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（２） －通信情報の利用と通信の秘密－
著者 / 所属	榎本　尚行 / 内閣委員会調査室
雑誌名 / ISSN	立法と調査 / 0915-1338
編集・発行	参議院事務局企画調整室
通号	477 号
刊行日	2025-7-25
頁	3-22
URL	https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/20250725.html

※ 本文中の意見にわたる部分は、執筆者個人の見解です。

能動的サイバー防御２法案の国会論議（２）

― 通信情報の利用と通信の秘密 ―

榎本　尚行
（内閣委員会調査室）

１．はじめに

能動的サイバー防御を導入するとして令和７年２月７日に国会に提出された、「重要電子計算機に対する不正な行為による被害の防止に関する法律案」（閣法第４号）（以下「サイバー対処能力強化法案」という。）及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案」（閣法第５号）は、大別して官民連携の強化、通信情報の利用及びアクセス・無害化措置の３本柱から成る。

前号掲載の「能動的サイバー防御２法案の国会論議（１）」では、制度の全体像及び官民連携の強化について整理した。本稿では、通信情報の利用について、その制度の概要を確認した上で、主な国会論議を整理する。アクセス・無害化措置については、本号掲載の「能動的サイバー防御２法案の国会論議（３）」を参照されたい。

２．通信情報の利用と憲法上の通信の秘密との関係

能動的サイバー防御を導入することが盛り込まれた国家安全保障戦略（令和４年12月16日国家安全保障会議決定・閣議決定）では、「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。」とされ、これに基づき通信情報の利用について検討が進められた。他方、通信情報の利用を検討する場合、憲法に定める通信の秘密との関係を整理する必要がある。

憲法第21条第２項では、「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。

この解釈について内閣法制局は、「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」、「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」旨答弁した[1]。

こうした規定や解釈を踏まえ、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。）においては、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、について議論された。有識者会議通信情報の利用に関するテーマ別会合では、通信情報の利用に関して、諸外国の例、参考とすべき法律等が示されている[2]。その中で、電気通信事業法（昭和59年法律第86号）の解釈にも触れられており、通信当事者の有効な同意がある場合、違法性阻却事由がある場合[3]の２つの場合において、通信の秘密の侵害に当たらないことが示された。

こうした解釈や不審なアクセスの大部分が国外からである実態[4]等を踏まえ、サイバー安全保障分野での対応能力の向上に向けた提言（令和６年11月29日）（以下「有識者会議提言」という。）では、国外が関係する通信について、通信情報を分析する必要が特にあるとされ、具体的には、「外外通信」「外内通信」「内外通信」（後掲**図表２**参照）について分析が必要であること、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した上で、具体的な制度については、先進主要国の法律で、おおむね共通する実施過程として準備・承認、通信事業者への措置、処理・分析、提供・共有等、保存・廃棄があるほか、独立機関による監督も共通しており、こうした仕組みを参考とすることなどが指摘された。

加えて、上記の通信の秘密をめぐる議論は、通信当事者の同意がない場合を前提としており、同意のある場合の通信情報の利用については、同意がない場合とは異なる制度により実施することも可能であるとされた。

３．サイバー対処能力強化法案における通信情報の利用に関する規定の概要

（１）通信情報の利用に関する制度概要

サイバー対処能力強化法案における通信情報の利用に関する規定の概要は、**図表１**のとおりである。全体的な制度の流れとしては、政府は通信情報を取得し、機械的情報に選別した上で、分析を行う。独立機関であるサイバー通信情報監理委員会がこれらの監視・監

---

[1] 第213回国会衆議院予算委員会議録第３号12頁（令6.2.5）。なお、憲法の規定を受け、電気通信事業法第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。

[2] 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（令6.6.19）資料<https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai3/siryou5-2.pdf>（以下、ＵＲＬはすべて令和７年７月９日最終アクセス。）

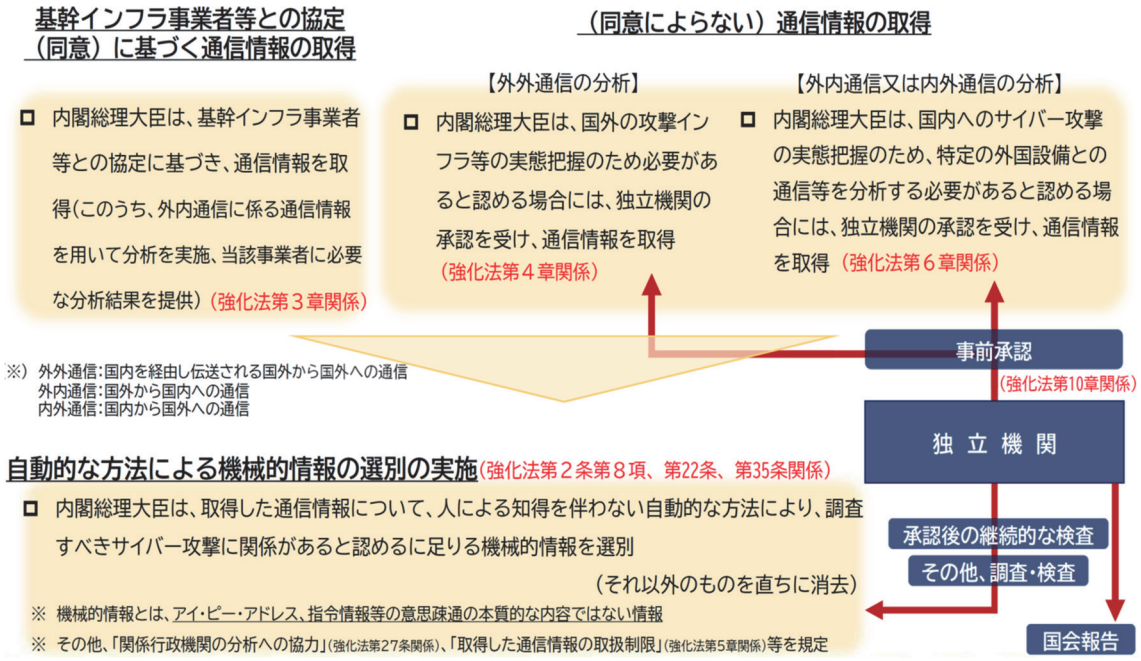
[3] 具体的には、①法令行為に該当する場合、②正当業務行為に該当する場合、及び③正当防衛、緊急避難に該当する場合に違法性が阻却される。

[4] 「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」（令和７年３月警察庁サイバー警察局）５頁によると、不審なアクセスのうち99.4％が海外を送信元とするアクセスで占められている。

