能動的サイバー防御の課題：対処プロセス、リスク推定、効果測定

芝浦工業大学
持永 大*

本稿では、日本版能動的サイバー防御における課題を指摘する。具体的には、対処プロセスの確立、サイバー攻撃被害のリスク推定、そして対処の効果測定である。能動的サイバー防御とは、サイバー攻撃による被害を防ぐために、注意喚起等をはじめとする複数の対象を組み合わせる防御手法である。

なかでもアクセス・無害化措置は、日本政府の対処手段を拡大する新たな措置である。2025年５月に成立した重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（サイバー対処能力強化法整備法）により、政府は被害が顕在化する前に、民間事業者が管理するコンピュータへ対処できるようになった。

しかし、国際的にアクセス・無害化措置は、防御側が取り得る最後の手段と位置付けられている。そのため政府は、実施前にその適切性を慎重に判断し、対象となるコンピュータの数を絞り込み、実施後には対処が適切であったことを説明しなければならない。

以上をふまえ、本稿ではまず対処プロセス確立の必要性を指摘する。攻撃兆候の認知からアクセス・無害化措置に至る一連の対処プロセスを確立すれば、政府は対処の適切性を判断しやすくなる。なぜなら、複数の対処を実施する際、「いつ」「誰が」「どんな基準で」対処するかを明確にしておくことが、対処をエスカレートさせる際に不可欠だからである。

また、政府が事前に対処プロセスを確立すれば、政府内で共通認識が醸成され、迅速な対処につながる。この共通認識があれば、各省庁は対処の段階的なエスカレーションを相互に把握し、対処期間を有効活用できるようになる。

第二に、サイバー攻撃被害のリスク推定の必要性を指摘する。政府は日本にとっての「重大な危害」を認定する際、どのような指標を用いるべきかを検討し、定量化する必要がある。一般的に、サイバー攻撃に伴うリスクは定性的・定量的な観点から分析する。しかし、サイバー対処能力強化法整備法における「重大な危害」の定義は明確ではない。

新法では、「国家及び国民の安全を著しく損なう事態」や「特定侵害事象」という概念を示しているものの、定量化は難しい。そのため、サイバー攻撃被害が重大な危害に該当するかを判断できる定量的な指標が必要である。

また、対処の適切性について国内的な観点からみれば、政府による対処の対象は、基幹インフラに設置された重要電子計算機を狙う規模の大きいサイバー攻撃である。国際的な観点からみれば、サイバー対処能力強化法整備法は海外のコンピュータへの対処も認めているため、政府は国際法上の正当性も検討しなければならない。

国際法の基準からみれば、アクセス・無害化措置が正当と認められるのは、領土の一体性、政府の統治機能、国家の本質的な利益が損なわれた場合である。また、2015 年の国連政府専門家会合の報

* 芝浦工業大学システム理工学部 准教授

告書では重要インフラに対する攻撃をしてはならないと結論しており、他国による日本の重要インフラへの攻撃を国際法違反と指摘できる可能性もある。

国会での審議にもあったとおり、アクセス・無害化措置を海外のコンピュータに対して実施する場合、緊急状態（緊急避難、Necessity）と対抗措置（Countermeasures）として位置付けることができる[1]。例えば、2024 年に米国が実施したボルトタイフーンへの対処では、初期段階は通信インフラで利用される機器への攻撃という差し迫ったリスクへの対応であり、緊急避難に近かった。その後、米国は攻撃への中国政府の関与を認定し、対抗措置（制裁、外交的抗議、継続的テイクダウン）へ移行した。

第三に、サイバー攻撃キャンペーンへの対処には、事前の適切性と事後の有効性を評価する効果測定が必要である。攻撃者の戦術変化等によって想定した効果が得られない場合、措置が数か月、場合によっては 1 年以上続く可能性がある。こうした長期化に対応するため、措置の継続や方針転換を判断する効果測定が必要である。さらに、日本のサイバー対処能力強化法整備法においても、独立機関による監査、措置期間の延長に承認が必要なこと、国会に対する報告が定められている。措置の延長を判断する基準や国会への報告という観点からも、効果測定を検討すべきである。

1．対処プロセスの確立

能動的サイバー防御では、攻撃キャンペーンへの対処プロセスを確立する必要がある。防御側は一定の被害を受けた後、限られた時間で対応しなければならない。そのため、攻撃の効果を低減し、さらなる被害拡大を防ぐ行動を迅速に実行する必要がある。本稿では、攻撃単位での防御ではなく、攻撃キャンペーンに対する対処を検討する。ここで攻撃キャンペーンとは、一定期間内に特定の目的のために、特定の攻撃手法や攻撃インフラを用いるサイバー攻撃活動を指す。この活動は数年単位で繰り返されることもある。具体的には、「いつ」「誰が」「何を」実施するかという観点から対処を検討する。

