www.rusi.org

RUSI

オケージョナルペーパー

英日サイバーパートナーシップの未来

Joseph Jarnecki、Philip Shetler-Jones、
Pia Hüsch

オケージョナルペーパー

193年の歴史を持つ防衛・安全保障分野の独立系シンクタンク

英国王立防衛安全保障研究所（RUSI）は、防衛・安全保障分野において世界で最も長い歴史を有する、英国を代表するシンクタンクである。RUSIのミッションは、より安全で安定した世界についての情報を提供し、影響を与え、公の議論を促進することである。RUSIは研究を柱とする組織であり、今日の複雑な課題に取り組むための実践的かつ革新的な分析を独立した立場から提供している。

1831年の創立以来、RUSIの活動は会員に支えられてきた。会員からの支援と、研究、出版、各種カンファレンスを通じて得た収入をもとに、RUSIは193年間にわたり、政治的独立を維持している。

発行年：2024年
発行者：英国王立防衛安全保障研究所（RUSI）

RUSIオケージョナルペーパー、2024年9月。ISSN 2397-0286（オンライン）

表紙画像：Ko Hong-Wei/Alamy Stock Photo

英国王立防衛安全保障研究所（RUSI）
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
登録チャリティ番号：210639

目次

略語

ACD – アクティブ・サイバー・ディフェンス
AJCCBC – 日ASEANサイバーセキュリティ能力構築センター
CAO – 内閣府（日本）
CCB – サイバー分野のキャパシティ・ビルディング
CISA – サイバーセキュリティ・インフラセキュリティ庁（米国）
CO – 内閣府（英国）
CYDEF – サイバーディフェンスイノベーション機構
DBT – ビジネス・通商省（英国）
DfT – 運輸省（英国）
DSIT – 科学・イノベーション・技術省（英国）
FCDO – 外務・英連邦・開発省（英国）
G2G – 政府間
GCAP – グローバル戦闘航空プログラム
HO – 内務省（英国）
IPA – 情報処理推進機構（日本）
ISAC – アイザック（情報共有及び分析を行う組織）
JFY – 日本の会計年度
JICA – 国際協力機構（日本）
JMoD – 防衛省（日本）
JPCERT/CC – JPCERTコーディネーションセンター
METI – 経済産業省（日本）
MIC – 総務省（日本）
MoD – 国防省（英国）
MOFA – 外務省（日本）
MSDF – 海上自衛隊（日本）
NCA – 国家犯罪対策庁（英国）
NCAB – 国家サイバー諮問委員会（英国）
NCSC – 国家サイバーセキュリティ・センター（英国）
NISC – 内閣サイバーセキュリティセンター（日本）
OEWG – オープン・エンド作業部会
PPP – 官民連携
SDF – 自衛隊（日本）
SME – 中小企業

エグゼクティブサマリー

英日サイバーパートナーシップは、複数の政策分野にまたがる運用活動が促進する、的を絞った取組みの価値を示している。今後は、英日サイバーパートナーシップが初年度の勢いを維持し、課題を乗り越え、サイバー分野の取組みがもたらすインパクトをさらに拡大するための活動を展開する必要がある。

本稿では、英日サイバーパートナーシップを分析し、その活動に影響を与える要因を検討する。また、同パートナーシップが現在の戦略的優先事項の範囲内で実施すべきさらなる活動や、活動範囲の拡大についても提言を行う。本稿の提言は以下の通りである。

- **能力開発：**日本と英国は訓練、交流、演習を通じて、人材育成における相互努力をさらに拡大していく必要がある。技術者の維持・採用に関する政策対話を継続することは、ベストプラクティスの普及にもつながる。同様に、両国が現在の取組みを深化・拡大するためには、機密情報を含む、様々な情報を安全に共有できる信頼性の高いプロセスを確立することが不可欠である。
- **官民連携：**英国と日本は、政府以外のステークホルダーが主導するサイバー分野の取組みを拡大するべきである。例えば、英日パートナーシップが発展を続けるためには、地域サイバークラスターの形成を奨励する必要がある。また、セクター別ISAC（Information Sharing and Analysis Centerの略。業界内での情報共有・連携を推進する組織）間の連携を促す活動も欠かせない。両国政府はパートナーシップを促進し、両国が競争力を持つ分野を特定することにより、商業分野におけるサイバーセキュリティ活動の拡大・支援にも積極的に取り組む必要がある。また、国家官民連携への相互の関与を促進するために展開している活動（例：Industry 100）も拡大するべきである。
- **世界的な共通利益の増進：**ASEANやインド太平洋広域には、サイバー能力構築における二国間協力を拡大し、攻撃の抑止に的を絞った支援を提供する大きな機会と意欲がある。 英国と日本は、サイバー空間におけるグローバルなルールと規範を促進するために、アトリビューション（攻撃の主体や手口、目的を明らかにする活動）に共同で取り組むなど、さらなる緊密な連携に努めるべきである。また、国際的なサイバー危機に対して、積極的な支援を提供する方法を整合させる方法も検討する必要がある。
- **サイバー・レジリエント・エコシステム：**英国と日本は、英日サイバーパートナーシップの範囲をニーズや機会に応じて継続的に拡大する必要がある。例えば「サイバー・レジリエント・エコシステム」は、政府の構造、立法、規制、レジリエンスに対する改革に協力することだと理解されているが、これも範囲とすべき分野のひとつだ。英国と日本は、サイバーセキュリティ分野の専門家が従うべき標準のアラインメントに関する検討を進め、標準や相互運用性に関する対話を年2回のペースで継続的に実施する体制を整備する必要がある。

この他、英国と日本が実施すべき活動には、協力活動に対する十分な資金の提供、サイバー教育における連携の試験的な強化、パートナーシップの進捗状況の定期的な評価等がある。

こうした提言は、本稿の以下の所見に基づいている。

- 現在、英日サイバーパートナーシップの継続・拡大に対する気運は高まっており、熱意や機会が存在する。
- サイバーセキュリティは英日関係を構成する重要な活動であると同時に、両国が安全保障や防衛等の分野で、さらなる活動を展開することを可能にするものでもある。
- 日本と英国は、両国のサイバーエコシステム改革に対する協力を拡大できるが、両国の立場は対等なものでなければならない。
- 英日サイバーパートナーシップを深化させるためには、行政構造の改革、情報セキュリティの向上、能力開発に対する日本のコミットメントが欠かせない。
- 根深い課題や障害が英日パートナーシップのスピード感や範囲に影響を与えている。

重要なのは、英日サイバーパートナーシップが現在の軌道を維持できるようにすることである。両国のステークホルダーは、英日サイバーパートナーシップには勢いがあり、取組みを拡大する余地があると考えている。この機会を捉え、無駄な活動や不要な活動を回避することで、両国は英日関係全体を進化させることができる。日本と英国がパートナーシップの拡大に取り組む中、サイバーセキュリティはパートナーシップを成功に導き、より広範な戦略的取組みを実現するための足がかりとなる。

はじめに

2012年、英国と日本は「アジア及び欧州それぞれにおいて、相手国の最も重要なパートナー」であることに合意する共同声明に署名した。[1]以来、歴代の英日政府は協力を重視し、英日関係はその恩恵を受けてきた。多様な問題に対する共通の関心は、協力の機会を次々と生み出した。両国は日英関係の重要性を再確認し、戦略的パートナーシップを拡大し続けるため、2023年5月に広島アコードに合意した。広島アコードは、両国の優先事項を次のように定め、日英関係に戦略的な枠組みを与えた。

- 技術に裏打ちされた経済的繁栄
- 気候変動等の脅威に対するグローバルな強靱性
- 防衛と安全保障、その枠組みの中での英日サイバーパートナーシップに対する具体的なコミットメント[2]

[3]英日サイバーパートナーシップは、サイバー協力の「あらゆる面」を追求する画期的な合意であり、次の3つを重要な戦略分野としている。

- 官民連携（PPP）の強化
- サイバー能力の強化
- 世界的な共通利益の増進[4]

こうした戦略的コミットメントは、英日サイバーパートナーシップの下で展開された様々な取組み、例えば日本経済団体連合会（経団連）と英国の国家サイバー諮問委員会（NCAB）との会合、日本の自衛隊と英国軍の共同訓練等にも反映されている。

合意された戦略的優先事項と具体的な活動は、英日サイバーパートナーシップを取り巻く気運が高まっていることを示すと同時に、両国が国際的な政策分野として、サイバー分野を重視していることを反映している。これまでのパートナーシップの歩みは、サイバー分野における英日間協力の価値を示している。こうした協力活動は、両国の幅広い協力関係の一例であるだけでなく、両国の他の側面、例えば防衛産業との協力や経済安全保障、レジリエンス（強靱性）を支えるものとなっている。優先すべきは、英日サイバーパートナーシップのどの取組みが効果をあげたか、それはなぜか、どうすれば両国の協力関係をさらに拡大できるかを明らかにすることである。

英日サイバーパートナーシップをさらに発展させるためには、英日両国が既存の取組みを定期的に見直し、将来の機会を探る必要がある。そのためには、両国は以下を検討しなければならない。

---

1. 日本国総理大臣, '日英両国首相による共同声明～世界の繁栄と安全保障を先導する戦略的パートナーシップ～（英語版）', 2012年4月10日, <https://japan.kantei.go.jp/noda/diplomatic/201204/10uk_e.html>, 2024年2月16日閲覧。
2. '強化された日英のグローバルな戦略的パートナーシップに関する広島アコード（英語版）', 2023年5月18日, <https://www.mofa.go.jp/files/100505906.pdf>, 2024年2月14日閲覧。
3. 同上
4. 同上

- 現在、英日サイバーパートナーシップの下でどのような活動が推進され、こうした活動は二国間の目標にどのように貢献しているか。
- 英日サイバーパートナーシップを効果的に活用することで、両国のサイバー分野の優先事項も達成できるか。
- 英日サイバーパートナーシップに関して、さらに検討すべき活動や戦略的取組みの分野は何か。

本稿では、英日サイバーパートナーシップの幅と深さを持続可能な方法で計画的に拡大することで、両国が共有する戦略的優先事項に対する対応を促進することを提案する。第I章では、英日関係と両国のサイバーエコシステムの背景を説明する。第II章では、サイバー分野の取組みの全体像を説明したのち、関係する主体とそれぞれの権限について詳述する。第III章では、英日サイバーパートナーシップの戦略的優先事項が、両国の広範な協力関係とどのように整合しているかを検証するとともに、各国のサイバー戦略をもとに新たな協力分野を探る。第IV章では、英日サイバーパートナーシップを戦略的に考察し、既存の枠組みの中で展開し得る新たな活動を提言するとともに、「サイバー・レジリエント・エコシステム」という新たな柱の導入を提案する。

方法論

本稿の執筆にあたってRUSIが実施した調査は、英国の外務・英連邦・開発省（FCDO）が出資する「インド太平洋サイバー・プログラム」の一環として行われた。RUSIは、同プログラムの実施機関であるコンソーシアムのメンバーである。

調査は2023年11月から2024年2月にかけて、迅速エビデンス評価法、半構造化インタビュー、ラウンドテーブル等の質的調査手法を用いて実施された。

- **迅速エビデンス評価法**：過去15年間に発表されたオープンソースの学術文献及び灰色文献のショートレビューを実施した。
- **半構造化インタビュー**：英国と日本の公共セクター、民間セクター、市民社会組織のステークホルダーを対象に、29件の半構造化インタビューをオンライン又は対面（ロンドンと東京）で実施した。実施期間は2023年11月～2024年2月である。インタビューデータは全て匿名化した。
- **ラウンドテーブル**：データ収集を目的としたラウンドテーブルを1度開催した。ラウンドテーブルでは、ステークホルダーがサイバーガバナンスとサイバーセキュリティに関する官民連携に対するアプローチ等のテーマについて議論した。主に日本の民間セクターから15名以上が参加し、2024年1月18日にロンドンで対面形式で開催された。

制限事項

本稿の執筆のために実施した調査では、日本語の文献又はインタビューは限定的にしか使用しなかった。ステークホルダーとの議論の一部は、日本語の話者である研究者1名が日本語で行った。調査チームはオンライン翻訳ソフトウェア（Google翻訳とDeepL）を使って、限られた日本語文献を参照した。調査チームは、英語に偏ったデータ収集では包括的な調査結果を導き出すことは難しいことを認識しており、日本のシンクタンクや学術機関によるさらなる調査を歓迎したい。

