最終とりまとめ

令和６年１月 19 日

経済安全保障分野におけるセキュリティ・クリアランス

制度等に関する有識者会議

目次

１　はじめに

・　セキュリティ･クリアランス制度とは､国家における情報保全措置の一環として、政府が保有する安全保障上重要な情報として指定された情報（以下「ＣＩ」（Classified Information）という。）にアクセスする必要がある者（政府職員及び必要に応じ民間事業者等の従業者）に対して政府による調査を実施し、当該者の信頼性を確認した上でアクセスを認める制度である（ただし、実際にアクセスするには、当該情報を知る必要性（いわゆるNeed-to-Know）が認められることが前提となる。また、民間事業者等に政府から当該情報が共有される場合には、民間事業者等の保全体制（施設等）の確認（施設クリアランス）等も併せて実施される。）。

・　ＣＩを取り扱うに当たっては、特別の情報管理ルールを定め、漏洩した場合には厳罰を科すことが通例とされている。

・　我が国では、セキュリティ・クリアランス制度を規定している法律として、特定秘密の保護に関する法律（以下「特定秘密保護法」という。）がある。

・　このセキュリティ・クリアランス制度に関するこれまでの動きとして、まず、令和４年５月に成立した経済安全保障推進法の衆議院及び参議院各内閣委員会における附帯決議において、国際共同研究の円滑な推進も念頭に、我が国の技術的優位性を確保、維持するため、情報を取り扱う者の適性について、民間人も含め認証を行う制度の構築を検討した上で、法制上の措置を含めて、必要な措置を講ずるとの趣旨が明記された。

・　その後、政府は、令和４年12月に閣議決定された国家安全保障戦略において、主要国の情報保全の在り方や産業界等のニーズも踏まえ、セキュリティ・クリアランスを含む我が国の情報保全の強化に向け、政府としての検討を進めるとの方針を示した。

・　これらを受け、令和５年２月 14 日に開催された第４回経済安全保障推進会議において、総理から、経済安全保障分野におけるセキュリティ・クリアランス制度の法整備等に向け、制度のニーズや論点等を専門的な見地から検討する有識者会議を立ち上げ、今後１年程度をめどに、可能な限り速やかに検討作業を進めるよう指示があった。本有識者会議は、総理指示を受け、同年２月21日に設置されたものである。

・　本有識者会議では、２月の立ち上げから約４か月間で６回にわたって議論を重ねたが、その間、様々な企業からニーズや要望等を直接ヒアリングし、また、政府から情報保全に係る現行制度や運用等の説明も受けつつ、あり得べき制度の方向性について検討を重ね、６月６日に、中間論点整理をまとめた。

・　その後、同年10月11日から議論を再開し、中間論点整理で指摘された論点を中心に議論を続けてきた。本とりまとめは、これらの有識者会議の委員の検討の最終的な結果をとりまとめたものであり、政府に対し、本とりまとめが示した方向

性を踏まえ、法整備を含めた対応を促すものである。

２　セキュリティ・クリアランス制度に関する必要性

（１）セキュリティ・クリアランス制度に関する国としての必要性

・　安全保障の概念が、防衛や外交という伝統的な領域から経済・技術の分野に大きく拡大し、軍事技術・非軍事技術の境目も曖昧となっている中、国家安全保障のための情報に関する能力の強化は、一層重要になっており、経済安全保障分野においても、厳しい安全保障環境を踏まえた情報漏洩のリスクに万全を期すべく、セキュリティ・クリアランス制度を含む我が国の情報保全の更なる強化を図る必要がある。

・　我が国の既存の情報保全制度のうち、例えば、特定秘密保護法の施行により、我が国の情報保全制度の信頼性が高まり、同盟国・同志国との情報共有が一層円滑になった一方、主要国と異なり、同法では政府が特定秘密として指定できる情報の範囲が、防衛、外交、特定有害活動の防止、テロリズムの防止の４分野に関する一定の要件を満たす事項に限られており、経済安全保障に関する情報が必ずしも明示的に保全の対象となっていない。こうした特定秘密保護法等に基づく情報保全制度の下で、指定された情報にアクセスできる民間事業者等はいわゆる防衛産業に集中している。このため、経済安全保障上重要な情報に関して、特に、経済関係省庁や防衛産業を超えた民間において、セキュリティ・クリアランス制度を含む情報保全の一層の強化が必要となっている。なお、クリアランス保有者は、米国では民間も含め 400 万人以上、その他の主要国でも数十万人以上いるとされ、官民のクリアランス保有者の比率についても、米国では官対民で７割対３割程度となっているなど、制度として定着している（令和４年末時点で、我が国で特定秘密の取扱いの業務を行うことができる者の数は約 13 万人、保有者の比率は、官が 97％、民が３％）*。

