「わが国におけるアクティブサイバーディフェンスに関する法制度研究会」報告書

能動的サイバー防御実現のための提言とともに

－ 国民の生活と安全を守るために必要な議論を求める －

2023 年 6 月

紀尾井町戦略研究所株式会社 編集

はじめに
－ 暗闇から抜け出すために　－

本報告書は「能動的サイバー防御」に関する報告と提言を主題とするものであり，「能動的サイバー防御」に関する議論が論点を漏らすことなく行われていくための起点を目指す。「能動的サイバー防御」について「防衛三文書」では明確な定義を記載していない。 本報告書においては「能動的サイバー防御」という言葉は，サイバー攻撃をしているコンピュータをテイクダウンする行為などの直接的な防御行為や相手方を特定するために行われるアトリビューションといった行為だけを指すものではなく，サイバー攻撃の端緒を探索することから始まり，サイバー攻撃を仕掛けてきている相手方を特定し，当該サイバー攻撃を無力化するために必要な行為を行うという総合的な防御対応全体を指して用いている。このように広く「能動的サイバー防御」を捉えなければならない背景は本報告書で詳述しているが，攻撃者が誰であるのか，どのような攻撃手段を用いているのかを把握することなしに，攻撃に対する適切な防御を行うことができないことにある。なお，アトリビューションやテイクダウンなど「能動的サイバー防御」に含まれる狭義の行為を指す場合には「サイバー防御措置」という文言を用いるものとする。

本報告書をこの時期にまとめた理由は，国内におけるサイバー攻撃に対する認識の変化がある。

「防衛三文書」の改訂が2022年末になされ，サイバー領域における防衛について「能動的サイバー防御」など従来よりも踏み込んだ記載がなされた。わが国が置かれた国際環境やロシアによるウクライナ侵攻で見られたようなサイバー空間での攻防を踏まえると，これまで正面から取り組むことが避けられてきた領域に取り組もうとしているものとして評価をしたい。しかしながら，安全保障を巡る議論がややもすると安全保障のための能力強化論対武力行使絶対反対論のような観念的な対立構造に陥ってしまい，必要な検討が十分になされないままになってしまう懸念がないとはいえない。日本国民の生命や身体や財産，そして産業を守るためには，ここで議論を後戻りさせることなく，遍く関連する論点について検討が行われることが必要であり，適切な議論が尽くされるよう民間からも論点を示し提言を行なっておきたい。

現在の日本は，サイバー空間での出来事についていわば自ら目隠しをして暗闇の中にいる状態にある。わが国は，サイバー空間で何が起こっているのかという全体像を把握できておらず，第三者から不正アクセスを受けたとしても，それが犯罪集団によるものなのか，他国によるものなのか，あるいは面白半分のハッカーによるものなのかさえ把握することが困難な状況にいる。一方，攻撃者側は目隠しを付けておらず自由自在に攻撃を仕掛けることができる環境にいる。このような事態は技術水準の差からもたらされているものではなく，わが国の法律に起因しているところが大きい。例えば，攻撃をしてきているサーバに無断でアクセスして必要な情報を解析し，指令を出している元まで辿っていくことは不正アクセス行為の禁止等に関する法律（いわゆる不正アクセス禁止法）などによって許されていないとされかねない。アクセスや解析のためのツールの作成や使用も刑法上の不正指令電磁的記録に関する罪（いわゆるウィルス罪）などによって大幅に制約されている。情報収集も，インターネットをはじめとした通信上の信号解析が電気通信事業法上の通信の秘密の保護に関する規制によって，罰則付きで禁止されているために充分に

行うことができない。以上の規制を踏まえると，攻撃ツールがダークウェブ[1]上で取引されていることがわかっていても，相手方に入り込んで正体に迫ることも，攻撃ツールを入手して解析することも非常に困難な状況にある。これが，現状である。それぞれの法律にも合理的な趣旨・目的はあるだろうが，「能動的サイバー防御」の実現との関係では，まさに自らの法律で自らに制約を課している状態であるといえる。

逆に言えば，どこまでの行動を許容すべきかの検討は必要であるが，憲法や国際法で許容される範囲において法律を改正し，制約をなくせば能動的サイバー防御は許されるということである。そして「能動的サイバー防御」の第一歩は，法律を変えて目隠しを外し目を見開き，暗闇から脱するということである。また「能動的サイバー防御」という表現からは，相手方に対する対抗措置の話だけであると捉えられがちであるが決してそうではない。対抗措置をどのように講ずるのかは相手方がわかってからの課題である。そもそもサイバー攻撃が誰によるものかさえ分からない状況では，適切な対処（対抗措置を含む）が難しいだけでなく，犯罪捜査としてアクションを起こせば良いのか，国の防衛としてアクションを起こせば良いのかもわからない。対処すべき行為主体を決めることさえ困難である。そしてその延長線上に技術的アトリビューションや解析ツールの利用，テイクダウン，ハックバックというものを考えていくことになる。

本報告書は道筋を示すために必要不可欠な議論や検討が迂回されることなく行われるために論点を示すことにより，国会議員を含む多くの人々に議論を尽していただくことを目指している。私たちは，サイバー空間という，国境がないだけではなく官民の境界も曖昧な領域で，どのように実効性ある安全保障を実現し，国民を守ることができるかについて余すことなく議論が行われることを望むものである。また，「能動的サイバー防御」が適切に機能することを目指すべきだという視点を失ってはならず，どのような行為を適法化するのかという議論と合わせて当該行為の限界についても見定めていかなければならないと考える。

能動的サイバー防御やインテリジェンスに関しては様々な見解があることは承知している。しかし，私たちの報告内容に単にノーを突きつけるだけでは何も生まれず，国民が直面している今ここにある危険を回避することには繋がらない。是非，クリティカルシンキングに基づいた発展的な議論に参加して頂きたいと考えている。加えて，この国に欠けてきた部分を補っていかなければならない課題故に提言の実現には時間を要するという側面も忘れてはならず，今すぐにあるいは短期的に実現不可能と思われる対応策を避けてしまうという選択も避けなければならない。それゆえ，私たちは，この提言に対する議論を避けることなく，より安全保障に資する多くの建設的な対案が出されることを期待して止まない。そのようにして産まれてくる議論こそが明日の日本に繋がると信じている。

[1] ダークウェブとは、匿名性の高い特別なネットワーク上に構築された Web サイトであり、ダークウェブ上では違法性の高い情報や物品が多く取引されている。また、取引に際しては暗号資産が対価として用いられることが多い。

本報告書の背景と構成

本研究会は，わが国において能動的サイバー防御の技術はありながらも，法制度の問題でこれを十分に実施できない現状を踏まえ，能動的サイバー防御を実施するためのフレームワークを構築するにあたりこれを阻む法制度を研究する目的で 2022 年 1 月に立ち上げられ，全５回の研究会での議論を経て，本報告書をとりまとめるに至ったものである。

本報告書は，紀尾井町戦略研究所が執筆した第１部の提言部分と，研究者の方々に執筆いただいた法律的な論点についての第２部という構成を採用している。第１部については研究者の方々の中でも様々な意見はあるものの，提言としてあるべき姿の一つを示すためのものであり，第２部は第１部の提言を支える法的枠組の可能性を示すためのものとなっている。特に第２部は研究者の方々に法的な枠組みの最大限を示していただくことに腐心いただき，本報告書の第１部で触れている手法について法律的にも可能性の範囲内にあることを示し，本報告書が建設的な議論のための叩き台となることを目指すものとなっている。このような難しい検討にご尽力いただいた研究者の方々に，取りまとめを行った紀尾井町戦略研究所として心から感謝を申し上げたい。

目　次

第１部

わが国における能動的サイバー防御のために

「はじめに」で記述したように，適切な情報収集なくして能動的サイバー防御は存立し得ない。そのため，本提言（本報告書における提言部分を，以下「本提言」という）は，必要不可欠な要素のプライオリティの順に情報収集，アトリビューション，テイクダウン，ハックバック，その他の執行について記述をしている。この順番は能動的サイバー防御の体系を考える上で重要であり，これらの要素を網羅して整備をしない限り機能し得ないものであることを最初に理解いただいておくことが肝要である。

能動的サイバー防御の行為主体―国と民間との共同体制

本提言において，能動的サイバー防御の主体は国またはその機関と位置付けている。民間の役割を否定するものではないが，能動的サイバー防御を実現するために対象行為の違法性を阻却させる必要性や国の防衛措置にも繋がる行為であることを考えると，さまざまな見解はあるものの現時点では，国またはその機関が主体となるという整理が望ましいからである。なお，能動的サイバー防御の整備はこれから緒につくところであることを考慮すれば，防御の実効性を評価しつつ必要に応じた民間の役割の強化を検討する可能性を否定するものではない。また，情報収集や情報提供など民間の協力が不可欠な領域における民間の役割が減殺されるわけではない。さらには，国またはその機関がその監督のもと，能動的サイバー防御の一部の行為について民間に委託することを否定するものではない。あくまでも主たる行為主体について，能動的サイバー防御を整備していく当初の段階においてどちらが主体となることが望ましいのかという視点での整理ととらえて頂きたい。

Ⅰ　能動的サイバー防御のための情報収集

1　一般情報[2]収集（民間による情報収集の促進と情報提供）

サイバー空間で起きている事象やどのような行為主体がいるのかについてわが国は情報をほとんど有していない[3]。しかし能動的サイバー防御を行なっていくためには，グローバルに何が起きているのかを把握する必要がある。そのために行うべきものはインターネット上での一般的な情報収集であり，この情報収集については行政機関に限定する必要はない。ここでは，より多くの情報を収集するためには民間の協力が不可欠であることを理解し，民間に情報提供義務を課すとともに，民間が情報収集を行う際の現行法における法律上の懸念（情報収集をしているハニーポットや Tor(The Onion Router)のノードが攻撃者に悪用された場合に幇助等の責任が問われる可能性など）については，それを払拭して，広く協力を求める必要があることも考慮に値する。これらに照らして，次のような施策を行うべきである。

---

[2] ここで「一般情報」とは公開されているか否かを問わず民間が通常の業務の過程で適法に入手している情報を指す。

[3] インターネット上で発生しているインシデント情報を有している企業は、オペレーティングシステム（OS）、検索エンジンなどのプラットフォーム、ウィルス対策ソフトウェアなどを提供している企業であるが、残念ながら日本企業でグローバルにそれらを提供している企業は存在していない。回線を提供している通信会社やインターネット接続サービスを提供する Internet Service Provider（ISP）も利用者端末に関する情報は有しているものの企業毎に分散して保有しているために全体像を把握することが難しい状況にある。

(1) OS 提供事業者，検索サービス提供事業者，ウィルス対策ソフトウェア提供事業者，電話会社， ISP のうち一定規模以上の民間企業（日本で事業を行う一定規模以上の海外企業を含む）に対して，インテリジェンス機関（詳細は後述）に対して把握しているサイバー攻撃（可能性を含む）の状況，入手した最新のコンピュータウィルスに関する情報，犯罪発生の可能性に関する情報，異常なアクセス情報，対外通信の内容（詳細は後述）などを提供する義務を課す。

(2) 行政機関や民間が適法にハニーポットや Tor のノード等を設置して情報収集するためのガイドラインを公表する（届出あるいは登録されたハニーポッドやノードについては，収集した情報についてインテリジェンス機関に提供を行なっている場合においては幇助責任等を問わないこととする等)。

(3) 全ての民間（企業）に対してサイバー攻撃を受けた可能性がある場合のインテリジェンス機関への報告義務（義務違反については可罰）を課す。

サイバー攻撃の実態を正確に把握するためには攻撃を受けた際に民間企業から情報提供がなされることが必要である。現状では情報共有が十分になされていないことからガイダンスなどが模索されている状況ではあるものの，任意の情報共有が進まない実態と能動的サイバー防御を実施していくための情報収集の必要性・重要性に鑑みると罰則付の一歩踏み込んだ国への報告について義務化を図っていくことが必要な段階にあると思料される。

２　インテリジェンス機関の必要性とあり方

能動的サイバー防御の実効性を高めるためには上述の一般情報収集に基づきインテリジェンス機関が情報分析収集を行わなければならない。情報収集はサイバー攻撃が行われている場合に限って行われるものではなく，サイバー上で何が起きているのかを常時分析し予見性を高めることが主目的である。インターネット上で行われている通信をはじめ，どのような通信が行われているのかという情報を収集分析することなくして的確なインテリジェンスを行うことは難しい。後述するように技術的手段によるアトリビューション（攻撃者特定）も制約されているが，仮に技術的アトリビューションの制約を取り除いたとしても，それだけで攻撃者の特定に十分な情報を得ることができるケースは少なく確度高く相手方を特定するためにはインテリジェンス活動による情報収集と分析が不可欠であるという現実がある。そのために個々の企業が保有していた情報を集積した上でSIGINT（Signal Intelligence）を行うことができる体制を整えておかなければならない。

また，ダークウェブ上で攻撃ツールの売買や攻撃によって入手されたデータの売買などが行われていることを観察はできるが，現状では売買の相手方となって当事者を特定したり，解析のためにツールを入手したりすることも制約を受けている。取引の相手方になることによって犯罪行為である不正指令電磁的記録提供の実行行為を行わせることに繋がることや，取引をしてツールを入手すること自体も不正指令電磁的記録取得に該当することになるために違法であると評価される可能性があるためである。また，攻撃者に対価を渡してしまうことで違法行為を助長することになるため，そこについてもどのように評価すべきかが不明確であることも行動の制約に繋がっている。インテリジェンス能力を高めるためには，これらについての考え方の明確化あるいは適法な行為として位置付けるための法律の修正が必要である。さらに，攻撃者のグループ内部への侵入を試みた際に，当該グループから能力等の確認のために不正アクセスなどの違法行為の実