督を行い、同委員会は、毎年、国会にその所掌事務の処理状況を報告する等とされている。

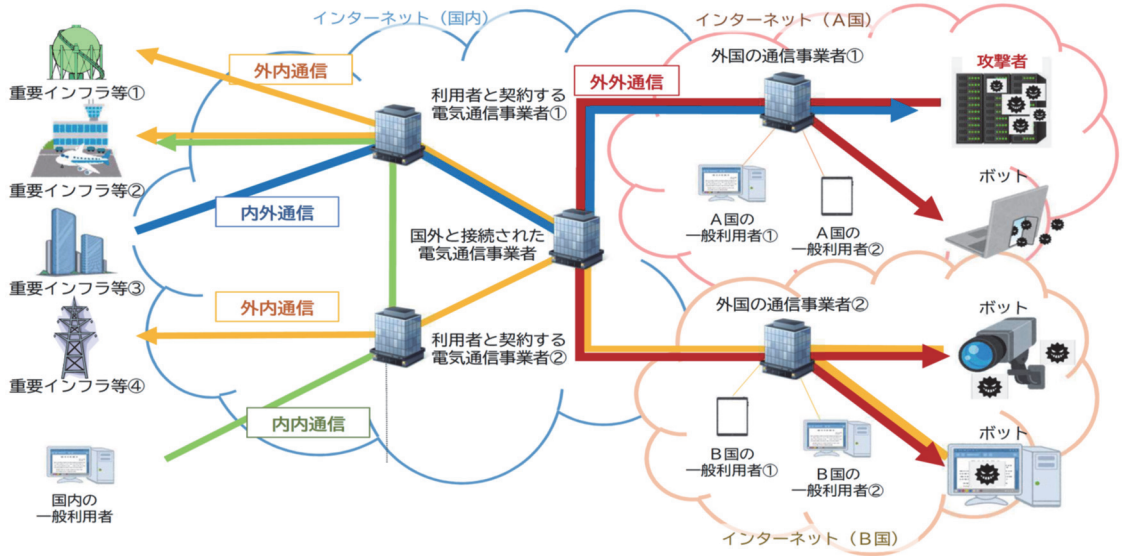
分析の対象となる通信情報は、外外通信、外内通信及び内外通信であり、**図表２**のように整理されている。通信情報の区分について、外外通信は、国内を経由して伝送される国外から国外への通信で、外内通信、内外通信は、いずれも外国と国内の間の通信である。法案では、この３類型の通信情報が分析対象とされる一方、国内間の通信である内内通信は分析対象外である。

図表１　通信情報の利用に関する制度概要



（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

図表２　国外が関係する通信、関係しない通信



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

（２）通信情報の取得及び自動選別

政府が取得する通信情報については、通信の秘密の解釈も踏まえ、同意に基づくか否かに大別されている。同意に基づく通信情報の取得と整理されているのが、政府が基幹インフラ事業者[5]等と協定を締結し、協定に基づいて通信情報を取得する制度である。一方、同意によらない通信情報の取得としては、一定の要件の下、サイバー通信情報監理委員会の承認を受けた上で行われる外外通信に係る措置や、特定の外国設備との通信情報を分析する必要が生じた場合の外内通信及び内外通信に係る措置が該当する。

このような取得通信情報[6]自体には分析対象以外の情報も含まれ得るところ、これらを人の知得を伴わない自動的方法により機械的情報のみに選別する、自動選別が行われる。

ア　同意によらない通信情報の取得（サイバー対処能力強化法案第４章、６章及び７章）

同意によらない通信情報の取得には、外外通信に係る措置と、特定の外国設備との通信情報を分析する必要が生じた場合における外内通信及び内外通信に係る措置とがある。

まず、外外通信に係る情報の取得については、条文上「外外通信目的送信措置」として規定されている。同措置では、内閣総理大臣は、①外外通信であって、②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[7]に関係するものが、③特定の国外関係電気通信設備により伝送されていると疑うに足りる状況がある場合には、④選別の条件を定めるための基準（外外通信選別条件設定基準）を定め、⑤サイバー通信情報監理委員会の承認を受けて、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（国外関係通信媒介中通信情報）の一部が複製され、内閣総理大臣の設置する設備（受信用設備）に送信されるようにするための措置を講ずることができる。

同措置においては、情報取得容量の上限や期間についての制限が設けられている。情報取得容量については、国外関係通信媒介中通信情報のうち伝送容量の30％が上限とされる。措置期間は６月とされているが、サイバー通信情報監理委員会が承認する場合の条件として６月未満の期間を定めたときは、その期間となるほか、同委員会の承認を受けて、措置期間を原則６月、延長することができる（再延長する場合も同様）。

次に、特定の外国設備との通信情報を分析する必要が生じた場合における外内通信及び内外通信に係る措置については、条文上、「特定外内通信目的送信措置」、「特定内外通信目的送信措置」として規定されている。内閣総理大臣は、①外内通信又は内外通信であって、②重要電子計算機に対する国外通信特定不正行為に用いられていると疑うに足

---

[5] 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）（経済安全保障推進法）に定める15分野の特定社会基盤事業者のうち、特定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、当事者協定の対象としている。

[6] 取得通信情報は、媒介中通信情報又は当事者管理通信情報を複製した情報であって、内閣総理大臣が提供を受けたもの（その全部又は一部を複製し、又は加工したものを含み、提供用選別後情報であるものを除く。）と定義されている。

[7] 国外通信特定不正行為は、国外にある電気通信設備（国外設備）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と定義されている。また、特定不正行為とは、刑法（明治40年法律第45号）の不正指令電磁的記録等供用罪、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）（不正アクセス禁止法）上の不正アクセス行為、電子計算機を用いて行われる業務に係る刑法の業務妨害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、という類型の行為と定義されている。

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特定の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、③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をとることができる。措置期間について３月とされているほかは、外外通信目的送信措置と同等の内容が規定されている。

イ　自動選別（同第22条）

取得通信情報には、分析の対象要件に該当しない情報も含まれ得るため、自動的方法により選別を行う。具体的には、内閣総理大臣は、取得通信情報を取得したときは、当該取得通信情報の中から一定の要件を満たす機械的情報であるもののみを選別して記録する措置であって、その選別が完了する前に当該取得通信情報が何人にも閲覧その他の知得をされない自動的な方法（自動的方法）で行われるもの（以下「自動選別」という。）を講じなければならない。選別に関する一定の要件としては、外外通信、外内通信といった通信の送信元・送信先の要件が適合していることのほか、サイバー攻撃に関連すると考えられるＩＰアドレス、指令情報（コマンド）等であることが求められる[8]。

内閣総理大臣は、自動選別終了後、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。

ウ　基幹インフラ事業者等との当事者協定（同意）による通信情報の取得（同第３章）

基幹インフラ事業者等との間では、当事者協定によって通信情報を取得する。同意によらない場合と異なり、協定を締結したとき等に、協定の内容をサイバー通信情報監理委員会に通知することで足りる。

内閣総理大臣は、基幹インフラ事業者その他の電気通信役務の利用者との協定に基づき、当該利用者を通信の当事者とする通信情報の提供を受ける。このうち、内閣総理大臣と基幹インフラ事業者の間の協定については、相互に、相手方に対し、協定締結のための協議を求めることができ、相手方は、正当な理由がない限り、協議に応じなければならない。

内閣総理大臣は、当事者協定により取得した通信情報のうち、外内通信に係る通信情報に自動選別を講じ[9]、その情報（選別後当事者通信情報）を用いて、当該当事者が使用する電子計算機のサイバーセキュリティの確保に資する分析を行った上で、当該利用者に対して、個別の分析情報を提供するものとされている。

---

[8] 条文上は、以下の３要件のうち２つ以上を選別の条件に用いて行わなければならない。３要件は、①「当該取得通信情報に係る対象不正行為に関係がある電気通信の送信元又は送信先であると認めるに足りる状況のある電気通信設備のアイ・ピー・アドレス等」、②「当該取得通信情報に係る対象不正行為の実施に用いられるものと認めるに足りる状況のある指令情報」、③「当該情報を選別の条件に用いて自動選別を行うことにより当該取得通信情報に係る対象不正行為に関係がある電気通信、電子計算機又は電磁的記録の探査が容易になると認めるに足りる状況のある情報」である。