*各国政府資料を基に事務局にて調べた情報（2023 年５月時点で判明しているもの）。日本については、特定秘密の指定及びその解除並びに適性評価の実施の状況に関する報告（令和５年６月版）。

・　こうした形での情報保全の強化は、安全保障の経済・技術分野への広がりを踏まえれば、同盟国・同志国との間で更に必要となるこれらの分野も含んだ国際的な枠組み*を整備していくこととあいまって、既に情報保全制度が経済・技術の分野においても定着し活用されている国々との間での協力を一層進めることを可能とし、ひいては、国家安全保障戦略が示す我が国の安全保障に関わる総合的な国力の向上にも資するものである。

*既存の国際的な枠組みとしては、我が国は、米、仏、豪、英、印、伊、韓、独、NATO の９箇国・機関との間でそれぞれ情報保護協定（協定に従って相互に提供される情報を受領する締約国の国内法令の範囲内で適切に保護するための手続等について定めるもの）を締結済み（米、印、韓との協定は、軍事情報のみが対象）。

（2）企業からのニーズ

・　スタートアップも含めた様々な企業から、同盟国等の政府調達等において、国際的に通用するセキュリティ・クリアランスの制度や国際的な枠組みがあれば変わったのではないかという観点から、主に以下のような声が聞かれた。

- ✓ ある海外企業から協力依頼があったが、機微に触れるということで相手から十分な情報が得られなかった。政府間の枠組みの下で、お互いにセキュリティ・クリアランスを保有している者同士で共同開発などができれば、もう少し踏み込んだものになったのではないか。
- ✓ 自衛隊の装備品とは関係ない国際共同開発において、セキュリティ・クリアランス保有者がいなかったために、秘密指定されていないが管理が必要な情報（いわゆるＣＵＩ（Controlled Unclassified Information））の開示を受けるまでに長い時間を要したにもかかわらず契約に至らなかったことや、最終的に開示を受けることができたが周辺情報だけに留まったこともあった。
- ✓ 防衛と民生が一緒になったデュアル・ユース技術に関する会議に参加する際、クリアランス・ホルダー・オンリーであるセミナー・コミュニティがあり、これらに参加できず最新のデュアル・ユース技術に触れることができない。
- ✓ 宇宙分野の海外政府からの入札に際し、セキュリティ・クリアランスを保有していることが説明会の参加要件になっていたり、商業利用分野であってもＣＩが含まれているので詳細が分からない等の不利な状況が生じている。
- ✓ 様々なサイバーセキュリティ・インシデントが起きている中で、政府側や諸外国が保有している様々な情報が共有されれば、個々の企業のセキュリティ・レベルの向上、ひいては我が国全体のセキュリティ・レベルの向上にもつながる。
- ✓ セキュリティ・クリアランス制度の導入によって、将来的に、例えば衛星・ＡＩ・量子、Beyond 5G といった次世代技術の国際共同開発に関する機会が拡充してくるのではないか。

・　こうした企業からの声は、経済・技術の分野にも対応した制度の下でセキュリティ・クリアランスを保有していれば、その結果として、その他の場面でも、いわば「信頼できる証」として対外的に通用することになるのではないかということを示唆している。

・　そして、このような制度においては、機微な情報を扱う者について信頼性の確認を行う必要があることはもちろんのこと、信頼性の確認を含む情報保全全般が米国を始めとする主要国との間でも認められるものでなくてはならないと考えられる。

