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の導入 －サイバー対処能力強化法案及び整備法案の概要と主な論点－
著者 / 所属	柿沼　重志 / 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	474 号
刊行日	2025-4-14
頁	3-26
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20250414.html

※ 本文中の意見にわたる部分は、執筆者個人の見解です。

※ 本稿を転載する場合には、事前に参議院事務局企画調整室までご連絡ください（TEL　03-3581-3111（内線 75020）／ 03-5521-7686（直通））。

能動的サイバー防御の導入

― サイバー対処能力強化法案及び整備法案の概要と主な論点―

柿沼　重志
（内閣委員会調査室）

１．サイバー対処能力強化のための２法案の国会提出[1]

令和４年12月16日に国家安全保障会議が決定し、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。そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御実施のための体制を整備する」とされ、以下の３つの柱を含む必要な措置の実現に向け検討を進めるとされた。

その後、令和６年６月６日に「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」の開催が決定され、同有識者会議は、全体会合に加えて、官民連携に関するテー

[1] 以下、本稿は、令和７年３月28日時点までの情報に基づき、執筆している。

マ別会合、通信情報の利用に関するテーマ別会合、そして、アクセス・無害化措置に関するテーマ別会合を開催するなどして議論を進めた。

また、同年７月10日には、サイバーセキュリティ戦略本部[2]から政府のサイバーセキュリティに関する年次計画・年次報告である「サイバーセキュリティ2024」が公表され、国家を背景とした攻撃の拡大、未知の脆弱性を悪用したゼロデイ攻撃[3]の増大等、サイバー攻撃の洗練化・巧妙化が一層進展していること等が指摘された。

そして、有識者会議は、同年８月７日に「これまでの議論の整理」を公表、その後、同年11月29日に、「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」（以下「有識者会議提言」という。）を公表している。

有識者会議提言を踏まえ、令和７年２月７日に「重要電子計算機[4]に対する不正な行為による被害の防止に関する法律案（以下「サイバー対処能力強化法案」という。）」（閣法第４号）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（以下「整備法案」という。）」（閣法第５号）が閣議決定され、同日、第217回国会（令和７年常会）に提出された。

２．サイバー対処能力強化法案及び整備法案の全体像

サイバー対処能力強化法案は官民連携の強化と通信情報の利用を規定した新法であり、本則は第１章から第12章までで構成される。一方、整備法案は「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。）や「自衛隊法」（昭和29年法律第165号）等の15の現行法の改正案を束ねており、アクセス・無害化措置とサイバー防御を担う組織や体制の整備を規定している（図表１）。

図表１　サイバー対処能力強化法案及び整備法案の全体像

<table>
<tr><td rowspan="3">サイバー対処能力強化法案</td><td>Ⅰ官民連携の強化
・基幹インフラ事業者（注）に対する一定の電子計算機の届出義務、インシデント報告義務（第２章）
・情報共有・対策のための協議会の設置（第９章：第45条）
・脆弱性対応の強化（第42条）</td></tr>
<tr><td>Ⅱ通信情報の利用
・基幹インフラ事業者等との協定（同意）に基づく通信情報の取得（第３章）
・（同意によらない）通信情報の取得（第４章、第６章）
・自動的な方法による機械的情報の選別の実施（第５章、第７章）
・関係行政機関の分析への協力（第27条）
・取得した通信情報の厳格な取扱い（第23条）
・サイバー通信情報監理委員会による事前審査・継続的検査等（第10章）</td></tr>
<tr><td>（ⅠとⅡによる）
・分析情報・脆弱性情報の提供等（第８章）</td></tr>
<tr><td></td><td>Ⅲアクセス・無害化措置</td></tr>
</table>

[2] 「サイバーセキュリティ基本法」（平成 26 年法律第 104 号）に基づくサイバーセキュリティ政策の司令塔となる組織であり、現行法では本部長は内閣官房長官。
[3] ソフトウェア等のメーカーが確認できていない脆弱性によるサイバー攻撃。
[4] 国の行政機関、基幹インフラ事業者及び重要情報を保有する事業者等が使用するコンピュータを指す。

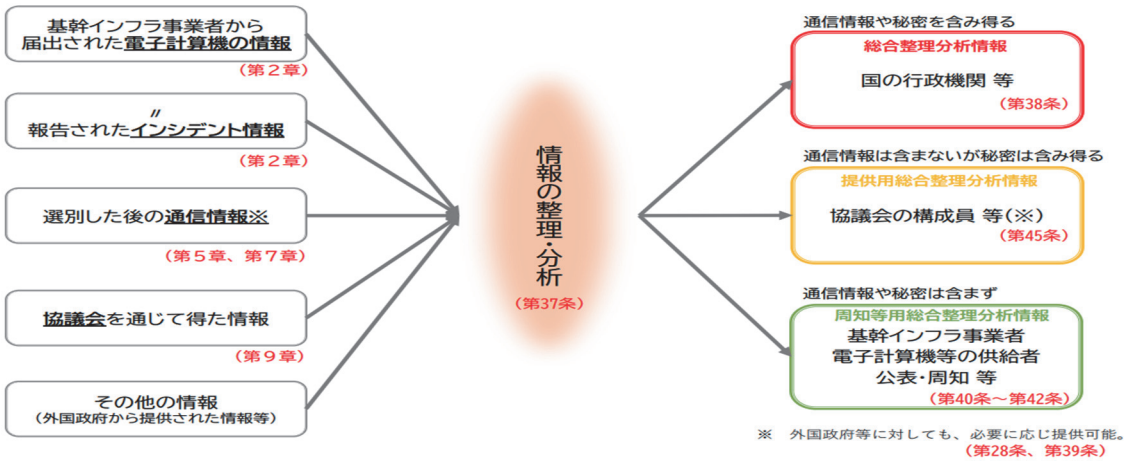
整備法案	・重大な危害を防止するための警察による措置 ・サイバー通信情報監理委員会の事前承認、警察庁長官の指揮　等 （以上、警職法改正） ・内閣総理大臣の命令による自衛隊の通信防護措置 ・自衛隊、日本に所在する米軍が使用するコンピュータ等の警護　等 （以上、自衛隊法改正）
	Ⅳ組織・体制整備等 ・サイバーセキュリティ戦略本部の改組、機能強化　等 （以上、サイバーセキュリティ基本法改正） ・内閣サイバー官の新設（内閣法改正）

（注）基幹インフラ事業者とは、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」（令和４年法律第43号）（以下「経済安全保障推進法」という。）に規定される特定社会基盤事業者のこと。令和６年５月17日、港湾運送を基幹インフラの対象事業とする改正経済安全保障推進法が公布され、基幹インフラ事業者の対象事業は、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、港湾運送、航空、空港、電気通信、放送、郵便、金融、クレジットカード）の15分野となっている（同改正法は令和７年４月１日から施行）。

（出所）内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」６頁を基に作成

なお、サイバー対処能力強化法案に基づき、集められた各種の情報（基幹インフラ事業者から報告されたインシデント情報、選別した後の通信情報等）は、内閣総理大臣によって、整理・分析が行われた後、①総合整理分析情報（通信情報や秘密を含み得る）、②提供用総合整理分析情報（通信情報は含まないが秘密は含み得る）、③周知等用総合整理分析情報（通信情報や秘密は含まない）の３つに大別され、国の行政機関、電気通信事業者[5]、協議会（**本稿３．（１）イを参照**）の構成員、外国の政府や国際機関等、基幹インフラ事業者及び電子計算機等の供給者等に提供される（図表２）。

図表２　政府によって整理・分析される情報と同情報の提供



（出所）内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」14頁

[5] 総合整理分析情報の提供を受けた総務大臣は、所定の場合に、電気通信事業者に総合整理分析情報を提供することができる旨が規定されている（サイバー対処能力強化法案第 38 条第４項）。

３．サイバー対処能力強化法案及び整備法案の概要

（１）官民連携の強化

有識者会議提言では、「官のみ・民のみでのサイバーセキュリティを確保することは極めて困難である。すなわち、サイバー攻撃による業務継続性への影響を減じ、社会全体の強靭性を高め、もって国民の生命、身体及び財産の安全を確保するためには、政府機関、重要インフラ事業者、製品ベンダその他サプライチェーンに関与する全ての者が連携してサイバーセキュリティの確保に努めていくことが必要であると言える」とされた。さらに、同提言では、欧米主要国では、情報提供が政府の役割として明確に位置付けられているところであるが、我が国においても、いわゆる「平時・有事」の区別なく、状況に応じて、政府が率先して情報提供し、官民双方向の状況提供を促進すべきことのほか、脆弱性情報の提供やサポート期限の明示など、製品ベンダ等が、利用者に対し適切にリスクコミュニケーションを行うべき旨を法的責務として規定すべきであること等が指摘されている。

それらを踏まえ、有識者会議提言では、情報共有を行う場合には、攻撃の目的や背景に関する情報などのうち、特に漏えいにより我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティ・クリアランス制度[6]を活用する等、適切な情報管理と情報共有を両立する仕組みを構築すべきである旨が示された。

ア　基幹インフラ事業者によるインシデント報告等

基幹インフラ事業者[7]は、重要電子計算機を導入したときは、その製品名及び製造者名その他の主務省令で定める事項を事業所管大臣に届け出なければならない（サイバー対処能力強化法案第４条第１項）。事業所管大臣は、同届出を受けたときは、当該届出に係る事項を内閣総理大臣に通知するものとする（サイバー対処能力強化法案第４条第２項）。

基幹インフラ事業者は、不正アクセス行為等により重要電子計算機のサイバーセキュリティが害されたこと又はその原因となり得る一定の事象を認知したときは、主務省令で定めるところにより、事業所管大臣及び内閣総理大臣に報告しなければならない（サイバー対処能力強化法案第５条）。

