参考資料２

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
（骨子たたき台）

はじめに

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
- 第２節　政府内の連携と総合調整
- 第３節　事業者等との連携
- 第４節　通信の秘密の尊重
- 第５節　重要電子計算機の定義の考え方
- 第６節　機械的情報の考え方

第２章　第 13 条に規定する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
- 第２節　当事者協定の締結に関して配慮すべき事項

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
- 第２節　通信情報の取扱いに関して配慮すべき事項

第４章　第 37 条の規定による情報の整理及び分析に関する基本的な事項
- 第１節　報告等情報の収集の考え方
- 第２節　収集した情報の整理及び分析の考え方
- 第３節　関係機関等への協力の要請
- 第４節　事務の委託に関する考え方

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　総合整理分析情報等の提供先と提供する内容の考え方
- 第２節　情報提供に当たっての関係行政機関の連携
- 第３節　守秘義務・安全管理措置の具体的内容
- 第４節　情報提供に当たって必要な配慮
- 第５節　事務の委託に関する考え方

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、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おり、本文は基本方針の骨子を定めるものである。

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、法に基づく種々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明示するとともに、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方針を示すものである。

基本方針に基づき、内閣府は、関係行政機関とともに、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）の総合調整の下、本法に規定された関係施策を、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、基本方針の骨子において使用する用語は、本法において使用する用語の例による。

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

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。攻撃の高度化・巧妙化も進み、また、サイバー攻撃関連通信数や被害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。このような認識の下、「国家安全保障戦略」（令和４年 12 月 16 日閣議決定）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。

当該戦略を受けて制定された本法では、サイバー攻撃により国家・国民の安全が害され、又は国民生活等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、これを分析するための制度を創設するとともに、被害報告や通信情報等から得られた情報を整理・分析し、これを情報の種別に応じて行政機関、事業者等に提供する措置を規定している。具体的には、特別社会基盤事業者による特定重要電子計算機の届出及び特定侵害事象等の報告の義務化、政府による当事者協定、外外通信目的送信措置等に基づく通信情報の利用、政府により整理分析した情報等の周知、情報共有及び対策に関する協議会の設置等の措置を定めている。

第２節　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の目的を効果的に実現するため、法に定められているとおり、関係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速やかに提供するなど、相互に緊密に連携協力をする。

また、内閣府をはじめとした関係行政機関による法に基づく事務又は関連する施策については、内閣サイバー官（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　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、官のみ又は民間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、関係諸外国との連携に努めていく。

第4節　通信の秘密の尊重

本法の適用に当たっては、法第１条に規定する法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。特に通信の秘密は、最大限に尊重されなければならず、法に基づく通信情報の利用に当たっては、法に規定する規律等の趣旨及び内容について、関連業務に携わる全ての関係職員が十分な認識を持ちつつ、厳格に業務に取り組むことを徹底する。

第5節　重要電子計算機の定義の考え方

法第２条第２項第１号に規定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事

務又は業務を行う組織の範囲を具体的に明確化する。

同項第２号に規定する特定重要電子計算機には、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号に規定する重要電子計算機については、重要情報を保有する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。

第6節　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は、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情報が該当する。内閣府令に定める機械的情報の範囲については、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適切に含まれるよう検討するとともに、意思疎通の本質的な内容に当たら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。

第2章　第 13 条に規定する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

当事者協定を締結するかどうかは、あくまでも当事者協定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当たっては、サイバーセキュリティの確保をより確実なものにするために官民双方の協力が重要であるとの観点から、内閣府は、当事者協定による対策の必要性について理解を求めるとともに、当事者協定の内容や、発生する対応・負担等の事項を当事者が適切に理解した上で、当事者協定が締結されるようにする。

第2節　当事者協定の締結に関して配慮すべき事項

⑴ 当事者協定制度の運用に関する配慮事項

内閣府は、当事者協定の締結を進めるに当たっては、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観点から優先度を考慮し、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ての協議を求めていくこととする。

内閣府は、当事者協定の締結により協定当事者が受けることができるメリットが増進されるよう努めるとともに、そのメリットが認知・理解されるよう周知・啓発等に努めることとする。

また、内閣府は、当事者協定に基づき提供した通信情報が法に規定する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、協定を締結することにより協定当事者が不当に責任を負うことのないよう配慮する。

⑵ 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向けた協議においては、内閣府は、必要事項を明確に説明し、協議の相手方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。

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許容されるものではなく、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配慮

するとともに、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一切の不利益な取扱いをしないものとする。

当事者協定の内容に関する予見性を高めるため、内閣府において、当事者協定のひな型を事前に作成し、協議に際して提示できるようにしておくことを検討する。

⑶ 当事者協定に基づく他目的利用に関する配慮事項

法第 23 条第4項第1号の規定による特定被害防止目的以外の目的のための選別後通信情報の利用又は提供(他目的利用)については、法第1条に規定する法目的の範囲内で行う必要があり、選別後通信情報は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においてしか利用又は提供しない。

また、他目的利用については、協定当事者から個別に具体的かつ明確な同意を得て、その範囲内で利用する必要がある。他目的利用に関する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、実効的な観点から明確に同意を得ることも重要である。

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

法に基づく通信情報の利用に関する制度では、通信の秘密等に十分に配慮するために様々な制約を課しているところ、当事者協定や外外通信目的送信措置等により取得した通信情報の利用に当たっては、通信情報保有機関は、法による規定を適切に遵守して、適正に通信情報を取り扱う。