３　新たな制度の基本的な骨格

・　冒頭でも述べたとおり、諸外国で運用されているセキュリティ・クリアランス制度は、国家における情報保全措置の一環として、政府が保有するＣＩにアクセスする必要がある者の信頼性を確認した上でアクセスを認める制度である。
・　今回、我が国で経済安全保障の観点からセキュリティ・クリアランス制度の整備を検討するに当たっては、主要な同盟国や同志国に通用するものとしなければならないことから、諸外国と同様に、ＣＩ保全制度の一環としてセキュリティ・クリアランスの仕組みを整備すべきである。
・　この点、前述のとおり、我が国には既に、セキュリティ・クリアランスを含むＣＩ保全制度として、平成 25 年に成立した特定秘密保護法に基づく特定秘密制度が存在する。特定秘密制度は、諸外国との情報保護協定において、トップ・シークレット（Top Secret）及びシークレット（Secret）に相当するＣＩの保全枠組みと位置付けられ、諸外国に通用するものとなっている。
・　したがって、今回の制度の検討に当たっては、特定秘密制度の中で整備するにせよ、経済安全保障に特化した別の制度として整備するにせよ、既存の特定秘密制度との整合性や連続性に配慮することが、諸外国との関係でも、ＣＩを管理する政府及びＣＩへのアクセスを要する民間事業者にとっても重要である。このため、仮に別の制度として整備するのであれば、基本的には、特定秘密保護法の構造を参照しつつ、新たな制度を検討することが適当である。
・　すなわち、①政府として秘匿すべき機密情報の指定・解除のルールを定めた上、②当該情報に対する厳格な管理や提供のルールを定め、併せて、③漏えいや不正取得に対する罰則も定めるのがＣＩ保全制度の基本的な骨格であり、②の管理・提供ルールの中で、情報へのアクセスの条件として個人や事業者のセキュリティ・クリアランスの仕組みを設ける必要がある。
・　当然ながら、ここでいう情報指定の対象は政府が保有する情報であり、また、セキュリティ・クリアランスを受けることとなる者は、政府職員のほか、政府からＣＩの提供を受ける意思を示し、政府と秘密保持契約を結んで政府が保有するＣＩの内容に触れることを要する業務を行おうとする事業者及びその従業者である。
・　なお、政府として秘匿すべき機密情報の対象として、現行の特定秘密制度が対応していない諸外国のコンフィデンシャル（Confidential）級のＣＩにも対応する形にすべきである。
・　また、信頼性確認の手続については、後述するとおり、調査機能を一元化していくことにより、政府全体での統一的な対応を行うとともに、調査の共通化を通じて、官民ともに信頼性確認を受ける者の負担の軽減をし、利便性を向上させることも検討すべきである。

４　新たな制度の具体的な方向性

（１）情報指定の範囲

①　制度の対象とすべき情報の分野

・　経済安全保障上重要な情報を指定していくに当たっては、我が国として真に守るべき政府が保有する情報に限定し、そこに厳重な鍵をかけるというのが基本的な考え方である。同時に、アクセスを認められている者の間では、Need-to-Know の原則の下でスムーズな情報交換ができるようにするべきである。

・　上記のとおり、特定秘密保護法においては、政府が特定秘密として指定できる情報の範囲は、防衛、外交、特定有害活動の防止、テロリズムの防止の４分野に関する一定の要件を満たす事項に限られているが、例えば、国家及び国民の安全を支える我が国の経済的な基盤の保護に関する情報として、サイバー関連情報（サイバー脅威・対策等に関する情報）や規制制度関連情報（審査等に係る検討・分析に関する情報）、調査・分析・研究開発関連情報（産業・技術戦略、サプライチェーン上の脆弱性等に関する情報）、国際協力関連情報（国際的な共同研究開発に関する情報）といった政府から本会議に示された経済安全保障上重要な情報の候補の中には、政府として、特定秘密と同様又はそれに準ずるものとして厳格に管理すべき情報もあると考えられるところ、そうした情報について、特定秘密制度によるにせよ、別の制度になるにせよ、シームレスに、取扱者のセキュリティ・クリアランスを含む厳格な管理が行われるようにすべきである。また、指定の対象となる情報の範囲については、法令等によりあらかじめ明確にしておくべきである。