イ　情報共有・対策のための協議会の設置

内閣総理大臣は、特定不正行為による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を設けた上で被害防止に資する情報を共有するとともに、必要な資料提出、意見の開陳、説明その他の協力を求めることができる（サイバー対処能力強化法案第45条）。この協議会はサイバーセキュリティ協議会[8]を廃止し、強化・新設されるものである。

---

[6] 第213回国会（令和６年常会）において、いわゆる経済安全保障分野におけるセキュリティ・クリアランス制度を構築するための「重要経済安保情報の保護及び活用に関する法律」（令和６年法律第27号）が成立し、令和６年５月17日に公布された（同法は令和７年５月16日施行予定）。

[7] 条文上は、経済安全保障推進法上の特定社会基盤事業者のうち重要電子計算機（サイバーセキュリティが害された場合に、重要設備の機能が停止し、又は低下するおそれがある一定の電子計算機）を使用するものを特別社会基盤事業者という（サイバー対処能力強化法案第２条第３項）。

[8] 平成30年12月のサイバーセキュリティ基本法の改正により、翌平成31年４月に創設された。サイバーセキュリティ協議会は脅威情報等に係る官民、業界といった従来の枠を越えたオールジャパンによる情報共有・分析等を行うこととされ、その構成員は令和６年６月13日時点で322者となっている。また、構成員には法

なお、特定不正行為とは、①「刑法」（明治40年法律第45条）第168条の２第２項の罪に当たる行為、すなわち、マルウェア[9]を他人のコンピュータにメール等で送信して実行可能にする等の供用罪に当たる行為、②「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）に規定する不正アクセス行為[10]、③電子計算機を用いて行われる業務に係る刑法第２編第35章の罪に当たる行為であって、当該電子計算機のサイバーセキュリティを害することによって行われるもの、すなわち、刑法上の業務妨害行為（大量のデータを送り、機能不全に陥らせるＤＤｏＳ攻撃等）のいずれかに該当する行為をいうものとすると定義される（サイバー対処能力強化法案第２条第４項）。

ウ　電子計算機の使用者に対する情報共有

内閣総理大臣は、重要電子計算機に対する特定不正行為による被害の防止のため必要があると認めるときは、電子計算機を使用する者等に対して周知等用総合整理分析情報を提供し、又はこれを公表その他の方法により周知することができる（サイバー対処能力強化法案第41条）。

エ　脆弱性対応の強化

内閣総理大臣又は重要電子計算機やそれに組み込まれるプログラムの供給を行う事業の所管大臣（経済産業大臣等）は、総合整理分析情報その他の情報により電子計算機等における脆弱性を認知したときは、必要に応じ、電子計算機等のベンダ等に対して当該脆弱性に関する情報を提供するとともに、当該情報又は当該脆弱性への対応方法について、公表その他の方法により周知することができる（サイバー対処能力強化法案第42条第１項）。

また、電子計算機等を供給する事業を所管する大臣は、基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機又は当該電子計算機に組み込まれるプログラムにおける脆弱性を認知した場合には、当該電子計算機等の供給者[11]に対し、特定不正行為による被害を防止するために必要な措置を講ずるよう要請することができる（サイバー対処能力強化法案第42条第２項）。

（２）通信情報の利用

通信の秘密に関しては、憲法第21条第２項において、「通信の秘密は、これを侵してはならない」とされ、「電気通信事業法」（昭和59年法律第86号）第４条においても、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない」と規定されている。

通信の秘密と憲法の規定との関係について、令和６年２月５日の衆議院予算委員会で、内閣法制局長官からは「通信の秘密はいわゆる自由権的、自然権的権利に属するものであるということから最大限に尊重されなければならない。その上で、通信の秘密についても、憲法第12条、第13条の規定からして、公共の福祉の観点から必要やむを得ない限度におい

律に基づく守秘義務が課せられている。

[9] 悪意のあるソフトウェア（Malicious Software）の略表記。

[10] 不正アクセス行為とは、他人のＩＤ・パスワードを悪用したり、システムの不備を衝くことにより、本来アクセス権限のないコンピュータを利用する行為のことである。

[11] 電子計算機等の生産者、輸入者、販売者及び提供者を意味している。

て一定の制約に服すべき場合があると考えている」旨の答弁があった[12]こと等も踏まえ、有識者会議では、①どのような範囲・方式の通信情報の利用が特に必要と考えられるか、②通信の秘密との関係について、どのような論理構成、考慮要素により憲法との適合性を検討すべきと考えられるかについて議論が行われた。また、有識者会議のテーマ別会合では、主要国においては、一定の条件の下、安全保障上の必要性等がある場合に、政府による通信情報の利用を許容する法律が整備されていることが示された（図表３）。

図表３　海外主要国における政府による通信情報の利用を許容する法律の例

	英国	ドイツ	米国	豪州
主な対象通信	海外関連通信（英諸島外の個人による送受信される通信）	外国の電気通信	国外所在の非米国人（の通信）	外国の通信（国外で送受信される通信）
通信情報の取得要件	・安全保障上の必要性又は重大犯罪の検知等の必要性（取得目的のリストは首相がレビュー）	・安全保障上の必要性 ・重大な危険分野（マルウェアによる国際的犯罪・テロ・国家攻撃、重要インフラに対する脅威等）に関する情報の入手のために必要	外国インテリジェンス情報（外国勢力等の活動・安保関連情報）の収集のために必要	・安全保障上の必要性 ・外国インテリジェンス情報（外国組織等の能力・意図・活動に関する情報）の収集のために必要
取得した情報を分析できる範囲	・必要性・比例性のある分析に限定 ・国内通信内容の分析を原則禁止	・私生活の中核的領域の分析を禁止 ・自国民等の個人データの分析を原則禁止	・米国人関連情報の分析は必要最小限	・国内通信記録は原則廃棄
その他利用制限	・閲覧・複製・開示は最小限	・外部提供可能な場合を法令上限定	・裁判での証拠としての利用を原則禁止	・裁判での証拠としての利用を原則禁止
独立機関の監督	あり	あり	あり	あり
法令名	調査権限法	連邦情報庁法	外国情報監視法	電気通信（傍受及びアクセス）法

（出所）内閣官房サイバー安全保障体制整備準備室「有識者会議通信情報の利用に関するテーマ別会合第１回事務局資料」９頁

また、同テーマ別会合では、通信の秘密の侵害に当たらない場合（電気通信事業法の解釈）として、通信当事者の有効な同意がある場合、違法性阻却事由（法令行為に該当する場合、正当業務行為に該当する場合及び正当防衛、緊急避難に該当する場合）がある場合の２つの場合が示された。

そして、有識者会議提言では、「外外通信（図表４の赤色で示された通信[13]）」「外内通信（図表４の黄色で示された通信）」「内外通信（図表４の青色で示された通信）」について分析が必要であること[14]、個人のコミュニケーションの本質的内容に関わる情報は、特に分析

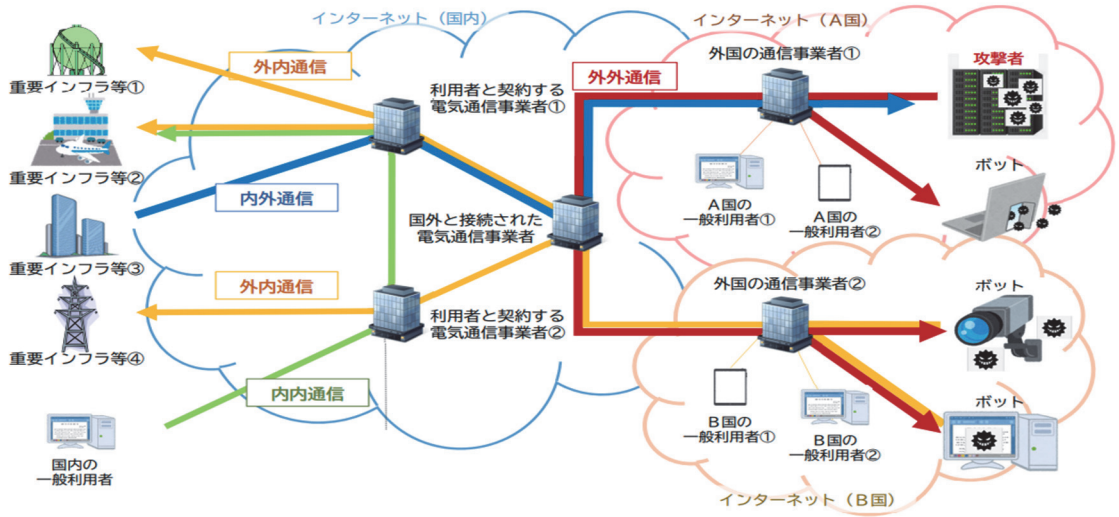
[12] 第 213 回国会衆議院予算委員会議録第３号 12 頁（令 6.2.5）

[13] アイ・ピー・アドレス等から判断して国外設備を送信元及び送信先とする電気通信であって、国内設備を媒介するものである。

[14] これに関連して、政府参考人からは「サイバー攻撃関連通信の 99.4%は国外からというデータもあり、サイバー攻撃が国外に所在する攻撃用のインフラから行われることが多いことを踏まえると、国内のみで閉じた通信の分析を行う必要は、現時点では必ずしもないと考えている」旨の答弁があった（第 217 回国会衆議院内閣委員会議録第６号（令 7.3.19））。また、自国領域を通る国際通信の取得と利用について、石破茂内閣総理大臣からは「国際法上、一般的に禁止されてはいないと承知している。現に、欧米各国による国際通信の安全保障目的での取得と利用も、国際法上、問題ないものとして国際的に受け入れられている」旨の答弁があった（第 217 回国会衆議院本会議録第９号（令 7.3.18））。

