参議院常任委員会調査室・特別調査室

論題	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－
著者 / 所属	榎本　尚行 / 内閣委員会調査室
雑誌名 / ISSN	立法と調査 / 0915-1338
編集・発行	参議院事務局企画調整室
通号	477 号
刊行日	2025-7-25
頁	23-43
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20250725.html

※ 本文中の意見にわたる部分は、執筆者個人の見解です。

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 ―

榎本　尚行
（内閣委員会調査室）

１．はじめに

能動的サイバー防御を導入するとして令和７年２月７日に国会に提出された、「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案」（閣法第４号）（以下「サイバー対処能力強化法案」という。）及び「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案」（閣法第５号）（以下「整備法案」という。）は、大別して官民連携の強化、通信情報の利用及びアクセス・無害化措置の３本柱から成る。

前号掲載の「能動的サイバー防御２法案の国会論議（１）」では制度の全体像及び官民連携の強化について整理し、本号掲載の「能動的サイバー防御２法案の国会論議（２）」では通信情報の利用について整理してきた。本稿では、残るアクセス・無害化措置について、その制度の概要を確認した上で、主な国会論議を整理する[1]。

２．国家安全保障戦略及び有識者会議提言

能動的サイバー防御の導入について示した国家安全保障戦略（令和４年12月16日国家安

[1] 自衛隊におけるアクセス・無害化措置の概要及び主な国会論議については、本号掲載の藤川隆明「サイバー空間における自衛隊のアクセス・無害化措置― 能動的サイバー防御導入に伴う自衛隊法改正の概要と国会論議 ―」も参照。

全保障会議決定・閣議決定）では、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に向上させるための取組として、「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。」とした上で、アクセス・無害化措置に関しては、「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。」とされた。

政府は、能動的サイバー防御を導入するため、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（以下「有識者会議」という。）で検討を進め、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（令和６年11月29日）（以下「有識者会議提言」という。）が取りまとめられた。同提言では、アクセス・無害化に関して、**図表１**のような指摘がなされ、これを踏まえて法案が検討された。

図表１　有識者会議提言におけるアクセス・無害化に関する提言概要

- サイバー攻撃の特徴（①危険の認知の困難性、②意図次第でいつでも攻撃可能、③被害の瞬時拡散性）を踏まえ、**被害防止を目的**としたアクセス・無害化を行う権限は、**緊急性を意識**し、**事象や状況の変化に応じて臨機応変かつ即時に対処可能な制度にすべき**。こうした措置は、比例原則を遵守し、必要な範囲で実施されるものとする必要。その際、執行のシステム等を含め、従前から機能してきた**警察官職務執行法を参考**としつつ、その**適正な実施を確保するための検討を行うべき**。
- 平時と有事の境がなく、事象の原因究明が困難な中で急激なエスカレートが想定されるサイバー攻撃の特性から、**武力攻撃事態に至らない段階から我が国を全方位でシームレスに守るための制度**とすべき。
- アクセス・無害化の措置の性格、既存の法執行システムとの接合性等を踏まえ、**権限の執行主体**は、**警察や防衛省・自衛隊**とし、その能力等を十全に活用すべき。**まずは警察が、公共の秩序維持の観点から特に必要がある場合には自衛隊が**これに加わり、共同で実効的に措置を**実施できるような制度とすべき**。
- 権限行使の対象は、**国の安全や国民の生命・身体・財産に深く関わる国、重要インフラ、事態発生時等に自衛隊等の活動が依存するインフラ**等へのサイバー攻撃に重点を置く一方、**必要性が認められる場合に適切に権限行使できる仕組み**とすべき。
- 国際法との関係では、他国の主権侵害に当たる行為をあらかじめ確定しておくことは困難。他国の主権侵害に当たる場合の違法性阻却事由としては、実務上は対抗措置法理より**緊急状態法理の方が援用**しやすいものと考えられるが、国際法上許容される範囲内でアクセス・無害化が行われるような仕組みを検討すべき。

（出所）有識者会議提言概要より抜粋

３．両法律案におけるアクセス・無害化措置関連規定の概要

（１）アクセス・無害化措置の概要

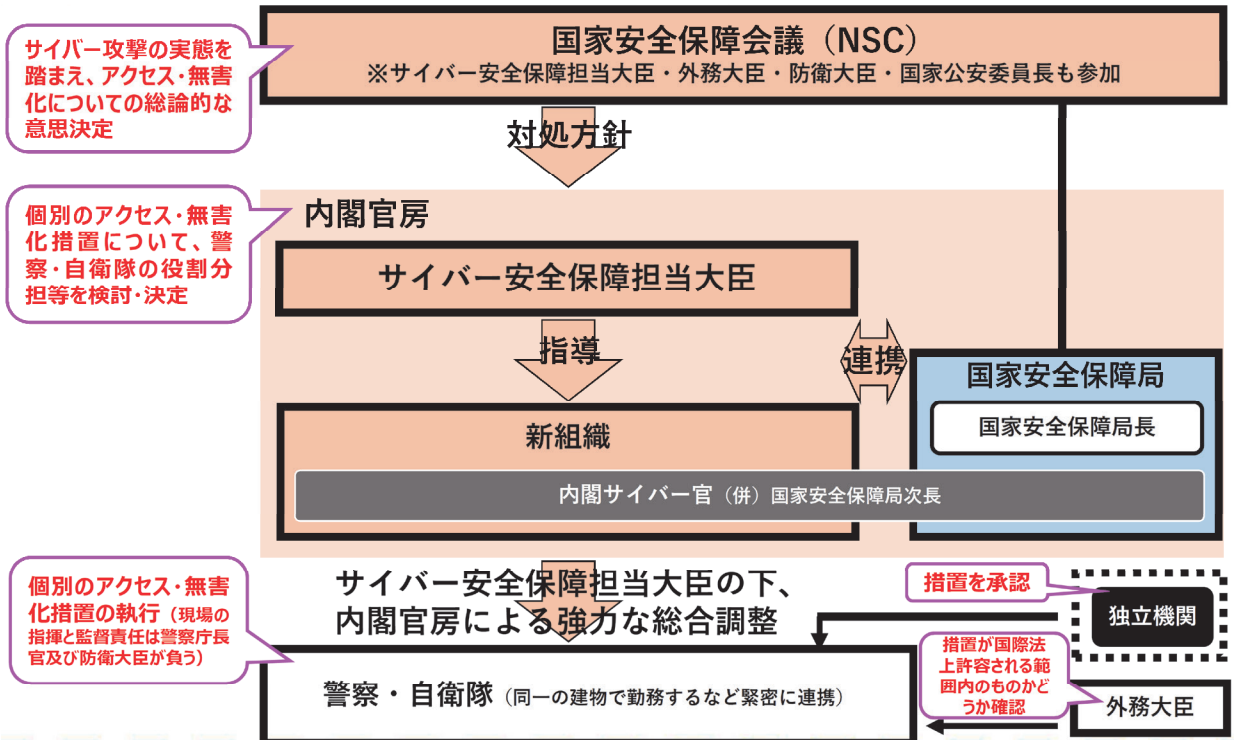
アクセス・無害化措置に関しては、主に整備法案に盛り込まれた警察官職務執行法（昭和23年法律第136号。以下「警職法」という。）、自衛隊法（昭和29年法律第165号）の一部改正において、関連規定の整備が行われている。実施主体は警察及び自衛隊とされており、

内閣官房の総合調整の下で措置を行う。

措置の流れは**図表２**のとおりであり、アクセス・無害化措置が必要となる場合、まず、国家安全保障会議（以下「ＮＳＣ」という。）四大臣会合[2]において総論的な対処方針を決定する。その後、内閣官房の総合調整により実施主体（警察又は自衛隊）の決定等を行った上で、実施主体が具体的な措置を実施する。なお、今回の整備法案には、ＮＳＣの関与等に関する改正は盛り込まれておらず、基本的には既存の法律を根拠として行われることとなる[3]。