・　また、このように厳格に管理すべき情報については、米国等では、ＣＩを、漏えいした場合の被害の深刻さ等に応じて、トップ・シークレット（Top Secret）、シークレット（Secret）、コンフィデンシャル（Confidential）等の複数の階層に分けて、機微度に応じた複層的な管理をするのが一般的である点にも留意が必要である。すなわち、我が国の特定秘密保護法では、特定秘密という単一の層しか規定されていないが、諸外国にも通用する制度を目指していく観点からは、情報指定の範囲を経済分野等も対象としていくとともに、単層構造から複層構造になるようにすべきである。その際、特定秘密は、我が国が諸外国と締結している情報保護協定上では、トップ・シークレットとシークレットの２階層に対応すると整理されているが、それらの下の階層であるコンフィデンシャルに相当する政府保有情報も、同様に法律に基づく情報指定の対象となるようにすべきである。

・　上記の検討に当たっては、新たな技術開発の進展など経済安全保障分野における変化の速さ等にも鑑み、情報の指定・解除に当たっては柔軟かつ機動的に対応できるように、政府以外の様々な関係者の意見も踏まえつつ、制度設計すべきである。

・　なお、これらの重要な情報のうち、要件を充足するものについては、各省庁にお

いて適切に情報指定されていくことが望ましく、各行政機関のリテラシーを高めるとともに、国家安全保障局等が中心となって、政府全体の総合調整を適切に実施していくべきである。

・　また、本会議では、必ずしも新たな制度の法形式について議論することを求められているわけではないが、仮に、特定秘密制度とは別の制度として整備することになるのであれば、諸外国ではＣＩは一つの制度で管理されているということとの関係にも十分に留意し、シームレスな運用を目指していくべきである。

②　民間事業者等が保有する情報

・　秘密指定の対象となるのは、政府が保有している情報であり、政府が保有するに至っていない情報を政府が一方的に秘密指定することは想定されない。

・　また、政府が民間事業者等から提供を受けて保有するに至った政府保有情報の取扱いについては、秘密指定すること自体が妨げられるものではないものの、秘密指定の効果は、政府との間で秘密保持契約を締結し、政府が秘密指定している情報と告げられてその提供を受けた者にのみ及び、かつ、それは、従前から民間事業者等が保有していた情報と重なる部分がある場合には、当該従前からの保有情報の管理に規制が加わるものではないと整理すべきである。

（２）情報の管理・提供ルール

・　セキュリティ・クリアランス制度に関わる情報の管理や提供のルールとしては、大きく、①行政機関内における管理ルール、②行政機関・民間事業者の別を問わず情報に接する必要性のある個人に対するクリアランス（Personnel Security Clearance：ＰＣＬ）、③事業者に対するクリアランス（Facility Security Clearance：ＦＣＬ）、の３つがある。そのうち、事業者に対するクリアランスについては、情報を物理的に保全するための施設の適格性の側面に加えて、事業者そのものの属性や組織の適格性も見る必要がある。

①　行政機関内における管理ルール

・　特定秘密保護法では、各行政機関が秘密保護規程を設けて適切な情報管理を実施している。

・　新たな制度においても、情報公開法や公文書管理法といった他法令との関係も踏まえながら、必要な規程を整備すること等によって、適切な情報管理に努めるようにすべきである。

②　個人に対するクリアランス

・　政府による調査とその調査結果に基づく信頼性の確認（評価）は、政府が保有する経済安全保障上重要な情報にアクセスし得る限られた者を特定する重要なプロセスであるところ、調査すべき項目や評価における着眼点といった点については、