I. 英国と日本のサイバーエコシステムの形

本章では、英国と日本のサイバーエコシステムの背景と、英日サイバーパートナーシップを形成している要因について説明する。

英国と日本のサイバー体制とガバナンス

英国と日本は国際的なサイバーランキングで高い評価を得ている。国際電気通信連合（ITU）の「世界サイバーセキュリティ指数（GCI）」（2020年）では、英国は2位、日本は7位につけている。[5]一方、e-Governance Academyによる「National Cyber Security Index（NCSI）（2016〜23年）」では、英国は9位、日本は52位である。[6]日本は近年、サイバーセキュリティへの取組みを強化しているが、パートナー国は取組みをさらに加速させることを求めている。特に米国のデニス・ブレア元国家情報長官と、国家安全保障局（NSA）のポール・ナカソネ長官（当時）は、日本は同盟国やパートナー国と同等の能力を身につける必要があると強調した。[7]こうした要請を受け、日本は「国家安全保障戦略2022」において、サイバー安全保障分野の対応能力を「欧米主要国と同等以上に向上させる」と宣言した。[8]

サイバーセキュリティに対する関心が英日両国で高まっている背景には、サイバー脅威の拡大がある。2023年には、名古屋港やロンドンの大英図書館等がランサムウェア攻撃を受け、莫大な金銭的、社会的損害が発生した。[9]英国では企業に対するサイバー犯罪の損害額が年間300億ポンドを超えており、インタビューで得たデータから、日本においても相当額の損害が発生していると推測される。[10]国家支援型の攻撃も依然として脅威となっている。例えば、2020年には日本の防衛関連ネットワークが、2022年には英国の選挙委員会のシステムが、中国と関係する犯罪者グループによるハッキング攻撃を受け

5. International Telecommunication Union, *Global Cybersecurity Index 2020: Measuring Commitment to Cybersecurity* (Geneva: ITU Publications, 2021), p. 25.
6. E-Governance Academy, 'National Cyber Security Index:Archived Data from 01.09.2023', <https://ncsi.ega.ee/ncsi-index/?archive=1>, 2024年1月16日閲覧。
7. ジャパン・ニューズ, 'Defense Perspective: Proposals/Cybersecurity Command Urgently Needed to Direct Active Cyber Defense', 2022年11月22日; ジャパン・ニューズ, 'US: Japan's Cybersecurity Measures "Too Little, Too Late"', 2024年2月6日。
8. 日本国政府, '国家安全保障戦略（英語仮訳版）', 2022年12月, p. 23, <https://www.mofa.go.jp/fp/nsp/page1we_000081.html>, 2024年8月18日閲覧。
9. Alessandro Mascellino, 'Nagoya Port Faces Disruption After Ransomware Attack', *Infosecurity Magazine*, 2023年7月5日, <https://www.infosecurity-magazine.com/news/nagoya-port-disruption-ransomware/>, 2024年8月16日閲覧。大英図書館, 'Learning Lessons from the Cyber-Attack: British Library Cyber Incident Review', 2024年3月8日, <https://blogs.bl.uk/living-knowledge/2024/03/learning-lessons-from-the-cyber-attack.html>, 2024年7月24日閲覧。
10. Beaming, 'The Price of Insecurity: The Cost of Business Cybercrime in 2023', <https://www.beaming.co.uk/wp-content/uploads/2024/02/Cost-of-Cyber-Crime-in-UK-Businesses-in-2023.pdf>, 2024年8月13日閲覧。2023年12月5日に著者が東京で実施した日本政府職員へのインタビュー。

た。[11]地政学的緊張は国家間の競争を加速させ、英日両国では国家サイバー防衛に対する関心が高まっている。

英国は2016年にサイバーセキュリティに対する国家的アプローチを刷新し、中央当局として国家サイバーセキュリティセンター（NCSC）を設立した上で、NCSCを英国政府通信本部（GCHQ）の下に置いた。NCSCに対応する日本の組織は、内閣官房に設置された内閣サイバーセキュリティセンター（NISC）である。NCSCと比べると、NISCが政府全体に対して持つ影響力は限られており、関係者を集め問題解決を促進する、いわゆる「Convening Power（糾合力）」以上の権限はない。常駐職員もおらず、産業界や他の政府機関からの出向者で運営されている。[12]NCSCに比べると技術者の数も少ない。技官は情報処理推進機構（IPA）や情報通信研究機構（NICT）に所属している。[13]日本の「国家安全保障戦略2022」は、NISCを「サイバー安全保障分野の政策を一元的に総合調整する」新たな組織に再編すると明言しているが、インタビュー対象者からは、英国のNCSCをモデルにしている可能性が指摘された。[14]

英国と日本は、どちらも過去に何度か国家サイバー戦略を策定している。英国は2009年、日本は2013年に初のサイバー戦略を公表した。現在、英国が推進している「国家サイバー戦略2022」は、戦略を支える5つの柱として「国内のサイバーエコシステム」、「国家のサイバーレジリエンス」、「技術的優位性の達成」、「国際的リーダーシップの追求」、「脅威への対抗」を掲げている。[15]一方、日本の2021年のサイバーセキュリティ戦略「誰も取り残さないサイバーセキュリティ」は、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせるデジタル社会の実現」、「国際社会の平和・安定及び日本の安全保障への寄与」という3つの方向性を示している。[16]どちらの戦略も多様なステークホルダーを巻き込むことの重要性を認識しており、英国はこれを「社会全体（whole of society）」、日本は「国全体（whole of nation）」のアプローチと呼んでいる。[17]

11. Ellen Nakashima, 'China Hacked Japan's Sensitive Defense Networks, Officials Say', *Washington Post*, 2023年8月7日。Electoral Commission, 'Electoral Commission Response to Cyber-Attack Attribution', 2024年3月25日, <https://www.electoralcommission.org.uk/media-centre/electoral-commission-response-cyber-attack-attribution-0>, 2024年1月15日閲覧。
12. 日本のサイバー・ガバナンス・エコシステムの概要は、内閣サイバーセキュリティセンター（NISC）の「自由、公正かつ安全なサイバー空間を確保するために（英語版）」を参照。<https://www.nisc.go.jp/eng/index.html>, 2024年1月12日閲覧。
13. 情報処理推進機構, 'IPAについて（英語版）' <https://www.ipa.go.jp/en/about/index.html>, 2024年1月20日閲覧。サイバーセキュリティ研究所, 'サイバーセキュリティ研究所とは（英語版）' <https://csri.nict.go.jp/en/index.html?_gl=1*17yq3um*_ga*MTEzNjkxMTk3My4xNzI1MTc0NTI3*_ga_GRHV5QN75N*MTcyNTE3NDUyNi4xLjEuMTcyNTE3NDUzMC4wLjAuMA..*_ga_H10Z448G8R*MTcyNTE3NDUyNy4xLjEuMTcyNTE3NDUzMC4wLjAuMA..>, 2024年9月3日閲覧。NICT, 'NICTについて' <https://www.nict.go.jp/en/about/index.html>, 2024年9月3日閲覧。
14. 日本政府, '国家安全保障戦略', p. 24。2023年12月～2024年2月に著者が東京及びオンラインで実施した日本政府職員及び市民社会組織代表者へのインタビュー。
15. 英国政府, 'National Cyber Strategy 2022: Pioneering a Cyber Future with the Whole of the UK', 2022年12月15日最終更新, <https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022>, 2024年1月20日閲覧。
16. 日本政府, 'Cybersecurity for All（英語版）' 2021年9月, <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf>, 2024年1月18日閲覧。
17. 英国政府, 'National Cyber Strategy 2022', 同上, p 7。

サイバー分野における英日間協力の推進要因

調査参加者は、英日サイバーパートナーシップが両国で継続的な支持を得ている理由として、いくつかの要因を挙げた。

まず、複数の参加者が英日サイバーパートナーシップと広範な英日関係は相互に補強し合っていると指摘した。両国が互いのサイバー能力に対する信頼を高めることは、英日関係全体の安全性も担保する。同様に、防衛や安全保障、標準の策定等、多様な分野での協力も、サイバーセキュリティ分野における協力の深化を促す。[18]例えば、インタビューでは多くの参加者が、英日関係の発展にサイバーセキュリティ分野での協力は不可欠な成功要因であることを示す例として、日英伊による第6世代戦闘機開発プロジェクト「グローバル戦闘航空プログラム（GCAP）」を挙げた。[19]もし英日関係に対するハイレベルのコミットメントが失われれば、英日サイバーパートナーシップもまた、広島アコードが生み出した気運を失う恐れがある。例えば、GCAPのような大規模活動が重大かつ公的な問題に見舞われた場合、他の活動にも悪影響が及ぶ可能性がある。英日サイバーパートナーシップを深化させるためには、サイバーセキュリティ分野で両国が協力することの重要性を継続的に訴え、緊密な信頼関係を維持するために協力する運用分野を確立することが重要となる。そのためには、英日サイバーパートナーシップの下で実施される活動に適切な枠組みを与え、二国間交流や複数年にわたる合同演習計画など、長期的な視点を取り入れることが、英日サイバーパートナーシップがもたらす機会を活用するための重要な方法となる。

英日サイバーパートナーシップの推進要因として、複数の調査参加者が挙げた第2の要因は、地政学的アラインメントである。日本は、故安倍晋三元首相の下で、防衛と安全保障に対するアプローチを刷新し、「集団的自衛権」の解釈を変更して、「自由で開かれたインド太平洋」構想を打ち出した。[20]こうした野心的な変化を背景に、日本のサイバー戦略は「自由、公正かつ安全」なサイバー空間の実現を目標に掲げ、様々な改革を展開した。「アクティブ・サイバー・ディフェンス（能動的サイバー防御、ACD）」の導入は、その一例である（ACDに対する理解の違いについては、次の「よくある誤解」セクションを参照）。英国は自由で開かれたインド太平洋に対する支持を表明し、新国家戦略「Integrated Review Refresh 2023」において、インド太平洋地域への「傾斜」を恒久的な柱と位置づけ、英日関係を強調した。[21]日本と同様に、英国も「自由で開かれた平和かつ安全なサ

18. 2023年11月27日及び12月5日に著者が東京で実施した日本政府関係者へのインタビュー。2024年1月5～15日に著者がロンドン及びオンラインで実施した英国政府関係者へのインタビュー。
19. 2023年11月～2024年2月に著者が東京、ロンドン、オンラインで実施した英国及び日本政府関係者、民間セクター、市民社会組織代表者へのインタビュー。Nanae BaldauffとYee-Kuang Heng, 'Evaluating Japan's Defense Cooperation Agreements and Their Transformative Potential:Upgrading Strategic Partnerships with Australia and the UK', *International Relations of the Asia-Pacific* (Vol. 24, No. 2, 2023), pp. 183–215.
20. 細谷雄一, 'FOIP 2.0:The Evolution of Japan's Free and Open Indo-Pacific Strategy', *Asia-Pacific Review* (Vol. 26, No. 1, 2019), pp. 18–28.
21. 英国政府, *Integrated Review Refresh 2023: Responding to a More Contested and Volatile World*, CP 811 (London: The Stationery Office, 2023), p. 13.