実施主体が決定された後は、警察又は自衛隊は、新設される警職法第６条の２又は自衛隊法で準用される警職法の同規定に沿ってアクセス・無害化措置を行う。アクセス・無害化措置を行う要件や手続の概要は**図表３**のとおりである。また、実施に当たって総合調整を担う内閣官房については、現行で設置されている内閣官房内閣サイバーセキュリティセンター（以下「ＮＩＳＣ」という。）を発展的に改組し、次官級の内閣サイバー官を置くことが整備法案に盛り込まれたほか、国家サイバー統括室を置くこととされている（同室の設置に係る規定については、政令事項。両者とも、関係規定の施行により令和７年７月１日に発足した。）。

図表２　アクセス・無害化措置の実施の流れ



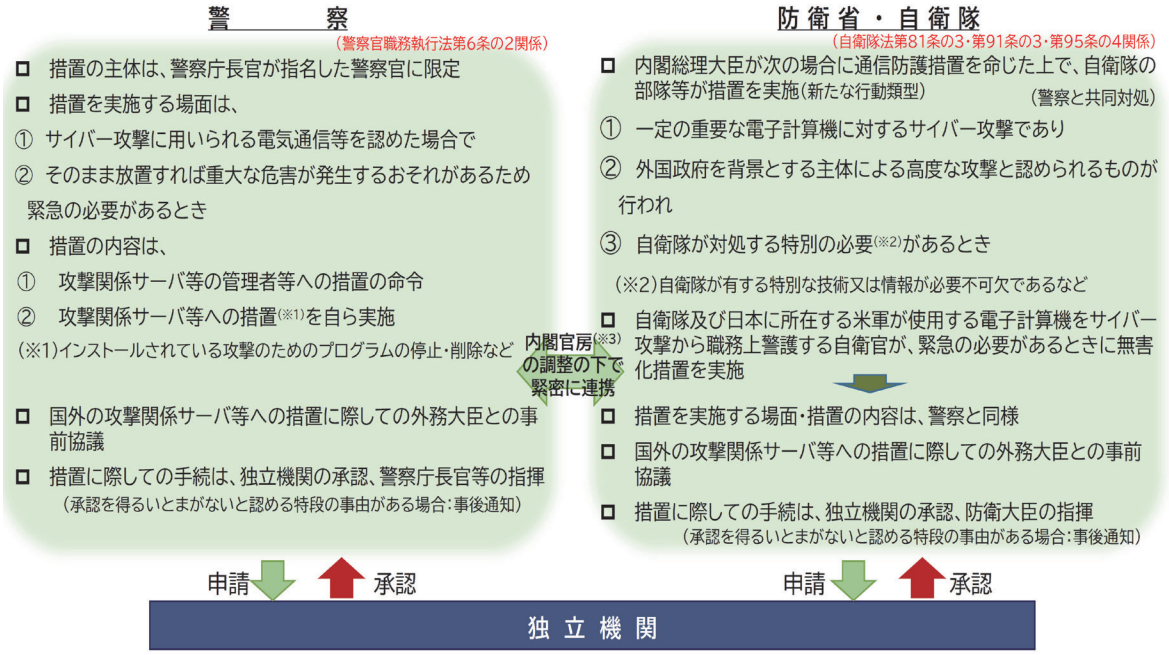
（出所）「サイバー対処能力強化法及び同整備法について」（令和７年５月内閣官房サイバー安全保障体制整備準備室）より抜粋

---

[2] 国家安全保障会議設置法（昭和61年法律第71号）では、内閣総理大臣、外務大臣、防衛大臣及び内閣官房長官の四大臣会合において、国家安全保障に関する外交政策、防衛政策及び経済政策の基本方針並びにこれらの政策に関する重要事項を審議することとされている。

[3] ＮＳＣについて国家安全保障会議設置法に規定が置かれているほか、内閣官房の総合調整について内閣法（昭和22年法律第５号）に規定が置かれている。

図表３　アクセス・無害化措置の概要



（※３）アクセス・無害化については、その実施主体が警察及び自衛隊になるが、こうした措置は国家安全保障の観点から整合性のとれた形で行われる必要があり、内閣官房（新組織）が、国家安全保障局（NSS）とも連携しつつ、その司令塔機能を発揮。

（出所）「サイバー対処能力強化法及び同整備法について」（令和７年５月内閣官房サイバー安全保障体制整備準備室）より抜粋

また、国外に所在するサーバ等に対するアクセス・無害化措置の実施については、当該国の主権侵害に該当するおそれがあることから、国際法との関係が議論となり得る。このため、実施主体は外務大臣との協議を行うこととされている。

国際法との関係について、「サイバー対処能力強化法及び同整備法について」（令和７年５月内閣官房サイバー安全保障体制整備準備室）（以下「準備室説明資料」という。）では、「措置を国外にあるサーバ等に対して行う場合、主権侵害に該当するとしても、「緊急状態」等の国際法上の法理を援用するなどして、国際法上許容される範囲内で実施。」とされている。「緊急状態」（Necessity）とは、「当該措置が、重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であり、相手国等の不可欠の利益を深刻に侵害しないといった一定の要件を満たす場合に、違法性が阻却されるという考え方。」とされている。

整備法案に盛り込まれた警職法及び自衛隊法の主な改正内容は、以下のとおりである。

（２）警察官職務執行法の一部改正

ア　サイバー危害防止措置執行官の指名

警察庁長官は、警察庁又は都道府県警察の警察官のうちから、イの規定による処置を適正にとるために必要な知識及び能力を有すると認められる警察官をサイバー危害防止措置執行官として指名するものとする（警職法第６条の２第１項）。

イ　サイバー危害防止措置執行官による措置

サイバー攻撃又はその疑いがある通信等を認めた場合であって、そのまま放置すれば、

人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときは、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、危害防止のため通常必要と認められる措置であって電気通信回線を介して行うものをとることを命じ、又は自らその措置をとることができることとする（同条第２項）[4]。

ウ　国外のサーバ等に対する措置の実施に当たっての外務大臣との協議

処置の対象たる電子計算機が国内に設置されていると認める相当な理由がない場合には、警察庁の警察官のみが処置をできることとし、あらかじめ、警察庁長官を通じて、外務大臣と協議しなければならない（同条第３項）。

なお、外務大臣との協議は、実施するアクセス・無害化措置が、国際法上許容される内容であることを担保するためのものであるとされる（詳細は４.の国会論議を参照。）。

エ　サイバー通信情報監理委員会の承認

サイバー危害防止措置執行官が、処置をとる場合には、あらかじめ、サイバー通信情報監理委員会（後述）の承認を得なければならない。ただし、サイバー通信情報監理委員会の承認を得るいとまがないと認める特段の事由がある場合にはこの限りでないこととし、当該処置後速やかに、当該処置についてサイバー通信情報監理委員会に通知しなければならない。通知を受けた同委員会は、必要に応じ勧告を実施する（同条第４項及び第９項）。

オ　警察庁長官等の指揮

サイバー危害防止措置執行官は、この条の規定による措置の実施について、警察庁長官等[5]の指揮を受けなければならない（同条第10項）。

（３）自衛隊法の一部改正

ア　通信防護措置の創設

自衛隊法の一部改正においては、同法第81条の３が新設され、新たな行動類型である通信防護措置が規定されている。

同条においては、内閣総理大臣は、①一定の重要電子計算機に対する攻撃であって、②本邦外にある者による特に高度に組織的かつ計画的な行為と認められるものが行われた場合において、③自衛隊が対処を行う特別の必要があると認めるときは、当該重要電子計算機に対する通信防護措置をとるべき旨を命ずることができる旨が規定されている。

さらに、③の「自衛隊が対処を行う特別の必要があるとき」の要件として、以下の３点の全てを満たす必要がある。

・当該特定不正行為により重要電子計算機に特定重大支障（重要電子計算機の機能の停止又は低下であって、当該機能の停止又は低下が生じた場合に、当該重要電子計算機に係る事務又は事業の安定的な遂行に容易に回復することができない支障が生

---

[4] なお、サイバー危害防止措置執行官は、第２項の規定による処置をとるに際しては、みだりに関係者の正当な業務を妨害してはならない（第７項）ほか、同執行官は、第２項の規定による処置をとったときは、当該加害関係電子計算機の管理者に同項に規定する措置をとることを命じた場合を除き、国家公安委員会規則で定めるところにより、遅滞なく、その旨を当該管理者に通知するものとされている（第８項）。