基本的に、特定秘密制度と差異を設ける理由はないと考えられる。

- 他方で、特定秘密保護法の下での個人の適性評価とそのための調査については、関係行政機関がそれぞれ実施することになっており、政府統一基準の下で運用されているところ、政府内の人事異動によって改めて適性評価とそれに伴う調査を実施することとしている点や、現行の枠組みの中で、政府と複数の契約をしている場合に、それぞれを所管する行政機関等から調査を別々に受けなければならないといった声が企業から聞かれている点も踏まえて、新たな制度においては、情報保全の効果を棄損しない範囲で適切に効率化の検討をすべきである。
- 具体的には、調査と信頼性の確認（評価）は別のプロセスであり、最終的な信頼性の確認はその情報保全に責任を持つ行政機関が行うことを前提に、調査機能を一元化することにより、調査結果が一度得られれば、一定の有効期間の間、当該調査結果が組織や部署を超えて有効となるような一定の「ポータビリティ」を持たせることが重要である。
- その際、政府における限られた資源を効率的・効果的に活用する観点からも、調査機能の一元化を通じて、調査結果を一つの機関に集約し、当該機関が調査実務を担うことで、手続の効率化及び政府内における統一的な対応を図るとともに、信頼性の確認を受ける者の重複調査の負担を減らし、上記企業の声に応えていくべきである。
- また、信頼性が確認された後又は信頼性の確認手続中に本人側の事情変更があった場合に、信頼性の確認（評価）を行う各行政機関や調査機関がこれをタイムリーに把握できるよう、本人からの自己申告等の仕組みを確保するとともに、信頼性が確認された後に各行政機関と本人とのコミュニケーション等により継続的に状況を把握する仕組みについても検討していくべきである。

③　事業者に対するクリアランス（民間事業者等に対する情報保全）

- 経済安全保障施策を進める中で、政府が保有する経済安全保障上の重要な情報を民間事業者等に共有していく場合も多くなると考えられる。上記のとおり、特定秘密保護法等を始めとした情報保全制度の下では、民間事業者等の従業者に対する調査や民間事業者等の保全体制（施設等）の確認が規定されているが、防衛産業にとどまらず、政府からＣＩの共有を受ける意思を示した民間事業者等及びその従業者であって、ＣＩへのアクセスを真に必要とするものについて、同様の厳格な対応を適用していくことが必要になると考えられる。
- 諸外国においても、こうした事業者に対するクリアランス制度は整備されており、民間事業者等が保有する施設などの物理的管理要件だけではなく、当該民間事業者等の株主構成や役員構成といった組織的要件も確認することとしている。特に、米国においては、国家産業保全計画（NISP: National Industrial Security Program）及びその運用マニュアル（NISPOM: National Industrial Security Program Operating Manual）があり、「外国による所有、管理又は影響（FOCI:

Foreign Ownership, Control or Influence)」を管理する規定があるほか、サイバーセキュリティに関する規定等もある。また、それらの解説であるハンドブック（Facility Clearance（FCL）Orientation Handbook）には、組織的要件の１つとして、ＣＥＯや取締役会議長のＰＣＬ取得が要求されるとの記述もある。

・ 国内においても、現行制度の運用や主要国の例も参照しつつ、我が国の企業等の実情や特定秘密保護法、外国為替及び外国貿易法、会社法等との整合性も踏まえながら、実効的かつ現実的な制度を整備していくべきである。

（３）プライバシーや労働法制等との関係

① 評価対象者への丁寧なプロセス

・ 重要情報を取り扱う業務に従事する従業者については、信頼性の確認とそのための調査が必要となる。

・ 当該調査は、本人の意思に反して行われるものではなく、ＣＩへのアクセスを必要とするためセキュリティ・クリアランスを真に必要とする者の任意の了解の下で行われるものである。現行の制度においても、特定秘密等に関わる政府職員や民間事業者等の従業者については、本人の同意を得るに当たって丁寧な手順を踏んだ上で一定の調査が実施されているが、経済安全保障上の重要な情報等に係るセキュリティ・クリアランス制度の検討に当たっても、同様に丁寧な手順を踏んだ上で本人の同意を得て調査を行うことが大前提である。

・ 本人の同意は、言うまでもなく、任意かつ真摯なものでなければならず、そのような真の同意を得るには、あらかじめ本人に対して、どのような調査が行われるのかを含め、同意の判断に必要な事項が知らされること、及び同意を拒否し又は取り下げても不当な取扱いが行われないことが担保されることが重要である。

・ また、経済安全保障に関するセキュリティ・クリアランスは民間に広がっていくことが想定されるところ、民間事業者等の従業者にあっては、行政機関から同意確認を受けるより前に、まず所属事業者等により、行政機関に提出する名簿に掲載するための同意確認が行われることとなるため、この場面における同意についても、同様に同意の判断に必要な事項が知らされるとともに、同意の拒否や取下げを理由とする不当な取扱いが行われないことが確保されるべきである。