イバー空間」の実現を目指している。[22]地政学的な緊張が高まる中、英日両国は国際安全保障上の重要な問題に対して共同歩調をとっており、例えばロシアによる違法な侵攻に対抗しているウクライナを支持し、台湾がレジリエンスを高められるよう支援している。[23] これまでのところ、両国の共同歩調は英日サイバーパートナーシップに恩恵をもたらしており、今後数年間で状況が変わると考える理由はほとんどない。本稿の執筆時点では、英国の労働党からも、日本の自由民主党からも、現在のコミットメントを撤回する動きは見られない。

第3に、調査に参加した日本人数名が、英国の「先行者」というイメージ、サイバー政策の様々な側面における透明性、日本との規模の類似性が英国と協力する動機になっていると指摘した。調査参加者が英国を「先行者」と見なす理由は、英国が2023年に「AI安全性サミット」を主催したこと、「ポール・モール・プロセス」を共同で主導したことによる。[24]また、英国は米国と比べて、規模、購買力、文化的態度などの点で日本に近いと見なされている。[25]サイバー政策の透明性について、インタビュー対象者が指摘したのは英国の国家サイバー部隊（NCF）の「責任あるサイバーパワーの実践（Responsible Cyber Power in Practice）」に関するガイダンスである。同ガイダンスには、英国がサイバー作戦をどのように、そしてなぜ展開しているのかがまとめられている。[26]

この他、複数の参加者が強調したのは、国内に英日サイバーパートナーシップの促進と実現に取り組む信頼できる代表者がいることの重要性である。例えば、ロンドンと東京の大使館にサイバー分野の英日協力の担当者がいたことを高く評価した。こうした職員が存在するからこそ、両国はサイバー分野に特化した対面の会合を定期的に開催できる。これが政府間協力の時間的、財政的負担を増大させやすい物理的距離というマイナス点を相殺している。

よくある誤解

英日サイバーパートナーシップは、用語の使い方の違いや互いの能力に対する認識不足の影響を受けている。

22. 英国政府, ‘National Cyber Strategy 2022’.
23. 2023年12月5日及び12日に著者がロンドン及びオンラインで実施した英国政府関係者へのインタビュー。2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。
24. 英国政府, ‘AI Safety Summit 2023’, 2023年11月1～2日, <https://www.gov.uk/government/topical-events/ai-safety-summit-2023>, 2024年1月18日閲覧。英国の外務・英連邦・開発省, ‘The Pall Mall Process Declaration: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities’, policy paper, 2024年2月6日, <https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities>, 2024年2月6日閲覧。ポール・モール（Pall Mall）プロセスは、営利目的でのサイバー侵入能力の拡散と無責任な使用に対抗するためにフランスと英国が2024年2月に開始したイニシアティブ。
25. 2023年11月27日及び12月19日、2024年2月6日に著者が東京及びオンラインで実施した日本政府関係者へのインタビュー。
26. National Cyber Force, ‘The National Cyber Force: Responsible Cyber Power in Practice’, March 2023, <https://www.gov.uk/government/publications/responsible-cyber-power-in-practice>, 2024年1月10日閲覧。2023年12月21日に著者がオンラインで実施した元日本政府関係者へのインタビュー。2023年12月4日及び5日に著者が東京で実施した日本政府関係者へのインタビュー。

英国と日本が重要な概念を異なった意味で使っているために、誤解が生じるケースが見られる。その一例が「アクティブ・サイバー・ディフェンス（ACD）」である。[27]英国におけるACDは、NCSCが主導する、大量のコモディティ型攻撃に対する介入策を指す。[28]一方、日本は「国家安全保障戦略2022」において、日本版ACD（能動的サイバー防御）を導入すると宣言し、主な活動領域として、以下の3つを挙げた。

1. 「民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有」を促進し、インシデント対応を強化する。
2. 国内の通信事業者と協力して「攻撃者による悪用が疑われる」行為を検知し、ブロックする。
3. 「未然に攻撃者のサーバー等への侵入・無害化ができるよう、政府に対し必要な権限が付与されるようにする。」[29]

日本では、この定義をもとに一部の市民社会組織から、ACDは政府による監視の範囲を拡大し、治外法権的な攻撃的サイバー作戦を可能にするものだという声があがった。その結果、ACDは日本国憲法が保障しているプライバシーや秘密通信の権利を侵害しているのではないかという疑念が広がり、日本の自衛権の行使に関する議論が巻き起こった。[30]ACDは、政治的に慎重な扱いを要する問題となり、そのために実施が遅れ、パートナーとなるはずだった民間セクターからも懐疑的な見方を示す企業が現れた。英国と日本の間でACDの定義やアプローチが異なることは、英日関係にも混乱をもたらした。一部のインタビュー対象者からは、ACDの活動に関する翻訳が混乱を招いているという声も上がった。例えば、あるインタビュー対象者は、国家安全保障戦略（日本語版）の「侵入・無害化」という文言が、英語版では「penetrate and neutralize（侵入し、そして無害化する）」と訳されているが、もとの日本語では、この文言は必ずしも「そして（and）」の意味を含まないと指摘した。[31]

言語の壁は、戦略や政策の枠組みに対する理解にずれを生み出し、このずれは大なり小なり、運用レベルでも混乱を引き起こしている。英国と日本は、どちらも外国語の学習能力では高い評価を得ているとは言いがたい。特定の英単語が、日本語では微妙に異なる複数の言葉に訳されているケースも見られる。例えば、「information sharing」という広い意味合いを持つ英語が、日本語では「情報交換」（情報を交換しあう）と「情報共有」（情報に対して共通の所有権を持つ）の両方に訳されることがある。逆に、英語が日本語に翻訳されず、そのままカタカナで表記されるケースもある。例えば「attribution」をその

27. 2023年12月4日に著者が東京で実施した日本政府関係者へのインタビュー。
28. 英国のACDプログラムは、コモディティ型サイバー攻撃（高い技術力を持たない攻撃主体でも使える、一般的に入手可能なツールやテクニックを利用した攻撃）による被害を減らすことを目的としたツールやサービスを提供する。参照：National Cyber Security Centre (NCSC), 'Active Cyber Defence', <https://www.ncsc.gov.uk/section/active-cyber-defence/introduction>, 2024年3月3日閲覧。
29. 日本政府、'国家安全保障戦略', 2022年, p.23。
30. 日本政府、「日本国憲法（英語版）」第13条及び21条, 1946年11月2日, <https://japan.kantei.go.jp/constitution_and_government_of_japan/constitution_e.html>, 2024年1月15日閲覧。Wilhelm Vosse, 'Japan's Gradual Shift from Passive to Active Cyber Defense:Evidence from the Domestic Discourse and International Cooperation', *Études Françaises de Renseignment et de Cyber* (Vol. 1, No. 2, 2024), pp. 89–106.
31. 2024年2月13日に著者がオンラインで実施した日本の民間セクター代表者へのインタビュー。

ままカタカナで「アトリビューション」と訳す場合、これが日本語の「特定」（specify）を意味するのか、「帰属」（attribute）を意味するのかはあいまいになる。[32]こうした微妙な違いを認識し、コミュニケーションの細部にまで注意を払うことが、こうした問題を緩和し、英日サイバーパートナーシップに対する両国の期待を管理する助けとなる。

調査参加者の多くは、あらゆる分野で日本のサイバーセキュリティ能力を低いと評価した。その根拠として、多くの参加者が指摘したのは、よく知られている日本の情報セキュリティ、特に防衛分野の情報セキュリティに関する問題である。[33]とはいえ、見過ごされやすいが日本が高い能力を持つ分野もある。[34]例えば日本では複数の省庁が2010年代初頭から官民連携を推進している。具体的には、経済産業省の「サイバー情報共有イニシアティブ（J-CSIP）」、防衛省の「サイバーディフェンス連携協議会（CDC）」、警察庁の「日本サイバー犯罪対策センター（JC3）」などだ。[35]また、外務省が所管する国際協力機構（JICA）は、東南アジア諸国連合（ASEAN）と協力し、域内諸国の政府及び重要インフラ分野のセキュリティ人材を育成する拠点として、「サイバーセキュリティ能力構築センター」を設立した。[36] 日本のサイバーセキュリティ能力、特に情報セキュリティ分野の能力に対する懸念は十分に根拠のあるものであり、広く知られている。しかし、日本のサイバー能力を一面的にしか捉えていないと、日本の進歩を過小評価し、対等な協力関係の構築は不可能だという印象を与えかねない。全てのサイバー攻撃を完璧に防いだ国はない。持続可能で成熟した英日サイバーパートナーシップを実現するためには、両国が改善すべき点を正直に認めた上で、既存の強みや新たな強みが互いのレジリエンスをどのように高め得るかを評価する必要がある。

32. 参照例：「国家のサイバー攻撃とパブリック・アトリビューション ：ファイブ・アイズ諸国のアトリビューション連合とSolarWinds事案対応」瀬戸 崇志 政策研究部グローバル安全保障研究室 第179号 2021年7月15日, <https://www.nids.mod.go.jp/publication/commentary/pdf/commentary179.pdf> 2024年8月10日閲覧。
33. 参照例：Kaori Kaneko, Tim Kelly and John Geddie, 'The Glitch in Japan's Plans to Bolster U.S. Defence', *Reuters*, 2024年4月26日。高橋浩祐, 'Why Japan is Lagging Behind in Cyber Defense Capabilities', *The Diplomat*、2024年5月24日。
34. Christopher B Johnstone, 'Japan's Transformational National Security Strategy', CSIS,2022年12月8日。
35. 山口嘉大, 'サイバー防衛における官民連携の強化について―エストニア共和国との比較を通じて（英語版）', NIDS Journal of Defense and Security, 2019年12月20日。警察庁,「日本サイバー犯罪対策センター（JC3）との連携」, <https://www.npa.go.jp/bureau/cyber/what-we-do/ppp/ppp-jc3.html>, 2024年7月25日閲覧。
36. ASEAN Japan Cybersecurity Capacity Building Centre, 'Who We Are', <https://ajccbc.ncsa.or.th/>, 2024年7月25日閲覧。2023年12月5日～2024年2月6日に著者が東京及びオンラインで実施した日本政府関係者へのインタビュー。

II. サイバーエンゲージメント：これまでの歩み

本章では、サイバー分野における英国と日本の協力活動を概観し、その構成と意図を評価する。

パートナーシップ活動と関与する主体

表1は、英国と日本がサイバー分野で展開している協力活動をまとめたものである。それぞれの活動について、関係する主体と協力のタイプ、英日サイバーパートナーシップの各テーマとの関連性を示した。

表内に記載した活動は、インタビューや公開情報をもとにピックアップしたものである。著者の知る限り、英日サイバーパートナーシップの下で展開されている活動の網羅的又は概要的なリストは存在しない。本表は、サイバー分野における英日間協力と合理的に関連付けられる活動を集め、テーマ、タイプ、責任主体を整理することで、英日サイバーパートナーシップの全体像を明らかにすることを目指したものである。表の内容は両国政府の確認を得たものではなく、機密扱いの情報も反映されていないため、パートナーシップの下で展開されている活動の公式なリストではない。従って、このリストに基づく推定は、リストが包括的ではない可能性を踏まえて、慎重に行わなければならない。

表1： サイバーパートナーシップ活動の概要：2023～24年

テーマ	タイプ	主体	活動
官民連携	「社会全体の取り組み（Whole-of-society approach）」による対話	CO、外務省、FCDO、NCAB、経団連	経団連が英国を訪れ、国家サイバー諮問委員会（NCAB）と会合し、協力覚書を締結[37]
		FCDO、DBT、DSIT、NCSC、IPA、学生	日本の産業サイバーセキュリティセンター（ICSCoE）が英国を訪問
		在日英国商業会議所（BCCJ）	英国と日本の民間企業による会議
	商業	DBT、FCDO	英国のサイバーセキュリティ通商使節団が来日
	技術	NCSC、日本サイバーディフェンス	日本サイバーディフェンスが NCSC の「サイバーインシデント・レスポンス（CIR）」認定を取得
		NCSC、富士通 UK、日本サイバーディフェンス	日本サイバーディフェンスと富士通 UK が「Industry 100」スキームに参加
能力開発	地方レベルの協力活動	Cyber Wales、Cyber Hiroshima	日本初のサイバークラスターの創設を支援
	演習	自衛隊、英国軍	NATO サイバー防衛協力センター（CCDCOE）が合同サイバー防衛演習「ロックド・シールズ 2024」を実施
		防衛省、MoD、自衛隊、英国軍	多国間サイバー防衛演習「2023 ディフェンス・サイバー・マーベル 2」、「2024 ディフェンス・サイバー・マーベル 3」、日本の多国間サイバー防護競技会「Cyber KONGO」に参加
		自衛隊／防衛省、MoD	日本が英国軍の「Cyber Spartan」演習を視察
	意識・スキル向上	FCDO、外務省	サイバースキルに関するコミットメントを含む、英日間の人的交流に関する協力覚書
		防衛省／自衛隊、英国の防衛企業	防衛省／自衛隊の訓練契約を英国のサイバーセキュリティ企業が受注
		FCDO、外務省	ジャパン・サイバー・フェローシップ（5 人の日本人がクランフィールド大学のサイバー政策・戦略に関する 5 週間のコースに参加）
		FCDO、Cyber Hiroshima、学校	日本の学校で「サイバー・ファースト・コンペティション」を試験開催

37. 国家サイバー諮問委員会及び経団連、‘サイバー分野における官民連携に関するNCABと経団連の協力覚書’, 2024年1月17日, <https://www.keidanren.or.jp/en/policy/2024/003.html>, 2024年2月10日閲覧。

