資料５

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（案）

令和７年〇月〇日
閣議決定

はじめに 3
第１章　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関する基本的な事項 4
第１節　本法による各種措置を行うこととなった背景・経緯 4
第２節　制度の基本的な考え方 5
第３節　政府内及び事業者等との連携と総合調整 6
⑴　政府内の連携と総合調整 6
⑵　事業者等との連携 7
第４節　通信の秘密の尊重 7
第５節　基本的な事項に関わる概念・定義の考え方 7
⑴　重要電子計算機の定義の考え方 7
⑵　機械的情報の考え方 9
第２章　当事者協定の締結に関する基本的な事項 10
第１節　基本的な考え方 10
第２節　当事者協定の締結を推進させるための基本的な事項 10
⑴　当事者協定の締結の推進に当たっての考え方 10
⑵　当事者協定の締結についての推進方策 11
第３節　当事者協定の締結に関する配慮事項 11
⑴　当事者協定の締結に向けた協議に関する配慮事項 11
⑵　当事者協定に基づく他目的利用に関する配慮事項 12
第３章　通信情報保有機関における通信情報の取扱いに関する基本的な事項 14
第１節　基本的な考え方 14
第２節　通信情報の利用を適切に機能させるための基本的な事項 15
⑴　通信情報の利用に係る能力構築の考え方 15
⑵　電気通信事業者の協力 15
第３節　通信情報の適正な取扱いに関する配慮事項 16
⑴　通信の秘密等への十分な配慮 16
⑵　通信情報の安全管理措置 18
⑶　提供用選別後情報の活用 18
⑷　サイバー通信情報監理委員会による監理 19
⑸　他法令の遵守に関する配慮事項 19

第4章　情報の整理及び分析に関する基本的な事項.....21
第1節　基本的な考え方.....21
第2節　報告等情報の収集の考え方.....21
⑴　特定重要電子計算機の届出の考え方.....21
⑵　特定侵害事象等の報告の考え方.....22
第3節　収集した情報の整理及び分析の考え方.....24
⑴　総合整理分析情報の作成の考え方.....24
⑵　提供用総合整理分析情報・周知等用総合整理分析情報の作成の考え方.....25
第4節　関係機関等への協力の要請.....25
第5節　事務の委託に関する考え方.....26
第5章　総合整理分析情報の提供に関する基本的な事項.....27
第1節　基本的な考え方.....27
第2節　総合整理分析情報等の提供先と提供する内容の考え方.....27
⑴　行政機関等に対する情報提供.....27
⑵　外国の政府等に対する情報提供.....28
⑶　協議会の構成員に対する情報提供.....28
⑷　特別社会基盤事業者に対する情報提供.....29
⑸　電子計算機を使用する者に対する周知等.....29
⑹　電子計算機等供給者に対する情報提供等、脆弱性情報に係る情報提供.....30
第3節　情報提供に当たっての関係行政機関の連携.....31
第4節　情報提供に当たって必要な配慮.....31
第5節　安全管理措置.....32
第6節　事務の委託に関する考え方.....32
第6章　協議会の組織に関する基本的な事項.....34
第1節　基本的な考え方.....34
第2節　協議会の取組内容・運営方針.....34
第3節　協議会で共有されるべき情報・協議する内容.....35
第4節　協議会の構成員.....36
第5節　安全管理措置.....37
第7章　その他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関し必要な事項.....38
第1節　制度及び基本方針の見直しに関する事項.....38
第2節　官民連携に関する関係省庁・関係機関等との連携等に関する事項.....38
第3節　アクセス・無害化措置との連携.....39

はじめに

「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」（令和７年法律第 42 号。以下「法」又は「本法」という。）第３条第１項は、内閣総理大臣が、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（以下「基本方針」という。）の案を作成し、閣議の決定を求めることとしている。また、同条第２項においては、基本方針において定める事項として、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関する基本的な事項、当事者協定の締結に関する基本的な事項、通信情報保有機関における通信情報の取扱いに関する基本的な事項、情報の整理及び分析に関する基本的な事項、総合整理分析情報の提供に関する基本的な事項、協議会の組織に関する基本的な事項並びにその他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関し必要な事項が掲げられている。

基本方針は、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という法目的を達成するため、法に基づく各般の施策を適切に機能させるための基本的な事項をあらかじめ示すとともに、これらの施策に係る事務の適正な実施を確保するための基本的な事項を示すために、これを定めるものである。

基本方針に基づき、内閣府は、特命担当大臣（サイバー安全保障）[1]の下、関係行政機関とともに法に基づく施策を総合的に推進する。これにより、サイバー攻撃により国家・国民の安全が害され、又は国民生活・経済活動に多大な影響が及ぶことを防ぐため、政府は、本法に基づき積極的に役割を発揮していく。また、その実行に当たっては、新たな司令塔組織として内閣官房に設置された内閣サイバー官（国家サイバー統括室）が、サイバー安全保障担当大臣[2]の下、総合調整機能を発揮し、政府一体となって、サイバーセキュリティ基本法（平成 26 年法律第 104 号）で政府が定めることとされているサイバーセキュリティ戦略[3]に基づく施策と相まって一体的、効果的かつ適正に実施していく。

なお、基本方針において使用する用語は、法において使用する用語の例による。

---

[1] 内閣府設置法（平成 11 年法律第 89 号）第9条第1項に規定する特命担当大臣であって、同項の規定により命を受けて同法第4条第1項第 37 号に掲げる事項に関する事務及び同条第3項第 27 号の7に掲げる事務を掌理するものをいう。

[2] サイバー安全保障の推進、サイバーセキュリティ（サイバーセキュリティ基本法（平成 26 年法律第 104 号）第2条に規定するサイバーセキュリティをいう。）の確保を担当する国務大臣をいう。

[3] サイバーセキュリティ基本法第 12 条第1項に規定するサイバーセキュリティ戦略をいう。

第１章　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関する基本的な事項

第１節　本法による各種措置を行うこととなった背景・経緯

昨今、厳しさを増す国際的な安全保障環境の中で、平素より国家を背景として、重要インフラの機能停止や機微情報の窃取等を目的としたサイバー攻撃が行われており、サイバー分野における安全保障の確保が切迫した課題となっている。この状況は、近年、一層深刻化し、攻撃の巧妙化・高度化が進むとともに、サイバー攻撃関連通信数も増加傾向にあり、質・量両面でサイバー攻撃の脅威は増大している。くわえて、社会全体のデジタル化やサプライチェーンの複雑化が進展することで、あらゆる主体がサイバー攻撃のリスクに晒されるとともに、一主体に対する攻撃による被害の影響が社会全体にまで波及するおそれをはらんでおり、サイバー脅威は国民生活・経済活動を脅かすまさに災害のような存在となっている。

「国家安全保障戦略」（令和4年 12 月 16 日国家安全保障会議及び閣議決定）では、サイバー安全保障分野の対応能力を欧米主要国と同等以上に向上させることとし、具体的には、武力攻撃に至らないものの、国や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にこれを未然に排除し、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こととした。当該戦略では、そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備することとされ、既に欧米諸国で取組が進められている官民連携の強化、通信情報の利用、アクセス・無害化措置のための権限の付与を含む必要な措置の実現に向けて検討を進めることとされた。

当該戦略に基づき、これら新たな取組の実現のために必要となる法制度の整備等について検討を行うため、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開催され、官民連携の強化、通信情報の利用、アクセス・無害化措置等に関する新たな制度・枠組みの方向性について令和6年 11 月に提言が取りまとめられた。令和7年2月には、当該提言に基づく法律案が国会に提出され、国会における審議を経て、官民連携の強化及び通信情報の利用に係る制度の導入を内容とする本法及びアクセス・無害化措置に係る制度の導入、組織・体制整備等を内容とする同法の施行に伴う関係法律の整備等に関する法律（令和7年法律第 43 号。第7章第3節において「整備法」という。）が成立し、同年5月 23 日に公布された。

法では、サイバー攻撃により国家・国民の安全が害され、又は国民生活・経済活動に多大な影響が及ぶことを防ぐため、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を目的として、政府が、一定の条件の下で通信情報を取得し、これを利用するための制度を導入するとともに、官民連携を強化するための様々な制度的な枠組みを創出し、これらの制度に基づき得られた通信情報や被害情報等を整理・分析し、作成した情報を行政機関、事業者等に提供する措置を規定している。今後、これらの背景・経緯を踏まえ、法の段階的な施行を経て、基本方針に基づき効果的かつ適正に制度の運用を図ることを通じ、関係機関・関係者が一体となってサイバー脅威に対する我が国のサイバー対処能力を強化する必要がある。

第2節　制度の基本的な考え方

法に基づく各般の施策を実施することにより、政府は、①サイバーセキュリティの対策に資する様々な情報の収集、②収集した情報とその他の手法により取得した情報の整理・分析、及び③整理・分析を踏まえて作成した情報の提供、の3つの機能を抜本的に強化して、重要電子計算機に対する不正な行為による被害の防止を図ることとしており、これにより我が国のサイバー対処能力を強化することとしている。

①情報の収集については、まず、法では、通信情報の利用に係る制度として、(ア)当事者協定、及び(イ)同意によらずに通信情報を利用する措置(外外通信目的送信措置等)を規定しており、一定の重大なサイバー攻撃(対象不正行為)に関係すると認められる通信情報を取得・利用することとしている。また、官民連携の強化に係る制度として、(ウ)特定重要電子計算機の届出義務、及び(エ)特定侵害事象等の報告義務を規定しており、特別社会基盤事業者からサイバーセキュリティの対策に必要となる報告等情報を取得することとしている。さらに、(オ)協議会の枠組みにおいては、被害防止情報を共有し、被害防止に必要となる情報を収集できることとしている。