する必要があるとまでは言えないなどとされた。また、通信の秘密との関係では、コミュニケーションの本質的な内容には当たらない通信情報も、憲法上の通信の秘密として適切に保護されなければならないとされた。

図表４　国外が関係する通信、関係しない通信の概念図



（出所）内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」28頁

ア　当事者協定（同意）に基づく通信情報の取得

内閣総理大臣は、基幹インフラ事業者との間で、内閣総理大臣が、当該事業者を通信の当事者とする通信情報の提供を受けた上で、当該通信情報のうち外内通信情報に該当するものを用いて、当該基幹インフラ事業者が使用する重要電子計算機その他の電子計算機のサイバーセキュリティの確保を図るために必要な分析を行い、その分析の結果及びこれに関連する情報を当該基幹インフラ事業者に提供することを内容とする協定を締結することができる（サイバー対処能力強化法案第11条第１項）。

内閣総理大臣及び基幹インフラ事業者は、当該協定を締結することについて協議を求めることができるものとし、当該求めを受けた内閣総理大臣又は基幹インフラ事業者は、正当な理由がない限り、当該求めに係る協議に応じなければならない（サイバー対処能力強化法案第11条第２項）。

また、内閣総理大臣は、電気通信サービスの利用者との間で協定を締結することができる旨が定められている。

内閣総理大臣は、当事者協定に基づき通信情報の提供を受ける方法として、協定当事者に係る当事者管理通信情報[15]を複製したものの提供を受ける方法をとることが困難な場合であって、媒介中通信情報[16]が複製され、送信されるようにする方法をとることにつ

15　通信の当事者の設備に送信された情報やそのログのうち当事者が管理している情報。
16　電気通信事業者が管理している情報。

いて当該協定当事者が同意したときは、当該協定当事者に事業電気通信役務を提供する電気通信業者に対して、当事者協定を締結することについて協議を求めることができる。この場合において、当該求めを受けた電気通信事業者は、正当な理由がない限り、当該求めに係る協議に応じなければならない（サイバー対処能力強化法案第13条）。

そして、内閣総理大臣は、その締結した当事者協定の求めるところに従い、通信情報の提供を受けることができる（サイバー対処能力強化法案第15条）。

提供を受けた後の措置としては、自動選別によって外内通信により送受信が行われたもののみが選別される（サイバー対処能力強化法案第22条）。内閣総理大臣は、選別後当事者通信情報を用いて、サイバーセキュリティ確保に資する情報を得るための分析を行った上で、協定当事者に提供するものとする（サイバー対処能力強化法案第16条第１項）。

イ　同意によらない通信情報の取得（外外通信の分析のための通信情報の取得）

内閣総理大臣は、外外通信であり、重要電子計算機に対する国外通信特定不正行為[17]のうちその実行のために用いられる電子計算機、当該電子計算機に動作をさせるために用いられる指令情報等の実態が明らかではないために重要電子計算機の被害を防止することが著しく困難であり、かつ、他の方法ではその実態の把握が著しく困難である国外通信特定不正行為に関係するものが、特定の国外関係電気通信設備を用いて提供される事業電気通信役務が媒介する国外関係通信に含まれると疑うに足りる場合において、必要と認めるときは、「外外通信選別条件設定基準」を定め、サイバー通信情報監理委員会（**本稿３．（４）を参照**）の承認を受けて、当該国外関係通信により送受信が行われる媒介中通信情報の一部（当該国外関係電気通信設備の伝送容量の100分の30を上限とする。）が複製され、内閣総理大臣の設置する設備に送信されるようにするための措置（外外通信目的送信措置）を講ずることができる（サイバー対処能力強化法案第17条第１項）。

なお、外外通信目的送信措置を講ずることができる期間は、６月とするが、同監理委員会が前述の承認をする場合の条件として６月未満の期間を定めたときは、その期間とされている（サイバー対処能力強化法案第17条第３項）。

ウ　同意によらない通信情報の取得（外内通信又は内外通信の分析のための通信情報の取得）

内閣総理大臣は、外内通信又は内外通信であり、国外通信特定不正行為に用いられていると疑うに足りる状況のある特定の外国設備と送受信し、又は当該状況のある機械的情報が含まれているものの分析をしなければ被害防止が著しく困難であり、他の方法ではこれらの通信の分析が著しく困難である場合には、自動選別の条件を定める基準（「特定外内通信選別条件設定基準」、「特定内外通信選別条件設定基準」[18]）を定め、サイバー通信情報監理委員会の承認を受けて、これらの通信が含まれると疑うに足りる外国関係

---

[17] 国外にある電気通信設備を送信元とする電気通信の送信により行われる特定不正行為をいうものとすると定義付けされている（サイバー対処能力強化法案第２条第７項）。

[18] 選別条件設定基準について、政府参考人からは「同意によらない通信情報の利用の措置の申請ごとに個別にその内容を定めるものであって、公表することは想定していない」旨の答弁があった（第217回国会衆議院内閣委員会議録第７号（令7.3.21））。

通信を伝送する電気通信設備から通信情報が送信されるようにする措置（特定外内通信目的送信措置、特定内外通信目的送信措置）をとることができ、これらの措置を講じることができる期間は３月以内とされている（サイバー対処能力強化法案第32条及び第33条）。

エ　整理・分析すべき情報の選別

有識者会議提言では、「通信情報は、ⅰ）電気通信設備等を識別する情報、ⅱ）コンピュータ等に一定の動作をするよう指令を与える情報、ⅲ）その他機械的な情報、ⅳ）個人のコミュニケーションの本質的内容に関わる情報、に主に分類できるが、このうちⅳ）は重大サイバー攻撃対策のためには特に分析する必要があるとまでは言えない。すなわち、メールの中身を逐一全て見るようなことは、重大サイバー攻撃対策としては適当とは言えない行為である。加えて、収集したデータ全てについて人間の目で判断することは不可能であり、またプライバシー保護等の観点から適切でもない。重大サイバー攻撃対策に必要な情報を取り出すため、機械的にデータを選別するとともに、検索条件等で絞っていくなどの工夫が必要である」とされている。

これを踏まえ、内閣総理大臣は、取得した通信情報について、人による知得を伴わない自動的な方法により、自動選別を行うとされている。また、内閣総理大臣は、自動選別を行い、機械的情報[19]のみに選別した選別後通信情報の中に、特定の個人を識別することができることとなるおそれが大きいと認められる情報（特定記述等）が含まれている場合、非識別化措置を講じなければならない。一方で、内閣総理大臣は、当該選別後通信情報と選別後通信情報以外の情報であって特定記述等を含むものとの照合による分析を行うことが特定被害防止目的[20]の達成のために特に必要があると認めるときは、再識別化措置（特定記述等の復元等）を講ずることができる。そして、再識別化措置を講じた選別後通信情報について、再識別化措置の必要がなくなったときは、直ちに、再び非識別化措置を講じなければならない。また、内閣総理大臣は、選別後通信情報の取扱いの業務を行わせる職員の範囲を定めるほか、取得通信情報の安全管理のために必要かつ適切なものとして内閣府令で定める措置を講じなければならない（サイバー対処能力強化法案第22条、第24条及び第26条第１項）。

内閣総理大臣は、自動選別を行ったときは、速やかに、サイバー通信情報監理委員会に通知し、同監理委員会は、その措置について検査するほか、自動選別が終了したときは、直ちに、当該自動選別により得られた取得通信情報を除き、自動選別の対象となった取得通信情報の全てを消去しなければならない（サイバー対処能力強化法案第30条、第35条及び第63条第１項）。

---

[19] 機械的情報には、①通信履歴に係る情報（アイ・ピー・アドレス等）、②指令情報（いわゆるコマンド）、③内閣府令で定める情報があり、③については、「電子計算機の動作の状況を示すために当該電子計算機が自動的に作成した情報その他のそれによっては通信の当事者が当該通信により伝達しようとする意思の本質的な内容を理解することができないと認められる情報」との限定が付されている（サイバー対処能力強化法案第２条第８項）。③について、政府参考人からは「個人の携帯電話番号やＬＩＮＥアカウント名も対象になり得る」旨の答弁があった（第217回国会衆議院内閣委員会議録第７号（令7.3.21））。

[20] 重要電子計算機に対する国外通信特定不正行為による被害を防止する目的のことをいう（サイバー対処能力強化法案第23条第２項）。

なお、内閣総理大臣は、選別後通信情報を加工して、協議会の構成員その他の者にこれを提供したとしてもその通信の当事者の通信に係る権利利益の保護に支障を生ずるおそれがないものとして内閣府令で定める基準を満たすもの（「提供用選別後情報」という。）を作成することができる。なお、同内閣府令を定めるときは、あらかじめサイバー通信情報監理委員会に協議しなければならない[21]（サイバー対処能力強化法案第29条及び第76条）。

オ　関係行政機関の分析への協力

内閣総理大臣は、自動選別又は選別後通信情報の分析をするために必要があると認めるときは、防衛大臣その他の関係行政機関の長に対し、必要な協力を要請できることとし、要請を受けた関係行政機関の長は、その所掌事務に支障を生じない限度において、協力を行うものとする（サイバー対処能力強化法案第27条）。

カ　取得した通信情報の利用及び提供の制限

内閣総理大臣は、取得した通信情報について、自動選別を行う場合を除き、自動選別を行う前の取得通信情報を自ら利用し、又は提供してはならない。選別後の通信情報についても、関係行政機関に分析を要請する場合、アクセス・無害化措置を行う行政機関又は外国の政府若しくは国際機関に提供する場合[22]等を除き、提供してはならない（サイバー対処能力強化法案第23条）。

