な課題の一つは、第5世代通信（5G）のような重要な分野で、中国の技術の代わりに活用できる代替技術を提供することである。東南アジアでは、中国がインフラ整備に力を入れていることに加え、ファーウェイ、アリババ、テンセントなども拡大しており、能力開発や技術移転を進めている。

これに対抗するため、日米は「オープンな無線アクセス・ネットワーク」を提唱している。東南アジアのデジタルギャップを補強し、中国への依存度を下げるための有力な選択肢として、最近拡大してきたスターリンクも注目に値する。

日本が信頼できるパートナーとしてこの地域で評価されていることから、日本政府が主導権を握り、米国政府がそれを補完する形で支援を行うことが戦略的であろう。

日本は、サイバーセキュリティの戦略的必要性について東南アジアを説得できる立場にある。日米は、サプライチェーンの強靭性、データフロー、クラウドや海底ケーブルのようなデジタル・インフラといったASEANの新たな政策課題に取り組むため、サイバー能力構築に向けた既存の取り組みを拡大することができる。

韓国やNATOのような、緊密で志を同じくする同盟国や組織とのパートナーシップも、デジタル公共財の提供やサイバー能力構築に役立つだろう。日韓関係が改善してきたことで、情報共有の拡大の見通しは明るくなった。同様に、クアッドのような地域外交プラットフォームでも、国際的な技術基準やサイバーセキュリティのリスク管理の枠組みの適用が引き続き取り上げられている。

日米の政策立案者がサイバー外交の範囲と幅を拡大しようとする中、何を優先するかが鍵となる。協議を重ねて努力の重複を避ければ、慎重な計画を立て、限られた資源をより効果的に配分し、政策においても一貫してサイバーに注目することができるだろう。

サイバー能力に対する民間部門の取り組みに関して、あまり大きな期待はしない方がよいかもしれない。マイクロソフトのような世界的なプレゼンスを持つ大手情報通信技術企業は、能力構築や規範の普及にかかるコストを喜んで負担するかもしれない。他方、中小企業は、コストを恐れてあまり関心を示さないかもしれない。能力向上に向けたインセンティブは、このギャップを縮めるのに役立つだろう。大企業は、その社会的責任の一環として、中小企業によるサイバーセキュリティ・ガイドラインの策定を支援することができる。

将来の危機を見越して適切なリソースを配置することも、優先順位付けの一環である。ロシアによるウクライナ侵攻は、本格的なサイバー戦争が発生した場合、事後よりも事前の対策を追求することが大きな利益をもたらすことを示した。将来を見据えて行動したウクライナの人々は、ロシアによる侵攻の前に、タイムリーかつ戦略的な方法でサイバー防衛を強固なものにし、情報共有を強化することができた。

地政学的環境が非常に不安定であることを踏まえ、日米は、サイバー戦争が勃発する可能性のあるホットスポットがどこなのかを検討することから戦略計画を立て始めるべきだ。候補地としては、台湾、中国、シンガポール、グアム、ハワイ、インドネシア、フィリピン、東南アジア、バルト諸国、ラテンアメリカなどがある。

生成AIがサイバーセキュリティに与える影響

生成AIは、マルウェア、ソーシャル・エンジニアリング、ディープフェイクの拡散など、新しい形の脆弱性をもたらすだろう。このようなブレイクスルーがあると、社会において人々が互いを信頼できなくなる可能性がある。戦略的に競争相手を負かしたいと思う者は、生成AIで監視を行い、ディープフェイクを使って偽情報を広めることができる。

国家は、イノベーションの推進とは別に、AIのガードレールの設定においても民間部門と競合している。マイクロソフト、グーグル、アップル、メタ、アマゾンのようなシリコンバレーを拠点とする企業は、生成AIを積極的にビジネスモデルに統合したり模索したりしている。AIガバナンスに関して世界的な流れを作っているのもこれらの企業である。このような動きがある中、イノベーションを促進しながらも規制の一貫性を確立することは大きな課題となる。相互運用性から安全保障に至るまで、軍事・非軍事に応用されるAI対応技術の発展を形作る、多くの問題を提起している。

高度なデータ駆動型分析や機械学習モデルの開発に加え、半導体も現在のAI開発競争の中心にある。エヌビディアと台湾セミコンダクター・マニュファクチャリング・カンパニーは、次世代のAIチップを開発するため、研究開発に多額の投資を行い、米国、アジア、ヨーロッパに工場を設立している。半導体企業は「CHIPSおよび科学法」から補助金を受けられるだろうが、日米の輸出規制が進化していく中、その影響を緩和するための実践的な解決策をまだ見つけていない。

現在の生成AIブームを受け、雇用の置き換えは日米にとって重要な問題となるだろう。競争力を維持するには、教育カリキュラムを見直し、デジタル経済時代にふさわしいものに変えていくことが急務である。生成AIの次は汎用AIだと見込まれている中、人間と機械の相互作用を再定義する上で、社会科学が極めて重要になる。科学、技術、工学、数学（STEM）に偏ったスキルにばかり焦点を当てない方がよい。芸術や人文科学にも力を入れ、分析力と適応力だけでなく創造性も兼ね備えた、バランスの取れた労働人口や有識者を生み出すことが重要だ。

継続的従事による集団的サイバー防衛と強靭性の構築

エミリー・O・ゴールドマン

サイバー領域における現状と戦略的収束

国家が支援する悪質なサイバー行為のほとんどは、武力紛争のレベルに満たない、非暴力的な活動である。まとまりのあるキャンペーンとなったものは、戦略的優位性の獲得・維持、または相手の国力の源泉や手段の弱体化を目指している。この活動が二重の役割を果たすこともある。将来の軍事化された危機や武力紛争において、国家や連合が勝利するための条件を整えることを目指しているのである。

このような工作やキャンペーンは、サイバー空間で実際起きていることに対する、米国の戦略的アプローチの進化を形作ってきた。2018年には、過去の戦略的損失を受け、一連の政策と法律が改正された。これにより、サイバーに携わる米国の軍関係者は、より自由に活動し、武力紛争未満のサイバー空間侵略に対抗できるようになった。日々の競争の経験を踏まえ、2018年から2022年にかけて米国の思想と実践が成熟し、こうした考え方が米国内外で支持されるようになった。ロシアがウクライナに侵攻する直前の2021年後半も、「有事に向けた作戦の成功は競争におけるサイバー活動から始まる」という洞察に基づいて、米国の思想と実践は成熟していった。

この進化の過程で、同盟国やパートナー国が不可欠な役割を担っていることが証明された。米国、そして民主主義の同盟国やパートナー国が抱える現在の課題は、協調してそれぞれのツール、洞察力、経験を集団的に発揮することである。これにより、ライバル国家による、武力紛争未満であるものの戦略的な影響をもたらす活動を阻止し、危機や武力紛争が発生した場合にそれを抑止し勝利するための条件を整えることができる。各国家のアプローチは当然、国際政治、国内法体系、文化的態度、地政学的状況、国際法の解釈によって形成されている。集団的な取り組みにおいては、それらを健全な形で受け入れることが必要である。アプローチの違いがあるとはいえ、これらの国家は共通の現実に直面している。サイバー空間はすべてがつながり競い合い続けている戦略的環境であり、優位性を得たい者は継続的に脆弱性につけこむことが可能である。このような共通の背景により、米国とそのパートナー国は、少しずつではあるが、積極的かつ持続的な従事、と言う形で視点が一致してきている[1]。

米国のアプローチの起源と進化

サイバー戦略環境においては、世界各地のコンピューターがつながっており、どこからでもアクセスが可能であるため、敵味方が常に接触できる構造的な相互接続性がある[2]。サイバー空間は、細かいところが脆弱（本質的に悪用されやすい）であると同時に、全体的には強靭（体系的に安定している）である。サイバー空間のこうした特質が組み合わさると、その相互接続性が攻撃的な国家や行為者に継続的に悪用されることになる。サイバーの脆弱性を悪用して優位に立とうとする主体は、常にどこかにいる。彼らが何度も成功すると、戦略的に大きな被害を及ぼすレベルにまで達してしまう可能性がある。このような活動はすべて、物理的な戦争の脅威や実践なしに起こる。サイバー空間においては、威圧したり戦ったりすることなく勝利することが可能なのである。

米国政策に携わる人々は、サイバー空間における武力紛争未満のキャンペーンが積み重なることで、国家の戦略的損失が

起きていることを認識してきた。その認識は次第に高まっている。大規模な知的財産の窃盗は、競争における米国の優位性と経済力を低下させている。軍事研究開発の窃盗や（もっと最近で言えば）サプライチェーンの混乱や操作は、軍事における米国の優位性を脅かしている。サイバーを利用して情報や影響力を操作した行為は、社会的結束と同盟国間の連帯を弱め、民主主義制度を弱体化させ、選挙結果に疑念を投げかけることによって、米国の政治的影響力を低下させた。

自制の姿勢や、「攻撃を受けたらそれに応じる」という抑止などの脅しはうまくいかなかった。タイムリーな対応が必要なほど個別の事件が深刻になることはめったにないため、敵の活動の大半は、米国が反撃しないまま終わった。その結果、敵はさらに図々しくなってほぼ無制限に活動し、繰り返しサイバー侵略で利益を得てきた。