② プライバシーとの関係

・ 信頼性の確認に当たって収集される情報は、対象者の個人情報であり、行政機関において厳重に管理されることが必須である。

・ この点、特定秘密制度では、評価対象者が適性評価の実施に同意せず又は同意を取り下げたこと及び評価対象者についての適性評価の結果その他適性評価の実施に当たって取得する個人情報について、特定秘密保護の目的以外での利用や提供が禁じられているところ、新たな制度においても、同様の措置を講じることが必要である。

・　なお、前記（２）②のとおり調査機能を一元的機関に集約し、そこで個人情報を保管することとする場合には、無用に長期にわたって情報が保管され続けないように配慮すべきである。
・　また、民間事業者等の従業者にあっては、調査において行政機関が収集した個人情報が所属事業者等に共有されるべきではなく、本人から行政機関への回答に所属事業者を介在させないなど、ここで収集される個人情報が所属事業者等の目に触れないような運用上の工夫もなされるべきである。

③　不利益取扱いの防止等
・　信頼性確認を受けることへの同意を拒否し若しくは取り下げ、又は評価の結果セキュリティ・クリアランスを得られなかった場合に、ＣＩを取り扱う業務に就けないのは制度上やむを得ないが、それを超えて、かかる同意拒否・取下げや評価結果を理由に不合理な配置転換などの不利益取扱いを受けることは許容されるべきでなく、そうした不利益取扱いを含む調査結果等の目的外利用は、特定秘密保護法と同様に禁止されるべきである。
・　また、信頼性の確認を受ける対象者が広がり得ることや、企業においては一般に雇用主からの求めによって信頼性の確認を受けることを念頭に置きつつ、労働法令との関係を十分踏まえ、同意プロセスの瑕疵や不当な取扱いを実効性をもって防ぐための方策についても検討すべきである。
・　さらに、評価の結果セキュリティ・クリアランスを得られなかった場合には、その結果と理由が本人に速やかに通知されること及び異を唱える機会が確保されることも重要である。
・　なお、不利益取扱いの予防措置として、ＣＩを取り扱う業務に就くことが予定される求職者については、セキュリティ・クリアランスが必要となることを採用前に告知した上、信頼性確認を受ける機会を設けること等により、採用内定後の内定取消しや採用後の解雇等の不利益取扱いに至ることを未然に防ぐという運用の在り方も検討されるべきである。

（４）漏えい等の罰則
・　ＣＩ保全制度においては、前記１のとおり、セキュリティ・クリアランスを始めとする特別の管理ルールを定めるほか、漏えいした場合に厳罰を科すのが通例であり、情報保全の実効性を担保する観点からも、主要国に通用するという観点からも、漏えい等に対する罰則を定めることは重要である。
・　この点、経済安全保障上重要な情報のうち、トップ・シークレット級及びシークレット級の情報については、特定秘密保護法の法定刑と同様の水準とすることが適当であることは言うまでもないが、コンフィデンシャル級の情報に対してどのような水準としていくかは、不正競争防止法や国家公務員法など漏えい

行為を処罰する国内法とのバランスも踏まえながら、政府において具体的に検討していくべきである。

・　また、漏えい等が法人の事業活動の一環として行われた場合に法人を処罰する規定を置くことについても検討すべきである。

（５）情報保全を適切に実施していくための取組

・　上記の方向性に基づく新たな制度を実効的なものとするためには、官民双方において、情報保全の重要性を理解した上で、適切に対応していくことが重要である。

・　そのため、まずは、政府において、こうした理解が国民に広く醸成されるよう、新たな制度の具体的な中身やその必要性、どのような事業者に影響が及ぶのか等について、分かりやすい説明を尽くしていくべきである。その際、特に、諸外国では、このような信頼性の確認を受けることで処遇面も含めて社会での活躍の幅が広がるものと認識されているということを踏まえることも重要である。

