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～
著者 / 所属	柿沼　重志・榎本　尚行 / 内閣委員会調査室
雑誌名 / ISSN	経済のプリズム / 1882-062X
編集・発行	参議院事務局 企画調整室（調査情報担当室）
通号	239 号
刊行日	2024-10-17
頁	1-40
URL	https://www.sangiin.go.jp/japanese/annai/chousa/keizai_prism/backnumber/r06pdf/202423901.pdf

※ 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 75044）／ 03-5521-7683（直通））。

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～

内閣委員会調査室　柿沼　重志・榎本　尚行

《要旨》

本稿では、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が令和６年８月７日に公表した「これまでの議論の整理」を基に、①官民連携の強化、②通信情報の利用、③アクセス・無害化措置の３点及び横断的課題の一部を取り上げ、能動的サイバー防御に係る制度構築の方向性と課題について整理する。

１．はじめに[1]

「国家安全保障戦略」（令和４年12月16日国家安全保障会議決定、閣議決定）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」とされた上で、能動的サイバー防御[2]の導入が明記された。

能動的サイバー防御の導入に向けて、同戦略では、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、下記の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（図表１）。

図表１　能動的サイバー防御の導入に際しての主な取組

（ア）　重要インフラ分野（注）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。
（イ）　国内の通信事業者が役務提供する通信に係る情報を活用し、攻撃者による悪用が疑われるサーバ等を検知するために、所要の取組を進める。
（ウ）　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

[1] 本稿は、令和６年10月８日の脱稿時点までの情報に基づき執筆している。また、国内のことについては和暦を用い、海外のことについては西暦を用いる。

[2] 能動的サイバー防御については、本稿２．（２）能動的サイバー防御の概念と導入に向けた課題を参照。

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。

（注）重要インフラのサイバーセキュリティに係る行動計画（令和６年３月８日サイバーセキュリティ戦略本部改定）に基づき、現在15分野が指定されている。
（出所）国家安全保障戦略より一部抜粋

令和５年１月31日、内閣官房サイバー安全保障体制整備準備室が設置され、能動的サイバー防御の導入に向けた検討が進められることとなった。他方、第213回国会（令和６年常会）の提出予定法案のリストには、能動的サイバー防御を導入するための法案が検討中の法案として掲載されていたが、令和６年５月の時点でも同法案の提出には至っていなかった。この点について、岸田文雄内閣総理大臣（当時）からは「能動的サイバー防御の実現に向けた法案については、現行法令との関係等も含め、通信の秘密との関係等の多岐にわたる事項を検討しており、可能な限り早期に法案を提出できるよう、検討を加速しているところである。国家安全保障戦略にも掲げているように、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、こういった目標に向けて引き続き努力をしていきたい」旨の答弁があった[3]。

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」が設置された。翌７日、第１回有識者会議が開かれ、岸田総理（当時）からサイバー安全保障分野を担当する河野太郎国務大臣（当時）に対して、有識者会議の成果を踏まえ、関係大臣とも協力の上、可能な限り早期に関連法案を取りまとめるよう指示があった。

有識者会議はその後、テーマ別の会合[4]を開催するなどして議論を進め、令和６年８月７日に「これまでの議論の整理」を公表している。

本稿では、有識者会議の「これまでの議論の整理」を基に、能動的サイバー防御に係る制度構築の方向性と課題について考察する。

２．サイバー攻撃の特性と能動的サイバー防御の概念

（１）サイバー攻撃の特性

サイバー攻撃には、攻撃者の優位性、瞬時拡散性、越境性といった３つの特性があるとされている（図表２）。

[3] 第213回国会参議院内閣委員会会議録第12号36頁（令6.5.9）
[4] 図表１（ア）、（イ）及び（ウ）に対応する形で、官民連携に関するテーマ別会合、通信情報の利用に関するテーマ別会合、及びアクセス・無害化措置に関するテーマ別会合が行われた。

図表２　サイバー攻撃の特性

特性１：攻撃者の優位性

攻撃元隠蔽の技術的容易性

○　マルウェアに感染させるなどして不正に外部から制御できるようになった通信機器を多数、多段的に組み合わされて構成された攻撃用のネットワーク（いわゆるボットネットワーク（注））を構成し、攻撃に利用

○　攻撃の受け手側からの追跡が困難

攻撃側と防御側の非対称性

○　攻撃側：手法や対象を自由に選択可能
　防御側：広範な攻撃手法や攻撃対象を想定した防御策が必要

○　攻撃側と防御側の非対称性から、防御側はサイバー攻撃が行われていることを認識することさえ困難な可能性

特性２：瞬時拡散性

○　グローバルなサプライチェーンを経由する製品・サービスの拡大・浸透、産業分野でのＩｏＴ機器の利用拡大（あらゆるモノがネットワークに接続されるようになること）等により、サイバー攻撃が発生した場合の経済社会活動への影響は、瞬時に、かつ、より広範に、多様な主体・場面に及ぶおそれ

特性３：越境性

○　サイバー攻撃は、攻撃元と被害発生地との地理的なつながりが希薄、国境を越えて事案が発生

○　安全保障環境の激しさが増す中、サイバー攻撃による重要インフラの機能停止や破壊、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている

（注）ボットとは、様々な作業を自動化するプログラムのことであり、感染してしまうと、そのコンピュータはボットネットの一部となってしまう。また、ボットネットワークは、ボットに感染したコンピュータと、攻撃者の命令を送信する指令、サーバによって構成されたネットワークのことであり、攻撃者はボットに感染したコンピュータに対して一斉に同じ指令を与えることができる（図表14も参照）。

（出所）通信情報の利用に関するテーマ別会合（第１回）資料より作成

（２）能動的サイバー防御の概念と導入に向けた課題

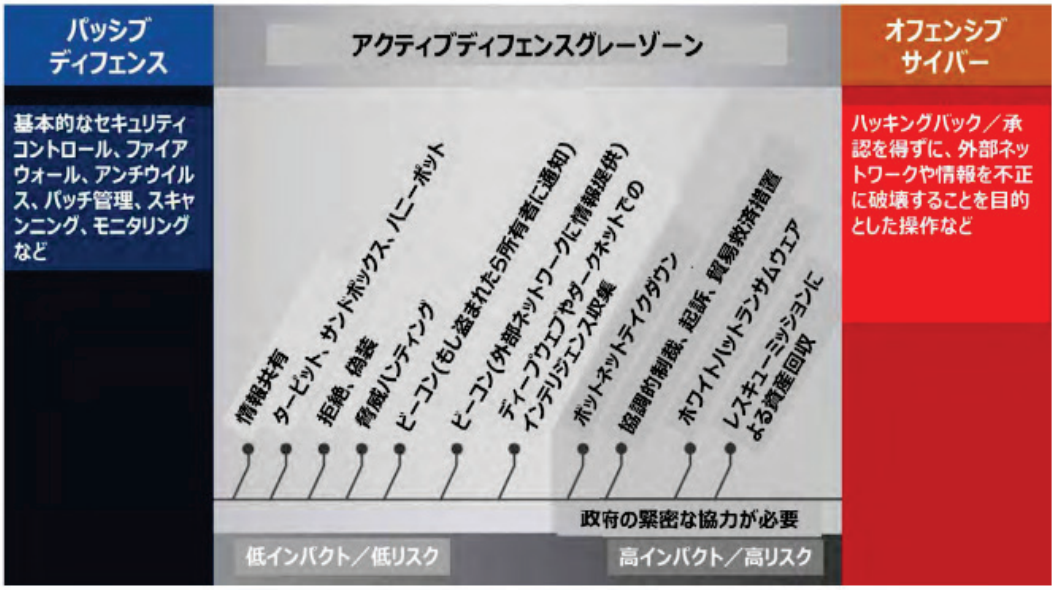
攻撃者の優位性、瞬時拡散性、越境性といった３つの特性を踏まえると、サイバー安全保障分野における対応能力の向上に当たっては、政府としてサイバー攻撃の実態を的確に把握し、防御側に対する施策を強化するにとどまらず、アクセス・無害化措置を含め、攻撃側への対処を強化する必要性や国際法との関係に留意する必要性が世界的に認識されてきた[5]。従前からの受動的サイバー

[5] この点に関連し、日本経済新聞は、「サイバー攻撃は狙う対象や方法によっては武力攻撃に匹

防御の強化だけではサイバー空間の安全を担保できないことを受け、米国、英国及びドイツ等では受動的なサイバー防御に加えて、ＡＣＤ（アクティブ・サイバー・ディフェンス）が実施されている[6]。

ＡＣＤの概念を精緻化した2016年のジョージ・ワシントン大学のプロジェクトによる整理では、“Cyber Operations（サイバー作戦）”について、自己の情報ネットワーク内における対策を“Passive Defence”、攻撃者の情報ネットワーク内での妨害・破壊を“Offensive Cyber（サイバー攻撃）”とそれぞれ位置付け、両者の間のグレーゾーンにある対策を“Active Defence”と整理している（図表３）。

図表３　ジョージ・ワシントン大学のプロジェクトによる整理



（出所）国立大学法人政策研究大学院大学政策研究院「個別調査分析２　サイバーセキュリティ領域」『「我が国が戦略的に育てるべき安全・安心の確保に係る重要技術等の検討業務」報告書』（令5.3）36頁

ジョージ・ワシントン大学のプロジェクトによる整理を始めとして、アカデミックな世界においては、ＡＣＤについては「サイバーインシデントが発生す

敵する攻撃を持つ。イメージダウンや防御レベルを知られるのを懸念して被害を公表しない事例が多いだけに政府主導で守る体制が欠かせない」と指摘している（『日本経済新聞』（令6.2.8））。

[6] 主要国の実施状況については、森秀勲「サイバー攻撃の脅威とサイバー安全保障－能動的サイバー防御の制度構築に向けた課題－」『立法と調査』No.462（令5.12）121～124頁を参照。

る前、または発生している最中に攻撃者に関与する対応」との定義がよく使われている[7]。

図表３のアクティブディフェンスグレーゾーンには、脅威ハンティング[8]等を始めとしたサイバー攻撃の主体を特定する活動を指すアトリビューションに関する措置が列挙されているほか、特定のウェブサイトやサーバを無効化又は削除することを指すテイクダウンやサイバー空間外の法執行として、協調的制裁、起訴、貿易救済措置等が挙げられている。

こうした海外での先行的な研究や実際の取組も踏まえ、国家安全保障戦略において、能動的サイバー防御の導入が掲げられた。内閣官房サイバー安全保障体制整備準備室が有識者会議で示した資料では、能動的サイバー防御を導入するための現行制度上の課題について、①官民連携の強化、②通信情報の活用、③アクセス・無害化措置の３点に分類して提示され（図表４[9]）、これらの取組を実現・促進するため、強力な情報収集・分析・対処調整機能を有する新たな司令塔組織を設置することが必要とされている。

図表４　能動的サイバー防御の導入をめぐる現行制度上の課題

①官民連携の強化 **高度な侵入・潜伏能力に対抗するため、政府の司令塔機能、情報収集・提供機能の強化が不可欠** ◆整理が必要な法令の例：サイバーセキュリティ基本法（平成26年法律第104号）、各種業法
②通信情報の活用 **悪用が疑われるサーバ等の検知には、「通信の秘密」を最大限に尊重しつつも、通信情報の活用が不可欠** ◆整理が必要な法令の例：日本国憲法第21条第２項（通信の秘密）
③アクセス・無害化措置 **重大なサイバー攻撃の未然防止・拡大防止を図るためには、政府に侵入・無害化の権限を付与することが不可欠** ◆整理が必要な法令の例：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）

（出所）有識者会議（第１回）資料より作成

[7] 大澤淳「サイバー領域の安全保障政策の方向性」笹川平和財団新領域研究会編『新領域安全保障　サイバー・宇宙・無人兵器をめぐる法的課題』（株式会社ウェッジ、令和６年）187頁