サイバー空間に対する米国のアプローチは、国内政治と作戦経験によって形成されている。2018年は転換点であった。米国防総省は「前方防衛」戦略を発表した[3]。米サイバー軍のマイク・ロジャース司令官は、同軍のビジョンである「サイバー空間における優位の達成と維持」に署名し、「継続的従事」の概念を導入した[4]。2019年の国防権限法は、サイバー空間での作戦を伝統的な軍事活動として定義し、秘密工作に適用される承認・監督手続きの対象外だとした。最後に、新たな大統領政策により、サイバー空間作戦に関するより多くの権限が国防総省に委譲された。サイバー空間に特化した軍の新しい作戦アプローチと、そのアプローチを実施するための法的権限と政治的ガイダンスが整備されたのである。

「前方防衛」と「継続的従事」はともに、安全保障の取り組みをサイバー空間の戦略的環境に適用した。重大なサイバー攻撃を抑止すると同時に、武力紛争に至らないサイバー空間作戦に直面した場合、継続性と強靭性を確保するようにしたのである。「継続的従事」は、競争、危機、武力紛争において米サイバー軍がどのように兵力を用いるかを導く一連の原則と運用概念を設け、脅威にしっかり対応できていない状況に対処する。今すぐ、

継続的かつ積極的に敵に対抗すること、国内および外国のパートナーに力を付けること、あらゆる形の競争にわたって主導権を獲得・維持するためにサイバー空間を通じて行動することを提唱している。

「継続的従事」とは、根本的には、安全保障と競争の条件を自らに有利に設定することに継続的に取り組むこと、脆弱性の利用に関する競争相手の計画を予測すること、発生したことに反応するのではなく、武器化や悪用されたりする前に適応することを意味する。サイバー軍は何かが起こるのを待っているのではなく、常に米国外で活動し、敵のツール、ハッカー、インフラ、マルウェアを特定している。また、このアプローチにおける重要な要素として、サイバーセキュリティの取り組みを拡大するため、情報、技術、シグネチャ、指標を民間部門と共有している。

「継続的従事」は、戦時における計画や実行よりも広い間口を設けている。武力紛争未満にとどまるように設計されたものの、累積して敵に戦略的利益をもたらす、サイバー空間における継続的で広範なキャンペーンに立ち向かっている。サイバー空間は構造的に行動せざるを得ない場である。そのため、「継続的従事」の目的は、悪意あるサイバー活動を抑止することではなく、相手の成功を不可能にすることである。

サイバー空間に携わる軍関係者がより自由に活動するにつれ、サイバー軍が「対応」から「継続」へと軸足を移したことは正しかったということが作戦経験から分かってきた。2018年の中間選挙をロシアの干渉と影響から守るため、米国政府は新しいアイデアも取り入れた。これらの作戦は、武力紛争にエスカレートさせることなく、米国が選挙を守り、選挙への干渉を目的としたサイバー活動を混乱させることができることを示した。ロシアの行為者がサイバー能力を利用して選挙を弱体化させることを妨害するサイバー活動もその一環であった。防衛サイバー・チームが（ホスト国の許可を得て）初めて海外に派遣され、外国のネットワークを使って米国本土に危害を加える可能性のある敵の活動を探した。敵が活動している場所に赴くことで、サイバー・チームは新たな活動を発見し、海外のパートナーに警告を

発して彼らのネットワークの安全確保を支援し、産業界と直接情報を共有して緩和策を開発することができた。

「ハント・フォワード」と呼ばれるその後の軍事活動は、予期せぬ形でこの原則を成熟させた。諜報主導型でパートナーからの要請を踏まえたこれらの作戦は、当初、外国の干渉や影響から選挙を守るため、省庁を超えた広範な取り組みを支援することが目的であった。しかし彼らの活動により、悪意あるサイバー行為者が世界各地で何をしているかが明らかになった。インフラを強化するために国内外のパートナーと共有された洞察は、敵の活動やツールを暴いた。これにより、敵から時間、資金、アクセスを奪い、その活動コストを増加させた。これらの活動は重要性と影響力を増しており、今では新たなサイバーセキュリティ・パートナーシップを可能にし、インフラの強靭性を高め、新しい洞察を得ている。サイバーに携わる軍関係者は、攻撃が起きる前に国内外のパートナー・ネットワークでハンティングを行い、産業界に情報を提供し、悪意ある活動を公表し、マルウェアを暴露している。これを受け、悪意ある行為者は、選択肢が狭まり、攻撃ベクトルが減り、侵入することができなくなる。米国によるこうした活動は、同盟国やパートナー国を安心させ、パートナーシップを構築・強化し、米国、同盟国、パートナー国の重要なネットワークの防衛を強化する。

米国は、ウクライナでも自国の国家安全保障目標を支援する作戦を行った。これは、危機や紛争において、サイバー空間での能力がどのような役割を務めるのかについて、米国の理解を深めた。有事作戦の成功は、競争における継続的従事（米国の2022年国家防衛戦略の言葉を借りれば「キャンペーン」）から始まる5。キャンペーンは、作戦行動に関する敵の自由を制限し、危機や紛争において影響力を持てないようにするための洞察、機会、選択肢を生み出す。また、情報公開の威力と、諜報共有できるパートナー・ネットワークを危機の前に確保することの必要性が、経験によって明らかになった。サイバー空間を通じて、現在も今後も継続的にキャンペーンを行うことは、競争における戦略的損失を減らし、危機や紛争において敵を抑止し勝利するための条件を設定することにつながる。

サイバー軍の経験は、サイバー空間における作戦活動の価値を明確にする上でも役立っている。従来の軍事評価方法は、紛争におけるサイバー作戦が、物理的な効果に代わる独立した決定的な成果をもたらすかどうかという観点から、成功や失敗を定義している。しかし、ロシア・ウクライナ紛争において米政府の目標を支援する作戦や活動により、この状況は変わった。サイバー空間における活動や作戦の価値は、敵に対して累積した影響や、米国とその連合パートナーの持続的な優位性という観点で捉えた方が有益だということが明らかになったのだ。時間は重要な変数であるため、即座に効果を出す必要もない。サイバー活動や作戦は、時間の経過とともに累積する影響により、徐々に相手を弱体化させることができる。敵が消耗戦を追求している状況では、信頼、効率、能力を継続的に低下させることが重要である。キャンペーンと連動させれば、小さな変化であっても、主導権を握る者に増幅的な影響を与える可能性がある。

軍のサイバー作戦やキャンペーンには、通常、省庁間のパートナーの目標や行動を支援し、より広範な国家の戦略目標を推進するためのさまざまな活動も含まれる。例えば、特定の手段を可能にし、制裁を増幅し、「正義への報酬プログラム」（アメリカ人の命を守り、米国の国家安全保障目標を促進する情報に対し、報奨を提供する米国務省のプログラム）に情報を提供し、起訴や逮捕をしやすくする。紛争における独立した決定的かつ戦略的な成果、という観点からサイバー行為の価値を評価することは、戦略的決定力と戦略的有用性を同一視しているため、間違った見方である。サイバー作戦やキャンペーンは、紛争において独立した戦略的決定力を持つとは限らないが、結果に直接または間接的に貢献する場合には、戦略的有用性を持つ。紛争や危機において、サイバー能力を通常能力から独立したもの（あるいは通常能力の代わり）として扱うことは、理論としては興味深いかもしれないが、作戦や戦略という意味では重要でない。サイバーの戦略的有用性は、利害を安定・前進させるために競争でそれを積極的に使用すること、将来起こりうる危機や紛争を管理するための条件を整えることで発揮される。

日米のパートナーシップの機会

同盟国やパートナー国との協力は、米国の防衛・軍事・サイバー戦略における重要な要素である。国防総省は、「米国が持つ同盟国やパートナー国との世界的なネットワークは、サイバー領域における根本的な優位性であり、それを保護・強化する必要がある」と認識している[6]。国家は、それぞれ異なる手法、リスク許容度、法的解釈、承認プロセス、タイムラインを持つ。これらを認識し、理解しなければ、集団的な努力が難しくなる可能性がある。達成可能な目標として、各国家が持つ機会と制約に沿って、互いを補完する形で予防的戦略を計画することができるだろう。そのためにはまず、重複し整合性がある部分に焦点を当てなければならない。日米については、サイバー戦略環境に対する理解と、継続的にキャンペーンを行うという考え方が共通項のようだ。

日本の国家安全保障戦略（2022年12月発表）と国家防衛戦略（2022年12月16日発表）は、「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、これを未然に排除」するため、「能動的サイバー防御」をそれぞれ独自に提唱した。「能動的サイバー防御」は、民間部門とこれまでより緊密に連携し、情報共有と悪意ある行動の検知が必要であるとしている。それを実行するには、悪意ある行動を事前に検知し、そこに侵入し、破壊または無力化する権限と能力を拡大するための法改正が必要である。これには「可能な限り未然に攻撃者のサーバ等への侵入・無害化ができる」権限も含まれる[7]。現在の法律では、このような措置は緊急事態や軍事攻撃の後にのみ発動される。能動的防御の下では、軍事組織の役割と任務は拡大するが、それが米国の「前方防衛」戦略に合致するかどうかはまだ不明である。能動的サイバー防御は、サイバー空間で起きていることに対して、より積極的で先を見据えたアプローチに転換することを意味する[8]。そういった意味では、「継続的従事」の根底にある論理と合致している[9]。