②情報の整理・分析については、①の(ア)から(オ)までの制度に基づき収集した情報とその他の手法により取得した情報をデータベース化、照合するなどして整理・分析し、その結果について必要な範囲に必要な情報提供を行うことができるよう、総合整理分析情報、通信情報を含まない提供用総合整理分析情報、及び通信情報・秘密を含まない周知等用総合整理分析情報をそれぞれ作成することとしている。

③情報の提供については、②で作成した総合整理分析情報等のいずれかを、法の規定に基づき、重要電子計算機に対する特定不正行為による被害防止やアクセス・無害化措置の実施等に役立てるため、(ア)行政機関等、(イ)外国の政府等、(ウ)協

議会の構成員、(エ)特別社会基盤事業者、(オ)電子計算機を使用する者、又は(カ)電子計算機等供給者に対して適切に提供等することとしており、これにより関係機関等におけるサイバーセキュリティの対策を促すこととしている。

なお、法に基づく各般の施策については、全てのステークホルダーが当該施策によるサイバーセキュリティ対策の一翼を担うとともに、そのメリットを実感できるサイバー攻撃対応のエコシステムを、官民を横断して構築することを目指さなければならない。このため、「当該施策が適切に機能する」ことにより法目的が効果的かつ効率的に達成される必要があるのはもちろんのこと、各施策を実施する際には通信情報を始めとした保護が必要となる様々な情報を取り扱うことになることから、「当該施策に係る事務を適正に実施する」ことも併せて必要であり、法の運用に関わる行政機関は、これらを施策の駆動力の両輪として適切かつ適正な制度の運用を図ることとする。

第3節　政府内及び事業者等との連携と総合調整

(1) 政府内の連携と総合調整

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という法目的を効果的かつ効率的に実現するため、法に定められているとおり、法の運用に関わる行政機関等は内閣府に対して必要な協力を行うとともに、内閣府は法に基づき整理・分析した情報を必要な関係行政機関等に対して速やかに提供し、その対策を促進するなど、内閣府を始めとした関係行政機関等は、政府一体となって法に基づく事務又は関連する施策が実施されるよう相互に緊密に連携協力をすることとする。

また、内閣府を始めとした関係行政機関等によるこれらの事務又は施策は、司令塔組織である内閣官房国家サイバー統括室による総合調整の下で実施することとする。これによりサイバーセキュリティ戦略に基づく施策を始めとした政府全体における各般のサイバーセキュリティ関連施策と法に基づく事務又は関連する施策が有機的に連携し、これらが一体的かつ整合的に実施されることで、我が国のサイバーセキュリティの確保が図られるよう努めていく。内閣官房国家サイバー統括室がこの総合調整機能を適切に発揮するためには、同室において我が国のサイバー脅威に関する的確な状況認識を形成することが重要であることから、当該関係行政機関等は、法に基づく事務又は関連する施策の実施を通じて得られたかかる状況認識の形成に資するサイバーセキュリティ関連情報を、同室に対して積極的に提供することとする。その上で、同室は、サイバー脅威に関する状況認識に資する情報を関係行政機関等に対して積極的に共有することとする。

⑵ 事業者等との連携

昨今の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、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、官のみ・民のみでサイバーセキュリティを確保することは極めて困難である。このため、政府が率先して情報を提供し官民双方向での情報共有を促進するなど、官民連携を強化し、我が国全体のサイバーセキュリティの強化を図ることが必要である。また、情報の整理・分析や脆弱性への対応等に当たっては、同盟国・同志国等の関係機関・団体との連携に努めていく。

また、重要電子計算機に対する不正な行為による被害の防止を図るという法目的を実現するため、本法に基づく措置は、特別社会基盤事業者はもとより、電子計算機を使用する者に対する周知など中小企業も含めて広く様々な事業者が対象となり得ることから、本法に基づく措置について必要な周知・広報を行う。

第4節　通信の秘密の尊重

本法の適用に当たっては、法目的を達成するために必要な最小限度において、法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、いやしくも日本国憲法（以下「憲法」という。）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。特に、憲法第21条第2項にその保障が規定されている通信の秘密は、いわゆる自由権的、自然権的権利に属するものであり、最大限に尊重されなければならないものであることから、関連業務に携わる通信情報保有機関[4]における全ての関係職員は、通信情報を取り扱うに当たってはこの点について十分な認識を持ち、通信の秘密を尊重しつつ厳格にその業務に取り組むことを徹底する。

第5節　基本的な事項に関わる概念・定義の考え方

⑴ 重要電子計算機の定義の考え方

本法は、行政機関や特定社会基盤事業者等が使用する電子計算機であって、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ような一定のものを重要電子計算機と定め、法に定める各般の施策等を通じて、重要電子計算機に対する不正な行為による被害

[4] 内閣府及び法第27条第3項、第31条第1・2項又は第38条第1・2項の規定により選別後通信情報（注釈7参照。法第36条の規定により選別後通信情報とみなされるものを含む。）の提供を受けた行政機関であって、現に当該選別後通信情報を保有しているもの（サイバー通信情報監理委員会を除く。）。

の防止を図ることとしている。法第2条第2項は、重要電子計算機の範囲を政令で定めることとしているが、その制定に当たっては、次の点を考慮することとする。

法第2条第2項第1号に該当する重要電子計算機については、国の行政機関、地方公共団体、独立行政法人、地方独立行政法人及び特殊法人等が使用する電子計算機に関し、管理される重要情報との関わり方又は重要な情報システムとの関係に着目して、そのサイバーセキュリティが害された場合に、重要情報の管理又は重要な情報システムの運用に関する事務の実施に重大な支障を生ずるおそれがある電子計算機の範囲を明確化する。また、同号ホに規定する法人については、同号イからニまでに規定する国の行政機関等に比肩する公共性を有する業務を行う組織の範囲を具体的に明確化する。

同項第2号に該当する特定重要電子計算機については、特定重要設備との関係に着目して、特定社会基盤事業者が使用する電子計算機のうち、そのサイバーセキュリティが害された場合に、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の範囲を明確化する。具体的には、特定重要設備に限らず、特定重要設備と接続され、一定の情報のやり取りが可能な情報システム(クラウドサービスを含む。)等が該当する。特定重要電子計算機の詳細は業態ごとのシステム特性が異なることから、事業者や専門家との協議を経て、法第2条第3項に規定する特別社会基盤事業者の業態別に明確化する。

同項第3号に該当する重要電子計算機については、重要情報を保有する装備品製造等事業者[5]など特別防衛秘密、特定秘密、装備品等秘密又は重要経済安保情報[6]である情報を取り扱う事業者が使用する電子計算機に関し、管理される重要情報との関わり方に着目して、そのサイバーセキュリティが害された場合において、重要情報の管理に関する業務の実施に重大な支障を生ずるおそれがある電子計算機の範囲を明確化する。

その上で、特に特定重要電子計算機については、これまでの国内外でのサイバー攻撃の事例や多層防御の観点から、特別社会基盤事業者の安定的な役務提供を確保するために特に保護が必要な機器を対象とする必要があり、セキュリティ対策に係る

[5] 重要情報を保有する防衛省が調達する装備品等の開発及び生産のための基盤の強化に関する法律(令和5年法律第 54 号)第2条第3項に規定する装備品製造等事業者をいう。
[6] 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)第3条第1項に規定する重要経済安保情報をいい、重要経済基盤(重要なインフラや物資のサプライチェーン)に関する一定の情報であって、公になっていないもののうち、その漏えいが我が国の安全保障に支障を与えるおそれがあるため、特に秘匿する必要があるものを指す。

国際標準等も踏まえてその類型化を行う。

⑵ 機械的情報の考え方

法第2条第8項に規定する機械的情報については、法による通信情報の利用に係る制度においてその分析の対象とする情報の項目を示すものであり、IP アドレスなど通信履歴に係る情報（同項第1号）、指令情報（同項第2号）及び同項第3号に規定する内閣府令で定める通信の当事者の意思の本質的な内容を理解することができないと認められる情報がこれに該当する。

内閣府は、内閣府令に定める機械的情報に含まれる情報の項目の範囲について、攻撃通信の特徴、攻撃者が用いるサーバの状況等を解明するための分析に必要となる情報がその範囲に適切に含まれるよう検討するとともに、これが意思疎通の本質的な内容を理解することができないと認められる情報に厳に限定されるよう情報の項目を精査し、パブリックコメントやサイバー通信情報監理委員会との協議等の適切な手続を経た上で、適切な範囲の機械的情報を規定することとする。

第2章　当事者協定の締結に関する基本的な事項

第1節　基本的な考え方

法第 13 条に規定する当事者協定は、内閣府が、特別社会基盤事業者その他の事業電気通信役務の利用者（協定当事者）との間で協定（当事者協定）を締結し、当事者協定による同意の下で協定当事者から取得した通信情報を利用するための制度である。当該制度は、当事者協定により取得した通信情報を、①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、及び②協定当事者が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で利用することで、①’重要電子計算機を使用する我が国の行政機関や特別社会基盤事業者等の全体、及び②’協定当事者の双方におけるサイバーセキュリティの確保に資するものである。

特別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をより確実なものとするためには、官民相互の協力が重要となるところ、当事者協定の制度はこの協力の推進に資する枠組みとなっている。このため、当該制度が有効に活用されるよう、内閣府は特別社会基盤事業者等との間で着実に当事者協定の締結を進めていくこととする。一方で、当事者協定の締結は、あくまでもこれを締結しようとする者の判断に基づく任意のものであるため、当該者が、当事者協定を締結する意義や必要性、当事者協定の内容、これを締結することにより発生する対応・負担等の事項について適切に理解した上で、内閣府との間で当事者協定が締結されるよう、できる限り丁寧にその締結に向けた協議を行うこととする。