[9] 条文上、当事者協定に係る取得通信情報に外内通信以外の通信情報が含まれることが排除されてはおらず、自動選別により、分析対象の外内通信のみに選別される。なお、同意によらない通信情報の取得においては内外通信も対象とされているが、内外通信は当事者協定による通信情報の分析対象には含まれていない。

（３）通信情報の利用及び提供の制限（同第23条）

自動選別前の取得通信情報については、内閣総理大臣は、取得通信情報の自動選別を行う場合を除き、利用及び提供を行ってはならない。

自動選別により得られた選別後通信情報については、利用又は提供できる場合が限定されており、①当事者協定の協定当事者の同意を得て、自ら利用し、又は提供する場合、②特定被害防止目的の達成のために必要があると認めるとき等に、行政機関又は外国の政府若しくは国際機関に対しこの法律の所定の規定により選別後通信情報を提供する場合、③この法律の所定の規定の承認を求めるため等で、サイバー通信情報監理委員会に提供する場合の３類型においては、選別後通信情報を、特定被害防止目的以外の目的のために自ら利用し、又は提供することができる。

（４）選別後通信情報の取扱い（同第24条～第28条）

選別後通信情報については、（３）の利用等の制限のほか、その取扱いについて非識別化措置、保存期間、安全管理措置等が定められている。

選別後通信情報は、機械的情報のみに限られる一方で、電子メールアドレス等、特定の個人を識別することとなるおそれが大きい情報（特定記述等）が含まれ得る。このため、特定記述等について他の符号等に変換する等によって他の情報と照合しない限り特定の個人を識別することができないようにするための非識別化措置を講じなければならない。ただし、特定被害防止目的の達成のために特に必要があると認めるときは、特定記述等を利用することができるようにするための再識別化措置が可能とされる。

選別後通信情報が記録された文書の保存期間については、自動選別が終了した日の属する年度の翌年度の初日から起算して２年を超えない範囲内で、その期間を設定しなければならず（２年を超えない範囲内で延長可）、期間が満了したときは、できる限り速やかに消去しなければならないとされる。

取得通信情報の安全管理のための安全管理措置としては、取扱い業務を行わせる職員の範囲を定める等、内閣府令で定める措置を講じなければならないとされる。また、選別後通信情報の取扱いに関する事務に従事する内閣府の職員等には守秘義務が課され、違反した場合、３年以下の拘禁刑又は100万円以下の罰金に処せられる。

（５）サイバー通信情報監理委員会における監視・監督（同第10章）

サイバー対処能力強化法案では、独立機関として、いわゆる三条委員会[10]であるサイバー通信情報監理委員会を設置することとされている。同委員会は、委員長と委員４人の計５人で構成され[11]、内閣総理大臣による同意によらない国外関係通信の取得に際しての遅滞のない審査・承認、通信情報の取扱いに対する継続的な検査、アクセス・無害化措置に際しての審査・承認等の事務を担う。

---

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

[11] 委員長及び委員は、法律又はサイバーセキュリティ等のいずれかに関して専門的知識及び経験並びに高い識見を有する者で人格が高潔である者のうちから両議院の同意を得て内閣総理大臣が任命するとされている。

同委員会は、毎年、内閣総理大臣を経由して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ものとされている。

この点、衆議院におけるサイバー対処能力強化法案の修正により、国会報告の具体的内容が追加された。同修正により、通信情報の利用に関する報告事項については、各送信措置の承認に係る件数、自動選別、取得通信情報の取扱い等に係る検査の結果の概要等を報告することが明記された。

（６）通信の秘密への配慮等についての衆議院修正

サイバー対処能力強化法案においては、その政府原案に通信の秘密への配慮規定が盛り込まれていなかったが、（５）の衆議院修正に加え、「この法律の適用に当たっては、第１条に規定する目的を達成するために必要な最小限度において、この法律に定める規定に従って厳格にその権限を行使するものとし、いやしくも通信の秘密その他日本国憲法の保障する国民の権利と自由を不当に制限するようなことがあってはならない。」との規定を追加する修正が加えられた。

さらに、同法案の修正により検討規定も創設され、通信情報の利用に関する規定の施行後３年を目途として、特別社会基盤事業者（基幹インフラ事業者）による特定侵害事象等の報告（インシデント報告）、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通信情報の取得、当該通信情報の取扱い等の状況について検討を加え、必要があると認めるときは、その結果に基づいて所要の措置を講ずるものとされている。

（７）施行期日

通信情報の利用に関する規定は、公布の日から起算して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する。また、サイバー通信情報監理委員会の設置に関する規定は、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する。

４．国会における主な議論[12]

（１）憲法に定める通信の秘密等との関係

ア　通信の秘密の解釈と通信情報の利用との関係

通信情報の利用に当たっては、前述のとおり、憲法第21条第２項に定める通信の秘密に配慮する必要がある。この解釈について村上誠一郎総務大臣は、「国家が通信の秘密を含む通信情報を確認することは、通信の当事者の有効な同意がある場合や、本法のように法令に基づく行為など、違法性阻却事由が認められる場合を除き認められないと考えている」旨答弁した[13]。

さらに、サイバー対処能力強化法案における通信情報の利用と通信の秘密との関係について問われた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

[12] 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。
[13] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（令7.4.3）

重要な機能がサイバー攻撃によって損なわれることを防ぐという高い公益性があること、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って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などから、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。また、政府としては、コミュニケーションの本質的な内容ではない機械的情報も、通信の秘密との関係で、適切に保護されなければならないと考えている[14]。そのため、メールアドレス等については、他の情報と照合しない限り特定の個人を識別することができないようにする非識別化措置を講じることとしている」旨答弁した[15]。

イ　通信の秘密の尊重に係る衆議院における修正に至る議論

政府提出の原案では、通信の秘密を尊重する旨の明文規定は置かれていなかった。この理由について平国務大臣は、「通信の秘密については、憲法上規定されている権利であることから、条文上明記せずとも、当然のこととして、本法律案により通信の秘密が不当に侵害されることが許容されるものではない」旨答弁した[16]。

これに対して、例えば通信傍受法[17]や特定秘密保護法[18]において、通信の秘密を尊重する旨の規定が置かれていることとの関係について問われた。これに対して平国務大臣は、「通信傍受は、まさに犯罪捜査目的で、令状は取るとはいえ、コミュニケーションの中身を聞くという重大な通信の秘密に抵触することであり、特定秘密も、まさに何を特定秘密にするのかしっかり見なければいけないということで、こういった文言が入っていると思う」旨答弁した[19]。

こうした議論を踏まえて行われた衆議院修正について、修正案提出者からは、「他の法律に倣って明記すべきだと考えて修正した」旨の説明があった[20]。この修正への評価を問われた石破総理は、「政府の立場から評価することは差し控えるが、修正に係る議論の内容を十分に踏まえながら、関係職員への周知や啓発等により、通信の秘密を尊重、徹底するよう取り組んでいく」旨答弁した[21]。

また、基本方針[22]等との関係については、「政府としても、通信の秘密を尊重し、これを不当に侵害することのないよう、法律の規定を確実に遵守していくことは当然のことである。本法律案に基づく下位法令、基本方針などについても、修正に至る議論の内容

---

[14] 通信の秘密の保護対象とされる範囲については、さらに平将明国務大臣（サイバー安全保障担当大臣）から、「政府としては、ＩＰアドレスや送信日時等のメタデータも通信の秘密に該当し得るものであり、適切に保護されなければならないと考えている」旨答弁した（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））。

