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（１） －法案の全体像と官民連携の強化－
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	476 号
刊行日	2025-7-14
頁	41-59
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20250714.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２法案の国会論議（１）

― 法案の全体像と官民連携の強化 ―

榎本　尚行
（内閣委員会調査室）

１．はじめに
２．両法律案の検討、提出及び成立
３．両法律案の全体像及び官民連携の強化に関する制度の概要
４．国会における主な議論
５．小括

１．はじめに

令和５年７月の名古屋港におけるサイバー攻撃、令和６年末の航空会社や金融機関等へのサイバー攻撃[1]など、近年、サイバー攻撃の高度化、巧妙化が進んでいることから、対処の必要性が指摘されている。こうした中、従来からのサイバーセキュリティ対策に加えて、能動的サイバー防御を導入するための法整備として、令和７年の第217回国会（常会）において、「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）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）が国会に提出され、成立した。

両法律案に盛り込まれた能動的サイバー防御の内容は、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本柱に大別される。国会では、それぞれのテーマについて、憲法との関係を始め多岐にわたる議論が展開された。

本稿では、両法律案の全体像を概観し、３本柱のうちの官民連携の強化の概要に触れた上で、国会における主な議論を整理する。なお、通信情報の利用及びアクセス・無害化措

[1] 令和５年７月４日、名古屋港統一コンテナターミナルシステムにおいてサイバー攻撃による障害が発生し、名古屋港全コンテナターミナルの作業停止を余儀なくされた。障害はランサムウェア攻撃によるものであり、７月６日の夕刻に全ターミナルの作業が再開された。また、令和６年末には、航空会社、金融機関などの大手企業にサイバー攻撃が相次ぎ、一時的にシステムに不具合が起きたり、サイトが閲覧しづらくなったりするなどの影響が生じた（『ＮＨＫウェブサイト』（令7.1.12）<https://www3.nhk.or.jp/news/html/20250112/k10014691191000.html>（ＵＲＬは、令和７年６月27日最終アクセス（以下同じ。）。））。

置については、それぞれ別稿で整理する予定である。

２．両法律案の検討、提出及び成立

（１）国家安全保障戦略に基づく検討

令和４年12月16日、国家安全保障戦略が閣議決定され、能動的サイバー防御の導入等に向けて検討することとされた。その中では、「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、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。」ことが目標に掲げられた。

さらに、その目標達成のための具体的な取組内容として、①政府機関のシステムを常時評価し、政府機関等の脅威対策やシステムの脆弱性等を随時是正するための仕組みを構築すること、及び②能動的サイバー防御を導入することが盛り込まれた[2]。

能動的サイバー防御の内容については、「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」とした上で、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本柱が示された。

また、組織体制の整備について、「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[3]、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。」ことなどが掲げられた。

国家安全保障戦略を踏まえ、政府は令和６年６月から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。）を開催し、３本柱を中心に検討が進められた[4]。有識者会議においては、同年８月７日に「これまでの議論の整理」[5]が、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」[6]がまとめられた。

（２）両法律案の国会への提出及び国会審議

政府は令和７年２月７日、官民連携の強化や通信情報の利用について定める「**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」[7]という。）、及びアクセス・無害化措置、組織体制等について

---

[2] 加えて、経済安全保障、安全保障関連の技術力の向上等、サイバー安全保障の強化に資する他の政策との連携を強化すること、同盟国・同志国等と連携した形での情報収集・分析の強化、攻撃者の特定とその公表、国際的な枠組み・ルールの形成等のために引き続き取り組むことも盛り込まれた。

[3] 現行では、内閣官房長官を長とし、関係閣僚及び有識者で構成されるサイバーセキュリティ戦略本部が設置されているほか、内閣官房にＮＩＳＣが置かれている。また、関係機関として、総務省所管の国立研究開発法人情報通信研究機構（ＮＩＣＴ）や経済産業省所管の独立行政法人情報処理推進機構（ＩＰＡ）等がある。

[4] 有識者会議では、各テーマ別の会合も開催された。

[5] 有識者会議での「これまでの議論の整理」に向けた検討過程については、柿沼重志・榎本尚行「能動的サイバー防御に係る制度構築の方向性と課題～有識者会議「これまでの議論の整理」を中心とした整理～」（『経済のプリズム』No.239（令6.10.17））<https://www.sangiin.go.jp/japanese/annai/chousa/keizai_prism/backnumber/r06pdf/202423901.pdf>を参照。

[6] <https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/pdf/teigen.pdf>

[7] 略称については、能動的サイバー防御法案などの呼称も見られるが、本稿では、政府が呼称している「サイバー対処能力強化法案」を用いる。

定める「**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。）の２法律案を閣議決定し、国会（衆議院）に提出した。

衆議院では、３月18日の本会議において両法律案の趣旨説明・質疑が行われ、内閣委員会に付託された。同委員会では、翌19日に趣旨説明を聴取した後質疑に入り、対政府質疑のほか、参考人質疑、総務委員会及び安全保障委員会との連合審査会が行われた[8]。また、４月４日に対政府質疑及び対総理質疑を行い、質疑を終局した後、サイバー対処能力強化法案について、自民、立憲、維新、国民、公明、有志提出の修正案（通信の秘密の尊重、国会に対する報告事項の具体化、検討規定の追加）が提出され、サイバー対処能力強化法案について修正議決、整備法案について可決すべきものと決定した。なお、両法律案に対して、14項目から成る附帯決議が付された[9]。４月８日の衆議院本会議において、両法律案は委員会決定のとおり議決され、参議院に送付された。

参議院では、４月18日の本会議において趣旨説明・質疑が行われ、内閣委員会に付託された。同委員会では、４月22日に趣旨説明及び衆議院における修正部分の説明を聴取した後質疑に入り、対政府質疑のほか、参考人質疑、総務委員会及び外交防衛委員会との連合審査会が行われた[10]。また、５月15日に対政府質疑及び対総理質疑を行い、いずれも可決すべきものと決定した。なお、両法律案に対して、23項目から成る附帯決議が付された[11]。翌16日の本会議において、両法律案はいずれも可決・成立した（令和７年法律第42号及び第43号）。

３．両法律案の全体像及び官民連携の強化に関する制度の概要[12]

（１）両法律案の全体像

両法律案に盛り込まれた３本柱のうち、「通信情報の利用」については、政府は、経済安全保障推進法[13]に定める基幹インフラ事業者[14]等との間で協定を締結し、同意を得て通信情報を取得するほか、外外通信など、同意によらず一定の通信情報を取得する。取得した通信情報は、機械的情報のみに選別を行った上で分析を行う。

---

[8] なお、衆議院内閣委員会では、両法律案の担当大臣である平将明国務大臣（サイバー安全保障担当大臣）に加えて、４月２日には坂井学国家公安委員会委員長及び岩屋毅外務大臣が出席した（連合審査会では、平国務大臣のほか、村上誠一郎総務大臣及び中谷元防衛大臣が出席した。）。

[9] 衆議院ウェブサイト<https://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/naikaku11A6ECA8B6D9E53149258C65002D5209.htm>

[10] なお、参議院内閣委員会では、平国務大臣に加えて、４月24日には坂井国家公安委員会委員長が出席した（連合審査会では、平国務大臣のほか、村上総務大臣、岩屋外務大臣及び中谷防衛大臣が出席した。）。

[11] 参議院ウェブサイト<https://www.sangiin.go.jp/japanese/gianjoho/ketsugi/current/f063_051501.pdf>

