2025 年 4 月 21 日　全 10 頁

能動的サイバー防御の導入に向けた政策動向

激化するサイバー攻撃に先手を打って被害を防ぐ

デジタルソリューション研究開発部　横平 健

要約

- 政府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を目指し、能動的サイバー防御を導入するための関連法案を 2 月 7 日に閣議決定した。同法案は 2025 年の通常国会での成立を目指している。

- 2022 年 12 月に改定された国家安全保障戦略において、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の実現に向けた検討を進めることが明記された。

- 能動的サイバー防御を導入することで、他国からのサイバー攻撃を受ける前に無害化措置を講じることが可能となり、重要インフラ等に対する被害の未然防止が期待できる。

- 欧米主要国では、すでに能動的サイバー防御に関する法制度が整備されている国も多く、政府による情報共有や国外関連の通信情報の取得、国外サーバに対する無害化措置などが実施されている。

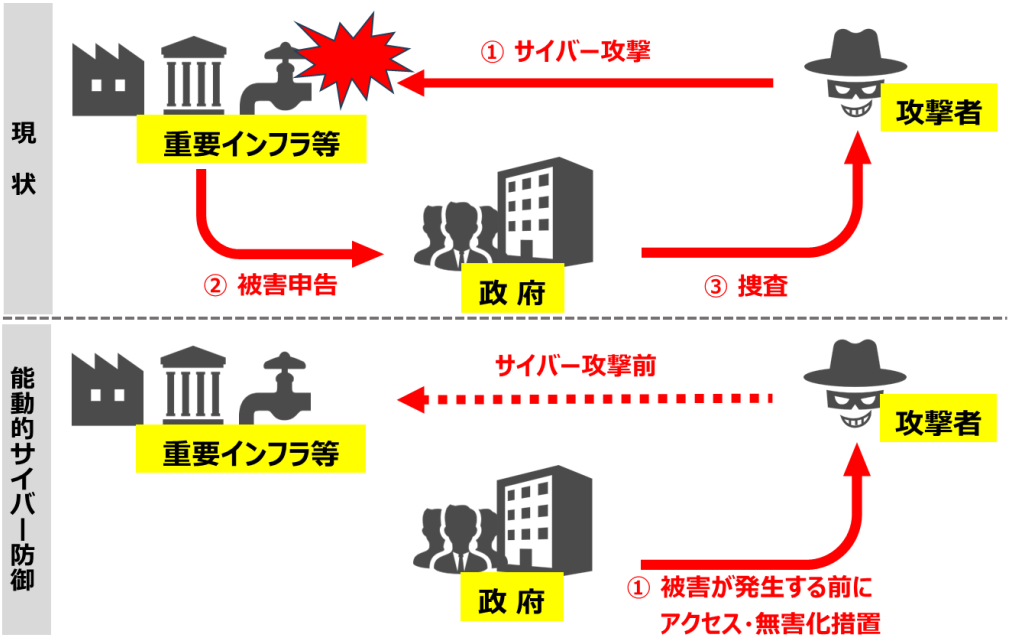
- 基幹インフラ事業者は、政府に対して導入機器の届出やインシデント発生時の報告が義務化されるなどの影響が見込まれるため、今後の動向を注視すると共に、法律の施行に向けた体制の検討が必要となる。

概要

能動的サイバー防御とは、外部からの重要インフラ等に対するサイバー攻撃を防止するため、攻撃の兆候等を収集することで、攻撃を事前に検知し、攻撃元を特定するとともに、攻撃元に対して無害化措置を講じるセキュリティ対策のことで、英語では「Active Cyber Defense（ACD）」と表現されます。

従来、日本の法律では他者システムへ無断でアクセスすることは禁止されており、サイバー攻撃を受けた際に攻撃元の機器に対して反撃するいわゆる「ハックバック」は法的に困難でした。そのため、サイバー攻撃に対して防御的な措置を講じることに重点を置かざるを得ず、攻撃者に対する積極的な対策が取れない状況が続いていました。しかし、近年、国内ではサイバー攻撃による政府機関や企業を狙った情報窃取が深刻な問題となっている他、重要インフラ等の機能を停止させることを目的とした高度な侵入・潜伏能力を持つサイバー攻撃への懸念が急速に高まっています。特に、重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃は、国家の関与が疑われる形でも日常的に行われており、安全保障上の大きな懸念となっています。