[15] 第217回国会衆議院本会議録第９号（令7.3.18）

[16] 第217回国会衆議院内閣委員会議録第８号１～２頁（令7.3.26）

[17] 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）

[18] 特定秘密の保護に関する法律（平成25年法律第108号）

[19] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）

[20] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）

[21] 第217回国会参議院本会議録第14号（令7.4.18）

[22] サイバー対処能力強化法案第３条では、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の基本的な方針（基本方針）について閣議決定することとされている。

を踏まえつつ、通信の秘密に十分に配慮をしながら定めることとしており、通信の秘密の尊重を徹底していきたい」旨答弁した[23]。

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。）[24]においては、「一　通信の秘密及びプライバシーの保護を十分に尊重することと通信情報の利用及びアクセス・無害化措置の円滑な実施とのバランスをとり、効果的に制度を運用すること。あわせて、平素から政府により通信情報が監視され得るのではないかとの国民の懸念を払拭できるよう、積極的な広報活動等により制度に対する国民の理解醸成を図ること。」とされた。

ウ　令状主義との関係

憲法第35条では、「何人も、その住居、書類及び所持品について、侵入、捜索及び押収を受けることのない権利は、第33条の場合を除いては、正当な理由に基いて発せられ、且つ捜索する場所及び押収する物を明示する令状がなければ、侵されない。」（第１項）、「捜索又は押収は、権限を有する司法官憲が発する各別の令状により、これを行ふ。」（第２項）と規定されている。

通信情報の利用と憲法第35条に定める令状主義との関係について問われた平国務大臣は、「憲法第35条と行政手続の関係については、最高裁判所の判例があるものと承知している[25]。これを踏まえ、本法案の通信情報の送信の措置については、行政上の目的を達成するための手続で、刑事責任の追及を目的とする手続ではなく、そのための資料の取得、収集に直接結び付く作用を一般的に有するものではないこと、国家及び国民の安全の確保等の観点から重要な電子計算機に対する不正な行為による被害を防止することを目的としている点で高い公益性を有すること、本措置は他の方法によっては実態の把握が著しく困難である場合に限り行われるもので、かつ取得した通信情報からは機械的情報のみが自動的に選別され分析されること、さらには、サイバー通信情報監理委員会の検査によりこれらの遵守を確保すること等により通信の当事者の権利制限を必要最小限度にとどめることとしていることから、裁判官の令状発付を要することとしなくても憲法第35条の法意に反しないと考えている」旨答弁した[26]。

---

[23] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

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

[25] 川崎民商事件（最大判昭47.11.22刑集26巻９号554頁）において、旧所得税法上の質問検査権（収税官吏が税務調査にあたり納税義務者等に質問し、帳簿等の物件を検査でき、これを拒否した者には罰則が適用されるという制度）に基づく調査を拒否して起訴された被告人が、質問検査が、令状主義（憲法第35条）、黙秘権の保障（同38条）に反すると主張した。これに対して最高裁は、35条・38条は行政手続にも及ぶ（適用される）ことを原則的に認めつつ（黙秘権は「純然たる刑事手続においてばかりでなく、それ以外の手続においても、実質上、刑事責任追及のための資料の取得収集に直接結びつく作用を一般的に有する手続にはひとしく及ぶ」。）、質問検査権については、①刑事責任の追及を目的とする手続ではないこと、②実質上、刑事責任追及のための資料の取得収集に直接結びつく作用を一般的に有するものではないこと、③強制の度合が低く、直接的・物理的な強制と同視すべき程度に達していないこと、④租税の公平な徴収等の公益目的を実現するために実効性のある検査制度が不可欠であることを理由に、違憲ではない、と判示した（芦部信喜著、高橋和之補訂『憲法 第８版』（岩波書店、令和５年９月）268頁）。

[26] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

（２）各情報を取得する目的及び内内通信情報の取扱い

ア　各情報を分析する目的

通信情報のうち、内内通信は分析の対象外とされる一方、外外通信、内外通信及び外内通信が分析の対象とされている[27]。その理由について、内閣官房は、「まず、外外通信を分析することについては、攻撃用のインフラを構成するボット[28]やＣ２サーバ[29]などの設備は主として国外に所在すると考えられることから、国外の設備から国外の設備に送信される外外通信により、国外の攻撃インフラの実態を把握しようとするものである。その上で、外内通信の分析については、既に把握した国外の攻撃用インフラから国内への攻撃を捉えるために、内外通信の分析については、マルウェア等に感染した国内の設備から国外の設備に対し不正に情報を漏えいするなどの攻撃に関係する通信がなされていると疑われる場合に、例えばその実態を把握するためにそれぞれ必要となるものと考えている」旨答弁した[30]。

イ　内内通信を分析する必要性に係る議論

内内通信が対象外とされたことに関連して、内内通信を分析する必要性について議論が行われた。まず、衆議院では、平国務大臣からは、「立法事実として、サイバー攻撃関連通信の99.4％が国外からだというデータ[31]を基にこの法律を作成しており、外外、その次に外内、その次に内外を分析すれば足りる。今回の法案では、基幹インフラの重要なサーバを守るという目的の上で、機械的情報を分析するという立て付けでやってきたので、そもそも、内内を前提に法律も作っていないし、議論もしていない」旨答弁した[32]。さらに、将来的に内内通信を対象とする場合や機械的情報の範囲の変更が必要となる場合には、法律の立て付け自体を議論し直すことが必要ではないかとの指摘に対しては、「今回の法律の立て付けとは全く違うため、憲法の制約の中で、公共の福祉と通信の秘密をどうバランスを取りながらその法律を構築していくのかということになる。イメージとしては、別の法律をしっかりと憲法の制約の範囲内でどう作るかという議論が必要だろうと思う」旨答弁した[33]。

次に、衆議院修正において検討規定が盛り込まれたところ、参議院においては、その対象に内内通信が含まれるか質疑があった。これに対して衆議院修正案提出者は、「内内通信も当然に含まれるものと考えている。この利用の可否も含め、慎重に検討が加えら

---

[27] なお、国外の通信情報を取得することが主権侵害に当たり得るかについて、石破総理は、「自国領域を通る国際通信の取得と利用は、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」旨答弁した（第217回国会衆議院本会議録第９号（令7.3.18））。

[28] 攻撃者は、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、多段的に組み合わせて攻撃用のボットネットワークを構成し、利用しているとされる。

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

[30] 第217回国会衆議院内閣委員会議録第６号５頁（令7.3.19）

[31] 前掲脚注４参照

[32] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（令7.4.3）

[33] 第217回国会衆議院内閣委員会総務委員会安全保障委員会連合審査会議録第１号（令7.4.3）

れ、必要があると認めるときは所要の措置が講ぜられると考えている」旨答弁した[34]。

また、内内通信が全体の通信に占める割合について、平国務大臣は、「総務省によれば、国外と交換されるトラフィックは6.4％、内内通信は93.6％」である旨答弁した[35]。この点、今般の法案によって分析対象となる通信情報は限定的であるが、将来的に政府が幅広く情報を見ることになるとの懸念に対して、平国務大臣は、「野放図に拡大するのではないかという懸念は当たらず、自動選別で、あくまで疑わしいＩＰアドレス、コマンド、ソフトウェアなどを、ある程度特定して複数以上で検索するため、どんどん拡大していくことはこの法律の中でも認めておらず、考えていない」旨答弁した[36]。

