日本版「能動的サイバー防御（ACD）」を支える政府組織のデザイン

――インテリジェンス駆動型サイバーセキュリティ政策を支える２つの「出島組織」

防衛研究所
瀬戸 崇志*

2022 年 12 月の「国家安全保障戦略」が掲げた、日本政府による「能動的サイバー防御（active cyber defense）」（以下：日本版 ACD）の導入は、2025 年 5 月のサイバー対処能力強化法及び同整備法（以下：ACD 関連法）の成立に伴い、法的な基盤整備の面では一つの節目を迎えた。しかし、日本版 ACD が列挙する（ア）官民連携強化（イ）通信情報利用（ウ）アクセス・無害化、の運用指針策定や、その実務を支える実働部門の編制といった、政府側の体制/態勢整備は、ACD 関連法施行と措置の運用開始まで急務であり続けている。

ACD 関連法に関する内閣官房の説明資料によると、日本版 ACD による各種措置の実務について、官民連携強化や通信情報の利用は、（A）内閣サイバーセキュリティセンター（NISC）の発展的改組により置かれる内閣官房・内閣府の新組織により、他方で（B）アクセス・無害化は、事案の性質に応じ、警察もしくは自衛隊の部隊が担う。また通信情報利用やアクセス・無害化は、（C）新設の独立機関の事前・事後承認を通じ、適法性や説明責任の担保が目指されるほか、安全保障政策との整合性の観点から、（D）国家安全保障会議（NSC）とその事務局（NSS）との緊密な連携・調整も想定される[1]。

以上を踏まえ、本稿では近年の諸外国事例や学術研究の知見を基に、日本版 ACD をめぐる体制/態勢整備の論点である新たな政府組織をめぐる問題を考察する。ここでは紙幅の制約から、後述の「サイバーセキュリティ政策（以下：CS 政策）の所要」を踏まえ、「政府のインテリジェンス機能」（以下：政府の情報機能）を調節する「出島組織」の役割を果たす、上記４類型では（A）と（B）に相当する政府組織に焦点を絞り、論点の概観を目指す。

１．日本版 ACD の歴史的意義―公助の積極化

2025 年 12 月 23 日に閣議決定された新たな「サイバーセキュリティ戦略」は、国が従来以上に積極的な役割を果たすことを強調したうえで、日本政府による必要な体制/態勢整備を踏まえ、日本版 ACD の（ア）～（ウ）の柱を相互に、従来の様々な施策とも有機的に連動させつつ政策目標を追求する方針を示す[2]。日本版 ACD を、個々の措置の柱を超えて通底する理念に立脚した一連の改革パッケージと捉える場合、日本版 ACD の「A（active）」は、CS 政策での「政府の役割（公助）の積極化」という理念を象徴するとも解釈できる。同旨の理念は

*政策研究部 サイバー安全保障研究室 研究員
[1] 内閣官房国家サイバー統括室（以下: NCO）「サイバー対処能力強化法及び同整備法について」（2025 年 9 月）、36–38 頁。
[2] NCO「サイバーセキュリティ戦略」サイバーセキュリティ戦略本部 閣議決定（2025 年 12 月 23 日）、3–4 頁, 10–20 頁。

2010 年代に英国で先行し[3]、近年では米国、豪州、オランダといった各国の CS 戦略にもみられる、近年の先進民主主義国の CS 政策のパラダイムとなった[4]。

この CS 政策のパラダイムの転換こそが、日本版 ACD 導入の歴史的意義の一つであろう。「国家安全保障戦略」の文言を借りれば「欧米主要国と同等以上」の能力を目指して導入された日本版 ACD の（ア）～（ウ）の柱は、総じて「政府の役割（公助）の積極化」を梃に、民間セクターでの「自助」と「共助」の取組を支え、官民に跨る国家全体での CS のエコシステム強化を目指す点では一貫する[5]。そして、こうした日本版 ACD の具体化に向け、政府有識者会議でも必要性が強く認識されてきたのが、冒頭で触れた「政府の情報機能」の強化であった[6]。