（３）アクセス・無害化措置

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、武力攻撃に至らない状況下を念頭に置いている。その上で、同戦略では、アクセス・無害化については、「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。

さらに、有識者会議提言では、アクセス・無害化措置の権限の執行主体については、現に組織統制、教育制度等を備え、サイバー脅威への対処に関する権限執行や武力攻撃事態等への備えを行っている、警察や防衛省・自衛隊とし、その保有する能力・機能を十全に活用すべきであるとされた。また、同提言では、アクセス・無害化の対象については、社会全体の機能維持（レジリエンス）と安全保障能力の基盤確保という安全保障上の必要性を念頭に、国の安全や国民の生命・身体・財産に深く関わる国、重要インフラのほか、事態発生時に自衛隊や在日米軍の活動が依存するインフラ等に対するサイバー攻撃を重点とすべきものと考えられるとされた。

---

[21] 内閣府令について、平将明国務大臣からは「内閣府令の制定に当たっては、行政手続法の規定に従いパブリックコメントの募集が行われるほか、サイバー通信情報監理委員会との協議も必須としている。よって、政府が内閣府令を恣意的に定めて、分析の範囲をいたずらに拡大することはないと考えている」旨の答弁があった（第217回国会衆議院内閣委員会議録第７号（令7.3.21））。

[22] サイバー対処能力強化法案第28条で規定されている。

警察によるサイバー事案への対処に関しては、従来は、各都道府県警察が捜査権限を執行し、警察庁は必要な指示や調整等を実施していた。しかし、サイバー空間には国境がないことから、外国捜査機関等との連携が不可欠であり、都道府県警察の捜査のみを前提とする仕組みでは、その対処に支障が生じていた。こうした事態を受け、令和４年４月に警察法が改正され、警察庁にサイバー警察局が設置されるとともに、重大サイバー事案[23]における捜査権限の執行を行うサイバー特別捜査隊が設置された。その後、令和６年４月に、同特別捜査隊は、サイバー特別捜査部[24]に昇格している。

また、防衛省・自衛隊による対処としては、令和４年３月、陸海空自衛隊の共同の部隊として、自衛隊サイバー防衛隊（防衛大臣の直轄部隊）が新編され、サイバー攻撃などへの対処等を実施している。また、同年 12 月 16 日に国家安全保障会議が決定し、閣議決定もされた「防衛力整備計画（令和９年度までの計画）」においては、令和６年度末現在で 2,410 人のサイバー専門部隊を約 4,000 人に拡充すること等が盛り込まれた。

なお、米国、英国、カナダ、豪州などの海外主要国においては、アクセス・無害化措置に当たる措置が既に実施されている[25]。

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、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（整備法案第２条（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が措置をとる場面と措置の具体的な内容

サイバー危害防止措置執行官は、①加害関係電気通信[26]等を認めた場合であって、②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に措置をとることができる（整備法案第２条（警職法第６条の２第２項））。なお、サイバー危害防止措置執行官は、処置をとるに際しては関係者の正当な業務を妨害してはならない（整備法案第２条（警職法第６条の２第７項））。

措置の具体的な内容について、石破茂内閣総理大臣からは「まず、攻撃に使用されているサーバ等に対し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等の措置を行うことを想定している」旨の答弁があった[27]。

ウ　外務大臣との協議

---

[23] 重大サイバー事案とは、サイバーセキュリティが害されることその他情報技術を用いた不正な行為により生ずる個人の生命、身体及び財産並びに公共の安全と秩序を害し、又は害するおそれのある事案（サイバー事案）のうち、①国、地方公共団体の機関や重要インフラ等に重大な支障が生じる事案、②対処に高度な技術を要する事案、③海外からのサイバー攻撃集団による攻撃のいずれかに該当するものをいう。

[24] 同特別捜査部の人員規模は約 300 人となっている（警察庁サイバー警察局「令和６年におけるサイバー空間をめぐる脅威の情勢等について」（令 7.3.13）39 頁）。

[25] 内閣官房サイバー安全保障体制整備準備室「有識者会議アクセス・無害化措置に関するテーマ別会合（第１回）事務局資料」９頁等を参照。

[26] 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行為に用いられる電気通信若しくはその疑いがある電気通信。

[27] 第 217 回国会衆議院本会議録第９号（令 7.3.18）

処置の対象たる加害関係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、つまり国外に設置されていると想定される場合には、警察庁の警察官であるサイバー危害防止措置執行官に限り措置をとることができることとし、あらかじめ、警察庁長官を通じて、外務大臣に協議しなければならない（整備法案第２条（警職法第６条の２第３項））。

アクセス・無害化と国際法との関係について、有識者会議提言は、「アクセス・無害化の対象サーバ等が海外に所在した場合において、同措置が当該国に対する主権侵害に当たるか否かは、個別の措置についてどういう影響が生じるかを踏まえた上で、措置の目的、あるいは相手側の対象の性質を加味して個別具体的に判断される必要があり、どのような行為が他国の主権侵害に当たるかをあらかじめ確定しておくことは困難である」としている。さらに、同提言では、「アクセス・無害化の国際法上の評価について一概に述べることは困難であるが、当該措置が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も考えられるほか、他国の主権侵害に当たり得るものである場合であっても、国際法上の違法性が阻却される場合がある。その違法性阻却事由としては、『対抗措置（Countermeasures）[28]』や『緊急状態（Necessity）[29]』が考えられるが、『対抗措置』については、相手国の先行する違法行為の存在や被害の程度との均衡性を証明しなければならないなどの点を踏まえると、実務上、援用する違法性阻却事由としては、『緊急状態』の方が援用しやすい[30]ものと考えられるが、こうした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について検討すべきである」旨が指摘されている[31]。

以上を踏まえ、国外にあるサーバ等にアクセス・無害化措置をとるような場合には、国際法上許容される範囲内で行うことを確保する観点から、警察庁長官を通じた外務大臣との協議が規定されている。

エ　サイバー通信情報監理委員会の承認と承認を得るいとまがない場合の通知

サイバー危害防止措置執行官が、アクセス・無害化措置をとる場合には、あらかじめ、サイバー通信情報監理委員会の承認を得なければならないこととする。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[32]にはこ

---

[28] 国際違法行為により被害を受けた国が、その限りにおいて、当該行為の責任を負う相手国に対して、その行為を中止させ、自国が受けた被害の回復を図る際に、被った被害と均衡する措置を一定の条件の下で措置をとる場合に違法性阻却が認められるという考え方。

[29] 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、当該行為が相手国又は国際共同体の不可欠の利益を深刻に侵害せず、状態の発生に寄与していない場合に違法性阻却が認められるという考え方。なお、国連憲章を始めとした現行の国際規範をサイバー空間に当てはめたらどうなるかを、有識者が条文の形でまとめたものであるタリン・マニュアルの和訳ではNecessityを緊急避難と訳している。

[30] その一方で、緊急避難は、緊急時の一時的な抗弁でしか認められないという限界があり、能動的サイバー防御を正当化する枠組みとして適さないとの指摘もある（黒﨑将広「能動的サイバー防御の国際法枠組み」『国際問題』No.716（令5.12））。

[31] これに関連して、穂坂泰内閣府副大臣からは「我が国におけるアクセス・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の対抗措置をとること、あるいは緊急状態を援用することは、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」旨の答弁があった（第217回国会衆議院内閣委員会議録第６号（令7.3.19））。

[32] 特段の事由について、石破茂内閣総理大臣からは「例えば、サイバー攻撃により、基幹インフラ事業者に現

の限りでないこととし、処置をとったときは速やかに、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。なお、同監理委員会は、その措置が適切に行われたかどうかを確認し、適正な実施を確保するため必要があると認めるときは、勧告するものとする（整備法案第２条（警職法第６条の２第４項、第９項及び第10項））。

オ　警察庁長官等による指揮

サイバー危害防止措置執行官は、措置の実施について、警察庁長官又は警視総監若しくは道府県警察本部長の指揮を受けなければならない（整備法案第２条（警職法第６条の２第11項））。

カ　自衛隊による通信防護措置

内閣総理大臣は、重要電子計算機に対する攻撃であって、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[33]と認められるものが行われた場合において、自衛隊が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。**※国家及び国民の安全を著しく損なう事態が生じるおそれが大きく、自衛隊が有する特別の技術又は情報が不可欠であり、国家公安委員会からの要請又はその同意がある場合**（整備法案第４条（自衛隊法第81条の３第１項及び第２項））。

なお、自衛隊法において、自衛隊は、我が国の平和と独立を守り、国の安全を保つため、我が国を防衛することを主たる任務とし、必要に応じ、公共の秩序の維持に当たるものとするとされている（自衛隊法第３条）。主たる任務とは、自衛隊法第76条に規定される武力攻撃事態における防衛出動等を指す。また、自衛隊法第３条の「必要に応じ、公共の秩序の維持に当たる」という部分が自衛隊の従たる任務となる。

通信防護措置をとるべき旨を命ぜられた部隊等は、警察庁又は都道府県警察と共同して当該通信防護措置を実施するものとする（整備法案第４条（自衛隊法第81条の３第３項））。

内閣総理大臣は、部隊等に通信防護措置をとるべき旨を命ずる場合には、あらかじめ、防衛大臣と国家公安委員会との間で協議をさせた上で、通信防護措置として実施すべき措置に関する事項や通信防護措置の期間、警察庁等と共同して通信防護措置を実施する要領その他の警察庁等との連携に関する事項等を指定しなければならない（整備法案第４条（自衛隊法第81条の３第４項））。