（３）当事者協定に関する議論

ア　協定が事実上の強制になる懸念

当事者協定については、政府、基幹インフラ事業者の双方に対して、協議に応じることが義務付けられている一方、協定の締結の義務付けまでは行われていない。他方で、事実上の強制につながるのではないかとの懸念について問われた。これに対して石破総理は、「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に対して協定の締結を強制することはない」旨答弁した[37]。

さらに、協定を締結しなかったとしても不利益を与えないことを明確にすべきとの指摘に対して、平国務大臣は、「仮に不利益な取扱いを背景として協定の締結が得られたとしても、同意に基づく当事者協定とは言えず、この協定に基づく通信情報の取得は、通信の秘密との関係で問題が生じる可能性があると考えている。したがって、政府としては、協定を締結しなかった事業者に対して不利益な取扱いをすることはなく、この法律の趣旨から明定すべき必要もないと考えている」旨答弁した[38]。

この点、参議院附帯決議においては、「五　当事者協定の締結が事実上の強制とならないよう留意するとともに、協定を締結しない場合に不利益を与えない旨を基本方針等に明記すること。」とされた。

イ　当事者協定に係る通信情報取得について要件が課されていない理由

外外通信目的送信措置等、同意によらない通信情報の取得においては、措置を行う要件が法文上定められているが、当事者協定に基づいて通信情報を取得する際には、こうした要件は定められていないところ、その理由について質疑があった。これについて内閣官房は、「当事者協定は、通信の当事者である基幹インフラ事業者等が送受信する通信情報をその事業者等の同意を得て利用する制度であり、通信当事者の同意によらずに通信事業者が伝送中の通信情報を取得するという外外通信目的送信措置等とは前提が大きく異なる。そのため、同意によらない利用の場合と同じ要件を定める必要があるとは言えないと考えている。その上で、当事者協定により取得する通信情報の範囲や取得する

---

[34] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[35] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
[36] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
[37] 第217回国会衆議院本会議録第９号（令7.3.18）
[38] 第217回国会衆議院内閣委員会議録第７号９頁（令7.3.21）

期間は協定によってあらかじめ定めることとしており、その際は、法目的の達成のために必要な範囲内に限り、かつ協定当事者も必要であると認めた内容を定めることとなるということは当然であり、必要性もない状態で通信情報を取得するということではない」旨答弁した[39]。

ウ　外内通信以外の情報の取得自体は許容されることの是非

当事者協定に基づく通信情報の分析対象は外内通信に限定されている一方、政府が情報を取得する時点においては、外内通信に限らず内内通信も含めた情報を取得することが可能とされ、その上で、外内通信のみに自動選別を行うとされている。この点が、内内通信の利用に当たるのではないかとの指摘に対して平国務大臣は、「通信当事者との協定において提供を受ける通信情報をあらかじめ外内通信情報に限定することは、協力する通信当事者にとっては負担となり、技術的に困難な場合もあることから、取得する通信には内内通信が含まれる場合もあると考えている。ただし、そうした場合であっても、本法律案で、内閣総理大臣が分析を行うことができるのは、当事者協定により提供を受けた通信情報のうち、人による閲覧等の知得を伴わない自動的な方法により選別された外内通信の通信情報に限定されることになり、内内通信の通信情報は閲覧されることなく消去される。そのため、当事者協定により内内通信の通信情報を利用しているとの指摘は当たらない」旨答弁した[40]。

エ　当事者協定を締結する事業者等の範囲

当事者協定を締結する事業者等について内閣官房は、「政府における人員あるいは予算には限りがあるところ、社会全体の重大サイバー攻撃対策のため、重要度が高いと考えられる分野や事業者を優先して協議を求めることが想定される。優先順位について、具体的には、サイバー攻撃の状況、攻撃を受けた場合の被害の範囲といった事情も踏まえて検討していきたい。また、協定の締結については、基幹インフラ事業者の各法人単位で行うことが基本と考えており、子会社との協定の締結については、個々の事例に即して判断していきたい」旨答弁した[41]。

オ　当事者協定に基づき基幹インフラ事業者等から提供される情報の内容

協定を締結した基幹インフラ事業者等から提供されることとなる通信情報の内容について問われた内閣官房は、「例えば事業者のウェブサイトにおいて送受信される通信情報の提供を受ける場合には、当該ウェブサイトにユーザーから入力された住所、電話番号等が含まれる可能性はある。しかし、本法案においては、内閣総理大臣が通信情報を取得したときは、機械的情報のみを選別して分析することとし、それ以外のものを消去する措置を講じなければならないこととされている。そのため、提供を受けた情報に通

---

[39] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

[40] さらに内閣官房は、「条文上は、サイバー対処能力強化法案第22条第１項に自動選別の実施があり、第15条の当事者協定の規定により取得した取得通信情報については、外内通信により送受信が行われたものであることということは要件として書かれており、要件を満たす機械的情報であるもののみを選別して記録する措置を講じることが規定されている。あわせて、第30条に、自動選別を行ったときは、サイバー通信情報監理委員会に通知することとされ、それが適正に行われているかチェックを受ける仕組みが規定されている」旨答弁した（第217回国会参議院内閣委員会会議録第13号（令7.5.13））。

[41] 第217回国会衆議院内閣委員会議録第10号（令7.4.2）

常のユーザーが入力した住所、電話番号等が含まれていたとしても、それらが分析の対象となることは想定されていない」旨答弁した[42]。

カ　当事者協定に基づき政府から提供される分析情報の内容

当事者協定に基づく通信情報を取得した政府は、分析結果を当事者に提供することとされている。その内容について問われた内閣官房は、「協定は、双方がそのメリットを認めて初めて締結がなされると理解している。通信情報の分析結果の提供については、協定当事者との協議を踏まえて、協定の中で方法を定めていくが、例えば、通信情報を分析したことで得られた内容に加え、可能であれば、検出されたサイバー攻撃に対してどのような対策を講じればよいかといった情報も含めることも想定している。また、情報提供のタイミング、頻度についても、できる限り有用なものとなるように配慮していきたい」旨答弁した[43]。

（４）同意によらない通信情報の取得・分析に関する議論

ア　外外通信に係る情報の取得要件

外外通信に係る情報を取得する際には、他の方法ではその実態の把握が著しく困難であることが要件の一つとされている。これについて平国務大臣は、「他の方法とは、例えば本法律案に基づくインシデント報告の規定により事業者から提供された情報や、当事者協定により取得した通信情報、外国政府から提供された情報などを基に攻撃インフラの実態を把握し、重要電子計算機の被害を防止することを想定している。政府としては、例えば攻撃元の隠蔽のため国外のボット等を交えた攻撃インフラが用いられていると考えられる場合などについてはこうした他の方法による被害の防止が著しく困難であると考えており、迅速かつ適切な判断を行うことができるよう必要な体制の整備を図っていきたいと考えている」旨答弁した[44]。

イ　外外通信等に係る情報の取得容量及び期間

まず、取得容量に30％の上限を設けた理由等を問われた平国務大臣は、「外外通信の分析においては、あらかじめ対象のサーバ等を特定して通信情報を分析するものではないことから、分析される潜在的な容量についての上限を設定しておくことが望ましいと考えられたため、外国の法制度を参考に上限を規定することとしたものである。具体的には、ドイツの連邦情報局法において、外外通信に相当する電気通信に含まれる通信情報の利用の措置を講ずる場合、対象となる通信量は既存の電子通信網の30％を上限として