行を求められた場合に当該違法行為を適法化できる余地を設ける必要性なども検討しなければならない。これらのアンダーカバー活動に関する規律が必要である。

加えて付言するならば，Five Eyesのメンバー国として認められるための要件としてもSIGINT機能を強化することは必須であるということも見据えておくべきである。

インテリジェンス機関に通信に関する情報を集約してSIGINTを行っていくための議論はわが国においては十分に行われてきていない。わが国にも内閣や警察，自衛隊などにそれぞれインテリジェンスを担う機関が存在し重要な役割を担ってきており，それらの活動の継続や強化はますます重要である。上記のダークウェブ上などにおけるアンダーカバー活動を担う能力を備えている組織は既存の組織に他ならない。しかし，それに加えて通信の解析を中心とするSIGINT機能やアンダーカバー活動の強化もまた必要であるというのが本提言の趣旨である。もちろん，ここで述べたようなSIGINT機能の強化は不要である，あるいは，別な方法でも十分な情報収集ができるのではないかといった意見もあると認識しており，具体的にどのような方法であれば十分な情報収集と分析を実施することができるのかという対案も期待したい。

(1) 上記の通り，何が起ころうとしているのかと言う予見性を高め，誰が実行行為者であるのかを確度高く特定し，海外からも信頼されるようになるにはインテリジェンス機能を強化することが不可欠である。そのために必要な施策としては次のものが挙げられる。

- サイバー攻撃の準備行為や国の安全保障に関する情報収集を違法行為とした上で，当該行為を調査できる下記の権限を行政機関（以下「インテリジェンス機関」という）に付与し，必要な設備（データセンターを含む）を整える。なお，インテリジェンス機関は高度な秘密保持の必要性と専門性を確保するため定期的な人事異動を行わない専任組織とする必要がある。既に，内閣サイバーセキュリティセンター（NISC）を改組するという案も出されているようであるが，新組織を創設するにしろ，現状の組織を改組するにしろ，ここに記述する機能を持たせる必要がある。
- 対外国通信の分析のためのメタ情報の取得と通信内容の把握のために，日本国内でサービスを提供している電気通信事業者に対してインテリジェンス機関への情報提供義務（あるいは機器へのアクセス権）を課す。これには，発信者特定に資するトレースバックの仕組を組み込む義務を電気通信事業者に課すことを含む。
- 上記の一部として海外プラットフォーマーとインテリジェンス機関との間で情報提供に関する協定締結し，自主的な情報提供の枠組を設定する。
- ダークウェブ上での攻撃ツールの売買，データ売買の当事者を特定する目的で行うアンダーカバー活動を行うことができる権限をインテリジェンス機関に付与し，法令行為として正当な行為とする。これには，違法攻撃ツールの入手と解析を可能とできるよう権限をインテリジェンス機関に付与することを含む。
- インテリジェンス機関内に収集した情報の集積，分析のためのデータセンター設置，ツール等のテスト環境の構築を行う。

(2) インテリジェンス機関が収集した情報のうち特定秘密に該当するものは，国会報告の対象

とする。

(3) 収集した情報については原則としてインテリジェンス機関が安全保障の目的の範囲内で使用するものとするが，司法捜査や自衛隊の職責に係る場合には，当該情報をインテリジェンス機関から捜査機関，自衛隊に提供することができるものとする。ただし，インテリジェンス機関が収集した情報については刑事手続上の証拠能力は認めず，司法手続において必要な証拠収集は司法捜査機関が独立して行うものとする。

(4) インテリジェンス機関の予算及び決算については，国会の秘密会において厳格に審査するものとする。また，インテリジェンス機関の活動については，第三者機関による監査を受けるものとし，定期的に国会に監査結果を報告するものとする。

(5) インテリジェンス機関による情報収集，分析結果については内閣総理大臣に対して毎日レポートを行うことを義務づける。

わが国にはFive Eyes諸国が有しているような幅広く通信情報を収集分析するようなSIGINT機能を有した機関はまだ存在しておらず，一から創り上げていかなければならない。組織や設備の整備と合わせて手法を確立していくためには経験の積み重ね（年月）が必要であることは言うまでもなく，着手が遅くなればなるほど何もできない期間が伸びていくことになることを忘れてはならない。

参考文献

警察庁、総務省、経済産業省、サイバーセキュリティ協議会事務局（内閣官房内閣サイバーセキュリティセンター、政令指定法人JPCERT/CC)「サイバー攻撃被害に係る情報の共有・公表ガイダンス」(2023年3月8日)

山本龍彦「まつろわぬインフラ――情報通信、「情報戦」、グローバル・プラットフォーム」(法律時報2022年9月号)

茂田忠良「米国国家安全保障庁の実態研究」(警察政策学会資料082第２章2015年9月)

Ⅱ　能動的サイバー防御措置

１　技術的アトリビューション[4]

攻撃を受けた際[5]に相手方を特定するための情報収集として下記のような技術的アトリビューションを実施可能とする。

(1) アトリビューションの実行当事者はインテリジェンス機関，捜査機関または自衛隊とし，相互協力も可能とする。なお，司法捜査として捜査機関がアトリビューションを行う場合には令状に基づく検証として取り扱うものとする。

(2) アトリビューションに必要なテクノロジーを適法に行使できるように下記の行為について法令行為として適法化する。なお，サイバー攻撃の準備行為を違法行為とし，スニッフィングを受けた段階から行政機関がアトリビューションを開始できるようにする必要がある。

- 攻撃元を特定するために，攻撃側のコンピュータ（仲介コンピュータを含

[4] アトリビューション（Attribution）とは、サイバー攻撃における主体を特定する活動をさす。

[5] 日本の能動的サイバー防御を行うための行為であることを前提としているため、日本の国、行政機関、自治体、法人等や日本人が管理するコンピュータ（ネットワークを含む）が攻撃を受けた場合を指すものとする。

む）に無許可でアクセスし，情報を収集すること。

- 侵入元を特定するために， サイバー侵入に反応して位置情報または帰属情報をビーコンで表示または返すプログラム， コード， コマンド等を使用すること。
- 情報収集のために使用するプログラム（以下「ガバメントウェア」という[6]）を作成及び使用すること。但しガバメントウェアの作成にあたっては侵入者や仲介コンピュータの管理者等の資産を故意に破壊することを行わないものであるように設計しなければならないものとする。なお，作成については当該行政機関の管理するシステム上で， セキュリティクリアランスを通過した民間企業に作成させた上で， 当該行政機関が検収の上で使用することも可能とする。

2　不正に取得された情報の削除，ハックバック[7]，テイクダウン[8]等（以下「テイクダウン等」という）

アトリビューションを経て，他のインテリジェンス情報と総合し相手方が特定できた場合，防犯措置あるいは自衛措置としてテイクダウン等を行うことを法令行為として適法なものと位置付ける。なお， テイクダウン等を行うことができる機関は捜査機関または自衛隊としインテリジェンス機関はテイクダウン等を行わないものとする。法令において， 実施機関がテイクダウン等を実施する際には必要以上に攻撃者等（仲介サーバの保有者を含む）のコンピュータ設備に影響を及ぼさないよう注意義務を課すこととし， 捜査機関が防犯装置として行うテイクダウン等が故意に，攻撃者等に適切な防御を超えた損害を発生させた場合には，損害賠償義務は免責されない旨の規定も必要となる。

3　サイバー空間外の法執行等

サイバー攻撃に対する能動的サイバー防御の実効性を高めるためには， サイバー上で行う行為（行動）に止まらず， サイバー空間の外においても有効な手段と組み合わせて行うことが必要となる。そのため，パブリック・アトリビューション，有責者のサーバの差し押さえ，国内財産の差し押さえや没収，海外移転の禁止，入国の禁止等の措置を講じることができるよう行政機関に執行権限を付与する必要がある。

Ⅲ　能動的サイバー防御を実施するための適正性と透明性の確保

---

[6] 海外で「ポリスウェア」と呼ばれているものと同種のものであるが，使用権限を捜査機関以外にも付与する必要があるためここでは「ガバメントウェア」という呼称を用いている。

[7] ハックバック（hackback、hacking back）とはハッキングしてくる相手に対してハッキングし返すことをさして用いられるため、攻撃者のシステムの脆弱性を見つけて、侵入すれば、その時点で、それはハックバックと呼ばれるが、ここではアトリビューションの限度で行為を超えて、攻撃者のシステムの機能やデータに影響を与え何らかの不具合を発生させるための行為を意味して用いている。

[8] テイクダウン（takedown）は、サイバー攻撃に対する対策の一つで、特定のウェブサイトやサーバを無効化、または削除することを指す用語。テイクダウンの方法には、サーバに対する差止など司法手続に基づく執行なども含まれるが、ここでは例えば攻撃者のウィルスを無効化する信号を送信することによって無効化するといった主に技術的手段を用いた対抗手段を意味して用いている。

実効性ある能動的サイバー防御を行うために不可欠な論点や施策については前述した通りであるが，その記述中でも一部触れたとおり能動的サイバー防御を適正に実施していくためには，どのような機関を置き，どのように相互牽制が働くよう設計するかが重要である。同時に情報収集を含めて，行政機関が行なっていることに対して国民から信頼を得られるよう透明性を確保できる監査の仕組も設計しておかなければならない。信頼性を醸成するための機関設計のためには次のような点を踏まえるべきである。

(1) インテリジェンス機関とオペレーション機関のあり方を工夫してインテリジェンス機関の暴走を防ぐ体制が必要である。

(2) 捜査機関の行う司法警察活動としての刑事訴訟法上の証拠収集についてはインテリジェンス機関が行わないことが重要である。

(3) 自衛権の具体的行使は自衛隊の所管であり，インテリジェンス機関自身の判断で自衛権の行使を行うことは認めないものとする。

(4) 透明性の確保の観点と情報の厳格な管理を保証する観点からはインテリジェンス機関の行為については記録を作成し，必要に応じてレビューできるように厳重に保管をしておく必要がある。

(5)インテリジェンス機関が収集した情報のうち特定秘密に該当するものは，国会報告の対象とする。

(6) 監視のための第三者機関を設置し，インテリジェンス機関の行動に関する苦情等の受付と調査を担うことも考慮に値する。

Ⅳ　能動的サイバー防御を実現するための法制度のあり方

本報告書に記載した内容を法律として規定する場合，抵触する可能性のある全ての法律を調査し個別に修正する方法は，今後の技術水準の進歩によって新たな手法が生まれてくる蓋然性が高いことに照らすと適切ではない。そのため，本提言の実現のためにはインテリジェンス活動等を含めた能動的サイバー防御に関する包括法を立法することが望ましい。技術的にはサイバーセキュリティ基本法の改正という手法もあるが方法論としてそこに拘泥する訳ではない。また，手法の正当化根拠と合わせて担当すべき行政機関の根拠法の対応も必要になるが，根拠法については他の行政機関との役割の調整が必要になることから，包括法ではなく，当該部分についてぞれぞれの行政機関の根拠法毎の改正が必要となることは言うまでもない。

Ⅴ　中期計画の必要性

1　実現までに要する時間の考慮

これまで述べてきた提言内容を完全に実現するまでには相当の時間を要する。どこから着手するべきかというプライオリティ付けもさることながら，時間軸を設定し人員や設備を整備していかなければならない。セキュリティ人材の確保については想起されやすい課題であるが，データセンターの整備などの設備をどのように整備するのかについても検討が必要である。行政庁によっては「工程表」を作成している例もあるが，そういったほとんどの工程表には必要なコストや人員，設備についての記載がなされていない。この分野については，少なくとも必要なコストや

人員，設備についての記載を伴った工程表が作成されなければならないことを付言しておきたい。

２　インターネットガバナンスへのコミットメント

また，インターネット上のサイバーセキュリティを考える際にはインターネットガバナンスそのものへの日本のコミットメントも重要であることを最後に述べておきたい。インターネットを社会インフラとして利用しながら，日本は民間（企業や市民団体）を含めてインターネットガバナンスを担うインターナショナルのコミュニティの中で十分な役割を果たしてきていない。より安全なインターネット環境を整備していくためにはインターネットガバナンスに官民あげて取り組んでいくことの重要性を認識する必要があることも忘れてはならない。

Ⅵ　法的視点からの検討

本提言の実現可能性について法律的側面についてさらなる検討が不可欠であり，その一助として提言内容を含む能動的サイバー防御に関する法的視点からの考察を第２部として提示する。能動的サイバー防御に関連する領域は，これまでその実現を考慮する機会に恵まれなかったこともあり十分に想定されてこなかった領域ではある。しかしながら，立法論としてみた場合，本提言は決して不可能なことを提案している訳ではない。たくさんの考慮要素はあるもののその多くは実現できるものであると考えており，第２部を通してご理解いただけるものと考えている。

Ⅶ　第１部の終わりに

能動的サイバー防御を実現していく第一ステップは，冒頭に述べた通り自らの目隠しを外し暗闇から抜け出すことである。そのためには，現実に起きていることを知ることができない状態では人々を守ることができないという事実を多くの人々に認識してもらうことが出発点である。自由や人権を国から守ることが根幹的な価値であることを認識しつつ，同時に，現代は自由や人権を国によって守っていかなければならない環境に置かれているということも深く考えていかなければならない。多くの人々が思考停止になることなく，本報告書の提言によって，より生産的な議論が生まれてくることを願う。

