新たな段階に進む「能動的サイバー防御（ACD）」

東京海上ディーアール株式会社
主席研究員 川口貴久*

2025 年 5 月 16 日、サイバー対処能力強化法案及び同整備法案[1]が通常国会で可決された。「国家安全保障戦略」（2022 年 12 月閣議決定）で掲げた「能動的サイバー防御（active cyber defense: ACD）」態勢は制度的基盤が整備されたことにより、能力構築とオペレーションという次の段階に移行する。

そこで本稿は ACD を構成する 3 つの措置の概要と能力構築・オペレーション段階で想定される論点を明示したい。

1．日本版 ACD

2022 年国家安保戦略は、日本のサイバー安全保障分野での対応能力を「欧米主要国と同等以上」とするという高い目標を掲げ、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃」を未然に排除し、攻撃の被害拡大を防止するために、ACD を導入する、とした[2]。

つまり「日本版 ACD」の焦点は武力攻撃「未満」のサイバー攻撃である。日本やその同盟国は、国連憲章を含む既存の国際法はサイバー活動にも適用されるとの立場から、一定のサイバー攻撃を「武力攻撃」とみなしうる。しかし、ACD が武力攻撃未満のサイバー攻撃に焦点を当てたことには理由がある。第一に、武力攻撃相当のサイバー攻撃は既に「防衛大綱」（2018 年 12 月閣議決定）の中で「相手方によるサイバー空間の利用を妨げる能力」を開発・行使することで対処する、としている。第二に、より重要な点として、これまで武力攻撃に相当するサイバー攻撃は確認されておらず、日本や各国が直面してきたサイバー脅威は諜報活動、先端技術や軍事技術の窃取、重要インフラに対する破壊的・妨害的攻撃とその準備活動であった。こうした攻撃や活動は単なる「犯罪」を超えているが、「武力攻撃」の閾値を超えていないという意味で、サイバー空間の「グレーゾーン活動」とも呼べる。こうした事情から、ACD の適用範囲を主に武力攻撃未満のサイバー攻撃とした。

国家安保戦略や「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 6 月～11 月）の報告書では、ACD は①官民連携の強化、②通信情報の利用、③アクセス・無害化の 3 つの措置と、横断的課題として組織・体制整備等から構成される。

2．官民連携の強化

「官民連携の強化」とは、基幹インフラ事業者による特定の電子計算機の届け出やインシデント報告の

---

* 東京海上ディーアール株式会社 ビジネスリスク本部 兼 経営企画部 主席研究員、マネージャー。

[1] 法案の詳細は、内閣官房サイバー安全保障体制整備準備室「サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）」を参照。

[2] 『国家安全保障戦略 2022』（国家安全保障会議および閣議決定、2022 年 12 月 16 日）、30 頁。

義務化、情報共有・対策のための新たな協議会の設置、脆弱性対応の強化等を含む。

この取組みは近年制定された２つの経済安全保障関連法、すなわち経済安全保障推進法と重要経済安保情報保護活用法との相乗効果が期待される。経済安全保障推進法の 4 本柱の１つは、基幹インフラのサプライチェーン・サイバーセキュリティを強化するもので、同法等で指定された 15 業種・215 の基幹インフラ事業者は ACD 関連法案によって新たな義務が課される。また、重要経済安保情報保護活用法はセキュリティ・クリアランス制度の民間適用を大幅に拡大するもので、ACD 関連法案で設置される協議会での機微なサイバー脅威情報共有でも適用・運用が期待される。

「官民連携の強化」は、基幹インフラ事業者、ソフトウェア・ベンダ、その他事業者等、最も民間事業者とのかかわりが大きい措置である。今後の詳細な制度設計や運用では、民間事業者にどれだけメリットと実利があり、実質的かつ積極的な参画が期待できるかがポイントの一つであろう。例えば、インシデントを報告した場合、当該企業は政府による支援や公助が期待できるのか、民間事業者のクリアランス取得者が協議会から有益なインテリジェンスを即時に得られるか等である。

３．通信情報の利用

「通信情報の利用」とはインターネット・サービス・プロバイダ（ISP）や移動体通信等の通信事業者や一部の基幹インフラ事業者と協力し、通信情報を収集・分析し、攻撃や攻撃インフラを検知し、サイバーセキュリティ環境の改善を図るものである。これは、憲法 21 条の「通信の秘密」との整合の観点から、法案審議で最も注目を浴びた措置であろう。

日本のサイバー安全保障能力の向上という文脈では、「通信情報の利用」は日本の SIGINT（signals intelligence）能力、正確にはデジタル有線情報の SIGINT 能力を大きく向上させることが期待される。