このような背景から、従来の受動的な防御策だけでは不十分であるとの認識が広がり、政府は後述する『**国家安全保障戦略（2022年 12 月 16 日改定）**(*1)』に基づき、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を目指し、能動的サイバー防御の導入に向けた政策を進めています。

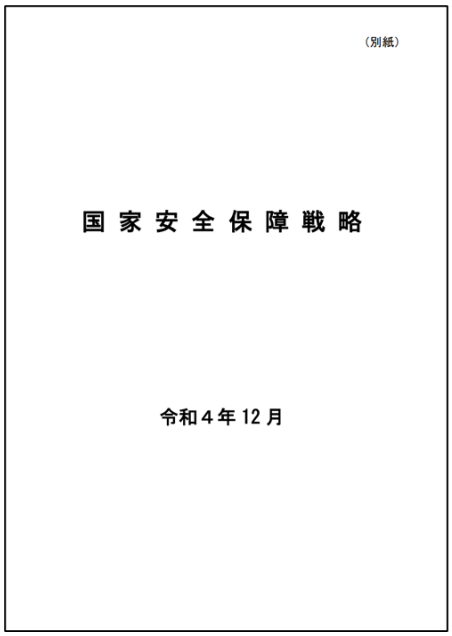


出典：大和総研作成

国家安全保障戦略について

『国家安全保障戦略』とは、日本の国家安全保障に関する基本方針を定めた最上位の政策文書であり、外交、防衛、経済安全保障、サイバーなど多岐にわたる分野が含まれています。本戦略は 10 年程度の期間を念頭に置いており、2013 年 12 月 17 日に初めて策定され、2022 年 12 月 16 日に初改定されました。

(*1) 内閣官房『国家安全保障戦略について』


（別紙）

国 家 安 全 保 障 戦 略

令和４年 12 月

安保関連３文書の位置づけ

国家安全保障戦略	日本の国家安全保障に関する基本方針（10年程度の期間を念頭）
↓ 基本方針を基に設定	
国家防衛戦略	防衛目標を設定し、それを達成するためのアプローチと手段を明示（10年程度の期間を念頭）
↓ 防衛目標を達成するよう計画	
防衛力整備計画	10年後の自衛隊の体制や5年間の防衛費の見積り等を明示

出典：大和総研作成

改定された国家安全保障戦略では、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、能動的サイバー防御の実施のための体制を整備し、以下の3つを含む必要な措置の実現に向け検討を進めることが明記されました。

① **官民連携の強化**

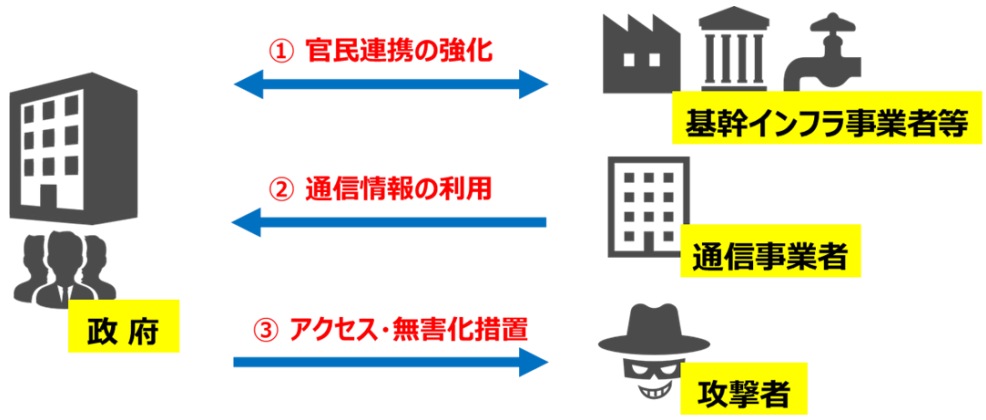
重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。