日米両国は、収束しつつあるアプローチを基盤として、集団的サイバー防衛と継続的な活動を通じた強靭性を推進することができる。サイバーに携わる軍関係者の役割と任務を集団的な

ものに適応させることで、両国は、国家全体の取り組みを拡大することができる。これにより、武力紛争未満の敵対的なサイバー活動やサイバーが可能にする活動に対し、機敏な形で連携し、継続的に圧力をかけることができる。

今後力を入れていく価値のある取り組みは複数ある。第一に、ネットワークの安全確保、運用、防衛を強化するための能力構築に焦点を当てた、「サイバーセキュリティの基盤」の整備である。第二に、共通の防衛と相互運用性を実現するため、情報と諜報共有のためのネットワークを確保することである。これは、危機や紛争に先立ち、パートナーとともに任務を追求する環境を強化し、有事作戦を成功させるための条件を整えるものでなければならない。また、統合サイバー活動に焦点を当てた「サイバー空間作戦」の展開に向けた前提条件でもある。最後に、情報のサニタイズや機密指定の引き下げなどを通じて情報共有がしやすいようにし、可能な限り連携に対する障害を軽減することが挙げられる。

何よりも、脅威を積極的に探し対抗するためには、政府、社会、国家における信頼と共通理解が必要である。それぞれの国の関心、状況、権限に合わせた「継続的従事」のようなアプローチが広く受け入れられつつあることは、前向きな一歩である。今後は、規模を拡大し、取り組みを増やし、戦略的一貫性を高めることで、戦略と最終的な目標を明確に持ち、野心的で資金が潤沢な敵に対抗していくことができるだろう。

本稿に示された見解は筆者自身のものであり、国防総省や米国政府機関の公式見解を反映するものではない。

[1] Richard J. Harknett, Michael P. Fischerkeller, Emily O. Goldman, "U.K. National Cyber Force, Responsible Cyber Power, and Cyber Persistence Theory" (April 5, 2023), https://www.lawfaremedia.org/article/uk-national-cyber-force-responsible-cyber-power-and-cyber-persistence-theory; Alexander Martin, "NATO's Christian-Marc Lifländer on how the alliance can take a 'proactive' cyber stance," The Record (July 10, 2023), https://therecord.media/christian-marc-liflander-on-nato-cyber-defense.

[2] Michael P. Fischerkeller, Emily O. Goldman and Richard J. Harknett, Cyber Persistence Theory: Redefining National Security in Cyberspace (Oxford University Press, 2022).

[3] Department of Defense Cyber Strategy Summary (2018), https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.

[4] Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command (2018) https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf.

[5] National Defense Strategy of the United States of America (2022) https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF

[6] Fact Sheet: 2023 DoD Cyber Strategy, https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

[7]「国家家安全保障戦略」(2022年12月), p. 30.

[8] https://asia.nikkei.com/Politics/Japan-to-upgrade-cyber-defense-allowing-preemptive-measures; https://www.dragonflyintelligence.com/news/japan-shift-to-a-more-offensive-cyber-posture-in-2023/; Tokuchi Hideshi, "Japan's New National Security Strategy and Contribution to a Networked Regional Security Architecture," CSIS (June 23, 2023), https://www.csis.org/analysis/japans-new-national-security-strategy-and-contribution-networked-regional-security.

[9] 国防総省やIT業界における従来の使い方によれば、「継続的従事」は、米国の原則として、「能動的サイバー防御」以上のものである。米国における「能動的なサイバー防御」は、自らのネットワーク上での活動や、紛争領域を直接管理することに限定される。「継続的従事」は、積極的にデジタル空間全体の状況を見極め、先回りして条件を設定・リセットすることを意味する。

インド太平洋地域で起こりうる危機に対処するための日米サイバーセキュリティ協力

松原 実穂子

サイバーセキュリティ協力は、経済と国家安全保障の観点から、日米でこれまで以上に重要である。同盟国である両国は、サイバースパイ活動や破壊工作に対する懸念を共有している。サイバースパイ活動は、情報を盗むための今後の活動に備えた、破壊行為や妨害行為の前兆となることもある。情報通信技術（ICTs）への依存度が世界的に高まる中、サイバーセキュリティは、経済的繁栄だけでなく、国際安全保障にとっても極めて重要になっている。日米両国は、変化するサイバー脅威の状況に対処するため、重要な取り組み（ランサムウェア、重要インフラ保護、サイバー脅威インテリジェンスなど）を推進しつつあり、サイバーセキュリティ協力を強化する強い決意を示している。

ランサムウェアに対する取り組み

2021年5月に発生したコロニアル・パイプラインへのランサムウェア攻撃は、政策立案者にとって大きな衝撃となった。財政的動機に基づく犯罪集団が、単一の組織のサプライチェーンを攻撃することで、経済や国家安全保障に混乱をもたらすことができるということが判明したのだ。米国の大手エネルギー会社であるコロニアル・パイプラインは、結局6日間燃料供給を停止せざるを得なかった[10]。

2023年7月には、日本最大の貨物取扱量を誇る名古屋港がランサムウェア攻撃を受け、ほぼ2日間にわたり船舶の運航が中断された。この事件により、トヨタ自動車も、4つの物流センターで自動車部品の出荷を1日停止せざるを得なくなった[11]。にもかかわらず、名古屋港はデータを迅速に復旧し、わずか2日で業務を再開した。ランサムウェア攻撃の平均的なダウンタイムが25日であることを考えれば、これは驚くべきことである[12]。それでも、このようなサイバー攻撃が頻発したことで、サイバーの強靭性がいかに重要であるかが強調された。相互依存性が高い商業においては特に、事業継続性を確保し、ドミノ効果を最小限に抑えることの重要性が示された。

重大なサイバー攻撃がもたらした大きな混乱を受け、米国政府は2021年10月、日本を含む30カ国の同盟国や同志国を招待し、「カウンターランサムウェア・イニシアティブ会合」をオンラインで開催した[13]。2022年10月から11月にかけては、集団的強靭性とランサムウェア活動の妨害に取り組むため、同会合が対面で開かれた[14]。

日本はすでに、実用的な諜報を共有することで、この国際的な取り組みに貢献し始めている。例えば、2023年5月、米国司法省は、ロシア国籍のミハイル・パブロヴィッチ・マトヴェエフの2件の起訴につながったとして、日本の警察庁による支援を称えた[15]。マトヴェエフは、米国内の重要インフラに対してランサムウェア攻撃を行っていた。将来的な犯罪捜査や諜報収集をめぐる機密保持のため、警察庁による協力の詳細な内容は明らかにされなかった。いずれにせよ、この起訴は、犯人の責任を追及し、

その活動を妨害する上で、ランサムウェアに関する日米の法執行機関の緊密な協力が重要であることを示している。

重要インフラの保護

重要インフラの強靭性と保護は、インド太平洋地域の安全保障と安定にとって不可欠である。台湾海峡における潜在的な危機への関心が高まっていることを考えれば、なおさらのことである[16]。最近のサイバー脅威は、台湾有事の可能性がますます高まっていることを示しているとも考えられる。

2023年5月にマイクロソフトは、2021年半ば以降、「中国を拠点とする、国家の支援を受けた行為者」が「グアムや米国のその他の地域の重要インフラ組織」、特に通信や公共事業を標的にしていると警告した。グローバルICT企業である同社は、サイバースパイ活動の最終目的は、「将来危機が起きた際に、米国とアジア地域との間の重要な通信インフラを混乱させること」であろうと推測している[17]。台湾有事が起きれば、米国の主要な空軍基地と港湾であるグアムが米軍の作戦において重要な役割を果たすことは明らかである[18]。2023年7月現在、報道によれば、米国政府は、米国内外の軍事基地を支援するための通信、電力、水道のネットワークの中で、中国製マルウェアの脅威ハンティングを行っているようだ。有事が起きれば、このマルウェアは、米軍の派遣を遅らせる可能性があると考えられている[19]。

脅威ハンティングは、これまで起こりえた侵害を積極的に探し、ネットワークにおける敵のアクセスをなくし、サイバー攻撃による被害を最小限に抑え、組織の強靭性を強化することを目的としている。しかし、政府が単独でこれを行うことはできない。共有されたサイバー脅威インテリジェンスに基づき、重要インフラネットワークにおける敵の痕跡を効果的に探索し、対抗するには、国際的な官民パートナーシップが不可欠である。日米は、電力[20]、金融[21]、情報技術[22]などの重要インフラ分野を保護するため、サイバー脅威インテリジェンスやサイバーセキュリティのベストプラクティスを共有してきた。

日本のサイバー政策における最近の動向は、米国との協力範囲をさらに拡大するかもしれない。2022年12月に日本は国家防衛戦略を発表し、自衛隊法で課されていないにもかかわらず、防衛省と自衛隊が2027年度までに「自衛隊以外へのサイバーセキュリティを支援」できる態勢を整えると宣言した[23]。新たな防衛力整備計画も、自衛隊が脅威ハンティングを実施する可能性を支援する[24]。