2．CS 政策とインテリジェンスを繋ぐ「出島組織」

20 世紀の両大戦期と冷戦期における信号情報（SIGINT）を含めた様々な機微・公開情報の収集・分析を通じて、各国政府の意思決定を支えるインテリジェンス機関（national intelligence services：NIS）は、20 世紀後半来の「サイバー空間をめぐる安全保障政策」の形成期から一貫して重要なアクターであった[7]。ただし、「NIS」と「CS（政策）」の関係を歴史的・理論的に辿ると、両者の関係性は以下の 2 つの理由から必ずしも単純ではない。

第 1 に各国の NIS は、確かに「情報収集・分析を通じた政策決定者の意思決定支援」という NIS 固有の任務を指す「インテリジェンス（活動）」を支えるため、通信情報利用から第三者への秘密裡のアクセスまで「国家安全保障政策のためのサイバー空間の利活用」を牽引してきた。しかし、それは NIS が、例えば民間事業者のネットワーク防護のための官民連携等も含む「CS（政策）」の実践まで全て牽引してきたことを意味しない。歴史的には 20 世紀後半来の「情報セキュリティ」や「CS」の実践は、民間主導で形成され、NIS と異なる出自の専門家たちによる「CS コミュニティ」も形成されてきた。こうした「CS コミュニティ」と、NIS や法執行機関を含めた「安全保障コミュニティ」は、事案の情報共有をめぐる姿勢の乖離が大きく、各国でも脆弱性情報の取扱いや官民の事案対処連携をめぐる軋轢の源泉となってきた[8]。

第 2 に、近年の各国 NIS による CS 政策への関与は、前段で触れた NIS の固有任務としてのインテリジェンスの想定から逸脱する要素を含む。例えば注意喚起の公表等、近年の NIS による民間への脅威情報提供は、NIS の情報収集・分析の成果物が、政策決定者と NIS を繋ぐインテリジェンスサイクル内で生産・消費されるという想定とは異なる。後述の無害化作戦での NIS の役割も、インテリジェンスの政治化を回避するため、NIS が政策形成・執行に関与し

---

[3] 英国での「介入主義的アプローチ（interventionist approach）」と呼ばれる CS 政策のパラダイムについては、以下を参照。Ciaran Martin, “The Development of the United Kingdom’s Cyber Posture,” in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed. Robert Chesney and Max Smeets (Georgetown University Press, 2023), 206–215.

[4] 米豪蘭の 3 か国の政府の役割の積極化（官民の責任の再分配）の思想は、3 か国の戦略文書の以下該当箇所を参照。White House, *National Cybersecurity Strategy*, (March 2023), 4–5. ; Department of Home Affairs, *2023-2030 Australian Cyber Security Strategy*, (November 2023) 5, 30.; National Cyber Security Centre, *The Netherlands Cybersecurity Strategy 2022-2028*, (October 2022), 3–4, 8.

[5] この日本版 ACD の思想は、例えば以下を参照。NCO「サイバー対処能力強化法及び同整備法について」（2025 年 9 月）、5 頁。

[6] 内閣官房「サイバー安全保障分野での対応能力の向上に向けた提言」サイバー安全保障分野での対応能力の向上に向けた有識者会議（2024 年 11 月 29 日）6 頁, 13–14 頁。

[7] この点の史的展開は、次を参照。土屋大洋 「サイバーセキュリティとインテリジェンス機関―米英における技術変化のインパクト」『国際政治』第 179 号（2015 年 2 月）、44–56 頁。

[8] CS 政策を支える異なる専門家コミュニティの摩擦の問題は、例えば以下を参照。Sergei Boeke, “First Responder or Last Resort? The Role of the Ministry of Defence in National Cyber Crisis Management in Four European Countries,” (Leiden University, September 2016) 4–5.; Jason Healey, “The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers.” (Columbia University, November 2016).