テーマ	タイプ	主体	活動
世界的な共通利益の増進	多様なステークホルダーの関与	慶応義塾大学、日本政府、FCDO、MITRE Corporation	第13回サイバーセキュリティ国際シンポジウム英国を含む複数の国際パートナーによる多国間連携
		HO、日本経済新聞社、英国と日本の産業界	日経主催のカンファレンス「サイバーイニシアチブ東京」英国を含む複数の国際パートナーによる多国間連携
		サイバーディフェンスイノベーション機構、英国と日本の産業界及び市民社会組織	CYDEFカンファレンス英国を含む複数の国際パートナーによる多国間連携
	多国間フォーラムにおける協調	外務省、FCDO、NCSC	営利目的のサイバー侵入攻撃に対抗するポール・モール・プロセスへの参加。日本を含む複数の国際パートナーが参加する多国間協力
		FCDO、外務省、HO	OEWGやサイバー犯罪条約策定に関するアドホック委員会等、国連プロセスへのアプローチに関するコミュニケーション
		HO、NCSC、NISC、警察庁	「カウンターランサムウェア・イニシアティブ会合」に他50カ国超と共に参加。
		HO、警察庁	「国際詐欺サミット」に他11カ国と共に参加
		DSIT、総務省	オーストラリア、米国、カナダと共に「電気通信に関するグローバル連合」の設立に関する共同声明を発表
		DfT、NISC	「世界海上輸送システムサイバーセキュリティ会議」に英国と日本が他20カ国以上と共に参加
	抑止力／国際基準	FCDO、外務省	サイバー空間における国際法に関する共同声明
		FCDO、外務省	関係組織間における非公式なサイバー脅威情報の共有による抑止力の向上
		FCDO、外務省、NISC、警察庁	日本と英国、他数カ国が中国政府系ハッカー集団「APT40」に関する技術アドバイザリーに共同署名ハッカー集団「APT31」に対する英国のアトリビューションを日本が支持[38]
	サイバー分野のキャパシティ・ビルディング	FCDO、外務省、JICA	2024年2月、英国が出資する研修コースをAJCCBCを通じて実施。

38. NCSC, 'The NCSC and Partners Issue Alert About Evolving Techniques Used by China State-Sponsored Cyber Attackers' 2024年7月9日, <https://www.ncsc.gov.uk/news/ncsc-and-partners-issue-alert-about-evolving-techniques-used-by-china-state-sponsored-cyber-attacks>, 2024年7月10日閲覧。英国政府, 'UK Holds China State-affiliated Organisations and Individuals Responsible for Malicious Cyber Activity', プレスリリース, 2024年3月25日, <https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity>。2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。

テーマ	タイプ	主体	活動
サイバー・レジリエント・エコシステム	標準・規制の統一	NCSC、NISC、CO	英国と日本、他 18 カ国が「セキュア AI システム開発ガイドライン」に共同署名
		DSIT、内閣官房デジタル市場競争本部事務局（日本）	アプリのセキュリティ及びプライバシーの確保に関する共同声明 [39]
		NCSC、JPCERT/CC、NISC	米サイバーセキュリティ・インフラセキュリティ庁（CISA）が主導する、ソフトウェア開発等における「セキュア・バイ・デザイン」ガイダンスに他 10 カ国以上と共に貢献 [40]
		NCSC、警察庁、JPCERT/CC	CISA が主導する市民社会組織のためのサイバー脅威緩和に関するガイダンスに他の 3 カ国と共に貢献
	政府間対話	NISC、自衛隊／防衛省、外務省、MoD、FCDO 他	各国のサイバー構造とアプローチについて議論
		FCDO、MoD、外務省、防衛省	第 5 回日英外務・防衛閣僚会合 [41]
		DSIT、経済産業省、NCSC	両国の制度の相互承認、標準、規制について議論（例：IoT 製品のセキュリティやサイバースキルの同等性）

39. Department for Science, Innovation and Technology, ‘Joint Statement Between the United Kingdom and Japan on Ensuring App Security and Privacy’, 2023年2月28日, <https://www.gov.uk/government/publications/joint-statement-between-the-united-kingdom-and-japan-on-ensuring-app-security-and-privacy>, 2024年1月16日閲覧。
40. 米国サイバーセキュリティ・インフラセキュリティ庁他, ‘Secure by Design: Shifting the Balance of Cybersecurity Risk:Principles and Approaches for Secure by Design Software’, 2023年4月, <https://www.cisa.gov/sites/default/files/2023-10/Shifting-the-Balance-of-Cybersecurity-Risk-Principles-and-Approaches-for-Secure-by-Design-Software.pdf>, 2024年1月18日閲覧。
41. 外務省, 第5回日英外務・防衛閣僚会合（英語版）, 2023年11月7日, <https://www.mofa.go.jp/press/release/press4e_003333.html>, 2023年11月15日閲覧。

テーマ	タイプ	主体	活動
その他		CO、FCDO、CAO、デジタル庁（日本）	英国副首相が来日
		NCSC、国家安全保障局（日本）、総務省、外務省、NISC、警察庁	NCSC 長官が来日
		自衛隊、海上自衛隊、英国軍、防衛省、MoD	年次会合、幕僚協議等、日英両国の軍事・防衛組織高官の会合を定期的に開催。主なテーマは能力、人材、脅威。ジム・ホッケンハル大将、木村顕継陸将補、加藤康博空将補等、軍事・防衛組織高官が訪問
		外務省、FCDO が主導	年次サイバー対話
		日本のデジタル庁、英国の政府デジタルサービス、中央デジタル・データ・オフィス、NCSC	公共セクターにおける AI の活用、ゼロ・トラスト・アーキテクチャ、インシデント対応について議論
		国家安全保障局副局長が率いる省庁横断的な日本代表団	「CYBERUK 2024」カンファレンスに他数カ国と共に参加

出所：インタビューと公開情報をもとに著者が作成。

注：表内の略語は本稿の冒頭に掲載した「略語」リストを参照。「テーマ」には英日サイバーパートナーシップの優先事項（官民連携、能力開発、世界的な共通利益の増進）に「ガバナンス」と「その他」を追加した。

英日サイバーパートナーシップの成熟に合わせて、実施とリソースの確保の透明性向上も検討する必要がある。例えば、現時点ではパートナーシップのモニタリングやリソースの確保に関する情報はほとんど公表されていないが、公的に合意されているマイルストーン等には、パートナーシップのコミットメントを果たすためにはリソースの確保が重要であると明記してもよい。透明性が高すぎれば、コミットメントが骨抜きになったり、曖昧になったりするリスクはあるが、それでも両国は英日サイバーパートナーシップの詳細を明確に伝えることを検討する必要がある。

活動のテーマ

表1が示しているように、サイバー分野の協力活動は英日サイバーパートナーシップの優先分野とおおむね一致している。

パートナーシップのテーマのうち、最も多くの活動が行われているのは「世界的な共通利益の増進」と「能力開発」である。この2つは、調査参加者が協力の重要性を指摘した分野でもあった。調査参加者によれば、この2つの分野には明確な役割と動機を有する実施主体が複数存在し、それぞれがコミットメントを果たすためにリソースの確保を強化しているという。例えば、日本と英国はランサムウェア対策イニシアティブやOEWG等の共に参加している国際的フォーラムにおいて、緊密に連携してきた。しかし、おそらくもっと重要なのは、ポール・モール・プロセスやサイバーセキュリティ国際シンポジウムといったミニラテラル（少数国で構成する協力枠組み）な取組みへの参加や支援を優先してきたことだろう。同様に、データ収集の結果、両国は能力の構築・強化を目的とした共同演習や、スキル構築のための取組みに重点を置いていることも分かった。

多国間プラットフォームを通じて「世界的な共通利益の増進」を図る活動は、既存の取組みを強化したもので、英日サイバーパートナーシップは協力をゼロサム的な観点では捉えていないことを示している。つまり、サイバー分野における英日間協力は、他の国との活動を妨げるものではなく、また妨げることもできない。[42]「能力開発」に関する取組みは、防衛と安全保障の分野に集中している。特に、合同サイバー防衛演習「ロックド・シールズ」に英国と日本が合同チームを編成して参加したことが、能力構築や信頼の向上、両国の共同歩調を世界に示す活動として強調された。[43]しかし一部の英国政府関係者からは、作戦活動に十二分な数の人員を投入することが難しいという理由から、今後も合同チームを組成して演習に参加できるかどうかは分からないという声が上がった。[44]リソースの確保に関する懸念は、調査参加者からは頻繁には上がらなかった。調査チームでは、英日サイバーパートナーシップの優先順位はトップダウンで決められているためリソースを確保する上での障害が少なかったこと、又は活動に要する費用がそこまで多くなかったことをその理由と結論した。英日サイバーパートナーシップが今後も現状の意欲をもっ

42. 2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。2023年12月5日に著者が東京で実施した市民社会組織代表者へのインタビュー。
43. 2023年12月4日に著者が東京で実施した日本政府関係者へのインタビュー。2023年12月5日に著者が東京で実施した英国政府関係者へのインタビュー。
44. 2024年1月12日に著者がオンラインで実施した英国政府関係者へのインタビュー。

て続けられる場合、サイバー分野の人材不足がリソース確保の問題を悪化させる可能性がある。

「官民連携」に関する活動は、両国がさらに緊密に協力できる可能性を示しているが、これまでのところ、活動の担い手は主に英国で活動している日本企業である。これは、日本に拠点を置く英国企業が比較的少ないことが一因だと調査チームは分析している。

調査チームは「サイバー・レジリエント・エコシステム」というテーマを追加し、国レベルの改革を支援する活動や、標準・規制に関する活動を分類した。このテーマに分類できるのは、既存又は進行中の活動のみであり、この分野におけるパートナーシップの重要性を指摘した調査参加者の知見が反映されている。[45]特に重要なのは、構造改革やセキュアAI、標準化といった分野でのカウンターパート同士の議論である。英国と日本はどちらも、EUのような超国家的な規制機関には所属しておらず、米国や中国のような市場支配力も持たない。規制やアプローチに関する対話を増やすことは、英国と日本が世界的な逆風に影響を与え、学びやベストプラクティスを共有し、パートナーシップをさらに深化させる機会を生み出す。

活動のタイプ

本稿では、特定した英日間の協力活動を12のタイプのいずれかに割り当てた。その目的は、活動をグループ化し、合理化することで、英日サイバーパートナーシップが協力体制をさらに強化できるよう支援することである。繰り返すが、本表に掲載した活動のリストは決定的なものではなく、タイプの多様性には英日サイバーパートナーシップが多様で包括的な取組みを目指していることが肯定的に反映されている。以下のセクションでは、各タイプの代表的な活動を説明する。

予想通り、政府間対話に関する活動は多岐にわたり、防衛や安全保障といった慎重な扱いを要する問題を含む、様々なテーマに及んだ。両国が相互理解を深め、さらなる協力の機会を探るためには、実のある対話を定期的に実施することが重要となる。定期的な政府間対話やマルチステークホルダー対話は、他の活動も促進する。調査データが示しているように、標準や製品の安全性に関する共同合意のような活動は、初期の広範な議論から生まれることが多い。英国の科学・イノベーション・技術省（DSIT）と日本の経済産業省の対話は、その一例である。[46]

以下は、調査参加者がさらなる協力活動を展開する機会があると指摘した活動のタイプである。[47]

- **技術**：調査参加者は、英国のNCSC等はサイバーセキュリティ企業の技術保証や認証制度を加速できる可能性があると指摘した。これまでの活動は日本企業の英国進出を

45. 2023年12月4日～2024年2月13日に著者がロンドン、東京及びオンラインで実施したステークホルダー集団へのインタビュー。
46. 2023年12月19日に著者がオンラインで実施した日本政府関係者へのインタビュー。
47. 2023年12月1日～2024年2月13日に著者がロンドン、東京及びオンラインで実施したステークホルダー集団へのインタビュー。

促進し、英国の消費者に便益をもたらした。この活動を発展させ、今後は英国企業の日本進出を後押しすることもできる。[48]

- **抑止力／国際基準**：英国のステークホルダーは、このタイプの活動を特に重視していた。英国は、緊密なパートナーシップ関係にある国々との共同アトリビューションはインパクトが大きいと考えている。[49]日本の政府関係者からは、アトリビューション活動を拡大したいという声とともに、精度の重要性を強調する声が頻繁に聞かれた。[50]一部の調査参加者は、日本にはアトリビューションを支える技術的評価の実施能力がほとんどないと述べ、また情報セキュリティ上の懸念から、データを日本と共有することに慎重な立場を示した。[51]一方、日本の政府関係者は機密情報を含むさらなる情報へのアクセスを希望した。日本政府は現在、警察庁やNISC、JPCERTコーディネーションセンター（JPCERT/CC）、IPAから情報を得ている。こうした情報は政治上の意思決定にも活用できる。このタイプの活動に対する協力を拡大することは、技術というより、政治の問題である可能性が高い。
- **地方レベルの協力活動**：英国と日本の地域サイバークラスター間の協力関係、具体的にはCyber Hiroshimaと Cyber Walesの関係は、調査チームを驚かせた。2つの組織はベストプラクティスの共有や共同活動を積極的に推進し、パートナーシップに熱心に取り組んでいる。このモデルは双方に明確な価値をもたらしている。
- **商業**：日本と英国はどちらも先進的なデジタル経済を有し、ロボット工学、スマートシティ、AI等のハイテク分野で活発に活動している。こうした産業にとって、サイバーセキュリティは重要な問題であり、データ収集の結果、両国の企業には相手国のカウンターパートと組んで、製品やサービスを輸出したり、購入したりする機会があることが分かった。[52]今回のデータ収集では詳細な市場調査は実施していないが、両国の通商関連省庁がこうした情報を作成・公表し、企業を支援することが望ましい。
- **サイバー分野のキャパシティ・ビルディング（CCB）**：英日両国の調査参加者は、新たな協力の機会がある分野としてサイバー分野のキャパシティ・ビルディング（CCB）を挙げた。[53]JICAとFCDOは、CCBに関して国際的に高い評価を得ている組織である。2024年2月には、英国が資金を提供した訓練コースが日ASEANサイバーセキュリティ能力構築センター（AJCCBC）を通じて実施された。こうした活動は、人材育成を重視する日本の姿勢とも一致しており、このタイプの活動には両国が協力できる余地があることを示している。