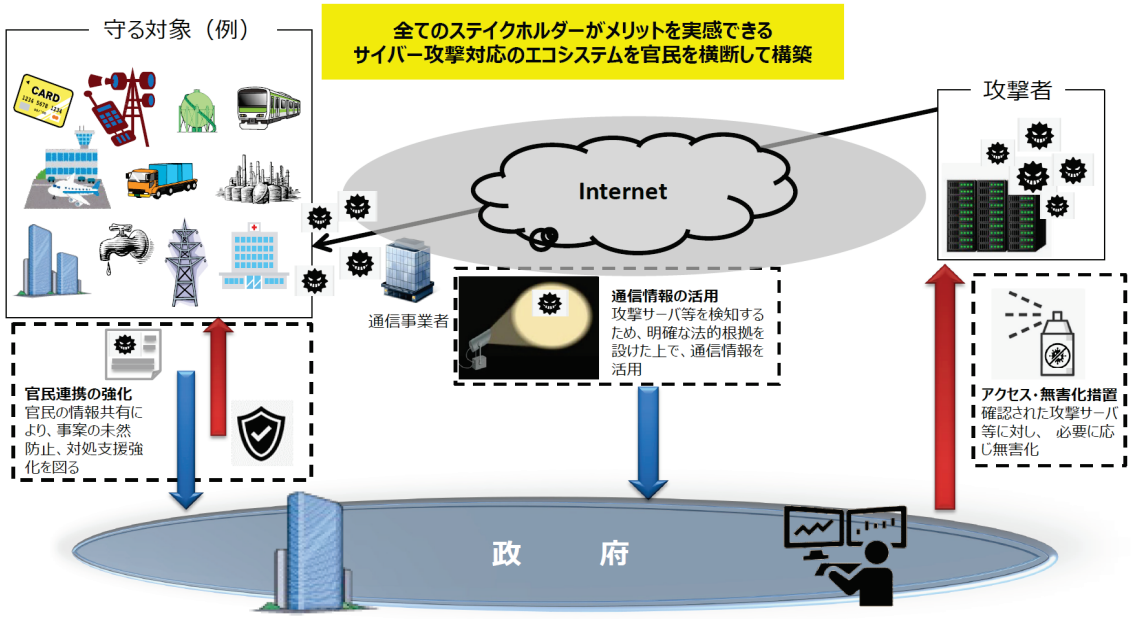
[8] 脅威ハンティングとは、従来のセキュリティ対策をくぐり抜ける可能性のある潜在的な脅威を特定し、無力化するように設計されたプロアクティブ（主体的に対応を実践する）なセキュリティ戦略のことを指す。

[9] ３点はそれぞれ、図表１で示した国家安全保障戦略の（ア）～（ウ）の取組に対応している。

３．能動的サイバー防御の導入をめぐる現行制度上の課題

以下では、令和６年８月７日に公表された有識者会議の「これまでの議論の整理」のうち、諸外国の事例も踏まえ、①官民連携の強化、②通信情報の利用、③アクセス・無害化措置の３点のほか、横断的課題の一部[10]についても取り上げる（図表５）。

図表５　全体イメージ



（出所）有識者会議（第１回）資料より一部抜粋

３－１．官民連携の強化

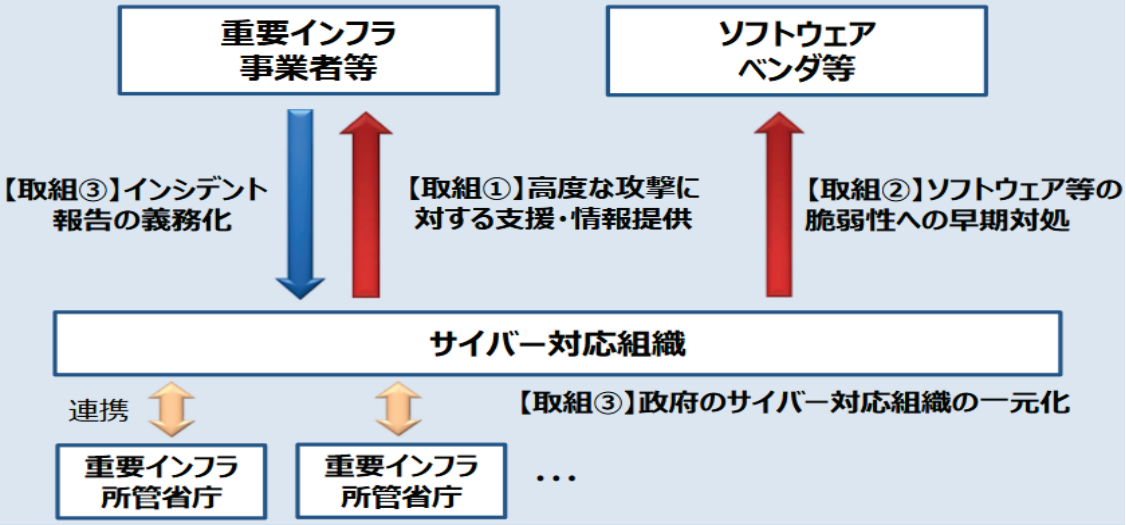
サイバー攻撃が発生した場合の海外主要国の取組を整理すると、①高度な攻撃に対する支援・情報提供、②ソフトウェア等の脆弱性への早期対処、③インシデント報告の義務化・政府のサイバー対応組織の一元化といった３つに集約される（図表６）。近年、海外主要国では官民連携が進み、高度なサイバー攻撃に対する支援・情報提供や、ゼロデイ脆弱性[11]の早期対処に必要な枠組みを強

[10] 横断的課題として、①サイバーセキュリティ戦略本部・ＮＩＳＣ（内閣サイバーセキュリティセンター）・関係省庁が連携した施策の推進、②重要インフラ事業者等の対策強化、③政府機関等の対策強化、④サイバーセキュリティ人材の育成・確保、⑤中小企業を含めた対策強化、⑥その他の論点の６点が挙げられているが、本稿では紙幅の都合もあり、経済や産業の観点から特に重要であると考えられる①、②及び⑤について取り上げることとする。

[11] ソフトウェアに見つかったセキュリティ上の脆弱性の中でも、その存在が公表される前や修正用プログラムがリリースされる前の脆弱性を指す。

化してきているとされる。

図表６　サイバー攻撃が発生した場合の海外主要国の取組



（出所）官民連携に関するテーマ別会合（第１回）資料より一部抜粋

（１）対応能力向上のための官民連携の必要性

対応能力向上のための官民連携の必要性については、①重要インフラ等への攻撃の高度化、②重要インフラ等のデジタル化、③社会全体の強靭化の必要性の３つの観点から議論が整理されている（図表７）。

図表７　対応能力向上のための官民連携の必要性

①重要インフラ等への攻撃の高度化 ・サイバー攻撃は**一段と巧妙化、高度化、複雑化、組織化されている**ことが顕在化している。 ・攻撃の高度化に伴い、**近年の攻撃は単純なインディケータ情報（注）の共有では検知や対策が困難**になってきている。 ・現状、**インシデントの報告窓口は複数存在**しており、一刻を争う状況の中で、報告コストを下げるため、**窓口の一本化やフォーマットの統一**が求められる。
②重要インフラ等のデジタル化 ・**重要インフラのＤＸが進んだ結果**、インターネット等への依存が高まり、**サイバーセキュリティのリスクも高まった**。 ・重要インフラを守ることの大きな目的は、**国民視点でサービスが持続的に提供される**ということ。
③社会全体の強靭化の必要性 ・サプライチェーン全体を考慮したとき、**国家のレジリエンスを確保するためには、数の上で90%以上を占める中小企業の対策は絶対的に必要**。 ・セキュリティ人材の重要性が叫ばれて久しいが、**セキュリティ分野に実際に人材が流入するような状況にはなっていない**。

・**国家のサイバーセキュリティの力**とは、その国における**サイバーセキュリティ人材の層の厚さ**である。

（注）攻撃者のＩＰアドレス等のハッシュ値（特定のアルゴリズムによって生成される不規則な文字列）など、攻撃者による侵害の痕跡を探すための指標となる情報。
（出所）「これまでの議論の整理」

有識者会議（第１回）資料では、「サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い。」との情勢認識が示されている。こうした情勢認識の下、有識者会議では、「鉄道など、サプライチェーンも含めて主な担い手は監督官庁ではなく民間」であり、「官民が連携して重要インフラのサスティナビリティを保っていくということが特に重要になる」、また、「これまでの情報窃取型だけではなく、システムを停止させるタイプの攻撃が増えてきている。重要インフラ事業者を含め民間事業者にとって、サイバーリスクは事業継続を損なうリスクになりつつある。」等の議論が行われている[12]。

（２）高度な攻撃に対する支援・情報提供

高度な攻撃に対する支援・情報提供については、政府の役割、提供されるべき情報、情報提供の方法について、それぞれ整理されている（図表８）。

図表８　高度な攻撃に対する支援・情報提供

＜① 政府の役割について＞
・サイバー攻撃による業務継続性への影響や事業者間の相互依存関係を考慮し、日本全体の強靭性を最大化できるよう、リスクコミュニケーションや支援を行うべきではないか。
・情報共有は社会全体の強靭性を高める上で最重要であり、被害組織が情報提供するインセンティブの設計が必要。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、官民双方向の情報共有を促進すべきではないか。
＜② 提供されるべき情報について＞
・高度な侵入・潜伏能力を備えた攻撃に対し、事業者等が具体的行動を取れるよう、攻撃者の動向を踏まえつつ、アナリスト向けの技術情報に加え、経営層が判断を下す際に必要な攻撃の背景や目的なども共有すべきではないか。

[12] 有識者会議（第１回）議事要旨５～６頁

・近年の攻撃は、単純なインディケータ情報の共有では検知や対策が困難であり、脅威ハンティングを効率的に行えるよう、攻撃者の手法に関する具体的情報の提供も必要ではないか。

＜③ 情報提供の方法について＞

・セキュリティクリアランス制度の活用や情報共有ポリシーの設定により、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はないか。
・緊急性の高い情報発信は、発信機関ごとに差異が生じないよう、ワンボイスで行うべきではないか。また、友好国との間での相互運用性に配慮すべきではないか。

（出所）「これまでの議論の整理」概要

海外主要国では、情報提供を政府の役割として明確化しているとされる。具体的には、これまで行われてきた攻撃検知に必要なインディケータ情報の提供に加え、高度なサイバー攻撃に対し、事業者等が具体的行動を取りやすいよう、インテリジェンス情報等に基づく脅威ハンティングの支援が実施されているほか、攻撃背景等の経営層の意思決定に有用な情報提供も実施されるなど、事業者側のインセンティブを考慮した設計が行われている（図表９）。

図表９　政府の役割としての「情報提供の在り方」（海外主要国の事例）

- ✓ 「具体的な行動に結びつく情報の適時の共有は、機密性のあるものを含め、事業者等によるリスク管理に不可欠」【米：重要インフラに係る国家安全保障覚書 (NSM-22, 2024年)】
- ✓ 「事業者等が具体的な行動を取れるような規模と頻度で脅威情報を提供」【英：国家サイバー戦略 (2022年)】
- ✓ 「政府は、専門知識と機密情報源へのアクセスを活用し、事業者等による高度なサイバー脅威への対処を支援」【豪州サイバーセキュリティ戦略 (2023年)】

（出所）官民連携に関するテーマ別会合（第１回）資料より一部抜粋

我が国で従前から行われている取組としては、業界ごとの情報共有・分析を行う組織（ＩＳＡＣ）の編成や、サイバーセキュリティ基本法の規定に基づき、原則システムを活用して脅威情報等の共有・分析、対策情報等の作出・共有等を迅速に行うサイバーセキュリティ協議会の取組がある。この取組は、事業者が持つ情報や分析内容を持ち寄る仕組みとされている。

また、提供方法に関連して、令和６年の常会で、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、我が国においても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が整備された。能動的サイバー防御とセキュリティクリアランス制度の関係について、岸田総理（当時）

からは「能動的サイバー防御の実現に当たっては官と民の連携が重要であると認識をしており、サイバー安全保障分野におけるセキュリティクリアランス制度の活用も含め検討を進めていく。」旨の答弁があった[13]が、サイバー防衛における同盟国・同志国との政策協調の観点からもセキュリティクリアランス制度の活用は極めて重要であろう[14]。