第 2 部

わが国における能動的サイバー防御のための法整備

Ⅰ　能動的サイバー防御の法益

サイバー攻撃は今日の国際社会において武力攻撃にも匹敵するほどの大きな脅威になっていることは，2007 年のエストニアへのサイバー攻撃によって同国の政府機能が麻痺した例などからも明らかである。日本でもその脅威が深刻化している。また，国家や企業の機密情報を窃取するサイバー諜報の事案も増加している。サイバー諜報や攻撃は資力のない個人や団体によっても行うことが可能であり，さらに攻撃元を特定することが困難であることも脅威の度合を増す要因となっている。電子化の高度に進展した現代社会において大規模なサイバー攻撃が発生して原発や航空管制などをはじめとする重要インフラが機能麻痺した場合には，多数の人命が奪われ膨大な物損が生じるのみならず，社会秩序が崩壊することが強く懸念される。このような悲劇を防ぐため，能動的サイバー防御をすすめることが不可欠である。

HUMINT や SIGINT によるスパイ（諜報）活動については，国際法はそれ自体を包括的には禁止していない。但し各国が反スパイ法を制定してスパイ活動に対して刑事罰を科すことは国際法上，可能である[中谷 2023]。タリン・マニュアル 2.0 の規則 32 は，「国家による平時のサイバー諜報はそれ自体は国際法に違反しないが，それを遂行する方法は国際法違反となりうる」と規定する。

しかしながらわが国は反スパイ法を制定するという情報防衛のための自助努力を行っていない。このような予防的な諜報の欠如という厳しい状況に鑑みると，能動的なサイバー防御は一層，日本国と日本国民の利益を守るために不可欠である。能動的なサイバー防御も手当しないことは，国民の生命と財産を危機にさらすものである。国家として無責任な対応と言わざるを得ない。

また，能動的サイバー防御によってサイバー諜報やサイバー攻撃から防衛する体制を整えておかないと，例えばサイバー犯罪について国際共同捜査を行う上での大きな障害になりかねない。サイバー分野での国際協力がうまく行くためには，参加各国が一定以上のサイバー能力を有し，かつ機密情報を提供できることが当然の前提である。それらを欠く場合には，自助努力もせずにただ乗りしているとして批判され，国際共同捜査の枠組から排除されかねない。

さらに，一国に対するサイバー攻撃の悪影響は当該国内にとどまるものではなく，他国にも悪影響が及ぶことが不可避であることに鑑みると，サイバー攻撃を予防するために能動的サイバー防御を行うことは，国際社会に対する責務といっても過言ではない。国際社会における法の支配を重視するわが国としては，サイバー分野においても責任ある行動をとることが必須であり，その中には関連する国内法を整備することも当然に含まれる。

能動的サイバー防御は，「Ⅱ 国際法における能動的サイバー防御の位置付け」において後述するように，国際法上，基本的に合法である。国内法を整備してアクティブサイバーディフェンスの体制を整えることがわが国の国益にとって不可欠である。

2022年12月に閣議決定された「国家安全保障戦略」では，「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のおそれがある場合，これを未然に排除し，また，このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。」としている。能動的サイバー防御が本来的にはインテリジェンス活動にあることに鑑みると，これを担うのは内閣情報調査室等のインテリジェンス機関とすることが自然である。他方，わが国には，米国のような秘密工作（covert action）につい

て定めた明白な法的規範がないことから，その手続等を法令で定める必要があるとともに，インテリジェンス機関の下で能動的サイバー防御を担える人材，技術，設備等をどのように整備するかという課題が生じる。

いうまでもなく，行政機関による能動的サイバー防御の行使につき，国会による民主統制は必要である。なお，現行法の下でも，能動的サイバー防御に関する情報を特定秘密に指定すれば，衆議院及び参議院の情報監視審査会から提示を求められた場合，その提出がわが国の安全保障に著しい支障を及ぼすおそれがある場合を除き，その求めに応じなければならないという規定で対処可能であろう（特定秘密保護法第 10 条第 1 号イ）。

参考文献
中谷和弘「サイバー諜報と国際法」『国際法外交雑誌』122 巻 1 号（2023 年）

Ⅱ 国際法における能動的サイバー防御の位置付け

1　能動的サイバー防御の意義

「能動的サイバー防御」を規律する条約はない。また一部の国が具体的な方策をとっているが（「Ⅳ　米国における能動的サイバー防御と法」参照），これについて慣習国際法上の新しい規則が確立していると言えるほどの広範かつ一貫した国家実践はない。しかし，既存の国際法の適用はある（サイバー行動一般について，［外務省 2021 年］）。本節では，能動的サイバー防御が主権尊重原則と武力不行使原則に反しないかを検討する。なお，単独で実施することが国際法に反する場合であっても，領域国の同意を得て措置をとることは可能である（「Ⅲ　国際司法共助・国際情報共有とそのための国内体制」参照）。

2　主権尊重原則

他国領域における領域国の同意のない力の行使は，それが当該国の主権権能（sovereign powers）の簒奪と見做される場合に主権侵害に当たる。例えば，その性質上国家しかできないことを行うことや，領域国の主権権能の簒奪を目的とした行為をすることがこれに当たる。

サイバー空間における国家による措置がこれに該当するかについては争いがある。一方では，サイバー空間も物理的なインフラから構築されていることから，三次元の非サイバー空間を基礎に発展してきた規則が妥当するという考え方がある。サイバー空間は端末やサーバなどの物理的媒体から構成されるネットワークであり，それらインフラに対する各国の領域主権は及ぶためである。他方で，既存の国際法が妥当することを認めつつも，サイバー空間独自の規則を認める考え方もある。サイバー空間は，当局が自国にいながらにして，遠隔の他国のサーバにアクセスすることができるという点で，非サイバー空間とはトポロジーが異なるためである。後者の見解の方が能動的サイバー防御を認める余地が広くなる。

能動的サイバー防御としてとられる措置は多岐にわたり，個別の評価が必要である。ハニーポットによる囮システムや，ビーコンの使用などは他国領域に効果が及んでいるとは言い難く，問題なく認められる。ボットネット・テイクダウンはそれがもたらす規模と効果に応じて評価が分かれる。ハックバックも烈度が低い場合には許容されうるが，当事国領域内のインフラ破壊を行うことは，国家が行う場合には他国主権の侵害になりうる。

しかしながら，たとえ通常の状況では違法になる場合であっても，相手国の武力攻撃に対する個別的・集団的自衛権の行使に要件を満たす場合には合法である。また相手国の国際法違反に対する対抗措置（countermeasures）に該当する場合には，違法性が阻却されて容認されることになる。対抗措置の要件は，①先行する違法行為があり，②規模，性質の面で違法行為に比例し，③違法行為から生じる損害する均衡するものであることである[国家責任条文 49-51 条]。2017 年 4 月の「サイバー空間における責任ある国家の行動に関する G7（ルッカ）宣言」において，「国際違法行為の被害者である国家は，一定の場合には，その違法行為について責任を有する国家に国際的な義務を遵守させるために，当該責任を有する国家に対して均衡性のある対抗措置（ＩＣＴを介して実施する措置を含む）及びその他の合法的な対応をとることができる。」として，サイバー手段を含む対抗措置が国際法上合法であることを確認したことにも留意すべきである。ただし措置の相手国へのアトリビューションができない場合や，危険を未然に排除する場合には対抗措置は援用できない。

さらに，サイバー措置が緊急避難（necessity）に該当する場合には違法性が阻却される。緊急避難は当該行為が，重大かつ急迫した危険から不可欠の利益を守るために，当該国によって唯一の手段であり，かつ，当該行為がその義務の相手国または国際社会全体の不可欠の利益に対する深刻な侵害とならない場合に認められる。しかし，国は問題とされる国際義務が緊急避難の援用の可能性を排除している場合，または当該国が緊急避難の状態の発生に寄与した場合には，緊急避難を違法性阻却事由として援用することができない[国家責任条文 25 条]。これらの要件は厳格であるので認められる余地は狭い。しかし，緊急避難は国家への帰属が証明できない場合，また危険が現実に生じていない場合でも援用できる。

３　武力不行使原則

国連憲章 2 条 4 項は，加盟国は「その国際関係において，武力による威嚇又は武力の行使を，いかなる国の領土保全又は政治的独立に対するものも（中略）慎まなければならない」として，武力不行使原則を定める。この規範は他国との合意による逸脱が許されない強行規範（jus cogens）と解されている。

まず能動的サイバー防御措置が「武力」（force）に該当するかが問題となる。「武力」の意義については見解の相違が大きいものの，少なくとも「国際関係」における一定の強制的措置であることが必要である。

武力不行使原則の国連憲章上認められている例外は，安全保障理事会の憲章 7 章下の加盟国に対する授権がある場合と，憲章 51 条の自衛権行使である場合である。後者の自衛権の行使は，先行する「武力攻撃」（armed attack）がある場合に認められる。武力攻撃は，国際司法裁判所（ICJ）によれば，「より重大な形態の武力の行使」である[ICJ 1986, para. 191]。また，ICJ は，自衛の可否を判断する際に，攻撃の特別の意図（specific intention）を考慮に入れたことがある[ICJ 2003, para. 64]。

また，武力攻撃は国家によるものに限定されるか，テロ組織などの非国家行為体によるものも含むかには争いがある。ICJ は前者により整合的な見解をとっていると考えられる[ICJ 2004, para. 139]。ただし，領域国が領域内私人の危害行為を抑止する意思も能力もない場合に，そのような行為を防止するための最小限の実力を行使することはこの武力に当たらないとする見解もある。いずれにしても，自衛権の要件は相当に厳格である。能動的サイバー防御が武力に該当す

るほど大規模なものに至る場合には，自衛権の行使として正当化される余地は小さくなる。

4　サイバー行動の国際的規律

サイバー行動については，様々な国際的フォーラムを通じた規律がなされている。国連の「国際安全保障の文脈における情報通信分野の発展に関する政府専門グループ」報告書[GGE]，国連オープンエンド作業部会最終報告書[UN 2021]，北大西洋条約機構（NATO）サイバー防衛協力センターの支援の下で専門家会合が採択したタリン・マニュアル 2.0[Schmitt 2017；中谷 2018]等の研究成果などがある。また政府によるデータアクセスに関しては，2022 年 12 月に OECD が採択した「民間部門が保有するデータへのガバメントアクセス」原則もある[OECD 2022]。能動的サイバー防御も，これらの原則や指針に沿ってなされるべきである。

参考文献

外務省「サイバー行動に適用される国際法に関する日本政府の基本的な立場」(2021 年 5 月 28 日), https://www.mofa.go.jp/mofaj/files/100200951.pdf.

国家責任条文: Responsibility of States for Internationally Wrongful Acts, Annex, General Assembly resolution 56/83 of 12 December 2001, *Yearbook of the International Law Commission*, 2001, Vol. II.

中谷和弘＝河野桂子＝黒崎将広『サイバー攻撃の国際法―タリン・マニュアル 2.0 の解説』(信山社，2018 年)

GGE 2019 Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (A/76/135), https://www.un.org/disarmament/group-of-governmental-experts/

ICJ 1986: Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of 27 June 1986

ICJ 2003: Oil Platforms (Islamic Republic of Iran v. United States of America), 6 November 2003

ICJ 2004: Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004

OECD 2022, Declaration on Government Access to Personal Data Held by Private Sector Entities, 14 December 2022, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

Schmitt, Michael N. 2017. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press

UN 2021 Open-ended Working Group, A/AC.290/2021/CRP.2, 10 March 2021, https://www.un.org/disarmament/open-ended-working-group/

Ⅲ　国際司法共助・国際情報共有とそのための国内体制

1　国際司法共助と国際情報共有

国際司法共助とは，外国の要請により，当該外国の刑事事件の捜査に必要な証拠の提供をすることをいう（国際捜査共助等に関する法律 1 条 1 項）。司法共助は条約に基づいて行う場合と，条約はないものの外交ルートを通じた個別の要請に応じて行う場合とがある。

司法共助条約（MLAT）は，相互主義に基づく，証拠の提供，法的文書の翻訳等を含む協力義務が定めることが多い。日本は，米国，韓国，中国，香港，欧州連合（EU），ロシアとの間で，共助協定を締結している。他方で，条約がなければ共助要請に応じる義務はない。

2001 年サイバー犯罪条約は，不正アクセス等のサイバー犯罪が行われたとき，加盟国の間で協力してコンピュータ記録の保存や提供が行えるように，加盟国に法律を整備することを義務付ける。2021 年同第 2 追加議定書では，加盟国の中央当局間の迅速な情報交換を義務付けている。

国際情報共有枠組みは，異なる国家間での情報の共有を目的とする。必ずしも裁判手続きのために行われるものではないという点で，司法共助より協力の範囲は広い。扱われる情報の種類や，枠組みの法的性質は多岐にわたる。情報共有の際に，情報の収集，分析，交換，共有の方法を調和化したり，情報を共有するための技術的なインフラの整備を行ったりすることも多い。そのために，国家間の信頼関係を強化し，共通の認識を醸成することも期待される。日本政府は 2023 年 1 月，「国家安全保障戦略」を受けて，調達するソフトウェアに米国と同水準の安全基準を設けるなどして，サイバーセキュリティの分野で，米国との協力を強化することを決定した。