第2節　当事者協定の締結を推進させるための基本的な事項

⑴　当事者協定の締結の推進に当たっての考え方

当事者協定の締結を進めるに当たっては、内閣府は、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という観点から、例えば、重大なサイバー攻撃が行われている状況や攻撃を受けた場合の被害の範囲及び影響の深刻度合いの想定等を踏まえて優先度を考慮し、当事者協定を締結する重要性の高い特別社会基盤事業者等から当該締結に向けた協議を求めていくこととする。この協議を通じて当事者協定が締結された場合には、内閣府は、当事者協定に基づき通信情報を利用することで、当該特別社会基盤事業者等が使用する重要電子計算機等に対する国外からの不審な通信を検出し、その被害を防止するための対策を促すことができ得ることとなり、本制度の効果的かつ効率的な運用が図られることとなる。

⑵ 当事者協定の締結についての推進方策

内閣府は、当事者協定の締結を推進するため、協定当事者におけるサイバーセキュリティの確保を図るために有効な個別分析情報又は利用者個別分析情報を作成し、提供することに加えて、例えば、協定当事者に対して、サイバー攻撃が疑われる不審な通信を検出した場合にその通知を行うとともに、関連する分析や背景情報等、これへの対策に係る付随的な情報を提供するなど、当事者協定の締結によるメリットが増進されるよう努める。くわえて、そのメリットが特別社会基盤事業者等に広く認知・理解されるよう周知・啓発等に努めることとする。

さらに、本制度に基づく協定当事者による通信情報の提供は、我が国におけるサイバーセキュリティの向上に貢献するものであることから、この点が国民にも広く理解され、ましてや協定当事者が当事者協定を締結したことにより非難を受けることがないよう、本制度の意義等についての広報活動を行うよう努めることとする。また、特別社会基盤事業者等が当事者協定に基づく通信情報の提供について何らかの懸念を有している場合には、当事者協定の締結を躊躇することも考えられるため、かかる懸念が払拭されるよう、内閣府は、当事者協定に基づき提供した通信情報が法の規律により保護されること等について丁寧な説明を行うとともに、協定当事者が通信情報の提供に関して不当に責任を負うことがないように配慮する。

また、当事者協定の内容に関する協定当事者による予見性を高めることは、当事者協定の締結に向けた協議の円滑な実施に資することから、内閣府において、当事者協定の標準的な項目及びその内容を示したひな型を事前に作成し、協議に際して当事者協定を締結しようとする者がこれを参照できるようにしておくことを検討する。なお、当該ひな型については、当事者協定の標準的な内容等を示したものであることから、実際には、協議において当事者協定を締結しようとする者の意見、運用の想定等を踏まえてその内容を発展させ、最終的な当事者協定を締結することとする。

第3節　当事者協定の締結に関する配慮事項

⑴ 当事者協定の締結に向けた協議に関する配慮事項

当事者協定の締結については、これを締結しようとする者の判断に基づく任意のものであるため、当事者協定の締結に向けた協議においては、内閣府は、政府が当事者協定により取得した通信情報を利用する目的（第1節①及び②）、当事者協定の意義（第1節①’及び②’）やこれを締結するメリット、当事者協定に基づき協定当事者が

対応することとなる事項や想定される負担等の事項を明確に説明することとする。くわえて、協定当事者が提供することとなる通信情報の範囲や内閣府からの個別分析情報の提供の要領等の当事者協定に含める内容についての意向を丁寧に聴取するなど、当該者の判断に資するようできる限り丁寧に協議を行うよう努めることとする。

また、本制度は、当事者協定の締結により協定当事者から同意を得ていることを前提として、その同意の範囲内で通信情報を利用するものであることから、有効な同意に基づかない当事者協定による通信情報の利用は、本制度の趣旨からしても、また、通信の秘密との関係においても許容されるものではない。このため、内閣府は、当事者協定の締結が事実上の強制とならないよう十分に配慮するとともに、間接的な強制を回避するためにも協議の結果として当事者協定を締結しなかった者に対して不当に不利益な取扱いをしないこととする。

⑵ 当事者協定に基づく他目的利用に関する配慮事項

法に基づく分析の対象となる選別後通信情報[7]については、法第 23 条第2項又は第3項の規定により、原則的に、特定被害防止目的[8]以外の目的のための利用又は提供（以下「他目的利用」という。）を禁止しているが、その例外として、当事者協定により取得した通信情報を自動選別することにより得られた選別後通信情報については、同条第4項第1号の規定により、協定当事者の同意を得ている場合には他目的利用をすることができるとしている。この場合における他目的利用の例外については、当事者協定の制度の趣旨に即して、協定当事者から追加の同意を得て、その同意の範囲内で一定程度柔軟な選別後通信情報の利用を行うことができるようにしたものであり、通信の秘密への配慮と我が国におけるサイバーセキュリティの確保の両方の観点を踏まえて規定した措置となっている。

一方で、他目的利用をする場合には、内閣府は、①その利用又は提供する範囲を含めて他目的利用の条件について個別に慎重な検討をした上で、協定当事者から具体的かつ明確な同意を得ることとする。その上で、内閣府を始めとした通信情報保有機関は、②当該同意の範囲内で利用又は提供すること、及び③法第1条に規定する法目的の範囲内で利用又は提供することを徹底し、これにより他目的利用が重要電子計算機の被害の防止につながり得るサイバーセキュリティの対策のためにのみ行わ

---

[7] 自動選別により得られた取得通信情報（当該取得通信情報を複製し、又は加工して作成された情報（提供用選別後情報となったものを除く。）を含む。）

[8] 重要電子計算機に対する国外通信特定不正行為（対象不正行為であって当該国外通信特定不正行為に該当しないものを含む。）による被害を防止する目的。

れることを確保することとする。

特に、①の具体的かつ明確な同意を得るという点については、内閣府は、同意の中で、(ア)他目的利用される選別後通信情報の範囲、(イ)他目的利用をする主体、(ウ)他目的利用の具体的な目的といった事項を明確にした上で、協定当事者から同意を得ることとする。また、実効的な観点から明確に同意を得ることも重要であり、例えば、他目的利用に関して(ア)～(ウ)の事項を含む同意の範囲が明示された書面を取り交わすなどの厳密な方法を採ることとする。

また、②の同意の範囲内での利用について、通信情報保有機関は、他目的利用として選別後通信情報を関係機関に対して提供する場合に、当該関係機関においても同意の範囲内で選別後通信情報が利用されることが同様に確保されるよう、例えば、通信情報保有機関は当該関係機関との間で事前に書面を取り交わし、当該書面の中で、選別後通信情報を利用することのできる目的や範囲等の事項を明確にするとともに、その提供後に当該関係機関において同意の範囲内での適正な利用がされているかの状況を確認できることを担保する等の手続を採ることとする。

なお、③の法目的には、犯罪捜査目的は含まれないことから、通信情報保有機関は、本法に基づく他目的利用には犯罪捜査のための選別後通信情報の利用は含まれ得ないことにも留意する[9]。

[9] 他の法律に基づき選別後通信情報の提供を求められた場合の対応については、第3章第3節⑸を参照。

第3章　通信情報保有機関における通信情報の取扱いに関する基本的な事項

第1節　基本的な考え方

巧妙化・高度化したサイバー攻撃においては、攻撃者はその攻撃元を隠蔽するため、一般利用者の通信機器を乗っ取った多数のボットやC2サーバ[10]を多段階に組み合わせ、これにより構成した攻撃用のインフラを通じて攻撃を行うという手法を用いることが確認されている。このような複雑、かつ、これを構成するボット等の多くが国外に所在すると考えられるような攻撃用のインフラの実態を把握するためには、これまでの情報収集・分析の手段では限界があり、サイバー攻撃関連通信情報を分析してその対処を図ることが必要不可欠である。このように、巧妙化・高度化するサイバー攻撃に対処するため、本法において通信情報を利用するための制度が導入されたものである。

本制度の運用に当たっては、内閣府及び関係行政機関は、通信情報の利用に係るシステム・設備の的確な整備や人材の確保・育成を通じて能力構築を図るとともに、過度な負担にならない範囲で電気通信事業者からも適切な協力を得ることにより、本制度を効果的かつ効率的に機能させ、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の防止を図ることとする。

一方で、当事者協定、又は通信の当事者の同意によらずに通信情報を取得し、利用するための措置[11]により取得した通信情報については、憲法第 21 条第2項が保障する通信の秘密等に十分に配慮してこれを取り扱う必要がある。このため、法では、通信情報の利用に伴う通信の秘密に対する制約が、公共の福祉との関係でやむを得ない限度に留まるよう、取得した通信情報に対する自動選別の実施などの様々な規律を課しているところであり、内閣府を始めとする通信情報保有機関は、当該規律を厳格に遵守して適正に通信情報を取り扱うこととする。

あわせて、法では、独立性を有する機関であるサイバー通信情報監理委員会が、通信情報保有機関に対して法の規定に基づく検査等を行うことにより、通信情報保有機関における法の規律の遵守を確保することとしていることから、同委員会が適切にその機能を果たすことができるよう同委員会の体制構築や事務運営を図ることとする。

---

[10] C2（Command and Control）サーバとは、クラウド・ホスティングサービス上等で、マルウェアに感染させるなどして乗っ取った通信機器（ボット）を操作し、情報の収集や攻撃等の指令を出すサーバのこと。

[11] 法第 17 条第1項に規定する外外通信目的送信措置、法第 32 条に規定する特定外内通信目的送信措置及び法第 33 条に規定する特定内外通信目的送信措置を指す。

第2節　通信情報の利用を適切に機能させるための基本的な事項

⑴ 通信情報の利用に係る能力構築の考え方

通信情報の利用に係る制度の運用に当たっては、内閣府及び法第 27 条第1項の関係行政機関は、情報保全にも配慮しつつ、通信情報の利用に係る分析能力の構築に努めることとする。具体的には、巧妙化・高度化するサイバー攻撃にも有効に対処できるよう、関係行政機関は、通信情報の自動選別や整理・分析等を効果的に行うために必要な機能を具備したシステム・設備の的確な整備を進めることとする。また、情報の整理・分析その他の本制度の運用に係る事務に従事する職員についても、サイバー安全保障、情報通信技術、法律などの専門的知識及び経験を有する多様な人材を確保するとともに、組織的かつ計画的にその育成を図ることとする。