（３）ソフトウェア等の脆弱性対応

ソフトウェア等の脆弱性対応については、ベンダ[15]の責務及び脆弱性情報等の提供に分類して整理されている（図表10）。

図表10　ソフトウェア等の脆弱性対応

＜① ベンダの責務について＞
・安全な製品開発や脆弱性の対応に関するベンダの責任を規定すべきではないか。
・官民が連携してゼロデイ脆弱性を早期認知・対処できるよう、システム開発やセキュリティ監視等を担うベンダとの連携を深めるとともに、観測基盤を強化すべきではないか。
・攻撃を受けたソフトウェアベンダからユーザーに被害が拡散する「サプライチェーン攻撃」を防ぐため、海外事例等も参考に、安全性のテスト基準などベンダの規律を設定し、セキュアな製品の提供や脆弱性情報の報告等を求めるべきではないか。
・ＩｏＴ機器等の中小ベンダは資源が限定的であり、厳しい価格競争も踏まえると、単にベンダに責任を負わせるのではなく、セキュアな製品開発・供給にあたっての支援も検討すべきではないか。
＜② 脆弱性情報等の提供について＞
・侵害有無の調査方法や緩和策など、ベンダが提供すべき情報を整理すべきではないか。
・事業者等が膨大な脆弱性情報の中から優先順位を付けられるよう、国内で悪用されている脆弱性情報を一元的に分かりやすく発信すべきではないか。
・国民生活等の基盤となる事業者については、政府が資産情報を把握し、関連するゼロデイ情報等を速やかに提供する枠組みを構築すべきではないか。

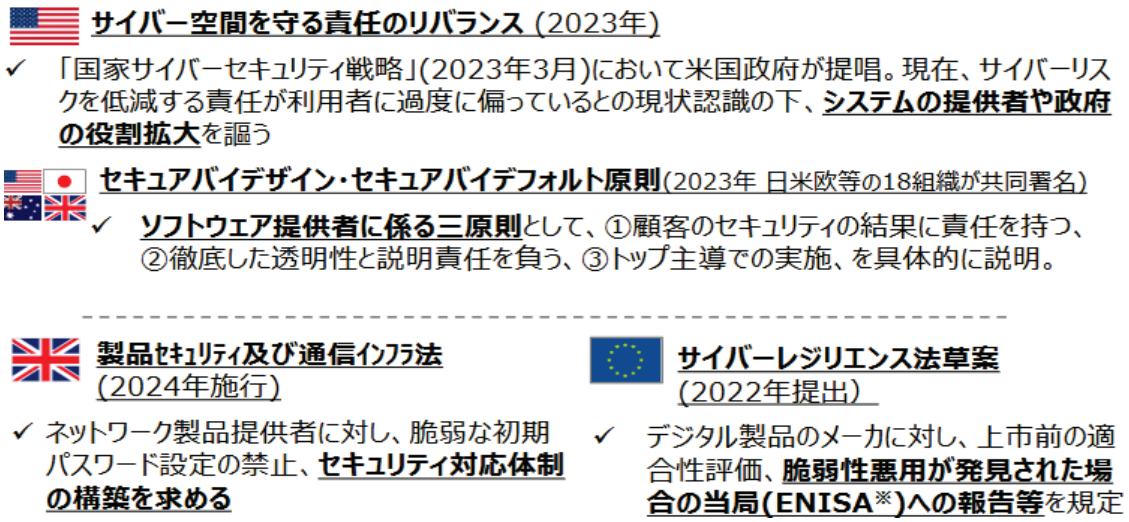
（出所）「これまでの議論の整理」概要

[13] 第213回国会参議院本会議録第12号10頁（令6.4.17）
[14] こうした点に関連して、2022年11月に米国メリーランド州アナポリスで開催された日米ＮＥＸＴ同盟イニシアティブの会議において、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＞）。
[15] 主に製造元、販売供給元のことを指す。

特に、安全な製品開発や脆弱性の対応に関するベンダの責任について、海外では責務の明確化や法的義務の導入の動きが顕著である（図表11）。

また、ソフトウェア等の脆弱性に対して早期に対応する観点から、海外では、米国において政府が既知の脆弱性情報を一覧化して公表する取組が行われるなど、踏み込んだリスク情報の提供が行われるようになっているとされる。

図表11　ベンダの責任を明確化するための海外主要国等の事例



（注）ENISA：欧州連合サイバーセキュリティ機関

（出所）官民連携に関するテーマ別会合（第１回）資料より一部抜粋

（４）政府の情報提供・対処を支える制度

政府の情報提供・対処を支える制度については、以下の指摘がなされている（図表12）。

図表12　政府の情報提供・対処を支える制度

＜① インシデント報告の義務化、情報共有を促進する仕組みについて＞

・重要インフラのデジタル依存度が増していることを踏まえれば、継続的なサービス提供のため、影響の大きさに応じ、インシデント報告を義務化し、情報共有を促進すべきではないか。デジタルインフラと電力は特に重要なインフラとして扱うべきではないか。

・インフラ以外の事業者についても、国内外での情報窃取事案や、サプライチェーンにおける重要性等に鑑みれば、官民の会議体を設置するなど、情報共有を促進する仕組みを設けるべきではないか。

・その制度設計に際しては、ＩＳＡＣやサイバーセキュリティ協議会等の既存枠組の効果を検証すべきではないか。また、現場レベルで官民の対応者が集結できる仕組みが必要ではないか。

＜② インシデント報告の迅速化について＞
・被害組織の負担軽減と政府の対応迅速化を図るため、インシデント報告先の一元化や報告様式の統一化、速報の簡素化を進めるべきではないか。
・有効な対処には、数分・数十分というタイムスケールでの迅速な情報収集・共有が必須であり、インシデント報告において自動化技術を活用すべきではないか。
＜③ 報告された情報の取扱いについて＞
・報告された情報は、経営上機微な情報を含み得るため、慎重に取り扱うべき。報告された情報の利用目的を明確化し、情報の不用意な流出や制裁目的での利用防止を規定すべきではないか。

（出所）「これまでの議論の整理」概要

官民の会議体について、例えば米国ではＪＣＤＣ（官民サイバーセキュリティ協力枠組）が2021年に設置され、政府機関とセキュリティベンダ、グーグルのようなビッグテック等が連携し、情報共有が行われてきている[16]。こうした海外の先行的な取組を参考にして、我が国においても制度設計が行われると考えられる。

また、インシデント報告の迅速化については、特に、サイバー対応組織及びインシデント報告先の一元化が欧米主要国では進展しており、その際には、報告先集約化による負担軽減を図る仕組みが整備されている（図表13）。

図表13　サイバー対応組織等の一元化に関する欧米主要国の事例

（出所）官民連携に関するテーマ別会合（第１回）資料より一部抜粋

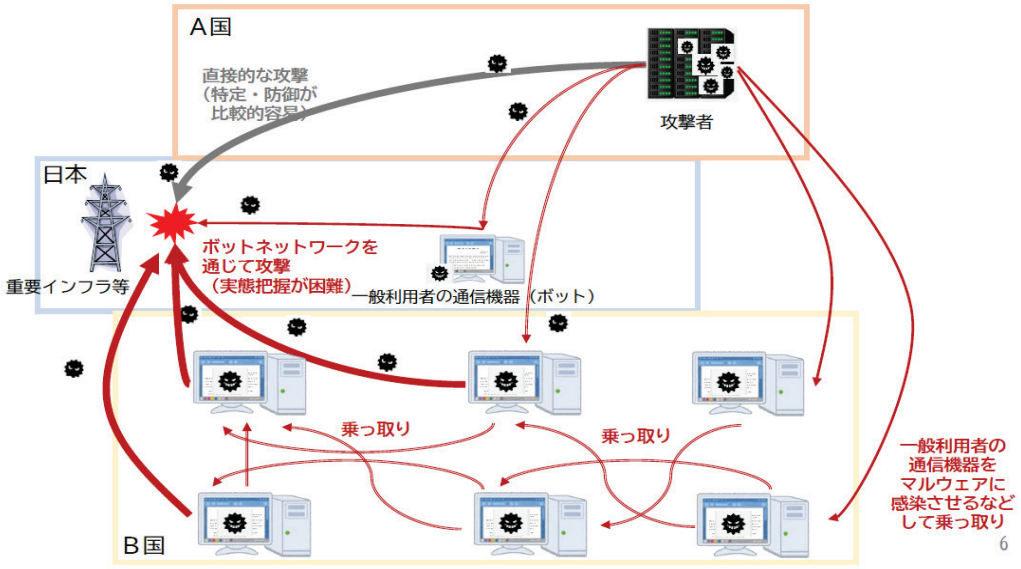
[16] ＪＣＤＣでは、未公開情報を官民で共有し、起こり得る危機のシナリオを共同で研究している。また、ＮＴＴ（日本電信電話株式会社）も 2022 年 12 月にメンバーに加わっている（『読売新聞』（令 6.6.17））。

３－２．通信情報の利用

（１）通信情報の利用の必要性

攻撃者は、攻撃元を隠蔽するため、一般利用者の乗っ取られた通信機器で構成されるボットネットワーク等を攻撃に利用することが通常とされる。攻撃者が存在する国（A国）とは別の国（B国）の通信機器を経由して、攻撃が行われる場合が多く、その実態を把握することが困難とされる（図表14）。

図表14　想定されるサイバー攻撃の経路の例（イメージ）



（出所）通信情報の利用に関するテーマ別会合（第１回）資料より一部抜粋

こうした状況を踏まえ、通信情報の利用について、平時から分析することにより、ボットネットワーク等の攻撃の実態を把握することが必要であるとされている（図表15）。

図表15　攻撃実態解明のための通信情報利用の必要性

- 一般利用者の乗っ取られた通信機器で構成されるボットネットワーク等の攻撃の実態を把握するためには、通信情報の分析が必要。また、その分析は、平時から行うことが必要ではないか。
- 国家安全保障等の観点からサイバー攻撃対策のためにも通信情報を利用している先進主要国の状況に鑑み、日本でも、重大なサイバー攻撃への対策のため独自の分析を行えるよう、一定の条件の下での通信情報の利用を検討することが必要ではないか。
- 通信情報利用は先進主要国との連携でも有意義。日本の能力向上は国際的にも要請されている。

（出所）「これまでの議論の整理」概要

（２）通信の秘密との関係及び独立機関の在り方

サイバー空間における通信情報の種類について、有識者会議では以下に分類され、通信情報の利用について議論が行われている（図表16）。

図表16　サイバー空間における通信情報の種類

１　電気通信設備等を識別する情報
送信日時、ＩＰアドレス、ポート番号、ドメイン名等
２　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
不正なＣ２コマンド、エクスプロイトコード[17]、マルウェア等
３　その他機械的な情報
プロトコル、通信量、端末が使用するブラウザやＯＳの種類等
４　個人のコミュニケーションの本質的内容に関わる情報
電子メール本文・件名、添付ファイルの内容・名称、ＩＰ電話の通話内容、Webサイトに掲載されている文章や画像等

（出所）通信情報の利用に関するテーマ別会合（第１回）資料より作成

通信の秘密について、憲法第21条第２項後段では、「通信の秘密は、これを侵してはならない。」と規定されている。また、これを具体化するものとして、電気通信事業法（昭和59年法律第86号）第４条第１項において「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。

通信の秘密を保障する範囲については、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれる[18]。一方で、通信の秘密の保障も絶対的なものではないと解され、内閣法制局長官が「通信の秘密はいわゆる自由権的、自然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ものであるということだが、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て一定の制約に服すべき場合があるというふうに考えている。」旨答弁している[19]。また、通信の秘密の侵害に当たらない場合としては、通信の秘密の侵害について通信当事者の有効な同意がある場合があるほか、法令行為等に該当する場合には違法性が阻却され[20]、通信の

---

[17] プログラムのセキュリティ上の脆弱性を攻撃するために作成された簡易なプログラムの総称。

[18] 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12頁

[19] 第213回国会衆議院予算委員会議録第３号12頁（令6.2.5）

[20] 刑法（明治40年法律第45号）には、「法令又は正当な業務による行為は、罰しない。」（第35条）等と規定されている。

秘密の侵害が許容される[21]。これらを踏まえた法制度を検討する必要がある。

有識者会議では、犯罪捜査のための通信傍受に関する法律（平成11年法律第137号。以下「通信傍受法」という。）に基づく通信傍受の仕組みが参考とされている。通信傍受法においては、傍受の要件[22]が定められているが、「通信傍受法による通信傍受は、電話番号やメールアドレスなどにより特定され、傍受令状に記載された通信手段に対して行うが、サイバー攻撃対策では、攻撃元の隠蔽が容易というインターネットの技術的特性の下で、ボットネットワーク等の攻撃の実態を把握することがまず必要となるため、攻撃に関連する通信に用いられるＩＰアドレス等をあらかじめ特定して実施することは通常困難と考えられる。」とされている[23]。