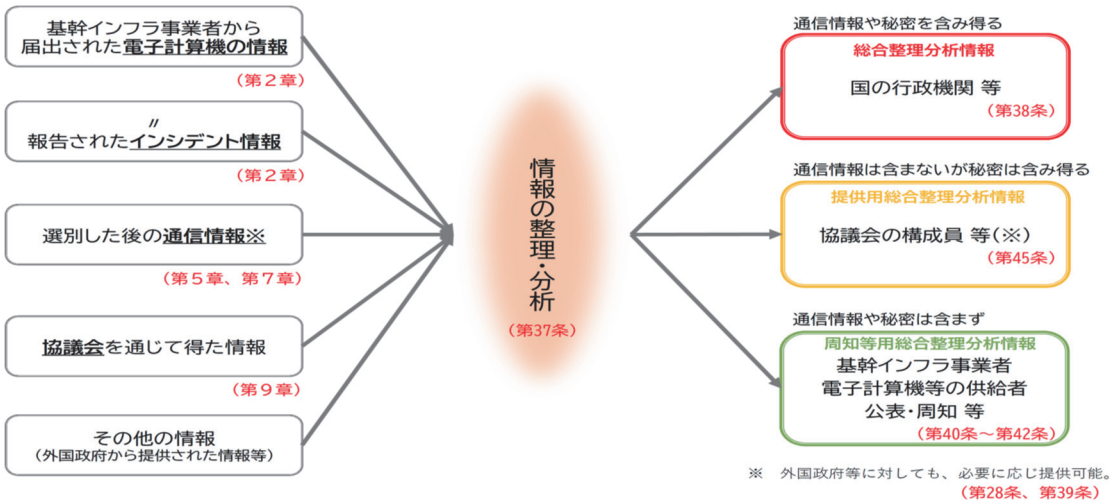
[12] 両法律案の概要については、柿沼重志「能動的サイバー防御の導入－サイバー対処能力強化法案及び整備法案の概要と主な論点－」『立法と調査』No.474（令7.4.14）<https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2025pdf/20250414003.pdf>を参照。

[13] 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）

[14] 経済安全保障推進法においては、基幹インフラ役務の安定的な提供の確保に関する制度が定められている。同制度は、15分野の基幹的なインフラ事業を行う事業者（基幹インフラ事業者（特定社会基盤事業者として指定された者））が、特定の重要設備（特定重要設備）について、導入や重要な維持管理等の委託をしようとする際に、事前に国に届出を行い、審査を受ける制度であり、令和７年６月25日時点で254者が基幹インフラ事業者として指定されている。

「官民連携の強化」については、基幹インフラ事業者に対する政府へのインシデント報告等の義務付けが措置されているほか、新たに官民で構成される協議会を設置し、協議会において情報を共有する。政府は、これらに基づきサイバー攻撃に関連する情報を収集し、通信情報の利用により得た情報などとあわせて整理・分析を行う。整理・分析した総合整理分析情報等は、関係する国の行政機関、協議会の構成員、基幹インフラ事業者等と共有されるほか、外国政府等にも必要に応じて情報提供が可能とされる（**図表１**参照）。

図表１　情報の収集・提供等



（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
（注）赤字で記載の条文番号等は、サイバー対処能力強化法案の規定に対応している。

加えて、サイバー攻撃の未然防止のため、一定の要件下でアクセス・無害化措置を実施することが可能とされており、実施主体である警察・自衛隊の役割分担等を決定した上で、攻撃に使用されているサーバ等にアクセスして攻撃プログラム等を確認し、無害化を行う。

（２）官民連携の強化に関する欧米主要国の取組

国家安全保障戦略では、官民連携に関して、「重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。」とされている。

官民連携の取組は、欧米主要国においても先行的に行われており、近年、高度な攻撃に対する支援・情報提供や、ゼロデイ脆弱性[15]の早期対処に必要な枠組みの強化が進められている。また、脅威ハンティング[16]部門の設置やクリアランス活用のほか、製品ベンダの役割

[15] ソフトウェア等のメーカーが確認できていない脆弱性であり、この脆弱性を突いたゼロデイ攻撃が行われている。
[16] 脅威ハンティングについては、有識者会議第１回官民連携に関するテーマ別会合（令6.7.3）の事務局資料７頁によると、「未知の脆弱性の悪用やマルウェアを用いない攻撃は、指標の一致・不一致では検知困難。このため、侵入を前提に、システムの作動状況から侵害の痕跡を探索する「脅威ハンティング」が必要となるが、標的組織や攻撃手法などの情報がないと、処理量が膨大となり、効果的探索は困難。」とされている。

の明確化等が進められている。同時に、政府の対処・情報収集能力を支えるためのサイバー対応機能の一元化や、重要インフラ事業者に対するインシデント報告の義務化が進められているとされる（**図表２**参照）。

図表２　主要国における官民連携等の主な取組

	英国	EU	米国	豪州
高度な攻撃に対する支援・情報提供	脅威情報のオンライン共有基盤（CISP, 2013） クリアランスを保有する産業界関係者との協業（Industry 100）	主に各々の加盟国が実施	CISAに脅威ハンティング部門を設置 企業との情報共有枠組みの設置（JCDC, 2021）	脅威情報のオンライン共有基盤（CTIS, 2021）
ゼロデイ脆弱性の対処	NCSCによる脆弱性情報の収集・分析・公開 製品ベンダによる脆弱性窓口設置等を義務化（PSTI法, 2022）	製品ベンダに対する脆弱性悪用時の報告義務化等を検討中（サイバーレジリエンス法草案）	CISAによる脆弱性情報の収集・分析・公開 製品ベンダの責任を明記（国家サイバーセキュリティ戦略, 2023）	ACSCによる脆弱性情報の収集・分析・公開 重要システムに対する脆弱性評価の実施義務化（SOCI法, 2022）
政府の情報収集・対処等を支える制度	国家サイバーセキュリティセンター(NCSC)設置(2016) 重要インフラ事業者の報告義務化(NIS規則,2018)	重要インフラ事業者の報告義務化(NIS指令,2016)	サイバー対応機能を国土安全保障省CISAに集約（CISA法, 2018） 重要インフラ事業者の報告義務化(CIRCIA法, 2022 ※未施行)	豪州サイバーセキュリティセンター(ACSC)設置(2014) 重要インフラ事業者の資産登録・報告義務化（SOCI法, 2021）

CISP【英】: サイバーセキュリティ情報共有パートナーシップ　NIS指令【EU】:ネットワーク及び情報システム指令　CTIS【豪】: サイバー脅威情報共有枠組
PSTI法【英】: 製品セキュリティ及び通信インフラ法　CISA【米】:サイバーセキュリティ・インフラセキュリティ庁　SOCI法【豪】: 重要インフラ保安法
NIS規則【英】: ネットワーク及び情報システム規則　JCDC【米】: 官民サイバーセキュリティ協力枠組

（出所）第１回有識者会議（令和６年６月７日）資料より抜粋

なお、有識者会議における一般社団法人日本経済団体連合会へのヒアリング（令和６年７月８日）においては、英国の取組が紹介された。英国では、ＮＣＳＣ（国家サイバーセキュリティセンター）が対策を主導し、事業所管官庁等に対してもリーダーシップを発揮することや、年間100名を目安に、民間企業の専門家をＮＣＳＣに受け入れて、民間が保有する知識・経験をいかす仕組み（i100（Industry 100））等が行われており、我が国においても官民人材交流に関する枠組みを導入すべきとの指摘がなされた[17]。