ないことを求める規範とは抵触しうる[9]。

以上の点は、本稿でみる（A）・（B）の二類型の組織の設計思想の理解にも重要となる。CS 政策の所要からすれば、NIS は、民間企業を含め、従来のインテリジェンスサイクル内の政策決定者とは異なるカスタマーと意思疎通をはかる必要があり、NIS の秘密主義や政策執行からの中立性を含めた伝統的な原則からの逸脱も要求される。他方、従来の原則は、情報収集・分析による政策決定支援という意味でのインテリジェンスの任務の合理性からは必要であり、NIS が完全に放棄できる（すべき）ものでもない。

よって近年の各国政府は、政府の情報機能を CS 政策の需要に沿って調整するため、NIS 本体の「原則からの例外」を許容する「出島組織」を編制・運用する傾向があり、本稿が以下着目する（A）・（B）の組織類型もこれにあたる。ただし、両者はその主任務がサイバー攻撃の「被害者」と「加害者」のいずれに作用するかという点で異なる機能を備えている。

3．A：政府の情報機能と被害者支援の強化[10]

近年、各国政府に設置される CS 専門機関は、一義的にはサイバー攻撃による現在または将来の潜在的「被害者」の対処能力強化（以下：被害者支援）を任務とする。その手段は官民の脅威情報共有枠組みの運営、技術的助言・注意喚起、事案対処支援の提供まで多岐に渡るが、そこで求められる技術的専門性や国際連携から、こうした政府の CS 専門機関は、各国政府を代表した CERT 組織としての機能を期待されることが通例である。

近年、欧米主要国の政府 CS 専門機関の改革では、政府 CS 専門機関と NIS の関係性の再定義が論点となっている。国家を背景としたものを含む高度なサイバー攻撃キャンペーンへの対処を念頭に、各国では両者の組織的統合または相互連携を通じ、既存の NIS の能力基盤のバックアップを通じて政府 CS 専門機関の被害者支援強化を試みてきた。

その嚆矢たる事例の一つは、2016 年新編の英国国家サイバーセキュリティセンター（NCSC-UK）である。NCSC-UK は政府 CS 専門機関として、専門技術的知見に基づく官民の被害者支援任務を目的とするが、英国政府通信本部（GCHQ）の専門人材、SIGINT 基盤、諸外国 NIS からの機微情報も含め、GCHQ の有形無形の資源を利活用するため、指揮系統上は GCHQ の傘下に置かれた。その一方で NIS としての GCHQ の秘密主義や厳格な情報保全規則の一律な適用は、政府 CS 専門機関としての官民連携による被害者支援には重大な障壁となる。この障壁の克服に向け、NCSC-UK は GCHQ と接続されつつ、GCHQ 本体と異なる原理原則で運営される出島組織として設計された。GCHQ 本体と異なり、NCSC-UK は首都ロンドンの中核拠点を軸に、積極的な情報発信とアウトリーチを重視する組織文化を培い、GCHQ の能力を駆使した取組から官民連携まで、様々な被害者支援サービスを提供している[11]。

こうした取組を支える制度設計は、国毎に様々である。NIS と政府 CS 専門機関の両者の組織的統合の上で、後者を NIS の「出島組織」で追求する英国モデルは、豪州、カナダ、デンマーク、スウェーデンといった国々が採用する。これに対し米国やオランダのように双方の独立を維持しつつ、NIS の官民連携拠点新設や双方間の調整枠組みを通じて、両者の有機的な連携強化で同様の効果を追求する国々もあ

---

[9] インテリジェンスの定義と NIS の行動規範に関する伝統的立場は、例えば次を参照。小林良樹『なぜ、インテリジェンスは必要なのか』（慶應義塾大学出版会、2021 年）、16–37 頁。

[10] （A）の組織類型の先行研究、本稿第 3 節の記述は、別途の引用注で断りが無い限りは、以下を参照。瀬戸 崇志「『顕教』と『密教』のあいだ―近年の欧米諸国による政府のサイバー安全保障体制改革の潮流」『治安フォーラム』第 30 巻、第 11 号（2024 年 11 月）、45–54 頁。

[11] NCSC-UK の創設経緯は前掲注 3 ならびに次も参照。Robert Hannigan, *Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre,* （RUSI, 2019).