これらを踏まえ、利用する通信情報の対象について議論がなされている。「これまでの議論の整理」における通信の秘密との関係に係る記載は以下のとおりである（図表17）。

図表17　通信の秘密との関係

・通信の秘密であっても、法律により公共の福祉のために必要かつ合理的な制限を受ける。 ・具体的な制度設計の各場面において、丁寧な検討を行うべき。 ・先進主要国を参考にしながら、緻密な法制度を、作り上げていくことが必要ではないか。 ・定められた規律の遵守を確保するための仕組みが必要ではないか。明確で詳細なルールも重要ではないか。 ・情報処理の各プロセス（実施過程）でどのような統制や規律が必要なのか、整理していくべき。 →先進主要国では、準備・承認、電気通信事業者への措置、処理・分析、共有、廃棄等の一連の実施過程が法律で定められ、独立機関が監督。

[21] 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13頁

[22] ①一定の重大な犯罪（対象犯罪）が犯されたと疑うに足りる十分な理由があり、②当該犯罪の実行に関連する通信（「犯罪関連通信」）が行われると疑うに足りる状況がある場合で③他の方法によっては、犯人の特定、犯行の状況・内容を明らかにすることが著しく困難である場合に④裁判官の発する傍受令状により⑤被疑者が使用している又は犯人による犯罪関連通信に使用されると疑われる特定の通信手段について、⑥これを用いて行われる犯罪関連通信の傍受をすることができる、とされている。

[23] 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14頁。このほかに通信の秘密に関連して参照される取組としては、総務省、国立研究開発法人情報通信研究機構（ＮＩＣＴ）等が連携してＩＤ・パスワードに脆弱性があるＩｏＴ機器の調査を行うNOTICEが挙げられる（NOTICEの概要は<https://notice.go.jp/>参照）。NOTICEは、ＩｏＴ機器と第三者との間の通信の内容等を知得、窃用又は漏えいするものではなく、通信の秘密の侵害には該当しないとされている（第201回国会衆議院安全保障委員会議録第３号11頁（令2.4.3））。

・独立機関は重要。各国の司法制度等との関係や日本の他法での類例を含め、検討していくべきではないか。
・なお、通信の秘密の制限に対する通信利用者の有効な同意がある場合の通信情報の利用は、憲法上許容される。その場合の同意の在り方は更に検討していく必要があるが、制度により規格化された内容による同意が方法として考えられるのではないか。

（出所）「これまでの議論の整理」概要

これに対して、海外主要国の制度については、以下のとおりである（図表18）。通信情報の取得要件が定められているほか、取得した情報を分析することのできる範囲について、国内や自国民に関する分析が禁止されている例があることが注目される。

図表18　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

※1 上記の制度は、主要国において、個別具体的な調査対象を事前に特定せず、通信情報を調査できる法的枠組の例。
（これら以外に存在しないという趣旨ではない）
※2 公表済の各国法令の条文を参照して作成。各国政府の確認を経たものではなく、また、各国政府による対策の実態まで示すものではない。

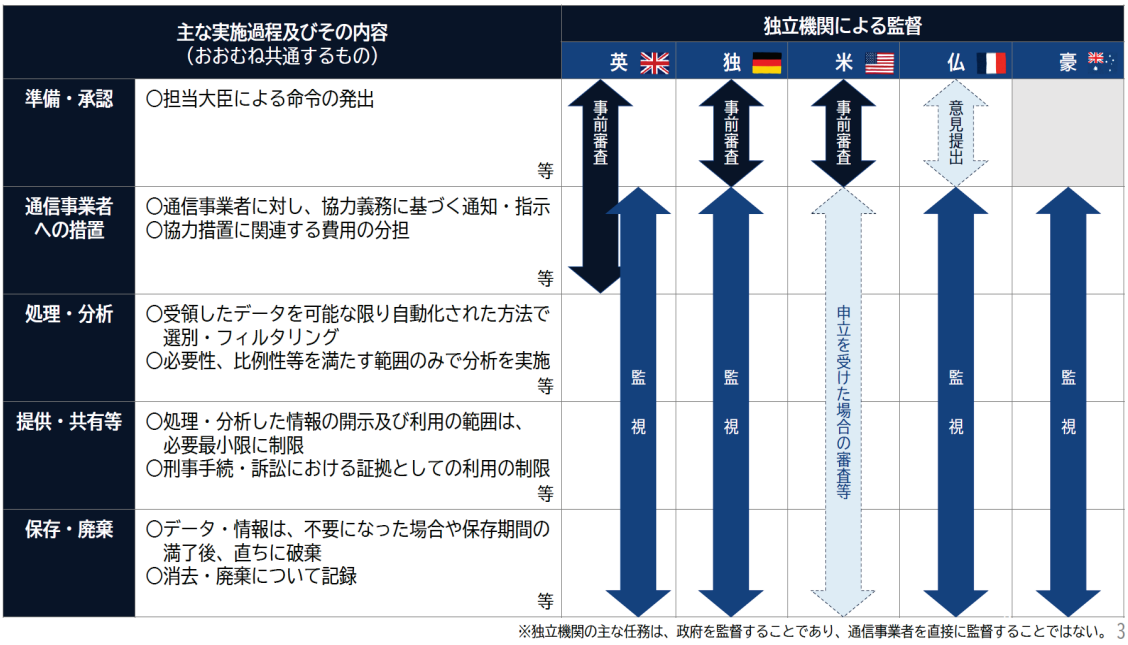
9

（出所）通信情報の利用に関するテーマ別会合（第１回）資料より一部抜粋

また、海外主要国における通信情報の利用の実施過程については、おおむね共通するものとして、「①開始前の準備・承認、②通信事業者への通知・指示等の措置、③受領したデータの処理・分析、④処理・分析した情報の提供・共有等、⑤データ・情報の保存・廃棄の各段階」とされ、これらの各段階について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（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とされている（図表19））。

図表19　海外主要国における通信情報の利用の実施過程と独立機関の関わり



（出所）通信情報の利用に関するテーマ別会合（第２回）資料より一部抜粋

（３）通信情報の利用の範囲及び方式

通信情報の利用の範囲及び方式については、以下のように整理されている（図表20）。

図表20　利用の範囲及び方式

- 外国が関係する通信の分析が特に必要。日本を経由する外国から外国への通信（トランジット通信）については先進主要国と同等の方法の分析をできるようにしておく必要があるのではないか。
- 制度全体として重大サイバー攻撃対策の観点で弱点がないものとなるよう検討していくべき。
- 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、特に分析する必要があるとまでは言えないのではないか。メールの中身を逐一全て見るようなことは適当ではないのではないか。
- 収集したデータ全てを人間の目で判断することは不可能かつ不適切。機械的な選別等が重要ではないか。最初は広く、懸念が見つかれば深くとの考え方が妥当ではないか。
- データ分析の技術、能力、設備等も重要。

（出所）「これまでの議論の整理」概要

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、特に分析する必要があるとまでは言えないのではないかと指摘されているとおり、「利用する通信情報は、インターネット上の住所に当たるＩＰアドレス（識別番号）や通信量の変化といった付随的な「メタ情報」を平時から収集する方向で調整」とされるほか、「各事業者に外国から国内への通信情報について、政府側への提供を求めて事前同意に基づいて取得し、監視する」、「事前同意を得る具体的な方法や、どの事業者を対象とするかなどの制度設計を急ぐ方針」との報道がある[24]。

（４）電気通信事業者の協力

通信情報の利用には電気通信事業者の協力が必要とされ、以下のように整理されている（図表21）。

図表21　電気通信事業者の協力

・協力を行う電気通信事業者は社会の安全のために貢献しているとして肯定的に評価されるべき。 ・電気通信事業者に求められる協力が、電気通信事業者の実施可能な範囲内になるよう、明確化していく必要があるのではないか。 ・電気通信事業者が直面し得るリスクや負担等について回避策を十分に検討していくべき。法整備により、国の責任で取り組むとすることが必要ではないか。 ・官民の適正な連携のためにも、独立機関等のガバナンスの仕組みを検討することが必要ではないか。

（出所）「これまでの議論の整理」概要

電気通信事業者の範囲については、有識者会議において「旧来型のキャリア以外にも、（中略）いわゆるプラットフォーマーと言われているような事業者からもデータを取れるようにするということも非常に重要だと思う。」との指摘があった[25]。また、電気通信事業者が直面し得るリスクや負担については、訴訟リスク、レピュテーションリスクや通信ネットワーク運営に対する負担が挙げられている。

３－３．アクセス・無害化措置

（１）国家安全保障戦略の方針と自衛権との関係

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

[24] 『東京新聞』（令6.7.24）、『読売新聞』（令6.8.12）
[25] 有識者会議（第３回）議事要旨５頁

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」において、そうした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。

武力攻撃に当たる場合について木原防衛大臣（当時）は、「武力攻撃に当たるかについては、その時点の国際情勢や、また相手方の明示された意図であるとか、あるいは攻撃の手段、態様等を踏まえて、個別の状況に応じて判断すべきものであると考えているが、その上で、一般論として言えば、サイバー攻撃のみであっても、例えば物理的手段による攻撃と同様の極めて深刻な被害が発生し、これが相手方により組織的、計画的に行われている場合には武力攻撃に当たり得る」旨答弁した[26]。この答弁から、能動的サイバー防御は、こうした要件に至らないサイバー攻撃が念頭に置かれていると考えられる。

（２）現行でとり得る対処策と実効的な制度構築の必要性

サイバー攻撃は、複雑化するネットワークにおいて、多数の通信とプログラム・データの複合的作用により発生している。その中で、ゼロデイ脆弱性の積極活用により制御系システムに至る高度な侵入能力や、システム内寄生戦術による検知回避等を用いた高度な潜伏能力を有するという実態があるとされる。これに対して、現行でとり得る対処策は以下のようなものに限定されている（図表22）。

図表22　現行でとり得る対処策

パブリック・アトリビューション等の外国機関と連携した対処	サイバー攻撃を受けた機器やサイバー攻撃に使用された不正プログラムを解析するなど、総合的な分析を行い、攻撃者や手口に関する実態解明を進め、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
任意のテイクダウン	サイバー攻撃に使用されたサーバ等を把握し、不正な機能を停止（テイクダウン）するよう、サーバ管理者に依頼
攻撃に利用され得る機器への対処	総務省及びＮＩＣＴは、ＮＩＣＴ法に基づき、電気通信事業者等と連携して、インターネットに直接接続されている機器がサイバー攻撃に悪用されるおそれのある場合に、利用者への注意喚起等により対処を促進
攻撃手口の公表	攻撃手口を公表し、広く一般に、あるいは、特定の事業者に対策を促すことで、サイバー攻撃を抑止

（出所）アクセス・無害化措置に関するテーマ別会合（第１回）資料を基に作成

[26] 第213回国会衆議院予算委員会議録第13号46頁（令6.2.22）

上記のとおり、サイバー攻撃に使用されたサーバ等のテイクダウンについては、国内に所在している場合であってもサーバ管理者を通じた任意のものにとどまる。国外に所在している場合には、所在国によっては必ずしも協力を得られるとは限らない等の制約がある。このため、例えば、サーバ管理者を通じて国内のサーバについて停止措置を講じたとしても、当該サーバが踏み台とされたものにすぎず、国外に別の指令関与サーバがある場合には、国外の指令関与サーバによる被害は止まないという状況が生じており、これに対処することが求められている。

こうした点を踏まえ、実効的な制度構築の必要性としては、以下のように整理されている（図表23）。

図表23　実効的な制度構築の必要性

・無害化措置は、我々が価値創造を行う安全なサイバー空間を守る観点で必要。 ・新制度は、被害の未然防止を目的とする重要なものであり、インシデントが起こってから令状を取得し捜査を行う、刑事手続の令状審査では対処できないのではないか。政治・外交等の手段も活用していく必要があることも踏まえ、行政作用法として規律されるのが妥当ではないか。また、従来の法執行システムと接合的で連続的な仕組みとして構想すべきではないか。 ・事象や状況の変化に臨機応変に対応し、講じるべき措置を変化させていく現場対応的な力が必要ではないか。個別の要件を法定し、あらかじめメニュー化された措置を講じる制度はなじまず、むしろ、状況に応じた措置を即時的に実施する現行の警察官職務執行法を参考とすべきではないか。その際には、執行に係る全体のプロセスやシステムも参考とすべきではないか。 ・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などのサイバー攻撃の特性から、事態を細かく区切り事態を認定するという従来の事態認定の方式ではなく、平素から我が国を全方位でシームレスに守るための制度の構築が必要ではないか。