サイバー脅威インテリジェンスの共有の取り組みをさらに強化 するための鍵となるのは、相互運用可能なセキュリティ・クリアランスである。なぜなら、一部の諜報は政府によってのみ取得可能であり、文脈情報などの特定の諜報は機密解除やサニタイズができないからである。これが実施されれば、日米両政府と重要インフラ企業との間の既存の取り決めにプラスになる。2023年6月に高市早苗経済安全保障担当大臣は、2024年に経済安全保障を推進するため、米国や欧州の制度に類似したセキュリティ・クリアランスを展開する法案を提出する意向を表明した[25]。相互運用可能なセキュリティ・クリアランスがなければ、日本、米国、パートナー諸国が、異なるインテリジェンス・フィードを融合し、サイバー脅威の状況についてより明確なイメージを入手・共有し、潜在的な被害をタイムリーな形で最小化することは困難であろう。当然のことながら、政府の仕組み、技術、機密情報隔離施設（SCIF）にまたがるセキュリティ・クリアランス制度を確立し、インテリジェンス・フィードの収集、分析、処理、普及に取り組むには、時間と資源が必要である。

サイバー脅威インテリジェンスの共有

セキュリティ・クリアランス制度の確立と並行して、日本は、必ずしもセキュリティ・クリアランスを保持していないサイバー防衛者の間でサイバー脅威インテリジェンスを迅速に共有するためのプラットフォームを構築する必要がある。日本は、米国サイバーセキュリティ・インフラストラクチャーセキュリティ庁の「

シールド・アップ」キャンペーンのウェブサイトから学ぶことができる。2022年2月にロシアがウクライナに侵攻する数日前に開設されたこのオンライン・ポータルは、最新のサイバー脅威と緩和策に関して、重要インフラ防衛者だけでなく、業界のリーダーにも警告を発している[26]。

日本政府が同様のリソースを構築すれば、日米や同志国の政策立案者や産業界の代表者に貴重な知見をもたらすことになる。戦略的には、そこで共有・入手された情報は調整の改善に役立つ。インド太平洋地域での有事の危険性が高いことを考えれば、なおさら有益だろう。運用面でも、このオンライン・プラットフォームは、サイバー・インテリジェンス・フィードをタイムリーに提供し続ける上で不可欠となるだろう[27]。

結論

「カウンターランサムウェア・イニシアティブ会合」のような国際的な取り組みによって、過去1年間、日米両国がサイバーセキュリティ協力において具体的な進展を遂げてきたことは明らかである。しかし、両国は今、インド太平洋地域で起こりうる危機に焦点を移さなければならない。集団的強靭性はさらに重要になるだろう。重要インフラにおける脅威ハンティングを日本の国家安全保障戦略が可能にしたことで、日米はより多くのことを追求できるようになるだろう。サイバー脅威インテリジェンスの取り決めを拡大することは、機密情報と非機密情報を処理し、脅威の連携を緩和するための次のステップにもなり得る。企業がますますサイバー攻撃を受けている中、これは特に重要である。

[10] Mary Louise Kelly, Jason Fuller, and Justine Kenin, "The Colonial Pipeline CEO Explains The Decision To Pay Hackers A $4.4 Million Ransom," NPR, June 3, 2021, https://www.npr.org/2021/06/03/1003020300/colonial-pipeline-ceo-explains-the-decision-to-pay-hackers-4-4-million-ransom.
[11] Apurva Venkat, "Japan's Nagoya port resumes operations after ransomware attack," CSO Online, July 6, 2023, https://www.csoonline.com/article/644765/japans-nagoya-port-resumes-operations-after-ransomware-attack.html.
[12] Coveware, "Uber Verdict Raises New Risks for Ransom Payments," October 26, 2022, https://www.coveware.com/blog/2022/10/26/q3-2022-quarterly-report.
[13] The White House, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/.
[14] The White House, "International Counter Ransomware Initiative 2022 Joint Statement," November 1, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/.
[15] U.S. Department of Justice, "Press Release: Russian National Charged with Ransomware Attacks Against Critical Infrastructure," May 16, 2023, https://www.justice.gov/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure.
[16] Alex Willemyns, "CIA director: China readying for Taiwan invasion by 2027," Radio Free Asia, February 3, 2023, https://www.rfa.org/english/news/china/cia-taiwan-invasion-02032023160341.html.
[17] Microsoft, "Volt Typhoon targets US critical infrastructure with living-off-the-land techniques," May 24, 2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
[18] David E. Sanger, "Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?," The New York Times, May 24, 2023, https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html.
[19] David E. Sanger and Juliane E. Barnes, "U.S. hunts Chinese malware amid military disruption fears," The New York Times, July 29, 2023, https://www.nytimes.com/2023/07/29/us/politics/china-malware-us-military-bases-taiwan.html.
[20] EE-ISAC, "Trilateral Memorandum of Understanding | JE-ISAC, US-ISAC, EE-ISAC," October 17, 2018, https://www.ee-isac.eu/trilateral-memorandum-of-understanding-between-japan-u-s-and-european-energy-isac/. ISAC stands for Information Sharing and Analysis Center, referring to critical infrastructure sector-driven cooperation to share cyber threat intelligence and best practices.

[21] Financial ISAC, “Cooperation with FS-ISAC,” Accessed August 8, 2023, https://www.f-isac.jp/cooperation/index_e.html.
[22] Scott Algeier, “IT-ISAC Formalizes Operational Partnership with ICT-ISAC Japan,” November 12, 2019, IT-ISAC, https://www.it-isac.org/post/it-isac-formalizes-operational-partnership-with-ict-isac-japan.
[23] 防衛省「国家防衛戦略」(2022年12月16日), https://www.mod.go.jp/j/policy/agenda/guideline/strategy/pdf/strategy.pdf, p. 20.
[24] 防衛省「防衛力整備計画」(2022年12月16日), https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf, p. 11.
[25] Erika Kobayashi, “Japan plans security clearances similar to U.S. and Europe,” Nikkei Asia, June 7, 2023, https://asia.nikkei.com/Politics/Defense/Japan-plans-security-clearances-similar-to-U.S.-and-Europe.
[26] Cybersecurity and Infrastructure Security Agency, “Shields Up!,” Accessed August 7, 2023, https://www.cisa.gov/shields-up.
[27] デビッド・ビーバウトへのメールインタビュー（2023年8月7日）。

東南アジアとインド太平洋における米国のサイバー外交

ベンジャミン・バートレット

東南アジアでのサイバーセキュリティの能力構築に対する支援において、これまで米国は、比較的小さな役割しか果たしてこなかった。世界全体における能力構築を目指す事業以外で、同地域に能力構築支援を提供する主な取り組みは、トランプ政権下で始まり、バイデン政権下で継続・拡大されている。こうした取り組みは、東南アジアにおける中国の影響力に対抗するため、東南アジアに関与するという広範な戦略の一環であるように見える。しかし、サイバーセキュリティに関する米国と東南アジア間の協力的な取り組みはまだきちんと制度化されておらず、米国の次期政権がバイデン政権の取り組みを引き継ぐかどうかは不明である。また、時間と資源に限りがある上、東南アジアにおけるサイバーセキュリティの能力構築支援には、日本がすでに力を入れている。そうなると米国は、独自の貢献ができる分野や、新しい「継続的従事」サイバー戦略に明確に合致する分野に焦点を絞った方がよいかもしれない。

勢いが増してきた米・ASEANサイバー協力

米国がこの地域で支援した最初の大規模事業は、シンガポールとの協力で2016年に始まった。「シンガポール・米国第三国訓練プログラム」（TCTP）のサイバーセキュリティ・ワークショップは、それ以来少なくとも5回開催され、サイバーセキュリティ戦略の策定、インシデント管理の枠組み、広報キャンペーン、サイバー空間における責任ある国家行動などを取り上げてきた[28]。両国はまた、2019年に「米国・シンガポール・サイバーセキュリティ支援プログラム」を共同で立ち上げ、ASEAN加盟国に対し、コンピュータ緊急対応チーム（CERT）の能力と成熟度を高める方法について、産業界の視点を提供した[29]。シンガポールはサイバーセキュリティに関して、米国にとって主要なパートナーである。両国は、2016年に締結された覚書に基づき、2021年にはサイバーセキュリティ協力の強化に関する3つの覚書に署名した[30]。

米国が資金を提供した東南アジアの他の事業には、ジョージ・C・マーシャル欧州安全保障研究センターによる運営の下、2018年から2022年にかけて実施された「マルウェア軽減支援プログラム」も含まれる。同プログラムでは、インドネシア、フィリピン、タイ、マレーシアからの参加者を対象に、北朝鮮の不正なサイバー活動についての研修が行われた[31]。2021年に実施された、データ保護とサイバーセキュリティの国際基準をタイが準拠することを支援するための米国貿易開発庁による事業[32]も挙げられる。2023年にサイバーセキュリティ・インフラストラクチャーセキュリティ庁が実施したプログラム「タイ、フィリピン、インドネシアにおけるサイバー衛生能力の構築」では、複数の分野から参加者を招き、さまざまなサイバーセキュリティ関連の問題について話し合った[33]。米国はまた、2018年の「産業制御システムサイバーセキュリティのための日米共同訓練」[34] や「インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク」[35] など、日本やEUとの共同プログラムも実施してきた。