② **通信情報の利用**

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。

③ **アクセス・無害化措置**

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。



出典：大和総研作成

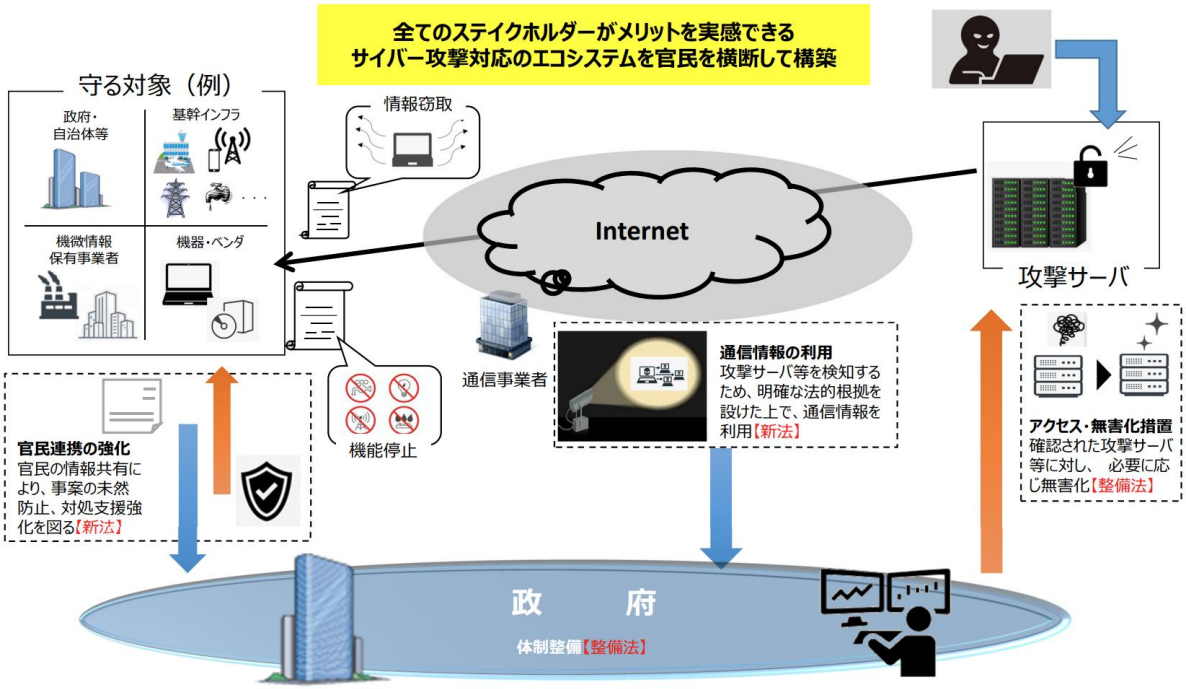
導入に向けた政府の動き

政府は国家安全保障戦略に明記した能動的サイバー防御の導入に向けて、2023 年 1 月に内閣官房にサイバー安全保障体制整備準備室を設置し、サイバー安全保障分野における対応能力の向上を図るべく準備を進めてきました。また、2024 年 6 月には、サイバーセキュリティ対策の実務者や研究者などから構成される有識者会議を設置し、現行法との整合性を整理するなど、必要な法整備に向けた課題を洗い出し、複数回にわたって検討を行ってきました。そして、同年 11 月に有識者会議から法制化に向けた最終提言が取りまとめられ、これを基に政府は法案の内容を固め、2025 年 2 月に関連法案が閣議決定されました。

なお、閣議決定された法案は、現在開会中の 2025 年の通常国会(*1)で審議されており、今国会での成立を目指しています。

年月日	概要
2022/12/16	「**国家安全保障戦略**」を改定し、「**能動的サイバー防御**」の導入を明記
2023/1/31	必要な法整備を進めるため、「**内閣官房サイバー安全保障体制整備準備室**」を設置
2024/6/7 ～ 2024/11/29	**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**(*2)（4度の全体会、9度のテーマ別会合）を実施
2024/11/29	有識者会議は『**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**(*3)』を取りまとめて公表
2025/2/7	「能動的サイバー防御」を導入する関連法案を閣議決定(*4) → **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【新法】** → **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【整備法】**

出典：大和総研作成



出典：内閣官房『サイバー対処能力強化法案及び同整備法案について(*5)』より抜粋

(*1) 2025 年の通常国会の会期は 1 月 24 日から 6 月 22 日までの 150 日間の予定（延長の可能性あり）。

(*2) 内閣官房「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」

(*3) 内閣官房「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」

(*4) 内閣官房「サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）」

(*5) 内閣官房『サイバー対処能力強化法案及び同整備法案について』

法案の主な内容

2025 年2月7日に閣議決定された法案は、新たな法律として定める「**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**」(**新法**)と、既存の法律を改正するための「**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**」(**整備法**)の2つから成ります。また、整備法において改正の対象としている法律は、サイバーセキュリティ基本法や警察官職務執行法など、合計 15 本あり、能動的サイバー防御の導入を実現するために、複数の法律を組み合わせて必要な法的枠組みを整備しています。