---

[42] 第217回国会衆議院内閣委員会議録第７号12頁（令7.3.21）。なお、機械的情報の具体的内容としては、メールアドレスやＩＰアドレス以外に、例えば携帯電話の番号、ＬＩＮＥのアカウントの名前等も含まれるとされる（第217回国会衆議院内閣委員会議録第７号３頁（令7.3.21））。

[43] 第217回国会衆議院内閣委員会議録第６号５頁（令7.3.19）

[44] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）。なお、サイバー通信情報監理委員会における承認プロセスについて平国務大臣は、「要件を満たす場合に、内閣府が措置の必要性や要件が満たされていると認めた理由、政府に通信情報を送信することとなる電気通信事業者の設備が国外関係電気通信設備であること、自動選別の選別条件を設定する基準等をサイバー通信情報監理委員会に示して承認を求めることになる。そして、承認を得た場合に、通信情報の送信を開始し、通信情報を取得する」旨答弁した（第217回国会衆議院内閣委員会議録第11号（令7.4.4））。

いるものと承知しており、このドイツの制度を参考にして30％としている。これにより、現時点では、通信情報の利用を必要最小限度の範囲にとどめつつ、攻撃インフラの実態把握という目的を達成することが可能になるものと考えている。30％であっても十分目的の達成には適切な量のデータが得られるものと想定している」旨答弁した[45]。

次に、措置を講ずる期間の考え方や常時取得の懸念について問われた内閣官房は、「外外通信目的送信措置は、国外から行われる重大サイバー攻撃の実態が不明である場合に外外通信を分析してその実態を把握するために実施するものであり、分析の対象となる通信情報を特定の国外設備等に限定せずに一定の期間受信を継続する必要がある。この措置期間を６月としたのは、類似の海外制度であるイギリスの調査権限法における規定を参考としたものである。また、措置期間については、本法律案の規定により延長することも可能としており、再延長も可能となっている。一方で、延長する場合にはその都度サイバー通信情報監理委員会の事前の承認を受ける必要があり、延長による措置が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といった要件を引き続き満たしているかどうかを改めて確認した上で延長が承認される。また、委員会は措置期間の延長に係る承認の求めとその承認の件数について毎年国会に報告することとされている。このため、通信情報の取得が漫然と継続するようなことはないと考えている」旨答弁した[46]。

ウ　電気通信事業者の協力

外外通信目的送信措置等の通信情報を取得するに当たっては、電気通信事業者に協力を求めることとされている。この点、有識者会議提言においては、電気通信事業者が直面し得る訴訟等のリスクについて回避策を十分に検討していくべきであると指摘されていることとの関係について質疑があった。これに対して平国務大臣は、「例えば外外通信目的送信措置等の実施について、サイバー対処能力強化法案第20条、第32条、第33条により、機器の接続その他の必要な協力を求めることとしている。政府では、提言の内容も踏まえ本法律案の検討を行い、具体的には、電気通信事業者は通信の当事者との関係で通信の秘密を守る義務があることから、政府の責任において通信の秘密に制約を加えるものである外外通信目的送信措置等の実施に協力する法的根拠を明確にすること等により、電気通信事業者が法的責任を問われることがないように措置をすることとした。電気通信事業者が政府からの協力の求めに対し、その保有する設備や技術では対応困難であるなどの正当な理由があれば拒むことができることとしている」として、「本法律案が成立した場合には、有識者会議提言も踏まえつつ、こうした規定の運用の開始に向けて更なる必要な検討を行っていきたい」旨答弁した[47]（費用負担の在り方について（９）参照）。

なお、参議院附帯決議（第四後段）では、「通信情報を提供する電気通信事業者の訴訟リスクの軽減や実際に事務を取り扱う労働者の権利保護の重要性に十分配意すること。」

---

[45] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[46] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
[47] 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）

とされている。

（５）自動選別等の在り方

自動選別に用いるシステムの検討状況、諸外国の参考事例について内閣官房は、「自動選別については、例えば、ドイツの連邦情報局法で、特定の法人、居住者の個人データを分析しないよう自動的にフィルタリングする技術を用いることとしている。また、イギリスの調査権限法では、取得したデータについて、許可状に指定された運用目的のために必要かつ比例的な範囲に制限するため、できる限り自動的な方法で用いることとしている。このような諸外国の例については、本法案の自動選別の考え方と類似する部分があるものと考えている。また、非識別化措置については、主要国において通信情報の利用を規定している法制度においては、同様の措置を規定している例は承知していない。いずれにしても、自動選別や非識別化措置については、諸外国の例を参考にしていくこともあるが、利用可能な国産の技術も積極的に取り入れて、しっかりと開発していきたい」旨答弁した[48]。なお、自動選別後の情報の消去方法については、「選別後に、選別元の情報を次々と必要のない別の情報で上書きしてしまうことを想定しており、復元できないように消去していることについて、サイバー通信情報監理委員会が継続的に検査し、遵守を確保する」旨答弁した[49]。

次に、取得通信情報の安全管理措置について問われた石破総理は、「サイバー対処能力強化法案では、内閣総理大臣は、取得した通信情報について、その安全管理のために必要かつ適切な措置を講じなければならない旨を規定するとともに、サイバー通信情報監理委員会がその遵守状況を継続的に検査する。安全管理措置の具体的な内容としては、例えば通信情報の取扱いの業務を行わせる職員の範囲を適切に定めることなどが挙げられるが、詳細については今後内閣府令で定める。サイバー通信情報監理委員会とも協議し、パブリックコメントの内容も考慮した上で適切な安全管理措置が講じられるよう検討を行っていく。安全管理措置のために必要な予算規模を現時点で示すことは困難であるが、法案が成立した場合には、必要な予算が十分に確保できるよう取り組んでいく」旨答弁した[50]。

参議院附帯決議では、「十　政府の体制整備に当たっては、両法の実効性のある運用に必要な人員及び組織体制を確保・構築するとともに、通信情報の取得、自動選別等に必要となる設備等の整備のために十分な予算を確保すること。」とされた。

（６）選別後通信情報の利用目的の制限と犯罪捜査等との関係

ア　選別後通信情報の利用

サイバー対処能力強化法案第23条では、選別後通信情報の利用目的が制限されている一方で、特定被害防止目的以外の目的で利用することは可能とされている。この妥当性、

---

[48] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）。なお、国産技術の活用等に関して、参議院附帯決議（第二十三前段）において、「国産技術を核としたサイバー対処能力の向上のため、機器の開発を含めて支援するとともに、ＡＩ等の新たな技術を活用したサイバー対処業務の効率化について、民間等の取組状況やニーズを踏まえつつ、官民で連携して必要な施策を検討し、推進すること。」とされた。

[49] 第217回国会衆議院内閣委員会議録第６号11頁（令7.3.19）

[50] 第217回国会参議院本会議録第14号（令7.4.18）

とりわけ犯罪捜査に利用することが可能かどうかについて質疑が行われた。

まず、選別後通信情報を目的外で利用し、捜査に利用することの有無について問われた内閣官房は、「本法律案第23条第４項第１号の規定により、協定当事者の同意を得た場合にはその利用目的は必ずしも特定被害防止目的に限られないということになる。しかしながら、選別後通信情報であり、自動的な方法による選別により、一定の重大なサイバー攻撃に関係があると認めるに足りるＩＰアドレスあるいはコマンドなどの機械的情報に限定されたものであり、また非識別化措置も講ずるということから、いずれにしても、サイバーセキュリティに関係する業務で用いられることが想定される。したがって、通信情報保有機関においてサイバーセキュリティと無関係な業務のために利用されることは、協定当事者の同意がある場合を考慮に入れたとしても、通常想定されるものではない」旨答弁した[51]。