（出所）「これまでの議論の整理」概要

アクセス・無害化に関して実効的な制度を構築する観点から、「これまでの議論の整理」では臨機応変の対応が重視されている。特に、一般的な刑事手続では迅速に対処することが難しいことから、警察官職務執行法（昭和23年法律第136号）を参考とした取組とすべきことが示されている。

刑事手続において強制力を有する捜査等を行う際には、基本的人権を守る観点から、裁判官の事前の司法審査に基づいて発付された令状によることが原則

とされる（令状主義）[27]。他方、警察官職務執行法では、警察官がその職権職務を遂行するための手段として、要件を付した上で、保護、避難等の措置、犯罪の予防及び制止、立入、及び武器の使用を認めている。

関連して「これまでの議論の整理」では、「警察官職務執行法を参考とするに当たっては、その背景や周辺にある警察制度、警察官の教練、日常の警らの活動、様々な制度の中で即時執行を可能にしているという視点が重要である[28]。サイバー空間においても、無害化措置という手法単体ではなく、連続するプロセスにおいて段階的な権限行使をしていく中で、無害化措置というものをどう位置付け、どう正当性を担保していくのか等の一連のプロセスとして議論していくべきではないか。」とされている。加えて、有識者会議の中でも「現実空間とサイバー空間における危険の顕在化には相当の違いがあることから、現行の警察官職務執行法そのままの形で当てはめるというのは難しく、法制度設計においては、サイバー空間の特性を踏まえた調整が必要であることには留意が必要。」との指摘もなされている[29]。こうした点を踏まえた検討が求められ、今後の議論が注目される。

また、「これまでの議論の整理」においては、状況に応じた措置を即時的に実施する方向で検討している一方で、措置の具体的内容については言及されておらず、資料でその具体的内容のイメージが一部示されるにとどまり、どこまでの行為を許容するかは具体的には示されていない[30]。

他方で、こうした行為は、不正アクセス禁止法[31]や刑法といった刑罰法規に

---

[27] 令状には、逮捕状のほか、強制的に住居等に立ち入り、犯罪と関連がある物を取得する捜査を許可する令状である捜索差押許可状等がある。

[28] 警察制度においては、警察法（昭和29年法律第162号）第２条第１項に「警察は、個人の生命、身体及び財産の保護に任じ、犯罪の予防、鎮圧及び捜査、被疑者の逮捕、交通の取締その他公共の安全と秩序の維持に当ることをもつてその責務とする。」との責務規定が置かれているほか、公安委員会による管理の仕組みが設けられている。

[29] アクセス・無害化措置に関するテーマ別会合（第２回）議事要旨４頁

[30] 有識者会議の資料では、具体的な措置の例として、不正プログラムそのものの消去、不正プログラムの停止のための変更、不正プログラムのみの停止、不正プログラムを消去するための通信機器の再起動といった取組が列挙されている（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５頁）。このほかにも、アクセス、脅威の特定、無害化措置の段階に分類された上で、アクセスにおいては、脆弱性等を利用したアクセス、アクセス用プログラムの送信、アクセス継続のためのユーザー設定等が、脅威の特定においては、プログラム一覧の確認、ログファイルの確認、コマンド実行履歴の確認等が、無害化措置においては、無害化プログラムの実行、不正プログラムの停止・変更・消去、攻撃者の再ログイン防止のための設定変更、攻撃者が利用するアカウント等の消去等がそれぞれ示されている資料も見られる（アクセス・無害化措置に関するテーマ別会合（第２回）事務局資料４頁）。

[31] 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）

抵触する行為が含まれることが想定される[32]。能動的サイバー防御として行われる行為がこれらの犯罪の構成要件に該当する場合に、法令行為とするなどの整理を行い、違法性を阻却する必要がある[33]が、他方で、既存の法律が保護しようとしている権利等にも配慮した制度構築が求められよう。

（３）措置の実施主体・対象

アクセス・無害化措置の実施主体については、防衛省・自衛隊や警察が念頭に置かれている。この点、「これまでの議論の整理」では、以下の内容が盛り込まれている（図表24）。

図表24　措置の実施主体・措置の対象

・諸外国での無害化措置の実行・運用主体を考慮すると、日本国内においては防衛省・自衛隊、警察等が保有する能力を活用すること、その能力を高度化することが極めて重要ではないか。 ・能力やリソースが限られることを勘案し、措置を講じる事案の優先順位付けを考える必要があり、国民の生命・安全に関わる重要インフラや有事において自衛隊や在日米軍の活動が依存する通信・電力などのインフラ等が優先順位が高いのではないか。 ・対象事案のスコープは、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を重視すべきではないか。

（出所）「これまでの議論の整理」概要

実施主体については、主に防衛省・自衛隊、警察等が保有する能力を活用するとされている。この点、防衛省・自衛隊に関しては、図表23でも触れられている「事態認定」との関係が議論されている。そもそも自衛隊の活動を規律する自衛隊法（昭和29年法律第165号）においては、自衛隊の行う活動がポジティブリスト方式で定められている[34]。また、武力攻撃事態を始めとする各事態については、事態対処についての各法律によってその要件、国会承認等の手続が

---

[32] 不正アクセス禁止法においては、不正アクセス行為を定義した上で、同法第３条で「何人も不正アクセスをしてはならない」と規定されている。刑法には、電磁的記録不正作出及び供用、不正指令電磁的記録作成等、電子計算機損壊等業務妨害といった犯罪が定められている。

[33] 前掲注20参照

[34] 自衛隊法では、同法第６章において、自衛隊の行動として、防衛出動、治安出動等が列挙されている。なお、防衛省における一般的なサイバー空間における情報収集については、特段の命令に基づくものを除き、防衛省設置法（昭和29年法律第164号）第４条第１項第４号（防衛及び警備等の事務に必要な情報の収集整理に関すること）及び第18号（所掌事務の遂行に必要な調査及び研究を行うこと）に基づき実施しているとされる（第213回国会衆議院安全保障委員会議録第４号９頁（令6.4.2））。

定められている。こうした現行制度との関係では、自衛隊がアクセス・無害化措置を行う場合においても、根拠となる何らかの法的措置が必要になることが想起される。一方で、「これまでの議論の整理」では「従来の事態認定の方式ではなく、平素から我が国を全方位でシームレスに守るための制度の構築が必要ではないか。」とされている。さらに、有識者会議においては、「平時と有事で境がないということは強調していただいているが、それに対処できる組織の在り方というのは、もう一段深めて議論する機会があるといいのかなと思う。事態認定の前後にこだわって、前はこの組織でやります、後になったらこの組織でやりますと言っている猶予は全然ない」との指摘もなされている[35]。

加えて、「仮に、リアルで事態が進行した場合、又は、リアルとサイバーで同時に事態が起こった場合、新しい概念との間で、どう整合性をとっていくのか。従来の法律を変える必要があるのか、自衛隊が出動して海外のサーバに無害化措置を行う場合、これとリアルがどのような関係になるのか概念をうまく整理して検討していく必要があるのではないか。」との意見[36]や、「事態認定方式をとらないとすると国の安全保障とサイバー防御を両立するシステム、国家安全保障とどう関係するか」、あるいは、「例えば自衛隊が無害化の措置を取る場合、これは海外での武力行使に当たらないのかといった疑問や批判もあるかもしれない。こうした部分も整理していただきたい。」との問題提起[37]もなされている。

（４）国際法との関係[38]

国際法との関係については、以下のように整理されている（図表25）。

図表25　国際法との関係

・措置により生じる影響、措置の目的、対象の性質等を加味して国際法上の違法性を考えなければならず、具体的にどの行為が他国の主権侵害に当たるかをあらかじめ確定することは困難。 ・他国の主権侵害に当たる場合の国際法上の違法性阻却事由として、実務上は対抗措置法理よりも緊急避難法理の方が援用しやすいのではないか。 ・アクセス・無害化措置は国家実行として国際法規則の形成に影響を与える。サイバー空間での活動の特徴を踏まえ、慎重に法制度の発展が図られるべきではないか。

（出所）「これまでの議論の整理」概要

[35] 有識者会議（第３回）議事要旨５頁
[36] アクセス・無害化措置に関するテーマ別会合（第２回）議事要旨５頁
[37] 有識者会議（第３回）議事要旨11頁
[38] 前掲注６・127～128頁も参照。

令和３年５月28日に外務省から公表された「サイバー行動に適用される国際法に関する日本政府の基本的な立場」では、国連憲章全体を含む既存の国際法はサイバー行動にも適用されるとの考え方が明らかにされている。また、サイバー行動における国際法上の違法性阻却事由[39]のうち、特に対抗措置、緊急避難の取扱いについて、「国際違法行為に対し対抗措置をとることは、一定の条件の下で、国際法上認められている。」、「ILC[40]国家責任条文25条に示された要件に合致する場合には緊急避難を援用することも国際法上認められていると考える。」とそれぞれ整理されている。なお、「これまでの議論の整理」では、能動的サイバー防御への緊急避難の援用を積極的に捉える記載が見られる一方で、国際法上の確立したルールが存在するわけではなく[41]、慎重に法制度の発展が図られるべきであることも指摘されている[42]。

（５）制度構築に当たっての留意点

制度構築に当たっての留意点[43]については、以下のように整理されている（図表26）。

図表26　制度構築に当たっての留意点

＜制度構築に当たっての留意点＞
- 無害化措置は、臨機応変な執行を可能としつつも、比例原則を遵守し必要な範囲で実施されるものであるべき。
- 透明性や公正性の担保、プライバシー保護、また、サイバー攻撃の特性に応じた執行の観点から、アクセス・無害化措置の適正性を確保する制度の検討（独立した立場からの監督など）、意図しない結果が生じた際の対応、現場における執行権限の必要性等に配意すべきではないか。

---

[39] 他国の主権侵害に当たる行為についての国際法上の違法性阻却事由については、行為の国家への帰属、国際法上の義務違反という２つの要件を満たす必要があるとされる（中谷和弘ほか『国際法〔第５版〕』（株式会社有斐閣、令和６年）144頁）。

[40] ILC(International Law Commission)とは国連国際法委員会のことである。

[41] サイバー行動に関する国際ルールについては、「タリン・マニュアル」が、包括的なルールを提示している。タリン・マニュアルは個人資格の有識者により作成され、拘束力を有しないが、外務省の文書でもその議論が踏まえられており、一定の権威を有しているとされる（タリン・マニュアルについては、中谷和弘ほか『サイバー攻撃の国際法―タリン・マニュアル2.0の解説―【増補版】』（株式会社信山社、令和５年）参照）。

[42] アクセス・無害化措置に関するテーマ別会合（第１回）議論の概要２頁。なお、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））。

[43] このほか、「これまでの議論の整理」では、制度の運用に当たっての留意点も整理されているが、紙幅の関係から本稿では省略する。

・個別のオペレーションに政治が個別に承認するのではなく、適切なポリシーの下で専門家集団がオペレーションを回せるようにする必要があるのではないか。

（出所）「これまでの議論の整理」概要

アクセス・無害化において適正性を確保する制度については、「現場で即時実力行使できるように警察・自衛隊に執行権限を行使する権限を与える場合、独立性を持った機関が事後監査を行うこととすべきではないか。」とされているにとどまる。この点について有識者会議では、「独立機関による事前審査、承認によらない現場対応が想定されていると思う。そうすると、法制度としては、警察官職務執行法を参考とした即時強制の制度づくり等が考えられるわけだが、この点に関して、現行の警職法には能動的サイバー防御を全く想定していないということもあり、国民の理解を得ていくための方策がいろいろ必要だろう。具体的には、こうした措置を取る場合に例えば警察であれば警察庁長官への報告をルール化するとか、独立した立場からの監督の仕組みが設けられるとか、あるいは、意図せず、あまり好ましくないような結果になった場合のその報告、判断を誤った場合などの事後報告についても、何らかのルール、制度が設けられると、そういった方向の議論、検討がさらに煮詰められるべきではないか」との意見が出されている[44]。

３－４．横断的課題として挙げられた課題

以下では、「これまでの議論の整理」で挙げられていた横断的課題のうち、①サイバーセキュリティ戦略本部・ＮＩＳＣ[45]・関係省庁が連携した施策の推進、②重要インフラ事業者等の対策強化、③中小企業を含めた対策強化の３点に絞り、整理を行う。