る。いずれも官民の各々の比較優位を梃にした双方向的な脅威情報共有を促し、国全体の脅威状況把握・事案対処能力の底上げを図る理念がある[12]。

４．B：政府の情報機能と無害化作戦の支援[13]

「政府の役割の積極化」の潮流のなかで、各国政府は前節の「強化された被害者支援」と並び、「加害者の継戦基盤に対する無害化作戦」（以下：無害化作戦）も追求してきた。そのなかでも、攻撃に悪用されるC&Cサーバーや端末への侵入と設定変更といった、標的への秘密裡のアクセスを伴う無害化作戦は、その効果的遂行には無害化の標的と手段を絞り込むターゲティングの精緻化が不可欠となり、事前の標的へのアクセスを通じた情報収集・分析を踏まえた準備が必要となる。

その機微性から、無害化作戦は通例は各国の法執行機関や軍事組織の法的権限と責任に依拠する。そのうえで法執行機関や軍事組織とNISの共同でのタスクフォース型組織（以下：無害化TF）が置かれる例も多い。米国連邦捜査局（FBI）主管の国家サイバー捜査統合タスクフォース（NCIJTF）[14]や、米国サイバー軍（USCYBERCOM）主管の選挙セキュリティグループ（ESG）[15]は典型例である。この他、英国防省、GCHQ、秘密情報部（SIS）等を構成機関とする英国国家サイバー部隊（NCF）[16]や、豪州連邦警察（AFP）と豪州信号総局（ASD）のサイバー犯罪集団への無害化共同部隊[17]も例となる。

これら無害化TFや類似のTF型組織の歴史的先例からは、その機能・意義は次の3点に要約される。第1に、NISの能力を活用したターゲティングや打撃の効果測定といった「作戦情報支援（intelligence support for operations）」、第2に、政府内外の利害関係者との作戦上の衝突回避（deconfliction）の調整、第3には同一施設での勤務等を介したTF構成組織要員間での対処権限の隙間や組織文化の溝の克服も含めた相互運用性の強化である[18]。

この無害化TFも、（A）と異なる意味でNIS本体との関係では「出島組織」となる。政策決定者の戦略級の意思決定支援と異なる戦術・作戦級の情報収集・分析需要が大きく、「作戦とインテリジェンスの融合（ops/intel-fusion）」と呼ばれる通例のNISとは異なる行動原理も要求されるからである。

５．むすびにかえて―日本の現在地と論点

以上の2つの組織類型は、いずれもNIS本体の原理原則と異なる運用がなされる「出島組織」であり、近年のCS政策の要請とNISの能力基盤を接続し、政府の情報機能を活用したオペレーションを通じてCS政策執行を支援する。ただし（A）は、被害者支援のための対外的情報発信や官民連携を重

---

[12] 瀬戸 崇志「CTIの生態系/市場と対峙する政府のインテリジェンス」防衛研究所 新領域研究会（2024年3月1日）8–18頁。

[13] 本稿の（B）の組織類型の先行研究ならびに本稿第4節の記述は、別途の引用注で断りが無い限りは、以下を参照。瀬戸 崇志「民主主義国家の『サイバー軍』による攻勢的サイバー作戦能力の整備と運用―米軍とオランダ軍における『二重の統合』の過程に着目した比較事例研究」『安全保障戦略研究』第4巻第2号（2024年3月）177–201頁。

[14] FBI, "National Cyber Investigative Joint Task Force,"(no date); White House, *National Cybersecurity Strategy*, (March 2023), .11–15.

[15] U.S. Department of War, "How U.S. Cyber Command, NSA are Defending Midterm Elections: One Team, One Fight," (August 2022).

[16] National Cyber Force (NCF), "Responsible Cyber Power in Practice," (April 2023).; NCF, "National Cyber Force Explainer,"(no date).