この点、サイバーセキュリティに関係する業務で用いられることについてさらに確認を求められ、内閣官房は、「特定被害防止目的とは、通信の秘密に十分配慮するために、選別後通信情報の利用範囲を限定するものとして、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を基本として規定しているものであり、当事者協定により取得し、選別して得た選別後通信情報については、これに加え、協定当事者の使用する電子計算機に対する特定不正行為による被害を防止する目的も含むものとして規定している。一方で、法目的は、重要電子計算機に対する不正な行為による被害の防止を図ることであり、重要電子計算機の被害防止にもつながり得るサイバーセキュリティの取組が広く含まれるものと考えている。重要電子計算機に必ずしも限られない一般の電子計算機のサイバーセキュリティの向上を目的として利用することは、特定被害防止目的には当たらないものであるが、法目的の範囲内にはなる利用に当たる場合がある。具体的には、例えば、一般の電子計算機のサイバーセキュリティ向上のために民間のサイバーセキュリティ事業者が選別後通信情報を利用することや、基幹インフラ事業者と同一の業界に属する小規模事業者の一般の電子計算機に対する個別のサイバー攻撃の対処のために選別後通信情報を事業者団体が利用することが考えられる」旨答弁した[52]。一方、選別後通信情報の利用範囲を限定する明文規定を置く必要性について平国務大臣は、「法案において既に個別かつ一律に限定されていると考えており、修正は必要ない」旨答弁した[53]。

そして、協定当事者の同意については、「当事者協定により取得した通信情報の他目的利用に当たっては、協定当事者が他目的利用に関する同意の内容について十分に理解した上で同意をすることが必要であると考えている。より具体的には、例えば協定当事者との同意の中では、①他目的利用される選別後通信情報の範囲、つまりサイバー攻撃に関係があると認めるに足りるものであり、かつ外内通信に限られ、かつ機械的情報のみに限定される情報のうち、更にどの範囲の情報に限って利用するか、②他目的利用する

---

[51] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[52] 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
[53] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）

主体はどこか、③具体的な利用の目的は何か、などを明確にしておくことが必要であると考えており、協定当事者が、これらの事項を適切に理解した上で同意がされるよう、協定当事者と事前に丁寧な協議を行っていきたい。加えて、他目的利用の際は、例えば他目的利用に関する事項を含めた同意の範囲が明示された書面を交わすなどの厳密な方法を取ることにより、実効的にも明確な同意とすることを考えている」旨答弁した[54]。

イ　犯罪捜査との関係

選別後通信情報が犯罪捜査に利用される懸念について問われた警察庁は、「選別後通信情報は意思疎通の本質的な内容を含まない機械的情報であるため、そもそも刑事事件の証拠としてこれを利用することが必要となる場面は極めて限定的、例外的と考えている」として、「仮に捜査に利用する場合には、令状を取得して選別後通信情報を差し押さえるなど、個別具体の状況に応じて、刑事訴訟法（昭和23年法律第131号）の規定に基づく厳格な手続にのっとって適切に対応することとなる」旨答弁した[55]。また、犯罪捜査に利用することができないような根拠規定を置く必要性について問われた内閣官房は、「法制上の確立された解釈として、犯罪捜査とは、捜査機関が、犯罪があると思料するときに、事案の真相を明らかにし、刑罰法令を適用実現するため、犯人及び証拠を発見、収集、保全する手続を指すということであり、本法案で、通信情報を利用する目的である重要電子計算機に対する一定の国外通信特定不正行為による被害を防止するという行政上の目的とは明確に異なるものであると考えている。したがって、捜査のための利用が特定被害防止目的に当たると解するとは考えておらず、提出した法案の内容により誤解が生じるおそれはないと考えている」旨答弁した[56]。

さらに、石破総理は、「他目的利用をする場合であっても、そもそもこの法律の目的規定において、重要な電子計算機に対する不正な行為による被害の防止を図ること、つまりサイバーセキュリティ対策に関するものと規定され、この目的の範囲を超えた利用は第１条に定めた法目的に反するので許容されないと考えている。この法目的に犯罪捜査目的が含まれることはなく、本法律案に基づく他目的利用により犯罪捜査のために通信情報を提供することも許容されないと考えている。その上で、選別後通信情報が法目的の範囲内で適切に利用されていることなどについても、サイバー通信情報監理委員会が継続的に検査を行うことを想定している。これは本法案第63条第２項に定めているが、これらの規定により、適切な目的での選別後通信情報の利用が担保されることになると考えている」旨答弁した[57]。

この点、参議院附帯決議では、「六　内閣総理大臣が取得した情報等については、安全

---

54 第217回国会参議院内閣委員会会議録第13号（令7.5.13）
55 第217回国会衆議院内閣委員会議録第10号（令7.4.2）
56 第217回国会衆議院内閣委員会議録第10号（令7.4.2）
57 第217回国会参議院内閣委員会会議録第14号（令7.5.15）。なお、特定被害防止目的と武力攻撃事態との関係については、内閣官房から、「通信情報の利用については、まず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制度検討を行ったものであるが、武力攻撃事態においても重大なサイバー攻撃が発生するおそれがあることから、こうした攻撃から重要電子計算機に対する被害を防止する目的である特定被害防止目的のため、選別後通信情報を利用することが可能である」旨の答弁もなされた（第217回国会衆議院内閣委員会議録第10号（令7.4.2））。

管理措置等に万全を期すとともに、情報提供の際には、被害を受けた事業者等の権利利益の保護に十分に配慮すること。当事者協定に基づく選別後通信情報の利用及び提供については、犯罪捜査目的ではなく、サイバーセキュリティ対策に係る場合に限定すること。」とされた。

（７）政府における情報分析能力の向上策

政府は、取得した通信情報の分析を行い、サイバーセキュリティの向上につなげていく必要があるが、そのための情報分析能力の構築について平国務大臣は、「まず、本法案により、政府としては、基幹インフラ事業者等からのインシデント報告の受領や通信情報の収集、分析が可能となり、より早期かつ効果的にサイバー攻撃を把握して対応することができるようになると考えている。また、政府においては、令和６年７月に、内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）に、サイバー空間におけるインテリジェンスを担当するサイバー対処・情報ユニットを設置した。ＮＩＳＣにおける複数の幹部職員の設置や定員、予算の大幅な拡充を行うこと等により、情報収集、分析を始めとしたサイバー対応能力の機能強化に向けて、体制の抜本的強化を図っている。さらに、サイバー安全保障分野における情報に加え、それらと関連したサイバー以外の軍事情報や外部情報等も効果的に活用することが重要である。このため、内閣官房に設置する新組織においては、関係省庁と緊密に連携の上、これらの情報を効果的に分析する体制を構築し、政府全体としてインテリジェンス機能の強化に努めていく」旨答弁した[58]。

この点、参議院附帯決議では、「十一　今般の新制度には多くの行政機関が関与することに鑑み、省庁間連携に万全を期すこと。特に、インテリジェンス機能については、内閣官房の新組織は関係機関と緊密に連携し、サイバー安全保障分野における情報やその他の外部情報等を効果的に収集、分析する体制を構築し、その強化を図ること。」とされた。