（１）サイバーセキュリティ戦略本部・ＮＩＳＣ・関係省庁が連携した施策の推進

サイバーセキュリティ戦略本部・ＮＩＳＣ・関係省庁が連携した施策の推進については、以下の点が指摘されている（図表27)。

図表27　サイバーセキュリティ戦略本部・ＮＩＳＣ・関係省庁が連携した施策の推進

・事案発生時の役割や基本的な方針等を決定する役割等を踏まえて、有識者等が助言

[44] 有識者会議（第３回）議事要旨12頁

[45] ＮＩＳＣ（National center of Incident readiness and Strategy for Cybersecurity）とは内閣サイバーセキュリティセンターのことで、平成27年１月に内閣官房に設置された。

をする別の組織を設けることを含め、サイバーセキュリティ戦略本部の構成の在り方等を検討すべきではないか。 ・関係省庁や地方公共団体等と戦略本部との役割分担や責任範囲を整理するとともに、関係省庁のサイバーセキュリティ部局が物理的に同じ場所で協働できるよう、基盤となるしっかりとしたインフラ（建物、スペース、勤務環境、セキュリティ等）の確保を図るべき。

（出所）「これまでの議論の整理」概要

１点目の指摘は、サイバーセキュリティ戦略本部の構成[46]の在り方等を検討すべきではないかとの指摘である。諸外国の官民連携の仕組みも参照しながら、司令塔になる部分とサイバーセキュリティの専門家の部分、それを全体としてチェックする第三者機関といった部分に詳細化することについて検討が進められると考えられる。

２点目は、関係省庁や地方公共団体等と戦略本部との役割分担や責任範囲を整理するとともに、各府省庁がサイバーセキュリティ部門を物理的に中央に寄せ、協働できるようなインフラの構築を図るべきとの指摘である。そうすることで、サイバー防御に対し迅速な対応が期待でき、現場に沿った制度改革が進められるという意図であると考えられる。

（２）重要インフラ事業者等の対策強化

重要インフラ事業者等の対策強化については、以下の点が指摘されている（図表28）。

図表28　重要インフラ事業者等の対策強化

・デジタル空間における位置づけ等を踏まえた重要インフラ分野の範囲等を検討すべきではないか。 ・サービスの継続とサプライチェーンを含めたレジリエンス強化の観点を踏まえて、政府が普段から重要インフラ等の国民生活や社会経済に対する影響度や相互依存関係を適切に把握し、必要な連携や優先度等を踏まえた対応ができるように備えるべきではないか。 ・基準・ガイドライン等の手法を活用し、分かりやすく取り組むべき事項の明確化が必要ではないか。 ・基準等については常に見直しを図るとともに、基準に対する取組状況を把握し、優れた取組を展開することを含め、実効性を高める仕組みを検討すべきではないか。

（出所）「これまでの議論の整理」概要

[46] 現行の構成については、本稿補論１．（４）を参照。

１点目は、現在15分野が指定されている重要インフラ分野の範囲[47]について、不断に見直しをすべきとの指摘である。

２点目は、政府が重要インフラの国民生活や社会経済に対する影響度や相互依存関係を適切に把握しておき、有事の時に官民でどのように連携するか、何を優先すべきかについて備えるべきとの指摘である。なお、中小企業を含むサプライチェーン全体のレジリエンス強化については、令和２年11月に、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指した「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（ＳＣ３）」が設立され、取組の検討や推進が行われている。

３点目及び４点目は、基準・ガイドライン等の一層の活用及び実効性を高める仕組みの検討についての指摘である。現在、「重要インフラのサイバーセキュリティに係る安全基準等策定指針[48]」があるが、同指針には遵守の実効性を確保する仕組みがあるわけではない。サイバー攻撃による被害を極小化するためにも、この点についても改善する必要があるという趣旨であると考えられる。

（３）中小企業を含めた対策強化

中小企業を含めた対策強化については、以下の点が指摘されている（図表29）。

図表29　中小企業を含めた対策強化

・社会全体の強靭性を高める観点で、基幹インフラのサプライチェーンなど中小企業のセキュリティ対策について、ツールの提供などを含めた支援を検討すべきではないか。 ・大企業が下請け企業のセキュリティ対策を要請することに関して、サプライチェーンセキュリティに関する独占禁止法（注）等の明確な整理を行うべきではないか。

（注）私的独占の禁止及び公正取引の確保に関する法律（昭和22年法律第54号）
（出所）「これまでの議論の整理」概要

１点目は、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靭性を高める観点からは、セキュリティ対策が遅れ

[47] 重要インフラ分野の沿革については、本稿補論２．（２）を参照。
[48] 重要インフラのサイバーセキュリティに係る安全基準等策定指針については、本稿補論２．（３）を参照。

ている中小企業[49]の対策強化が急務であり、政府による支援も検討すべきであるという指摘である[50]。

２点目は、大企業がサプライチェーンを構成する中小企業に対し、セキュリティ対策を要請することが、独占禁止法上の優越的地位の濫用や下請法[51]に抵触しないのか等について明確な整理を行うべきではないかという指摘である。

４．おわりに

平成26年のサイバーセキュリティ基本法の施行から約10年が経過し、その間、令和４年５月には、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。）が成立した。経済安全保障推進法による基幹インフラ制度[52]は、令和６年５月17日から届出義務の運用が開始された。この基幹インフラ制度は、電力を始めとした基幹インフラをサイバー攻撃等の妨害行為から防護するため、事業者が設備の導入等を行う場合には、事前に導入等計画書を届け出るとともに、事業所管大臣による審査を受けなければならないとする制度である。同導入等計画書では、導入する設備に関して、事業者がサイバー攻撃等の兆候を把握するための体制や、仮にサイバー攻撃を受けたとしても、サービス提供に支障がないようにする事業継続リスク対策が求められており、サイバーセキュリティとも関連が深い[53]。

---

[49] 令和６年７月８日に開催された有識者会議（第２回）では、中小企業のセキュリティ対策について「東京商工会議所で調査したものによれば、86%以上の企業が自分たちは何らかの対策はしているといった認識を持っているが、中身を見てみると、『ウイルス対策ソフトを入れている』とか『ソフトウェアを定期的にアップデートしている』といった基本的なレベルにとどまっていて、本当の意味の専門的な教育や訓練まで取り組んでいるのは３割以下と進んでいないのが実態である」旨の発言があった（議事要旨６～７頁）。

[50] 例えば、令和５年のランサムウェア（感染するとパソコン等に保存されているデータを暗号化して使用できない状態にした上で、そのデータを復号する対価を要求する不正プログラム）による被害（197件）を企業・団体等の規模別に見ると、中小企業は102件であり、全体の52%となっている（警察庁「令和５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6.3.14））。

[51] 下請代金支払遅延等防止法（昭和31年法律第120号）

[52] 重要インフラと経済安全保障推進法による基幹インフラは、大半が重なっているが一致していない分野がある。両者の違いについては、柿沼重志、小林惇「経済安全保障推進法制定後の動きと今後の課題－経済的威圧に対抗するための体制構築に向けて－」『立法と調査』No.461（令5.11）13～14頁を参照。

[53] 蔦大輔、新井雄也「基幹インフラ審査制度－サプライチェーン・サイバーセキュリティ」『ジュリスト』NO.1601（令6.9）36頁、40頁。なお、経済安全保障推進法上の特定重要設備に関しては、能動的サイバー防御の一環として、設備のネットワークに付けたセンサーの情報を政府側と共有し、サイバー攻撃の発生を即時共有する案も出ている旨の報道もある（『読売新聞』（令

重要インフラがサイバー攻撃を受けた際に顕在化するリスクの代表例としては、情報セキュリティリスクのほか、ランサムウェア等によってシステムが停止し、事業継続に影響が生じ得るという事業継続リスクが挙げられ[54]、サイバー犯罪はまさにこうしたリスクに狙いを定めたものが多いと思われる。

米国の戦略国際問題研究所（ＣＳＩＳ）とマカフィー[55]の調査によると、サイバー犯罪による2020年の世界全体の損失は１兆ドル超に上り、世界の国内総生産（ＧＤＰ）の１％を占めるとされている[56]。

サイバー攻撃によって、こうした経済的な損失を国家や企業がなるべく負うことがないようにするためには、サイバーセキュリティ基本法や経済安全保障推進法によって、中小企業を含めた社会全体でのサイバー攻撃に対する強靭化に向けた取組を一層推進することに加え、サイバー脅威への対応に向けた同盟国・同志国間の政策協調の動きを強化することが不可欠である。

以下、能動的サイバー防御の導入に当たっての主な課題を列挙する。

（１）民間事業者との情報共有の在り方

有識者会議での議論において、経済団体からは、現行において事業者は複数の政府機関にインシデント報告等を行っているとして、負担に留意した制度とすべきこと、また、サイバーセキュリティ基本法に基づくサイバーセキュリティ協議会の取組について早期に検証を行うこと等が指摘されている。既に情報共有の取組が行われていながら、情報共有が十分になされていない要因が明らかになっていない側面があると思われ、こうした点についての検証が急務である。

さらに、個人情報保護法制においては、漏えい事案の報告や本人への通知が事業者に義務付けられているが、サイバー攻撃を受けた場合、事業者は、サイバー攻撃への対処に加えて個人情報保護法[57]上の対応も求められる場合がある。こうしたインシデント報告が過度の負担につながらないよう、各制度を見渡して効率的な制度とすることも求められよう。加えて、有識者会議では、政府からの質の高い情報を求める声も上がっており、インテリジェンス機能の強化等も含め、双方向の情報共有が図られる体制づくりも求められる。

6.8.12)）。

[54] 蔦大輔、新井雄也「基幹インフラ審査制度－サプライチェーン・サイバーセキュリティ」（前掲注53）36頁

[55] コンピュータセキュリティ関連のソフトウェアとハードウェアを製作・販売する会社。

[56] 『日本経済新聞』（令6.2.8）

[57] 個人情報の保護に関する法律（平成15年法律第57号）

（２）セキュリティクリアランス制度との関係等

セキュリティクリアランス制度については、その活用が経済団体からも指摘されている。一方で、同制度では秘密保全が強く要請されており、秘密保全の要請と情報共有の迅速性をどのように両立、担保するのかが課題となろう。事業者には、秘密を取り扱うための施設整備や、従業者の適性評価などが求められるため、そうした負担の在り方も含め、効率的な制度設計が求められる。

また、能動的サイバー防御の制度を構築し、同制度が有効に機能するためには、同盟国・同志国間での情報交換・政策協調が重要であり、セキュリティクリアランス制度の活用も重要な鍵を握ると思われる。

（３）平時・有事の両局面における対応の在り方

能動的サイバー防御の議論においては、サイバー空間では平時と有事の境界が曖昧であることが強調されているため、既存の法制度を踏まえ、どのような対応を行うことができるようにするのか、今後の検討が注目される。その際、民間事業者に協力を仰ぐのであれば、どの段階でどのような行動をとっていくのかについて､事前に提示していくかといった論点も考えていく必要があろう。刑罰法規や国際的なルール等に抵触するリスクがないことを事前に示し、民間事業者が安心して協力できる制度づくりが求められる。

（４）国民の不安の払拭

特に通信情報の利用に関しては、プライバシーの侵害になるのではないかといった懸念が生じかねない問題であるが、こうした点については、取得した情報が漏えいしたり、他の目的で使用されたりしないための実効的な歯止めとなり得る独立機関（第三者機関）などを整備するとともに、サイバー攻撃に対応していくための措置は必要最低限にとどめるということを政府が真摯かつ丁寧に説明し、国民の不安の払拭を行っていくことが求められる。