調査チームは、上記の分野では現在、活発な活動が行われておらず、そのことが逆に、上記の分野には機会があると研究参加者が考える一因になっている可能性もあると指摘している。

48. 2023年12月5日に著者が東京で実施した英国の民間セクター代表者へのインタビュー。2024年1月18日にロンドンで開催されたデータ収集ラウンドテーブル。
49. 2023年12月5日及び11日に著者が東京及びオンラインで実施した英国政府関係者へのインタビュー。
50. 2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。
51. 2023年12月5～9日に著者が東京及びオンラインで実施した英国政府関係者へのインタビュー。
52. 2023年12月5日～2024年2月13日に著者が東京、ロンドン及びオンラインで実施した英国及び日本の民間セクター代表者へのインタビュー。
53. 2023年12月4～5日に著者が東京で実施した日本政府関係者へのインタビュー。2023年11月24日～12月5日に著者が東京、ロンドン及びオンラインで実施した英国政府関係者へのインタビュー。2024年1月18日にロンドンで開催された情報収集ラウンドテーブル。

関与する主体

表1の活動に関与している主体は多岐にわたる。これはサイバー分野における協力は分散的であり、多くの組織は相手国のパートナーとの関係を独自に構築し、維持していることを示している。これは複数の政府関係者の証言でも裏付けられている。例えばその中の一人は、内閣サイバーセキュリティセンター（NISC）を改革する前に、日本は政府全体で取り組んでいくことが望ましいと述べた。[54]特定の組織が全体を縫製するという中央集権的な体制にもメリットはあるが、複数の分野で英日間協力を加速させるためには、幅広い政府機関が相手国のカウンターパートと直接接点を持つ必要がある。英日間協力をどこまで中央集権的なものにするかを決めておくことも重要だ。過度の中央集権化は組織間の協力を阻み、スピードを遅らせる可能性があるが、逆に分散化しすぎれば活動がサイロ化し、両国が共有する戦略的優先事項とのずれが生じる恐れがある。また、全体の活動を牽引する中央集権的なイニシアティブが少なすぎれば、英日間協力に関与しない政府機関が生まれる可能性もある。例えば、英日サイバーパートナーシップに関する議論において、調査参加者が日本の情報処理推進機構（IPA）に言及することはほとんどなかった。

英日間協力については、役割や責任が釣り合うカウンターパートが存在しない場合があることも問題視されている。[55]例えば日本では、パブリック・アトリビューションの調整は国家安全保障局が担い、技術情報は警察庁やその他のインテリジェンス機関が提供し、外交的な影響に関する助言は外務省が行う。これに対して、英国では政治的責任は外務・英連邦・開発省（FCDO）が担い、技術的な助言は国家サイバーセキュリティセンター（NCSC）が行う。実際には、政策や運用上の課題によって、各省庁や機関のカウンターパートは異なる場合がある。

英日サイバーパートナーシップが有効に機能するためには、両国のカウンターパート組織の間をとりもち、円滑な連携を支援する調整役が欠かせない。こうした調整役が存在しない場合、適切なカウンターパートを見つけ連携することができず、協力関係が損なわれる恐れがある。

機関・部門横断的なキャリアパスがあれば、異なる政府部門でサイバー政策の様々な側面に取り組んでいる主体間の対話を強化できる。サイバーのような広範なテーマに取り組むためには、政府部門のサイロ化を回避しなければならない。英国は、こうした仕組みをすでに整備しており、公務員はサイバー関連機関の間を異動できる。例えば、国家犯罪対策庁（NCA）からNCSCや国家サイバー部隊（NCF）への異動も可能だ。[56]日本では一時的な出向という形をとることが一般的だが、サイバー分野に特化したキャリアパスを設ければ、政府はサイバー分野の人材を強化し国際協力を促進できるだけでなく、職員も複数のポストを経験し、信頼と能力を高められる。

54. 2024年2月6日に著者がオンラインで実施した日本政府関係者へのインタビュー。
55. 小川秀俊及び土屋大洋, ‘Cybersecurity Governance in Japan’, *International Journal of Cyber Diplomacy*(Vol. 2, 2021年)。
56. 2023年12月11日に著者がオンラインで実施した英国政府関係者へのインタビュー。

その他の検討事項

本セクションでは、英国と日本の協力活動の発展と優先順位を形成した、その他の検討事項について概説する。

- **私的なネットワークが活動の広がりを支援**：一次データを収集した結果、一部の活動は両国の担当者間に個人的なつながりがあり、協力の機会を共同で探ることで実現したことが分かった。特に、年次サイバー対話への参加がこうした関係の構築に重要だったという指摘があった。この指摘を踏まえると、資金面の制約から対話に参加できなかったという回答が一部の政府関係者から上がったことは憂慮すべき事態と言える。[57]政府は費用対効果を確保すべきだが、個人レベルの関係は英日間協力にプラスの影響を与える。英国と日本の地理的、言語的距離は両国が協力する上での障害となりかねない。特に予算が限られている場合、政府関係者は活動に参加するためのリソースをまかなえない可能性がある。必要なリソースの規模を考えると、これを確保できるかどうかは政治的な意思に左右される可能性が高い。しかし英日サイバーパートナーシップに対するハイレベルのコミットメントが続く限りは、相応の資金が提供されるはずである。
- **協力の形は様々**：表1では、英日間の協力活動をカテゴリーごとにまとめ、整理して表示している。この方法は、英日サイバーパートナーシップの全体像をつかむ助けにはなるが、両国の関係には個別の活動からは見えてこないものもある。例えば「サイバー・レジリエント・エコシステム」に分類された活動は少なかったが、一部の高官はこの分野を最優先事項に挙げた。これは優先順位が具体的な活動に適切に反映されなかった可能性もあるが、収集したデータが示しているのは、むしろこのテーマに対する取組みは具体的な活動に依存しない可能性だ。つまり、個々の活動を列記するだけでは、英日サイバーパートナーシップを十分に評価することはできない。複数の日本のステークホルダーが英国の構造や法律を模範と見なし、その理由として両国の類似性や親密な英日関係を挙げた。[58]また、「世界的な共通利益の増進」に分類された活動とは別に、表には掲載されていないが、様々なフォーラムにおいて非公式の小規模でアドホックな協力活動も定常的に行われている。
- **一部の分野では影響は限定的**：協力の機会を増やしたからといって、より多くのインパクトを生み出せるとは限らない。サイバー分野の取組みであっても、英日間協力に適さないものは効率が悪いか、不利に働く可能性がある。その一例が、サイバー犯罪捜査における業務協力の形式化である。実際問題として、英国の国家犯罪対策庁（NCA）が扱う事件と日本の警察庁が扱う事件が重なることはほとんどない。ごくまれに関連する事件があっても、当局同士の連携は特定の業務上の目的を果たすための一時的なものにとどまる。[59]こうした限定的な協力活動をあえて形式化しようとするのは、善意に

57. 2023年11月24日～12月13日に著者が東京、ロンドン及びオンラインで実施した英国政府関係者へのインタビュー。2023年11月27日～2024年2月6日に著者が東京及びオンラインで実施した日本政府関係者へのインタビュー。
58. 2023年11月5日及び12月21日に著者が東京及びオンラインで実施した日本の市民社会組織代表者へのインタビュー。2024年1月12日に著者がオンラインで実施した英国政府関係者へのインタビュー。2023年11月27日～12月19日に著者が東京及びオンラインで実施した日本政府関係者へのインタビュー。
59. 2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。2023年11月24日に著者がオンラインで実施した英国政府関係者へのインタビュー。

よるものであっても、リソースの有効活用にも効率化にもつながらない。英国と日本とでは、サイバー犯罪の脅威の状況は違う。この違いは両国が国家として直面している脅威の違いにもある程度反映されている。日本は、中国や北朝鮮からのサイバー脅威に注目しているが、英国はロシアからの攻撃への対応を優先することが多い。その結果、両国間の情報共有は的外れなものになる可能性がある。しかし、多くの調査参加者はこの違いを付加的なものと捉えていた。[60]情報共有が可能であれば、得た情報を自国のサイバー防御の強化に活用できる。[61]英国と日本の政府関係者は、価値ある協力関係を拡大できる余地が一定以上ある分野を模索する必要がある。

60. 2023年11月5日及び17日に著者がオンラインで実施した市民社会組織代表者へのインタビュー。
61. 米国と日本による同様のイニシアティブについては、以下を参照：朝日新聞, 'Japan to Give U.S. the Data it Gathers for Active Cyberdefense', 2024年7月24日, <https://www.asahi.com/ajw/articles/15359703>, 2024年7月25日閲覧。

III.戦略的アラインメント

本章では、既存の活動の背景を説明するとともに、現在の英日サイバーパートナーシップのコミットメントが、英日関係全体の優先事項とどのように一致しているかを評価し、両国の国家戦略に基づいて、さらなる協力の機会を探る。

サイバーパートナーシップと広島アコードのアラインメント

英日サイバーパートナーシップの重点項目は次の通りである。

- 官民連携の強化
- サイバー能力の強化
- 世界的な共通利益の増進

前述したように、この3つの優先事項は本稿で取り上げてきたサイバー分野の協力活動とおおむね一致している。例外は、著者が新しい分野（サイバー・レジリエント・エコシステム）に関連付けた活動と、「その他」に分類された一握りの活動（全て政府間対話）のみである。

英日サイバーパートナーシップの創設を呼びかけた広島アコードは、以下を約束している。

1. 「世界の平和と安定の擁護のため、共通の安全保障上の能力を強化する」
2. 「共有の繁栄を創出し、貿易及び投資を増加させるため、両国の経済関係の深化にコミットする」
3. 「全ての人にとって、より良く、より持続可能な未来を実現するための国際的な取組を主導する」[62]

英日サイバーパートナーシップは、3つのカテゴリーの1つ目で言及されている。このことからも分かる通り、英日サイバーパートナーシップの重点領域は防衛と安全保障である。表1に掲載した活動では、自衛隊と英国軍の合同演習などがこれに当たる。しかし、意識の向上やスキル開発、標準や規制のアラインメントに関する活動が示唆しているように、英日サイバーパートナーシップの範囲は防衛と安全保障にとどまらない。この結論は、政府関係者との議論でも裏付けられた。[63]英日サイバーパートナーシップは当初、防衛と安全保障に焦点を合わせたものだったが、現在は非公式ながらも広島アコードの他の優先事

62. ‘強化された日英のグローバルな戦略的パートナーシップに関する広島アコード（英語版）’, pp. 1–2.
63. 2023年11月27日～2024年2月11日に著者が東京、ロンドン及びオンラインで実施したステークホルダー集団へのインタビュー。2024年1月18日にロンドンで開催されたデータ収集ラウンドテーブル。

項、例えば「経済的繁栄」や「グローバルな強靱性のための国際的な取組の主導」にも取り組んでいる。

英日サイバーパートナーシップでは、広島アコードの3つの優先事項の全てと一致した活動が行われるようになり、一定の成果も上がりつつあるが、今後協力のペースが高まるかどうかは不透明である。