サイバーセキュリティの能力構築に関して、米国と東南アジアの協力はまだ大きく制度化されていないとはいえ、米国とASEAN加盟国の首脳は、2018年11月の第6回ASEAN・米国首脳

会議でサイバーセキュリティ協力に関する声明を発表した。同声明では、安全な情報技術（IT）環境の維持と能力構築について協力することに合意した。また、国際法がサイバー空間に適用することを再確認し[36]、2019年にはASEAN・米サイバー対話を設立した。同対話はこれまでに3回開催され、5Gの技術、国際法やサイバー規範の適用可能性、サイバーセキュリティの能力構築を含む地域協力の可能性などのテーマを取り上げている[37,38]。

サイバーセキュリティに関する米国と東南アジア諸国の協力関係が強化されるのと同じタイミングで、米国政府関係者は、自己主張を強める中国に対抗するため、米国がもっと努力しなければならないと考えるようになってきた。これは、2022年にバイデン政権が米国とASEANの関係を「包括的戦略パートナーシップ」に昇格させたことでも明らかである[39]。しかし、今後の米政権も東南アジアとの協力強化に投資し続けるかどうかは不明である。

東南アジアのみならず、広範なインド太平洋地域（オーストラリアを除く）におけるパートナー国やパートナーとなりうる国の間でも、米国とのサイバーセキュリティ協力がうまくいっていない。主な要因の一つは、米国がサイバー脅威やサイバー事件に関する情報の共有に消極的であることである。米国はパートナー国に共有した情報が漏れることを懸念しており、最悪のシナリオとしては、米国の情報源や手段にまつわる情報が敵に伝わる可能性を恐れている[40]。しかし、漏洩のリスクがあったとしても、米国は情報を共有する方法を見つけるべきである。例えば、情報源や手段が暴かれる可能性を低くするような方法で情報をサニタイズすることができる。さらに、米国は、共有された情報を保護するための明確なガイドラインをパートナー国や同盟国に提供すべきである。

対中政策を踏まえた日米サイバーセキュリティ協力

東南アジアやインド太平洋地域における中国の技術の影響力や拡散を制限しようとする米国の取り組みはサイバーセキュリティ協力だけではない。「デジタル・シルクロード」の取り組み

もその一例である。米国は、同盟国でありパートナーでもある日本と協力している。例えば、2021年4月、両国は「日米競争力・強靱性（コア）パートナーシップ」を発表した[41]。このパートナーシップの下、両国は、異なるベンダーの携帯電話機器間の相互運用性を可能にする、携帯電話ネットワークのオープン無線アクセスネットワーク（RAN）の推進など、デジタル技術に関連する多くの問題で協力することに合意した。中国のサプライヤーであるファーウェイの大きな利点は、5Gのプロトコル・スタック全体にわたって機器とサービスを提供できることである。異なるベンダーの機器が相互運用可能であれば、中国以外の企業も競争しやすくなる[42]。

日米は、二国間およびクアッドを通じて国際技術標準を開発・推進することを合意した。国際技術標準は、国際市場においてどの製品がより人気となるかに影響を与えることがある。また、異なる国の製品やサービス間の相互運用性にも影響を及ぼし、倫理や規範の側面から国際的な慣例を作り出すこともある。このような理由から、中国は近年、国際的な技術標準設定に対する影響力の拡大に努めている[43]。

日米両国はまた、インド太平洋地域において質の高いインフラ整備を支援することでも合意している。東南アジアにおけるインフラに関し、日本は「品質」に焦点を当てることで中国と競争してきた[44]。クラウド・コンピューティングのような分野で米国が優位に立っていることを考えれば、米国にも同様のことをするチャンスがある。しかし、重要なのは品質だけではない。中国が自国の技術に手厚い資金を提供しているため、価格も問題である。米国はこれに対抗するため、独自の融資を行う姿勢を強めている[45]。より困難な第二の課題は、中国の技術がしばしば監視のツールとして使われる一方で、日米は規範や倫理の理由からそれを拒否していることである[46]。残念ながら、東南アジアの多くの政府にとって、監視技術は魅力的である。

東南アジアにおける中国の影響力への対抗とサイバーセキュリティ能力の構築に関しては、日米は連携を強化できるだろう。難点の一つは、IT外交とサイバー外交がそれぞれの国で完

全に連携していないことである。両国ともIT外交とサイバー外交を司る官僚的な組織が分かれており、それぞれ独自の事業を推進している。各政府でこうした取り組みの調整を担当し、他の組織との窓口になれる単一の組織があれば楽であろう。サイバーセキュリティに関して言えば、米国ではサイバーセキュリティ・インフラストラクチャーセキュリティ庁（CISA）、日本では内閣サイバーセキュリティセンター（NISC）[47] が考えられる。

今後協力できる分野

東南アジアあるいはインド太平洋地域におけるサイバー能力構築支援やその他のサイバー外交で日米がうまく協力できるようになるには、まず解決しなければならない重要な課題がある。すなわち、米国がどの程度大きな役割を果たすべきかということである。日本がすでにこの地域で活動していることを考えると、これは特に重要な点だ。少なくとも、米国が日本の努力を補完する形でどのような付加価値を提供できるかを考えることは有益だろう。

米国は今や、敵の行為を予測し、敵に対応させることを目標とする「継続的従事」戦略に転換している。他方、上記の取り組みは、中国の行動や影響力に対応することに重点を置き、後から反応するようなものである。それが米国の資源を活用する最善策かどうかは、未解決の重要な問題である。米国がサイバー協力やサイバー外交を避けるべきだと言うのではなく、新しい戦略全体に合う形で協力を調整した方がよい、ということだ。その手始めとして、この地域の信頼できる同盟国に対し、ハント・フォワード作戦の概念を紹介することも検討してよいだろう。

[28] Cybil, "Singapore-United States Third Country Training Programme (TCTP) Cybersecurity Workshops - Cybil Portal," February 22, 2021, https://web.archive.org/web/20230803154534/https://cybilportal.org/projects/singapore-united-states-third-country-training-programme-tctp-cybersecurity-workshops/.
[29] Cybil, "US-SG Cybersecurity Technical Assistance Programme - Cybil Portal," December 2, 2020, https://web.archive.org/web/20230803175522/https://cybilportal.org/projects/us-sg-cybersecurity-technical-assistance-programme/.
[30] Aqil Haziq Mahmud, "More Cybersecurity Cooperation between Singapore, US in Public, Defence and Financial Sectors," Channel News Asia, August 23, 2021, https://web.archive.org/web/20230804142738/https://www.channelnewsasia.com/singapore/singapore-us-mou-cybersecurity-cooperation-public-defence-finance-2130121.

[31] Cybil, “Malware Mitigation Assistance - Cybil Portal,” October 21, 2021, https://web.archive.org/web/20230803174833/https://cybilportal.org/projects/malware-mitigation-assistance/.
[32] U.S. Trade and Development Agency, “Thailand Cybersecurity and Data Protection Standards Workshop,” January 26, 2021, https://web.archive.org/web/20230803175148/https://ustda.gov/wp-content/uploads/STCP-Thailand-Cyber-Security-Workshop-Flyer.pdf.
[33] Jamila Baraka, “CISA - Building Cyber Hygiene Capacity in Thailand, the Philippines and Indonesia | CISA,” April 21, 2023, https://web.archive.org/web/20230803180053/https://www.cisa.gov/news-events/news/cisa-building-cyber-hygiene-capacity-thailand-philippines-and-indonesia.
[34] Cybil, “Japan & US Joint Training for Industrial Control Systems Cybersecurity - Cybil Portal,” June 15, 2020, https://web.archive.org/web/20230803180623/https://cybilportal.org/projects/japan-us-joint-training-for-industrial-control-systems-cybersecurity/.
[35] 経済産業省「『インド太平洋地域向け日米EU産業制御システムサイバーセキュリティウィーク』を実施しました」(2022年10月 31日), https://www.meti.go.jp/press/2022/10/20221031001/20221031001.html.
[36] Governments of the Member States of ASEAN and Government of the United States of America, “ASEAN-United States Leaders’ Statement on Cybersecurity Cooperation,” November 7, 2018, https://web.archive.org/web/20230803181029/https://asean.org/wp-content/uploads/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf.
[37] Prashanth Parameswaran, “What’s Behind the New US-ASEAN Cyber Dialogue?,” The Diplomat, October 4, 2019, https://web.archive.org/web/20230803184859/https://thediplomat.com/2019/10/whats-behind-the-new-us-asean-cyber-dialogue/.
[38] Government of the United States of America and Government of Indonesia, “Co-Chairs’ Statement on the Third ASEAN-U.S. Cyber Policy Dialogue,” United States Department of State (blog), February 3, 2023, https://web.archive.org/web/20230803185822/https://www.state.gov/co-chairs-statement-on-the-third-asean-u-s-cyber-policy-dialogue/.
[39] The White House, “FACT SHEET: President Biden and ASEAN Leaders Launch the U.S.-ASEAN Comprehensive Strategic Partnership,” The White House, November 12, 2022, https://web.archive.org/web/20230609054019/https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/12/fact-sheet-president-biden-and-asean-leaders-launch-the-u-s-asean-comprehensive-strategic-partnership/.
[40] 政府関係者との会話に基づく。
[41] The White House, “Fact Sheet: U.S.-Japan Competitiveness and Resilience (CoRe) Partnership | The White House,” April 16, 2021, https://web.archive.org/web/20230720185825/https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/16/fact-sheet-u-s-japan-competitiveness-and-resilience-core-partnership/.
[42] David Sacks, “China’s Huawei Is Winning the 5G Race. Here’s What the United States Should Do To Respond | Council on Foreign Relations,” March 29, 2021, https://web.archive.org/web/20230803191950/https://www.cfr.org/blog/china-huawei-5g.
[43] Robert D. Hormats, “Who Will Set Standards for 21st Century Technologies — the US or

China?," Text, The Hill (blog), June 3, 2021, https://web.archive.org/web/20230804150949/https://thehill.com/opinion/technology/556047-who-will-set-standards-for-21st-century-technologies-the-us-or-china/.