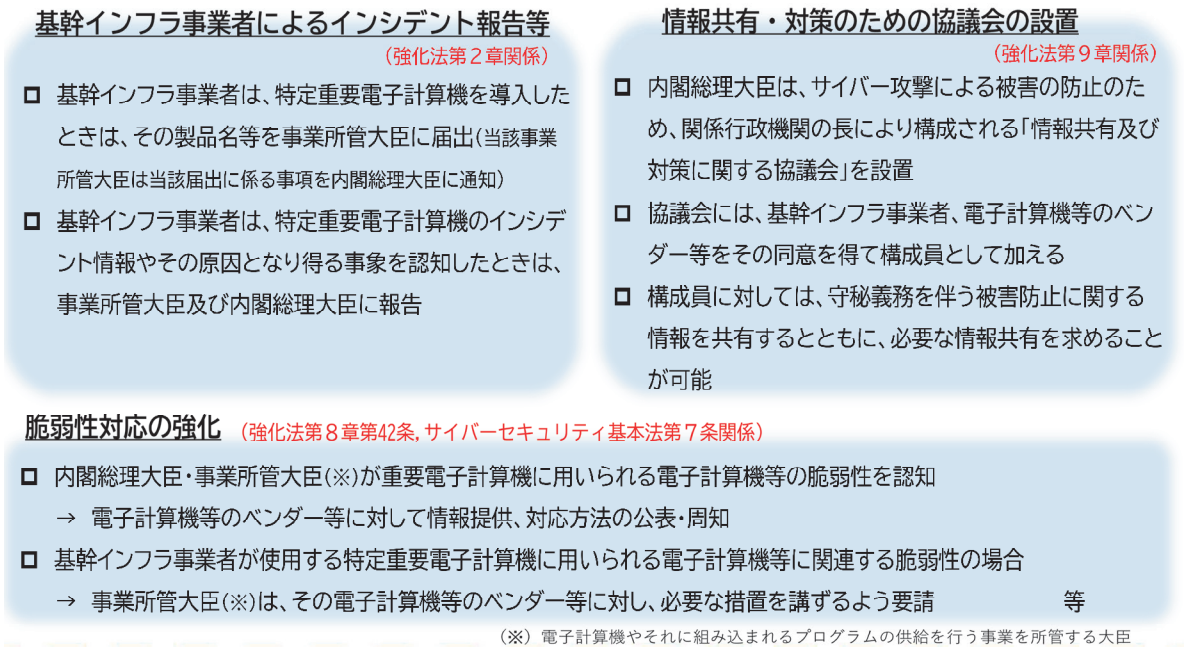
（３）両法律案における官民連携に関する規定の概要

サイバー対処能力強化法案では、基幹インフラ事業者によるインシデント報告等、情報共有・対策のための協議会の設置、及び脆弱性対応の強化が主に措置されている。脆弱性対応の強化の一部の規定は、整備法案のサイバーセキュリティ基本法（平成26年法律第104号）の一部改正の中に盛り込まれている（**図表３**参照）。各取組に関する規定の概要は以下のとおりである。

---

[17] このほか、有識者会議のヒアリングにおいて日本商工会議所から、中小企業の対応強化に向けた支援の強化等の要望があった。また、公益社団法人経済同友会は、欧米諸国は近年サイバーセキュリティの強化に向けて法整備化を加速しているなどの現状認識を示した上で、能動的サイバー防御の早期導入、重要インフラ事業者への報告義務化といった法案に関連する事項、新たな官民連携組織の在り方、サイバーセキュリティ人材定義と可視化、企業のサイバーセキュリティ対応における情報開示、サイバーセキュリティ産業振興、サイバー保険の在り方などの法案以外の課題を盛り込んだ提言を公表した（<https://www.doyukai.or.jp/policyproposals/uploads/docs/20241023c.pdf>）。

図表３　官民連携の強化に関する規定の概要



（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

ア　特定重要電子計算機の導入に係る届出

特別社会基盤事業者（基幹インフラ事業者）[18]は、特定重要電子計算機を導入したときは、主務省令で定めるところにより、特定重要電子計算機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特別社会基盤事業所管大臣に届け出なければならないもの等とする。届出に係る命令違反に対しては、200万円以下の罰金が科される。

イ　インシデント報告（特定侵害事象に係る報告）

特別社会基盤事業者は、特定重要電子計算機に係る特定侵害事象[19]又は当該特定侵害事象の原因となり得る事象として主務省令で定めるものの発生を認知したときは、主務省令で定めるところにより、その旨及び主務省令で定める事項を特別社会基盤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ものとする。報告に係る命令違反に対しては、200万円以下の罰金が科される。

ウ　協議会

内閣総理大臣は、内閣総理大臣及び関係行政機関の長により構成される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の情報共有及び対策に関する協議会を組織するとともに、当該協議会に、重要電子計算機を使用する者等をその同意を得て構成員として加えることができる。

---

[18] サイバー対処能力強化法案では、基幹インフラ事業者、すなわち経済安全保障推進法上の特定社会基盤事業者（前掲脚注14参照）のうち、重要電子計算機を使用する者を「特別社会基盤事業者」と定義している。また、特別社会基盤事業者が使用する重要電子計算機を「特定重要電子計算機」と定義している。

[19] 特定侵害事象とは、重要電子計算機に対する特定不正行為（不正アクセス行為等）により、当該重要電子計算機のサイバーセキュリティが害されることをいう。

協議会は、その目的を達成するため、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に資する被害防止情報[20]を共有するとともに、所定の事項について協議を行う。協議会の構成員は、当該協議の結果に基づき、協議会で知り得た被害防止情報の適正な管理その他の必要な取組を行うものとされている。行政職員及び協議会構成員等による秘密の不正な利用、漏えいの行為に対しては、２年以下の拘禁刑又は100万円以下の罰金が科される。

エ　脆弱性対応の強化

内閣総理大臣及び所管大臣[21]は、重要電子計算機として用いられる電子計算機やプログラムにおける脆弱性を認知したときには、当該電子計算機等の供給者[22]に対し情報を提供することができる。また、同所管大臣は、脆弱性が、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等に関連するものである場合には、当該電子計算機等の供給者に対し、サイバー攻撃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。

このほか、電子計算機やプログラム等の供給者に対する責務規定（利用者のサイバーセキュリティ確保のための設計・開発、情報の継続的な提供等に努める旨）を設ける。

（４）施行期日

サイバー対処能力強化法及び整備法は、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する。

４．国会における主な議論[23]

両法律案に関しては、テーマごとに異なる議論が展開された。以下では、国会における議論のうち、まず総論的な論点に触れ、次いで官民連携の強化に関連する主な議論を紹介する。

（１）能動的サイバー防御の意義及び期待される効果

能動的サイバー防御の意義について問われた内閣官房は、「国家安全保障戦略において、能動的サイバー防御は、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導入するものとされている」旨答弁した上で、具体例として、「有事における機能不全を生じさせることを念頭に、そうした事態に至る前の段階から基幹インフラのシステム内部へのアクセスを確保するタイプのサイバー攻撃などが考えられる。こうした攻撃に関しては、事業者からのインシデント報告や通信情報の利用によってその手法等を把握できれば、他の事業者

---

[20] 提供用総合整理分析情報その他の情報（選別後通信情報を含むものを除く。）。

[21] 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を所管する大臣（電子計算機等供給事業所管大臣）。