さらに、サイバー攻撃に用いられる技術や手法は不断に巧妙化・高度化を遂げていくことが予測されることから、これに応じて本制度の施行後も継続的にシステム・設備及び人材に係る能力強化を推進し、内閣府及び関係行政機関における通信情報の利用に係る能力構築を不断に図ることとする。特に、技術の進展に合わせて、サイバー攻撃への有効な対策、事務の効率化等に資する AI 等の新たな技術の活用を積極的に図ることとする。

また、本制度を運用する主たる行政機関である内閣府がその機能を適切に発揮するためには、通信情報の取得については電気通信事業者から、自動選別の実施や通信情報の分析等については関係行政機関からそれぞれ必要な協力を得ることが不可欠であることから、官民の関係機関との間で適切な協力関係を構築することとする。くわえて、これらの協力を得て内閣府が通信情報を含めた各種のサイバーセキュリティ関連情報を分析した結果については、法の規定に基づき必要な行政機関等に対して適切な内容・形式の情報を適切なタイミングで提供するなど関係機関との相互の連携を緊密に図ることとする。

⑵ 電気通信事業者の協力

通信の当事者の同意によらずに通信情報を取得し、利用する措置の実施に当たっては、内閣府が設置する受信用設備に通信情報を送信する電気通信事業者の協力が必須である。このため、法第 20 条では、内閣総理大臣は、法第 17 条第1項に規定

する外外通信目的送信措置[12]の実施に関し、国外関係電気通信設備[13]を設置する電気通信事業者に対して、当該国外関係電気通信設備に関する情報の提供、当該実施のための機器の接続その他の必要な協力を求めることができると規定しており、また、当該協力の求めを受けた電気通信事業者は、正当な理由がない限り、これを拒んではならないと規定している。

電気通信事業者によるこの協力は、法に基づく義務として規定されているものであり、かつ、通信情報の利用により行政機関、特別社会基盤事業者等が果たしている重要な機能がサイバー攻撃により損なわれることを防ぐという、政府の責任において実施する公益性の高い措置への協力であることから、当該協力を行う電気通信事業者は国家及び国民の安全に貢献しているとして肯定的に評価されるべきであり、決して社会的に非難されるようなことがあってはならない。

なお、法第 20 条に規定する「正当な理由」に該当する場合としては、例えば、内閣府が求める協力が、電気通信事業者が保有する設備又は技術によって対応することができる能力の範囲を超えた協力内容となっている場合や、協力をすることにより電気通信事業者による利用者に対する役務の提供に少なからず支障を与えることが予測される場合等が想定され、このような場合には、電気通信事業者は内閣府からの協力を拒むことができる。

また、このような正当な理由に該当しない場合であっても、内閣府は、電気通信事業者が行う協力に関する負担が過度なものとならないように配慮するとともに、協力の具体的な内容や諸条件について事前に丁寧に説明を行うものとする。さらに、内閣府は、その協力により電気通信事業者が直面し得る通信ネットワーク運営等に対する負担についても回避策を十分に検討することとする。くわえて、内閣府は、通信ユーザの利便性低下やコスト負担が生じるようなことも避けられるよう配慮することとする。

第3節　通信情報の適正な取扱いに関する配慮事項

⑴ 通信の秘密等への十分な配慮

[12] 法第 20 条の規定を法第 32 条第2項又は第 33 条第2項の規定において準用することにより、特定外内通信目的送信措置又は特定内外通信目的送信措置の実施に関しても同様に、電気通信事業者に対して必要な協力を求めることができる。

[13] 電気通信事業者の電気通信事業の用に供する電気通信設備であって、他の電気通信設備との接続の状況その他の事項により、当該電気通信設備を用いて提供される事業電気通信役務が国外関係通信を媒介していると認められるもの。

法に基づく通信情報の利用は通信の秘密の制約を伴うものであるが、法第4章から第7章までに規定する通信情報の取得及び取扱いに係る各種の手続や条件、制限等の規律が適切に遵守されることにより、その制約を公共の福祉の観点から必要やむを得ない限度に留めることとしている。

すなわち、法では、①法第 17 条、第 23 条第2項等に規定しているように、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といった高い公益性の実現のために通信情報を取得し、及び利用することとしている。また、②法第 22 条第1項に規定しているように、取得した通信情報は、何人も閲覧等ができない自動的な方法による自動選別によって重要電子計算機に対する国外通信特定不正行為[14]に関係があると認めるに足りる機械的情報を選別した上で、選別したもののみを分析の対象とするなど、厳格な手続や条件を定めている[15]。くわえて、③通信情報保有機関における当該規律の遵守については、法第 10 章に基づきサイバー通信情報監理委員会が審査及び検査を行い、監理されることとしている。これら①～③により、通信情報の利用による通信の秘密の制約が公共の福祉の観点から必要やむを得ない限度に留まることが確保される制度となっている。

本制度の下で、通信の秘密や通信の当事者のプライバシーに十分に配慮して通信情報を利用するため、関連業務に携わる通信情報保有機関における全ての関係職員は、法に規定する規律の趣旨及び内容を十分に理解し、かかる認識の下で当該規律を厳格に遵守し、適正に業務を行うことを徹底する。

具体的には、例えば、自動選別により分析の対象を一定の機械的情報に限定し、当該機械的情報を除き、自動選別の対象となった通信情報の全てを確実に消去することや、法に規定する場合を除き選別後通信情報の提供や特定被害防止目的以外の目的のための利用を行わないこと、分析の対象となる機械的情報に対して他の情報と照合しない限り特定の個人を識別できないようにする非識別化措置を講ずること等の法の規律を厳格に遵守し、適正に業務を行うこととする。

あわせて、法に基づく通信情報の利用に係る制度について、本制度の意義に加えて、本制度においては法の規律により通信の秘密を始めとする国民の権利利益の保

---

[14] 法第 21 条に規定する対象不正行為であって、重要電子計算機に対する国外通信特定不正行為に該当しないものを含む。

[15] 自動選別のほか、法では、通信情報の利用及び提供の制限（法第 23 条）、非識別化措置等（法第 24 条）、選別後通信情報の保存期間等（法第 25 条）、安全管理措置等（法第 26 条）、サイバー通信情報監理委員会への通知（法第 30 条）、通信情報保有機関における選別後通信情報の取扱い（法第 31 条）等の手続、条件、制限等を規定している。

護に係る様々な措置が講じられることについて、内閣府は、積極的に広報活動を行い、この点が国民にも広く理解され、本制度について信頼が得られるよう周知・啓発に努めることとする。くわえて、通信情報の利用について国民から決して懸念を抱かれることがないよう、通信情報保有機関は、サイバー通信情報監理委員会による審査及び検査に対して誠実に応じることを含めて制度の運用について可能な限り透明性を高める。

⑵ 通信情報の安全管理措置

通信情報の安全管理については、仮にこれが不十分な場合には、通信の秘密に影響を及ぼし得るのみならず、通信情報の利用に係る制度そのものの信頼性まで失われかねないことから、特に万全を期す必要があるものである。このため、法第 26 条第1項の内閣府令で定める通信情報の安全管理措置については、通信情報保有機関においてこれが適切に遵守されることで通信情報が漏えい等するリスクを最小限に留めることが出来るよう考慮して、適切にその内容を規定するとともに、通信情報保有機関は規定された内容を遵守して適正に業務を実施することとする。

具体的には、内閣府は、選別後通信情報の取扱いの業務を行わせる職員の範囲の限定等の組織的な安全管理措置や、選別後通信情報へのアクセス権限の付与等の技術的な安全管理措置、取得通信情報を取り扱うことのできる区域の設定等の物理的な安全管理措置などの各種措置について検討し、パブリックコメントやサイバー通信情報監理委員会との協議等の適切な手続を経た上で、内閣府令にこれを規定することとする。

⑶ 提供用選別後情報の活用

法第 29 条に規定する提供用選別後情報については、それを協議会の構成員等に提供したとしても通信の当事者の通信に係る権利利益の保護に支障を生ずるおそれがないと判断できる水準にまで選別後通信情報を加工することにより、法第5章及び第7章に規定する選別後通信情報の取扱いに係る規律の適用を受けずに、柔軟に情報を利用及び提供することができるようにしたものである。提供用選別後情報は、通信の秘密を害することなく、サイバーセキュリティの対策のためにより広範な用途で、より広範な関係機関がこれを利用することができるものであるから、通信情報保有機関は、重要電子計算機の被害の防止のためにこれを有効に活用することとする。

提供用選別後情報の該当性を判断するための基準は、内閣府令で定めることとし

ているところ、内閣府は、選別後通信情報が個別の通信から十分に切り離され、これを提供したとしても通信の秘密等との関係で支障が生じ得ないと判断できる基準を検討し、パブリックコメントやサイバー通信情報監理委員会との協議等の適切な手続を経た上で、これを規定することとする。

⑷ サイバー通信情報監理委員会による監理

法では、法第 10 章により設置されるサイバー通信情報監理委員会（以下この項において「委員会」という。）が、同意によらずに通信情報を利用するための措置の実施に係る承認の求めに対する審査や、通信情報保有機関が法の規定を遵守して通信情報を取り扱っているかどうかについての検査等を行い、これらを通じて通信情報保有機関における通信情報の適正な取扱いを監理することで、重要電子計算機に対する不正な行為による被害の防止のための措置の適正な実施を確保することとしている。

このような委員会の機能が適切に発揮されるようにするためには、まずは十分な体制の事務局を構築することが必要であり、審査及び検査に必要となる法律、技術等に関する専門的な知識・経験を有する職員を確保するとともに、審査の迅速性[16]や検査の有効性等の観点も踏まえて必要な規模の体制を構築することとする。また、委員会の運営においては、委員会は法に規定する任務を達成するため、法の規定に基づき、諸外国の例も参考にしつつ、効果的かつ効率的にその職権を行使し、所掌事務を執り行うものとする。

