資料４

2025 年 10 月 30 日

サイバーセキュリティ戦略（案）に関する意見提出書

慶應義塾大学教授／国際文化会館常務理事
神保　謙

１．抑止論の体系化と戦略３文書との融合

本戦略（案）は、従来の任務保証とリスク管理を軸とした受動的防御から脱却し、サイバー空間における能動的な防御と抑止の一体化を明確に打ち出した点で高く評価できる。サイバー脅威が平時と有事の境界を曖昧化させる中で、本戦略（案）が「能動的サイバー防御」を中核的施策として位置づけたことは、我が国の安全保障政策の重要な転換点である。

本戦略（案）は、能動的サイバー防御の実現に向けて、これまでの防御的・受動的な枠組みを越え、政府の主導的役割を明確にしている。その中核は、①国家サイバー統括室（NCO）における情報集約と統合分析の強化、②官民における脅威ハンティングの実施拡大、③アクセス・無害化措置をはじめとする能動的な防御・抑止の運用体制確立、の三つの施策である。

これらはいずれも、2021 年戦略で示された「官民情報共有と包括的対処の理念」を基礎に、これを平素からの能動的防御と抑止の体制へと発展させた制度設計として位置づけられる。とりわけ、NCO による情報集約と分析強化は、これまで各機関に分散していたインシデント情報を統合し、潜在的脅威の早期発見・特定を可能にする基盤的改革である。

さらに、本戦略は、抑止理論の三層構造を明示的に整理している。すなわち、①攻撃の探知・妨害による拒否的抑止（deterrence by denial）、②法的措置や無害化措置の示唆による懲罰的抑止（deterrence by punishment）、③情報共有・能力開示・国際連携による関与的抑止（deterrence by entanglement）の三層を組み合わせ、攻撃者に複合的なコストを課す設計となっている。

２．制度の成熟化に向けた補強

第一に、能動的サイバー防御の階層的整理である。アクセス・無害化措置を国家による最終手段と位置づけつつ、その前段階の警告・封じ込め・模擬侵入演習などを「準能動的措置」として制度化することが望ましい。各段階において成果指標（KPI）を設定し、検知速度・被害抑止率・再発防止効果などを定期的に把握することで、政策の説明責任と透明性を高めることができる。

第二に、通信情報利用とアクセス措置の監理・説明責任の強化である。サイバー対処能力強化法に基づく通信情報監理委員会を中心に、年次報告（実施件数等）の国会への報告

及び国民への公表を着実に実施すべきである。高度な機微情報に関する保全上の制約を踏まえつつも、制度運用の実績を定期的に示すことが、能動的サイバー防御への国民的理解と信頼を高める上で不可欠である。

第三に、官民脅威ハンティング体制の恒常化である。政府・企業・研究機関が共同で脅威探索を行う「官民サイバー連携タスクフォース」を常設し、重要インフラや防衛産業を中心に実戦的演習を定例化することが望ましい。これにより、民間の技術力と分析力を国家防衛の一翼として制度的に統合できる。

３．国際整合性とエスカレーション管理の制度化

能動的防御の拡充にあたっては、国際法上の整合性を確保することが不可欠である。タリン・マニュアルに示される「必要性・比例性・帰属可能性」の原則を厳格に適用し、アクセス・無害化措置が他国の主権侵害や武力行使に該当しない範囲を法的指針として明確化すべきである。

さらに、攻撃源に外国政府の関与が疑われる場合には、外交チャンネルを通じた事前通知・事後通報・国際協議の枠組みを整備し、誤認やエスカレーションの連鎖を防ぐ必要がある。日米同盟および同志国との間で能動的防御に関する「相互運用原則（Rules of Engagement)」と「情報共有閾値」を整合させ、共同抑止の一体性を高めることが望ましい。これにより、対外的誤解や過剰反応を最小化し、国際社会に対して法的正当性と透明性を示すことができる。

能動的防御の実施においては、外交的エスカレーションだけでなく、国内における作戦レベルのエスカレーション管理も極めて重要である。国家サイバー統括室（NCO)、警察庁、防衛省・自衛隊は、平素から有事に至るまで一貫した情報共有・判断・対処のプロセスを構築することが求められる。

４．結語

本戦略（案）は、日本が「サイバー空間の受動的被害国」から「能動的防御国家」へと移行するための制度的基盤を提示するものである。今後は、①抑止構造の多層化、②権限行使の説明責任、③国際整合性とエスカレーション管理の制度化を三位一体で成熟させ、抑止とレジリエンスを同時に高める戦略として発展させることを強く期待する。

（了）