ここからはこの新法及び整備法について、国家安全保障戦略で必要な措置として揚げられている **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** とこれら措置に必要となる **④組織体制等** に分けて、主な内容を紹介します。

① 官民連携の強化

法案の規定事項	概要
導入製品の届出の義務化	基幹インフラ事業者に対し、サイバーセキュリティが害された場合にインフラサービスの提供に影響を及ぼす恐れのある機器を導入した際は、その製品名などを政府に届け出ることを義務化する。
インシデント報告の義務化	基幹インフラ事業者に対し、インフラサービスを提供する機器へのサイバー攻撃のインシデント情報や、その原因となり得る事象を認知したときの政府への報告を義務化する。
協議会の設置	あらかじめ同意を得た基幹インフラ事業者やベンダー等を構成員とする協議会を設置する。また、政府は構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求める。
脆弱性対応の強化	政府は、政府機関や基幹インフラ事業者等において保護の対象となる機器(プログラムを含む)の脆弱性を認知した場合、その供給者(生産者、販売者等)に対して情報提供を行う。また、当該脆弱性が基幹インフラ事業者のインフラサービスの提供に関連する場合は、供給者に対して被害を防止するために必要な措置を講じるよう要請する。
罰則の整備	■行政職員及び協議会構成員等による秘密の不正利用・漏えい行為 ⇒2年以下の拘禁刑又は 100 万円以下の罰金 ■基幹インフラ事業者がインシデント報告を行わず、是正命令にも対応しない場合 ⇒200 万円以下の罰金 ■基幹インフラ事業者がインシデント報告等に関し、資料提出等の求めに応じない場合 ⇒30 万円以下の罰金

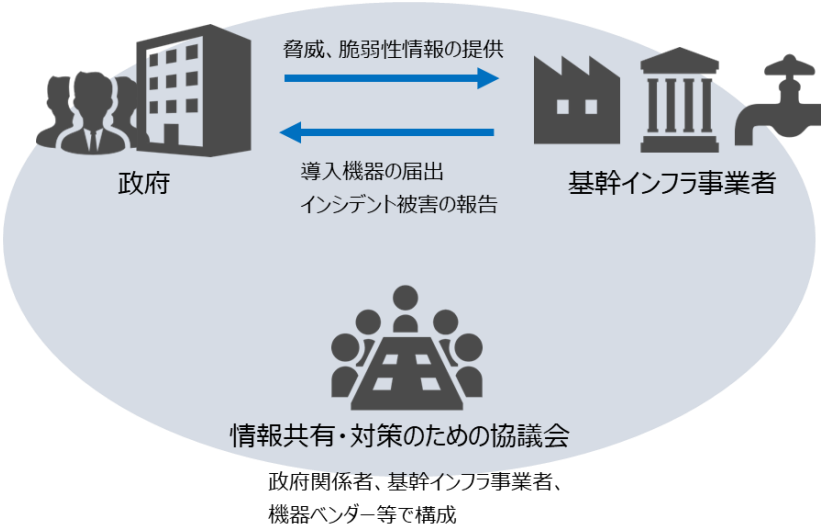
出典:内閣官房『サイバー対処能力強化法案及び同整備法案について』を基に大和総研作成

「官民連携の強化」においては、基幹インフラ事業者に対して新たな規制が導入される予定です。基幹インフラ事業者とは、経済安全保障推進法の対象となる 15 事業の中から、国が一定の基準に基づいて指定した事業者を指し、2025 年 3 月 11 日時点で 215 者が指定されています。この法案では、これら基幹インフラ事業者に対し、政府への「**導入製品の届出の義務化**」及び「**インシデント報告の義務化**」が規定されています。

「**導入製品の届出の義務化**」は、基幹インフラ事業者が利用する機器の脆弱性を早期に認識し、迅速な対応を可能にすることが目的です。システムへの不正侵入などに悪用される脆弱性は、開発段階でどれだけ注意しても発生し得るものであり、特にゼロデイ攻撃と呼ばれる修正プログラムの公開前を狙った攻撃では脆弱性の悪用が先行するため、利用者が自らのリスクを適切に理解し、対策を講じることが難しい状況でした。このような背景の中で、導入製品の届出義務を設けることによって、基幹インフラ事業者は自らが使用している機器に関する情報を政府に提供し、政府はその情報を基に迅速かつ的確な攻撃関連情報を提供することができます。これにより、利用者は自らのシステムに対する脅威を早期に認識し、適切な対策を講じることが可能になることが期待されます。