[5] 警察庁長官又は警視総監若しくは道府県警察本部長。

じ、これによって国家及び国民の安全を著しく損なう事態が生ずるものをいう。）が生ずるおそれが大きいと認めること。

・特定重大支障の発生を防止するために自衛隊が有する特別の技術又は情報が必要不可欠であること。

・国家公安委員会からの要請又はその同意があること。

イ　警察との共同対処

通信防護措置をとるべき旨を命ぜられた部隊等[6]は、警察と共同して当該通信防護措置を実施する。その際、改正警職法を準用し、（２）と類似の手続を行うこととされており、具体的には、外務大臣との協議及びサイバー通信情報監理委員会の承認について、当該部隊等の自衛官は防衛大臣を通じて行うこととされている。さらに、当該部隊等の自衛官は、実施について防衛大臣の指揮を受けなければならない。

ウ　防衛出動時等における措置の実施

治安出動及び防衛出動時における公共の秩序維持について、改正警職法の規定を準用するほか、自衛隊又は日本国にあるアメリカ合衆国の軍隊が使用する一定の電子計算機をサイバーセキュリティを害することその他情報技術を用いた不正な行為から職務上警護する自衛官の職務の執行について、改正警職法の規定を準用する。

（４）サイバー通信情報監理委員会の承認

サイバー対処能力強化法案において、監視・監督を行ういわゆる三条委員会[7]として、「サイバー通信情報監理委員会」を置くとされている。同委員会では、アクセス・無害化措置における承認及び承認の求めに対する審査、事後通知があった場合における確認及び勧告を所掌する。同委員会の事務の実施状況について、国会に報告することとされているところ、衆議院における修正により、承認の件数等を報告しなければならないとする規定が追加され、報告内容の具体化が図られた。

（５）内閣法の一部改正

内閣法の一部改正により、内閣官房に、サイバーセキュリティの確保に関する事務等を掌理する内閣サイバー官（次官級の特別職）１人を新たに置く。また、国家安全保障局次長を３人に増やすこととし、うち１人を内閣サイバー官をもって充てる。

（６）施行期日

警察官職務執行法の一部改正、自衛隊法の一部改正の規定は、サイバー対処能力強化法の施行の日から施行することとされており、具体的には、サイバー対処能力強化法の公布の日から起算して１年６月を超えない範囲内において政令で定める日から施行される。

また、内閣サイバー官の設置に関する規定等については、サイバー対処能力強化法の公

---

[6] 陸上自衛隊、海上自衛隊又は航空自衛隊の部隊及び機関。

[7] 一定の独立性を持つ機関であり、公正取引委員会、個人情報保護委員会等が該当する。

布の日から起算して６月を超えない範囲内において政令で定める日から施行される[8]。

４．アクセス・無害化措置についての主な国会論議[9]

アクセス・無害化措置については、国会審議において国内法・国際法の両面で様々な論点が取り上げられた。以下では、アクセス・無害化措置と、国内法・国際法に関係する議論や、措置の実施に向けた手続等についての議論を紹介する。また、特に、実施主体の一つである警察に関連する主な議論は、５．において整理する。

（１）武力の行使との関係及びエスカレーションリスクの懸念

国家安全保障戦略では、「武力攻撃に至らない」段階を対象として能動的サイバー防御を導入することが掲げられていた。同戦略に基づく検討を踏まえて法案に規定されたアクセス・無害化措置が、憲法を始めとした国内法に照らして武力の行使に当たらないとする理由について問われた。石破茂内閣総理大臣は、「アクセス・無害化措置は、公共の秩序の維持の観点から、警察権の範囲内で必要最小限度の措置として行うものであり、攻撃サーバ等にアクセスして不正プログラムを無害化する措置等を想定している。措置の対象となるサーバ等に対して、物理的被害や機能喪失など、その本来の機能に大きな影響を生じさせることは想定していない。そのため、当該措置は、人を殺傷し又は物を破壊するという戦闘行為には当たらず、憲法第９条が禁ずる国際的な武力紛争の一環としての戦闘行為、すなわち武力の行使に当たるものではない」旨答弁した[10]。

また、能動的サイバー防御が武力攻撃と捉えられるおそれや、アクセス・無害化措置を起点として予期せぬ事態のエスカレートを招くエスカレーションリスクについての懸念に対して、内閣官房は、「今回のアクセス・無害化措置は、そもそも武力の行使と評価されるものではなく、武力攻撃や先制攻撃とみなされるようなものではない。このため、我が国の措置が起点となって予期せぬ事態のエスカレートを招くようなことはないと考えている」としつつ、その上で、アクセス・無害化措置の制度に沿って運用することで、「政府としては、万が一にも予期せぬ事態のエスカレーションが生じることのないように対応していく」旨答弁した[11]。

（２）総論的な対処方針及び実施主体の決定

アクセス・無害化措置は、警察又は防衛省・自衛隊が実施することとされているところ、実施に当たっては、まず総論的な対処方針は、ＮＳＣ四大臣会合で決定され、その後、内閣官房の総合調整により、実施主体の決定等が行われるとされる。措置の実施に至るまでの流れに関して質疑が行われた。

---

[8] 前述のとおり、内閣サイバー官の設置等については令和７年７月１日から施行されている。
[9] 以下、会議録の引用部分については、発言の趣旨が変わらない範囲で要約や字句修正を施している。
[10] 第217回国会衆議院本会議録第９号（令7.3.18）
[11] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

ア　国家安全保障会議四大臣会合における総論的な対処方針の決定

準備室説明資料では、アクセス・無害化措置を実施するに当たっては、サイバー攻撃の実態を踏まえ、アクセス・無害化についての総論的な意思決定が行われるとされている（**図表２**）。

この趣旨について問われた石破総理は、まず、総論的な意思決定について、「国、基幹インフラ事業者等に対する一連の重大なサイバー攻撃の発生又は予兆を認知し、アクセス・無害化措置を実施する必要があると認められる場合には、国家安全保障の観点からこれが適切に行われるよう、私自身が議長を務める国家安全保障会議（ＮＳＣ）で速やかに審議をした上で総論的な対処方針を定める。総論的な対処方針とは、一連の重大なサイバー攻撃､いわゆるサイバー攻撃キャンペーンの対応における基本的な方針である」とした。その上で､「この総論的な対処方針に基づき、サイバー安全保障担当大臣の指導の下で、内閣官房に置かれる新組織が、国家安全保障局（以下「ＮＳＳ」という。）と緊密に連携して、個別のアクセス・無害化措置の執行についての警察、自衛隊の役割分担等を速やかに決定し、その後、措置の実施主体たる警察又は自衛隊が個別の措置についての法的手続に入る」旨答弁した[12]。

「攻撃キャンペーン」の定義等について内閣官房は､「おおむねある特定のハッカー集団等が特定の目的の達成に向けて一定の時間的範囲の中で計画し、実施するサイバー攻撃のまとまりという意味で使われていると承知している。したがって、ＮＳＣ四大臣会合を開催する以前の段階として、攻撃キャンペーンが行われる、あるいは行われるであろうという予兆を把握するということになり、サイバー新組織、あるいは関係省庁と連携して、それに対するアクセス・無害化措置が必要であるという判断をした場合にはＮＳＣを速やかに開催する」旨答弁した[13]。

さらに、内閣官房から､「一つのサイバー攻撃キャンペーンに対して、基本的に一度ＮＳＣを行う」こと[14]､「個別のサーバへの個別のアクセス・無害化措置に関して、ＮＳＣが個々に関与し決定するという形ではない」ことが説明され[15]、その上で、ＮＳＣでの具体的な審議の在り方については､「ＮＳＣ四大臣会合に、国家公安委員会委員長、サイバー安全保障大臣を呼び、外交的な考慮についての検討を行う」とされ[16]、その他の審議内容としては､「例えば､その時々の我が国を取り巻く安全保障環境の中において当該攻

---

[12] 第217回国会参議院本会議録第14号（令7.4.18）

[13] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

[14] なお、内閣官房は､「総論的な対処方針の決定の後、それを変えなければいけない事態が出てくることも想定される。その場合、一度ＮＳＣを開いたキャンペーンであっても、改めてのＮＳＣを開催することは考えられる」旨答弁した（第217回国会参議院内閣委員会会議録第14号（令7.5.15））。