[44] Sophie Jackman, "Japan Pushing 'quality' Aid to Counter China's Clout in ASEAN," Japan Today, September 12, 2016, https://web.archive.org/web/20160912163507/https://www.japantoday.com/category/politics/view/japan-pushing-quality-aid-to-counter-chinas-clout-in-asean.

[45] Stu Woo, "U.S. to Offer Loans to Lure Developing Countries Away From Chinese Telecom Gear," Wall Street Journal, October 18, 2020, sec. Tech, https://web.archive.org/web/20230510203906/https://www.wsj.com/articles/u-s-to-offer-loans-to-lure-developing-countries-away-from-chinese-telecom-gear-11603036800.

[46] Bulelani Jili, "China's Surveillance Ecosystem and the Global Spread of Its Tools," Atlantic Council (blog), October 17, 2022, https://web.archive.org/web/20230803193105/https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools/.

[47] 現在、日本国内ではNISCを別の組織に置き換える可能性が議論されているが、その場合はこの組織が適切だろう。

人工知能がサイバーセキュリティと国際協力に与える影響

アンドリュー・J・ローン

多くの国と同様、米国と日本も、サイバー攻撃の範囲と規模の拡大に苦しんでいる。この課題にさらに拍車をかけているのが、同時にAIがサイバー脅威環境を変化させていることである。このような激動の状況において、リスクを誇張したり見誤ったりしてしまうアナリストは多いだろう。逆に、注意を払う価値のあるリスクも数多く存在する。一部のリスクは誇張され過ぎていない。他のリスクは、必ずしも危険性が高いか低いかではなく、サイバー脅威がこれまでとは異なる種類、規模、スピードを持つものに今後変化していくことを予測している。防御面で言えば、AI技術の中には、多くの人が期待しているほど価値が高くないものもあれば、より有望なものもある。本稿では、これらのトピックに関して、セキュリティ・新興技術センターで「CyberAIプロジェクト」が行ってきた研究の一部を振り返り、説明する。

偽情報、フィッシング、詐欺

偽情報は今や、サイバー活動の一つとして見なされることが多い。CyberAIプロジェクトも、セキュリティ・新興技術センターが設立された2019年以来、偽情報を研究してきた。私たちは早いうちから、大規模言語モデルがどれくらい世論を形成するのかを評価することができた[48]。その後私たちは、自動化された偽情報のキルチェーン、影響を緩和する方法、偽物のコンテンツを検知する方法など、その脅威の様々な側面を研究してきた[49]。

その脅威は相当なものである。言語モデルは説得力のあるテキストを生成できる。特に文面を編集する人間がいたりフィルタがあったりすれば、効果的な文章を素早く選択したり、メッセージに沿ったものになるよう微調整したり、自動であることが分かるような間違いや省略をなくしたりすることができる。そして、その文章を偽物として検知することは極めて難しい。しかし、必ずしも悪意あるチャットボットだけが将来蔓延する訳ではない。偽情報キャンペーンを拡大するには、多くのコンテンツを書くだけでは不十分である。偽物の電子メール、場合によってはクレジットカード番号を含む、偽物のアカウントから成るインフラが必要になる。多くの場合、複数の国を経由するサーバーのネットワークが必要であり、これらのアカウントと、発信元を追跡するのが困難な方法で通信する必要がある。また、労力とメンテナンスが必要である。人間による旧態依然のオペレーションがいかに効果的であるかを考えると、労力を正当化することが難しい状況もあるだろう。

これらのモデルが詐欺にどのような影響を与えるかを理解する上でも、人間主導であることが鍵となる。お金を要求する偽のナイジェリアの王子のような例は、たいてい文法の間違いや誤字脱字に満ちており、偽物であることが明らかなのが有名だ。言語モデルにより、このような詐欺も偽物だと分かりづらいものに変わるだろう、とこの分野に関心のある人の多くが考えている。その見解では、間違った文法や見るからに偽物であることが取り除くべきバグであると考えているが、それが逆に詐欺師の意図的な手口である可能性もある。最も騙されやすい人以外は、見知らぬ人

にお金を振り込む前に考え直すだろうから、より説得力のあるメッセージを作成することは、詐欺師にとっても面倒である可能性がある[50]。音声詐欺にはこれはまだ適用しない。AIが家族、友人、同僚の声を真似た電話には、少なくとも今のところ、そこまで騙されやすくない人も騙されている。今後このような手口も有名になりすぎて、明らかに偽物だということが周知の事実になるのか、有名になっても人が騙され続けるのかはまだ分からない。

フィッシングは、詐欺が依然として効果的であることを証明している。クリック率は3%程度であるため、大規模なキャンペーンの場合、少なくとも1人はほぼ確実に被害に遭う[51]。しかし、大規模なフィッシング・キャンペーンは、防御側に気付かれる可能性も高い。このことから、AIが生成するフィッシングの場合、ハッカーにとっての価値は、侵入の成功率を高めることよりも、防御側に気付かれる確率を下げることにあるのかもしれない。その場合、AIを使ったものは、送信されるフィッシング・メッセージの数が少ないかもしれない。

逆に、価値の高いターゲットを狙うことに意味があるのかもしれない。スピアフィッシングの場合、メッセージはほんの一握りで済み、手作業で簡単に書けるため、AIで生成するメリットはわずかだ。しかし、さまざまな組織をスピアフィッシングできるという利点はあるかもしれない。その意味で、注意深く作られたメッセージの量をAIで増やし、インターネット上のあちこちで価値の高いアカウントに向けて送ることは可能だろう。

マルウェア生成とハッキング

フィッシングで最初に人を引き込むのにAIが使われるかもしれないのは前述のとおりである。その後の悪意あるサイバー活動においても、特に生成AIが重要な役割を果たすかもしれない。AIはソフトウェアの一部を作成することができるため、要は単なるソフトウェアであるマルウェア作成の一端を担うこともできる[52]。現在のところ、AIのコード生成システムは、最初から最後

まで完全なマルウェアを作成することに長けていないようだ。例外があるとすれば、すべてのコードがインターネット検索で簡単に入手できるような、一般的なマルウェアであろう。それでも、新たなマルウェアの開発にかかる時間は、AIのおかげでいくらか短縮したと思われる。

しかし、フィッシング・メールと同様、マルウェアの作成は通常、より大きな作戦におけるステップの一つに過ぎない。このような作業には、多くのステップが必要であり、高度に自動化されたツールがすでに多く使われている。コンピューターやデバイスに侵入したハッカーは、近くの標的をスキャンするツール、ディレクトリやフォルダを検索するツール、何十億ものパスワードを試すツールを使う。人間は、主にそのプロセスの大部分を誘導し、正しいツールや設定を選択する。AIもツールの選択と実行を手伝うことができるかもしれないが、私たちの初期テストでは、一部の人が懸念しているほどAIはまだ器用ではないことが示唆されている[53]。

防衛におけるプログラミング

マルウェアの作成に生成AIが利用できるなら、マルウェアをブロックするために必要なアップデートやパッチの作成にもAIが利用できると考える人は多いだろう。しかし、パッチの作成はすでに比較的効率良く行われているため、AIは限られた進歩しかもたらさないだろう。防御側はすでに脆弱性を認識しており、約80%の確率で発表前にパッチを作成している。残りの20%の脆弱性についても、パッチをすぐに提供する。そのうちの80%は、最初の2カ月以内に提供されている。遅れが生じる主な要因は、パッチの作成よりも、利用者がそれを採用するスピードにある[54]。

このことを踏まえると、防御側がパッチをテストし、どれの適用が最も重要であるかを理解するのに、AIが役立つ可能性がある。また、防御側は、アップデートすることが通常の作業の妨げになるリスクがあることも理解する必要がある。アップデート