通信情報保有機関においては、委員会による審査及び検査が法に基づく通信情報の適正な利用を確保するために重要な役割を果たすものであることを十分に認識し、当該認識の下で、平素から、委員会に対して、サイバーセキュリティ情勢やそれを踏まえた認識など関連する情報を前広に共有する等誠実かつ適切に協力をすることとする。

また、委員会による所掌事務の処理状況についての法第 61 条の規定に基づく国会への報告は、通信情報の利用に係る制度の透明性を高めて国民の信頼を得るために重要なものであるため、委員会は、同条の規定に基づき適切に報告を行うとともに、その内容の充実に努めることとする。

⑸ 他法令の遵守に関する配慮事項

[16] 法第 18 条において、「承認の求めがあった場合において、当該求めに理由があると認めるときは、遅滞なく、当該承認をするものとする」と規定されている。

通信情報の利用に関する事務の実施においては、通信情報保有機関は、個人情報の保護に関する法律（平成 15 年法律第 57 号。第7章第2節において「個人情報保護法」という。）を始めとする他法令を適切に遵守する必要があることに留意する。

また、内閣府を始めとした通信情報保有機関は、全ての通信情報保有機関において適切かつ一律に他法令の遵守が図られるよう努めることとし、必要な場合には、例えば、内閣府が特定の他法令を所管する省庁と協議の上、通信情報保有機関に対してその事務の実施に当たって当該他法令を遵守するための留意点等を適切な方法で示し、これを受けた通信情報保有機関がこれに従い他法令を適切かつ一律に遵守する等の措置を講ずることとする。

なお、他の法律に基づき選別後通信情報の提供を求められた場合には、当該提供は追加的な通信の秘密の制約となり得ることから、法第 23 条第2項又は第3項において選別後通信情報の特定被害防止目的以外の目的による利用又は提供を原則的に禁止していることに鑑み、法律に基づき提供しなければならない場合を除き、これを利用又は提供しない。

第4章　情報の整理及び分析に関する基本的な事項

第1節　基本的な考え方

内閣府は、法の規定に基づき収集した特定重要電子計算機の届出情報、特定侵害事象等の報告情報、選別後通信情報、提供用選別後情報、協議会を通じて得た情報等やその他の手法により収集した情報について、民間事業者による対策の促進や政府による必要な措置の実施など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有効に活用されるよう、法第 37 条の規定に基づき総合的かつ業種横断的に整理及び分析を行う。

情報の整理及び分析に用いられる報告等情報の収集に関し、法第4条の規定に基づく特定重要電子計算機の届出や法第5条の規定に基づく特定侵害事象等の報告については、特別社会基盤事業者の負担にもよく留意しつつ [17]、重要電子計算機の被害の防止のために必要かつ合理的な制度設計・運用を行うこととする。また、情報の作成に当たっては、必要な範囲に必要な情報提供を行うことができるよう、選別後通信情報を含まない情報の作成や秘密を含まない情報の作成も行うこととする。

また、情報の整理及び分析を通じて重要電子計算機の被害防止に効果的な情報の作成を行うため、内閣府は、法第 71 条の規定に基づき、必要性を確認しつつ関係機関等に情報の提供その他必要な協力を求めるとともに、法第 72 条の規定に基づき、その適切な事務実施を確保しつつ、情報の整理及び分析の事務の一部の委託を必要に応じて行う。

第2節　報告等情報の収集の考え方

⑴ 特定重要電子計算機の届出の考え方

特定重要電子計算機の届出情報に関しては、内閣府が横断的に管理し、例えば脆弱性情報や特定侵害事象等の報告情報との照合など、必要な整理・分析を行った上で、特別社会基盤事業者に対して、脆弱性情報等の被害の防止のために効果的な情報を提供することその他政府による必要な対応を実施するために活用する。こうした観点から、個別事業者向けの専用設計品等に関しては届出を不要とし、届出を求める内容については、届出対象となる特定重要電子計算機の機器の分類ごとに整理

[17] 特別社会基盤事業者の負担も踏まえた制度設計・運用とすることで、当該事業者から協力が求められる電子計算機等供給者等の負担の軽減にも資すると考えられる。

する。

また、特定重要電子計算機の届出を求めるに当たっては、特別社会基盤事業者の負担にも配慮する。例えば、機器更新等により特定重要電子計算機の届出情報に変更があった場合に特別社会基盤事業者に求める対応や、特別社会基盤事業者自らが直接管理していない特定重要電子計算機に係る届出については、その特別社会基盤事業者の対応に係る負担の大きさにもよく留意しつつ、実情に応じた合理的な制度設計・運用となるよう努めることとする。

さらに、本法においては、施行の際現に導入している特定重要電子計算機（以下この節において「既設特定重要電子計算機」という。）についても届出を行う必要がある。特に既設特定重要電子計算機の届出に当たって、その対象となる機器が膨大となり、届出に時間を要すると考えられるところ、特別社会基盤事業者からの特定重要電子計算機に係る届出が円滑に行われるよう、政府は、中小企業も含めた特別社会基盤事業者からの相談等への適切な対応に努める。なお、法附則第4条において、既設特定重要電子計算機について6月の経過措置を規定しているところ、施行後6月の間に新たに導入する特定重要電子計算機であって、既設特定重要電子計算機と一体として運用するものについては、既設特定重要電子計算機と同一時期に届出を行うことが適当であると考えられる。

⑵ 特定侵害事象等の報告の考え方

特別社会基盤事業者による特定侵害事象等の報告については、官民で有効な対処を行う観点からも、報告を行う事業者において判断に迷うことがないよう、サイバー攻撃に用いられる戦術等を体系化した既存のフレームワークも参考に、その報告を求める範囲が明確となるよう設定する。

その際、例えば特定重要設備や特定重要設備を含む領域など、そのサイバーセキュリティが害された場合に、特定重要設備の機能が停止し、又は低下するおそれが特に大きいものについては、不正な通信を検知した場合なども含め、報告を求める範囲を設定することとする。他方、例えばファイアウォール等のインターネットとの接続点となる機器については、平時から大量の攻撃性通信をブロックしており、そのような事象まで含めて一律に報告を求めると、特別社会基盤事業者に過度な負担を強いることとなる。そのため、例えば明確に侵入を検知した後の事象のみを対象とするなど、官民での有効な対処及び事業者の負担の観点から適切に報告範囲を設定する。その上で、万が一、特別社会基盤事業者において報告すべきかどうか判断に迷うことが生じ

た場合にも当該事業者が円滑に対応できるよう、政府は、中小企業も含めた特別社会基盤事業者からの相談等への適切な対応に努める。

また、特定重要電子計算機の機能がクラウドサービス上で実装されている場合の考え方については、クラウドサービスの利用形態ごとに整理する。

また、攻撃の高度化やシステム構成の変化により、サイバー攻撃の態様は変化していくことが想定され、また、Living Off The Land 攻撃[18]のように高度な潜伏能力を持つ攻撃については、一事業者では検知が困難であり、不審な通信等のきっかけとなる事象を基に分析を行う必要がある。このため、法第5条の規定に基づく特定侵害事象等の報告の範囲とは別に、政府として把握したい事象についての目安をより抽象的に設定し、サイバーセキュリティ戦略を踏まえた「重要インフラのサイバーセキュリティに係る行動計画」（令和7年（2025 年）6月 27 日サイバーセキュリティ戦略本部改定）や法第9条に規定する報告徴収、法第 45 条第1項に規定する協議会も活用しながら、柔軟な情報収集を行うこととする。

さらに、より網羅的に重要インフラ等への攻撃の試みを把握するため、特別社会基盤事業者のうち、特に重要な事業者については、事業者等の負担に十分配慮した上で、攻撃予兆情報について機械的に連携する手法についても検討を進める。

また、特定侵害事象等の報告内容については、不確実な内容も含めて報告時点で判明した事項を記載すれば速報として足りることとする等、タイミングに即して特別社会基盤事業者にとって過度な負担とならないよう設定する。また、特別社会基盤事業者自らが直接管理していない特定重要電子計算機に係る特定侵害事象等の報告については、その情報の取得可能性やその特定重要電子計算機に係る管理の実情にもよく留意しつつ、合理的な制度設計・運用となるよう努めることとする。

報告の期限について、諸外国での同様の報告手続を設けている国の例や、官民で有効な対処を行う観点も踏まえて期限を設定することとする。

また、サイバー攻撃の被害拡大の防止の観点からは、特定侵害事象等の報告が速やかに行われ、特別社会基盤事業者の負担をかけずに効率的に情報収集し、フィードバックを行うことが重要である。こうしたサイバー攻撃に係る被害組織の負担軽減と政府の対応迅速化を図る観点から、関係行政機関で緊密な連携を図りつつ、特定侵

[18] 対策側の検知等を回避するため、システム内に組み込まれている正規の管理ツール、コマンド、機能等を用いたシステム内寄生型の攻撃。

害事象等の報告と他の法令に基づく報告の様式の統一化に加えて、官民連携基盤による報告窓口の一元化について所要の調整を進める。

第3節　収集した情報の整理及び分析の考え方

⑴ 総合整理分析情報の作成の考え方

内閣府は、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に資する情報を作成し、これが行政機関や特別社会基盤事業者を始めとする重要電子計算機の使用者等に有効に活用されるよう、法の規定に基づき収集した各種の情報やその他の手法により収集した情報について、法第37条の規定に基づき総合的かつ業種横断的に整理及び分析を行い、総合整理分析情報を作成することとする。

具体的には、内閣府は、本法に基づき特定重要電子計算機の届出情報、特定侵害事象等の報告情報、選別後通信情報、提供用選別後情報、協議会を通じて得た情報等を収集するとともに、その他の手法により行政機関の端末における監視・分析データ等の行政機関が保有する情報、重要電子計算機の脆弱性情報、国内の関係機関や外国の政府等から提供を受けた情報、地政学的情勢等の攻撃の目的や背景に関する情報等を収集する。その上で、これら種々の情報のデータベース化等による整理や、各種の情報間の照合等の分析を行うことにより、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効果的な総合整理分析情報の作成に努めることとする。