（内線75103）

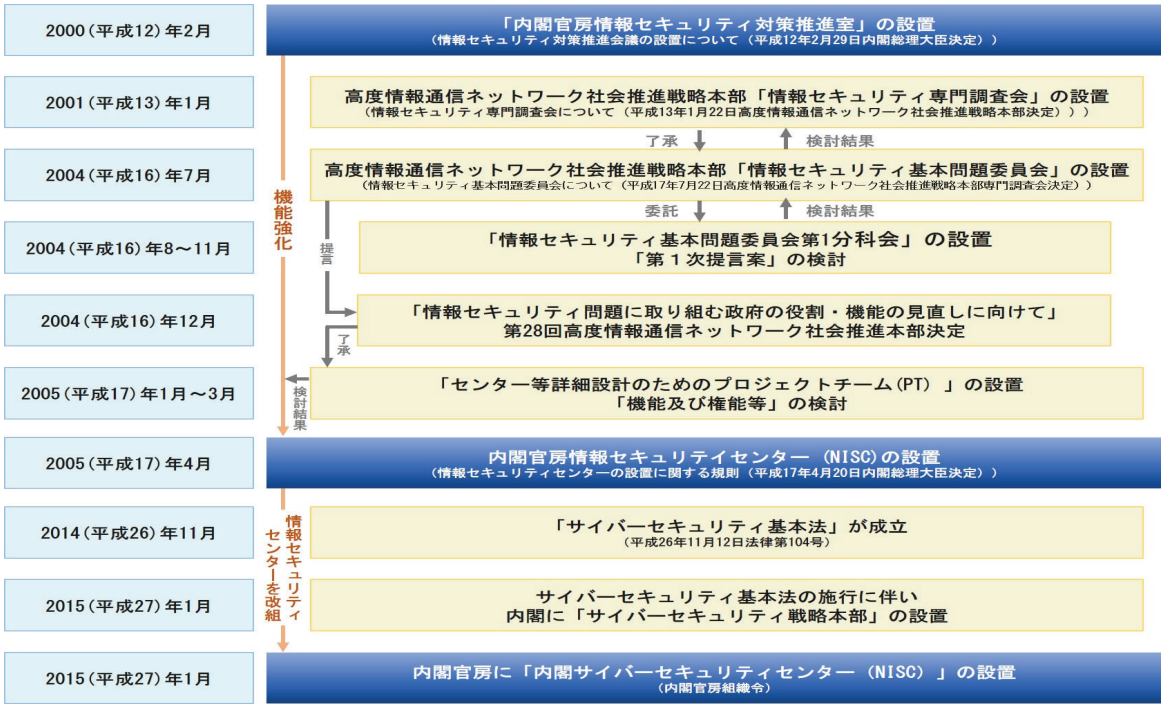
【補論】サイバーセキュリティ基本法と重要インフラ指定の沿革等

１．　サイバーセキュリティ基本法と同法に基づく戦略や組織

（１）サイバーセキュリティ基本法制定以前の推進体制

我が国のサイバーセキュリティ政策は、サイバーセキュリティ基本法に基づいて推進されている。同法の制定以前には、ＩＴ政策の推進について定めた高度情報通信ネットワーク社会形成基本法（ＩＴ基本法。平成 12 年法律第 144 号）[1]に高度情報通信ネットワークの安全性の確保等の規定が盛り込まれてはいたものの、サイバーセキュリティ政策自体に関する法律は制定されず、政府内でも、高度情報通信ネットワーク社会推進戦略本部（以下「ＩＴ総合戦略本部」という。）の下に設置された組織の下で[2]、サイバーセキュリティ政策の取組が進められてきた経緯がある（補論図表１）。

補論図表１　サイバーセキュリティ政策を担う組織の沿革



（出所）ＮＩＳＣウェブサイト

[1] ＩＴ基本法は令和３年にデジタル社会形成基本法（令和３年法律第 35 号）が成立したことに伴い、廃止された。
[2] 平成 17 年５月、ＩＴ総合戦略本部の下に情報セキュリティ政策会議が設置され、戦略の策定等を担っていた。

その後、国境を越えたサイバー攻撃等を背景として、我が国のサイバーセキュリティ対策の推進体制を抜本的に強化する必要性が認識され、平成26年11月、サイバーセキュリティ基本法が制定された。

（２）サイバーセキュリティ基本法の概要

サイバーセキュリティ基本法は、５章、38条から構成されている。同法の目的としては、大きく分けて、①経済社会の活力の向上及び持続的発展、②国民が安全で安心して暮らせる社会の実現、③国際社会の平和及び安全の確保並びに我が国の安全保障への寄与、の３点が規定されている（第１条）。また、「サイバーセキュリティ」については、情報、情報システム、情報通信ネットワークに着目した定義規定が置かれている（第２条）[3]。その上で、基本理念や基本的施策、推進体制等、我が国のサイバーセキュリティ政策を推進するための様々な規定が置かれている（補論図表２）。

補論図表２　サイバーセキュリティ基本法の構成

第１章　総則（第１条～第11条） 目的、定義、基本理念、関係者の責務等について規定
第２章　サイバーセキュリティ戦略（第12条） 同戦略に、サイバーセキュリティに関する施策の基本的な方針、重要インフラ事業者等におけるサイバーセキュリティの確保の促進等を盛り込むこと等を規定
第３章　基本的施策（第13条～第24条） 国等が行うべき基本的施策について規定 （平成30年の改正によりサイバーセキュリティ協議会に関する規定が新設。）
第４章　サイバーセキュリティ戦略本部（第25条～37条） 本部の所掌事務等について規定
第５章　罰則（第38条） サイバーセキュリティ協議会等に係る秘密保持義務違反

（出所）サイバーセキュリティ基本法を基に作成

[3] 具体的には、「電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）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に必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。」と定義されている。

なお、サイバーセキュリティ基本法は、これまでに、平成27年に発生した日本年金機構が不正アクセスにより個人情報を漏えいさせた事案を受け、平成28年に、国が行う不正な通信の監視、監査、原因究明調査等の対象範囲を拡大する等の改正が行われた[4]ほか、オリンピック・パラリンピック東京大会に向けた官民の情報共有体制の強化を図るため、平成30年にサイバーセキュリティ協議会を新設する改正などが行われてきている。

（３）サイバーセキュリティ戦略

サイバーセキュリティ戦略については、サイバーセキュリティ基本法制定以前から策定されてきており、平成25年６月10日、サイバーセキュリティ戦略が情報セキュリティ政策会議[5]で決定されていた。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に関する施策の総合的かつ効果的な推進を図るため、サイバーセキュリティ戦略を閣議決定すること等が規定された[6]ことから、平成27年９月４日、同法に基づく最初のサイバーセキュリティ戦略が閣議決定されている。次いで、平成30年７月27日及び令和３年９月28日に新たなサイバーセキュリティ戦略がそれぞれ閣議決定された。

現行のサイバーセキュリティ戦略では、「Cybersecurity for All」（誰も取り残さないサイバーセキュリティ）の確保に向けた取組を進める必要があるとの考え方の下で、①デジタル改革を踏まえたデジタルトランスフォーメーション[7]とサイバーセキュリティの同時推進、②公共空間化と相互連関・連鎖が進展するサイバー空間全体を俯瞰した安全・安心の確保、③安全保障の観点からの取組強化といった３つの方向性に基づき、施策を推進するとされた。

なお、同戦略は、「中長期的視点から、（中略）2020年代初めの今後３年間に

---

[4] この改正により、国の行政機関のほか、独立行政法人、特殊法人等が、国が行う監視、監査、原因究明調査等の対象となっている。

[5] 情報セキュリティ政策会議については、前掲注２を参照。サイバーセキュリティ基本法の施行により、同会議を改組する形でサイバーセキュリティ戦略本部が置かれることとなった。

[6] 同戦略には、①サイバーセキュリティに関する施策の基本的な方針、②国の行政機関等におけるサイバーセキュリティの確保、③重要インフラ事業者等におけるサイバーセキュリティの確保の促進、④その他、必要な事項を盛り込むことが規定されている。

[7] 「デジタルトランスフォーメーション」は、一般的にＤＸと略される。平成30年９月７日に経済産業省デジタルトランスフォーメーションに向けた研究会が取りまとめた「ＤＸレポート」においては、「企業が外部エコシステム（顧客、市場）の破壊的な変化に対応しつつ、内部エコシステム（組織、文化、従業員）の変革を牽引しながら、第３のプラットフォーム（クラウド、モビリティ、ビッグデータ/アナリティクス、ソーシャル技術）を利用して、新しい製品やサービス、新しいビジネス・モデルを通じて、ネットとリアルの両面での顧客エクスペリエンスの変革を図ることで価値を創出し、競争上の優位性を確立すること」と定義されている。

とるべき諸施策の目標や実施方針を示すものである」とされているとおり、定期的な改定を想定したものとなっている。

また、同戦略では、計画期間内の各年度の年次計画及び施策の進捗状況を検証した年次報告を取りまとめることとされている。令和６年７月 10 日にサイバーセキュリティ本部で決定された「サイバーセキュリティ 2024（2023 年度年次報告・2024 年度年次計画）」では、令和６年度特に強力に取り組む施策として、政府機関や重要インフラ等の対処能力の向上、サプライチェーン・リスクへの対応強化とＤＸを推進・支援する取組の強化、欧米主要国を始めとする関係国との連携を一層強化することが掲げられている。

（４）サイバーセキュリティ戦略本部

サイバーセキュリティ基本法の制定前に設置されていた情報セキュリティ政策会議は、ＩＴ総合戦略本部の下に置かれた組織であり、同政策会議の権限や機能は法律に基づくものではなかった[8]。

その後、サイバーセキュリティをめぐる情勢の変化を受け、政府において司令塔的な役割を担う政策会議の機能を強化し、各府省の情報共有、迅速な対応、連携等を図る必要が高まった。これを受け、サイバーセキュリティ基本法により、我が国におけるサイバーセキュリティに関する施策の司令塔となるサイバーセキュリティ戦略本部を置き、国の行政機関等における対策の実施状況に関する監査、重大事象に対する原因究明のための調査等を行う機能を持たせたとされる[9]。

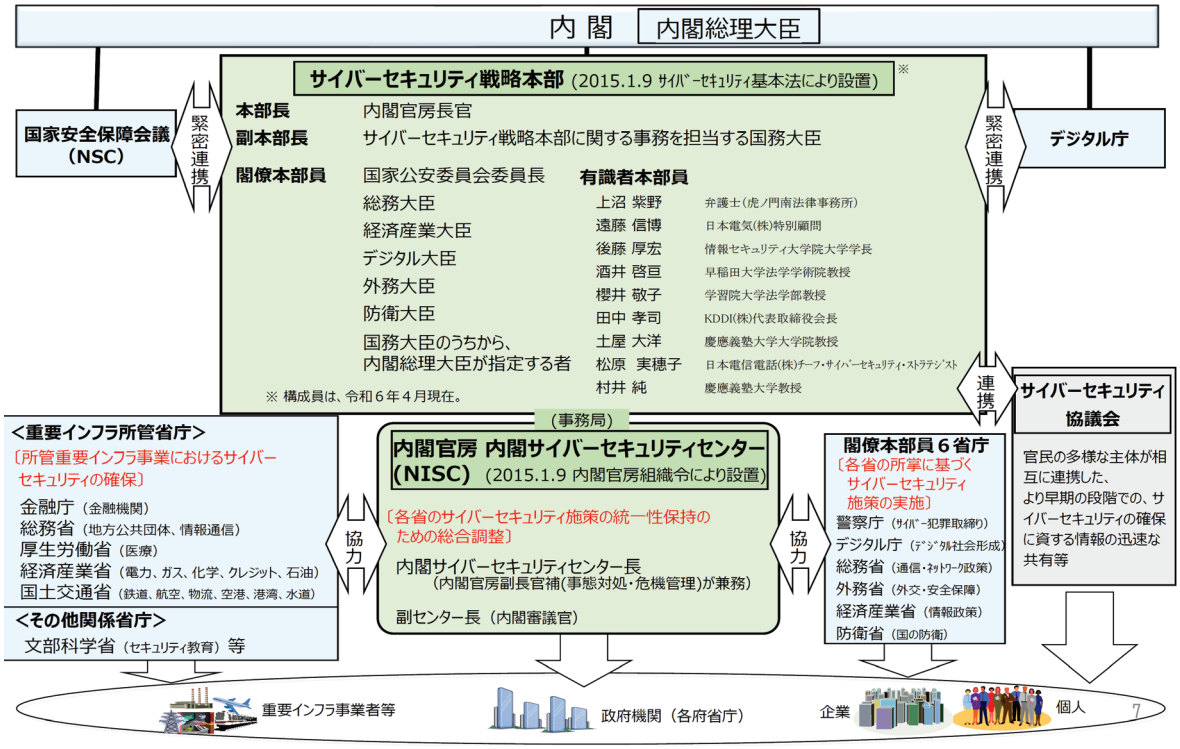
サイバーセキュリティ戦略本部の所掌事務は、サイバーセキュリティ戦略の案の作成等、国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準作成等、サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整等とされている（サイバーセキュリティ基本法第 26 条第１項）。

また、サイバーセキュリティ政策における推進体制の中核を成すのが、サイバーセキュリティ戦略本部であり、同本部は、国家安全保障会議やデジタル庁、サイバーセキュリティ協議会と連携を図っている。また、ＮＩＳＣは同本部の事務等をつかさどる（補論図表３）（サイバーセキュリティ基本法第 35 条、内