[22] 「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）では、電子計算機等の生産者、輸入者、販売者及び提供者とされている。

[23] 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。

に対しても情報提供することやアクセス・無害化措置を講ずることなどにより被害の拡大などを防止することが可能となる。このほか、いわゆるＤＤｏＳ攻撃やランサムウェアなどに対しても対応能力を向上させることが可能となる」旨答弁した。さらに、ＤＤｏＳ攻撃については、「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攻撃（ＤＤｏＳ攻撃）が生じている場合を例にすると、インシデント報告を踏まえて通信情報を分析することなどにより、必要に応じ、乗っ取られた機器に対し指令を出しているサーバを割り出し、当該指令サーバにアクセスして不正プログラムを無害化することで被害の拡大を防止することが考えられる」とした。また、ランサムウェアについては、「データを不正に暗号化し、また盗み出し、身代金を要求するランサムウェアのうち高度な手法を用いるものに対しては、例えば、インシデント報告を受けた場合に、その内容を踏まえながら、必要に応じ、通信情報等も併せて分析するなどした上で、その結果に応じ、必要な注意喚起を行うことなどによって被害の最小化を図るといったことも想定される」旨答弁した[24]。

また、両法律案によってサイバー攻撃が防げるようになるのかという点について、平将明国務大臣（サイバー安全保障担当大臣）は、「全てを防ぎ切ると断言できる状態にはないが、堅牢なシステムの構築といった平素からの対策に加えて、サイバー攻撃が発生した場合、その状況を迅速に把握し対処することで被害を低減することは十分に可能と考えている」との認識を示した上で、「制度を整備して終わりではなく、運用に万全を期すことが重要である。このため、サイバーセキュリティ戦略本部の機能強化や内閣サイバー官の設置など、司令塔機能の強化に必要な事項も本法案に盛り込んだところであり、政府一丸となって我が国全体のサイバーセキュリティの強化を図っていきたい。国家としてのサイバーセキュリティの能力は格段に上がる可能性を持った法律であると言ってよい」旨答弁した[25]。

なお、冒頭で触れた令和５年７月に発生した名古屋港におけるサイバー攻撃を例にして、新たな制度で取り得る対応について問われた平国務大臣は、「今回の制度整備により得られた情報や分析結果により悪用された機器の脆弱性や攻撃に用いられた攻撃者のＩＰアドレス等に関する注意喚起を行うことで、事業者の対策を促し、被害を未然に防ぐことや被害を最小化することに貢献できた可能性もあるものと考えている」としたほか、「一般論であるが、今のところは被害が発生してから所管省庁に報告することになっているが、インシデントの時点で、例えばその侵入された痕跡がある時点で情報共有されることになる。さらには、様々な情報ソースから、今こういった勢力がこういった国でこういうインフラを対象にしてこういった攻撃をしているといった情報も共有できることになり、また重要電子計算機を届け出てもらうため、どこかで重要電子計算機の脆弱性が明らかになったら、その脆弱性のある情報について、重要電子計算機を持っているインフラ事業者に対して、蓋然性が高ければ、こういう脆弱性があるからパッチを当ててください、ソフトウェアを変えてくださいということもできるので、できることは多くなるほか、更に情報のやり取

[24] 第217回国会参議院内閣委員会会議録第10号（令7.4.22）
[25] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

り、意思疎通が密になると思われ、防御する力は高まっていく」旨答弁した[26]。

（２）国家安全保障戦略で示された目標との関係及び同盟国等との連携

国家安全保障戦略では、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ことが目標として掲げられている。その目標達成の時期や達成に向けた具体的な取組内容について問われた平国務大臣は、「政府機関のシステムの常時評価については、法整備を待つことなく令和６年度から取組に着手しており、引き続き強力に推進していく[27]。能動的サイバー防御の導入及び新たな組織の設置については、今回の法案提出により着手することとしており、その施行期日に向け、組織体制の整備に加え、官民双方からの高度なサイバー人材の確保、通信情報の利用に向けた高性能なシステムの導入などにも取り組んでいく。いずれにしても、法案が成立した暁には、法律の万全な運用に取り組んでいく」旨答弁した[28]。また、石破茂内閣総理大臣からは、「同等以上にしないとこれから先、日本はやっていけぬという強い危機感と使命感の表れだと承知している」旨の答弁があった[29]。

また、同盟国、同志国との連携について石破総理は、「一国だけでは絶対対応はできないものなので、同盟国、同志国との連携を強めていくということは極めて喫緊の課題であると承知している。具体的には、同盟国、同志国と共同でサイバー攻撃の主体を特定してパブリックアトリビューション[30]を実施する、アメリカを始めとする諸外国との間でサイバー攻撃への対処に関する演習、協議を行う等々、国際的な連携強化を図ってきたところであるが、今般の立法措置により、我が国のサイバー対処能力は抜本的に強化されることになる。サイバー攻撃への対処をより的確かつ効果的に行うためにも、同盟国、同志国とは一層の情報収集、分析の段階からの連携強化に努めていきたい」旨答弁した[31]。

（３）重要電子計算機の定義

両法律案の目的を理解するに当たって、そもそも重要電子計算機とは何かと問われた内閣官房は、「両法律案においては、重要電子計算機を大きく３類型から定義している。第一に、国の行政機関などが使用する電子計算機である。このうち、そのサイバーセキュリティが害された場合において、その機関などにおける重要情報の管理又は重要な情報システム

---

[26] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

[27] なお、内閣官房は、「政府機関へのサイバー攻撃等について、24時間体制による横断的な監視及び分析を行い不審な通信等を検知し、対応が必要と判断した際には当該政府機関に通知、通報し、必要な場合には実効性のある対策を直ちに実施するよう求める」旨答弁した（第217回国会参議院内閣委員会会議録第10号（令7.4.22））。

[28] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

[29] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）。この点について、参議院内閣委員会で持永大参考人（芝浦工業大学システム理工学部准教授）は、「欧米と外から見た制度上はほぼ同等のことができるような仕組みになった」、「運用が始まってから日本がどれだけその運用を効率化して適切に対処できるか、対処した後に透明性が確保されているのか、あとは、その対処自身も常に技術的に革新的なものを採用しているのかが課題である」旨述べた（第217回国会参議院内閣委員会会議録第12号（令7.5.8））。

[30] サイバー攻撃の攻撃者を公表し、非難することでサイバー攻撃を抑止する取組。

[31] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

の運用に関する事務の実施に重大な支障が生ずるおそれがあるものを重要電子計算機と定義している。第二に、基幹インフラ事業者が使用する電子計算機である。このうち、そのサイバーセキュリティが害された場合において、特定重要設備の機能が停止し、又は低下するおそれがあるものを重要電子計算機と定義している。第三に、重要情報[32]を保有する事業者が使用する電子計算機である。このうち、そのサイバーセキュリティが害された場合において、当該事業者における重要情報の管理に関する業務の実施に重大な支障が生ずるおそれがあるものを重要電子計算機と定義している。これら３類型の重要電子計算機は、サイバー攻撃を受けた場合に、国家及び国民の安全を害し、又は国民生活若しくは経済活動に多大な影響を及ぼすおそれがあることから、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との法案名の下、本法案を通じ、サイバー攻撃による被害の防止を図っていく必要があるものとして位置付けている」旨答弁した[33]。