キ　通信防護措置の際の権限

警職法第６条の２第２項から第11項までの規定（サイバー危害防止措置執行官によるアクセス・無害化措置に関する規定）は、自衛隊法81条の３第１項の規定により通信防

に重大な障害が発生している状況等が想定される」旨の答弁があった（第 217 回国会衆議院本会議録第９号（令 7.3.18））。

[33] 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に当たるサイバー攻撃について、本田太郎防衛副大臣からは「国家のリソースを投じることなどによって、最適な攻撃機会を狙って対象システム内に長期にわたり潜伏できる高い組織性や計画性を有し、高度な堅牢性を備えた攻撃インフラを構築し、未知の脆弱性やマルウェアなどの高度な手法を用いるなどの特徴を有していると考えている」旨の答弁があった（第 217 回国会衆議院内閣委員会議録第７号（令 7.3.21））。

護措置をとるべき旨を命ぜられた部隊等の自衛官の職務の執行について準用する[34]。

通信防護措置をとるべき旨を命ぜられた部隊等の自衛官は、

① 通信防護措置の対象となる重要電子計算機に対する加害関係電気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、加害関係電子計算機の管理者その他の関係者に対し、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加害電子計算機の動作に係る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。

② 国外に設置されていると想定される加害関係電子計算機の動作に係る処置をとる場合、あらかじめ、防衛大臣を通じて、外務大臣に協議しなければならない。

③ 処置をとる場合、あらかじめ、防衛大臣を通じて、サイバー通信情報監理委員会の承認を得なければならない。なお、同監理委員会の承認を得るいとまがなく、承認を得ないで処置をとった場合には、速やかに、当該処置について、防衛大臣を通じて同委員会に通知しなければならない。また、同監理委員会は、その通知に係る処置が規定に照らして適切に行われたかどうかを確認し、必要があると認めるときは、防衛大臣に対し、必要な措置をとるべきことを勧告するものとする。

④ 通信防護措置をとった場合、防衛省令で定めるところにより、遅滞なく、その旨を部隊等の長を通じて、当該加害関係電子計算機の管理者に通知するものとする。

⑤ 通信防護措置をとるべき旨を命ぜられた部隊等の自衛官は、措置の実施について、防衛大臣の指揮を受けなければならない。

（以上、整備法案第４条（自衛隊法第91条の３））

ク　自衛隊等電子計算機警護

自衛隊が使用する特定電子計算機と日本に所在する米軍が使用する特定電子計算機[35]をサイバー攻撃から警護する自衛官の警護任務に必要な権限について、警職法第６条の２第２項から第11項までの規定を準用する（整備法案第４条（自衛隊法第95条の４））。

ケ　アクセス・無害化措置に関わる組織等

２法案の条文には必ずしも明示的に表出してこないが、政府の説明資料（図表５）では、①国家安全保障会議（ＮＳＣ）が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を行うこと、②内閣官房が個別のアクセス・無害化措置について、警察・自衛隊の役割分担等を検討・決定すること[36]等が示されている（図表５）。

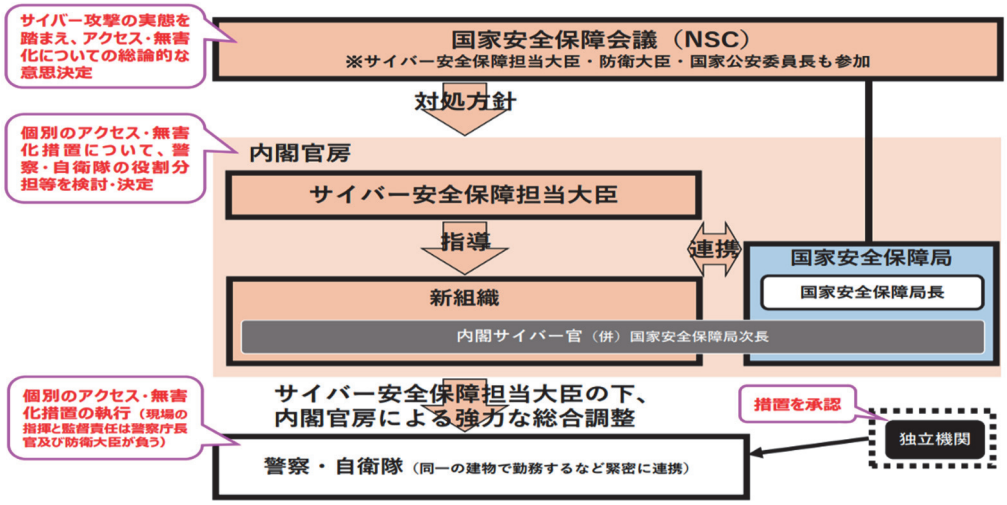
---

[34] これに関連して、石破茂内閣総理大臣からは「自衛隊によるアクセス・無害化措置は、武力攻撃事態に至らない状況下における対処を念頭に、平素の段階から公共の秩序の維持を目的として実施するものである。そのため、自衛権ではなく警察権の行使として、比例原則に基づき、目的を達成するために必要最小限度の措置として行うこととしている」旨の答弁があった（第217回国会衆議院本会議録第９号（令7.3.18））。

[35] 日本に所在する米軍が使用する特定電子計算機の警護について、石破茂内閣総理大臣からは「要請の判断主体は米軍であるが、当該要請に基づく自衛隊の警護の実施に当たっては、国際情勢や米軍の状況等を踏まえ、防衛大臣がその必要性を判断するものであり、アクセス・無害化措置に当たっても、防衛大臣の指揮を受けることになるため、日本が米軍の指揮下に入ることはない」旨の答弁があった（第217回国会衆議院本会議録第９号（令7.3.18））。

[36] 「国家安全保障会議設置法」（昭和61年法律第71号）第２条第１項第11号に、国家安全保障会議は、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につい

図表５　アクセス・無害化措置に関わる組織等



（出所）内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」33頁

（４）サイバー通信情報監理委員会

有識者会議の通信情報の利用に関するテーマ別会合では、通信情報の利用の実施過程の各段階について、先進主要国では、独立機関が監督しており、事前の関与及び開始後の実施状況の監視を組み合わせて統制を図っているものと考えられるが、例外として、豪州は独立機関が事前審査に関与しない方式となっていることが示されている（図表６）。

図表６　先進主要国における通信情報の利用の実施過程と独立機関による監督

主な実施過程及びその内容（おおむね共通するもの）		独立機関による監督				
		英	独	米	仏	豪
準備・承認	○担当大臣による命令の発出 等	事前審査	事前審査	事前審査	意見提出	
通信事業者への措置	○通信事業者に対し、協力義務に基づく通知・指示 ○協力措置に関連する費用の分担 等	監視	監視	申立を受けた場合の審査等	監視	監視
処理・分析	○受領したデータを可能な限り自動化された方法で選別・フィルタリング ○必要性、比例性等を満たす範囲のみで分析を実施 等					
提供・共有等	○処理・分析した情報の開示及び利用の範囲は、必要最小限に制限 ○刑事手続・訴訟における証拠としての利用の制限 等					
保存・廃棄	○データ・情報は、不要になった場合や保存期間の満了後、直ちに破棄 ○消去・廃棄について記録 等					

（出所）内閣官房サイバー安全保障体制整備準備室「有識者会議通信情報の利用に関するテーマ会合（第２回資料）」３頁より一部抜粋

て審議し、必要に応じ、内閣総理大臣に対し、意見を述べる旨が規定されている。また、「内閣法」（昭和 22 年法律第５号）第 16 条第２項第１号には、国家安全保障局は、我が国の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に関する事務をつかさどる旨が規定されており、これらの規定に基づくものと考えられる。

また、有識者会議提言では、独立機関は重要であり、各国の司法制度等との関係や日本の他法での類例を考慮しながら、具体的な組織の在り方が検討されるべきとされた。加えて、国民の理解を得るための方策に関連して、非公開とすべき範囲が一定程度存在する一方で透明性を高めることも同時に行う必要があるとして、「情報の公開が難しい部分を独立機関の監督で補う必要があると考えられ、その意味でも、独立機関の構成や業務の在り方が重要である」とされた。

こうした議論を踏まえ、独立機関として、いわゆる３条機関[37]であるサイバー通信情報監理委員会を置くものとし、同監理委員会は、内閣総理大臣の所轄に属するものとする（サイバー対処能力強化法案第46条第１項及び同条第２項）。

同監理委員会は、重要電子計算機に対する不正な行為による被害の防止のための措置の適正な実施を確保するための審査及び検査を行うことを任務とするものとする（サイバー対処能力強化法案第47条）。

また、同監理委員会の主な所掌事務は以下のとおりである（サイバー対処能力強化法案第48条）（図表７）。

図表７　サイバー通信情報監理委員会の主な所掌事務

・　同意によらない通信情報取得の措置(注)を講じようとするときの承認及び承認の求めに対する審査に関すること。
・　自動選別、非識別化措置又は再識別化措置等が行われたときの検査や継続的な検査に関すること。
・　通信情報保有機関における取得通信情報の取扱いについて違反があった場合の当該通信情報保有機関の長に対する通知、懲戒処分の要求や違反防止のための勧告に関すること。
・　アクセス・無害化措置の承認及び当該承認の求めに対する審査、承認のいとまがない場合の事後の確認及び勧告に関すること。

（注）外外通信目的送信措置、特定外内通信目的送信措置及び特定内外通信目的送信措置

（出所）筆者作成

次に、同監理委員会の組織等については以下のとおりである（サイバー対処能力強化法案第49条、第50条、第51条、第56条、第57条及び第59条）（図表８）。

図表８　サイバー通信情報監理委員会の組織等

・　委員会の委員長及び委員は、独立してその職権を行う。
・　委員会は、委員長及び委員４人をもって組織する。
・　委員のうち２人は、非常勤とすることができる。
・　委員長及び委員は、①裁判官であった者その他の法律に関して専門的知識及び経験並