[15] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

[16] 四大臣会合には、サイバー安全保障担当大臣が常時出席することとはされていないが、この理由や妥当性等について平将明国務大臣（サイバー安全保障担当大臣）は､「ＮＳＣ四大臣会合の審議事項にサイバー安全保障が含まれるとの解釈は政府内で確立している。また、アクセス・無害化措置の実施に関する総論的な対処方針等を審議するＮＳＣ四大臣会合にはサイバー安全保障担当大臣も参加することになるが、この対処方針等の審議に必要な情報については、ＮＳＣの事務局であるＮＳＳから事前に提供を受けることと承知している。したがって、サイバー安全保障担当大臣も四大臣会合に参加をする他の閣僚と共通の認識の下、ＮＳＣ四大臣会合の審議に参加することとなり、総合調整への支障が生じることはない」旨答弁した（第217回国会参議院内閣委員会会議録第13号（令7.5.13））。

撃キャンペーンがどう位置付けられるのかということ、あるいは過去に発生した我が国へのサイバー攻撃と今行われようとしている攻撃との関連性についてはＮＳＣ四大臣会合の中で議論されるのではないかと考えている」旨答弁した[17]。

また、速やかにアクセス・無害化措置を行うためのＮＳＣにおける意思決定や体制について内閣官房は、「速やかに行うことが非常に重要と思っている。ＮＳＣについては、緊急の場合における会議の開催について規則が定められている。例えば四大臣会合は、過半数を超える場合には開催できる、開催する場合に欠席の大臣がいる場合については副大臣で代替できる等の細かい規則が定められている。そうした規則に基づき、会議の体制を更に強化して、速やかな検討、決定ができるような体制を整えていきたい」旨答弁した[18]。

イ　役割分担の決定

総論的な対処方針が定められると、内閣官房の総合調整の下で警察と自衛隊の役割分担が決定されるが、役割分担について内閣官房は「警察においては、これまでのサイバー攻撃の捜査、その他の対処や外国治安機関等との連携を通じて積み上げてきた不正プログラムの解析等の高度なフォレンジック能力[19]や、攻撃者や手口等を解明する高度な情報分析能力等を有している。また、自衛隊においては、武力攻撃事態等における高烈度なサイバー攻撃に対処するために構築してきた高度なサイバー防衛能力や、米軍等との訓練、協力によって獲得しているサイバー攻撃対処手法等を有している」旨、それぞれの強みを説明した上で、「まずは公共の安全と秩序の維持を責務とする警察が、サイバー攻撃を受けている被害組織にかかわらず対処し、国や基幹インフラ等の一定の重要な電子計算機に対する本邦外にある者による特に高度に組織的かつ計画的なサイバー攻撃には内閣総理大臣の命令を受け自衛隊が警察と共同して措置を行う対処体制を整備することを考えている」旨答弁した[20]。

また、準備室説明資料（**図表２**）では、役割分担の決定は、内閣官房がＮＳＳと連携して行う旨が記載されている。この点について内閣官房は、「内閣官房の新組織とＮＳＳの関係については、ＮＳＳはＮＳＣ四大臣会合を主催する国家安全保障会議事務局であり、総論的な対処方針の決定、あるいは対処方針に基づくアクセス・無害化措置の実施が我が国の安全保障政策の中で整合性の取れた形で行われるようにするという点においては責任を共有している。そういった観点から、内閣官房の新組織を率いる内閣サイバー官は、ＮＳＳ次長を兼ねる。しっかりと連携していく体制をつくりたい」旨答弁した[21]。

さらに、実施主体と内閣官房の具体的な連携確保策について、内閣官房は、「警察、自衛隊が有する情報を平素から司令塔組織を含め相互に十分に共有すること、司令塔組織

---

17 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
18 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
19 警察では、デジタル・フォレンジック（犯罪の立証のための電磁的記録の解析技術及びその手続）を活用し、電子機器等から電磁的記録を抽出した上で、文字や画像等の人が認識できる形に変換する電磁的記録の解析を行っている。
20 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
21 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

の役割分担等の調整を踏まえ両者が有機的に連携すること、両者が実施する措置の内容を相互に十分に認識した上で措置を実施し、措置の結果についても直ちに司令塔組織を含め共有をすることなど、運用上の工夫が必要になる。こうした連携が可能になるように、必要な共同訓練、演習の実施や人材育成等についても検討していきたい」旨答弁した[22]。

この点、参議院内閣委員会の附帯決議（以下「参議院附帯決議」という。）[23]では、「十五　アクセス・無害化措置の実施に当たる警察や自衛隊については、サイバー分野の高度な専門教育や同盟国・同志国等との共同演習などを通じ、専門性を継続的に高めるよう、必要な取組を推進すること。」とされた。

ウ　自衛隊の通信防護措置を行う場合の法的手続等

実施主体が決定されると、措置の実施に向けた具体的な手続に入るが、自衛隊が措置を実施する場合には、自衛隊法の一部改正の規定により通信防護措置が発令される。通信防護措置には要件等が定められているが、その内容や手続について平国務大臣は、「新設する自衛隊法第81条の３に基づく内閣総理大臣による通信防護措置の発令は、内閣の首長として行うものであることから、閣議決定に基づいて行うこととなる。また、内閣総理大臣が通信防護措置を発令する際は、あらかじめ、防衛大臣と国家公安委員会との間で協議させた上で、通信防護措置により対処を行う特定不正行為、通信防護措置として実施すべき措置に関する事項などを指定する[24]。内閣総理大臣による通信防護措置等の発令に関する閣議決定は自衛隊法第81条の３に規定する法的要件を満たした上で行われることになるが、その具体的な手続については、措置の実効性等を考慮しつつ、今後検討していく」旨答弁した[25]。

この点、参議院附帯決議では、「十三　通信防護措置の発令を迅速に行う重要性を踏まえ、状況の判断に資する各種情報の収集・分析体制を十分に構築すること。」とされた。

また、通信防護措置発令時において、警察と自衛隊は共同して対処するとされているところ、その指揮命令系統について防衛省は、「自衛隊は、内閣総理大臣による通信防護措置に関する命令に基づき、防衛大臣の指揮により活動することとなっている。他方、警察は、国家公安委員会の管理の下、警察庁長官等の指揮を受け、措置を実施する。別々の指揮命令の下で実施される」旨答弁した[26]。

これらを踏まえ、措置の実施までの各段階での責任主体について、平国務大臣は、「方針はＮＳＣ、総合調整等の判断は担当大臣であり、執行については、実施主体は警察又

---

[22] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

[23] 参議院ウェブサイト〈https://www.sangiin.go.jp/japanese/gianjoho/ketsugi/current/f063_051501.pdf〉（令和７年７月９日最終アクセス）

[24] なお、自衛隊の通信防護措置の要件の一つとして、国家公安委員会の要請又は同意が必要とされている。国家公安委員会の迅速な判断の必要性について、坂井学国家公安委員会委員長は、「国家公安委員会においては、緊急の事態に際しての意思決定手続を定めているが、こうした手続の活用も含め、法施行までの間に検討を進めるほか、平素から内閣官房や防衛省との間で情報共有を緊密に行うよう警察庁を指導し、必要な措置が適時適切に行われるように努めていきたい」旨答弁した（第217回国会参議院内閣委員会会議録第11号（令7.4.24））。

[25] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

[26] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

は自衛隊であるため、警察庁長官又は防衛大臣である」旨答弁し[27]、石破総理は、ＮＳＣの運用上の責任について、「内閣総理大臣が政府を代表してこの責任を負う」旨答弁した[28]。

（３）アクセス・無害化措置の内容等

ア　措置の実施対象及び内容

アクセス・無害化措置については、警職法に定める要件に適合するものについて実施されるが、その具体的内容について問われた。まず、実施対象について警察庁は、「特定の攻撃形態に対して必ず措置を実施するというものではないが、例えば、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のほか、多数の乗っ取られた機器から特定のサーバに対して一度に大量の通信を送出し、通信ネットワークやサーバの処理能力をあふれさせることなどによって被害者側のサービス提供を妨げるいわゆるＤＤｏＳ攻撃などが対象となることはあり得る」旨答弁した[29]。