英日両政府の行動には、サイバーセキュリティを通じて両国の経済関係を深めたいという意思がすでに見られる。日本は自衛隊と防衛省の職員を対象とするサイバーセキュリティ訓練の実施を英国企業に委託した。英国のNCSCは、富士通UKを「Industry 100」スキームに招き入れ、日本サイバーディフェンスをインシデント対応プロバイダーとして認定した。[64]それにもかかわらず、サイバー分野における貿易と投資の伸びは鈍い。民間セクターのステークホルダーは外国市場への進出は難しいと考えている。一部の企業が懸念しているのは、コストの高さだ。防衛セクターでは、必要なクリアランスを取得できるかどうかを不安視する声も聞かれる。[65]共通の言語がないことも大きな障害だ。人工知能（AI）を利用したモデルが登場するなど、翻訳ソフトは言語の壁を乗り越える助けとなっているが、障壁が完全に無くなったわけではない。市場構造にも課題がある。日本の企業は、サイバーセキュリティ分野の製品やサービスを少数の大手ベンダーから調達する傾向がある。[66]ベンダーはリスクを嫌い、中小企業の製品やサービスをなかなか取り入れようとしない。その結果、日英両国の中小企業は不利な立場に置かれている。一方、英国の大手サイバーセキュリティ企業はあまりベンダーを使わない。現地オフィスを構えるだけのリソースはあるが、時間とコストの負担は大きい。英国企業は、必要なスキルを持つバイリンガルの日本人従業員の確保が不可欠だと考えているが、適格な人材の採用に非常に苦労していると回答した。日本企業の調査参加者も、英国市場への参入に懸念を示したが、英国企業ほど具体的な問題点は挙げなかった。[67]両国の政府関係者は、サイバー分野を通じた経済的パートナーシップの深化に強い関心を示しているが、データ収集の結果、未解決の課題があることが分かった。

英日サイバーパートナーシップの3つ目の優先事項は、広島アコードの第3の柱とすでにある程度一致している。共通利益の増進（影響力の向上、攻撃者への対抗等）に取り組みながら、より良い未来や持続可能な世界を作ることは可能である。例えば英国と日本はどちらもサイバー分野のキャパシティ・ビルディング（CCB）を通じて、攻撃を受ける国のサイバーレジリエンス、意識、安全保障の向上を図っている。CCBは、攻撃を受ける側の能力を強化し、サイバー攻撃の被害を軽減するだけでなく、影響力、安全保障、経済に関する目標の達成にも寄与する。英国は「インド太平洋サイバー・プログラム」をはじめ、複

64. 2023年11月30日に著者が東京で実施した英国の民間セクター代表者へのインタビュー。NCSC, 'Annual Review 2023:Making the UK the Safest Place to Live and Work Online', p. 52, <https://www.ncsc.gov.uk/pdfs/reports/Annual_Review_2023.pdf>, 2023年12月10日閲覧。NCSC, 'Cyber Incident Response', <https://www.ncsc.gov.uk/schemes/cyber-incident-response/find-a-provider>, 2024年4月12日閲覧。
65. 2023年12月1日及び5日に著者が東京及びオンラインで実施した英国の民間セクター代表者へのインタビュー。2023年12月5日及び2024年1月9日と2月13日に著者が東京及びオンラインで実施した日本の民間セクター代表者へのインタビュー。
66. 2023年12月5日及び2024年1月9日と2月13日に著者が東京及びオンラインで実施した日本の民間セクター代表者へのインタビュー。2023年12月4日に著者が東京で実施した日本の市民社会組織代表者へのインタビュー。
67. 同上

数の国際的なCCBプログラムを展開している。一方の日本は現在、インド太平洋諸国に重点を置いており、JICAはオセアニアとアフリカでの活動を拡大しようとしている。[68]さらに、アジア太平洋地域におけるサイバー分野のキャパシティ・ビルディングの要として、日ASEANサイバーセキュリティ能力構築センター（AJCCBC）を設立した。[69]表1に記載されているように、英国はAJCCBCを通じて、CCBを支援した。英国と日本は、それぞれCCBに意欲的に取り組んできた。さらなるアラインメントは両国の取組みを増幅させる可能性がある。英国と日本がCCBに関する活動をどの程度調整できるかは、戦略面、実務面の検討事項に左右される。CCBにどこで、どのように、いつリソースを投じるかについて、両国は合意しているか。実際、両国が協力して、活動を効果的に進めることは可能なのか。仕事の進め方や情報共有のプロセスにずれはないか。英国と日本は志を同じくするパートナーだが、両国の外交政策は多様な個別要因によって形成されている。

国家戦略のアラインメントとさらなる共通点

英国と日本は、どちらも包括的な国家サイバーセキュリティ戦略を掲げている。表2は、その骨子をまとめたものである。

デジタル社会のセキュリティとレジリエンスを強化することは、英国と日本が共有する戦略的コミットメントである。日本の包括的な目標は「自由、公正かつ安全なサイバー空間」の確保であり、英国のビジョンは「自由で開かれた平和かつ安全なサイバー空間」である。[70]両国の戦略は重なる部分が多く、サイバー政策の優先事項も似通っている。英国も日本も、民間セクターが果たす役割の必要性を認識しており、標準や規制の優先度を高める一方で、国際的な目標を達成するためにサイバー分野を積極的に活用している。両国は、脅威の性質に対する理解も共有している。こうした収束点が英日サイバーパートナーシップの推進力となり、初年度は官民連携、世界的な共通利益の増進、能力開発を中心に多くの活動が行われた。

68. 2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。JICA, JICA グローバル・アジェンダ No.15「デジタル化の促進」 クラスター事業戦略「サイバーセキュリティ」（英語版）, 2023年5月, <https://www.jica.go.jp/Resource/english/our_work/thematic_issues/digital/fp4rrb000000t57s-att/overview_03.pdf>, 2023年12月3日閲覧。
69. AJCCBC, 'Who We Are'.
70. 日本政府 'Cybersecurity for All（英語版）', p. 4; 英国政府, 'National Cyber Strategy 2022', p. 33.

表2：英国と日本のサイバー戦略の柱

英国	日本
英国のサイバーエコシステムの強化	経済社会の活力の向上及び持続的発展
サイバーレジリエンス	国民が安全で安心して暮らせるデジタル社会の実現
技術的優位性	国際社会の平和・安定及び日本の安全保障への寄与
グローバルリーダーシップ	サイバーセキュリティに対する横断的施策
脅威への対抗	

出所：英国政府, 'National Cyber Strategy 2022'。日本政府, 'Cybersecurity for All（英語版）', 2021年1月, <https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021-en-booklet.pdf>, 2024年8月19日閲覧。

英国と日本の戦略には大きく類似する分野がいくつかあるが、協力が難しい点も見られる。例えば、標準の相互運用性、サイバー脅威インテリジェンスの共有、共同ハントフォワード作戦、研究・学術分野のパートナーシップ等である。[71]第IV章では、こうした分野に関するメリットと課題を論じる。

71. 「ハントフォワード（Hunt forward）」作戦は米国のサイバー軍が始めたもので、悪意のある活動を特定し、撃退するために、友好国のネットワーク上で共同で展開する防衛サイバー作戦。

IV.戦略的な考慮事項と提言

これまでに述べてきたように、英国と日本は多くの課題や機会を共有しているため、英日サイバーパートナーシップは複数の分野で大きな勢いを得てきた。しかし、両国のパートナーシップはまだ初期の段階にあり、成長の余地は大きい。現在の戦略的優先事項は両国のパートナーシップに沿ったものだが、今後活動の範囲を広げ、重点分野を拡大することは可能である。

本章では、2年目を迎える英日サイバーパートナーシップについて、戦略面の考慮事項と実行可能な活動を提言する。

戦略的な考慮事項

日本と英国が後述する提言に取り組むためには、以下の点を考慮する必要がある。

現在の方向性を維持する：英日サイバーパートナーシップと、その創設を提唱した広島アコードは、どちらも比較的新しいイニシアティブである。英国と日本の親密度はこの10年で高まっているが、国内の政治的優先事項によっては、英日関係への注目度が下がる可能性もある。英日サイバーパートナーシップのこれまでの成果を適切に伝えること、そしてパートナーシップが特定した協力分野を定着させることが重要である。英日サイバーパートナーシップに対する注目を維持することは、英日関係全体にも利益をもたらす。

サイバーパートナーシップは関係の一部にすぎない：両国の協力関係を単体で捉えることは有益ではない。英国と日本は志を同じくするパートナーだが、その関係は複雑に張り巡らされた多数国間・少数国間協定の1つにすぎない。二国間の活動を重視することは理解できるが、どちらの国も、Five EyesやAUKUS、QUAD（日米豪印）といった戦略的利害を共有するグループにおいて他のパートナー国とのイニシアティブに参加することを控えるべきではない。しかし、英日両国に比較優位をもたらす二国間協力の機会は、可能な限り追求する必要がある。

サイバー改革に対する支援は互恵的である：現在、日本はサイバー分野の法律と体制の抜本的な改革を進めている。英国を含むパートナー国は、様々な情報や援助を提供し、このプロセスを支援したいと考えている。一方、日本のステークホルダーも世界のベストプラクティスから学ぼうとしている。とはいえ、英日サイバーパートナーシップを能力構築のためのイニシアティブと捉えるべきではない。例えばグローバル戦闘航空プログラム（GCAP）のような活動では、英国と日本は対等な立場にある。このように、英日サイバーパートナーシップは今後も、英国と日本が対等な立場で協力するイニシアティブと位置づけなければならない。サイバー分野では、日本は英国に「追いつく」ことを目指しているが、短期的にはまだ共有すべき教訓はあり、日本の能力も急速に向上していることから、中長期的には両国の協力関係をさらに深める機会は多い。

サイバーセキュリティは手段であり、活動でもある：サイバーセキュリティ分野で信頼と協力を強化できれば、英国と日本はさらに広い分野で協力関係を深められるようになる。英国と日本が防衛・安全保障分野での協力を優先していることを考えると、これは特に重要である。同様に、サイバーセキュリティ分野に関する取組みは、それ自体を目的と捉えるべきである。英日サイバーパートナーシップの価値をこうした観点から評価することは、どのくらいのリソースを割り当てるべきかを判断する上でも重要である。

遅れや行き詰まりをあらかじめ織り込んでおく：英日サイバーパートナーシップは、初年度は良好な勢いを示したものの、短期的には解決の見込みがない課題や障害も存在する。こうした問題には、これまでの章でも取り上げてきた、国内の政治的コミットメントや相反する国際的な優先事項といった戦略的リスクもあれば、リソースの確保、言語、情報セキュリティ、脅威の状況の違い、地理的距離といった戦術面の障害、さらには共通の実施計画の欠如などがある。本稿では、こうした課題を指摘するとともに、英日サイバーパートナーシップの戦略的動機の概説と二国間活動の特定に重点を置いている。英日サイバーパートナーシップが直面している課題の重要性と幅を深く理解するためには、さらなる調査が求められる。

推奨される活動

1. 能力開発

サイバー分野の技術者は世界的に不足している。各国政府は熟練した職員の育成と維持に苦労しており、人材不足は技術的ソリューションを評価し、開発し、実施する能力にも影響を及ぼしている。熟練した人材の不足は、国家のサイバー防衛に寄与するサイバーセキュリティ分野の製品・サービスに対する各国政府のアクセスにも悪影響を及ぼしている。政府や非専門企業内の能力ギャップが広がるにつれて、サイバーセキュリティの提供や導入を担う業者への依存度が高まっている。以下の提言は、英国と日本が能力の開発・向上において、どのように協力し続けられるかを示したものである。

提言1：部門を問わず、再現可能な人材育成のための協力活動を確立する。

調整機関、国の技術当局、外務担当省庁は、特異性のある確固とした人材育成活動を確立する必要がある。こうした活動は、様々な政府部門が比較的容易に再現できるものでなければならない。主な内容は次の通りである。

- **訓練**：技術訓練は職員のスキルアップを可能にする重要な手段であり、職員が組織にとどまる非金銭的なインセンティブとなる。日本の場合、必要な訓練の規模を考えると、民間セクターの支援は不可欠である。例えば、日本の防衛省は2027年度末までに自衛隊のサイバー中核人材を2022年度の約890人から約4,000人に、同省全体ではサイバー分野の人員を約2万人（自衛隊のサイバー中核人材を含む）に増やすことを目標

に掲げている。[72]英国のサイバーセキュリティ業界には、この種の訓練サービスを提供する企業が多い。そのため、英日サイバーパートナーシップを通じて、各社に日本政府との契約に応札するインセンティブを提供する。訓練には技術以外の内容も含めるべきだ。例えば防衛政策に関するインタラクティブなセッションが考えられるが、実現には英国国防省の直接参加が必要となる可能性が高い。[73]

- **人材交流**：英日両国で定期的に連携している政府機関、部門、省庁で、その活動範囲が明確に重複している場合は、人材交流を推進するべきである。特に英国のDSITや日本の経済産業省など、最先端のサイバー分野や技術分野の規制に取り組んでいる組織は、こうした交流の恩恵を受ける。交流活動は、本稿の随所で言及してきた言語の壁の影響を受けやすい。集中的な語学研修などの創造的なソリューションは、こうした課題がもたらす影響を緩和する可能性がある。しかし、多くのリソースを必要とする場合があるため、人材交流と語学研修の機会を組み合わせることを検討してもよい。
- **演習**：国際演習に合同チームとして参加したり、互いの国内演習に参加したりすることは、両国の運用面の親和性を高め、参加者のスキルを強化し、両国のパートナーシップを世界に示す機会となる。しかし当然ながら、こうしたメリットを享受するためには、演習に必要なリソースも確保しなければならず、この点が懸念材料となる。