[37] いわゆる３条機関とは、「国家行政組織法」（昭和 23 年法律第 120 号）第３条又は「内閣府設置法」（平成 11 年法律第 89 号）第 49 条に基づき設置される機関であり、職権行使に高度な独立性が確保されている。サイバー通信情報監理委員会は、サイバー対処能力強化法案に所掌事務等の規定が置かれるとともに、整備法案において、内閣府設置法の一部改正が盛り込まれている。内閣府設置法に根拠のある同種の機関としては、公正取引委員会、国家公安委員会、個人情報保護委員会、カジノ管理委員会がある。

びに高い識見を有する者、②サイバーセキュリティ又は情報通信技術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のいずれかに該当する者であって、人格が高潔であるもののうちから、両議院の同意を得て、内閣総理大臣が任命する。
・　委員長及び委員の任期は、５年とする。
・　委員会に、専門の事項を調査させるため、専門委員を置くことができる。
・　委員会の事務を処理するため、委員会に事務局を置く。
・　委員長、委員、専門委員及び事務局の職員は、職務上知ることのできた秘密を漏らし、又は盗用してはならない。

（出所）筆者作成

そして、同監理委員会は、毎年、国会に対し所掌事務の処理状況を報告するとともに、その概要を公表しなければならない（サイバー対処能力強化法案第61条）[38]。

（５）組織体制整備等

ア　サイバーセキュリティ戦略本部の改組

サイバーセキュリティ戦略本部は、平成27年１月のサイバーセキュリティ基本法の施行に伴い、内閣に設置された。内閣官房長官が本部長、国家公安委員会委員長、総務大臣、経済産業大臣、デジタル大臣、外務大臣、防衛大臣のほか、内閣総理大臣が指定する者（国務大臣のほか有識者も含む）を本部員とするとされている。同戦略本部について、内閣総理大臣を本部長、全ての国務大臣を本部員とする組織に改組するとともに、有識者から構成されるサイバーセキュリティ推進専門家会議を置くこととする（整備法案第12条（サイバーセキュリティ基本法第28条、第30条及び第30条の２））[39]。

イ　サイバーセキュリティ戦略本部の機能強化

サイバーセキュリティ戦略本部の所掌事務として、①基幹インフラ事業者等のサイバーセキュリティ確保に関する国の基準の作成、②国の行政機関、独立行政法人等におけるサイバーセキュリティの確保の状況の評価を追加することとする（整備法案第12条（サイバーセキュリティ基本法第26条））。

ウ　独立行政法人情報処理推進機構（ＩＰＡ）及び国立研究開発法人情報通信研究機構（ＮＩＣＴ）における業務追加における事務の追加

独立行政法人情報処理推進機構（ＩＰＡ）の事務として、①情報の整理分析及びサイバー被害防止に必要な情報の周知等の事務（内閣総理大臣からの委託）、②基幹インフラ事業者等のサイバーセキュリティの確保の状況の調査（サイバーセキュリティ戦略本部からの委託）を追加することとする（サイバー対処能力強化法案第72条第１項及び第２

---

[38] 国会に対する報告について、石破茂内閣総理大臣は「現時点では、例えば、同意によらない通信情報の取得やアクセス・無害化措置に関する承認の申請や承認した件数のほか、勧告についてはその概要等も報告することを想定している」旨の答弁があった（第217回国会衆議院本会議録第９号（令7.3.18））。

[39] 現行のサイバーセキュリティ基本法第30条第２項第８号では、「サイバーセキュリティに関し優れた識見を有する者のうちから、内閣総理大臣が任命する者」を本部員とする旨が規定されており、同規定に基づき、有識者が本部員に任命されている。整備法案ではこれを削除するとともに、第30条の２を新設し、有識者から構成されるサイバーセキュリティ推進専門家会議を置く。

項、整備法案第５条、第６条及び第13条（情報処理の促進に関する法律第51条及びサイバーセキュリティ基本法第31条））。

また、国立研究開発法人情報通信研究機構の業務に、国の行政機関、独立行政法人等の情報システムに対する不正な活動の監視及び分析に係る事務（サイバーセキュリティ戦略本部からの委託）を追加する（整備法案第７条（「国立研究開発法人情報通信研究機構法」（平成11年法律第162号）第14条））。

エ　内閣府における所掌事務の追加等と内閣府特命担当大臣の設置

内閣府の所掌事務にサイバー対処能力強化法案に関する事務（官民連携の強化及び通信情報の利用に関する事務）を追加するとともに、内閣府にサイバー通信情報監理委員会を置くこととする（整備法案第17条（「内閣府設置法」（平成11年法律第89号）第４条及び第64条））。

また、サイバー対処能力強化法案に関する事務を掌理する内閣府特命担当大臣を置くことができることとする（整備法案第17条（内閣府設置法第４条[40]））。

オ　内閣サイバー官の設置

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[41]（特別職）１人を置くこととする（整備法案第１条及び第15条（「国家公務員法」（昭和22年法律第120号）第２条第３項及び内閣法第19条の２））。

（６）主な罰則[42]

ア　官民連携の強化関係

行政機関及び協議会の構成員等による秘密の不正な利用・漏えいを行った者には、２年以下の拘禁刑又は100万円以下の罰金に処する（サイバー対処能力強化法案第82条）。

また、基幹インフラ事業者がインシデント報告等を行わず、是正命令を受けてもなお対応しない場合には、200万円以下の罰金に処する（サイバー対処能力強化法案第83条）。

さらに、基幹インフラ事業者がインシデント報告等に関連し、資料の提出をせず、又は虚偽の報告をし、若しくは虚偽の資料を提出したときは、当該違反行為をした者は、30万円以下の罰金に処する（サイバー対処能力強化法案第84条）。

イ　通信情報の利用関係

通信情報保有機関又はサイバー通信情報監理委員会において取得通信情報の取扱いに関する事務に従事する者による通信情報の不正な利用・漏えいの行為のうち、データベースの提供を行った者については、４年以下の拘禁刑若しくは200万円以下の罰金に処し、

---

[40] なお、同法第９条では、「内閣総理大臣は、内閣の重要政策に関して行政各部の施策の統一を図るために特に必要がある場合においては、内閣府に、内閣総理大臣を助け、命を受けて第４条第１項及び第２項に規定する事務並びにこれに関連する同条第３項に規定する事務（これらの事務のうち大臣委員会等の所掌に属するものを除く。）を掌理する職（以下「特命担当大臣」という。）を置くことができる。」と規定されている。

[41] 内閣サイバー官について、政府参考人からは「時の内閣総理大臣がその任にふさわしい者を多角的、総合的な観点で機動的に登用することができるよう、今般の整備法において国家公務員法を一部改正し、特別職として設置をするものである」旨の答弁があった（第217回国会衆議院内閣委員会議録第６号（令7.3.19））。

[42] 第80条第１項、第83条又は第84条の違反行為をした場合の両罰規定も規定されている（サイバー対処能力強化法案第86条）。

又はこれを併科する（サイバー対処能力強化法案第79条）。データベース以外の提供を行った者については、３年以下の拘禁刑又は100万円以下の罰金に処する（サイバー対処能力強化法案第81条）。

また、通信情報保有機関の管理を侵害する行為により、通信情報を取得した者については、３年以下の拘禁刑又は150万円以下の罰金に処する（サイバー対処能力強化法案第80条第１項）。

（７）施行期日

サイバー対処能力強化法案については、①一部を除き、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、②サイバー通信情報監理委員会の委員長及び委員の任命に係る準備行為等は公布の日から施行、③サイバー通信情報監理委員会の設置等については１年を超えない範囲内において政令で定める日から施行、④通信情報の利用関係等については一部を除き２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と規定されている（サイバー対処能力強化法案附則第１条）。

また、整備法案については、①サイバー対処能力強化法の施行の日から施行、②ただし、サイバーセキュリティ戦略本部の改組等については、公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と規定されている（整備法案附則第１条）。

４．主な論点

サイバー攻撃によるリスクや損失を認識し、国家として、サイバー攻撃に対する対処能力を向上させることは不可避であると考えられ、こうした点に対し、国民の理解も深まりつつある[43]が、法制度の在り方、そして運用面における懸念点、とりわけ、国民からも懸念の声が少なくない通信の秘密との整合性の問題や警察や自衛隊によるアクセス・無害化措置の問題については、国会論議を通じて、議論を深めていく必要があろう[44]。以下では、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本柱に係る論点、そして人材育成等の横断的な課題等について、主な論点を列挙する。

【官民連携の強化に係る論点】

① 基幹インフラ事業者等に対する重要電子計算機の届出の範囲によっては、事務負担が過大になるおそれが生じる。届出範囲については、現実的かつ真に必要な範囲に限定するよう留意する必要があるのではないか。

---

[43] 例えば、令和６年４月に読売新聞社が公表した世論調査では、サイバー攻撃を受けた民間企業などと政府が情報共有することに賛成は89%、攻撃者が使うサーバを把握して被害を防ぐため、通信事業者から情報を受けることに賛成は88%、攻撃元のシステムに侵入し、無力化することに賛成は82%であったとしている（『読売新聞』（令6.4.8））。また、日本経済新聞社とテレビ東京が共同で令和７年１月に行った世論調査では、能動的サイバー防御を導入するための法案に賛成が65%であったとしている（『日本経済新聞』（令7.1.26））。