[8] 三角育生「サイバーセキュリティ基本法制定・改正の経緯」『日本セキュリティ・マネジメント学会誌』Vol.34,No.1（令 2.5）、30 頁を参照。
[9] 第 186 回国会衆議院内閣委員会議録第 23 号２頁（平 26.6.11）

閣官房組織令（昭和 32 年政令第 219 号）第４条の２）。

補論図表３　サイバーセキュリティ政策の推進体制



（注）内閣総理大臣は、閣僚本部員として経済安全保障担当大臣を指定
（出所）ＮＩＳＣウェブサイト

（５）サイバーセキュリティ協議会

サイバーセキュリティ協議会とは、我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行うことを目的としたものであり、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。

同協議会は、脅威情報等の共有・分析、対策情報等の作出・共有等を迅速に行うこととされている。なお、協議会の構成員になるためには、国の関係行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業者（主にセキュリティ関連事業者を想定）、大学・教育研究機関等であり、協議会の活動に賛同する者（事業者の団体等も含む）という要件を満たし、運営委員会（運営委員はサイバーセキュリティ戦略本部長等）の承認を得なければならないとされている。構成員は、令和元年５月 17 日に決定された 91 者から徐々に拡大を続け、

令和６年６月 13 日時点で 322 者となっている。

ＮＩＳＣは、同協議会の特徴として、①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体制、②システムを用いて情報共有等を行う「バーチャル協議会」、③直感的な違和感といった早期の段階からの情報提供、相談等を促進（構成員には、法律に基づく守秘義務（罰則付き）、情報提供義務が適用）、④ギブアンドテイクルールを徹底し、積極的な情報提供者へのメリットを増加[10]といった４点を挙げている[11]。

能動的サイバー防御の導入に向けても、官民連携の強化が大きな論点の一つとなっているが、サイバーセキュリティ協議会はまさに官民連携の仕組みであり、これを発展させる方向で制度設計が行われるものと考えられる。

２．重要インフラ防護に関する取組

（１）サイバーセキュリティ基本法上の重要インフラの位置付け

サイバーセキュリティ基本法では、重要社会基盤事業者及び重要社会基盤事業者等を以下のように定義している（同法第３条第１項及び第 12 条第２項第３号参照）（補論図表４）。

補論図表４　重要インフラ事業者の定義

重要社会基盤事業者	**国民生活及び経済活動の基盤であって、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ずるものに関する事業を行う者**
重要社会基盤事業者等	**重要社会基盤事業者及びその組織する団体並びに地方公共団体**

（出所）サイバーセキュリティ基本法を基に作成

なお、サイバーセキュリティ戦略本部が決定する「行動計画」（補論２．（２）を参照）では、重要インフラ事業者の定義について、同法第３条第１項に規定する重要社会基盤事業者をいうとしている。

また、重要社会基盤事業者や地方公共団体等の責務については、以下のように規定されている（同法第５条、第６条、第７条及び第９条参照）（補論図表５）。

[10] 積極的な情報提供に意欲と能力のある構成員を「タスクフォース」としてグループ化。
[11] <https://www.nisc.go.jp/pdf/council/cs/kyogikai/kyogikai_gaiyou.pdf>

補論図表５　重要社会基盤事業者等の責務等

重要社会基盤事業者の責務	基本理念にのっとり、そのサービスを安定的かつ適切に提供するため、サイバーセキュリティの重要性に関する関心と理解を深め、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とともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
地方公共団体の責務	基本理念にのっとり、国との適切な役割分担を踏まえて、サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する。
サイバー関連事業者その他の事業者の責務	基本理念にのっとり、その事業活動に関し、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とともに、国又は地方公共団体が実施するサイバーセキュリティに関する施策に協力するよう努めるものとする。
国民の努力	基本理念にのっとり、サイバーセキュリティの重要性に関する関心と理解を深め、サイバーセキュリティの確保に注意を払うよう努めるものとする。

（出所）サイバーセキュリティ基本法を基に作成

さらに、施策に関連して、重要社会基盤事業者等におけるサイバーセキュリティの確保の促進及びサイバーセキュリティ戦略本部の所掌業務が、それぞれ以下のように規定されている（同法第 14 条及び第 26 条第１項第５号参照）（補論図表６）。

補論図表６　施策に関連した規定

（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）
国は、重要社会基盤事業者等におけるサイバーセキュリティに関し、基準の策定、演習及び訓練、情報の共有その他の自主的な取組の促進その他の必要な施策を講ずるものとする。
（サイバーセキュリティ本部の所掌事務）
サイバーセキュリティに関する施策で重要なものの企画に関する調査審議、府省横断的な計画、関係行政機関の経費の見積りの方針及び施策の実施に関する指針の作成並びに施策の評価その他の当該施策の実施の推進並びに総合調整に関すること。

（出所）サイバーセキュリティ基本法を基に作成

（２）重要インフラの対象分野の指定等

我が国では、平成 26 年のサイバーセキュリティ基本法制定よりも以前から、重要インフラ防護に係る官民の基本的な枠組みを定めた「行動計画」に基づい

て、重要インフラの対象分野が指定され、重要インフラの防護に係る取組が行われてきた（補論図表７）。

補論図表７　重要インフラ分野の指定等に関する沿革

年月	行動計画の策定等
平成 12 年 12 月	「重要インフラのサイバーテロ対策に係る特別行動計画」 ・**重要インフラとして７分野を指定** **（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。））**
平成 17 年５月	ＩＴ総合戦略本部の下に「情報セキュリティ政策会議」を設置
平成 17 年 12 月	「重要インフラの情報セキュリティ対策に係る行動計画」（第１次行動計画） **・水道、医療、物流を追加し計 10 分野** （海外で対象とされているものを念頭に検討し、追加） ・重要インフラの定義や対象事業者等の明確化 ・政府の指針等を踏まえた業界による安全基準等の整備
平成 21 年２月	「重要インフラの情報セキュリティ対策に係る第２次行動計画」 ・対象分野の変更なし ※第２次行動計画は、平成 24 年４月に改定
平成 26 年５月	「重要インフラの情報セキュリティ対策に係る第３次行動計画」 **・石油、化学、クレジットを追加し計 13 分野** ※第３次行動計画は、平成 27 年５月に改定
平成 26 年 11 月	サイバーセキュリティ基本法制定
平成 29 年４月	「重要インフラの情報セキュリティ対策に係る第４次行動計画」
平成 30 年７月	第４次行動計画の１次改定 **・重要インフラに空港を追加し計 14 分野**
令和２年１月	第４次行動計画の２次改定 ・法改正等を踏まえた微修正
令和４年６月	「重要インフラのサイバーセキュリティに係る行動計画」
令和６年３月	重要インフラのサイバーセキュリティに係る行動計画の改定 **・港湾を追加し計 15 分野** （名古屋港におけるシステム障害を踏まえた対応）

（注）サイバーセキュリティ基本法制定後の「行動計画」は同法第 14 条及び第 26 条第１項第５号の規定に基づき、サイバーセキュリティ戦略本部が決定する。

（出所）三角育生「我が国のサイバー/情報セキュリティ政策の変遷（重要インフラ編）～今後の重要インフラに係るサイバーセキュリティ政策立案において考慮すべき観点～」『ＪＣＩＣレポート』（令 6.5.1）等より作成

補論図表７のとおり、直近では、令和５年７月の名古屋港におけるシステム

障害を踏まえた対応として、令和６年３月に港湾が重要インフラに指定され、15 分野が重要インフラに指定されている（重要インフラ所管省庁と重要インフラについては下図を参照（補論図表８））。

補論図表８　重要インフラの所管省庁と重要インフラ

（出所）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）資料より一部抜粋

ただし、15 分野の重要インフラ分野に関する事業がすべて重要インフラ事業者（重要社会基盤事業者）となるわけではなく、定義（前掲図表４参照）の後段にあるように、機能停止等の場合に多大な影響を及ぼすおそれが生ずるとの要件にも該当することが求められている。

また、令和６年３月に改定された「重要インフラのサイバーセキュリティに係る行動計画」では、官民連携による重要インフラ防護の推進のため、①任務保証[12]の考え方を踏まえ、重要インフラサービスの安全かつ持続的な提供を実現すること、②官民が一丸となって重要インフラのサイバーセキュリティの確保に向けた取組を推進することが掲げられている。

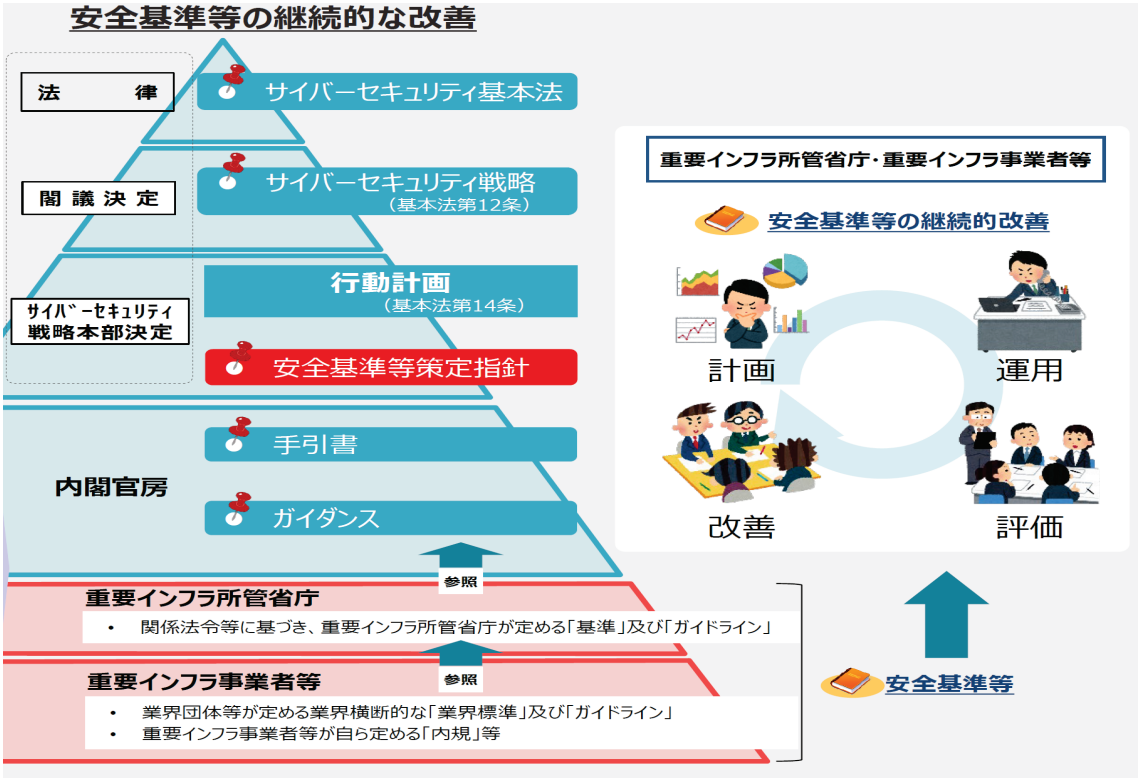
（３）安全基準等策定指針

サイバーセキュリティ戦略本部は、重要インフラサービスの安全かつ持続的

[12] 任務保証とは、企業、重要インフラ事業者や政府機関に代表されるあらゆる組織が、自らが遂行すべき業務やサービスを「任務」と捉え、係る「任務」を着実に遂行するために必要となる能力及び資産を確保することであり、サイバーセキュリティに関する取組そのものを目的化するのではなく、各々の組織の経営層・幹部が、「任務」に該当する業務やサービスを見定めて、その安全かつ持続的な提供に関する責任を全うするという考え方である。

な提供を図る観点から、「安全基準等策定指針」を策定し、適宜、行動計画の改定、サイバーセキュリティを取り巻く環境の変化等を踏まえて見直しを実施してきている。なお、安全基準等策定指針を始めとした安全基準に関する法令等は以下のとおりとなっている（補論図表９）。

補論図表９　安全基準等策定指針を始めとした安全基準に関する法令等



（出所）ＮＩＳＣウェブサイト

令和５年７月に策定された「重要インフラのサイバーセキュリティに係る安全基準等策定指針」が現行の「安全基準等策定指針」であり、同指針では、重要インフラ事業者に対し、ＣＩＳＯ（サイバーセキュリティに関する責任者）等を任命することを求め、経営層クラスから任命することが推奨されている。

ただし、「安全基準等策定指針」には、遵守の実効性を確保する仕組みがあるわけではない。