次に、具体的な実施内容について問われた石破総理は、「具体的には、まず、攻撃に使用されているサーバ等に対して遠隔からログインを行い、当該サーバ等にインストールされているプログラムなどを確認した上で、当該サーバ等が攻撃に用いられないよう、インストールされている攻撃のためのプログラムの停止、削除や、攻撃者が当該サーバなどへアクセスできないような設定変更などの措置を行うことを想定している。これらの具体的な手法については、個別具体の状況に応じて適切に判断する」旨答弁した[30]。

イ　措置を行う端緒となる攻撃の予兆の把握方法

アクセス・無害化措置を実施するに当たっては、攻撃の予兆を把握する必要がある。その方法について内閣官房は、「サイバー対処能力強化法案においては、基幹インフラ事業者に対するインシデント報告等の義務付けなどにより、複数のインフラ事業者の制御システムを標的としたマルウェアの設置など、政府として重大なサイバー攻撃やその予兆の把握が可能となる。こうした情報に加え、通信情報の利用、協議会を通じて把握した情報、サイバー攻撃に関するオープンソースである公刊情報、同盟国、同志国との連携により共有された情報など、様々な情報を踏まえ、改正後の警職法に規定する要件を満たすか否かを適切に判断していくことになる」旨答弁した[31]。

ウ　サイバー危害防止措置執行官の行為が違法とされない根拠

警職法では、指名された警察官であるサイバー危害防止措置執行官が措置を実施するとされる。これについて、同執行官はその業務として行った行為が違法であるとして処罰されないことの確認があり、平国務大臣は、「アクセス・無害化措置についてはその行

---

[27] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）
[28] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
[29] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[30] 第217回国会衆議院本会議録第９号（令7.3.18）
[31] 第217回国会衆議院内閣委員会議録第８号６～７頁（令7.3.26）

為は不正アクセス禁止法[32]等の刑罰法令に抵触し得るものであるが、たとえ個別の犯罪構成要件に該当したとしても、警職法第６条の２第２項の要件を満たす限り、刑法（明治40年法律第45号）第35条の規定[33]により、法令行為として違法性が阻却されることになる。また、この点については、例えば何らかの理由により、アクセスはしたものの、結果的に無害化措置に至らなかった場合も同様であり、警職法第６条の２第２項の要件を満たす限り、違法性が阻却される」旨答弁した[34]。

一方で、同執行官が職務を怠った場合や、故意に悪質行為を行ってしまった場合などへの対応について、坂井国家公安委員会委員長は、「アクセス・無害化措置の実施については、警察庁長官等の指揮を受けなければならないこととしており、これにより適正な職務執行が担保されるとまずは考えているが、万が一サイバー危害防止措置執行官における非違事案等が発生した場合には、国家公務員法（昭和22年法律第120号）等に基づく懲戒処分等により適切に対応していくよう指導していく」旨答弁した[35]。

エ　措置により個人情報を取得しアクセス・無害化以外に利用する懸念

アクセス・無害化措置の過程で個人情報を取得する可能性について問われた平国務大臣は、「必要最小限度の範囲で、当該サーバ等に記録されているその動作に係る記録を確認することもあり得るが、通信に関係する情報を確認しようとする行為を含め、独立の立場にあるサイバー通信情報監理委員会の承認を得ることで必要最小限度の措置となる制度となっているものと考えている。個人が特定されるような通信情報の取得、把握に関しては、危害防止のために必要と認めざるを得ない場合には、アクセス・無害化措置の過程で、攻撃に利用されるサーバ等の通信履歴といった通信に関する情報を把握する可能性も排除されない」旨答弁した[36]。また、内閣官房は、「アクセス・無害化措置の状況によっては、攻撃側のサーバにアクセスして、中で動いているプログラム、あるいはそのプログラムの関係する通信履歴等を確認することがある。その過程でプライバシーに関わるような情報というのを確認することはある」とし、条文上は「警職法第６条の２第２項で「適切に危害防止を図るために通常必要と認められる限度において、電気通信回線を介して当該加害関係電子計算機に接続して当該加害関係電子計算機に記録されたその動作に係る電磁的記録を確認することを含む。」とされており、その限度において確認をする」旨答弁した[37]。

（４）サイバー通信情報監理委員会による承認

ア　事前承認の制度概要及び事前に承認を得ない場合が常態化する懸念

アクセス・無害化措置は、原則としてサイバー通信情報監理委員会の承認を得て行うとされるが、承認を得るいとまがないと認める特段の事由がある場合、事前の承認を得

---

[32] 不正アクセス行為の禁止等に関する法律（平成11年法律第128号）
[33] 同条では、「法令又は正当な業務による行為は、罰しない。」と規定されている。
[34] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[35] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）
[36] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）
[37] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）

ずに実施され、事後通知となることが条文上規定されている。これに関して、同措置は、そもそも緊急の必要があるときに行われるものであることから、事後通知が常態化する懸念が示された。まず、緊急の必要があるときの具体例について内閣官房は、「警察、自衛隊がアクセス・無害化措置を行う要件である緊急の必要があるときとは、いつでもサイバー攻撃が敢行されてもおかしくない状況にあるということである。アクセス・無害化措置の実施の必要性は、個別具体の事案に応じて判断される」とした上で、例えば、サイバー攻撃に用いられるマルウェアに感染したＩｏＴ機器を発見した場合について、「マルウェアはいまだ発動されていないものの、当該マルウェアとＣ２サーバ[38]が定期的に通信を行っていると認められるため、攻撃者の意図次第でいつでもサイバー攻撃が行われると認められる場合、アクセス・無害化措置を行う緊急の必要がある場合と判断して、事前承認を得るいとまがないと認める特段の事由がない限り、あらかじめサイバー通信情報監理委員会の承認を得ることになる。なお、このように事前承認を得ることが原則ではあるが、サイバー攻撃により現に重大な障害が発生している場合など、事前承認を得るいとまがないと認める特段の事由が生じれば、当該承認を得ることなくアクセス・無害化措置を取ることができるということになっており、こうした真に必要な場合には、遅きに失することなく必要な措置を講ずることが可能になると考えている」旨答弁した[39]。

事後通知が常態化するとの懸念に対して石破総理は、「委員会では迅速かつ的確に承認が行われるものと想定しており、事後通知が常態化することはないと考えている」旨答弁し、さらに、委員会の事前承認を得るいとまがないと認める特段の事由については、「例えば、サイバー攻撃により、基幹インフラ事業者に現に重大な障害が発生している状況等が想定される。この場合、アクセス・無害化措置も早急に完了する必要があると考えられることから、制度上、事後承認を得ることとはしていない。もっとも、通知を受けた委員会は、実施された措置が適切かどうかを確認し、必要に応じて勧告することができることとされており、このような手続を設けることにより、権利の濫用の抑止を図り、措置の適正性を十分に確保することができると考えている」旨答弁した[40]。

イ　承認を求める場合等における手続及び承認の単位

実施主体がサイバー通信情報監理委員会の承認を求める際の具体的な方法について問われた平国務大臣は、「委員会への承認の求めについては、サイバー攻撃に利用されているサーバ等であると認めた理由、サイバー攻撃による危害の防止という目的を達成するために取り得るアクセス・無害化措置の内容等を示す疎明資料を委員会に示すこととなる。これらの疎明資料については、政府として入手、利用可能な各種情報として、例え

---

[38] Command and Control Serverの略でＣ＆Ｃサーバとも呼称される。攻撃者の命令に基づいて動作する、マルウェアに感染したコンピュータに指令を送り、制御の中心となるサーバのこと。

[39] 第217回国会衆議院内閣委員会議録第６号15頁（令7.3.19）

[40] 第217回国会衆議院本会議録第９号（令7.3.18）。なお、承認までに要する期間について問われた平国務大臣は、「個別具体の事案により異なることが想定されることから、あらかじめ予断を持って答えることは困難である。いずれにせよ、サイバー攻撃への対処には迅速な対応が求められるところで、施行に向けて、委員会の事務が適切かつ遅滞なく処理される体制が構築されるよう取り組んでいきたい」旨答弁した（第217回国会衆議院内閣委員会議録第７号５頁（令7.3.21））。