政府への「**インシデント報告の義務化**」については、すでに放送法や電気通信事業法などの個別業法に基づき、所管省庁へのインシデント報告の義務が課されているところですが、国家や国民の安全に大きな影響を及ぼし得る基幹インフラ事業者に対しては、より迅速な報告義務を課すことで、政府が早期に事態を把握し、他の基幹インフラ事業者を含めた被害拡大を防止する意図があるとみられます。

さらに、法案では新たに協議会を設置し、政府が事業者に対して被害防止に資する情報を共有することを規定しています。この協議会には基幹インフラ事業者の他、機器ベンダーなども参加することが想定されており、より広範な情報共有と協力が促進されることが期待されます。



出典：大和総研作成

また、基幹インフラ事業者によるインシデント報告や協議会での秘密保持を徹底するために罰則が設けられています。具体的には、基幹インフラ事業者がインシデント報告を怠ったり、是正命令に従わなかった場合には、最高で 200 万円の罰金が科せられることになります。

この罰則により、基幹インフラ事業者の責任が明確化され、インシデント発生時には迅速に対応する意識改革が進むことが期待されます。また、罰則の存在は、事業者に法令遵守の重要性を再認識させる効果もあります。特に、サイバー攻撃の脅威が増大する中で、基幹インフラの安全性を確保することは、経済活動や国民生活の安定に直結します。そのため、法案に基づく罰則は、単なる制裁にとどまらず、事業者が自発的にサイバーセキュリティ対策の強化を講じる動機付けにもなると考えられます。