また、作成する総合整理分析情報については、それが効果的に活用されるようにするため、情報が活用される用途・場面、情報を活用する者（情報の閲読者）等を適切に設定して総合整理分析情報を作成するよう努める。具体的には、例えば、サイバー攻撃の検知や予防策を講ずるために戦術的に活用される場合や、実際にサイバー攻撃や侵害を受けたときに迅速かつ効果的な運用上の対策を講ずるために活用される場合、行政機関や民間事業者等が所有する重要電子計算機を防護するための組織における戦略的な意思決定・判断に活用される場合等に応じて情報を作成することや、情報の閲読者等に応じて情報の内容やそこで用いる用語、及び情報の形式が適切なものとなるよう努めることとする。

その際、行政機関や協議会の構成員を始めとする民間事業者のニーズもよく踏まえつつ、政府だからこそ取得や、整理・分析が可能な情報を基とした情報の作成や、その情報の受け手におけ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に向けた具体的な行動につながるような情報の作成に努めることとする。

内閣府から総合整理分析情報の提供を受けた行政機関は、当該行政機関が自ら使用する重要電子計算機やその所管に係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を図るために当該総合整理分析情報を有効に活用するよう努めるものとし、例えば、当該総合整理分析情報について、内閣府とも必要な連携を取りながら、これを加工して必要な範囲の関係機関・関係者に対して必要な情報共有を図るなどの適切な措置を講ずるよう努めることが考えられる。

⑵ 提供用総合整理分析情報・周知等用総合整理分析情報の作成の考え方

総合整理分析情報にその取扱いに十分な配慮が必要となる選別後通信情報が含まれる場合には、その提供を行う場合や提供先の範囲は真に必要な範囲に限定されるべきものであることから、内閣府は、提供用総合整理分析情報として、総合整理分析情報を加工して選別後通信情報を含まない情報を作成する[19]。提供用総合整理分析情報には、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の秘密が含まれ得ることから、その取扱いに当たっては、法に規定する守秘義務・安全管理措置等が講じられていることが必要である。

また、提供用総合整理分析情報には秘密が含まれ得ることから、広くインフラ事業者や電子計算機の供給者等に対しても情報を提供できるようにするため、内閣府は、周知等用総合整理分析情報として、提供用総合整理分析情報を加工して秘密を含まない情報を作成する[20]。

第4節　関係機関等への協力の要請

より巧妙化・高度化するサイバー攻撃に対して、効果的に対処するためには、その攻撃や被害等の全容を把握すべく、政府や関係機関が一体となって情報を収集・集約することが必要である。このため、内閣府は、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に効果的な総合整理分析情報を作成するため、必要性を確認しつつ、関係機関等に情報の提供その他必要な協力を求めることとする。

例えば、関係行政機関に対してそれぞれの所管業種に関する情報を求めることや、独立行政法人情報処理推進機構（IPA）、国立研究開発法人情報通信研究機構

---

[19] 提供用総合整理分析情報の作成については、通信情報を含む総合整理分析情報から通信情報を含まないよう加工して作成する場合のほか、最初から通信情報を用いずに作成する場合もあり得る。

[20] 周知等用総合整理分析情報の作成については、秘密を含む提供用総合整理分析情報から秘密を含まないよう加工して作成する場合のほか、最初から秘密を含む情報を用いずに作成する場合もあり得る。

（NICT）、一般社団法人 JPCERT コーディネーションセンター等のサイバーセキュリティに関する高い専門性と情報収集能力を有する関係機関に対して、当該関係機関が検知・分析した脆弱性情報やネットワークの観測状況、その他当該機関の高い専門性に基づく情報等の情報提供を求めることが想定される。また、協議会の構成員に対して当該構成員が受けたサイバー攻撃に係る情報を求めることや、セキュリティベンダに対して重要電子計算機に対する特定不正行為による被害に係る分析結果等の情報提供を必要に応じて求めることも想定される。

第5節　事務の委託に関する考え方

法第 72 条第1項の規定により、特定重要電子計算機の届出情報、特定侵害事象等の報告情報、協議会を通じて得た情報等の整理及び分析の事務の一部（選別後通信情報を取り扱うものを除く。）を、独立行政法人情報処理推進機構その他の十分な技術的能力及び専門的な知識経験を有し、当該事務を確実に実施できると見込まれる者に委託することができることとされている。

具体的には、独立行政法人情報処理推進機構に対して、特定重要電子計算機の届出情報や特定侵害事象等の報告情報等の内容の整理・分析、重要電子計算機の脆弱性情報の整理・分析、特定重要電子計算機の届出情報と特定侵害事象等の報告情報や脆弱性情報との照合等の事務を、また、国立研究開発法人情報通信研究機構に対して、当該機構が有する分析能力や観測網等のリソースを活用した上記業務の高度化に係る事務を委託することが想定される。

なお、こうした法第 72 条第1項の規定による事務の委託を受けた者（受託者）の役員・職員又はこれらの職にあった者は、同条第4項の規定により、正当な理由がなく当該委託に係る事務に関して知り得た秘密の漏えい・盗用をしてはならないこととされている[21]。

[21] 本法においては、法第 72 条第4項の規定に違反して秘密を漏らし、又は盗用した者について罰則を設けている。また、受託者の役員・職員であって当該委託に係る事務に従事するものに対する刑法その他の罰則の適用については、同条第5項の規定に基づき、法令により公務に従事する職員とみなされる。

第5章　総合整理分析情報の提供に関する基本的な事項

第1節　基本的な考え方

内閣府又は関係行政機関は、各種情報の提供を受けた者において、必要な対策・措置の検討・実施など、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有効に活用されるよう、法第 38 条の規定により行政機関等に対して総合整理分析情報を、法第 28 条及び第 39 条の規定により外国の政府等に対して総合整理分析情報等を、法第 45 条の規定により協議会の構成員に対して提供用総合整理分析情報等を、法第 40 条の規定により特別社会基盤事業者に対して周知等用総合整理分析情報を、法第 41 条の規定により電子計算機を使用する者等に対して周知等用総合整理分析情報を、法第 42 条の規定により電子計算機等供給者等に対して脆弱性に関する周知等用総合整理分析情報等を、それぞれ適切なタイミングで提供する。

その際、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という法目的を効果的に実現するため、情報を提供する関係行政機関は、内閣官房国家サイバー統括室の総合調整の下でこれを実施し、その一体性・整合性を図る。また、政府は、情報提供を受けた者からのフィードバック等を踏まえて、情報提供の在り方についても不断に改善を図るとともに、政府に対して情報提供を行った事業者に対して、政府から積極的にフィードバック等を行い、情報共有がより活発となるよう取り組む。

同時に、政府は、法第 43 条の規定にのっとり、通信の当事者その他の者の権利利益の保護に配慮するとともに、選別後通信情報の取扱いについては法第 26 条第1項の規定に基づく安全管理措置を、また、要管理提供用総合整理分析情報の取扱いについては法第 44 条第1項の規定に基づく安全管理措置をそれぞれ講ずる。また、法第 26 条第2項及び第 44 条第2項の規定により管理が必要とされる情報を取り扱う職員等には守秘義務が課される。

また、法第 72 条の規定に基づき、その適切な事務実施を確保しつつ、電子計算機を使用する者に対する周知等の事務の一部と電子計算機等供給者に対する脆弱性情報の提供等の事務の一部の委託を必要に応じて行う。

第2節　総合整理分析情報等の提供先と提供する内容の考え方

⑴ 行政機関等に対する情報提供

内閣府は、行政機関等がサイバーセキュリティの対策や措置を講ずる必要がある場合において、当該行政機関等に対し、かかる対策や措置に必要となる総合整理分析情報を、法の規定に基づき速やかに提供することとする。具体的には、例えば、行政機関が使用する重要電子計算機に対する特定不正行為による被害が発生する可能性があることを把握した場合や、当該重要電子計算機に脆弱性が含まれていること等により被害が連鎖的に拡大する可能性があることを把握した場合、特定重要電子計算機に対する特定不正行為により特別社会基盤事業者における役務提供に支障を及ぼすおそれがあると認める場合、特定の選別後通信情報が警察又は防衛省・自衛隊が実施するアクセス・無害化措置に資すると認める場合等には、それぞれ該当する行政機関や所管省庁に対し、適切な総合整理分析情報を提供することとする。

また、内閣府から総合整理分析情報の提供を受けた総務省は、当該総合整理分析情報により、国内の電気通信設備が重要電子計算機に対する国外通信特定不正行為に利用されていることが判明した場合には、必要に応じ、法第 38 条第4項の規定を活用して、電気通信事業者に対して必要な情報を提供し当該国外通信特定不正行為へのおそれへの対処を求めることとする。

⑵ 外国の政府等に対する情報提供

法目的を効果的かつ効率的に達成するためには、例えば、我が国の重要電子計算機に対する攻撃に用いられている攻撃のインフラに関して幅広い観点からの把握を行うために外国の政府と連携して分析をする場合や、その攻撃のインフラが所在すると考えられる外国の政府に対応を依頼する場合など、外国の政府等に対して総合整理分析情報等を提供することが有効な場合も想定され得るところである。

このような場合においては、内閣府又は通信情報保有機関は、法第28条又は第39条の規定に基づき、①当該提供が法の規定による提供目的の制限に適合するかを個別かつ適切に判断するとともに、②提供する外国の政府等が法に規定する情報の取扱いに係る措置に相当する適切な措置を講じていることを明示的に確認した上で、その必要な範囲において総合整理分析情報等を提供することとする。なお、法に基づき適正に外国の政府等に対する情報提供がなされることにより、法目的が効果的かつ効率的に達成されるのみならず、外国の政府等との間でサイバーセキュリティ対策に係る関係構築及び国際協力が進展することで、我が国のサイバー対処能力の強化にもつながり得ることにも留意する。