軍事面では，情報保護協定において機密情報を含む情報を共有することがある。日本は，米国，韓国，インドと秘密軍事保護協定を結んでおり，北大西洋条約機構，英国，フランス，イタリア，豪州と情報保護協定を結んでいる。内容や手続きに相違はあるものの，締約国政府の国家安全保障のために保護を必要とする情報を，適切に保護するための基本原則や仕組みについて定め，秘密指定を付して共有する仕組みを設けている。各協定に共通する原則としては，受領国が提供国の承認なしに，提供される秘密軍事情報を第三国に提供しないこと，情報について提供国と同等の保護措置をとること，目的外使用をしないこと，企業秘密等の私権を尊重することなどがある。

サイバー空間における攻撃などに迅速に対応できる仕組みを構築するためには，国家間で迅速な情報共有などについての協力を緊密化する必要がある。そのために，多層的な情報共有の仕組みを構築することが有益とされる。サイバー攻撃の場合は，その検知，マルウェアや IP アドレスの解析，実際の対応などの運用対応を行う CSIRT（computer security incident response team）の連携，捜査権限を持ち被害拡大を防ぐ役割を担う法執行機関の連携，事件の全体像や必要な政策対応を迅速に把握する政策レベルの連携，予期せぬ紛争への拡大を防ぐ外交レベルの情報共有等が重要とされる。日本は，二国間枠組みや，国連等のフォーラムなどを含めた多国間枠組みにおいて，サイバーセキュリティのための協議等を行なっている（https://www.nisc.go.jp/policy/group/kokusai/policy.html）。安全保障面においては，自衛隊がサイバー攻撃対処に関する意見交換や多国間演習への参加によって，関係国との連携，協力を強化している（令和 2 年度・防衛白書，https://www.mod.go.jp/j/publication/wp/wp2020/html/n33302000.html）（特に NATO とは運用面での協力を視野に入れて意見交換や訓練等を行なっている）。

さらに，シンガポール，ベトナム，インドネシアの防衛当局間と協力して，人材育成や技術支援などを行なっている。このような協力を進め，サイバー空間における保安体制を強化することが重要である。

2　事業者との直接協力

サイバー攻撃等は通信事業者が提供するネットワークを通じて行われるため，事業者らが保有する情報を取得することが必要になる。米国 CLOUD 法をはじめとして，一部の国は外国事業者についてもそのような情報の保管，開示，提供を義務付ける立法例がある（西村高等法務研究所 2023)。また，外国事業者らから情報を直接取得する仕組み（直接協力）を認める条約としては，米国 CLOUD 法が定める行政協定や，サイバー犯罪条約第２追加議定書がある。

事業者らを通じて，そのような攻撃を検知，監視する仕組みを設けることにも需要がある。ただし，通信の秘密を不当に侵害しないような立法上の手当が必要になる（「Ⅸ　能動的サイバー防御のおける SIGINT の役割と「通信の秘密」との関係」「Ⅹ　SIGINT に必要な通信法関連の法整備」参照)。なお，日本政府は 2024 年にも通信事業者が提供するネットワーク下でサイバー攻撃を監視できるようにすると報じられている。

3　国際的に情報提供できるような国内体制の整備

一般的に，国際的に情報提供できるような国内体制を整備するには次の取り組みが必要である。まず，情報共有に関する法律や制度を整備することである。これには，情報の機密性やセキュリティを保護する制度の整備や機密漏洩の場合の制裁が含まれる。国内の政府機関や組織間の情報共有を促進するための制度やメカニズムを設けることも必要である。次に，情報収集を所轄する組織の整備と強化である。これには情報管理インフラの整備，担当する人材の育成も含まれる。情報システムやデータベース，情報の暗号化やセキュリティ対策の強化，情報の共有を容易にするツールやプラットフォームの構築など，技術的なインフラの整備も欠かせない。

上記の日本の国際協力は，これらの整備を進めつつ，新規の立法を必要としない範囲で行なっている。

他方で，日本の情報秘密保護法制は，他国と安全保障上の機密情報を共有するには十分ではないとも批判される。2014 年の特定秘密保護法は，予め指定された特定秘密情報を，取り扱い者が漏洩することを禁止するもので，規制の範囲が狭い。さらに，日本では，他国の諜報活動を防止する体制が整っていない。例えば，日本では反スパイ法が制定されていない（「Ⅰ能動的サイバー防御の法益」参照)。また，Five Eyes 参加国等，主要国は防諜組織を持つのに対して，日本はそれに相当する専門組織がない。他国との協力を強化する上では，中長期的にはこれらの領域における法整備が必要となると考える。

参考文献

西村高等法務研究所(NIALS)「CLOUD Act（クラウド法） 研究会報告書 Ver.2.0
－ 企業が保有するデータと捜査を巡る法的課題の検討と提言 －」（2023）
https://www.nishimura.com/ja/knowledge/publications/92692

Ⅳ　米国における能動的サイバー防御と法

比較法として，本報告書においては，米国の状況を紹介する。

1　2018 年国防総省サイバー戦略（要旨）

米国は，2018 年に，従来のサイバー戦略を破棄して「2018 年国防総省サイバー戦略（要旨）（The 2018 DoD Cyber Strategy (Summary)）」を採用し，武力紛争に至らないレベルの活動（activity that falls below the level of armed conflict）を含め，悪意のあるサイバー活動をその発信源で中断又は停止させるために前方防衛を行う（defend forward）という戦略を打ち出した。これが，米国における能動的サイバー防御（アクティブサイバーディフェンス）である（なお，2023 会計年度国防授権法に関する両院合同付帯説明書（337 頁）では，2023 会計年度中に新たな国防総省サイバー戦略の公表が示唆されているものの，2023 年３月 31 日の時点では公表されていないことから，本稿では論じていない）。

具体的には，米国にとって戦略的に脅威となる相手に打ち勝つために，①サイバー空間を含むあらゆる領域で戦い，戦争に勝利するための軍事的能力を確保するとともに，国防総省関連のシステム，ネットワーク及び情報を悪意のあるサイバー活動から防御し，②悪意のあるサイバー活動による重大なサイバーインシデントから米国の重要インフラを保護するために，この脅威が攻撃対象に到達する前に阻止する積極的な防御を行い，③同盟国等とともに，サイバー能力を強化し，サイバー空間における共同作戦を拡大し，双方向の情報共有を行うとしている。

国防総省は，2023 年５月 26 日に「国防総省は，2023 年国防総省サイバー戦略を（連邦議会に）送付」という報道発表を行い，機密指定された 2023 国防総省サイバー戦略（2023 DoD Cyber Strategy）を，週の初めに連邦議会に送付したことを明らかにした。また，この発表に伴い，同戦略に関する機密解除された概要報告（unclassified fact sheet）が公表されたものの，機密解除された「2023 年国防総省サイバー戦略（要旨）」は数ヶ月以内に公表される予定であるとしている。なお，この概要報告を見る限り，2023 国防総省サイバー戦略は，2018 年国防総省サイバー戦略に規定された方向性に基づくものであることから，上記の 2018 年国防総省サイバー戦略に基づいた前方防衛の記述に大きな変更はないと言える。

２　前方防衛の具体例

それでは，武力紛争に至らないレベルの活動において，悪意のあるサイバー活動をその発信源で中断又は停止させるための前方防衛とは，どのようなものであろうか。その具体例として，連邦政府が報道機関に対して意図的にリークしたとされる 2019 年のニューヨークタイムスによる報道「米国はロシアの電力網へのオンライン攻撃を増加」(David Sanger & Nicole Perlroth, U.S. Escalates Online Attacks on Russian Power Grid, N.Y.Times, June 15, 2019）の内容を見てみたい。

本件では，ロシアが，以前から米国の発電所・石油・ガス・パイプライン・浄水場等の施設に，将来の米国との紛争に備えてマルウェアを設置してきたことに対して，法的には対抗措置ととれる形で，米国サイバー軍がロシアの電力網に「潜在的に大損害を与える有害プログラム」を埋め込むという前方防衛を実施し，これを公表することでロシアへの警告を発したものとされている。この対処は，以下の説明で述べるとおり，武力行使ではなく，軍による「秘密軍事活動又は作戦」，すなわちインテリジェンス活動として理解することができる。

３　連邦法及び大統領覚書における中心的な規定

連邦議会は，この前方防衛に関する中心的な規定として，2019 会計年度国防授権法第 1632 条「国防長官がサイバー空間における軍事行為又は作戦を実施する権限の承認」において，①国防

長官に，外国権力（foreign power）による米国又は米国市民への悪意のあるサイバー活動に対して，米国とその同盟国を守るために，サイバー空間における軍事サイバー活動又は作戦（秘密軍事活動又は作戦（clandestine military activity or operation）を含む）を実施する権限を与え，②この作戦には，「敵対行為に至らない場合（short of hostilities)」又は「敵対行為が起きていない地域」におけるものが含まれとし，③この「秘密軍事活動又は作戦」を 1947 年国防授権法における秘密工作（covert action）ではなく，伝統的な軍事活動（traditional military activity）とみなすと規定し，④国防長官が連邦上下院の軍事委員会に，サイバー空間における軍事活動（サイバー空間における秘密軍事活動又は作戦を含む）につき，四半期ごとに報告する義務を課している。この規定のうち③の規定は，サイバー軍が秘密裏に外国のネットワークに侵入する作戦を実施するにあたり，これをインテリジェンス機関の秘密工作に対して厳しい手続を課す規定の対象から外したことを意味している。

また，2019 会計年度国防授権法第 1642 条「サイバー空間におけるロシア連邦，中華人民共和国，朝鮮民主主義人民共和国及びイラン・イスラム共和国による攻撃に対する積極防衛」第(a)項第(1)号では，「国家指揮権限（National Command Authority）により，ロシア連邦，中華人民共和国，朝鮮民主主義人民共和国又はイラン・イスラム共和国が，サイバー空間において，米国政府又はその市民に対して，積極的，組織的かつ継続的な攻撃作戦（これには，米国の選挙及び民主的政治過程に影響を及ぼそうとするものも含まれる）を行っていると決定された場合には，国家指揮権限は，国防長官，具体的には米国サイバー軍司令官に，国防長官が伝統的な軍事活動としてサイバー作戦及び情報作戦を行う場合の権限と指針とに基づいて，当該攻撃を中断，撃破及び抑止するために，外国のサイバー空間において，適切かつ均衡性に基づいた行動をとることを認めることができる。」と規定している。なお，本条第(a)項第(２)号(A)では，本項第(1)号で規定された権限が行使される場合，国防長官は，合衆国法典第 10 編第 395 条に基づき，機微な軍事的サイバー作戦（sensitive military cyber operation)」を，その実行から 48 時間が経過するまでに，書面により連邦議会上下院の軍事委員会に通知しなければならないと規定している。

なお，トランプ大統領は，2018 年夏に，現在も機密指定されている国家安全保障大統領覚書第 13 号（National Security Presidential Memoranda 13）を発出したが，その内容はサイバー軍に 2019 会計年度国防授権法において認められた権限を改めて認めるとともに，同軍が，緊急の場合には大統領の事前承認を得ることなく，前方防衛を行うことを認めたものであると言われている。

Ⅴ　能動的サイバー防御における政府の責務

１　能動的サイバー防御における民間部門及び公的部門の関係

(1) 民間部門及び公的部門の役割

近現代の法治国家において，民間部門の構成要素である市民の生命，自由，財産の保護，また，対外的・対内的安全の保障が政府の責務とされる一方で，市民相互間の（広義の）自助・自救は，法秩序によって禁止され，正当防衛，緊急避難，自力救済・自救行為といった例外のみが許容される。このような体制は，サイバー空間にも妥当し，不正アクセスが禁止されている現行刑事法の枠内における自助及び共助の手段として，自己のシステム及びネットワーク内部で実施される受動的サイバー防御（passive cyber defense）―例えば，ファイヤーウォールの設置，ウィルス

対策ソフトの導入など―が最低限度の措置として講じられてきた。しかし，近時のサイバー空間においては，サイバー攻撃が高度化し，場合によっては，特定の外国やそのエージェントが主体となったサイバー攻撃が大規模に展開されていること等を背景に，受動的サイバー防御の限界がより認識されるようになり，場合によっては自己のシステムやネットワークの外部にまで及びうる能動的サイバー防御（active cyber defense）の必要性を求める声が民間部門の側から上がっている。世界的には，このような防御措置に部分的に踏み込む民間部門がみられている。

このような現状において，能動的サイバー防御に係る法政策上の可能性としては，①民間部門の自助及び共助の法的可能性の明確化及び拡大，②公的部門による公助の法的可能性の拡大が考えられる。もっとも，①の方向性に進む場合にあっても，一般市民や中小企業にあっては，その法的手段を講ずることは資源や能力の観点から現実的に困難であって，それだけ②の方向性の法政策が重要な意味を帯びることになるだろう。このことを踏まえて，①と②について順に検討する。