ば、当事者協定により取得した通信情報、インシデント報告や協議会を通じて把握した情報、通信情報の利用により取得する情報、サイバー攻撃に関する公開情報、同盟国、同志国との連携により共有された情報を必要に応じて用いつつ、作成していくことが考えられる」旨答弁した[41]。また、事後通知となる場合の手続については、「承認を得るいとまがない場合の事後通知については、事前承認の場合と同様の資料を出す。それに加えて、事前承認を得るいとまがないと認めた特段の事由に関する疎明資料も必要となる」旨答弁した[42]。

次に、承認の単位について平国務大臣は、「当該承認の求めに当たっては、例えば、特定の事業者に対するサイバー攻撃に悪用されており、具体的な危害を生じさせる懸念があるため、アクセス・無害化措置を行う必要のある特定の攻撃サーバ等を示した上で承認を求めることを想定している。なお、委員会に示すこの対処すべき攻撃サーバ等については、一回の承認の求めであっても、必要があれば複数のサーバ等になる場合もあり得ると考えている」とし、さらにより具体的な承認申請の手続については、「個別具体的にサーバを特定する。そのサーバはボットネットだったりするため複数ある可能性はあるが、個別に申請をして承認をもらう仕組みで運用されるものと想定している」とし、「例えば、ボルト・タイフーンのような著名な攻撃者がいて、それに対する防御をひとまとまりで承認してくださいということはない。そういう攻撃者がやってくる攻撃、Aパターン、Bパターンごとに攻撃の仕方が違い、対応方法も違うので、その攻撃パターンごとにサーバを特定して、それに対して承認を取る」旨答弁した[43]。

ウ　サイバー通信情報監理委員会の体制

アクセス・無害化措置の承認は、迅速に行われる必要があるところ、サイバー通信情報監理委員会の体制を24時間体制にするのか問われた。これに対して内閣官房は、「アクセス・無害化措置の承認に係る審査が迅速かつ的確に行われるようにするため、法律や情報通信技術に関して専門的知識等を有する者を委員とするほか、委員会事務局の体制についても適切な専門性を有する職員による必要な規模の体制が確保できるようにする。この点、アクセス・無害化に係る承認に当たり、緊急の場合等において委員会が具体的にどのような形で議決するのか等については今後委員会において決められるものと考えているが、いずれにしても、委員会の重要性に鑑み、対応に遺漏のないように措置されるものと考えている」旨答弁した[44]。また、委員長及び委員の選任について、内閣官房は、「サイバー通信情報監理委員会の委員長と委員は、サイバー対処能力強化法案第50条において、法律あるいはサイバーセキュリティ等のいずれかに関して専門的知識及び経験並びに高い識見を有する者で人格が高潔である者のうちから両議院の同意を得て内閣総理大臣が任命することとされており、これにより適切な人選を行うこととなる。また、委員会の規模については、委員会の任務である審査及び検査には高い専門性と的確な職

41 第217回国会衆議院内閣委員会議録第11号（令7.4.4）
42 第217回国会衆議院内閣委員会議録第11号（令7.4.4）
43 第217回国会衆議院内閣委員会議録第11号（令7.4.4）
44 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

務執行が求められることから、委員会は複数の分野の専門家から構成されることが望ましく、かつ、それらの専門家による慎重な合議が求められること、また、他のいわゆる三条委員会の例も踏まえ、第50条において委員長１人、委員４人と規定している」旨答弁した[45]。

（５）国外のサーバ等に対してアクセス・無害化措置を行う場合における諸課題

ア　外務大臣との協議

警職法第６条の２第３項においては、外務大臣と協議を行うこととされているが、協議内容についての具体的な規定が置かれていない。これについて内閣官房は、「個別に協議の内容については規定していないが、国際法上の適法性の担保のための協議と理解している」とし、将来的に解釈が変更される懸念に対しては、「時間の経過によって解釈が変わることはない」旨答弁した[46]。また、アクセス・無害化措置については、外交上の観点からも検討を行うべきではないかとの指摘に対して、外務省は、「この協議においては、外務大臣は、その措置が国際法上許容される範囲内のものかどうかのみを判断するということとなっている」旨、内閣官房は、「ＮＳＣ四大臣会合において定める総論的な対処方針は、外交的観点を踏まえたものとなる。外務大臣は、この対処方針を審議する四大臣会合に出席し、主に外交政策上の観点から議論に参画するため、同会合における当該決定において外交的観点が十分に考慮される」旨答弁した[47]。

協議に当たって実施主体から提供される情報について、平国務大臣は、「措置の実施主体は、例えば、重大な危害の内容や我が国が取る措置の内容、さらには措置の対象となるサーバ等を具体的に示した上で協議を行う。これを受け、外務省においては評価、判断を行い、協議が調えば、国際法上許容される範囲内で措置を取る」旨答弁した[48]。

また、緊急性が高いことから迅速に協議を行う必要があるとの指摘に対して、内閣官房は、「協議を迅速に行うことは極めて重要であり、平素から内閣官房、警察庁、防衛省及び外務省との間で緊密に連携して、この協議を適切かつ迅速に行うことができるよう取り組んでいく」旨答弁した[49]。

この点、参議院附帯決議では、「十六　外務大臣は、アクセス・無害化措置に関する協議について、迅速かつ適切に対応できる実効性のある体制を構築すること。また、国家安全保障会議四大臣会合等において、アクセス・無害化措置を行う際の外交上の観点からの懸念点を共有するなど適切に関与すること。」とされた。

イ　国際法との関係

アクセス・無害化措置を実施する際の違法性阻却事由としては、緊急状態等を援用することが想定されているが、警職法第６条の２においてはその要件に該当する規定が置かれていない。そうした規定を置くべきとの指摘、また、そうした規定がないことによっ

---

[45] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
[46] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）
[47] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[48] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（令7.4.3）
[49] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

て実施主体による恣意的な運用が行われるとの懸念に対して、平国務大臣は、まず、「アクセス・無害化措置を含むサイバー行動の国際法上の評価については、個別具体的な状況に応じて判断されるため、一概に答えることは困難である。そもそも国際法上禁止されていない合法的な行為に当たる場合や、サーバ所在国の領域主権の侵害に当たり得るとしてもその違法性を阻却できる場合がある。その上で、国外に所在する攻撃サーバ等へのアクセス・無害化措置が仮にサーバ所在国の領域主権の侵害に当たり得るとしても、例えば、国際違法行為に対して一定の条件の下で対抗措置をとること、あるいは国際法上の緊急状態という考え方を援用することはサイバー空間における国際法の適用についても認められていると考えている」とした上で、いわゆるタリン・マニュアル[50]について、「サイバー攻撃に適用される国際法に関する研究の成果として専門家によって作成された文書であると承知している。いずれにせよ、緊急状態を援用する際には、国家責任条文[51]第25条の要件に照らして、個別具体的な状況を踏まえて適切に判断していくこととなる」と国際法との関係について説明し、さらに、「アクセス・無害化措置は、攻撃者が利用しているサーバ等を発見した上で、当該サーバ等を用いていつサイバー攻撃が行われ重大な危害が発生してもおかしくない緊急の必要性がある状態において講じることが想定されていることから、急迫した危険といった国際法上の要件を満たす状況で行われるものと考えている」として、「法案に緊急状態の要件を反映させる必要はないと考えられ、また、措置の実施主体による恣意的な運用となるとの指摘は当たらない」旨答弁した[52]。

この点に関して、参議院内閣委員会の参考人質疑において、早稲田大学法学学術院教授酒井啓亘参考人[53]は、「警職法第６条の２、とりわけ第２項の規定は、必ずしも国際法上の対抗措置、緊急状態の要件を定めたものではない。むしろ、仮に違法行為になりそうな場合の行為であっても、違法性阻却に該当することを妨げないような立て付けの規定だと理解している。元々はこの規定は、国家として行為を行うその国内法上の要件を具備するということと思われ、国際法上の要件として、対抗措置なり、緊急状態が満たされなければならないというのはまた別建てということになる」とし、「新しい警職法第６条の２第２項に基づいて措置をとり、それが相手方から国際法違反だと指摘された場合に、必ずしもこの法案を通じて国内法で議論するのではなくて、あくまでも慣習国際法上の国家責任法のレベルで相手方に対して主張し、説得するということになる。このため緊急状態にせよ対抗措置にせよ、全てあらかじめ国内法に要件を書き込んでおくこ