（４）重要インフラ分野のサイバーセキュリティ対策

重要インフラ事業者に対するこれまでのサイバーセキュリティ対策の取組及び法改正による新たな取組について質疑があった。平国務大臣は、これまでの取組について、「サイバーセキュリティ戦略本部においては、内閣サイバーセキュリティセンター（ＮＩＳＣ）が事務局を務め、重要インフラ事業者等における自主的な取組を促進するため、重要インフラのサイバーセキュリティに係る行動計画を策定するとともに、各重要インフラ分野に共通して求められるセキュリティ対策を安全基準等策定指針として策定している」[34]、また、「重要インフラ事業者等がサイバー攻撃を受けた場合には、当該事業者が所管省庁などに報告を行い、ＮＩＳＣは同省庁から情報提供を受けている。また、国内のより多くの組織が速やかな防護策を講じ、サイバー攻撃の被害を最小限にとどめるよう、情報処理推進機構（ＩＰＡ）、ＪＰＣＥＲＴコーディネーションセンター[35]、情報通信研究機構（ＮＩＣＴ）等の関係機関と連携し、脅威、脆弱性対策について注意喚起を行っている。一方で、これらの取組について基本的には各主体の自主性に基づくものであり、迅速かつ業界横断的に情報を集約、整理、分析して対処していくことに一定の課題があった」旨答弁した[36]。

新たな取組について平国務大臣は、「今般のサイバーセキュリティ基本法の改正では、取組の実効性を高めるため、サイバーセキュリティ戦略本部において重要インフラを所管する各省庁が統一的に実施すべき施策の基準を定め、各省庁では、当該基準に基づき重要インフラ事業者等に一定の対策を求めるなどの施策を実施することとしている。当該基準に基づき各省庁が実施する施策については戦略本部において評価を行うこととしており、これにより、各省庁の施策が一層強化されることを通じ重要インフラ全体で平素からのセ

---

[32] 特定秘密の保護に関する法律（平成25年法律第108号）などの関係法律に規定される特別防衛秘密、特定秘密、装備品等秘密及び重要経済安保情報を指す。

[33] 第217回国会参議院内閣委員会会議録第10号（令7.4.22）

[34] 第217回国会参議院内閣委員会会議録第10号（令7.4.22）

[35] Japan Computer Emergency Response Team Coordination Centerの略(JPCERT/CC)で、国内に関するインシデント等の報告の受付、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを技術的な立場から行う機関であり、特定の政府機関や企業からは独立した中立の組織である。

[36] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

キュリティ対策を強化していきたいと考えている」旨答弁した[37]。

（５）インシデント報告等

ア　対象事業者を基幹インフラ事業者とした理由

特別社会基盤事業者（基幹インフラ事業者）にインシデント報告等を義務付けることとした理由及びサイバーセキュリティ基本法に基づく「重要インフラ事業者」との相違点について質疑があった。これに対して内閣官房は、「重要インフラ事業者は、同法に基づき、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生じるものに関する事業を行う者が幅広く位置付けられており、自主的かつ積極的にサイバーセキュリティの確保に努めることが求められている。一方で、基幹インフラ事業者は、経済安全保障推進法に基づき、その安定的な提供に支障が生じた場合に国家及び国民の安全を損なう事態を生じるおそれがあるものの提供を行う者として215者に限り指定されている[38]もので、同法に基づき一定の重要設備を導入する際の事前届出が義務付けられている。今回の法案においては、有識者会議においても、重要インフラ事業者等の中でも、サイバー攻撃が発生した場合に国家及び国民の安全を損なう事態が生じるおそれがある基幹インフラ事業者に対して、インシデント報告を義務化し情報共有を促進すべきとの提言があった。サイバー攻撃を受けた場合の影響を踏まえて、基幹インフラ事業者に対し資産届出やインシデント報告を義務付けることとした」旨答弁した[39]。

イ　特定重要電子計算機を導入した場合の届出

基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を届け出なければならないとされ、詳細は主務省令に委ねられている。導入の「時期」の考え方について内閣官房は、「下位法令の策定時に事業者と相談しながら設定していきたい。導入に関しては、クラウドの所有権などを考えると難しいことになるため、基幹インフラ事業者が一定の電子計算機を設置するなど、自らが利用できる状態になっているというタイミングを適切に設定していきたい」旨答弁した[40]。

また、具体的な機器の届出対象について、内閣官房は、「例えば、ファイアウォールやＶＰＮ装置[41]と言われる、事業者の内部システムと外部のインターネットの接点となるような機器を届け出てもらう。また、認証サーバと言われるシステム管理において重大な役割を果たしている機器を想定している。その上で、それぞれの具体的な範囲は、今後政令で規定していくことになるが、業界ごとのシステムの特性についてよく配慮した上で、事業者や専門家の意見を聴きながら丁寧に制度設計し、相談しながら進めていきたい」旨答弁した[42]。また、製品名等についての主務省令の具体的内容としては、「関係

---

37 第217回国会参議院内閣委員会会議録第10号（令7.4.22）
38 最新の指定数については前掲脚注14参照。
39 第217回国会参議院内閣委員会会議録第10号（令7.4.22）
40 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
41 Virtual Private Networkの略（仮想専用通信網）で、テレワークなどに用いられる。
42 第217回国会参議院内閣委員会会議録第10号（令7.4.22）。関連して、汎用のパソコン等が特定重要電子計算

業界、事業者と相談していくが、現時点では、製造者名、インターネットから一定のネットワーク機器を通じて特定重要設備と接続されるまでの機器同士の関係を示すネットワーク構成図等を想定している」旨答弁した[43]。

ウ　インシデント報告

報告の対象となる特定侵害事象[44]等の想定としては、「特定重要電子計算機においてマルウェアが実行されることが判明した場合、ネットワーク機器の脆弱性を悪用することなどにより特定重要電子計算機に対して不正アクセス行為が行われたことが判明した場合、また、ランサムウェアによる暗号化や大量のパケットを送り付けるＤＤｏＳ攻撃のような特定重要電子計算機の機能を低下又は停止させられたことが判明した場合において報告を求めることを想定している。また、特定侵害事象の原因となり得る事象としては、特定重要電子計算機に保管されているシステム管理者等のＩＤ、パスワードが窃取され、システム全体への広域、広範な攻撃が可能となったことが判明した場合、特定重要電子計算機において、マルウェア自体は見付かっていないが、その実行された痕跡が残っている場合といったことについて報告を求めることを想定している」、「いずれにしても、今後主務省令における報告対象の具体化については専門家や事業者の意見も伺いながら丁寧に制度設計していきたい」旨答弁した[45]。

エ　事業者の負担軽減策

インシデント報告等については、既存の業法や個人情報保護法[46]においても報告義務が課されているものがあることから、事業者の負担を軽減する必要がある旨の指摘があった。これに対して内閣官房は、「有識者会議からも、インシデント報告先の一元化、また報告様式の統一化等を進めることが必要である旨の提言をいただいたところである。

機の対象となるか問われた内閣官房は、「過去に国内外で発生した事案を踏まえると、被害組織の従業員が使用する汎用的なパソコンが侵害されたことを皮切りに、組織内に感染が拡大する可能性があるということも事実であり、感染リスクの高さは、例えば、汎用的なパソコンが、システム構成上、基幹インフラ事業を行う上で最も重要である特定重要設備とどの程度隔離されているのかといったシステム特性に依存すると考えられる。その上で、現時点で断定することはできないが、例えば発電所や浄水場などにおいて基幹的なインフラ設備を直接制御するシステムに汎用的なパソコンが用いられている場合、汎用的なパソコンであっても対象になり得る可能性はあると思う。いずれにせよ、事業者や専門家の意見を聴きながら、事業者の過度な負担にならないように、丁寧に検討を進めていきたい」旨答弁した（第217回国会参議院内閣委員会会議録第14号（令7.5.15））。