[17] 前掲注4 豪州CS戦略 21頁他、次を参照。David Hollingworth, "AFP Commissioner Outlines Medibank Hacker Hunt and Impact of Sanctions," *CyberDaily.au,* February 15, 2024.

[18] 本段落の記述は、前掲注13のほか、以下の先行研究も参照。Anonymous, "All about access: Insights from NLD DISS Cyber Operations and Their Implications for Digital Striking Power," *Militaire Spectator*, vol. 191, no. 9 (September 2022). ; Evan Munsing and Christopher J. Lamb, *Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success*, (NDU Press, 2011).

視するのに対し、（B）は無害化作戦の運用保全（OPSEC）の要請や危機管理の要請上、（A）に比して元来の NIS に近い秘密主義や自己完結性を重視する誘因は強くなる。この点が英国や豪州が、同一の NIS の基盤に依拠しつつ、（A）と（B）に応じた別個の組織体を置く背景の一つとみられる。

現在の日本政府の体制/態勢整備も、この国際的潮流に沿う。（A）は、2025 年 12 月 23 日に閣議決定された「サイバーセキュリティ戦略」ならびに「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」を踏まえると、警察や防衛省・自衛隊の脅威ハンティング能力も含め、サイバー脅威情報の収集・分析とその成果物の民間や同盟・同志国との共用における国の役割の強化を規定しつつ、政府 CS 専門機関としての国家サイバー統括室・内閣府を介した有機的な省庁間・官民連携強化が模索されている[19]。（B）も、既存法令（警察官職務執行法ならびに自衛隊法）の改正をふまえた、従来の令状でのサイバー犯罪捜査とも有事（武力攻撃）の認定後の軍事作戦とも異なる平素の無害化作戦のための権限新設や、アクセス・無害化措置をめぐる警察と自衛隊の共同運用強化の取り組みは、諸外国の無害化 TF に近しい[20]。

最後に、今後の体制/態勢整備で論点となりうる点に触れたい。第 1 に、本稿が触れた 2 つの出島組織の連携であり、各々の任務の権限で得た情報を相互の任務支援に活用する方法が論点となる[21]。第 2 に、新設の独立機関と無害化 TF との関係性であり、アクセスを伴う無害化に必要な現場の運用裁量や OPSEC の要請と、独立機関の関与による民主的説明責任の担保の均衡点をいかに見出すか、である[22]。これらはいずれも本稿の紙幅を超えるが、2 つの「出島組織」を通じた日本版 ACD の具体化を考えるに際し、今後の研究の進展が望まれよう。

（2025 年 12 月 25 日脱稿）

本稿は、東京海上ディーアール株式会社が運営する調査研究プロジェクト「サイバー安全保障と能動的サイバー防御（ACD）」の成果の一部です。
https://www.tokio-dr.jp/thinktank/acd/

[19] 前掲注 1 （「サイバーセキュリティ戦略」） 15 頁-17 頁のほか、次を参照。内閣府政策統括官（サイバー安全保障担当）「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」サイバーセキュリティ戦略本部 閣議決定（2025 年 12 月 23 日）；NCO「各ユニットの概要」（2025 年 10 月 1 日）。

[20] 前掲注 1 （「サイバーセキュリティ戦略」） 14 頁ならびに前掲注 2（「サイバー対処能力強化法及び同整備法について」）13-14 頁。

[21] こうした活用事例は、例えば次を参照。RSA Conference, "Integrating Cyber Operations: CISA & CyberCom-CNMF Partnership," *YouTube*, June 7, 2023.; 瀬戸 崇志「米国サイバー軍の『ハントフォワード作戦（Hunt Forward Operations）』（2018 年～2025 年）――データ・歴史・実務の視点から捉える 7 年間の発展の軌跡」『NIDS Research＆Analysis』No.5（防衛研究所、2025 年 12 月） 22-26 頁。

[22] 以下を参照。"Can Lawyers Lose Wars by Stifling Cyber Capabilities?," *Binding Hook*, July 23, 2024.