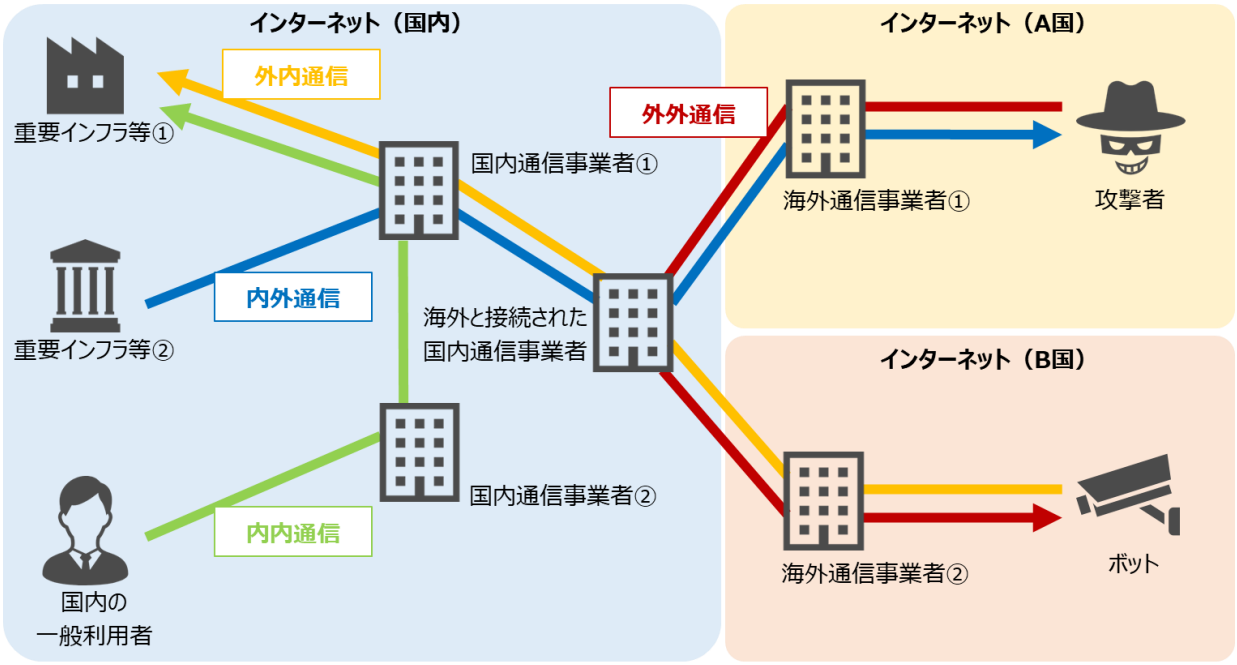
② 通信情報の利用

法案の規定事項	概要
同意によらない通信情報の取得	首相はサイバー攻撃の実態把握のために必要があると認める場合には、サイバー通信情報監理委員会の承認を受け、サイバー攻撃に関係する国外関係通信の情報を取得できるようにする。
同意に基づく通信情報の取得	首相は基幹インフラ事業者や通信サービスの利用者との協定に基づき、当該利用者が送受信する通信情報の提供を受けることができる。また、この通信情報のうち、外国から国内に係る通信情報を分析し、当該利用者のサイバーセキュリティの確保のために必要な分析結果を提供する。
情報の選別	首相は取得した通信情報のうち、IP アドレス等の調査すべきサイバー攻撃に関係するもののみを自動選別し、それ以外の通信情報は直ちに消去する。
独立機関の設置	通信情報の利用の適正確保のため、**サイバー通信情報監理委員会**を設置する。 また、同委員会に国外関係通信の取得及び無害化措置に際しての審査・承認等の権限を与える。
罰則の整備	■通信情報を取り扱う行政職員による、通信情報の不正利用・漏えい行為 ⇒データベースの提供は、4年以下の拘禁刑又は 200 万円以下の罰金 その他は、3年以下の拘禁刑又は 100 万円以下の罰金 ■通信情報を保有する行政機関の管理を侵害して通信情報を取得する行為 ⇒3年以下の拘禁刑又は 150 万円以下の罰金 ■その他の行政職員及び協議会の事務の従事者による秘密の不正利用・漏えい行為 ⇒2年以下の拘禁刑又は 100 万円以下の罰金

出典：内閣官房『サイバー対処能力強化法案及び同整備法案について』を基に大和総研作成

「通信情報の利用」では、政府がサイバー攻撃の実態把握のために通信情報を取得する方法として、「**同意によらない通信情報の取得**」と「**同意に基づく通信情報の取得**」が規定されています。いずれの取得方法についても調査すべき情報であるサイバー攻撃に関係するもののみを選別したうえで、取得することとして

おり、国内に閉じられた通信（下図の「内内通信」）情報は取得の対象外としています。この理由は、現在国内で観測されているサイバー攻撃に関連する通信のほとんどが国外から発信されているため、特に国外に関連する通信の分析が必要であることに加え、憲法上の通信の秘密を侵害しないよう、国内の通信においては国外が関係する通信とは区別し、より慎重に取り扱うべきであると判断されたためだとみられます。



出典：内閣官房『サイバー対処能力強化法案及び同整備法案について』を基に大和総研作成

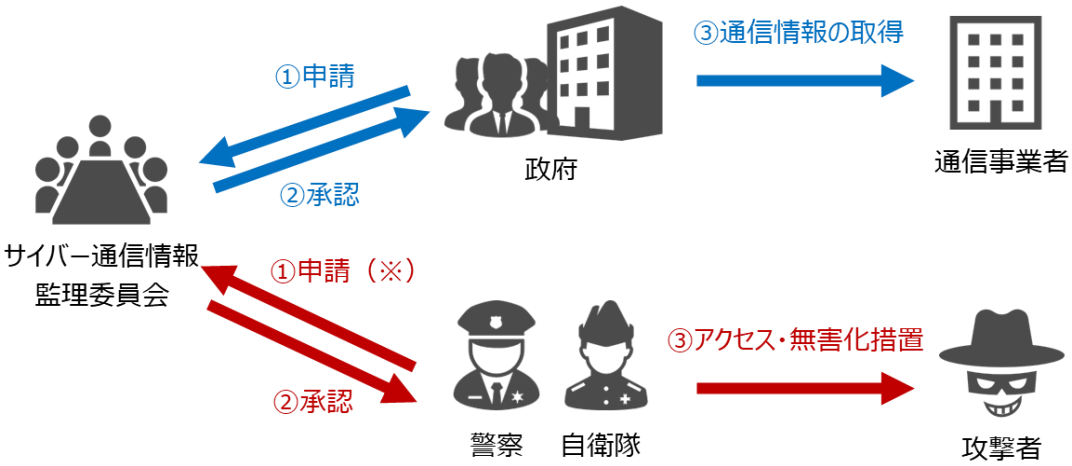
また、政府が取得した情報の分析は、原則として電子メールの本文や IP 電話の通話内容といったコミュニケーションの本質的な内容に当たる情報には触れず、それ以外の送受信日時や IP アドレス、通信量などの情報に限定されています。これに関しても、憲法上の通信の秘密を侵害しないための措置であり、分析の対象外となる情報は、あらかじめ自動選別され、直ちに消去されることになっています。政府の法案説明資料では、コミュニケーションの本質的な内容に当たらない例と当たる例が以下のとおり示されていますが、国民の信頼を得るためには、より具体的な選別基準やプロセスを示して、透明性を確保する必要があると考えられます。