43 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

44 前掲脚注19のとおり、特定侵害事象はサイバーセキュリティが害されることを指すが、この点についてさらに説明を求められた内閣官房は、「サイバーセキュリティとは、サイバーセキュリティ基本法第２条において、電磁的方法により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のための必要な措置、また情報システム及び情報通信システムの安全性及び信頼性の確保のための必要な措置が講じられ、その状態が適切に維持管理されていることと定義されている。特定重要電子計算機のサイバーセキュリティが害された状態というのは、まさにサイバー攻撃等によりこれらの措置が講じられた状態が損なわれたということが指される」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））。

45 なお、ＩＰＡが公表している情報セキュリティ10大脅威<https://www.ipa.go.jp/security/10threats/10threats2025.html>との関係について内閣官房は、「法律の義務は基幹インフラ事業者に限定されているが、情報セキュリティ10大脅威を見ると、組織向け、個人向けで書いてあるので、全てがこの対象となるわけではないが、当然ながら、その中で特定侵害事象と関係がある事象については報告対象になることになろうかとは思う」旨も答弁した（第217回国会参議院内閣委員会会議録第13号（令7.5.13））。

46 個人情報の保護に関する法律（平成15年法律第57号）

サイバー対処能力強化法案においては、まず、基幹インフラ事業者によるインシデント報告を、内閣総理大臣及び特別社会基盤事業所管大臣に同報する旨を規定している。その上で、政府としては、本法案におけるインシデント報告に限らず、個人情報保護法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」とした上で、具体的には、「件数が多く、初動対応中の報告となることから被害組織による負担が大きくなる、ランサムウェア事案、ＤＤｏＳ事案について、法案施行までの可能な限り早い段階から業法と個人情報保護法に基づく報告や警察への相談に共通して使えるような様式の統一を先行実施する。また、法案成立後は、システム整備によりサイバー対処能力強化法案の報告窓口を一本化し、報告を受けた情報を関係府省にも共有できるような環境を整備したいと考えている」旨答弁した[47]。

また、基幹インフラ事業者に対しては、経済安全保障推進法の重要設備の導入等に係る委託を行う際の事前届出も課されている。両法の手続の合理化を図る必要性について平国務大臣は、「経済安全保障推進法における導入等計画書の届出と、サイバー対処能力強化法案における特定重要電子計算機の届出では、届出の対象設備について一部重複する部分が生じることが想定される。その上で、経済安全保障推進法は、例えば電力の需給制御システムなどの特定重要設備について、導入前に届出を求めてその内容を審査するものであるのに対し、本法案は、政府から基幹インフラ事業者に情報提供するため、特定重要設備に接続されているネットワーク機器等を事後的に届けてもらうものであり、それぞれの制度趣旨、対象機器、届出のタイミングを踏まえると、両制度の手続を一体化することは困難と考えている」とした上で、「届出の具体的な方法などについては、主務省令において定めていく。その際、事業者に過度な負担にならないように配慮することは重要だと認識しており、専門家や事業者の意見も伺いつつ、丁寧な制度設計を行っていく」旨答弁した[48]。

これらの議論に関連して、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。）では、「三　インシデント報告等において経済安全保障推進法、個人情報保護法等の関係法令への対応との重複を回避するとともに、被害を受けた事業者等の負担軽減と政府の対応の迅速化を図るため、報告先の一元化や報告様式の統一化、速報の簡素化、報告基準・内容の明確化を進めること。」とされている。

この点、サイバー対処能力強化法案等の成立後に策定された「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和７年５月28日関係省庁申合せ）では、ランサムウェア事案、ＤＤｏＳ事案それぞれについて、個人情報保護法や既存の業法に基づく報告に係る共通様式が公表され、所要の制度改正やパブリックコメント等を経て、令和７年10月１日から適用するとされている。同申合せでは、サイバー対処能力強化法案に基づくものについては、規定の施行に併せ、官公署への報告等に際して利用できる共通様式を整備し、さらに官民連携基盤の整備により、これらの報告の窓口を一

47 第217回国会衆議院内閣委員会議録第６号４頁（令7.3.19）
48 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

元化するよう所要の調整を進めるとされている。

（６）協議会

ア　現行の協議会の取組との相違点及び取組内容

現行のサイバーセキュリティ基本法では、「サイバーセキュリティ協議会」が組織され、官民の情報共有が行われている。この協議会に代わって新たな協議会が設けられることに関して、現行の取組との相違点等について質疑がなされた。これについて平国務大臣は、「現行のサイバーセキュリティ協議会は、官民が相互に連携し、サイバーセキュリティの確保に資する情報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予防と拡大防止に一定の成果を上げてきたものと認識している。具体的には、例えば構成員となっているセキュリティベンダがサイバー攻撃に関する専門的な分析内容を持ち寄り、対応策等を整理した上で他のメンバーに共有等を行うなどしている。他方で、国家を背景とした高度なサイバー攻撃への懸念の拡大や社会全体におけるデジタルトランスフォーメーションの進展を踏まえると、政府が率先して情報提供し、官民双方向での情報共有を更に強力に推進する必要があると考えている」旨の問題意識を示し、サイバー対処能力強化法案における協議会については、「政府が保有する秘匿性の高い情報についても共有できるよう、協議会の構成員による安全管理措置を法定しているほか、守秘義務違反に対する罰則の引上げも行っている。加えて、一定の機微な情報についても、適切な情報管理の下で協議会の構成員など必要な者が取り扱えるようにするため、セキュリティ・クリアランス制度の活用について必要な検討を進めていきたい[49]。また、それぞれの事業者には個別の事情があることから、政府が提供する情報の内容やその取扱いなど、運用面を検討するに当たっては、専門家や事業者などの意見を丁寧に伺っていきたい。いずれにしても、丁寧な制度設計を行い、官民双方向の情報共有が我が国全体のサイバーセキュリティの対策強化につながるという好循環を実現できる仕組みとしていきたい」旨答弁した[50]。

また、情報共有に当たって経営層の意思決定に有用な情報の提供が必要であることが指摘されたことに対して、平国務大臣は、「事業者が具体的な行動を取れるようにするためには、サイバーの専門家が求める技術情報に限らず、経済同友会の提言[51]で指摘されているような、経営層が判断を下す際に必要な攻撃の背景や目的などに関する情報も重要

---

[49] 経済安全保障分野におけるセキュリティ・クリアランス制度について定める重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）（令和６年法律第27号）が令和６年の常会（第213回国会）において成立し、令和７年５月16日から施行されている。協議会における情報保全や同制度の活用について問われた内閣官房は、「本法案に基づいて、政府としては、サイバーの専門家が求める技術情報や経営者の判断に必要な攻撃目的等に関する情報を積極的に提供していくことを想定している。このうち、攻撃者の詳細な活動状況といった秘匿性の高い情報については、一定の情報管理が義務付けられる協議会構成員などに限って提供できるとしている。その上で、より機微な情報についても適切な情報管理の下で事業者が取り扱えるようにするために、セキュリティ・クリアランス制度の活用についても必要な検討を進めていく。協議会の構成員の全てにセキュリティ・クリアランスの取得を求めるということは想定していない」旨答弁した（第217回国会衆議院内閣委員会議録第10号（令7.4.2））。