①については，少なくとも，民間部門が能動的サイバー防御として具体的にいかなる措置までを適法に講じ得るかについて不明確を可及的に縮減する必要がある（法的可能性の明確化）。そのような不明確が残されていると，民間部門の自助と共助を―現行法においても禁止されていない限度を超えて―過度に制約することになりかねないからである。具体的に考えられる明確化の方法としては，現行法解釈の明確化や行政機関によるガイドラインの制定が考えられるが，新規立法によって文言の明確化を図ることも一案であろう。このような明確化からさらに踏み込んで，民間部門が能動的サイバー防御として法的に講じ得る可能性を現行法よりも拡張することも考えられなくはない（法的可能性の拡張）が，かえってサイバー空間における市民相互間の法益侵害や無秩序を招来したり，外交・安全保障問題に発展するおそれもあることに注意が必要である。民間主体による能動的サイバー防御の法的可能性の明確化及び拡張のいずれにせよ，能動的サイバー防御のための具体的措置が，予測される効果のみでなくリスク（第三者に対する付随損害，プライバシー等の権利侵害，あるいは，エスカレーションのリスク）において高低があるなかで，具体的にいかなるものまでが立法として必要かつ可能であるかが問われる。

②については，国防を含む安全保障上の利益，国家機能及び公共秩序の維持，また，国民生活の基盤となる重要インフラの機能を保障することは政府の特有の責務であること，さらに，市民の生命，自由及び財産を保護することも政府の責務である一方で民間部門によるその保護のための自助及び共助の可能性が法令上及び―一般市民や中小事業者においては―現実的にも制限されていることからすればより一層のこと，これらの責務を政府が全うすることが求められる。サイバーセキュリティ基本法が国及び地方公共団体の責務を掲げている(5 条，6 条)ことは，能動的サイバー防御の文脈において一層重みをもっているといえよう。公的部門の権限については，下記「Ⅵ　能動的サイバー防御における政府の権限」において作用の性格の違いに応じて検討がなされる。

(2) 民間部門と公的部門の協働の必要性

以上のように，能動的サイバー防御においては，政府等の公的部門による公助が益々重要となるといえる。にもかかわらず，その実施においては民間部門との協働が必須であり，サイバーセキュリティ基本法が「多様な主体の連携」(3 条 1 項) を理念としている通りである。前述のように，民間部門が能動的サイバー防御を実施することを国内法が一定限度まで容認することを前提に，その中心を担い，またそのための能力や資源を備えている事業者，例えば，重要社会基盤事

業者等及びサイバー関連事業者等との公的部門の協働を一層発展させることが能動的サイバー防御の文脈でも重要であろう。というのは，能動的サイバー防御のために必要な技術，ノウハウ，能力及び資源を保有しているのは，現時点では特定の限られた民間事業者であり，また，重要インフラの機能保証のための管理運用責任を一次的に負っているのは重要社会基盤事業者等であるからでもある。この点に鑑みて，能動的サイバー防御の文脈においても，民間部門と公的部門の協働を一層促進することのみでなく，民間部門の自発的なサイバー防御能力向上のためのインセンティブを付与することでサイバー防御の集合的能力を向上させるように市場を間接的に誘導することが重要であり，その旨の規定を設けることも立法の方向性として考えられる。

民間部門による能動的サイバー防御については，既に述べたように，公的部門には，少なくとも， 法令やガイドライン等の整備を通じた法的可能性の明確化が求められる。これに加えて，民間部門による能動的サイバー防御には，公的部門との協働を必須とするものがあるから，ここでも公的部門の役割が求められる。資産凍結や法執行といった措置，また，特定の条件を備えた民間部門に対して一般に法令で禁止された行為を許可することは，高権的権利を有する政府でなければ実施ができない手段であり，これらは公的部門が担当しなければならない。

２　能動的サイバー防御における国の役割

能動的サイバー防御の事務が国と地方公共団体のいずれに帰属するかも問題とする余地がある。確かに，住民に身近な行政はできる限り地方公共団体に委ねられることが基本であり（地方自治法第１条の２），サイバー空間における地域住民の生命や財産の保護についても同様である。しかし，能動的サイバー防御については，例えば次の点で，国が事務の処理について適性を有し， 地方公共団体の事務遂行を補完する必要がある。一つは，一般にサイバー空間は，地域的境界のみでなく国境を相対化するという特徴を有するから，これを通じたインシデントの対応は，全国的・国際的になされる必要があり，それに適しているのは，各地方公共団体の事務処理のあり方を全国的視点に立って調整し，国際関係を処理すべき地位にある国であることである。また，能動的サイバー防御において機能保証が課題となる重要インフラはしばしば全国的な意味をもっていることも，同様の結論に結び付くであろう。さらに，近年のサイバー事案において攻撃主体として想定されているのは，国家やその援助を受けた主体であるところ，その攻撃への対処に適しているのは，相応の人的・財政的資源や情報を利用可能で，かつ，対外的事務―外交や防衛―を処理しうる地位にある国であることである。

Ⅵ　能動的サイバー防御における政府の権限

ここでは，能動的サイバー防御が，複数の法的枠組みに従って実施されうることを示した上で，能動的サイバー防御のために必要な具体的権限をその立法上の課題と併せて整理することで，議論の整理を図ることとする。

１　法執行権限

能動的サイバー防御を法執行の法的枠組みの下で実施するに際してまず問題となるのが，司法警察上の権限であり， これは，犯罪構成要件に該当する違法かつ有責で可罰的な行為が既に行われた場合において刑事罰を事後的に科すことによって将来的な抑止を一般に働かすというアプロ

ーチによる。このアプローチにおいて主体となるのは，警察， 検察及び裁判所である。能動的サイバー防御がこのアプローチに則って実施される限りにおいて，司法警察上の法的制約，例えば，令状主義や証拠法上のルールなどが遵守されなければならない。

サイバー空間における犯罪を的確に検挙し，刑事制裁を科すことは，サイバー攻撃者が訴追される可能性を高めることによって潜在的攻撃者にコストを課すことになる。また，Emotet を通じたボットネットをテイクダウンするための国際的な作戦において重要な意味をもったのは，捜査機関がコマンド＆コントロールサーバ（以下，C&C サーバ）を押収することであった。これらは，能動的サイバー防御を広い意味で捉え，サイバー空間外における諸措置も含むものとして捉える場合には，法執行活動が重要な意味をもつことを示している。このアプローチの下で捜査権限を拡充することは，広い意味における能動的サイバー防御の文脈でも意味をもつことになるだろう。この方向性における立法の一案として考えられるのは，諸外国で立法例がみられるように，捜査目的のために，ポリスウェアを利用可能とし，被疑者のシステムやネットワークに直接侵入することである。また，ボットネットのテイクダウンの方法として，C&C サーバへのハッキングを可能とすることも考えられる。これらはいずれも，被疑者のネットワークに許可なく侵入し証拠を収集する処分であるから，新たな強制処分として法律の根拠を要し，かつ，特定の犯罪に限定する，他に手段がないなど，一定の実体的要件の下，令状主義等の手続保障の要請に準拠しなくてはならない。そのため，このような措置を可能とするためには，現行法の改正を要するであろう。また，能動的サイバー防御の手段として，ダークウェブへの HUMINT も挙げられ，これが犯罪捜査目的でなされることも考えられる。こうした手段については，場合によってはいわゆる「おとり捜査」との関係で現行法上はグレーな領域に入り込むので，諸外国の立法例を参考に，身分秘匿捜査の根拠及び制約を法定することも考えられる。

このような司法警察上の権限とは別に，被害の未然防止や回復のための権限の問題を検討する余地もある。被害の未然防止目的でのビーコンやハニーポットの使用についていえば，国や地方公共団体が保有し管理するサーバに設置する場合はもとより，民間主体のシステムやネットワーク上に設置する場合にも，関連する第三者の有効な同意の下であれば，現行法の下でも可能であろう。他方， 国家安全保障戦略によれば，「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について， 可能な限り未然に攻撃者のサーバ等への侵入・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」ことが予定されているところ，その法律上の根拠及び制約の具体的内容が精査されなければならず（刑事法との関係では，「Ⅷ　国内法における立法措置の必要性　―刑事法の視点から―」を参照），また，そのための情報収集の可能性及び限界が「通信の秘密」との関係で精査されなければならない（「Ⅸ　能動的サイバー防御における SIGINT の役割と「通信の秘密」との関係」，「Ⅹ　SIGINT に必要な通信法関連の法整備」を参照）。

２　防衛権限

能動的サイバー防御を防衛の法的枠組みの下で実施するに際して問題となるのが，防衛上の権限である。このアプローチにおいて主体となるのは，自衛隊であり，自衛権や武力紛争法をはじめとした防衛に関する国際法的・国内法的枠組みの下で実施される。能動的サイバー防御は，論者によっては能動的サイバー「防衛」と訳出され，その語感からか防衛の問題と関連付けて論じられることがある。能動的サイバー防御と防衛の関係について議論の錯綜を回避するためにも，

能動的サイバー防御と防衛上の権限の関係について整理しておく必要があるだろう。

他国による「武力攻撃」に対して，わが国を防衛するために自衛権の行使として「武力の行使」をすることは，①わが国に対する武力攻撃が発生したこと（＋①’わが国と密接な関係にある他国に対する武力攻撃が発生し，これによりわが国の存立が脅かされ，国民の生命，自由及び幸福追求の権利が根底から覆される明白な危険があること），②これを排除し，わが国の存立を全うし，国民を守るために他に適当な手段がないこと，③必要最小限度度の実力行使にとどまるべきことの範囲で日本国憲法 9 条 1 項に反しない。サイバー攻撃との関係でみると，①の要件は，政府見解によれば，「武力攻撃の一環としてサイバー攻撃が行われた場合には，自衛権を発動して対処することは可能」とされており，「例えば，物理的手段による攻撃と同様の極めて深刻な被害が発生し，これが相手方によって組織的，計画的に行われている場合には，武力攻撃に当たり得る」とされる。このようなサイバー武力攻撃に対する防衛活動もまたサイバー手段によって実施されることが考えられるが，防衛出動時において武力攻撃を排除するために自衛隊がサイバー手段を訴えることも当然可能であり，その措置が「武力の行使」に該当するものである場合でも，自衛隊法 88 条 1 項の「武力の行使」の権限規定によってカバーされていると考えることができる。もちろん，武力紛争法等の国際法の規制の範囲内にとどまっていなければならないことはいうまでもない（参照，同 2 項）。これら限界の範囲内で実施されるサイバー防御措置は，「専守防衛」の範囲を超えるものではない。

もっとも，現代戦はハイブリット戦であって，攻撃国は，「武力攻撃」の閾値に達しない規模や効果において国家機関や重要インフラ等の機能を攪乱するために，武力攻撃に先行してサイバー攻撃をしかけるようになっている。このような国家によるサイバー攻撃を終止させるためにいかなる措置を取り得るかが―これを能動的サイバー防御の問題として位置付けるかは議論になるかもしれないが―防衛と密接に関連して問題となる。この問題との関係で注目されるのは，武力攻撃に至らない侵害に対して実施される，国際法上の対抗措置であり（但し，武力の行使に該当するものについては，タリンマニュアル 2.0 によれば，「加害国に対して（武力攻撃に至らない）武力行使に該当するサイバー対抗措置をとることができるかについては意見の一致に至らなかった」とされている（中谷和弘＝河野桂子＝黒崎将広『サイバー攻撃の国際法―タリン・マニュアル 2.0 の解説』（信山社，2018 年）25 頁））。その制約条件の範囲内でなされるサイバー対抗措置の実施主体が問題となる。この点，サイバー領域における防御措置のうち一定条件を備えたもの―例えば，国家機能や重要インフラ等の安全保障上の法益の防御のために実施されるもの，又は，武力攻撃の前段階としての性格を有するサイバー攻撃に対処するもの―に限定を加えつつ，これを自衛隊が実施することが考えられ，この場合，自衛隊に関わる特有の国内法的問題がある。まず，「武力の行使」（憲法 9 条 1 項）が三要件を充足した場合のみに許容されているとすれば，対抗措置として実施されるサイバー防御措置も「武力の行使」（憲法 9 条 1 項）に該当するものであってはならない。そして，このような措置は「武力の行使」に該当しない範囲内で実施されるものであること，及び，その措置がなお防御的性格を失わないことからしても，「専守防衛」には反しない。

このような措置を部隊行動として実施することとする場合には，現行のポジティブリストの規律方式によるならば，自衛隊法上の「行動」の規定―例えば，いわば「サイバー対抗措置」のための「行動」の規定―を新設することが検討されなければならず，この場合，文民統制を確保しつつも，サイバー防御措置が迅速性や秘密性を要することからして，これとの兼ね合いが問題と

なるだろう。他方，能動的サイバー防御のための「権限」（自衛隊法第 7 章）の規定の扱いも問題となり，その具体的措置の内容によっては，防衛省設置法の所掌事務規定（例えば，情報の収集整理（4 条 1 項 4 号），施設及び装備品等の管理（12 号及び 13 号），調査（18 号））で現行法の下でも対応が可能である。もっとも，上記のように対抗措置まで踏み込んだ立法を試みるのであれば，自衛隊法 88 条の「武力の行使」の包括的規定に準じて，能動的サイバー防御のための「権限」規定を―要件の限定の下で―特設することも検討を要する。