---

[50] ＮＡＴＯのサイバー防衛協力センターにおいて法律専門家が作成したものであり、サイバー攻撃に関する慣習国際法を包括的に記したものとして、国際社会において一定の権威を有しているとされる。2013（平成25）年にタリン・マニュアル1.0が、2017（平成29）年にタリン・マニュアル2.0がそれぞれまとめられている。

[51] 国家責任に関しては、国連国際法委員会（International Law Commission（ＩＬＣ））において法典化作業が進められ、1980（昭和55）年以降、条文草案の第一読、第二読が行われ、2001（平成13）年に終了した。同年の国連総会決議では、ＩＬＣの法典化作業の結果を評価し、第二読で採択された文書が添付されており、この文書が「国家の国際責任に関する条文」（国家責任条文）と呼ばれている。ただし、この文書を条約化するか否かの再検討作業は、その後の国連総会決議で延期されてきているとされる（中谷和弘ほか『国際法〔第５版〕』（有斐閣、令和６年３月）139～140頁）。

[52] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

[53] 政府の有識者会議の構成員の一人であり、有識者会議でも国際法の見地から意見を述べた。

とはこれまで行われてきておらず、今後も難しいだろうと考えられ、諸外国もその点では同じ考え方を持って立法を行っているのではないか」との旨の見解を述べた。一方、弁護士の齋藤裕参考人は、「警察官がきちんと国際法違反にならない、違法性阻却事由を満たすような行動をするような条文にする、警職法にきちんと要件を書き込むというのは非常に重要」である旨の見解を述べた[54]。

こうした議論を踏まえ、警職法の規定が国際法との関係を念頭に置いているか問われた平国務大臣は、「国際法上許容される範囲内で措置が行われることを確保する観点から、措置の実施主体は、警察庁長官又は防衛大臣を通じてあらかじめ外務大臣と協議することとしており、その意味で国際法との関係を念頭に置いている」旨答弁した[55]。他方、「緊急状態は、あくまで違法性を阻却する必要がある場合に援用する可能性がある法理の一つとして想定しているものであり、今般の措置をとるに当たって常に緊急状態を援用することを想定しているわけではない」、また、「国際法上の違法性阻却に関しては、改正警職法第６条の２の条文の要件のみで判断するものではなく、個別具体の要件ごとに判断すべきものであり、外務大臣との協議により、国際法上許容される範囲内で措置を行うことを確保する」旨の答弁もなされた[56]。

この点、参議院附帯決議では、「十七　外国に所在する攻撃サーバー等へのアクセス・無害化措置が国際法上許容される範囲内で行われることを担保する観点から、緊急状態を援用する際には国家責任条文第二十五条の要件を満たして同措置を行うこと。すなわち、国際法上の評価を行う外務大臣は、緊急状態を援用する場合、同措置が、重大かつ急迫した危険から不可欠の利益を守るための唯一の手段であること、及び他国の不可欠の利益を深刻に侵害しないことを満たしているかについて検討し、同措置の実施主体との協議に反映させること。」とされた。

また、国際法上のルールづくりに我が国も関与する必要性について問われた岩屋毅外務大臣は、「これまでの国連における議論の結果、国連憲章全体を含む既存の国際法がサイバー行動にも適用されることが確認されてきており、我が国も積極的に議論に参画してきた。現在、国連全加盟国が参加可能なサイバーセキュリティに関する議論の場として、国連総会決議に基づいて国連オープンエンド作業部会が設置されている。ここにおいて、これまでの議論の成果を基礎としつつ、サイバー行動に係る国際法を含め、国家の責任あるサイバー行動に関する議論が行われている。外務省としては、引き続き、こうした国際社会における議論に積極的に関与していきたい」旨答弁した[57]。

この点、参議院附帯決議では、「十八　外国に所在する攻撃サーバー等へのアクセス・無害化措置の実施が深刻な外交問題につながる懸念及び我が国の国家実行として国際法規則の形成に影響を与える事項であることに留意し、アクセス・無害化に係る我が国としての国際法上の整理を明確化するとともに、サイバー行動に係る国際法上のルール形

---

54 第217回国会参議院内閣委員会会議録第12号（令7.5.8）
55 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
56 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
57 第217回国会衆議院内閣委員会議録第10号（令7.4.2）

成に我が国として貢献していくこと。」とされた。

（６）事後的な検証の在り方

アクセス・無害化措置の実施においては、原則として事前にサイバー通信情報監理委員会の承認を得る必要があるが、事後的な検証の在り方について問われた。これに対して、警察庁は、「アクセス・無害化措置については、その適正性を確保する観点から事後的な検証を行う場合もあると考えられることから、当該検証に必要となる記録を適切に管理、保存することは重要である。その具体的な内容については、透明性、正当性の担保の点も含め、今後検討していくが、いずれにせよ、公文書管理法[58]その他の関係法令にのっとって適切に管理していく」旨[59]、また、「他の職務執行と同様、アクセス・無害化措置についても、警察の場合は、公安委員会に対して適時的確に所要の報告をするなどして、公安委員会の管理の下、適正に運用していく」旨[60]答弁した。また、防衛省は、「検証の必要性は重々承知している。他方で、その当該検証の具体的な方法がまだ決まっていない、これから検討しないといけないため、現時点では、公文書管理法等の関係法令に基づき、きっちりと記録を保管し、管理していくことが重要と考えている」旨答弁した[61]。

警察における検証について、参議院附帯決議では、「十四　警察におけるアクセス・無害化措置が適正に行われることを担保するため、公安委員会は警察からの報告を適時に受けて厳格な監督を行うとともに、警察は関係する記録を保存し、事後的な検証に努めること。」とされた。

（７）措置により損害が発生した場合の賠償の在り方

アクセス・無害化措置については、対象を誤った場合などに、損害を生じさせる可能性が指摘され、その場合の対応について問われた。これに対して平国務大臣は、アクセス・無害化措置は、必要最小限度の措置として実施されるものであるなどとして、「万が一にでも誤ったアクセス・無害化措置が行われることのないよう、適切に制度を運用していく」とした上で、「仮に我が国が実施したアクセス・無害化措置によって対象サーバ等の管理者等に損失が生じた旨の申出があった場合には、まず、当該損失が本当に我が国のアクセス・無害化措置によって生じたものかという点も含めて、関連の情報を確認することとなる。相手方への説明の在り方については、確認して判明した事実関係等を考慮するなど、その時々の個別具体的な状況に即して対応する必要があるほか、我が国の措置の詳細を明らかにすることは潜在的な攻撃者に対して手の内を明かすことにもつながることも踏まえる必要があるため、一概に答えることは困難である。いずれにしても、万が一我が国が実施し

---

[58] 公文書等の管理に関する法律（平成21年法律第66号）

[59] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

[60] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）。さらに、所要の報告の在り方について坂井国家公安委員会委員長は、「個別具体の事案に応じて、例えば実際に実施したアクセス・無害化措置の内容及びその結果を報告することなどが想定されているが、具体的な報告の在り方については、今般の国会での議論を踏まえ、国家公安委員会の管理の下、的確なものとなるよう警察庁を指導したい」旨答弁した（第217回国会参議院内閣委員会会議録第11号（令7.4.24））。

[61] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

た措置により損失が発生した場合には、政府として、いかなる対応が適切かを判断し、対処することとなる」旨答弁した[62]。

（８）措置に要する施設及び予算

アクセス・無害化措置について、準備室説明資料（**図表２**）においては、警察、自衛隊が緊密に連携するため同一の建物で勤務するとされている。この具体的な説明を求められた平国務大臣は、「施設や設備の概要や、その予算規模については現時点で具体的に定まっているわけではないが、関係機関の緊密な連携を確保できる施設等の在り方について検討を深めていく」とし、通信情報を保存、分析する施設の必要性も指摘されているところ、「国会審議で受けた意見は、施設を整備する際には参考にする」旨答弁した[63]。