[44] 例えば、日本弁護士連合会は能動的サイバー防御を導入するための法案について「基幹インフラ等に対するサイバー攻撃への対処能力を高めることを目的としており、本法案が規定する官民連携等については一定評価し得るところである。しかし、通信情報の利用及びアクセス・無害化については、国会における慎重な審議が必要である」旨の会長声明を発出している（日本弁護士連合会「重要電子計算機に対する不正な行為による被害防止に関する法律案（いわゆる「能動的サイバー防御」法案）に関する会長声明」（令7.2.19））。

② インシデント報告は事業者にとっては復旧対応が急がれる中での対応になるため、事務負担をできるだけ軽減すべく、効率化を図る工夫が求められよう[45]。

③ 協議会におけるセキュリティ・クリアランス制度の活用[46]による官民の情報連携の強化や適切な情報管理が重要になってくる。また、同盟国・同志国との情報連携も重要であると考えられるが、それらの国とギブアンドテイクの関係を構築するには、内閣サイバーセキュリティセンターを発展的に改組して設置するとされる国家サイバー統括室（仮称）を始めとした関係部局職員のインテリジェンス能力の向上に着手する必要があろう[47]。

④ 官民連携の強化に関連して、経済同友会からは「政府から民間企業等へ提供する情報については、経営層の意思決定に有用な情報提供を実施すべきである。具体的には、『攻撃者の主体、目的、背景』、『攻撃の緊急度、重要度』、『攻撃の被害想定、波及効果』、『初期対応や中長期の対応』が挙げられる」旨の提言がなされている[48]が、こうした情報について、どのレベルまでの情報であれば、我が国政府が民間企業に提供可能であるのか、真摯な検討が求められよう。

⑤ 今般のサイバー対処能力強化法案の第12条では基幹インフラ事業者以外の事業者との協定が規定されており、同規定に基づき、医療機関が内閣総理大臣と協定を締結することは可能な仕組みとなっている。しかしながら、医療機関を狙ったサイバー攻撃が多発していることに鑑みれば、医療を基幹インフラの対象事業に追加した方が整合的ではないかと考えるが、この点について、検討を加速すべきではないか[49]。

【通信情報の利用に係る論点】

⑥ 政府が分析する通信情報はコミュニケーションの本質的内容ではない情報に限定されることを運用面でも確実に担保すべきであり、その意味でも、独立機関であるサイバー

---

[45] この点について、政府参考人からは「インシデント報告に限らず、個人情報保護委員会に基づく個人データの漏えい等に係る報告、また警察への相談についても事業者からのニーズを踏まえ、順次、様式の統一や報告窓口の一元化をしっかり進めていく」旨の答弁があった（第217回国会衆議院内閣委員会議録第６号（令7.3.19））。

[46] この点について、石破茂内閣総理大臣からは「協議会においては、サイバー攻撃の目的や背景などの一定の機微な情報についても取り扱うことを想定していることから、その構成員の選定に当たっては、重要経済安保情報保護活用法のセキュリティ・クリアランス制度も活用して、適切な情報管理がなされますよう取り組んでいく考えである」旨の答弁があった（第217回国会衆議院本会議録第９号（令7.3.18））。

[47] こうした点に関連して、松原実穂子ＮＴＴチーフ・サイバーセキュリティ・ストラテジストは「日本は米国やクアッドなど同志国の官民関係者と共に、率先して国際的な合同サイバー演習を創設すべきである。日本の重要インフラ企業がセキュリティ・クリアランス保有者を配置するようになれば、こうしたサイバー演習が、機密指定の知見を共有する場にもなり、より幅広くサイバー防衛に役立つであろう」旨を述べている（松原実穂子「サイバーセキュリティとデータセキュリティの日米協力がなぜ両国の経済安全保障に不可欠か」８頁、＜https://spfusa.org/wp-content/uploads/2023/02/NAC-Mihoko-Matsubara-Japanese.pdf＞）。

[48] これに関連して、大澤淳中曽根平和研究所主任研究員は「ＳＳＯ（Special Source Operation、特別資料源作戦）によって行われる通信傍受、メタデータの収集が、米国の能動的サイバー防御における攻撃検知・攻撃者の特定の基盤となっている。今後、日本でも米国と同様の能動的サイバー防御を実施しようとすれば、相当の予算をかけて、デジタル時代のインテリジェンス能力を構築することが求められる」旨を指摘している（大澤淳「日本のインテリジェンスは必要十分か」秋山昌廣、小黒一正編『日本の安全保障』（日本経済新聞出版、令和７年）310頁）。

[49] この点について、手塚悟慶應義塾大学特任教授は「中国やロシアのサイバー攻撃の標的は国民生活に直接影響するものになりつつあり、特に医療機関が狙われている。医療機関も経済安全保障推進法に基づく『基幹インフラ』に位置付けた方がいい」と指摘している（『読売新聞』（令6.5.21））。

通信情報監理委員会がチェック機能を真に果たすことが重要であろう。特に、国民からの懸念の声も聞かれる「通信の秘密と能動的サイバー防御の整合性」について、政府は真摯に説明し、国民の不安の払拭に努めることが求められる[50]。

⑦　サイバー通信情報監理委員会は通信情報を漏えいした行政職員の懲戒処分を求めるほか、通信情報の不適切な扱いが発覚した場合に保有機関の長に対し勧告を行う等の権限を有するため、同監理委員会のガバナンスや運営における透明性の確保が極めて重要になるのではないか[51]。また、同監理委員会の事務局も含めて、サイバーセキュリティの専門家（技術系、法務系双方）等を確保し、監督を行うに当たって十分な体制を整備する必要があろう。

⑧　政府は、協定を締結して基幹インフラ事業者等の通信情報を取得することとしているが、協定の内容次第では事業者の負担が重くなることも懸念される。標準的な協定についてのひな形的なものをあらかじめ政府が示すことも考えられるのではないか。さらに、政府が協定の締結を強制することはないことを徹底する[52]とともに、協定に関する協議に応じなかった場合にも、その事業者は不利益な取扱いを受けないことを何らかの形で明記することを検討する必要はないか[53]。

⑨　基幹インフラ事業者や電気通信事業者が政府に提供した通信情報について、仮に情報漏えいが発生した場合には、それらの企業の信用を毀損することにつながってしまうのではないか。そうした事態を回避するためにも、政府においては、厳格な安全管理措置を講じることが重要になるのではないか。

⑩　特定の個人を識別することができるおそれが大きい情報が含まれる選別後通信情報も一定期間（原則２年を超えない範囲内、延長も可能）、内閣府で保存されることとなる。国民の不安を払拭するためにも、政府には厳格な情報管理が求められるが、どのような措置を講じていくのか。

⑪　非識別化措置を講じた選別後通信情報については、他の情報と照合・分析することが特に必要である場合、再識別化措置を講じることができる。再識別化措置を講じたときは、その旨をサイバー通信情報監理委員会に通知し、同監理委員会の検査を受けること

---

[50] これに関連して、石破茂内閣総理大臣は「サイバー対処能力強化法案に基づく通信情報の利用は、通信当事者の同意によらない場合であっても、国、基幹インフラ事業者等の重要な機能がサイバー攻撃により損なわれることを防ぐという高い公共性があること、他の方法によっては実態の把握、分析が著しく困難である場合に限って通信情報の利用を行うこと、一定の機械的な情報のみを自動的な方法により選別して分析すること、独立性の高いサイバー通信情報監理委員会が審査や検査を行うこと等から、通信の秘密に対する制約が公共の福祉の観点から必要やむを得ない限度にとどまる制度としている」旨の答弁があった（第217回国会衆議院本会議録第９号（令 7.3.18））。一方で、「安全保障と人権保障の天秤がサイバー攻撃対策を機に前者へ傾かないか、注視が必要だ」とする意見もある（『朝日新聞』（令7.3.25））。

[51] これに関連して、宍戸常寿東京大学教授は「取得された情報が適切に処理・分析され、利用・共有するためのガバナンスが全体として確保されなければ、情報を取得する段階で既に通信の秘密が侵害されたと見るべきである」旨の指摘を行っている（「能動的防御 独立機関が必須」『日本経済新聞』（令6.9.19））。

[52] この点について、石破茂内閣総理大臣は「協定の締結はあくまでも任意であり、政府が基幹インフラ事業者等に対して協定の締結を強制することはない」旨の答弁があった（第217回国会衆議院本会議録第９号（令7.3.18））。

[53] 基幹インフラ事業者等との協定について、政府参考人からは「政府だけではなくて双方がメリットを認めて初めて締結がなされるものというふうに理解している」旨の答弁があった（第217回国会衆議院内閣委員会議録第６号（令7.3.19））。

となっているが、プライバシー保護の観点からは、そもそも再識別化措置を講じるケースを限定することも検討に値するのではないか[54]。

【アクセス・無害化措置に係る論点】

⑫　サイバー通信情報監理委員会がアクセス・無害化措置を行おうとする判断が適切か否かを事前に検討し、承認する権限を有するが、「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はないとする例外規定が盛り込まれている。同例外規定は、サイバー攻撃の特徴である被害の瞬時拡散性に着目したものと推察されるが、事態の緊急性を広く認める運用がされれば、事前承認は形骸化しかねず、こうした点にどのように歯止めをかけるのか、政府は丁寧に説明する必要があろう。

⑬　自衛隊がアクセス・無害化措置の実施主体となるのは、「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」とされるが、どのような場合か、政府は具体的な事例を示すべきではないか[55]。特に、国家を背景としたサイバー攻撃であると判断するのは容易ではないと思われるが、どのようにそれを判断するのか。また、我が国がアクセス・無害化措置を実行した結果、他国から報復を受ける可能性も否定し切れないとの指摘もある[56]。さらに、我が国が誤ってアクセス・無害化措置をとることをどのようにして回避するのか、政府の明確な説明が求められよう[57]。