こうした活動に民間セクターが関与する場合、日本と英国はパートナーシップに両国の企業を巻き込むことを奨励する必要がある。

提言2：人材の維持・採用方針に関する非公式の議論を継続する。

英国の国防省と日本の防衛省は引き続き、人材の維持・採用に関する取組みを議論する必要がある。また、得られた教訓はサイバー担当者を雇用している他の政府機関（警察等）とも共有するべきである。英国と日本のサイバー予備役間の協力イニシアティブに関する提案は、その一例である。協力活動に予備役を含めることで、高度な専門知識を共有し、限られた人材にかかる負担を軽減できる。

提言3：より効果的な情報共有とサイバー脅威インテリジェンスのプロセスを確立する。

協力のスピードを早めるためには、日本と英国は情報をより効果的かつ積極的に共有していく必要がある。情報にはサイバー脅威インテリジェンスが含まれるが、それに限定されない。例えば、脅威主体の組織に関する情報も重要である。

情報共有プロセスの改善も求められる。サイバー脅威インテリジェンスの共有は、各国の固有のニーズとのバランスを取るために進められている改革の一例である。日本は現在、情報セキュリティ、セキュリティクリアランス、脅威情報の分類に関する政策やプロセスの改革を進めているが、英国のセキュリティ当局も十分な等価性を確保するためのアプロー

72. Shinnosuke Nagatomi, 'Japan Aims to Boost Self-Defense Force Cyber Personnel to 4,000', *Nikkei Asia*, 2024年7月3日, <https://asia.nikkei.com/Spotlight/Cybersecurity/Japan-aims-to-boost-Self-Defense-Force-cyber-personnel-to-4-000>, 2024年8月19日閲覧。2024年2月6日に著者がオンラインで実施した日本政府関係者へのインタビュー。日本政府, '防衛力整備計画'（2023年3月14日現在の暫定英語版）, 2022年12月16日, pp. 11–12, <https://www.mod.go.jp/j/policy/agenda/guideline/plan/pdf/program_en.pdf>, 2024年8月22日閲覧。
73. 2023年11月17日に著者がオンラインで実施した日本の市民社会組織代表者へのインタビュー。2023年12月18日に著者がオンラインで実施した日本政府関係者へのインタビュー。

チを見直している。サイバーセキュリティ分野の協力チャネルを通じた継続的な二国間対話は、両国の取組みの収斂を促進している。

グローバル戦闘航空プログラム（GCAP）では、各国の情報セキュリティに対するアプローチをすりあわせる取組みが進められてきた。2035年までに新型戦闘機を配備するという厳しいスケジュールを達成するためには、あらゆるレベルの情報について、情報共有に関する問題の解消を加速させなければならない。[74]情報共有を合理化しない限り、このプログラムの効率は下がることが懸念される。またスケジュールの遅れにより、悪意ある攻撃がもたらす脅威に効果的に対応できないことになる。現在のところ、GCAPの参加国が協働し情報をリアルタイムで共有するための、安全なデジタルプラットフォームを確立するという約束はまだ果たされていない。[75]第6世代戦闘機は、第1世代の技術では設計できない。情報共有の解決は技術的な問題であると同時に、政治的な問題でもある。現在のところ、一義的な責任を負うのは政府関係者だが、政府関係者は当然、リスクに敏感である。情報共有の取組みを大幅に、かつ適時に進展させることはGCAPにとっても、英日パートナーシップ全体にとっても不可欠だが、その実施には政治的意思決定者の積極的な関与が必要となる可能性が高い。信頼と情報セキュリティに関して、難しい決断を求められることもある。

2. 官民連携

民間企業はサイバー及びテクノロジー分野の重要な主体である。日本と英国は民間セクターと協力する必要性を認識しており、いずれも複数の官民連携プログラムを展開している。しかし、官民連携の分野で両国が協力するために解決しなければならない課題は多い。共通の言語がないこと、ビジネス文化が異なること、さらには、1つの政府のみならず2つの政府と協力する動機も様々であること等だ。

提言1：地域クラスター間のパートナーシップを実現する。

両国の地方政府は通商分野の省庁と協力して、地域サイバークラスター間のパートナーシップを奨励する必要がある。例えば、Cyber WalesがCyber Hiroshimaの設立を支援し、継続的に連携していることは、非政府組織間のサイバーパートナーシップの成功事例と言えよう。日本ではサイバークラスターの創設を検討する自治体が増えているため、両国の通商・デジタル分野の省庁は英国の既存のクラスターを積極的に紹介していくべきである。

74. Justin Bronk, 'The Global Combat Air Programme is Writing Cheques that Defence Can't Cash', *RUSI Commentary*, 2023年4月27日。
75. 「グローバル戦闘航空プログラム（GCAP）政府間機関の設立に関する条約」の第9章第52条では、「運営委員会は（中略）情報の保全に関する政策であって、情報の保全に関する全ての分野（サイバー分野に関する強靱性を含む。）において秘密情報を共通の程度で保護することを確保するものを維持する」と定めている。参照：MoD, 'Convention on the Establishment of the "Global Combat Air Programme (GCAP) – International Government Organisation"', 2023年12月14日, <https://www.gov.uk/government/publications/convention-on-the-establishment-of-the-global-combat-air-programme-gcap-international-government-organisation>, 2023年12月15日閲覧。

提言2：各セクターのISAC（情報共有分析組織）間の連携を促進する。

関係省庁・機関（NCSC、NISC、IPA等）は、各国のセクター別ISACと緊密に連携し、両国のカウンターパート間の対話を促進するべきである。さらに原子力、金融、自動車等、明確な関心分野がある場合には、セクター別ISAC間の協力を奨励し、必要な場合には支援を提供する必要がある。その際には、既存の国際的なISAC間協力と重複しないよう注意するとともに、明確なニーズや関心がない場合は協力を不必要に促進しないよう留意する。例えば、英国のサイバー・ディフェンス・アライアンス（CDA）と日本サイバー犯罪対策センター（JC3）の従前から良好な関係[76]を基礎として、さらなる協力関係を構築することもできる。CDAとJC3はどちらも、民間セクターや法執行機関と協力してサイバー脅威に対抗している非営利組織である。[77]

提言3：商業分野のサイバー活動に的を絞り、その拡大を積極的に支援する。

日本の経済産業省と英国のビジネス・通商省（DBT）は、自国の民間セクターと協力して、英国市場と日本市場へのアクセスを促進する戦略的アプローチを策定するべきである。例えば、英日企業間のパートナーシップを奨励し促進すること、両国の中小企業と大手企業が組み、共同で提案できるようにすること、両国の産業が優位性を持つニッチな分野を特定し、促進することなどが挙げられる。こうした原則は、定期的な貿易ミッションによって継続的に支援していくべきである。これらの活動は、サイバーセキュリティ分野の貿易障壁を低くし、企業にパートナーシップの機会を探る機会を提供する上でも重要である。

日本の経済産業省と英国のDBTは、両国のサイバーセキュリティ企業の事業拡大を支援する役割を果たすことをさらに検討するべきである。これは英国に進出している日本企業も参加する「Industry 100」プログラムのような取組みを補完するもので、英国企業と日本企業に新たな機会を示すことにつながる。非政府組織や準政府組織、特に貿易・産業団体（例：経団連、英国産業連盟、英国国家サイバー諮問委員会）も、二国間の商業機会を支援するよう促されるべきである。

提言4：国レベルの官民連携を拡大し、英国企業又は日本企業を巻き込む機会を探る。

国レベルの官民連携を運用している政府機関は、こうしたスキームを拡大し、外国企業（日本企業又は英国企業）も巻き込むことができないかを検討するべきである。サイバー脅威情報の共有や人材の出向等、様々なタイプのイニシアティブが考えられる。英国は「Industry 100」スキームを通じて、このアプローチを実践しており、すでに英国に拠点を持つ日本企業2社を巻き込むことに成功した。日本のサイバーディフェンス連携協議会（防衛産業の官民連携）は、サイバーセキュリティ協議会を通じて、同様のアプローチを実践することもできる。あるいは、日本に進出している英国企業からの出向者をNISCに

76. 参照例：JC3へのサイバー・ディフェンス・アライアンス（CDA）の参加、及びJC3代表理事のコメント。JC3, 'JC3 Forum 2021', <https://www.jc3.or.jp/activity-report/forum2021.html>, 2024年8月19日閲覧。'特別インタビュー：増大するサイバー犯罪の根源的な解決へ', NEC技報（英語版）(Vol. 12, No. 2)、2018年1月, <https://www.nec.com/en/global/techrep/journal/g17/n02/pdf/170202.pdf>, 2024年8月19日閲覧。

77 JC3, 'JC3とは', <https://www.jc3.or.jp/about/>, 2024年8月19日閲覧。CDA, 'Welcome to the Cyber Defence Alliance', <https://cyberdefencealliance.org/>, 2024年8月19日閲覧。

受け入れてもよい。しかし、そのためには日本に拠点を置く英国企業を増やさなければならない。

3. 世界的な共通利益の増進

英国と日本は、志を同じくする自由民主主義国家であり、多くの地政学的懸念や目標を共有している。どちらの国も「自由で開かれたインド太平洋」を支持しており、サイバー分野に対する責任あるアプローチを重視し、共通の敵に立ち向かっている。英日サイバーパートナーシップは、世界的な共通利益を実現するための協力を拡大できる、効果的なチャネルを提供している。

提言1：日ASEANサイバーセキュリティ能力構築センター（AJCCBC）を、ASEANにおけるサイバー分野のキャパシティ・ビルディング・ハブ（CCBハブ）と位置づけ、インド太平洋地域のモデルとして、共同プロジェクトを開発する。

日本の国際協力機構（JICA）と英国の外務・英連邦・開発省（FCDO）は、既存のイニシアティブを活用して、共同CCBプロジェクトを開発すべきである。これらのプロジェクトでは、総務省が提供する「実践的サイバー防御演習（CYDER）」や、オックスフォード大学が開発したサイバーセキュリティ能力成熟度評価といった最新の製品・サービスを利用する必要がある。[78]さらに、FCDOはAJCCBCを通じて、ASEAN諸国でCCB活動を展開することも検討するべきである。

JICAはCCB等のトピックスについて、AJCCBCをインド太平洋地域の他のサイバー人材育成拠点、例えばASEANシンガポール・サイバーセキュリティ・センター・オブ・エクセレンス（ASCCE）やサイバー専門的知識に関するグローバルフォーラム（GFCE）の「太平洋ハブ」と連携させることも検討するべきである。[79]その一環として、AJCCBCと各組織の定期交流の機会を拡大する。 FCDOは、CCB活動の調整・実施を担当した経験や、インド太平洋地域の安全保障に対するコミットメントを活用して、この取組みを支援するべきである。

年次英日サイバー対話では、CCBに関する意思決定について議論するとともに、可能であれば戦略的アラインメントを行う必要がある。このアラインメントでは、少なくとも衝突の回避を目指す。さらに踏み込んだアラインメントを行う場合は、地域パートナーのサイバーレジリエンスや防御力の向上、攻撃の抑止、拒否、妨害等の活動を調整する。2024年の英日サイバー対話では、CCBに関する三国間協力の優先パートナーとしてモンゴルと台湾を検討する。台湾の場合は共同演習のような、対等な立場での活動を含む可能性が高い。

78. 2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。University of Oxford, 'Global Cyber Security Capacity Centre', <https://gcscc.ox.ac.uk/the-cmm>, 2023年12月20日閲覧。
79. CSA Singapore, 'ASEAN-Singapore Cybersecurity Centre of Excellence', 2021年10月6日, <https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence>, 2024年8月19日閲覧。Global Forum for Cyber Expertise, 'Pacific', <https://thegfce.org/region/pacific/>, 2024年8月19日閲覧。

提言2：緊密な連携を通じて国際的なルールと規範を推進する。

日本と英国は、国際的なルールと規範に関して、構造的協力と活動ベースでの協力のアラインメント拡大に継続的に取り組むべきである。FCDOと外務省、そしてカウンターランサムウェア・イニシアティブ会合や国連OEWGといった国際的な枠組みに参加している他の省庁は、可能な限り一貫した立場を取る必要がある。また、さらなる連携を通じて、自由で公平で責任ある開かれたサイバー空間を、この原則にコミットしていない国々（特にASEAN諸国）に提唱していくべきである。