⑶ 協議会の構成員に対する情報提供

協議会の構成員におけ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、内閣府は、協議会の構成員に対して、通信の秘密を侵害しないよう加工して作成された提供用総合整理分析情報等を提供する。例えば、サイバーセキュリティの実務を担う専門家が求める技術情報に限らず、経営層の判断に必要となる攻撃の目的や背景等に関する情報を、適切なタイミングで積極的に提供する。この攻撃の目的や背景等に関する情報の中には、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得ることが想定される。

こうした情報提供を積極的に行うことで、構成員の協議会への参画意欲を高め、協議会が官民連携のエコシステムとして効果的に機能するよう取り組んでいく。その際、協議会の構成員との継続的なコミュニケーションを通じてニーズ把握に取り組み、そのニーズも踏まえた形式・内容での情報提供に取り組んでいく。

⑷ 特別社会基盤事業者に対する情報提供

特別社会基盤事業者におけ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、内閣府から情報提供を受けた特別社会基盤事業者の所管省庁は、特別社会基盤事業者に対して、攻撃技術情報などの周知等用総合整理分析情報を積極的に提供する。その際、特別社会基盤事業者による特定重要電子計算機の届出情報も活用し、より効果的な情報提供となるよう努める。

また、特別社会基盤事業者のうち、守秘義務及び安全管理措置の課せられる協議会の構成員である事業者に対しては、特別社会基盤事業者による電子計算機の届出情報も活用しつつ、上述の経営層の判断に必要な攻撃の目的や背景等に関する情報や、政府が把握した公表前の脆弱性情報を迅速かつ適切に提供する。

なお、特別社会基盤事業者の所管省庁から、周知等用総合整理分析情報の提供を受けた特別社会基盤事業者は、同情報を活用して、特定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に必要な措置を講ずるよう努めなければならないとされており、例えば提供される脆弱性情報が、特別社会基盤事業者の役務提供上重大なものと認められる場合等には、内閣府と所管省庁における緊密な連携の下で、所管省庁において適切な措置の実施を求めることとする。

⑸ 電子計算機を使用する者に対する周知等

近年のサイバー攻撃においては、マルウェア感染等により一般利用者の通信機器

等も利用して攻撃が行われることも見られることから、内閣府は、重要電子計算機を使用する者に限らず、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、特定不正行為に用いられるおそれのある電子計算機を使用する者や、重要電子計算機の維持管理を任されている者、その他の者に対して、周知等用総合整理分析情報を、公表や協議会等を通じた情報提供等により周知する。

例えば、協議会の構成員に対して提供するような脅威情報に必要な加工を行った上で、協議会の構成員以外の者に対して情報提供を行うことで、広く国内のサイバーセキュリティの強化を促し、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つなげていく。

⑹ 電子計算機等供給者に対する情報提供等、脆弱性情報に係る情報提供

ア 電子計算機等供給者に対する情報提供等

重要電子計算機における脆弱性を悪用した特定不正行為による被害の防止のため、内閣府又は電子計算機等の供給を行う事業の所管省庁は、必要に応じて、公表前の脆弱性情報をその重要電子計算機の供給者に対して迅速に提供する。

サイバーセキュリティ基本法においては、電子計算機等供給者は、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ことが責務として規定されている。こうした規定も踏まえ、電子計算機等の供給を行う事業の所管省庁は、法に基づき、脆弱性が、特別社会基盤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場合には、必要に応じ、その電子計算機等供給者に対し、特定不正行為による被害を防止するために必要な措置を講ずるよう要請する。

また、内閣府又は特別社会基盤事業者の所管省庁は、法第 42 条第3項の規定に基づき、総合整理分析情報その他の情報により特定重要電子計算機等における脆弱性を認知した場合であって、当該脆弱性に起因する特定不正行為による被害の防止を図るために必要があると認めるときは、その電子計算機等供給者に対し上述の要請を行うよう、電子計算機等の供給を行う事業の所管省庁に対し意見を述べることとする。

イ 脆弱性情報に係る情報提供

脆弱性情報の提供に当たっては、情報の秘匿性や緊急性も踏まえ、情報提供を受

けた者がその対策を行うことができるよう、適切な情報提供・情報管理に努めていく。また、脆弱性情報の公表に際しては、利用者が膨大な脆弱性情報の中から優先的に対応すべきものを特定できるよう、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できるよう努める。

また、関係省庁・関係機関による脆弱性関連情報の取扱いについては、特に、国家を背景とした、より高度なサイバー攻撃への対処能力の強化のため、重要電子計算機に関して官民連携を強化し、政府が集約した情報を整理・分析し率先して民間事業者等に対し提供するという、本法による官民連携の強化に係る規定やその趣旨に基づき、政府が本法に基づく官民連携に係る事務を着実かつ効果的に実施できるよう、関係する告示・ガイドラインの必要な見直しを行う。その上で、政府は、脆弱性に関して、重要電子計算機の被害防止のため効果的な情報提供を積極的に行う。

第3節　情報提供に当たっての関係行政機関の連携

内閣府を始めとした関係行政機関からの法に基づく情報提供及び関連する情報提供は、内閣官房国家サイバー統括室の総合調整の下で実施することとし、その一体性・整合性を図ることを通じ、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という法目的を効果的に実現する。

例えば、法に基づく内閣府からの情報提供や関係行政機関等からの情報提供において、ワンボイスで機関ごとにその内容に差異が生じないよう、関係行政機関等の間で緊密に連携を図る。

第4節　情報提供に当たって必要な配慮

政府は、各種の情報を提供するに当たっては、その情報が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有効に活用されるよう、情報を整理・分析し、正確な内容を適切なタイミングで積極的に情報提供するよう努める。また、情報提供後も、情報提供を受けた者からのフィードバック等を踏まえて、情報提供の在り方についても不断に改善を図っていく。

また、当事者協定に基づき通信情報を提供した事業者に対して、その分析結果及びこれに関連する情報を政府から提供するほか、インシデントに係る情報等を提供した事業者に対して政府から積極的にフィードバック等を行い、官民の情報共有がより活発となるよう取り組む。

また、内閣府、総務省、特別社会基盤事業者の所管省庁及び電子計算機等の供給者の所管省庁は、総合整理分析情報、提供用総合整理分析情報又は周知等総合整理分析情報を提供するに当たっては、法第 43 条の規定にのっとり、通信の当事者その他の者の権利利益の保護に配慮しなければならない。例えば、事業者を特定できる状態で情報提供を行った場合には、当該事業者の権利や競争上の地位を害するおそれがあることから、政府に情報提供した事業者が不利益を被らないよう、情報提供した事業者以外に対して情報提供を行う際には、当該事業者の同意を得た範囲でのみ情報提供を行うこと等とし、事業者等の権利利益の保護に十分に配慮する。

第5節　安全管理措置

特別社会基盤事業者による特定重要電子計算機の届出情報、特定侵害事象等の報告情報、選別後通信情報、協議会を通じて得た情報、関係機関から提供を受けた情報等や、これらの情報を基に整理・分析した情報等には、公表前のインシデントに係る情報など、政府として一定の秘匿が求められる機密性の高い情報も含まれ、これら情報が漏えいした場合には悪用されるおそれや、本法に基づく政府の情報取得等に対する国民の信頼を損なうおそれがある。

このため、これら情報を取り扱う特別社会基盤事業者の所管省庁及び内閣府は、法第 44 条第1項に基づき、情報の安全管理のために必要かつ適切な措置として、例えば、情報取扱者の特定、研修等の組織的な安全管理措置や保管庫の施錠等の物理的な安全管理措置、電子ファイルのアクセス制御等の技術的な安全管理措置などを講ずる。なお、選別後通信情報の取扱いについては法第 26 条第1項の規定に基づき安全管理措置を講ずる（第3章第3節⑵参照）。

第6節　事務の委託に関する考え方

法第 72 条第1項の規定により、電子計算機を使用する者に対する周知等の事務の一部を、独立行政法人情報処理推進機構その他の十分な技術的能力及び専門的な知識経験を有し、当該事務を確実に実施できると見込まれる者に委託することができることとされている。具体的には、独立行政法人情報処理推進機構及び一般社団法人 JPCERT コーディネーションセンターに対して、インシデントに係る注意喚起等の周知等総合整理分析情報の提供・公表等の事務を委託することが想定される。

また、法第 72 条第２項の規定により、電子計算機等供給者に対する脆弱性情報の提供等の事務の一部を、独立行政法人情報処理推進機構その他の十分な技

術的能力及び専門的な知識経験を有し、当該事務を確実に実施できると見込まれる者に委託することができることとされている。具体的には、独立行政法人情報処理推進機構、一般社団法人 JPCERT コーディネーションセンター及び国立研究開発法人情報通信研究機構に対して、電子計算機等供給者への脆弱性情報の提供・調整、脆弱性への対応方法等の周知等の事務を委託することが想定される。

なお、こうした法第 72 条第1項及び第 2 項の規定による事務の委託を受けた者(受託者)の役員・職員又はこれらの職にあった者は、同条第4項の規定により、正当な理由がなく当該委託に係る事務に関して知り得た秘密の漏えい・盗用をしてはならないこととされている[22]。

[22] 本法においては、法第 72 条第4項の規定に違反して秘密を漏らし、又は盗用した者について罰則を設けている。また、受託者の役員・職員であって当該委託に係る事務に従事するものに対する刑法その他の罰則の適用については、同条第5項の規定に基づき、法令により公務に従事する職員とみなされる。

第6章　協議会の組織に関する基本的な事項

第1節　基本的な考え方

内閣府は、法第 45 条第1項の規定に基づき、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、協議会を組織する。