[50] 第217回国会参議院内閣委員会会議録第10号（令7.4.22）

[51] 前掲脚注17参照

であると考えている。政府においては、本法案に基づき政府に集約される基幹インフラ事業者からのインシデント報告や通信情報の利用を通じて得られる情報のほか、防衛省、警察庁等が独自に収集した情報、外国機関から提供される情報なども活用し、総合的に分析を行い、必要な情報を事業者に提供していく」旨答弁した[52]。

加えて、協議会で行う情報共有以外の取組内容として、内閣官房は、「サイバー対処能力強化法案では、協議会構成員の間で被害防止のための対策に対する事項等を協議できると規定している。例えば、公表されていない脆弱性情報の共有と分析、さらには日頃からの対応策など、各事業者におけるベストプラクティスを意見交換することも想定している。こうした取組を通じて、我が国のサイバーセキュリティの強化に資するように、今後、具体的な制度設計について関係者の意見を踏まえながら進めていきたい」旨答弁した[53]（民間事業者に官民連携の意義を感じてもらい、協力を得る必要性については（**7**）も参照。）。

この点、セキュリティ・クリアランス制度との関係について、参議院附帯決議では、「九　協議会を活用した官民の情報共有においては、重要経済安保情報保護活用法に基づくセキュリティ・クリアランス制度の活用も図りながら、機微情報も含め迅速に提供し、サイバー対処能力を効果的に向上させること。また、それにより安定的な経済活動や我が国の技術的優位性を確保し、産業競争力の強化につなげていくこと。」とされた。

イ　構成員の在り方

新たな協議会では、内閣総理大臣は事業者等を構成員に加えることができるが、その場合、事業者等の同意を得る必要がある。構成員となるよう呼びかける範囲について内閣官房は、「基幹インフラ15業種に該当する事業者や、これら事業者との取引がある事業者に加えて、基幹インフラ事業者には該当しないインフラ事業者、システムやソフトウェアの提供やセキュリティ対策を行うベンダ、さらには機微技術を保有する事業者などにも必要に応じて参加してもらうことを想定している」旨答弁した[54]。

また、協議会における中小企業や地方公共団体の扱いも質された。まず、中小企業について石破総理は、「基幹インフラ事業者と取引のある中小企業も、必要があると認める場合には協議会の構成員となってもらうことを想定している」としつつ、「現段階において協議会に参加する事業者数の見込みを示すことは困難だが、必要な企業に参加してもらえるよう、協議会の意義等について適切に周知を図っていく」旨答弁した[55]。また、地方公共団体について平国務大臣は、「これまで以上に地方公共団体とは情報連携を図ることとしている。法案が成立した暁には、地方公共団体を含めた関係者の意見も丁寧に伺いつつ、施行に向けた具体化を進めていく」旨述べた[56]。

---

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 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
54 第217回国会参議院内閣委員会会議録第11号（令7.4.24）。なお、同意の取得方法等について内閣官房は、「事前の同意を得るに当たっては、求められる対応事項について丁寧に説明する。また、同意を得る方法については、当然、書面などの形になろうかと思う。適切なものになるように検討を進めていきたい」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））。
55 第217回国会参議院本会議録第14号（令7.4.18）
56 第217回国会参議院内閣委員会、総務委員会、外交防衛委員会連合審査会会議録第１号（令7.5.13）。なお、

この点、参議院附帯決議では、「八　協議会の構成員の在り方、提供する情報の内容や取扱い等の運用については、基幹インフラ事業者等のみならず中小企業や地方公共団体を含む関係者の意見を幅広く聴取し、各主体が協議会への参加の意義を実感できる仕組みとなるよう制度設計を進めること。」とされた。

また、外国企業の扱いについて問われた内閣官房は、「本法案の目的の達成のためには、電子計算機の使用者のみならず、製品ベンダやセキュリティベンダについても協議会に参加してもらい、脆弱性情報や対策情報を共有することが必要になる。そうしたベンダには、外国企業も多いことを考えれば、協議会に参加してもらうことは当然あり得る。ただし、情報管理等に係る措置が十分に講じられない可能性がある者については、そもそも協議会構成員に加えない運用になろうかと思っている」旨答弁した[57]。

ウ　協議会における情報窃取防止策

機微情報の窃取を目的に協議会に入ろうとする者を排除する仕組みの必要性について平国務大臣は、「協議会の情報の中には、攻撃者の詳細な活動状況やインフラ設備の具体的な脆弱性など、秘匿性の高い情報も含まれることが想定されている。このため、協議会の設置目的に照らして構成員を検討することとしており、本法律案においては、内閣総理大臣が必要と認めるときに限り、事業者をその同意を得て協議会に加入させることができることとした上で、協議会構成員に対しては一定の情報管理や守秘義務を義務付けることとしている。さらに、一定の機微な情報については適切な情報管理の下で事業者が取り扱えるようにするため、セキュリティ・クリアランス制度の活用についても必要な検討を進めていく考えである。内閣総理大臣がコントロールするので、懸念のある者は入れないという運用になろうかと思う」旨答弁した[58]。

（７）官民連携において民間事業者の協力を得る必要性

官民連携については、民間事業者に意義を実感してもらい、協力が得られるようにすることが重要とされる。この点、平国務大臣は、「民間事業者は、協議会に参加することによって、例えば、サイバーの専門家が求める技術情報といった即応性を重視した短期的な対処に必要な情報や、経営者の判断に必要な攻撃目的等に関する情報といった中長期的な対策に必要な情報を政府から適切なタイミングで受け取ることが可能となる。政府から構成員に対しては、適時適切に情報を共有することにより、民間事業者が協議会に参加するメリットを明確に感じることができるよう、協議会における情報共有の具体的な在り方等につい

多くの分野の事業者等が出席し、大規模になると考えられる協議会の運営方法について内閣官房は、「会議形式であれば、サイバーセキュリティの分野は通常、参集型とオンライン型をうまく使い分けながら効率的に行う会議が多いと思う」、「また、情報共有システムをうまく活用することも考えながら進めたい。また、分科会、グループ構成といったものを考えながら、基幹インフラ事業者の分野や業種、業態に応じた構成といったものも考えていく必要があろうかと思う」などと答弁した（第217回国会参議院内閣委員会会議録第11号（令7.4.24））。この点、参議院内閣委員会で持永大参考人（芝浦工業大学システム理工学部准教授）は、「オンラインで会議をやるというのが一つの方向性としてある」、「セキュリティが保たれたインターネット上の情報共有基盤があって政府側からの情報が見られる、定期的に政府側から案内が届くなど、時間を拘束しない方法もある」旨述べた（第217回国会参議院内閣委員会会議録第12号（令7.5.8））。

57 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

58 第217回国会参議院内閣委員会会議録第10号（令7.4.22）

てはしっかりと検討を進めていきたい」旨答弁した[59]。

併せて、平国務大臣は、「官民双方向での情報共有を推進するために、被害情報の提供などに貢献いただいた事業者が否定的に捉えられることがなく、肯定的に評価されることが重要である。このため、法案の施行に当たっては、被害情報の意図しない流出を防止するため、安全管理措置に万全を期すことはもちろんであるが、その上で、例えば協議会において、積極的に情報提供を行った事業者をサイバーセキュリティの向上に貢献しているとして評価する環境を整備するといった工夫が重要と考えている」旨答弁した[60]。