・　また、官民双方において、主要国の実態や動向も踏まえながら、適切な体制や設備を整備する必要がある。

・　この点、政府においては、情報保全を適切に実施するため必要な体制整備の在り方を検討する必要がある。前記（２）①のとおり、経済安全保障上の重要情報を管理するための保護規程を整備するとともに、調査に関して取得・作成した文書等について公文書管理法や個人情報保護法に基づき厳重に管理していくべきであるほか、実際の保全措置を講ずるに当たり、必要があれば、専用の区画や施設も設けていくべきである。

・　また、民間事業者等における適切な保全に資するよう、事業者から見て分かりやすい基準等の文書を作成、公表していくべきである。その際、経済安全保障分野に関する状況変化に応じて、又はその状況変化を見通して、不断の見直しを徹底していくことも重要である。

・　さらに、セキュリティ・クリアランス制度を日本の民間事業者等の海外ビジネス展開につなげていくためには、それを後押しするような同盟国・同志国との連携も重要であり、政府においては、今回の制度整備を踏まえ、同盟国・同志国との間で新たに必要となる国際的な枠組みについても取組を進めていくべきである。

・　このほか、民間事業者等においても、実際に政府から経済安全保障上の重要情報が提供された際には、専用の区画や施設を設ける必要があるが、こうした施設等の整備は、民間事業者等にとっては少なからぬ負担となるとも考えられる。かかる負担については、民間事業者等が政府からの協力要請に応じてＣＩに触れることとなる場合など、経緯や実態も踏まえて、民間事業者等における保全の取組に対する支援の在り方について合理的な範囲内で検討していく必要がある。

５　ＣＩ以外の重要な情報の取扱い

・　ＣＩ以外の情報については、諸外国でもセキュリティ・クリアランスの対象ではないため､今回のセキュリティ･クリアランス制度の検討の射程からは外れるが、例えば、情報の機微度はＣＩに指定するほどではないものの厳格に管理した方がよいと考えられる政府保有情報や、民間事業者等が保有している情報であって国として保全が必要と考えられる情報の取扱いについては、信頼性の確認のための調査も含め、ＣＩに対するものほど厳格ではないが一定の保全措置を講ずる必要性について、今後検討を進めていくべきである。
・　このうち、民間事業者等が保有している情報については、国が一方的に規制を課すことは民間活力を阻害する懸念もあることに留意が必要であり、民間事業者等が営業秘密として自主的に管理していくことが基本であると考えられるが、他方で、民間事業者等が自らのために営業秘密をしっかりと管理していくことは、我が国の経済安全保障にも資する面がある。
・　そこで、政府として、民間事業者等が真に必要な情報保全措置を講じられる環境を整えていけるよう、民間事業者等任せにせず、明確な指針等を示していくことの妥当性も含め検討を進める必要がある。

（参考１）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議構成員

（五十音順）

	梅津 英明	森・濱田松本法律事務所 パートナー弁護士
	北村 滋	北村エコノミックセキュリティ 代表
	久貝 卓	日本商工会議所 常務理事（第７回まで）
	小柴 満信	経済同友会 経済安全保障委員会 委員長
	境田 正樹	ＴＭＩ総合法律事務所 パートナー弁護士
○	鈴木 一人	東京大学公共政策大学院 教授
	冨田 珠代	日本労働組合総連合会 総合政策推進局総合局長
	永野 秀雄	法政大学人間環境学部 教授
	畠山 一成	日本商工会議所 常務理事（第８回から）
	原 一郎	一般社団法人 日本経済団体連合会 常務理事
	細川 昌彦	明星大学経営学部 教授
◎	渡部 俊也	東京大学未来ビジョン研究センター 教授

（◎：座長　○：座長代理）

（参考２）経済安全保障分野におけるセキュリティ・クリアランス制度等に関する有識者会議開催実績

第１回　　令和５年２月 22 日

第２回　　令和５年３月 14 日

第３回　　令和５年３月 27 日

第４回　　令和５年４月７日

第５回　　令和５年４月 25 日

第６回　　令和５年５月 29 日

（中間論点整理の公表 令和５年６月６日）

第７回　　令和５年 10 月 11 日

第８回　　令和５年 11 月 20 日

第９回　　令和５年 12 月 20 日

第 10 回　　令和６年１月 17 日