協議会では、法第 45 条第3項の規定に基づき、サイバーセキュリティの実務を担う専門家が求める技術情報や経営層の判断に必要となる攻撃の目的や背景等に関する情報等の被害防止に資する情報を政府から提供することや、脅威情報等の被害防止に資する情報を関係者間で共有し、協議を行うこと等に取り組む。また、協議会の運営に当たっては、その目的や協議会の構成員におけるニーズ等に応じて、グループ構成等を柔軟に選択し取り組んでいくことで、協議会の構成員による相互の情報提供・意見交換等を活性化させていく。

協議会の構成員は、法第 45 条第3項の規定により、政府から被害防止のための情報提供を受けることができる一方で、同条第5項の規定により、被害防止のために必要な情報に関する資料の提出の求めがあった場合における対応等が必要となることから、内閣府が必要と認めた構成員として協議会に参加するに当たっては、同条第2項の規定により、当事者から事前の同意を得ることとしている。また、協議会の構成員における相互の情報提供の活性化のためには適切な情報管理が前提となることから、協議会の構成員に対しては、同条第4項に基づき情報管理等を求める。

本法に基づく協議会の設置に伴い、改正前の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は廃止する。本法に基づく協議会は、従前のサイバーセキュリティ協議会における情報の官民共有の機能に加え、政府が収集し整理・分析した情報を政府から協議会の構成員に対して共有することが法に規定されるとともに、秘匿性の高い情報の共有のため、法第 45 条第4項の規定による安全管理措置の実施や同条第7項の規定による守秘義務の違反に対する罰則の引き上げが措置されている。

第2節　協議会の取組内容・運営方針

協議会では、政府から特定不正行為による被害を防止するための情報を提供することや被害の防止に資する情報を構成員間で共有し、協議を行うことのほか、政府から演習や初動対応支援等の機会を提供する。

協議会の運営に当たっては、共有する情報の内容や目的、参加者数等に応じてその運営の在り方を適切に設定することが重要である。例えば、会議形式としては、対面による参集型の会議やオンライン会議、情報共有システムの利用等を使い分けながら効果的かつ効率的に取り組むことが考えられる。また、グループ構成として、常設とするものやアドホックに設置されるもの、あるいは、特定社会基盤事業者の分野ごとのグループや分野横断的なグループ、特定事案に関係する者で構成されるグループを設けることも想定される。

こうした柔軟な運営方法を、その目的や協議会の構成員におけるニーズ等に応じて選択し取り組んでいくことで、協議会の構成員による自発的な相互の情報提供・意見交換等を活性化させていく。また、中長期的には、構成員のニーズも踏まえつつ官民が協働するプロジェクトの提供等の機能を具備していくことで、協議会を段階的に発展させるべく取り組む。

具体的な協議会の組織及び運営に関し必要な事項は、協議会が定める。

第3節　協議会で共有されるべき情報・協議する内容

協議会では、構成員におけ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、内閣府は、協議会の構成員に対して、サイバーセキュリティの実務を担う専門家が求める技術情報に限らず、経営層の判断に必要となる攻撃の目的や背景等に関する情報を、適切なタイミングで積極的に提供する。この攻撃の目的や背景等に関する情報の中には、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に関する情報などの秘匿性の高い情報も含まれ得ることが想定される。

こうした情報提供を積極的に行うことで、構成員の協議会への参画意欲を高め、協議会が官民連携のエコシステムとして効果的に機能するよう取り組んでいく。その際、協議会の構成員との継続的なコミュニケーションを通じてニーズ把握に取り組み、そのニーズも踏まえた形式・内容での情報提供に取り組んでいく。

また、協議会の構成員の間では、例えば、脅威情報の共有と分析、平時からの備えやインシデント対処に関する各事業者におけるベストプラクティスについて意見交換を行うこと等が想定される。

また、協議会では、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対策や、被害防止情報を適正に管理するために必要な措置、その他の被害の防

止のために必要な事項について、構成員で協議を行う。例えば、高度な潜伏性を備えた攻撃に対しても有効な検知方法の検討を行うことや、特定事案に関して被害組織との間で被害状況や対策等に関する協議を行うこと、平素からの対策に関して協議を行うこと等が想定される。

くわえて、協議会の構成員以外の者に対しても、秘密を含まない情報の提供を行うことで、広く国内のサイバーセキュリティ強化を促し、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つなげていく。その際、次節に記載の通り、例えば、構成員からの提供情報を基に政府が情報提供を行う場合には、当該構成員の同意を得た範囲でのみ情報提供を行うこと等とし、当該構成員等の権利利益の保護に十分に配慮する。

第4節　協議会の構成員

協議会の構成員は、政府から特定不正行為による被害の防止のための情報提供を受けることができる一方で、協議会で知り得た情報の適正な管理や被害の防止のために必要な情報に関する資料の提出の求めがあった場合における対応が必要となる。このため、内閣府は、協議会の設置趣旨に照らして構成員を検討することとし、内閣府が必要と認めた構成員として協議会に参加するに当たっては、こうした協議会の構成員となる利点や求められる対応等を説明した上で、当事者から事前の同意を得ることとしている。

具体的には、特定社会基盤事業者、システム・ソフトウェアの提供やセキュリティ対策を行うベンダ、機微技術を保有する事業者、特定社会基盤事業者と取引等がある事業者、特定社会基盤事業者には該当しないインフラ事業者、地方公共団体等に、必要に応じて参加していただくことを想定している。

その際、法第 45 条第5項の規定の下、特別社会基盤事業者による特定侵害事象等の報告義務に準ずる形で、機微技術を保有する事業者、特定社会基盤事業者と取引等がある事業者、特定社会基盤事業者には該当しないインフラ事業者といった協議会の構成員に対しても、政府に対する特定侵害事象等の報告を求めることも考えられる。

このように広く協議会の構成員に対して特定侵害事象等の報告を求める場合も含め、政府に情報提供した構成員が不利益を被らないよう、政府は、情報提供した構成員以外に対して情報提供を行う際には、当該構成員の同意を得た範囲でのみ情報提

供を行うこと等とし、情報提供した構成員等の権利利益の保護に十分に配慮して、その情報を取り扱うこととする。

第5節　安全管理措置

協議会の構成員における相互の情報提供を活性化させるためには、適切な情報管理が行われることが前提である。協議会の構成員に対する提供情報の中には秘匿性の高い情報も含まれ得ることから、協議会の構成員に対しては、協議会の事務従事者の特定、研修等の組織的な安全管理措置や保管庫の施錠等の物理的な安全管理措置、電子ファイルのアクセス制御等の技術的な安全管理措置など一定の情報管理を求める。

くわえて、例えば、重要経済安保情報についても、必要に応じて適切な情報管理の下で協議会の構成員が取り扱えるようにするために、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）に基づくセキュリティ・クリアランス制度を活用して、協議会の構成員への情報提供を行う。このため、当該制度の活用に向けた調整を進める。

第7章　その他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関し必要な事項

第1節　制度及び基本方針の見直しに関する事項

法附則第7条は、政府は、附則第1条第4号に掲げる規定の施行後3年を目途として、特別社会基盤事業者による特定侵害事象等の報告、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している。

政府は、国家及び国民の安全を害し、又は国民生活や経済活動に多大な影響を及ぼすおそれのある国等の重要な電子計算機のサイバーセキュリティを確保する重要性や、高度情報通信ネットワークの整備、情報通信技術の活用の進展、国際情勢の複雑化等を踏まえ、行政の効率性や特別社会基盤事業者等の負担等の観点にも留意しつつ、不断に取組状況の検証・評価を行うこととし、それに伴う制度の見直しを適時に行う。また、基本方針についても、上記の制度見直しや、国際情勢及び社会経済構造の変化等に応じて弾力的に見直しを行う。

第2節　官民連携に関する関係省庁・関係機関等との連携等に関する事項

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向けては、関係省庁や関係機関は、各機関が保有する情報の共有など、緊密な連絡・協力が不可欠である。特に、被害を受けた事業者の負担軽減や政府の対応迅速化、特定社会基盤事業者の安定的な役務提供の確保等の観点から、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）や個人情報保護法、その他関連する業法を所管する省庁とは、相互に連携しつつ合理的な制度設計・運用に努める。

内閣府、国の行政機関、独立行政法人情報処理推進機構、国立研究開発法人情報通信研究機構その他関係者は、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に関する事項について、相互に緊密に連絡し、及び協力しなければならないことを定める法第71条第2項の趣旨を踏まえ、法その他の法令、基本方針に基づき、相互に連絡・協力することとする。

また、法に基づく内閣府の事務については、内閣官房国家サイバー統括室の総合

調整の下で実施することとし、事務又は施策間の一体性・整合性を図ることを通じ、法目的を効果的に実現する。

第3節　アクセス・無害化措置との連携

国家安全保障戦略において「官民連携の強化」及び「通信情報の利用」と併せて能動的サイバー防御を実現するために必要な措置とされた「アクセス・無害化措置」については、本法と併せて整備法においてその制度が導入されている。能動的なサイバー防御が効果的かつ効率的に実現されるためには、法に基づく各般の施策とアクセス・無害化措置に係る施策が相互に有機的に連携し、これらが一体となって運用が行われることが必要である。

このため、サイバー安全保障担当大臣の下、司令塔組織である内閣官房国家サイバー統括室が総合調整機能を発揮し、関係行政機関は平素から必要な連携を図り、警察及び防衛省・自衛隊が個別のアクセス・無害化措置を執行する。この際、法に基づき収集及び整理・分析されたサイバーセキュリティ対策に係る情報がアクセス・無害化措置の実施のために適切に利用されるようにするため、内閣府を始めとした関係行政機関は、法第31条第1項及び第2項、第38条第2項等の規定に基づき、アクセス・無害化措置の実施に資すると認められる情報を、情報保全にも配慮しつつ、効果的かつ適正に内閣官房、警察、防衛省・自衛隊その他のアクセス・無害化措置の実施に関わる行政機関に提供することとする。