攻撃キャンペーンへの対処の具体例として、米国政府が実施したボルトタイフーンへの対処を詳しく見ていく。2023 年 12 月、米司法省は民間機器をサイバー攻撃から守る作戦を実行した。中国政府が支援するボルトタイフーンに乗っ取られた機器の制御を取り戻すため、米政府は裁判所の許可を得て機器に侵入し、マルウェアを除去したのである。この最終的な対処に至るまで、米政府は段階的に対処を進めていた。

2023 年 5 月、米政府やベンダは対処の初期段階として、注意喚起により脆弱性対策を呼びかけ、攻撃手法を公開した。この注意喚起は、家庭用ルータの保護方法や攻撃検知の方法を示し、民間事業者にも対策が呼びかけられた。米政府は、攻撃者が長期間にわたって重要インフラの情報システムや監視用カメラにアクセスしていたことを指摘した。その後、最後の段階として、裁判所の許可を得て、米司法省がマルウェアの除去や再感染防止措置を行った。

この対処例をふまえると、政府は対処開始の判断基準や対処の選択肢をあらかじめ設計しておく必要がある。

ボルトタイフーンの事例では、攻撃キャンペーンの開始から最終的な対処まで少なくとも 5 年を要した。内訳をみると、政府が攻撃を認知してから対処開始を判断するまで 2 年半、注意喚起から米司法省による機器への侵入まで 6 か月かかった。このように長期化する攻撃キャンペーンに対応するため、政府は対処のタイムラインを想定し、対処開始の判断基準と対処プロセスをあらかじめ定めておく必要がある。

2．対処のタイムラインと被害の閾値、リスク推定

対処プロセスを確立するには、まず政府が対処すべきサイバー攻撃を定義する必要がある。政府は、

[1] 榎本尚行「能動的サイバー防御 2 法案の国会論議（3） －アクセス・無害化措置の概要と論点－」『立法と調査 477 号』、2025 年 7 月 25 日

2022 年末の国家安全保障戦略において「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」、2025 年のサイバー対処能力強化法における審議では、例として、「有事における機能不全を生じさせることを念頭に、そうした事態に至る前の段階から基幹インフラのシステム内部へのアクセスを確保するタイプのサイバー攻撃」、分散型サービス妨害攻撃（DDoS 攻撃）、ランサムウェアを用いた攻撃としている[2]。いずれも、政府が対処を行う判断基準は、これらの攻撃の規模、効果の大きさ、または状況によると想定できる。

サイバー攻撃キャンペーンを認知した段階で、重大被害につながるかどうか、重大被害に達するまでの時間はどれくらいかを把握する必要がある。サイバー攻撃キャンペーンの認知には、一定の時間と被害の発生が必要である。なぜなら、攻撃側は検知されないよう隠密性を重視して活動するため、防御側が攻撃開始のタイミングを推測することは難しいからである。その結果、防御側は一定の被害が発生した後に初めて攻撃を認知することになる。

今後の政府による施策は、認知から対処を実施するまでの時間確保を念頭に、早期検知と迅速な判断を可能にする方針に基づくべきである。例えば、ソフトウェアや製品の脆弱性悪用状況、攻撃者や攻撃ツールの把握、インターネット上にある脆弱なコンピュータの数、基幹インフラで利用されるソフトウェアや製品への影響等を統合的に分析できるフレームワークが必要だろう。

特に、攻撃キャンペーンで狙われる脆弱性については、その悪用可能性や悪用開始時期を考慮できる仕組みが必要である。脆弱性の悪用状況を把握する上で、これまで対策や被害の見積もりに使われてきた CVSS（共通脆弱性評価システム）では、悪用によるインパクトは見積もれるが、どれくらいの時間で悪用されるかは分からない。

そこで、近年 EPSS（脆弱性悪用予測スコアリングシステム）が発表されている[3]。EPSS は脆弱性が実際に悪用される確率を予測する指標であり、現在も精度向上が進められている。加えて、政府が収集した情報に基づく客観的な指標も必要である。政府は基幹インフラ内の重要電子計算機やネットワーク構成等の評価データを取得でき、また通信情報の活用によって攻撃活動を把握できる。こうした独自の情報を活用し、対処開始のトリガーとなる指標を整備すべきである。