がダウンタイムやリセットを必要としたり、機能しているように見えるソフトウェアの動作を変更したりする可能性があるため、管理者はパッチの適用に躊躇することが多い。これらは、AIが解決するには難しい問題だが、対処できれば、パッチの作成を自動化するよりも多くの利益が得られる可能性がある。

検知を超えたAIによる防御

どのタイミングでどのパッチを適用すべきか、あるいはいつ、どのようにコンフィギュレーションを変更するかを決める過程は、防御側が攻撃者に対抗する戦略的なゲームのようなものだ。生成AIはゲームの遊び方に熟達していくかもしれないが、今のところその意味で最も有望なのはむしろ別のタイプのAIだ。強化学習（RL）は、デジタル・エージェントに、通常はシミュレートされた環境の中で何らかの目標を達成させるアプローチである。エージェントは行動を選択し、目標達成に向けてどれほど前進したかに基づいて、小さな報酬や罰を受け取る。これは人間の学習方法に非常に似ているが、世界最高のチェスや囲碁のプログラムを生み出した技術でもある。

ごく最近まで、RLがサイバー問題に適用されることはほとんどなかったが、その状況は変わりつつある[55]。現在では、主にファイブ・アイズやNATO諸国の防衛・情報部門による主導の下、高度な設定が可能なサイバー訓練環境がいくつか存在する。トレーニングジムのようなこれらのソフトには、誰でもダウンロードできるものもある。CybORGと名付けられたそのうちの1つは、国際的な参加者による一連の競技会の運営に使用されている[56]。

こうした取り組みは、脅威を検知するだけでなく、迅速に行動し、ネットワークやデバイスの設定を変更することができるエージェントを開発している。まだ始まったばかりであるため、テストされているネットワークは小規模で、エージェントが観測する変数の数も、エージェントが実行できるアクションの数も少ない。これらのエージェントが今後どの程度力を付けるかは不明だが、さらなる改善の余地は十分にある。これまで訓練されたエージェントは、他の分野における最先端AIシステムに比べれば、まだ未熟なものである。

国際協力の機会

日米や他の同盟国が協力できる機会は複数ある。まず、AIを防衛に応用することに関しては、まだ多くの研究が必要である。自律的なパッチ作成は一定の利益をもたらすが、それらのパッチを脆弱なネットワークにより早く適用できれば、さらに有益なものとなるだろう。また、どのコンフィギュレーションを変更し、どのデジタル・プロセスを止め、どのデバイスを隔離すべきかを確実かつ迅速に判断できる自律的な制御も、貴重なものになるだろう。これに関して言えば、RLを使った自律的なサイバー防御の開発が現在始まっているが、日本も貢献すれば、他の国際的なパートナーや同盟国から歓迎されることはほぼ間違いない。

攻撃者に目を向けると、日米には多くの共通の敵がいる。AIが脅威の規模を拡大させるのであれば、情報共有や共同で脅威ハンティングを行う機会も拡大させると言える。

攻撃の規模を拡大するには、通常、隠れたアイデンティティやデバイスを勝手に使ったボットネットなどのインフラも拡大する必要がある。また、多くの場合、同盟国を経由しなければこれらを広げることが難しい。このようなインフラは、国家間で共有できる手がかりとなる上、攻撃者がどこから来たかを追跡し、徹底的に無力化することにもつながる。AIは確かに新たな脅威をもたらすが、防衛や同盟国間の連携強化の機会も同時にもたらす可能性がある。

本稿に示された見解は筆者個人のものであり、必ずしもホワイトハウスや政権の見解を反映するものではない。

[48] Ben Buchanan, et al., "Truth, Lies, and Automation: How Langauge Models Could Change Disinformation," Center for Security and Emerging Technology (May 2021). https://cset.georgetown.edu/publication/truth-lies-and-automation/

[49] Katerina Sedova, et al., "AI and the Future of Disinformation Campaigns Part 1: The RICHDATA Framework," Center for Security and Emerging Technology (Dec 2021) https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/; Katerina Sedova, et al. "AI and the Future of Disinformation Campaigns Part 2: A Threat Model," Center for Security and Emerging Technology (Dec 2021) https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns-2/; Josh A. Goldstein, et al., "Generative Language Models and Automation Influence Operations: Emerging Threats and Potential Mitigations," arXiv 2301.04246 (Jan 2023). https://arxiv.org/pdf/2301.04246.pdf; Josh A. Goldstein, Andrew J. Lohn, "Finding Language Models in Influence Operations," Lawfare (June 20, 2023) https://www.lawfaremedia.org/article/finding-language-models-in-influence-operations.

[50] Cormac Herley, "Why do Nigerian Scammers Say They are from Nigeria?," Microsoft (Jun 2012) https://www.microsoft.com/en-us/research/wp-content/uploads/2016/02/WhyFromNigeria.pdf.

[51] "Verizon: 2021 Data Breach Investigations Report," Computer Fraud & Security 2021, no. 6 (2021): 4.

[52] Elias Groll, "ChatGPT shows promise of using AI to write malware," CYBERSCOOP (Dec 6, 2022). https://cyberscoop.com/chatgpt-ai-malware/.

[53] Lisa Lam, "Capturing the Flag with ChatGPT: Generative AI for Cyber Education," Center for Security and Emerging Technology (Jun 7, 2023). https://cset.georgetown.edu/article/capturing-the-flag-with-chatgpt-generative-ai-for-cyber-education/.

[54] Andrew Lohn, Krystal Jackson, "Will AI Make Cyber Swords or Shields?," Center for Security and Emerging Technology (Aug 2022) https://cset.georgetown.edu/publication/will-ai-make-cyber-swords-or-shields/; Andrew J. Lohn, Krystal Alex Jackson, "Will AI Make Cyber Swords or Shields: A few mathematical models," arXiv 2207.13825 (Jul 27, 2022) https://arxiv.org/abs/2207.13825.

[55] Andrew Lohn, et al., "Autonomous Cyber Defense: A Roadmap from Lap to Ops," Center for Security and Emerging Technology (Jun 2023) https://cset.georgetown.edu/publication/autonomous-cyber-defense/.

[56] The Technical Cooperation Program, "TTCP CAGE Challenge," GitHub https://github.com/cage-challenge.

生成AIがサイバーセキュリティに与える影響とそれをめぐる日米協力

高澤 美奈

はじめに

サイバーセキュリティを取り巻く環境は、拡大し続ける技術の能力によって急速に進化している。デジタル・トランスフォーメーションの時代において、大きな注目を集めている技術的進歩の1つが生成AIである。AIはサイバーセキュリティに大きな影響を与え得る。その機会と課題は、どちらも慎重な検討が必要である。さらに、国際社会がサイバー脅威に取り組む中、各国が協力し、サイバーセキュリティ強化のために生成AIの力を活用する効果的な戦略を策定することが不可欠となっている。本稿では、生成AIがサイバーセキュリティに与える影響をめぐる懸念を探り、そのポテンシャルをサイバー防衛に活用する方法を掘り下げるとともに、強固なサイバーセキュリティの枠組みを確立する上での日米協力の意義について語る。

生成AIがサイバーセキュリティに与える影響をめぐる懸念

生成AIは、画像やテキストの生成といった創造的なタスクにおいて目覚ましい能力を発揮するイノベーションであり、さまざまな領域に革命をもたらす可能性を秘めている。しかし、それがサイバーセキュリティに悪影響を与え得る可能性について、最近懸念が高まっている。生成AIを活用したサイバー攻撃はまだ洗練されたものではないが、その脅威は実際大きいものである。AIが生成したコンテンツを利用したプロパガンダや影響力工作の事例がすでに確認されており、事前対策の必要性を示唆している[57]。

ニュース記事やSNSの投稿など、説得力のあるフェイク・コンテンツを作成する生成AIの能力は、国民の信頼と情報の完全性に重大なリスクをもたらす。生成AIはおろか、AIの規制に関する世界的なコンセンサスもまだ形成されていない。生成AIが特定の政治的または個人的な目標を追求するために武器化され、社会の結束を弱体化させることを禁止できる国際的なガイドラインは存在しない。

人類の歴史を見ても、偽情報や外国に影響を与える活動は、常に情報のエコシステムを脅かしてきた。しかし、生成AIの台頭は、グローバルな情報エコシステムを弱体化する、悪意ある偽情報や誤情報キャンペーンの範囲、規模、効率を大幅に増大させる可能性がある。オンラインでの悪意ある活動は、人々の認識を操作し、選挙に影響を与え、社会的不和を広める可能性を秘めている。このような活動における生成AIの活用はより高度になっており、課題への対処が急務となっている。

大規模言語モデル（LLM）のような大きな基盤モデルの開発者は、これまで以上に高い基準を守り、責任ある形でAIが活用されることを保証しなければならない。

データサイエンティストやAIエンジニアは、AIシステムのライフサイクルを通じて責任あるAIの基準を実践し、意図とは異なる使用や悪意ある使用に対し、適切なガードレールを開発しなければならない。これが実現すれば、サイバー犯罪者が生成AIシステムを悪用できないという最良のシナリオとなるだろう。