SIGINT 能力とサイバーセキュリティは密接不可分にある。サイバー安全保障分野で日本がベンチマークする「欧米主要国」では、国家的なサイバーセキュリティ機関は、その国の SIGINT 能力を活用できるか、SIGINT 機関そのものである。例えば、2023 年 5 月に公表された Volt Typhoon によるサイバー攻撃キャンペーン[3]に対して、ファイブ・アイズ諸国（米英加豪 NZ で構成される機密情報共有の枠組み）は共同で注意喚起を行った[4]。実施主体は米国の国家安全保障局（NSA）、連邦捜査局（FBI）、サイバーセキュリティ・インフラセキュリティ庁（CISA）、英加豪 NZ のサイバーセキュリティ機関・部門である。このうち、NSA と４カ国のサイバーセキュリティ組織は、SIGINT 機関またはその一部組織・隷下機関である。

こうした意味で、「通信情報の利用」はサイバー安全保障能力を向上させる上で不可欠な取組みである。ただし、日本の通信情報の利用は欧米諸国と比べれば、極めて抑制的な制度設計である。①「目的」という観点ではサイバーセキュリティ向上に限定され（諸外国では治安・テロ対策や安全保障全般のためにも活用される）、②「対象」という点では内内通信（国内間の通信）が除外され、「個人のコミュニケーションの本質的内容に関わる情報」以外（メタデータや機械的情報）が対象であり、③「プロセス」という点ではまずは機械による自動処理が施され、データの保存期間も限定的である。

また、実際に通信情報を分析するハードおよびソフト面での準備がこれからだ。膨大なデータを収集・保管・処理する物理的インフラや処理装置、自動的な

[3] Microsoft 社や米国インテリジェンス・コミュニティ等によれば、Volt Typhoon は中国政府に関係するサイバー攻撃グループで、グアム、ハワイ、米国西海岸の重要インフラに侵入し、破壊・妨害工作のために「事前配置」活動を行った。その目的は、将来の東アジア有事で、米国の意思決定を阻害し、米国社会を混乱させ、米軍の即応展開を遅延させることである。

[4] “People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,” Cybersecurity and Infrastructure Security Agency, May 24, 2023.

機械処理のための具体的な設計等が必要である。通信情報から得られるサイバー脅威情報と地域情勢・地政学的動向を統合的に分析しなければならないかもしれない。

４．アクセス・無害化

「アクセス・無害化」とは、重大なサイバー攻撃を未然に防ぐため、攻撃サーバ等に侵入し、対象を無力化・無害化することである。実施主体は、警察や自衛隊とされている。

「アクセス」と「無害化」は並置されているが、両者の隔たりは小さくない。前者がサイバー空間での広範な探索活動と標的を絞った無害化準備活動を指すのに対し、後者は実際に不可逆な効果・影響をもたらすものである。 サイバー空間の“実質的な”国際法とも呼べる「タリン・マニュアル」に従えば、前者は多くの場合、合法であることが多いが、後者は適用される規範やその基準が不明確であり、今後の国家実行に委ねられる面が大きい（逆にいえば、無害化措置は国家実行として、国際法形成に貢献することが可能である）。

アクセス・無害化についても、その能力構築、発動の基準等、多くの論点がある。特に重要なことは、無害化措置は確かに強力な措置であるが、サイバー攻撃キャンペーンやサイバー攻撃者に対する対処手段の一つに過ぎず、異なる手段を組み合わせる必要がある点だ。その手段は、技術的措置に加えて、外交・経済的措置等の必要なあらゆる手段が含まれる。先行する欧米諸国の手段も含めると以下のようなオプションが考えられる[5]。

1. 注意喚起（一般向け連絡、非公開での情報共有活動参加者への連絡）
2. 情報共有（情報共有活動参加者へのインディケータ展開）
3. 関連組織への通知（脆弱な機器／侵害された機器の利用者への通知、不正な通信が発生している組織の特定と通知）
4. 解析レポートの公開（攻撃手法や攻撃インフラの暴露、侵害指標（IoC）等の脅威情報の共有）
5. フィルタリング
6. 事業者と協力した通信遮断・テイクダウン
7. 他者が管理するネットワーク・情報資産へのアクセス・情報収集
8. 無害化
9. パブリック・アトリビューション（特定したサイバー攻撃者の公開、名指し批判）
10. 刑事訴追等の司法的措置
11. ペルソナ・ノン・グラータ等の外交的措置
12. 金融制裁指定等の経済的措置

こうしたオプションを整備した上でも、さらに具体的な論点が浮かびあがる。どのような類のサイバー攻撃（者）にどのような対処オプション（の組み合わせ）が有効なのか。迅速性が求められる状況下で政治的決定と現場裁量の均衡をどのように図るのか。事後検証や説明責任の観点で、どのようなサイバー攻撃対処のプロセス・手続きを確立する必要があるのか。このプロセスで、民間事業者のどのような能力と協力が必要なのか。

日本版 ACD は関連２法案の成立で、能力構築と運用という新しい段階に進む。この段階での論点は少なくなく、いずれも重要なものである。東京海上ディーアールが設置した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）」は、能力構築とオペレーションという ACD の新しい段階で必要とされる論点について、議論と分析、発信と提言を行っていく。

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/

[5] 本文中のオプションは、研究プロジェクト・メンバーとの議論結果、特に石川朝久氏、佐々木勇人氏が提示した見解を反映したものである。