3　情報収集権限

能動的サイバー防御のためにサイバー空間の常時監視が必要であることが主張されることがある。ダークネット―インターネットで到達可能なグローバル IP アドレス空間のうち，いずれのネットワーク，コンピュータにも割り当てられていない未使用のアドレス群―の観測については，現行法においても可能であり，実際，無差別型サイバー攻撃の大局的な動向を把握することを目的としたサイバー攻撃観測・分析システムである NICTER によって観測がなされ，そのデータを政府が利用することも可能である。他方，国家機関が特定通信事業者から通信に関する情報を収集するためには，そのための権限の付与及び法的制約の規律を新たに法律で定めることが必要となる。例えば，国家や重要インフラの保護，あるいは，安全かつ安定的な通信役務の提供といった重要な法益の保護に目的を限定しつつ，一定の要件及び範囲において,少なくともメタ情報を提供する義務を，法律によって（又は法律に基づいて），電気通信事業者に対して課することが考えられる（もっとも，この場合，日本国憲法や電気通信事業法の「通信の秘密」の法的制約との関係が重要な問題となり，その制約の範囲内における具体的な法制度内容について，より厳密な精査が必要であろう）。

これらの方法によって収集された情報に加え，法執行や防衛等の目的で収集された情報を集約する機関のあり方やその提供，共有及び利用に対する法的な制約も問題になりうる（「Ⅶ 能動的サイバー防御における政府の組織」「Ⅸ 能動的サイバー防御のおける SIGINT の役割と「通信の秘密」」との関係を参照）。

4　その他の権限

能動的サイバー防御の方法として行政上の制裁措置が挙げられることがある。この文脈では，一つには，パブリック・アトリビューションを挙げることができる。これは，サイバー攻撃の身元を公に明らかにすることによって攻撃者にコストを科すことを意味する。国家が直接又は間接に関与したサイバー攻撃について政府が国際社会に向けてパブリック・アトリビューションを実施することは，外交作用の一環として特段の法律の根拠は要せず，現行法でも可能であろう。もちろん，それが国際関係に重要な影響を及ぼすことに鑑みて，それを実際に実施するには，政治的な判断を要し，また，政府機関によるアトリビューションにも高い確度を要する。もう一つは，能動的サイバー防御のための行政上の制裁については，攻撃者の日本国内資産の凍結や没収も考えられるが，これを可能とするためには，法律によって行政機関に権限を付与する必要があろう。また，制裁手段としては，入国禁止も考えられるが，出入国管理法では，上陸禁止の判断につき法務大臣に広範な裁量を認める規定となっているので（「前各号に掲げる者を除くほか，法務大臣において日本国の利益又は公安を害する行為を行うおそれがあると認めるに足りる相当の理由がある者」（出入国管理難民認定法 5 条 1 項 14 号）），この規定の運用によって現行法でも対応でき

る部分がある。ただ，上陸禁止の対象を制裁目的を含めより広いものとするために文言を改変又は補充することも立法論として考えられなくはない。

民間部門の実施する能動的サイバー防御に行政機関が関与する場合に，行政機関が民間部門に対して有する許可や認証の権限も問題となる。例えば，ホワイトランサムウェアの作成は，現行法では刑事法上一般に禁止されているところ，個別に許可を受けた民間主体であれば，例外的に作成が許されることとする場合には，そのための許可権限が行政機関に付与されていなければならない。また，民間主体である会社の従業員などにセキュリティクリアランスを実施する場合には，そのための情報収集権限と認証権限を付与する必要があるだろう。

参考文献

公益財団法人日工組社会安全研究財団「諸外国におけるサイバー事案の捜査手法に関する調査研究（報告書）」(2023 年)

Center for Cyber&Homeland Security(The George Washington University), Into The Gray Zone, 2016.

Sven Herpig, Active Cyber Defense Operations, 2021.

Ⅶ　能動的サイバー防御における政府の機関

1　能動的サイバー防御に関する情報の集約，分析及び総合調整機関

能動的サイバー防御のための情報を集約及び分析し，能動的サイバー防御のための諸措置を調整する機関が必要となる。下記の通り，能動的サイバー防御のための措置を実施する機関は，様々な所掌事務を担っている諸機関に分散しているので，これを調整し，また，サイバー戦略の下で全省庁的に統合的に運用していかなければならない。現在の組織編成からすれば，内閣サイバーセキュリティセンターに能動的サイバー防御の司令塔機能を担わせるか，これを母体として発展的改組を図ることが適切である。2022 年 12 月に閣議決定された「国家安全保障戦略」でも，「能動的サイバー防御を含むこれらの取組を実現・促進するために，内閣サイバーセキュリティセンター（NISC）を発展的に改組し，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を設置する。」とされている。この場合，内閣官房組織令の改正が必要であるが，この組織の重要性に鑑みて，その設置を法律で基礎付けることも考えられる。

2　能動的サイバー防御に関する実施機関

能動的サイバー防御は，アトリビューションに不可欠な情報収集のみでなく，ハックバック，テイクダウン，スレットハンティング等，サイバー空間内で実施される措置に加え，広くは，サイバー空間外における制裁措置や犯罪捜査等の措置にも及ぶうる。このことから，能動的サイバー防御に関する実施機関は，情報収集自体を主な任務とする情報機関のみでなく，法執行を担う警察，防衛を担う自衛隊，一般の行政事務を担当する行政機関など，多元的に存在し，それぞれの機関がその事務及び作用の範囲内で情報を収集し，能動的サイバー防御措置を分担する。その際に，外国の国家機関も含め，諸機関の協働が求められる。

能動的サイバー防御の実施の一翼を担うのは，法執行機関及び関連事業者―電気通信事業者や重要インフラ事業者―を所轄する行政機関である。また，（自衛権に基づく「武力の行使」として

のみならず)「武力の行使」(憲法 9 条 1 項) 未満の対抗措置として能動的サイバー防御措置を実施することについても，防衛省・自衛隊を実施機関とすることが立法論上の可能性として考えられなくはない (この場合の立法の具体的な形態については,「Ⅵ　能動的サイバー防御における政府の権限」の２を参照)。このように対抗措置を自衛隊に実施させることの利点は，武力攻撃に対して自衛権に基づいて武力を行使するのは自衛隊であることとの関係で対抗措置としての能動的サイバー防御との連続性が確保でき， 自衛隊のサイバー防衛隊等の―大幅な強化が予定されている―防衛能力を活用できることである。他方で，能動的サイバー防御の対象となる国家が， 自衛隊によって実施された能動的サイバー防御措置を,「武力の行使 (use of force)」(国連憲章 2 条 4 項)，さらには「武力攻撃 (armed attack)」(51 条) と捉える (又は戦略的に主張する) ことによって紛争がエスカレートするおそれもある。このことからすれば， 自衛隊とは別に， 既存の又新設される機関に対抗措置の実施機能を付与することが考えられるかもしれない。但し,そのような機関に米国の秘密工作 (covert action) に相当する機能を担わせるまでに踏み込んだ立法を模索する場合にはなおさら，そのような活動をタブー視してきた我が国においては，その立法論上の是非が根本的に問題となろうし，法的・政治的統制の方法についても極めて慎重な議論を要する。とりわけ，国会報告，予算統制，並びに能動的サイバー防御措置に関する特定秘密の国会提供の方法及び内容など，能動的サイバー防御と一対をなしている国会統制の具体的形態が検討課題となる。

Ⅷ　国内法における立法措置の必要性　―刑事法の視点から―

１　はじめに

(1) 刑法から見た能動的サイバー防御のオペレーションの特徴

上述してきたように，能動的サイバー防御は，特定の目的を達成するために，組織的にいわば一連の行為として遂行されることが多いといえる。

まず，攻撃者の攻撃手段を無力化するという目的があるとき，その目的を達成するために必要なプロセスは， 必ずしも， 刑事実体法の観点から見たときに， 1 つの犯罪として捉えられるわけではない。攻撃者のサーバの制御を取得して， これの機能を停止させる， というプロセスだけとってみても， 技術的な側面のみならず， 刑法の観点からも， ログインに相当する制御の取得と，シャットダウンに相当する機能の停止の 2 つの行為を分けて考察することが可能である。そのように行為を分けて考えるとき，前者については不正アクセス禁止法上の不正アクセス罪に，後者については，電子計算機損壊等業務妨害罪 (刑法 234 条の 2) や電磁的記録不正作出罪 (刑法 161 条の 2) 等の構成要件には該当する可能性がある。このことからは， 能動的サイバー防御の遂行のために， 特定の犯罪の適用除外を設けるだけでは，能動的サイバー防御の円滑な遂行を実現することが難しい場合が予想される。

次に， 目的達成のための手段も一様ではない。上記の攻撃者の攻撃手段を無力化することを目的とする場合においても， それを達成するための手段が制御の取得のみだというわけではない。サーバの制御を得なくても，特定のプログラムを送信し，そのプログラムがサーバ側でアクティベートされ，特定のデータが変更されることにより，サーバの機能の不正な部分を停止させることも可能である。この場合は， 電子計算機損壊等業務妨害罪や電磁的記録不正作出罪等の構成要件に該当する行為を行うために，不正アクセス罪ではなく，刑法上，不正指令電磁的記録供用罪

（刑法 168 条の 2 第 2 項）の構成要件に該当する行為を行ったと評価され得る。

なお，多様な手段を用いて，能動的サイバー防御が行われ得ること，また，その手段自体も随時研究の対象となっていて，攻撃手段の進化に対応して新たな能動的サイバー防御遂行のための手段も産まれることが容易に予想される。

そうすると，能動的サイバー防御の円滑な遂行のために，個別の刑罰規定に，法令行為の趣旨で既存の防御手法のみに焦点をあてた適用除外項目を設けるだけでは，機動性及び実効性に欠くおそれが大きい。

そこで，まずは，能動的サイバー防御のオペレーションに発生し得る法益侵害の種類・程度の総体を洗い出す作業を行った上で，それを正当化し得る，目的の正当性，行為の必要性・相当性の要件を，一般的に検討していく。

(2) 一般的な規範を用いた法令行為を創設する必要性

違法性阻却事由としては，刑法典で最初に出てくるのが刑法 35 条の正当行為の規定であり，これが法令による違法性阻却の根拠規範でもある。ただし，刑法 35 条は，「法令又は正当な業務による行為は，罰しない。」と規定するだけで，その内容は抽象的であり，そこから得られる情報は乏しい。また，同規定の解釈についても，違法性阻却事由そのものの捉え方に対応しており，目的の正当性，行為の必要性・相当性を充たす場合に，違法性が阻却される，と考えられているに止まる。

ここで，もちろん，特定の事案において行われた特定の能動的サイバー防御について，この 3 要件を充たす，と解釈することも不可能ではない。しかし，微妙な事案においては解釈・適用に関して見解の対立・相違が産まれることが容易に予想される。また，行為の相当性の限界ラインを定めづらいことは，行為に踏み切る主体に対して，一方では，適法との確信をもてない行為だからやめておこう，という意味での萎縮効果を，他方では，自身の行為を適法だと安易に信じたことによる濫用的な権限行使を発生させる虞があり，能動的サイバー防御によるサイバーセキュリティの維持という，本文書で論じられている重要な政策目的を達成できない可能性が生じる。

そこで，行政によるガイドラインは司法に対する拘束力をもつものではないことも考慮すると，民主的正統性をもつ法令行為のアプローチにより，能動的サイバー防御を類型的に適法化することが望ましい。

以上より，能動的サイバー防御による対応が必要になるサイバー攻撃及び能動的サイバー防御の特徴に適応し，将来的な能動的サイバー防御をも柔軟に適法化できるような違法性阻却の要件を予め考え，法令行為化をできないかをまず考えるべきである（一般の法令行為アプローチ）。これが難しい場合には，個別の刑罰規定に対して能動的サイバー防御の趣旨・目的に照らして適用除外するための要件を検討していくべきである（個別の法令行為アプローチ）。個別の法令行為アプローチの要件の検討の際には，一般の法令行為アプローチにおける議論を具体化して組み込んでいけばよいから，本文書においては，一般の法令行為アプローチのみ言及している。

なお，能動的サイバー防御を刑法上，適法とする場合，捜査機関が犯罪捜査のために国外にあるサーバにアクセスして必要な証拠を取得する行為についても，手続法上も（一定の手続が必要になると解する余地はあるものの，）適法だと解すべきである。それを確認的に規定しておくべきである。

2　違法性阻却の判断の拠り所

一般の法令行為アプローチと個別の法令行為アプローチのどちらのアプローチを採用する場合においても，法令行為として違法性を阻却する際の考察の拠り所が必要である。複数ある刑法の違法性阻却事由は，互いに重なり合う部分もあり得るが，一般には，緊急行為と，それ以外の行為に分けて考えられてきており，緊急行為には正当防衛や緊急避難などが，それ以外の行為については，被害者の同意に基づく行為等が挙げられる。これらは解釈論だけでなく，立法による正当化の際にも，正当化することが可能な理由を教えてくれるという意味で，つまり，その立法が妥当な根拠を示してくれる点で，重要な視点を提供する。

(1) 一案としての緊急行為としての位置付け

本文書では，能動的サイバー防御を，対サイバー攻撃者との関係では，緊急行為として正当化すべきである，という提案を行う。

三文書によれば，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のおそれがある場合，これを未然に排除し，また，このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する，という。

つまり，重要な法益が危険に晒されている事態に対応するための行為だと整理することができる。抽象的には「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」が能動的サイバー防御の対象であり，そのようなサイバー攻撃が現になされている場合にはその排除を，それが蓋然的な場合には，未然に排除するための措置が能動的サイバー防御なのだといえる。いずれにしても，能動的サイバー防御が向けられる対象は，主にサイバー攻撃を行う違法な侵害者，あるいは，その違法な侵害者によりコントロールされた第三者（例えば，違法な侵害者によりボット化されたコンピュータの管理者）だといえる。その観点からは，不正対正の構造を持つ正当防衛の発想での議論をしていきつつも，それが適わぬときのために正対正の構造を持つ緊急避難の法理の応用も考えていくのが妥当ではないか，と考える。