コミュニケーションの本質的な内容に<u>当たらない例</u>	○ 送受信日時	2024.04.01 12:00:04
	○ ＩＰアドレス	103.23.145.84
	○ 通信量	20kB
	○ ポート番号	80
	○ コマンド	POST/ A3fe e3844A7D35300734D2BA HTTP/1.1
	○ プロトコル（通信方式）	HTTP / SSL / SMTP
	○ ソフトウェアの種類	Mozilla/4.0(…Trident/7.0;NET4.0c;…)…
	○ ドメイン名	cas.go.jp
	○ メールアドレス	hogehoge@example.com （個人情報保護の観点から、個人を識別することができないように加工することが必要）

コミュニケーションの本質的な内容に<u>当たる例</u>	× 電子メールの本文・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、画像

出典：内閣官房『サイバー対処能力強化法案及び同整備法案について』より抜粋

さらに政府による制度の乱用を防止するため、新たに独立した第三者機関である「**サイバー通信情報監理委員会**」を創設し、その運用を監視することとしています。同委員会は委員長を含む5名で構成され、裁判官などの法律の専門家やサイバーセキュリティの有識者が国会の同意を得て、首相により任命される予定です。同委員会には政府による通信情報の取得に際して、事前審査や通信情報の取扱いに関する継続的な検査を行う権限が与えられる他、後述する警察及び自衛隊が実施する攻撃元へのアクセス・無害化措置に関する審査・承認の権限も与えられることになっています。



出典：大和総研作成

③ アクセス・無害化措置

法案の規定事項	概要
警察官職務執行法の改正	警察庁長官が指名する警察官は、サイバー攻撃又はその疑いがあり、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恐れがあるため緊急の必要があるときは、攻撃元の機器に対して、危害防止のための必要な措置（機器の管理者等への命令又は自らによる電気通信回線を介した措置）をとることができる。
自衛隊法の改正	首相は行政機関や基幹インフラ等の保護の対象となる機器へのサイバー攻撃であり、外国からの特に高度に組織的かつ計画的な行為と認められる場合は、自衛隊に対して当該機器に対する通信防護措置をとることを命じることができる。また、その際は警察と共同で当該措置を実施する。

出典：内閣官房『サイバー対処能力強化法案及び同整備法案について』を基に大和総研作成

「アクセス・無害化措置」では、「**警察官職務執行法**」と「**自衛隊法**」を改正し、新たな条文を追加することで、警察と自衛隊が攻撃元のサーバに侵入し、その機能を停止する措置を可能にしています。攻撃元へのアクセスと無害化措置は原則として警察が担当しますが、行政機関や基幹インフラを対象とした外国からの組織的かつ計画的な行為と認められる場合は、首相が自衛隊に命じて警察と共同で対処することが規定されています。

この法改正により、日本のサイバー攻撃への対応が大きく変わることが期待されます。従来の法律では防御的な措置しか取れず、迅速な反撃や攻撃元への対処が困難でしたが、新たな法改正により攻撃元に対して直接的な行動を取ることが可能となり、より積極的なサイバーセキュリティ対策が実施できるようになります。

ただし、この権限の行使には慎重な判断が必要です。攻撃元へのアクセスや無害化措置は国家の安全保障を強化する一方で、誤った情報や判断に基づく行動は国際的な摩擦を引き起こすリスクも伴います。そのため、国際法上許容される範囲内で対処するための仕組みを整備し、独立機関であるサイバー通信情報監理委員会による厳格な監視体制のもとで透明性のある運用を行うことが求められます。

④ 体制整備等

法案の規定事項	概要
体制整備	■サイバーセキュリティ戦略本部の改組・機能強化 ⇒首相を本部長、全ての国務大臣を本部員とする組織に改組 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設置 ■内閣サイバー官の新設 ⇒内閣官房に、サイバーセキュリティの確保に関する総合調整等の事務を掌理する内閣サイバー官を新設 ■情報処理推進機構(IPA)の事務の追加 ⇒基幹インフラ事業者のサイバーセキュリティの確保の状況の調査等を追加 ■情報通信研究機構(NICT)の事務の追加 ⇒国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を追加 ■内閣府における所掌事務の追加等 ⇒所掌事務に新法の「官民連携の強化」と「通信情報の利用」に関する事務を追加 同府にサイバー通信情報監理委員会を設置
施行期日	一部を除き、公布日から1年6月を超えない範囲内において政令で定める日