（８）サイバー通信情報監理委員会による監視・監督及び国会報告の在り方

通信情報の利用については、サイバー通信情報監理委員会が継続的検査を行うこととされている。この検査の内容や方法、頻度等について問われた平国務大臣は、「検査の具体的な方法としては、例えば、通信情報保有機関が委員会に行う通知の内容や状況を確認し、必要に応じ更に資料の提出を求める方法、定期的に通信情報保有機関で作成されている記録や資料の提出を求める方法、必要な場合に実地調査で通信情報の取扱状況を確認し、又は通信情報保有機関の職員に説明を求める方法などが考えられるものであり、また、これらの方法を組み合わせることも考えられているが、いずれにせよ、検査の有効性と効率性の観点を踏まえながら、委員会によって判断されるものと考えている」旨答弁した[59]。

次に、サイバー通信情報監理委員会の体制や人材の確保、育成について、平国務大臣は、「委員会については、アクセス・無害化措置の承認に係る審査を含め、事務処理が迅速かつ的確に行われるよう、法律や情報通信技術に関して専門的知識等を有する者を委員に任

---

[58] 第217回国会参議院内閣委員会会議録第11号（令7.4.24）
[59] 第217回国会参議院本会議録第14号（令7.4.18）

命することとしている。委員会事務局の体制についても、適切な専門性を有する職員により必要な規模の体制が確保できるようにすることとしたい。加えて、専門性の高い業務を円滑に実施できるよう、委員会事務局において、研修の実施などを通じ、人材の確保、育成に努めていくことも重要である」旨答弁した[60]。

さらに、衆議院において、同委員会からなされる国会報告の内容について具体的に規定する修正がなされたことに関連して、民主的統制を図る観点から、国会に対して規定内容以外の情報も公開する必要性について問われた。石破総理は、「サイバー通信情報監理委員会による国会への報告は、能動的サイバー防御に係る運用の透明性を高めて国民の信頼を得ていく上で極めて重要と考えている。衆議院における法案修正で追加された事項を上回る内容を国会に報告するか否かは、高い独立性を持つサイバー通信情報監理委員会において判断するものであり、国会報告の意義を踏まえて適切に判断される。なお、委員会による報告に加えて、国会から政府に対して国会法等に基づいて更なる報告などの求めがある場合には、関係法令にのっとって適切に対応していく」旨答弁した[61]。

（９）通信事業者に対する費用補償等の民間事業者の協力確保策

外外通信目的送信措置等においては、通信事業者に対して機器の接続その他の必要な協力を求めていることと関連して、通信事業者等に対する費用補償の必要性について問われた平国務大臣は、「英国、米国、フランス等における類似の制度においては、協力する通信事業者等に対し関連費用の補償を行う旨が規定されていると承知している。その上で、有識者会議提言の中では、このような電気通信事業者の協力に関して、協力を行う電気通信事業者に生じ得る通信ネットワーク運営に対する負担について、先進主要国の例も参考にしながら、回避策を十分に検討していくべきであるとし、加えて、通信ユーザーの利便性低下やコスト負担が生じるようなことも避けるべきであるとの提言を受けている。本法律案が成立した場合には、本提言の内容も踏まえて必要な検討を行っていく」旨答弁した[62]。

また、石破総理は、「通信情報の提供に関する協定の締結など、基幹インフラ事業者などによる協力を確保するためには、費用面の負担に適切に配慮することが重要であると考えている。この法案においては、事業者と締結する協定において、通信情報の提供のために

---

60 第217回国会参議院本会議録第14号（令7.4.18）

61 第217回国会参議院内閣委員会会議録第14号（令7.5.15）。関連して衆議院修正案提出者の本庄知史衆議院議員からは、「民主的統制をいかに実質化するかが重要なポイントである。そのためには、国会に対する報告の内容と同時に、受け手の国会側の受け皿の在り方が重要だと認識してきた」とした上で修正に至る経緯の説明があり、「施行後足らざるところがあれば、検討事項に基づいて、国会の受け皿の機能強化も改めて検討する、また、国会の受け皿の機能強化を待たずとも、民主的統制の確保のためには、国会が政府に説明を求める際には、誠実に対応し、説明責任を果たすことは当然だと考えている。国会法には秘密会の規定もあり、国会側の保秘の体制が整備されれば、様々な形で政府からの情報提供を受けることは可能だと考えている」旨答弁した（第217回国会参議院内閣委員会会議録第13号（令7.5.13））。これを受け、衆議院内閣委員会の附帯決議において、「十　サイバー通信情報監理委員会は、国会が実効的な監視機能を発揮するため、できる限り詳細かつ速やかに報告を行うこと。また、国会に対する報告については、今回の修正があったことを受け止め、法律上明示された事項以外の事項を含めてその内容の拡充に努めるものとし、国会が、当該報告等を契機として、両法に基づく措置に関し説明を求めた際には、民主的統制の重要性を踏まえ、誠実に対応し、その説明責任を果たすこと。」が盛り込まれた（参議院附帯決議第二十もおおむね同旨）。

62 第217回国会参議院内閣委員会会議録第11号（令7.4.24）

必要な施設又は施設の整備に関する事項についても定めるとしており、その中で費用負担についても定める方針である。事業者に過度な負担を負わせることがないようにしなければならない。丁寧に協議したい」旨答弁した[63]。

この点、参議院附帯決議（第十後段）では、「政府に協力を行う電気通信事業者に生じ得る通信ネットワーク運営に関する負担について、先進諸外国の例も参考にしながら、その回避策について責任を持って検討すること。」とされた。

５．小括

本稿では、能動的サイバー防御２法案のうち、通信情報の利用について取り上げ、国会論議を整理した。国会論議の中では、通信の秘密との関係やプライバシーの保護の観点を中心に多岐にわたる議論が展開され、その中では、通信情報の利用対象に内内通信を含めることについても議論がなされた。また、平時から通信情報を監視することや将来的に監視対象が広がることの懸念も示された。こうした懸念を背景として、衆議院で通信の秘密への配慮に関する規定が追加されており、同規定の趣旨を踏まえ、通信の秘密が侵害されないような運用に努めつつ、実効性のある取組とすることが求められよう。

他方、運用面に目を向けると、安全管理措置の具体的内容や自動選別に用いられるシステム等については、法成立後に検討することとされ、また、サイバー通信情報監理委員会が行う監視・監督についても、同委員会の設置後に委員会において運用の詳細を定めることとされているなど、今後の検討に委ねられ、国会審議で明確に方向性が示されなかったものも多い。

政府は、通信情報を収集・選別するための大規模な施設をつくる予定で、太平洋を横断する海底ケーブルの陸揚げ局が集まる千葉県の房総半島や三重県の志摩半島が候補地に挙げられているとする報道も見られている[64]。参議院附帯決議（第十前段）においても、「政府の体制整備に当たっては、両法の実効性のある運用に必要な人員及び組織体制を確保・構築するとともに、通信情報の取得、自動選別等に必要となる設備等の整備のために十分な予算を確保すること。」とされており、施行に向けた準備を注視する必要があろう。

（えのもと　なおゆき）

---

[63] 第217回国会参議院内閣委員会会議録第14号（令7.5.15）
[64] 『朝日新聞』（令7.5.17）など。