また，後述の警察官職務執行法やこれを準用する自衛隊法は，正当防衛や緊急避難のほかに，拡張的に正当化される状況をも法定していると解することができ，立法論の議論においても緊急行為（正当防衛及び緊急避難）としての正当化の議論が重要になる，と考えられる。

そこで，以下では，サイバー空間における不正な行為に対抗する措置につき，国内での議論がほとんどない状況であることを踏まえつつも，わが国の正当防衛に関する議論を適宜参照しつつ，能動的サイバー防御の適法性を基礎づけるための要素を洗い出す。その上で，緊急避難の法理についての検討も行う。

(2) 能動的サイバー防御の主体の限定の可能性

正当防衛の主体には制限はないが，私人が正当防衛をできる場合は限られている。私人による正当防衛の成否が問題になった事案において，最高裁判例（最決平成 29 年 4 月 26 日刑集 71 巻 4 号 275 頁）は，「公的機関による法的保護を求めることが期待できないときに」例外的に正当防衛の可能性を認める趣旨を明確にしている。こうした理解は緊急避難においても援用可能である。この最高裁判例の趣旨，及びサイバー攻撃の被害者になり得る民間の組織や企業による独自の能動的サイバー防御を認めると，さらなる報復の連鎖の虞や外交問題に発展し得るという弊害の可能性が指摘されていることも踏まえると，民間企業の裁量に基づいた能動的サイバー防御の実施を認めるのではなく，民間企業としては，公的機関に法的保護を求めるように促し，能動的サイバー防御の権限を原則として公的機関に付与することが考えられる。上記最高裁判例の射程外となる，公的機関において何ができるか，を考えていくことになる。

(3) 緊急性の評価について

正当防衛も緊急避難も緊急行為と呼ばれる違法性阻却事由であるが，正当防衛においては侵害の急迫性が，緊急避難のおいては危難の現在性が要件である。

まず，侵害の急迫性の判断は，最高裁判例上，「法益の侵害が現に存在しているか，または間近に押し迫っていること」（最判昭和 46 年 11 月 16 日刑集 25 巻 8 号 996 頁）が前提となる。ここで，サイバー攻撃を未然に防止しようとする場合に，この要件を充たすと評価できる場合は少ないのではないか，という懸念がある。

急迫というためには，単に近い将来において侵害が加えられる蓋然性が高いというだけでも足りず，少なくとも間近に押し迫っていることが必要になるが，攻撃をしてくるか否かそれ自体が疑わしい場合にそのような時間的切迫性を認めるのは困難である。確かに，高度な匿名性を前提とし，怨恨等の個人的な人的関係と全く関係なく，面識のない相手からの突然のサイバー攻撃が行われるのが日常茶飯事である，という事実もあるだろうが，それは攻撃をしてくるかもしれないと思うことの妥当性を基礎づけるに止まり，客観的な時間的切迫性も，主観的な時間的切迫性を基礎付ける事実の認識にも結びつきにくいからである。

以上，急迫の解釈で解決するには限界がありそうである（鎮目征樹ほか編著『情報刑法 I サイバーセキュリティ関連犯罪』（弘文堂，2022 年）66 頁〔遠藤聡太〕も参照）。そもそも，実際に，攻撃者に権限を奪取された時点で既に，情報の不正取得や不正改ざんが一挙に行われる蓋然性が極めて高くなるサイバー攻撃の特性，端的に言えば，サイバー攻撃と（ほぼ同時に）目標システムに被害が発生するため，サイバー攻撃を探知しても，既に反撃システム自体が制圧されてしまっているということが容易に起こり得ることに照らすと，急迫性の要件を充たすといえるサイバー攻撃が開始された段階においては，既に損害の拡大を止めることや犯人の特定の双方が困難なものになりかねない。

緊急避難の要件である危難の現在性についても，一般的な理解に従えば，法益侵害の時間的切迫性が要求されるがゆえに，サイバー攻撃の危険が具体化する以前の行為は「現在」性が否定されることになると指摘されており，結局，正当防衛の議論と同じ帰結になり得る（前掲『情報刑法 I』69 頁〔遠藤聡太〕）。

・警察官職務執行法の応用の可能性

物理空間では，法執行機関に対しては一定の権力的な職務遂行が法令によって認められていることがある。例えば，警察官職務執行法（警職法）5 条は「犯罪がまさに行われようとするのを認めたとき」に一定の要件の下「その行為を制止することができる」と規定し，警職法 7 条本文は「犯人の逮捕若しくは逃走の防止，自己若しくは他人に対する防護又は公務執行に対する抵抗の抑止のため必要であると認める相当な理由のある場合」に相当な態様での武器の使用を認め，さらに一定の重大な事由が存在する場合には，同条但書において，正当防衛，緊急避難に該当する場合のほか，それしか方法がない（補充性がある）と考えたことに過失がない場合に，武器の使用をして人に危害を加えることも許している。

警職法 5 条，7 条は，自衛隊の施設等の警護出動を行う場合の自衛官の職務の執行について準用されており（自衛隊法 91 条の 2，81 条の 2 参照），能動的サイバー防御の遂行をどの組織がどのように行うかにより，具体的な立法措置の方法は変わり得るものの，上記規定群から一定の示唆を得た立法措置が可能ではないか，と考えられる。

もっとも，例えば，警職法 5 条の制止については，サイバー空間における「制止」を観念でき

ないわけではないものの，警職法制定時にサイバー攻撃への対応が想定されていたわけではなく，能動的サイバー防御の特質を踏まえた特別な考慮が要求されることもあり得るのだから，直接的な適用は難しく，より規律密度の高い根拠規範に基づいて職務執行する必要がある（古谷洋一＝入谷誠『警察官職務執行法〔五訂版〕』344 頁注 17)），という指摘が既になされている。これは制止について述べたものではあるが，急迫性を充たしにくいとされる状況下における，損害の発生を防止するための能動的サイバー防御が許されるべき場合についても，要件を考えていくべきである。

以上の，警察官職務執行法は，確かに，正当防衛や緊急避難の規定を参照しているが，犯罪の未然防止という見地から，一定の権力的行為を許容する規定で，不正の侵害に対し警察権力による保護が間に合わない場合の自力救済を例外的に許容しようとする正当防衛法とは制度趣旨が異なる，といえそうである。このことと，能動的サイバー防御の行為主体を国家機関あるいはその委託を受けた民間業者等に限定する場合には，刑法上の緊急行為よりも，警察官職務執行法の規律に親和的な面もあると考えられる。警察官職務執行法的なアプローチからすれば，正当防衛や緊急避難の法理の解釈を必要に応じて借用しつつも，適法化のための新たな要件を，サイバー攻撃の未然防止や進行中のサイバー攻撃の被害拡大の防止の観点から検討していくことが課題になる。

・一案

具体的には，物理空間で行われる不正な侵害と異なって，急迫性の要件の代わりに，どのような要件が適切であるかを考えることが可能である。例えば償うことのできない損害を避けるために能動的サイバー防御が不可欠であることを要件とするなどの立論も考えるべきである（前掲『情報刑法 I』I69 頁〔遠藤聡太〕において紹介される，現在の危難についての有力説（深町晋也『緊急避難の理論とアクチュアリティ』（弘文堂，2018）144-145 頁）も参照)。

例えば，ネットワーク上に存在するノード（コンピュータ）の属性を調査しないと，実際にサイバー攻撃を受けそうになった時点において対応できない場合において，外からの犯罪構成要件に何ら触れない調査から，ある程度のサイバー攻撃を実行する可能性があると思われるノードに対しては，その可能性を調査するために必要な措置をとることができるようにする必要が大きい。

実際に，数多くのボットを制御して行われる DDoS 攻撃において，攻撃が行われてしまったら手遅れであることを前提とすると，同攻撃を行うために行われるボットネット構築行為それ自体を能動的サイバー防御を用いて妨害する必要があると考えられる。従来の緊急行為の枠組みだと，侵害者が武器を調達する行為自体は阻止できないところ，能動的サイバー防御の文脈では，それに相当する行為を阻止できるようにする必要もあり得る。

(4) 行為の相当性の判断

行為当時の判断として，それがもたらす便益と法益侵害について，それぞれその蓋然性（期待値）を比較して，便益の期待値が法益侵害の期待値を上回るのであれば，許された危険の範囲内として構成要件該当性または違法性を阻却するという理解がある。実際に達成され「た」利益と実際に発生し「た」法益侵害との比較ではないところが重要である。

本報告書では，正当防衛の法理の理解を借りながら，能動的サイバー防御の法令行為化を考えているところ，正当防衛についてみても，甚大な結果が生じたことのみを理由に，防衛行為の相当性は判断されず，生じた結果は行為の相当性判断の一考慮要素になるに止まる。つまり，たまたま予期しない重大な結果が生じたに過ぎない場合でも，防衛行為の相当性は肯定され得る。

対して，緊急避難の法理の場合には害の均衡が要件になるが，能動的サイバー防御の性質上，攻撃によって生じ得る害の予測を詳細かつ正確に行うのは類型的に困難であることが見込まれるとすれば，法令行為化する際に厳格にそれを要求しないという選択肢もあると思われる。

・過剰な行為の防止―適法な行為を担保するための手続の必要性

上記は，実体法的な観点からの相当な行為の限界であったが，過剰な行為を防止する法的仕組みについても考えておきたい。能動的サイバー防御においては，能動的サイバー防御を実行しようとする現場の職員が，能動的サイバー防御の必要性を基礎づける事実を認識して能動的サイバー防御を遂行するわけであり，独りよがりの判断になる危険が常にあるともいえるからである。具体的な局面においては，能動的サイバー防御を行う職員自体に冷静な判断が期待できない可能性もあり得る。

そこで，ここでいう，過剰な行為の防止のみならず，能動的サイバー防御の適法性を手続的に確保するために，（それは法適用の専門機関である）司法機関による「令状審査」を導入することも考えられるかもしれない。抽象的には法令が能動的サイバー防御の執行機関に権限を与えるが，司法機関において，提出された事実に基づいてできる事柄，つまり能動的サイバー防御の執行機関に付与されるべき具体的な権限を決定することにより，一定の事実関係の存在を前提とする過剰な能動的サイバー防御を防止することができると期待はされる。しかし，司法警察活動とはいいにくいこともある能動的サイバー防御においては令状を要求することは自明ではなく，それ以外の要件を厳格に定めることで足りるとも思われること（警職法上の「制止」の文脈），緊急性が高い能動的サイバー防御において逐一令状を要求していては手遅れになる可能性があり得ること，日々新しい攻撃手法が産まれてくる世界において判断が難しくなる可能性があり，そうであると司法機関の判断に時間がかかることが懸念されること，一方で簡易な判断でよいとすれば，その判断にどの程度の過剰行為発生の抑止効果が期待できるのか疑問もあることなどからすれば，必ずしも令状審査を要件とする必要はないと思われる。むしろ，能動的サイバー防御として行ったことのログ（とりわけ改ざん不能なログであることが望ましいと考えられる）をとっておき，これを検証して改善に努めていくことを法律上の義務にする等，能動的サイバー防御の妥当性についての事後的な検証が重要になろう。事前の手続き保障に関するハードルを下げる場合，人権保護の観点からは事後のガバナンスを厳格化することによってバランスを取る必要があり，事後のガバナンスをどのように構築するかの検討が求められる。こうした理解は，従前の規定では実現が難しいものだといい得，明確な立法措置が望ましい部分である。

Ⅸ　能動的サイバー防御における SIGINT の役割と「通信の秘密」との関係

①　「国家安全保障戦略」では，SIGINT の必要性に関して，真正面から論じた個所はないが，以下の理由から「能動的サイバー防御（Active Cyber Defense＝能動的サイバー防御）」には不可欠の機能である旨の了解が，関係者の間では共有されているものと推定される。a）能動的サイバー防御が「重大なサイバー攻撃のおそれを未然に排除し，それが発生した場合の被害の拡大を防止する」ものである以上，攻撃者となる可能性が高いシステムの状況を常時監視できることが前提となる，b）「サイバー安全保障での対応能力を欧米主要国と同等以上に向上させる」という高い目標を目指し，「わが国の安全保障に関わる総合的な国力の主な要素」の５つの中に「情報力」を挙げ，「人的情報，公開情報，電波情報，画像情報等，多様な情報源」による総合的な分析（オ

ール・ソース・アナリシス)で高付加価値の分析を行うとしている，c）インテリジェンスはHUMINTから始まり， 現在でもその重要性は高いが， 技術の高度化に伴って次第にSIGINTの役割が重要視され，特に国家のサイバーセキュリティに関しては，SIGINTなしのセキュリティ対策は考えられない。現にロシアのウクライナ侵攻で， 初期に最も効果を発揮したのはSIGINT情報であった，d）それを支援した米国では，大統領令（October 07, 2022）において，「自国と同盟国の安全保障のためにはSIGINT能力を保持し強化しなければならない」が，同時に「プライバシーなどの基本的人権を侵害しないような仕組みが必要」だとしている。