サイバー防衛者による生成AIの活用

生成AIを取り巻く懸念は正当なものであるが、サイバー防衛関係者が使えば、強力なツールにもなり得ることを認識すべきだ。

これまでの認識は、俊敏性において攻撃者が優位に立つ、というものであった。斬新な攻撃テクニックを持つ敵は通常、余裕のスタートを切り、すぐには検知されない。しかし、AIは俊敏性の振り子を防御側に戻す可能性を秘めている[58]。AIの大きな利点の1つは、膨大な量のセキュリティ関連データを、大規模なセキュリティ専門家チームよりもはるかに迅速に処理し、文脈を付け、分析する能力にある。改善策を複数提案することもできる。この能力により、組織は潜在的な脅威、脆弱性、異常を迅速に特定し、セキュリティ・インシデントを検出し、効果的な調査を迅速に実施することができるようになる。防御側の方が俊敏性において攻撃者よりも優位に立つことになるのだ。生成AIをセキュリティ目的で適切に訓練し、情報を提供すれば、サイバー専門家の調査プロセス全体を支援することで、攻撃への対抗に要する時間を大幅に短縮し、サイバーセキュリティの全体的な態勢を強化することができる。

生成AIがもたらし得る別の機会として、熟練したサイバーセキュリティ専門家の不足への対処がある。サイバーセキュリティ業界は、需要が高まっていく一方で人材が足りず、その状況は悪化するばかりである。2025年までに、世界全体で350万人のサイバーセキュリティ職が募集される見込みであるが、これは8年間で350%の増加を示す[59]。生成AIはこのギャップの解消に貢献できる。シミュレーションと実践的なシナリオを通じて初級レベルの専門家の教育と訓練を支援することで、生成AIは有能なサイバー防衛者の人材プールを拡大することができる。高い能力を持つサイバー専門家は、雑務や反復作業から解放され、人間の創意工夫を必要とする最も重要な仕事に集中できるようになる。

日米協力における生成AIの実用化

サイバー脅威はグローバルであるため、国際的な協力が必要だ。日米のパートナーシップはこうした課題に取り組む上で有望である。日本が最近国家安全保障戦略を改定し、日本政府のサイバーセキュリティ能力強化への決意を明記したように、この新たな戦略領域における日米間協力強化の機は熟している。生成AIの影響は、サイバーセキュリティはもとより、経済・社会生活の広範な側面に及ぶと予想される。そのため、日米の協力はAIとサイバーセキュリティの関係にのみ焦点を当てるのではなく、生成AIの影響も考慮すべきである。

第一に、日米両政府は、悪意あるサイバーアクターから高度な生成AI技術を守るため、責任あるAIの実践を共同で推進すべきである。LLMのような大きな基盤モデルには、膨大なコンピューティング、エンジニアリング、そして財政のリソースが必要であるため、悪意ある行為者自身がそれを独自に開発することは困難である。タイミングが非常に重要であるため、日米両国は、悪意ある行為者に対する効果的なガードレールの開発に今から着手すべきである。米国では、責任あるAIのためのホワイトハウス自主公約（ホワイトハウス 2023年）や、米国国立標準技術研究所（NIST）のリスク管理フレームワーク（RMF）などの取り組みが、責任あるAIガバナンスの基礎を築いてきた。同様に、日本の自民党も責任あるAIの導入を促進する取り組みを主導している。日本政府は、AIガイドラインを改定し、生成AIに関する内容を盛り込んだものを2023年末までに発表する予定である[60]。しかし、AIの状況が急速に進化していることを考慮すれば、日米両国は、さまざまな分野やプレーヤーにまたがる責任あるAIの実践を合理化・促進すべきである。生成AIの開発・導入ライフサイクル全体を通じてこれを実施することが特に重要である。

第二に、日米は、AIを管理する規制・政策の枠組みが一貫していることを確認し、相互運用性を確保すべきである。AI技術が本質的にグローバルであることや、国家間の断片的な規制枠組みがイノベーションに対する大きな障壁となりうることを考えれば、規制・政策の一貫性と相互運用性は極めて重要である。

また、誰もが責任ある形でAIの恩恵を受けられるようにするには、世界中の社会がAI技術を開発・共有でき、アクセスできる状況になければならない。法域を超えて一貫性と相互運用性を確保することが取り組みの中心となるべきである。日本は、G7議長国であった際に、加盟国間の政策・規制の一貫性を確保するため、広島AIプロセスに取り組んだ。国際的な規制の相互運用性に向けた重要な第一歩となること、より一貫したグローバル・ガバナンス・システムの火付け役となることがこの取り組みに期待される。世界中で起こりうる危害やリスクを最小限に抑えつつ、AIの力を活用する上で、こうした取り組みは極めて重要である。

AIを管理するグローバルな規範の策定については、責任あるAIに向けたOECDの基礎的枠組みが有用な参考となるかもしれない。日米は、ベストプラクティスをさらに共有するため、既存の枠組みを相互参照し、生成AIの領域における政策の一貫性と規制の相互運用性を促進することができるだろう。

第三に、サイバーセキュリティにおける生成AIに対する規制を形成する上で、官民パートナーシップの重要性はいくら強調してもしすぎることはない。技術はダイナミックに進化していくものであるため、規制、標準、プロトコルが急速な技術発展に対応するためには、政府と民間企業間の協力が不可欠である。例えば、NISTのAIリスク管理フレームワークは、政府機関、市民社会団体、複数のテクノロジー・リーダーを巻き込み、コンセンサス主導で透明性の高いプロセスを通じて開発された[61]。このフレームワークは、官民パートナーシップから生まれた有用なモデルであり、日本を含む他の政府もそれを参考にすることができる。日本政府も、新たなAIガイドライン案において、「アジャイル・ガバナンス」の重要性を述べている。今の急速な技術変化を背景として規制を形成する上で、官民連携の必要性を提唱するものである。日本政府は、AIが着目されているこのタイミングを捉え、日本の従来の規制プロセスを、官民間の継続的かつ双方向のコミュニケーションを伴うプロセスに革新すべきである。

第四に、日米両政府は、この新たなAI時代において、クラウドの導入がサイバーセキュリティ協力強化の鍵であり前提条件

になるという事実を認識する必要がある。ロシアがウクライナを侵攻した直後の数日間で分かったことだが、ロシアのミサイルは、まずウクライナ政府のデータセンターを標的にした。ウクライナでは、政府データをクラウドに移すことを認める法律が、攻撃のわずか1週間ほど前に通過していた。ロシアの執拗なサイバー攻撃にもかかわらず、戦争が始まって1年半が経った今も、クラウドのおかげでウクライナ政府は機能し続けている。

つまり、データは特定の場所よりもクラウドに保存する方がはるかに安全なのである。AIが台頭し、サイバーセキュリティの態勢を機械的な速度でアップグレードし強化する必要がある現状ではなおさらのことである。次のステップとして、日米両政府は協力し、サイバーセキュリティ強化のためのクラウド導入を加速させることができるだろう。この問題の範囲と深さを考慮すれば、まずは重要インフラ事業者のような戦略的に重要なセクターから始め、クラウドへの移行を支援することができるだろう。

結論

生成AI時代の今、効果的なサイバーセキュリティの最も重要な要素は技術、政策、国際協力である。生成AIに対する懸念が残る一方で、サイバー防衛の強化における潜在的なメリットも大きい。日米の協力は国際協力の模範となるものであり、サイバーセキュリティにおいて生成AIがもたらす課題に協力して取り組むことの重要性を示している。技術革新の岐路にある今、そのリスクへの警戒を怠ることなく、生成AIの可能性を活用することが前進につながる。

---

* 本稿に示された見解や意見は筆者自身のものであり、必ずしもマイクロソフトやその関連会社、その他言及されている組織の公式な方針や立場を反映するものではない。日本マイクロソフトおよび筆者は、内容の誤り、脱落、不正確さ、および本稿で提供された情報の使用から生じるいかなる結果に対して責任を負わない。

[57] Chen May Yee, "Microsoft Interview with Tom Burt," Microsoft, June 13, 2023.
[58] Charlie Bell, "How AI will impact the future of security," LinkedIN, March 2, 2023, https://www.linkedin.com/pulse/how-ai-impact-future-security-charlie-bell/.
[59] Steve Morgan, "Cybersecurity Job Report: 3.5 million Unfilled Positions in 2025," Cybersecurity Ventures, April 14, 2023, https://cybersecurityventures.com/jobs/.
[60] "Generation AI, guidelines for businesses to be integrated by the government within the year," June 26, 2023, Nikkei, https://www.nikkei.com/article/DGX-ZQOUA2630A0W3A620C2000000/.
[61] "Governing AI: Blueprint for the Future," Microsoft, May 25, 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW14Gtw.

著者一覧

マーク・ブライアン・マナンタン　編集
パシフィック・フォーラム
サイバーセキュリティ＆重要技術担当ディレクター

エミリー・ゴールドマン博士
米サイバー軍　ストラテジスト

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

ベンジャミン・バートレット博士
マイアミ大学政治学部　助教授

アンドリュー・J・ローン
セキュリティ・新興技術センター
シニアフェロー

高澤 美奈
日本マイクロソフト株式会社　政策渉外担当部長

PACIFIC FORUM
INTERNATIONAL

pacforum.org | pacificforum@pacforum.org