第2節　通信情報の取扱いに関して配慮すべき事項

⑴ 通信の秘密への十分な配慮

法に基づく通信情報の利用については、法第5章及び第7章における通信情報の取扱いに係る各種の手続や条件等の規律が適切に遵守されることにより、その利用が必要最小限となることが確保され、もって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保障されることとなる。したがって、通信情報の利用に関する業務に携わる全ての関係職員は、これらの法の規律を厳格に遵守して適正に業務を遂行することを徹底する。

⑵ 安全管理措置についての考え方

法第 26 条第 1 項に規定する通信情報の安全管理措置の具体的内容は、内閣府令で定めることとなっているが、厳格にその内容を規定する必要があり、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、パブリック・コメント等の適切な手続を経た上で規定する。

⑶ 通信情報の利用に係る機能強化の考え方

通信情報の利用に係る制度の運用に当たっては、高度化・巧妙化するサイバー攻撃にも有効に対処できるよう、情報の保全に留意しつつ、通信情報の自動選別や整理・分析等を行うためのシステム・設備の的確な整備やその分析能力の向上を図るほか、適切な人材確保・育成を図るなど、政府機関における機能強化を適切に推進する。

また、通信情報の利用について、制度運用を行う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電気通信事業者から、通信情報の分析等について関係行政機関から必要な協力を得るなど官民の関係機関との連携を緊密に図ることとする。

⑷ 電気通信事業者の協力に関する配慮事項

法第 20 条の規定による電気通信事業者の協力について、当該協力が、当該電気通信事業者が対応できる能力の範囲を超える場合や、その役務の提供に支障を与えることが予測される場合などは、同条に規定する当該協力を拒む「正当な理由」に該当し得るものである。

正当な理由に該当しない場合であっても、政府は、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。

⑸ 他法令の遵守に関する配慮事項

通信情報の利用に関する事務の実施においては、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）をはじ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。

一方で、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項においてそ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　第 37 条の規定による情報の整理及び分析に関する基本的な事項

第1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、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、脆弱性情報等を提供するために活用する。このため、政府が、その届出情報により、有効な脆弱性情報の提供が可能となるとは考えにくい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することが考えられる。

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。

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、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、その閾値が明確となるよう設定する。同時に、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ることから、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」や法第 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。

また、特定侵害事象等の報告内容については、報告時点で判明した事項を記載すれば初報として足りることとする等、タイミングに即し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にも配慮する。

第2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出の考え方

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出し、これが重要電子計算機の使用者等に有効に活用されるよう、本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出する。

具体的には、内閣府は、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、国の行政機関が保有する情報、外国の政府から提供を受けた情報、重要電子計算機の脆弱性情報等を収集するところ、これら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を通じて、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効果的な総合整理分析情報の作出に努める。

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出の考え方

総合整理分析情報にはその取扱いに十分な配慮が必要となる通信情報が含まれ、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出する。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提供するため、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出する。

第3節　関係機関等への協力の要請

より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出するため、必要に応じて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（NICT）等のサイバーセキュリティに関する高い専門性と情報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等の情報提供を求めることが想定される。

第4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、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委託することが想定される。

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　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

内閣府において、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、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、該当する行政機関に対し、それぞれの対策や措置に必要となる情報を、法の規定に基づき速やかに提供することとする。

また、総合整理分析情報により、国内の電気通信設備が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、総務大臣が電気通信事業者に必要な情報を提供し対処策を求めることとする。

⑵ 外国の政府等に対する情報提供

法目的を達成するためには、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、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適切な措置を講じていることを明示的に確認する。

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出された提供用総合整理分析情報を提供する。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。

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、協議会の構成員として守秘義務及び安全管理措置の課せられる特別社会基盤事業者に対しては、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活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提供する。

⑹ 電子計算機等供給者に対する情報提供、脆弱性情報に係る情報提供

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供給者の所管省庁は、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。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わかりやすく発信できるよう努める。また、本法による官民連携の強化に係る規定やその趣旨も踏まえ、関係省庁・関係機関による脆弱性関連情報の取扱いに関する制度の見直しを検討する。

なお、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。

第2節　情報提供に当たっての関係行政機関の連携

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、特に緊急性の高いものにつ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3節　守秘義務・安全管理措置の具体的内容

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や特定侵害事象等の報告情報は、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、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、職員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じる。

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、情報を整理し、正確な内容を適切なタイミングで情報提供するよう努める。また、情報提供後も、情報提供を受けた機関からのフィードバック等を踏まえて、情報提供のあり方

についても不断に改善を図っていく。

また、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、当該事業者に関する秘匿性の高い情報を削除して情報提供を行うこと等に取り組み、事業者等の権利利益の保護に十分に配慮する。また、情報提供した事業者に対しては、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。

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、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、周知等用総合整理分析情報の提供を行うべき者の整理やその提供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、脆弱性情報に関する電子計算機等供給者との調整・公表等の事務を委託することが想定される。

第6章　第 45 条第1項に規定する協議会の組織に関する基本的な事項

第1節　協議会の趣旨

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関係者間で共有・協議を行うこと等により、協議会の構成員における被害を防止することを目的として、協議会を設置する。

なお、これに伴い、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・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あ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率的・効果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を設けることも想定され、硬直的ではない運営とすることが考えられる。

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。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、日頃からの対応策など、各事業者におけるベストプラクティス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。

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、内閣府が必要と認めた構成員として協議会に参加いただくに当たっては、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。

第5節　守秘義務･安全管理措置の具体的内容

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、職員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及び守秘義務を設ける。

加えて、政府が保有する秘匿性の高い情報についても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・クリアランス制度の活用についても必要な検討をしていく。

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　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、高度通信情報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、国際情勢及び社会経済構造の変化等に応じて見直しを行う。

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、内閣官房の総合調整の下で実施する。