FCDO、外務省、及び関連する技術機関は、共同アトリビューションに参加する機会や、サイバー空間における国際的なルールや規範に対する立場を共同で表明する機会を引き続き積極的に模索するべきである。例えば、日本は2024年3月、ハッカー集団「APT31」は中国政府が支援するサイバー脅威者であるとする英国の主張を支持した。[80]セキュリティクリアランスの改革と情報共有の拡大により、今後はさらに多くの共同声明が生まれ、機密度の低い攻撃に対するアトリビューション活動が促進されると見られている。いずれにしても、英国と日本は互いの具体的な基準値や公式声明を出す意思を尊重する必要がある。

提言3：サイバー危機に対する積極的かつ国際的な支援活動のアラインメントを行う。

防衛・外務分野の省庁及び関連する技術機関は、大規模なサイバーインシデントに見舞われる危険性が高い第三国に対し積極的かつ国際的なサイバー支援を提供するため、協力関係を模索するべきである。積極的かつ国際的なサイバー危機支援では、協力活動の特定や戦略的優先事項のアラインメントを行う。

協力活動には、ハントフォワード作戦の形でイニシアティブを共同で推進することが含まれる場合がある。また、関係する政府部門は、ウクライナ等に対する国際的な危機支援を通じて得た教訓も共有するべきである。こうした情報をもとに、英国と日本は、第三国の大規模インシデントに対応するための共同出資メカニズムへの参加を議論するべきである。

サイバー危機に対する国際的な支援活動への協力を拡大する場合、英国と日本はこうした活動における権限、基準値、優先事項を明確化するべきである。

4. サイバー・レジリエント・エコシステム

サイバー・レジリエント・エコシステムは、その前提として、政府全体で役割と責任が明確に割り当てられている必要がある。英国は2016年にNCSCを設立して以来、サイバーガバナンスに大きな変更を加えていないが、日本は大規模なサイバーガバナンス改革のさなかにある。また、両国ともサイバーセキュリティをどのように、どこで、いつ規制すべきかを積極的に検討している。英日両国はEU、中国、米国という大きな規制圏の外側にある。両国が世界の複雑な規制環境に対応していくためには、サイバーセキュリティのガバナンスに関する協力が重要となる。英国は新しいサイバーセキュリティ・レジリエンス法案を計

80. 英国政府, 'UK Holds China State-affiliated Organisations and Individuals Responsible for Malicious Cyber Activity'。2023年12月5日に著者が東京で実施した日本政府関係者へのインタビュー。

画しており、日本は前述したように改革を推進中であることを考えると、英日サイバーパートナーシップの進展に合わせて、両国がサイバー・レジリエント・エコシステム及び必要な改革の面で協力することは「互恵的」と見なすべきである。

提言1：政府の構造やプロセスの構築を通じて得た統合的な知識を提供する。

NCSCは、他の関連省庁や元政府高官と協力しながら、英国が2016年以降、サイバー分野で実施した構造・法制改革を総括するべきである。この総括では、捜査権限の責任ある行使、機密情報と非機密情報を統合する仕組みの構築、運用機能から戦略機能への官民連携の拡大、社会全体のサイバーセキュリティを支援する製品の開発等に重点を置く。日本のサイバーセキュリティ戦略本部と内閣サイバーセキュリティセンター（NISC）は、このリソースを組織再編に活用し、英国のカウンターパートにフィードバックを提供することもできる。

提言2：軍事サイバー機能の開発とその有効化プロセスから得た教訓について議論する。

英国の国家サイバー部隊（NCF）、国防省、軍隊、及び諜報機関は、日本の自衛隊や防衛省（サイバー防衛隊や情報本部を含む）との二国間対話を継続するべきである。この対話では、情報の機密解除と共有のプロセス、責任ある透明な方法でのサイバー能力構築に重点を置く。いずれも日本政府のインタビュー参加者複数名が優先事項として挙げたものである。[81]

提言3：サイバー専門家の相互承認を進める。

英国の科学・イノベーション・技術省（DSIT）、日本の経済産業省、及び両国の関連省庁（例：英国のNCSC）は、サイバー専門家が従うべき標準の相互承認に取り組み、英国とシンガポールが締結しているサイバー・スキル・パートナーシップとの統合を目指すべきである。[82]

提言4：標準のアラインメントと相互運用性を探る対話を、年2回開催する。

DSITと経済産業省は、サイバーセキュリティと関連する標準のアラインメントを促進するために、年2回の対話を主導し、調整するべきである。こうした対話は、アプリケーションセキュリティ、AI、IoTに関する既存の取組みを強化するものであり、ソフトウェアのサプライチェーン・セキュリティや産業制御システム等の分野に対処することで実現される。また、英国のビジネス・通商省と日本の経済産業省は、貿易を促進する上で相互運用性が最も重要となる分野を産業界と協力して特定するべきである。例えば英国の「サイバー・エッセンシャルズ認証」は、政府契約を受注するために必ず守らなければならないスキームである。[83]

81. 2023年12月4日に著者が東京で実施した日本政府関係者へのインタビュー。
82. Cyber Security Agency Singapore, 'Joint Media Release by Cyber Security Agency of Singapore and Department for Science, Innovation and Technology, United Kingdom on Cyber Skills Cooperation', 2023年10月18日, <https://www.csa.gov.sg/News-Events/Press-Releases/2023/joint-media-release-by-cyber-security-agency-of-singapore-and-department-for-science-innovation-and-technology-united-kingdom-on-cyber-skills-cooperation>, 2023年12月10日閲覧。
83. NCSC, 'Cyber Essentials', <https://www.ncsc.gov.uk/section/products-services/cyber-essentials>, 2024年8月19日閲覧。

5. その他

英日サイバーパートナーシップの優先事項は、サイバー分野の英日間協力の大部分に影響を及ぼしているが、主体は他の機会を制限されるべきではない。政府の様々な部門で多彩な協力活動が分散的に行われることは、多くの機会をもたらす一方、一元的な追跡を困難にする。優先すべき分野に十分なリソースが配分されない可能性もある。

提言1：協力を可能にする活動を継続的に支援する。

年次サイバー対話では、政府の様々な部門が広く対話の機会を与えられるように、十分な資金を投入するべきである。日英両国がサイバー分野で迅速に協力できるようにするという共通目標を達成するためには、個人レベルの関係を維持することが欠かせない。

高官や政府代表者による訪問も継続する必要がある。トップダウンの指示は、政府関係者に英日間協力を優先する動機と権限を与える。

提言2：サイバー教育に関するパートナーシップを深める。

日本の文部科学省、英国の教育省、及び関連する高等教育当局は、サイバーセキュリティの分野で大学レベルのパートナーシップを促進するための施策を検討するべきである。具体的には、大学間の共同学位プログラム、語学試験の特別免除や特例の設置等を通じて、高等教育のモビリティを促進する必要がある。

関係省庁は、「日本サイバー・セキュリティ・フェローシップ」や「サイバー・ファースト・コンペティション」[84]の試行結果を評価し、プログラムを拡大すべきか否か判断するべきである。教育のあらゆる段階でさらなる活動を試験的に展開し、二国間協力が安全性やスキルの向上につながるかどうかを検証する必要がある。

提言3：英日サイバーパートナーシップの評価報告書を2〜3年ごとに作成する。

主たる責任を有する機関（例えばFCDO、外務省、NISC、NCSC等）は、サイバーパートナーシップの進捗状況を定期的に分析し、高い成果が見られた分野、得られた教訓、今後の機会等を継続的に評価する必要がある。この評価は、パートナーシップが十分な権限を与えられているかを検証するためにも活用するべきである。評価においては、合意されたマイルストーンに従って評価可能なパートナーシップの目標を履行するよう両国とも尽力する。評価の観点は公開できないが、英国と日本は日英デジタルパートナーシップが発行している進捗報告書と同様の報告書を公開することを目指すべきである。[85]

84. Cyber First, 'Cyber First Schools and Colleges', <https://www.cyberfirstschools.co.uk/>, 2024年8月19日閲覧。参照例：Cyber Wales, 'Cyber Hiroshima Cluster Hosts NCSC Cyber First Event', 2024年2月7日, <https://cyberwales.net/events/?event=hiroshima%20ctf>, 2024年8月19日閲覧。2023年12月19日に著者がオンラインで実施した日本政府関係者へのインタビュー。
85. Department of Science, Innovation and Technology, 'UK-Japan Digital Partnership:Progress Report', 2024年1月18日, <https://www.gov.uk/government/publications/uk-japan-digital-partnership/uk-japan-digital-partnership-progress-report-18-january-2024>, 2024年8月22日閲覧。

結論

サイバーセキュリティ分野における日本と英国の協力は、具体的な運用活動を通じて相互の利益を効果的に促進し、より広範な日英パートナーシップを可能にするものとなっている。英日サイバーパートナーシップは、初年度の勢いを維持しつつ、協力の深さと幅をさらに拡大することを目指すべきである。

本稿では、英日サイバーパートナーシップの活動と戦略的優先事項を概観するとともに、パートナーシップをさらに発展させるための提言を行った。現在のパートナーシップの優先事項は適切であり、活動には拡大の余地があることを示している。また現在、所定の優先事項の枠外で行われている協力活動は、パートナーシップの範囲を拡大する機会を示している。サイバー・レジリエント・エコシステムにおける協力は、既存の取組みを尊重しつつ、デジタル政府、技術標準、構造改革等の分野において、協力を拡大する余地を生み出している。

既存の優先事項の範囲でも、活動を拡大できる余地は十分にある。日本と英国はどちらも、サイバー能力の拡大、開発、維持に関する課題に取り組んでいる。知識の交換、協力の機会の特定、情報の共有は能力を強化する助けになる。商業分野の協力を促進することも、英日サイバーパートナーシップの優先事項である。言語の違いなどの課題はあるものの、企業の参入障壁を下げるプラットフォームは存在し、利用側にも提供側にも明確なメリットがある。英国にとっても日本にとっても、地政学的緊張の高まりは懸念事項である。サイバー分野での協力を拡大し、世界的な共通利益を増進するためには、サイバー分野のキャパシティ・ビルディングの重視、ルールと規範のアラインメントの強化、国際的なサイバー危機対策の検討等を実施する必要がある。

英日サイバーパートナーシップは、今後も主要な推進要因の恩恵を受けると期待されている。日本と英国は密接に連携しており、同じパートナーのネットワークに参加し、同じようなサイバーセキュリティ関連の課題や機会に直面している。両国は、GCAPのような長期イニシアティブにも共同で取り組んでおり、こうしたイニシアティブは両国が長期にわたって密接に連携するためのプラットフォームとなっている。米英豪の安全保障の枠組み「AUKUS」も、第2の柱である先端技術分野において日本と協力することを検討している。[86]しかし、英日サイバーパートナーシップの足を引っ張る障害も存在する。こうした障害は、もし解決されなければ両国の活動のペースや範囲に悪影響を与えかねない。この問題を解決するためには、情報共有に関する問題に取り組むこと、また競合する優先事項がある中で、英日パートナーシップが今後もリソースを確保できるようにすることが必要となる。

86. オーストラリア政府, 'Fact Sheet: Implementation of the Australia–United Kingdom–United States Partnership (AUKUS)', <https://pmtranscripts.pmc.gov.au/sites/default/files/AUKUS-factsheet.pdf>, 2024年8月19日閲覧。

著者について

Joseph Jarnecki：RUSIサイバー研究グループのリサーチフェロー。主な研究分野はサイバーと技術が可能にする紛争、サイバーセキュリティ能力構築、先端技術が経済安全保障にもたらす機会とリスク。キングス・カレッジ・ロンドンの戦争学部で国際紛争研究の修士号と国際関係学の学士号を取得。

Philip Shetler-Jones：RUSI国際安全保障研究グループの上級リサーチフェロー。現在の研究テーマはインド太平洋地域の安全保障。近著では、日本の防衛政策、NATOに対する中国の姿勢、台湾防衛に関するナラティブに注目。英国海兵隊コマンド部隊では将校を務めた。シェフィールド大学で博士号、修士号、学士号、タフツ大学フレッチャー法律外交大学院で修士号を取得。地政学評議会客員フェロー、シェフィールド大学東アジア研究学部名誉リサーチフェロー、東京大学公共政策大学院戦略的コミュニケーション教育・研究ユニットフェロー。

Pia Hüsch：RUSIサイバー研究グループのリサーチフェロー。主な研究分野はサイバー作戦の影響、社会的リスク、及び合法性、並びにAI等の破壊的技術が地政学や国家安全保障に与える影響。グラスゴー大学で国際法と安全保障の博士号及び法学修士号（優等）、マーストリヒト大学で欧州法の法学士号を取得。