⑭　外国にあるサーバ等に対してアクセス・無害化措置をとる場合、国際法の観点からのチェック機能は、警察又は自衛隊が外務大臣と協議することに委ねられており、外務大臣の責任は非常に重いと思われる。サイバー行動に係る国際法については、有識者会議提言においても、アクセス・無害化に関する国際法は未だ発展途上であるとされ、それらに係る国際法の議論に我が国として積極的に参画・貢献していくべき旨が示されている。サイバー行動に係る国際法の適用に関しては、不透明な部分があることは否めず、こうしたリスクも踏まえ、外務省としては、サイバー行動に係る国際法の議論において、国際世論をリードし、多くの国を味方につける努力が欠かせないのではないか[58]。

⑮　アクセス・無害化措置の執行に当たる警察・自衛隊は同一の建物で勤務するなど緊密

54　この点について、宮下紘中央大学教授は「復元できるのであれば、完全な『匿名化』とはいえない」とし、プライバシーが侵害される可能性について懸念を示している（『朝日新聞』（令 7.3.4））。

55　自衛隊と警察の役割分担について、石破茂内閣総理大臣は「個別具体的に判断されることになるが、警察と同等の権限に基づきつつも、自衛隊は、武力攻撃事態等における高列度なサイバー攻撃に対処するために構築しているサイバー防御能力や同盟国、同志国との訓練等によって獲得しているサイバー攻撃対処手法や情報を有しており、これらを活用することで適切に対処をしていく」旨の答弁があった（第 217 回国会衆議院本会議録第９号（令 7.3.18））。

56　この点について、井原聰東北大学名誉教授は「無害化措置が攻撃と捉えられて報復されるおそれもあるだろう。従って無害化措置に踏み出すかどうか、ゴーサインを出す機関の役割は重要になる。透明性を持って判断を下さなければならない」旨を述べている（『東京新聞』（令 7.1.29））。

57　この点について、政府参考人からは「アクセス・無害化措置を実施した結果については、一義的には、措置を実施した行政機関が責任を負うものと考えているが、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いう考えである」旨の答弁があった（第 217 回国会衆議院内閣委員会議録第６号（令 7.3.19））。

58　これに関連して、森永輔日経ビジネスシニアエディターは、「外務省は、警察及び自衛隊が実施する無害化措置が、タリン・マニュアルが定義する対抗措置もしくは緊急避難であると主張できるよう、日頃から理論武装しておく必要がある」との指摘を行っている。（森永輔「能動的サイバー防御法案が国会に　『警察』が担う日本の安全保障」『日経ビジネス電子版』（令 7.2.13））。

に連携を図るとされているが、両者の指揮系統は異なるため、適切に連携を図る工夫が求められる。警察・自衛隊の合同拠点は防衛省市ヶ谷庁舎の周辺に整備することが検討されているとの報道[59]があるが、どれぐらいの予算をかけて、どのようなスケジュールで整備を進めていくのかを示す必要があるのではないか。

【横断的な課題等に係る論点】

⑯　サイバー通信情報監理委員会は、毎年、国会に対し所掌事務の処理状況を報告するとともに、その概要を公表しなければならないとサイバー対処能力強化法案第61条で規定されている。サイバー通信情報監理委員会がチェック機能を果たしているのか、国会が適確に判断できるだけの内容が報告されるようにする必要があろう[60]。

⑰　例えば、自衛隊のサイバー専門部隊は令和９年度までに4,000人規模を目指すとの目標が掲げられているが、３万人とも言われる中国のサイバー攻撃部隊[61]と比較すると圧倒的に少ない。アクセス・無害化措置に係る人材を始め、警察や防衛省・自衛隊のサイバー人材を質量ともに充実させる必要があるのではないか[62]。

⑱　アクセス・無害化措置の実施に当たっては、内閣総理大臣、サイバー安全保障担当大臣のほか、サイバー通信情報監理委員会、防衛大臣、外務大臣等が関わることになるが、サイバー攻撃への対応には迅速な意思決定が必要であり、ケースごとに、どういう意思決定のルートをたどるのか、どういう分担、連携の体制をとるのか、事前にシミュレーションを重ねておく必要があるのではないか。

⑲　アクセス・無害化措置の実施を始めとした能動的サイバー防御のための対処には、技術的な情報収集や報告、技術的・法律的観点からの状況判断、これらを踏まえた政治判断が必要である。我が国のサイバーセキュリティ強化のためには、技術・法律・政治を統合した実践的なサイバー演習を積むことも有用であると考えられる[63]。

⑳　周囲を海に囲まれている我が国は国際通信の99％を海底ケーブルが支えている。地政学リスクの高まりもあり、世界各地で海底ケーブルの切断案件が報告される中で、同盟国、同志国とも連携し、海底ケーブルの安全性や強靱性を確保していくことが重要ではないか。また、房総半島や志摩半島には、海底ケーブルの陸揚げ局が集中し、国際通信のハブ（結節点）になっており、政府はこれらの地に通信情報を収集するための大規模な施設を設けることを検討している旨の報道[64]もあるが、どういった施設をどのようなスケジュール、予算で検討しているのか。また、それをどのように活用していく考えな

---

[59] 『読売新聞』（令 7.1.30）

[60] この点について、曽我部真裕京都大学大学院教授は「公表は『事務処理状況の概要』にとどまるが、可能な限り国民の知る権利に応える運用をするべきだ。例えば、アクセス・無害化の事前承認と事後承認の件数を明確にし、事前承認の制度が形骸化していないかを報告するべきである」旨の指摘を行っている（『東京新聞』（令 7.2.8））。

[61] 防衛省「令和６年版日本の防衛（防衛白書）」（令 6.7）186 頁

[62] これに関連して、吉田圭秀統合幕僚長は令和７年２月の記者会見で、日本のサイバー防御能力の現状について、「攻撃側の能力が日々向上し、我々が今のままでは対応できるとは認識していない」旨の発言を行ったとされる（『朝日新聞』（令 7.3.6））。

[63] 持永大芝浦工業大学准教授は政治判断を伴うサイバー訓練の必要性を指摘している（持永大『能動的サイバー防御　日本の国家安全保障戦略の進化』（日本経済新聞出版、令和７年２月）249-250 頁）。

[64] 『朝日新聞』（令 7.3.4）

のか。

㉑　サプライチェーンには中小企業も組み込まれているため、サイバー攻撃に対する社会全体の強靱性を高める観点からは、セキュリティ対策が遅れている中小企業の対策が急務であり、政府による実効性の高い支援を検討すべきではないか[65]。

サイバー対処能力強化法案と整備法案は、第208回国会（令和４年常会）における経済安全保障推進法の成立、第213回国会（令和６年常会）における重要経済安保情報保護活用法の成立から続く、相互に関連性のあるものであり、サイバー攻撃に対する対処能力の向上も含めた我が国の経済安全保障に関する能力を高め、あるいは脅威国からの攻撃に対する耐性を強めようとするものと位置付けられる。

今般提出された２法案は、国家としての安全保障政策、そして企業活動にも深く関係する重要なものであるほか、その運用次第では、通信の秘密の問題やプライバシーの侵害等への懸念を惹起する面もあり、丁寧かつ多角的な議論を踏まえる必要があると思われる。さらには、２法案の射程外ではあるが、サイバー攻撃が武力攻撃事態に当たり得ることについて、検討、検証を行う必要があると考える。アクセス・無害化措置の導入については、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のおそれがある場合、これを未然に排除するためのものと位置付けられ[66]、まずは平時から有事にエスカレーションさせないことが極めて重要となる。しかしながら、サイバー攻撃のみであっても武力攻撃事態に当たり得る場合がある[67]ことを踏まえ、万が一、有事にエスカレーションしてしまった場合の対応の在り方についても、政府の責任の下、官民共同でシミュレーションや訓練を実施し、それらを通じた検討、検証を重ねておくべきであろう[68]。

（かきぬま　しげし）

---

[65] これに関連して、石破茂内閣総理大臣からは「基幹インフラ事業者のサイバーセキュリティを確保するためには、これらの事業者と取引のある中小企業を含めたサプライチェーン全体での対策も重要である。本法律案では、基幹インフラ事業者以外の事業者についても、サイバー攻撃による被害の防止のために国が情報提供を行うことや、情報共有と対策を進めるための官民の協議会に構成員として参加してもらうことを可能とする規定を設けており、こうした取組によって、中小企業等のサイバーセキュリティ対策の強化を図っていく」旨の答弁があった（第 217 回国会衆議院本会議録第９号（令 7.3.18））。

[66] この点について、平将明国務大臣からは「アクセス・無害化措置は、サイバー攻撃による危害を防ぐために必要最小限度の措置として行うものであり、当該措置をとった場合の影響が最小限となるように措置をすることとなる。したがって、通常兵器による有形力の行使と同様の深刻な被害を伴うことは想定されず、国連憲章第２の４が禁ずる武力の行使に当たることはないと考え、その意味で先制攻撃になることはない」旨の答弁があった（第 217 回国会衆議院本会議録第９号（令 7.3.18））。

[67] 木原稔国務大臣（当時）からは「一般論として申し上げると、サイバー攻撃のみであっても、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て、これが相手方により組織的、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いうふうに思う」旨の答弁があった（第 213 回国会衆議院安全保障委員会議録第４号８頁（令 6.4.2））。

[68] これに関連して、初代警察庁サイバー警察局長を務めた河原淳平氏は「サイバー事案は治安の問題で完結するのか、安全保障の問題まで発展するのか初期段階では分からない」旨の指摘を行っている（『宮崎日日新聞』（令 7.1.16））。