出典:内閣官房『サイバー対処能力強化法案及び同整備法案について』を基に大和総研作成

体制整備においては、能動的サイバー防御の各種取り組みを実現・促進するために、政府内に新たな司令塔組織を設置するなどの組織改編が予定されています。また、政府の機能強化に伴い、外郭団体である情報処理推進機構(IPA)と情報通信研究機構(NICT)にも新たな業務が追加され、政府からの委託に基づいて、基幹インフラ事業者のサイバーセキュリティ確保状況の調査や、国等の情報システムに対する不正な活動の監視・分析を実施することとしています。

なお、施行期日は、一部を除き公布日から 1 年 6 カ月以内とされているため、現在行われている 2025 年通常国会の会期中に法案が成立した場合、早ければ 2026 年度中には制度が開始されることとなります。

欧米主要国の主な取り組み

欧米主要国では、すでに能動的サイバー防御に関する法制度が整備されている国も多く、政府による情報共有や国外関連の通信情報の取得、国外サーバに対する無害化措置などが実施されています。主なものとして、以下のような取り組みが挙げられます。

	主な取り組み
官民連携の強化	**米国** ✓重要インフラ事業者に対し、インシデント発生から72時間以内の政府への報告を義務付け【**重要インフラサイバーインシデント報告法（2022年）※未施行**】 ✓重要インフラ事業者に対し、機密情報を含むサイバーセキュリティの脅威情報を共有【**国家サイバーセキュリティ戦略（2023年）**】 **イギリス** ✓重要インフラ事業者等に対し、サービス継続に重大な影響を及ぼすインシデントを認識したとき、72時間以内に政府への義務付け【**NIS規則（2018年）**】 **EU** ✓重要インフラ事業者等に対し、インシデント発覚から24時間以内の早期通知や、72時間以内の重大性・影響の評価通知などを義務付け【**NIS2指令（2023年）**】
通信情報の利用	**米国** ✓外国の政府・組織による脅威やテロの防止等を目的に、国外所在の非米国人の通信情報を取得【**外国情報監視法（2008年改正）**】 **イギリス** ✓国の安全保障やテロを含む犯罪の予防・捜査を目的に、国外関連の通信情報を取得【**調査権限法（2016年制定）**】
アクセス・無害化措置	**米国** ✓Volt Typhoonのボットネットを構成する感染ルータ群に対し、当該ルータからマルウェアを削除するコマンドを送信するなどの無害化措置を実施（2024年） **カナダ** ✓政府ネットワークからの情報の窃取を防止するために、国外の攻撃サーバに対して無害化措置を実施（2019年以降）

出典:内閣官房『サイバー対処能力強化法案及び同整備法案について』及び各国法制度を基に大和総研作成

おわりに

能動的サイバー防御の導入をめぐっては、かねてより憲法で保障されている「通信の秘密」への抵触や、不正アクセス禁止法などの法令に違反するといった問題点が指摘されていました。しかし、2 月 7 日に閣議決定された法案では、政府が取得する情報の制限や関連法令の改正、独立した第三者機関による監督の下での運用を明記し、透明性と適正な手続きを確保する姿勢が示されています。これにより、国民のプライバシー保護と国内のサイバーセキュリティ強化を両立させることを目指しています。

一方で、本法案だけでは依然として不明確な点も多く残されています。例えば、基幹インフラ事業者に対してインシデントの報告を義務化することとしていますが、報告に必要な事項は別途、省令で定められることになっているため、具体的にどのような事象が報告対象となるのかや、報告期限などは明らかになっていません。また、独立した第三者機関となるサイバー通信情報監理委員会の役割についても、具体的な説明が求められます。この機関がどのように機能し、どのような基準で監視を行うのかが明確でなければ、国民の信頼を得ることは困難であると言えます。透明性のある運用が求められる中で、第三者機関の活動内容や評価基準を公開し、国民がその活動を理解できるようにすることが重要です。

以上のことから、本法案が成立した場合、実際の運用がどのように行われるのか、今後の動向にも十分注視が必要です。特に官民連携の強化に関して大きな影響を受けることが予想される基幹インフラ事業者においては、本法案の成立に伴い、セキュリティ体制の見直しが必要になることが想定されます。そのため、資産管理や脆弱性管理、インシデント発生時の体制などについて見直すべき点がないか事前に確認を行い、法律の施行に備えて適切な準備と対応策を講じておくことを推奨します。