また、民間事業者の協力を得るために事業者側にもメリットがもたらされるようにするため、丁寧な説明を求められたのに対して石破総理からは、「法案の策定に当たっては、有識者会議や個別の意見交換の場を通じて、事業者や専門家の方々から様々な意見を頂戴し、経団連、日本商工会議所も、本法案は経済界の意見も踏まえた内容となっているという認識を示している。下位法令においてインシデント報告の具体的な範囲など運用の詳細を定めていく際にも、事業者や専門家の方々の御意見をよく承り、また政府側からも改めて政策の背景などについて丁寧に分かりやすく説明することにより、民間の理解、協力を確保していきたい」とし、さらに「官民連携の推進のために、事業者が政府と連携することにメリットを感じてもらわなければならないので、協定を締結した事業者には通信情報の分析結果を提供することとなるが、事業者がサイバーセキュリティを確保する上で有意な情報が提供できるように、経済界の意見をよく承りながら法の的確、適切な運用に努めていきたい」旨の答弁があった[61]。

（８）中小企業を含むサプライチェーン全体におけるサイバーセキュリティ対策

我が国全体のサイバーセキュリティ向上に向けては、サプライチェーンを構成する基幹インフラ事業者以外の事業者の対策も必要であり、特に中小企業向けの支援等が必要であるとの指摘があった。平国務大臣は、「我が国の経済の基盤となる中小企業のサイバーセキュリティ対策の強化は喫緊の課題であり、サプライチェーン全体の防護の観点からも重要であると認識している。サイバー対処能力強化法案においては、サイバー攻撃による被害の防止のために必要があると認めるときは基幹インフラ事業者以外の事業者に対しても国が適切な情報提供を行うこととしているほか、情報共有、対策のための官民による協議会を設置することとしており、中小企業等を含めたサイバーセキュリティ対策の強化を図っていく」旨答弁した[62]。

また、中小企業のサイバーセキュリティ対策に関する既存の支援策及びその周知について、経済産業省は「例えば、セキュリティ対策に自分が取り組んでいるということを宣言するセキュリティアクションについては、令和３年度末時点から令和７年２月までの間に約21万件、宣言数が増えている」とした。さらに、中小企業に必要な対策を安価かつワン

---

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11号（令7.4.24）
61 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
62 第217回国会参議院内閣委員会会議録第10号（令7.4.22）

パッケージにまとめたサイバーセキュリティお助け隊サービスについて、「令和３年度末時点では利用実績は数百件であったものが、令和６年９月末時点では約７千件にも上っている。今後、更にサイバーセキュリティ対策を定着させていくためには、まだその必要性を感じていない中小企業、リソースに限りのある中小企業への細やかな対応が不可欠であると認識している。このため、経済産業省としては、産業界や関係省庁、支援機関とも連携しながら、その周知のため、リーフレット作成や政府広報の実施、サプライチェーン・サイバーセキュリティ・コンソーシアム[63]などを通じた中小企業団体等への強化、中小企業とセキュリティ専門家のマッチングなどに取り組んでいきたい」旨答弁した[64]。

この点、参議院附帯決議では、「二十一　サプライチェーンへのサイバー攻撃に対する強靭性を高めるため、基幹インフラ事業者等のみならず、サプライチェーンを構成する中小企業の体制整備とそれに伴う費用、的確なアドバイス等の経済的、人的支援を強化すること。特に、基幹インフラ事業者と取引のある中小企業については支援を適切に行うこと。」とされた。

（９）人材の育成・確保

我が国全体のサイバーセキュリティ向上に向けては、英国等の取組も参考に、人材の確保・育成に取り組んでいく必要性等が指摘された。これについて内閣官房は、「現在、政府においては、サイバーセキュリティ人材が担う役割や職種ごとに必要となる知識やスキルを体系的に整理､明確化することにより人材の可視化を図る枠組みの整備を検討している。その上で、この枠組みを例えば研修プログラムの提供や求人などの場面において官民が利用することによって、官民両者が連携して必要な人材育成、確保策を講じていけるような環境整備を行っていく予定としている。また､本年11月､若手人材向けの国際的なサイバー競技会であるインターナショナル・サイバーセキュリティ・チャレンジ（ＩＣＣ）を、ＮＩＳＣと民間のサイバーコミュニティーから成る準備委員会の両者の共催によって開催することを予定している。この大会を通じて、有望な若手がサイバーセキュリティ分野を志してもらえる流れも促進していきたい。これらの取組を通じて､引き続き､官民一体となってサイバーセキュリティ人材の育成や確保に取り組んでいきたい」旨答弁した[65]。また、文部科学省は、「文部科学省においては、平成29年度より、全国の大学、高専において数理、データサイエンス、ＡＩ教育を推進していく中において、令和４年度よりサイバーセキュリティ推進校を選定して、セキュリティに関するリテラシーを高める教材の開発、その展開等を支援している。また、大学・高専機能強化支援事業によって、意欲のある大学や高専においてサイバーセキュリティに係る高度情報専門人材の育成も含む学部、学科等の再編や定員増の支援も行っている。引き続き、関係省庁と連携しながら、今後ともサイバーセキュリティ人材の育成を推進していく」旨答弁した[66]。

---

[63] 同コンソーシアム（ＳＣ３）は、産業界が一体となって中小企業を含むサプライチェーン全体でのサイバーセキュリティ対策の推進運動を進めていくことを目的として令和２年11月に設立された。
[64] 第217回国会衆議院内閣委員会議録第７号（令7.3.21）
[65] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
[66] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

この点、参議院附帯決議では、「二十二　サイバーセキュリティ人材の確保及び育成については、経営層にサイバーセキュリティの重要性に対する理解を促し、同人材の地位向上や処遇改善につなげる取組を通じて強力に推進すること。」とされた。

５．小括

本稿では、能動的サイバー防御の２法律案の全体像と官民連携の強化に関する国会論議を整理してきた。

官民連携の強化では、民間事業者との情報共有を強化することが柱の一つとされている。他方、現行のサイバーセキュリティ基本法の下でもサイバーセキュリティ協議会が設置されるなど、これまでも一定の取組が進められてきたが、その実効性が課題となってきた。新たな制度によって政府からの情報提供を強化することで、官民連携を意義あるものとできるかが、サイバーセキュリティ向上のポイントとなろう。

また、今回の協議会は主に基幹インフラ事業者等が対象とされていると思われるが、中小企業等に対しても、十分な情報提供や支援を行い、サプライチェーン全体でサイバーセキュリティを強化していくことが重要となる。中小企業がサイバーセキュリティ強化のための取組を進めていくためには、協議会での情報共有のみならず適切な支援も必要となろう。関係する府省も多岐にわたることから、政府一体で取り組んでいくことが求められる。

加えて、官民連携の強化と通信情報の利用及びアクセス・無害化措置は相互に関連しており、各制度が一体として機能することも重要な点である。政府が民間事業者等と情報共有を行うためには、政府が必要な情報を取得し、十分な分析を行うことが不可欠であり、その前提として、通信情報の利用に関する取組が機能する必要がある。また、アクセス・無害化措置を実施する場合には、攻撃者の正確な情報が必要となるが、端緒となる情報がインシデント報告によりもたらされることも想定される。これら全体の制度が円滑に運用され、情報が迅速に共有されるよう、施行に向けて取り組んでいく必要があろう。

次号では、通信情報の利用及びアクセス・無害化措置について取り上げる。

（えのもと　なおゆき）