② わが国では「通信の秘密」は，憲法21条2項後段および電気通信事業法4条などで保護されており， 刑事罰を伴う解釈運用は世界的にも厳格だと評価されている（個人情報保護法の保護レベルがEUから「十分性」認定を受ける根拠ともなった)。しかし「通信内容」と「メタ情報」を峻別しない， 事業法の対象事業者が情報処理事業者の一部に拡大する一方外資系事業者は放置されてきた，などの問題点も明らかになっている。

③ 憲法学者の間では「検閲の禁止」は絶対的だが，「通信の秘密」の保護は相対的で，より上位の法益があれば制限される場合がある，という理解が通説になっている。現に特定の犯罪捜査のための通信傍受（通信傍受法）や，インターネット上の違法有害情報対策（両者の場合主として「通信内容」が問題になる）と，サイバーセキュリティを含むインターネットサービスの安定的な提供を行う場合（この場合は主として「メタ情報」が問題になる）に，「通信の秘密」の保護の制限が例外として認められている。

④ このうち，サイバーセキュリティに関する「通信の秘密」保護の制限は，総務省の研究会における第1次から第4次とりまとめ結果に基づき，事業者団体である「インターネットの安定的な運用に関する協議会」が公表している「電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン」において認められ，運用されている。

⑤ その実例は，NOTICE（National Operation Towards IoT Clean Environment）を含む送信型対電気通信設備サイバー攻撃対策とNetFlow分析の２施策である。前者は電気通信事業法(2018年の改正による116条の2)とNICT法（国立研究開発法人情報通信研究機構法，5年間の時限立法）による「法令に基づく正当行為」とされ，送信元の特定などの情報は「電気通信事業者の取扱中に係る通信」とみなされ(164条4項，5項)，その侵害には刑事罰が科せられる(同179条)。後者は，「通信の秘密」侵害の懸念に関して，違法性が阻却される「正当業務行為」と位置付けられている。

⑥ なお「通信の秘密」に関わる情報か否かに関わらず，サイバー脅威に関する情報共有の仕組みとしては，業界別のISAC（Information Sharing and Analysis Center）や「サイバーセキュリティ協議会」がある。前者は民間の自主的活動だが後者は法に基づくもので， 国の行政機関，重要社会基盤事業者， サイバー関連事業者や教育研究機関など官民の多様な主体が相互に連携し，より早期の段階で対策情報等を迅速に共有することにより， サイバー攻撃による被害の拡大を防ぐことなどを目的としている（サイバーセキュリティ基本法 17 条)。協議会の事務に従事する者又は従事していた者には守秘義務があり（17条4項），違反すると1年以下の懲役又は50 万円以下の罰金に処せられる（同38条。この罰則は，国家公務員法100条・109条と同じで，通信の秘密侵害罪よりも軽い)。

⑦ ただし， 電気通信事業者は「通信の秘密」保護の制限行為を自己判断として行うことはもとより， 情報の共有についても謙抑的である。なぜなら「秘密の保護」が原則で「保護の制限」は

例外処理であるため，例外に当たる正当行為・正当防衛・緊急避難などの要件に該当するか否か，慎重な判断を求められるからである。そこで勢い，新たな事項について制限する場合には，個別事案ごとに総務省研究会のとりまとめを受け，上記ガイドラインを改正することによって対処している。このため新たなサイバー攻撃が出てきても迅速に対応することが困難な状況にある。

⑧　このように上記の④と⑤は，ソフト・ローの範囲で対応しているが，個人情報保護法にあれだけの議論が巻き起こるのであれば，当然法制化（ハード・ロー化）が検討されてしかるべきであろう。現在ハード・ローとして存在するのは犯罪捜査に関する「通信傍受法」のみであり，国家安全保障に関して「通信の秘密」保護の制限を認める法律は存在しない。

X　SIGINT に必要な通信法関連の法整備

わが国には SIGINT に関する組織と権限を定めた法律は存在しないので，通信法関連の法整備を検討する前に，その制定が前提となろう。その際，Five Eyes の中心的存在である英米の法，すなわち英国の Investigatory Powers Act 2016 と，米国の大統領令（12333 号と前節「IX 能動的サイバー防御における SIGINT の役割と「通信の秘密」」との関係で述べた October 07, 2022 付）および FISA（Foreign Intelligence Surveillance Act of 1978）が参考になろう。前者は議院内閣制下の法律である点で，後者は軍事・非軍事を区分せず一般的原則を掲げている点で，わが国にも教訓を与えるものと思われる。

前節に基づく具体的な課題として，政府機関のシステムの常時監視とともに，能動的サイバー防御の実施体制整備のために挙げられている以下の３点の具体的措置に関して，「通信の秘密」の観点からの検討が必要である。

(a)「通信の秘密」保護を制限することによって得た（知得した）情報を，他者と共有する（官民共有を含む）ことの許容性

(b) 攻撃者による悪用が疑われるサーバ等を検知するために，国内の通信事業者が役務提供する通信に係る活用情報の範囲

(c) 重大なサイバー攻撃について，可能な限り未然に攻撃者のサーバ等への侵入・無害化ができるよう，政府に対して必要な権限の付与

上記の(a)および(b)については，政府による民間情報の利用（いわゆる government access）の構成要件を明確にする必要があり，そこでは「通信内容」と「メタ情報」は別扱いになると思われる（通信の秘密の対象とすべき範囲もしくはその取扱いは国によって異なっており，わが国では伝統的に通信の内容にとどまらず，通信の日時，場所，通信回数等のメタデータを含み一律の取扱いとするのが通説的な見解であるが，これらは区別して論じられるべきであるとの見解も出されている)。その際，現行の「通信の秘密」保護の制限の範囲を超える場合には，制限する根拠を法律レベルに明記するとともに，制限範囲を拡大する法的規定（ハード・ローおよびソフト・ロー）を追加する必要がある。しかし前節で述べたように，既に一部の施策は実施中であり全くの新規事項ではないので，さほどの困難を伴わないものと思われる。

一方(c)については，国家安全保障のために「通信の秘密」保護を制限する新規立法を行う必要がある。電気通信事業者およびコンピュータ・サーバ・システム運用者と共に，政府機関による SIGINT 情報を含む多様な情報源に基づく情報収集・分析能力の強化がなければ，「未然に攻撃者のサーバ等への侵入・無害化」を行うことは困難である。このため，政府機関自身が「通信の秘

密」保護を制限して，サイバーセキュリティのために情報を活用できるよう，根拠法の制定が必要になる。

電気通信事業者のインターネット防御能力強化のためには，技術力向上とともに「通信の秘密」保護を制限できる範囲の明確化，法律レベルでの規定の新設を行うことが必要である。これは電気通信事業法の設備に関する規律（同法 41 条～49 条など）をサイバー時代に合わせて改定することで，ほぼ達成可能と思われる。

問題は，電気通信事業法の規律下にない「情報処理システム」の運営者である。サイバーインシデントは，通信システムの部分で発生するものも多いが，情報処理システムが攻撃されて発生するものは更に多いと思われるので，後者の運営者に何らかのシステム管理責任を負ってもらいたいところである。1 つの案として，インターネットが「自律システム」の相互接続で成り立っていることから，「自律システムのセキュリティ対策は当該システムの管理者が負う」という「自律システム管理責任」を広く薄くかけていく案が考えられる（ある研究者は，サイバーセキュリティ基本法 7 条に 2 項以下を追加して「自律システム管理責任」を課す一方で，インシデント情報の活用・共有を認めることでインセンティブを与えようとしている）。

加えて，同法が指定する重要社会基盤事業者（6 条）には，更に一段上の義務（特にインシデント報告義務や公開義務）を課すことが議論されている。しかし，インシデントをそのまま公開したのでは，「犯罪者に入れ知恵する」結果にもなりかねない。そこで，政府自身がインシデント情報を自ら知得・分析して，非公開のまま重要社会基盤事業者に事前通知することができれば，give ＆ take のインセンティブとして期待できる。

通信の秘密は憲法上も保障された権利であるが，前述のとおり一定の制約を受けることは否定されていない。通信の発達と技術的進歩に鑑みると，現代においてサイバー防御を行っていくためには通信の解析を行わざるを得ない実態があり，他に代替できる手段がない以上は必要最低限度の制約が課されることは受容されると考えている。このように，サイバー防御によって国民の生命身体の安全そして基本的人権の保護を実現するために「通信の秘密」保護に対する制約をしていく必然性を認めた上で，基本的人権自体の保護と制約のバランスを確保していくための配慮・（濫用防止の）仕組みづくりが不可欠である。これは民主主義国家のみが保有する仕組みであり，これが欠けると非民主主義国家から「やっていることは同じではないか」との批判を招くことになる。この検討に際しては，EU-日本の十分性認定を行った理由と EU-米国のデータ・プライバシー・フレームワークの内容に加え，安全保障上の SIGINT 活動を規定している米国の FISA（その根拠となる大統領令を含む）や英国の IPA2016 の規定を能動的サイバー防御に係る法制度設計の参考にすることが望まれる。

参考文献

林紘一郎・田川義博「サイバーセキュリティと通信の秘密に関する提言：自律システム管理責任の明確化と対象を特定した通信ログの利活用を」『情報セキュリティ総合科学』vol.12
2020 年 11 月 1 日　http://www.iisec.ac.jp/proc/vol0012/hayashi-tagawa20.pdf

XI　有責者の資産凍結や入国禁止のための外為法・出入国管理難民認定法上の措置

サイバー攻撃に直接の責任を有する者個人や企業・団体の資産を凍結し，また当該個人の入国

を禁止することは米国やEUにおいて行われている。これらの措置はサイバー攻撃に対して諸国家が現実にとり，かつとった旨を公表している最も主要な措置となっている。資産凍結と入国禁止は，経済制裁の中でも標的制裁といわれるものである。国連決議に基づく場合にはスマート・サンクションの一環として位置づけられる。また，国連憲章103条に基づき，安保理決定の実施義務は，抵触する協定に優位する。国連決議に基づかなくても国際法違反（サイバー攻撃）を犯した国家や団体・個人への経済制裁の一部としてとることは国際法上，可能である。

わが国においては，資産凍結は外為為替及び外国貿易法（外為法）が，入国禁止については出入国管理及び難民認定法が措置の実施根拠となる。資産凍結については，第16条第1項において，①「わが国が締結した条約その他の国際約束を誠実に履行するため必要があると認めるとき」，②「国際平和のための国際的な努力にわが国として寄与するため特に必要があると認めるとき」，③「第10条第1項の閣議決定が行われたとき（同項では，わが国の平和及び安全の維持のため特に必要があるときは，閣議において対応措置を講ずべきことを決定できる旨，規定する)」のいずれかの場合にとることができる。①は国連安保理決議に基づく非軍事的強制措置の一環としてとる場合が典型である。②はロシアのウクライナ侵略に対する西側諸国による対ロシア経済制裁措置の一部としてのロシア資産凍結が最近の例である。わが国に対してサイバー攻撃がなされ，但し国連安保理やG7での合意に基づく反応としてとられるのではない場合（現実にはそのような場合が大半であると考えられる）においては，③のみが根拠になると解せられるが，閣議決定が確実かつ迅速になされる必要がある。このため，包括法においてサイバー攻撃に対する措置には，サイバー攻撃に責任を有する者の資産凍結が含まれる旨を明記しておくべきである。

サイバー攻撃に責任を有する者の入国禁止については，出入国管理及び難民認定法第５条１項において列挙された上陸拒否事由のうち該当すると思われるのは，「十四　法務大臣において日本国の利益又は公安を害する行為を行うおそれがあると認めるに足りる相当の理由がある者」にほぼ限定される。同号は「公安条項」と呼ばれ，「伝家の宝刀」として援用される場面はほぼ皆無であったが，2020年のCOVID-19の感染拡大時に感染者が搭乗するウエステルダム号（オランダ船籍）のわが国の港湾への入港を同号を根拠に拒否したことが注目される。包括法においてサイバー攻撃に対する反応措置には，サイバー攻撃に責任を有する者の入国禁止が含まれる旨を明記して，サイバー攻撃に責任を有する者の入国拒否が円滑にできるようにしておくこと（「伝家の宝刀」が床の間の飾りにとどまらないようにすること）が重要である。

Ⅻ　第２部の終わりに

第２部では必要な論点に関して法律的な視点でどのように考えうるのかという整理を提示した。視点として特に重要なことは既存の法律の解釈を行うことを目的としているものではなく，新しい枠組みのための立法を支えるということである。その意味で踏み込んだものとなっている部分があると考える方もいるかもしれないが，今，私たちが直面している現状が新しい枠組みを支える立法事実となるということを念頭に，国民の安全を守るためにあらゆる可能性を模索し，考察を深めていかなければならない。

「第2部　わが国における能動的サイバー防御のための法整備」執筆者/「わが国におけるアクティブサイバーディフェンスに関する法制度研究会」構成員

（五十音順）

石井　由梨佳	防衛大学校人文社会科学群国際関係学科准教授
伊東　寛	情報通信研究機構（NICT）主席研究員
鎮目　征樹	学習院大学法学部法学科教授
田川　義博	元情報セキュリティ大学院大学セキュアシステム研究所客員研究員
中谷　和弘	東京大学大学院法学政治学研究科教授
永野　秀雄	法政大学人間環境学部教授
西貝　吉晃	千葉大学大学院社会科学研究院准教授
林　紘一郎	情報セキュリティ大学院大学名誉教授
山中　倫太郎	防衛大学校人文社会科学群公共政策学科教授
山本　龍彦	慶應義塾大学大学院法務研究科教授

事務局　紀尾井町戦略研究所株式会社