リスク推定のフレームワークでは、インパクトと悪用可能性に基づくリスク算定が可能である。ここで悪用可能性とは、EPSS、インターネット上に露出している端末のスキャン結果、攻撃コード公開の有無等を指す。また、インパクトとは、CVSS 基本値、影響を受ける機器・システムの分布（基幹インフラを含む）、攻撃インフラ化の可能性、コンポーネント単位の波及等を指す。

特に、EPSS は CVSS よりも悪用されやすい脆弱性の絞り込みに有効であり、EPSS と CVSS の双方が高いものは、早期対処候補として重点監視するといった方法がある。一方、EPSS は日次で更新されモデル改訂も頻繁に行われるため、適切な閾値設定（例：悪用確率 1%以上を注視）や急上昇検知の運用が重要である。また、EPSS は 30 日先の予測に偏る傾向があるため、より長期的な見立てを補う検討も必要である。

さらに、重点監視対象となった脆弱性であっても、日本国内で利用されていないものは監視対象から外すといった最適化も求められる。なぜなら、基幹インフラで利用されていない機器やソフトウェアの脆弱性は新法のスコープ外であり、限られたリソースを有効活用する工夫が必要だからである。

3. 効果測定（事前評価／事後評価）

第三に、サイバー攻撃キャンペーンへの対処には、事前の適切性と事後の有効性を評価する効果測

[2]「第 217 回国会 参議院内閣委員会 第 10 号 令和 7 年 4 月 22 日」国会会議録検索システム（2025 年 10 月 15 日アクセス）
[3] "Exploit Prediction Scoring System (EPSS)," FIRST（2025 年 10 月 15 日アクセス）

定が必要である。

諸外国では、長期措置に対する司法監督や独立機関によるレビューが一般的である。日本では、新法により通信情報を活用したサイバー攻撃対処が可能となった。アクセス・無害化措置が通信情報活用の延長線上にあるならば、実施状況の公表や再評価といったガバナンスが重要となる。

効果測定には、事前評価と事後評価の両面がある。事前評価（実施判断）では、対処が引き起こす影響、対処に伴うリスク、対処手法・対象の適切性を評価する必要がある。また、手続きの透明性や人権・自由権への配慮も重要な評価項目である。実際、米国のサイバー作戦における事前評価では、対処の影響、対処に伴うリスク、対処方法、地理的条件・対処相手の識別、透明性と自由権といった項目を評価していた[4]。

事後評価では、対処目的の達成度（例：インターネット上の対象コンピュータの 8 割以上を処理）や攻撃キャンペーンの収束度合いを評価し、対処の効果を検証する必要がある。

さらに、対処の途中または終了後には、法的・技術的妥当性、運用リスク、調整プロセスの振り返りが重要である。欧米の事例をみると、米国では大統領政策指令 PPD-20 において年次報告を義務付け、法的妥当性・技術的実現性・運用リスク・調整手順を評価している。英国では調査権限法（IPA 2016）により、長期間にわたる監視措置は一度の承認で無期限に続けることはできず、定められた期間ごとに延長申請と独立機関による再審査を受ける仕組みがある[5]。ドイツでは、通信傍受等のサイバー作戦について立法府から独立した監督委員会が事前・事後審査を行っている。ドイツの連邦情報庁（BND）法は、政府が事前承認申請の段階で目的、範囲、実施期間を明示することや、承認を得た措置も無期限ではなく定められた期間経過後には承認失効または継続に再承認が必要であることを定めている[6]。

日本のサイバー対処能力強化法整備法においても、独立機関による監査、措置期間の延長への承認要件、国会への報告が定められている。これらの規定から、日本が欧米並みのサイバー対処能力の一環として、事前事後の評価を組み込もうとしていることがわかる。措置の延長を判断する基準や国会への報告という観点からも、効果測定は不可欠である。特に、通信情報の活用やアクセス・無害化措置といった措置が長期化した場合、政府は効果を検証すべきである。攻撃者の戦術変化等によって想定した効果が得られず、結果的に措置が数か月、場合によっては 1 年以上続く可能性があるからである。

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/

[4] "Obama tells intelligence chiefs to draw up cyber target list," The Guardian, June 7, 2023.
[5] "Investigatory Powers Act 2016," The National Archives of the UK（2025 年 10 月 15 日アクセス）
[6] "Drucksache 19/26103 19. Wahlperiode 25.01.2021Gesetzentwurf der Bundesregierung," Deutscher Bundestag, January 25, 2021.