５．警察によるアクセス・無害化措置についての主な国会論議

（１）これまでの警察の取組及び能動的サイバー防御２法案により期待される効果

警察におけるサイバー空間の脅威への対処の取組について問われ、坂井国家公安委員会委員長は、「警察においては、これまでも国内外からのサイバー攻撃の脅威に対して捜査や外国治安情報機関等との情報共有等を通じた攻撃インフラの把握、攻撃者を公表し、非難することでサイバー攻撃を抑止するパブリックアトリビューション等の取組を積極的に行ってきた」[64]とした一方、課題として、「機微情報の窃取、重要インフラの機能停止等を目的とする高度なサイバー攻撃に対する懸念が急速に高まっているところであり、国家を背景とした形での重大なサイバー攻撃も日常的に行われるなど、サイバー空間をめぐる脅威は極めて深刻な情勢が続いている。こうした情勢に鑑みれば、サイバー対応能力の向上は喫緊の課題であり、今回の立法措置により、既に欧米主要国で取組が進められている官民連携の強化、通信情報の利用、アクセス・無害化措置の権限付与などを通じ、サイバー攻撃に関連する情報収集・分析能力や重大なサイバー攻撃への対処能力の大幅な強化が可能となるものと考えている」旨答弁した[65]。

（２）警察官職務執行法にアクセス・無害化措置関連規定を盛り込むことの妥当性

アクセス・無害化措置に関する規定が、現場の警察官による危害防止のための手段を定める警職法にそぐわないのではないかとの懸念が示され、これに対して警察庁は、「アクセス・無害化措置は、重大なサイバー攻撃により発生するおそれのある人の生命、身体又は財産に対する危害の防止を目的として行われるものであり、これは個人の生命、身体及び

---

62 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
63 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
64 具体的な取組として、「令和６年８月、サイバー特別捜査部が国際共同捜査に参画する中で、外国捜査機関から提供を受けた情報を精査した結果、ＤＤｏＳ攻撃のためのウェブサービスを利用した国内被疑者を特定し、検挙した。また、令和６年12月、サイバー特別捜査部及び警視庁による捜査、分析の結果を総合的に評価し、北朝鮮を背景とするサイバー攻撃グループが我が国の暗号資産関連事業者からこの暗号資産を窃取したことを特定し、米国連邦捜査局（ＦＢＩ）等と共同でパブリックアトリビューションを実施するなどしている」との事例を挙げた（第217回国会参議院内閣委員会会議録第11号（令7.4.24））。
65 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

財産を保護し、その他公共の安全と秩序の維持に当たることを責務とする警察がその職務として実施すべきものであると考えられる。一たび重大なサイバー攻撃が発生すれば、国家国民に多大な損害を与えることに鑑みれば、アクセス・無害化措置は、サイバー攻撃の現実的、具体的な危険性や緊急性が認められる場合に即時強制として行うべきものと考えられる。警職法は、警察の責務を達成するために必要な手段を定めるもの、警察目的実現のための即時強制の定めをすることを主たる目的とするものと認識している。整備法案において、アクセス・無害化措置を実施するための所要の規定を整備することとしたものである」旨答弁した[66]。

この点、警職法第６条の「立入」が、危険な事態が発生し危害が切迫した場合に関する規定[67]であるのに対して、新設される第６条の２ではそうした要件が置かれていない理由について問われた。警察庁は、「第６条は現実空間を前提とした条文であるのに対して、改正後の警職法第６条の２は被害の瞬時拡散性などの特徴を持つサイバー空間を前提とした条文であり、サイバー攻撃をそのまま放置すれば重大な危害が発生するおそれがあるため緊急の必要がある場合に関する規定である。両者は適用される場面が根本的に異なるものであり、単純な用語の違いだけをもって両者の要件を比較して論じることは適当ではない」旨答弁した[68]。

（３）アクセス・無害化措置と犯罪捜査との関係

アクセス・無害化措置を講ずる過程で犯罪行為を認知した場合の対応について問われた警察庁は、「アクセス・無害化措置を講じる過程で把握した情報について、犯罪捜査に活用することは想定していない。その上で、アクセス・無害化措置とは別に、一般論として、サイバー攻撃の被害申告を受けるなどして犯罪があると思料するときは、刑事訴訟法（昭和23年法律第131号）に規定されているとおり、犯人及び証拠を捜査することとなると考えている」旨答弁した[69]。

（４）警察における人材確保策

アクセス・無害化措置を実施するためには、警察において人材を確保・育成する必要がある。まず、サイバー危害防止措置執行官の確保策について坂井国家公安委員会委員長は、「警察においてはこれまでも、都道府県警察を含めて全国で約3,400人のサイバー人材が

---

[66] 第217回国会衆議院内閣委員会議録第11号（令7.4.4）

[67] なお、同条と憲法第35条の令状主義との関係について警察庁は、「憲法第35条は、直接には刑事手続に関して行われる住居への立入り等を規制するものと承知している。他方、その他の行政手続についても、その性質や目的、強制の態様、目的と手段の均衡や合理性の有無等によっては令状主義の保障が及ぶことがあると解されているものと承知している。この点、警職法第６条第１項に基づく立入りは、危険な事態が発生した場合に専ら人の生命、身体又は財産を保護することを目的に行うものであって、刑事責任追及のための資料の獲得に直接結び付く作用を一般的に有するものではない。また、緊急やむを得ないと認める場合に合理的に必要と判断される限度で行うものである。こうしたことから、令状によることを要しないこととしても、憲法の趣旨に反するものではないと解されていると承知している」旨答弁した（第217回国会参議院内閣委員会会議録第13号（令7.5.13））。

[68] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

[69] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

サイバー部門において専従し、高度な知見と経験を積み重ねている。その中から、情報技術やサイバーセキュリティに関する高度な専門的知識、能力を有しているかなどの観点を総合的に勘案して、適切な警察官をサイバー危害防止措置執行官に指名し、この措置を実施する体制を整備していきたい。より詳細な基準や指名の人数といった詳細については今後具体的に検討を進めていくことであるが、いずれにせよ、法律の施行までには体制を整備するよう警察を指導していきたい」旨答弁した[70]。また、効率的な人材の活用については、「全ての都道府県警察においてサイバー事案への対処に特化した所属を設置しており、全国の約3,400人のうち約2,400人が都道府県警察で専従しているという状況で、こういった高度な人材を集中的に従事させる取組、効率的な人材の活用について既に進めている。さらに、警察庁においては、サイバー警察局及びサイバー特別捜査部が設置されており、全国からサイバー分野に長けた人材を集めている。引き続き、効率的な人材活用の具体的な在り方について、都道府県警察におけるサイバー危害防止措置執行官の配置も含めて検討するよう警察庁を指導していきたい」旨答弁した[71]。

６．おわりに

本稿を含め、３回にわたって能動的サイバー防御２法案の内容及び国会論議について整理を行ってきた。両法律案の一部の規定は、令和７年７月１日から施行され、内閣官房に内閣サイバー官が置かれ、国家サイバー統括室が発足するとともに、サイバーセキュリティ戦略本部について、内閣総理大臣を本部長とし、全ての国務大臣を構成員とする会議に改組された。同日、同戦略本部の初会合が開催され、サイバー対処能力強化法に基づく基本方針を年内に策定することとされるなど、制度運用に向けた検討が開始されている。

今後、各規定が順次施行されていくが、国会審議で示された懸念を払拭できるような準備が求められる。特に、通信情報の利用、アクセス・無害化措置の両制度については、憲法違反となる懸念が再三指摘されており、運用に細心の注意が求められ、システム整備や職員の能力向上等、政府全体の実施体制を強化し万全を期す必要がある。他方、サイバー安全保障をめぐる状況を踏まえると、各規定の施行を急ぐ必要もある。特に、１年６月以内に施行されるアクセス・無害化措置を実施するには、攻撃者を特定するための情報が必要となることから、２年６月以内に施行される通信情報の利用について、可能な限り早急に実施することが求められよう。

衆議院では、修正によってインシデント報告や通信情報の利用等についての検討規定が設けられ、参議院における審議においても、運用の在り方をめぐる議論が多くなされた。こうした点も念頭に置き、今後も、制度の実施状況やサイバー安全保障をめぐる状況を踏まえた不断の見直しが求められる。

（えのもと　なおゆき）

---

[70] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[71] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）