中間論点整理

令和５年６月６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。

・　このセキュリティ・クリアランス制度に関する最近の動きとして、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た。本提言は、これらの有識者会議の委員の検討の結果を中間的に論点整理したものであり、本提言が示した方向性を踏まえ、詳細な制度設計を含め、更なる検討を促すものである。

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、特定秘密の保護に関する法律（以下「特定秘密保護法」という。）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３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４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（以下「ＣＵＩ」(Controlled Unclassified Information) という。）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　新たな制度の方向性

（１）ＣＩを念頭に置いた制度

・　上記のとおり、セキュリティ・クリアランス制度とは、あくまで国として守らなければならないＣＩ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）に対して政府が調査を行い、当該者の信頼性を確認した上で、アクセスを認めるというものであることから、経済安全保障分野を中心にセキュリティ・クリアランス制度の在り方を検討していく上でも、あくまで、情報保全の主たる対象はＣＩであることを前提に検討していくことが必要である。

・　政府から民間事業者等にＣＩが共有される場合には、当該民間事業者等の従業者及び民間事業者等の保全体制（施設等）について、ＣＩを取り扱うに足る旨の信頼性の確認がなされる必要がある。

（２）主要国との間で通用する実効性のある制度、必要となる国際的な枠組み

・　今回の検討に当たっては、新たに設けられる制度が「相手国から信頼されるに足る実効性のある制度」とならなければ意味がなく、そこを目指すということが重要である。

・　ここでいう相手国とは、特に米国や英国を始めとする欧州等の主要な同志国を指すが、これらの国の情報保全制度は米国と比較的整合性のある実効的な制度となっており、こうした同盟国・同志国の制度も踏まえ、検討を進めていくことが必要である。

・　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検討を進めていくべきである。

（３）政府横断的・分野横断的な制度の検討

・　我が国では既に、特定秘密保護法等を始めとした情報保全制度があり、防衛分野を中心に、政府及び民間事業者等の間では情報保全体制が構築されている実態があることから、今回の検討が既存の諸制度と切り離されたものとなると、政府内だけではなく、民間事業者等にとっての運用コストや管理コストが増すことにもつながる。このため、経済等の新たな分野を含めた政府横断的・分野横断的な視点を持ち、従来の防衛分野における情報保全制度を始め既存の諸制度等との整合性にも留意しつつ、あるべき制度を検討することが必要である。

・　また、情報保全制度だけではなく、情報公開法や公文書管理法といった他法令とも関係することが想定されるため、これらとの整合性についても今後検討が必要である。

４　具体的な方向性

（１）情報指定の範囲

・　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、経済制裁に関する分析関連情報や経済安全保障上の規制制度における審査関連の情報、サイバー分野における脅威情報や防御策に係る情報、宇宙・サイバー分野等での政府レベルの国際共同開発にもつながり得る重要技術情報といった情報などの中には、政府として、上記４分野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、経済関係省庁等も含めて政府内で議論を深め、上記４分野との整理も含め情報指定の範囲についての検討を深めるべきである。

・　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していくことも検討すべきである。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おり、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情報の取扱いについても検討する必要がある。

・　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も踏まえて必要な情報を柔軟に指定できるような制度設計が望ましいほか、政府以外の様々な関係者の意見も踏まえつつ、情報の指定・解除に当たっては機動的に対応できるようにしていくことの検討も必要である。

（２）信頼性の確認（評価）とそのための調査

・　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）については、政府の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。

・　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等につき、更に運用の実態を踏まえつつ、情報保全の効果を棄損しない範囲で効率性を追求するべく検討を深める必要がある。

- また、企業からは、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聞かれている点にも留意が必要である。
- 米国等主要国の例も参考に、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が想定されるが、例えば、調査については、既存の諸制度との整合性や防衛省・防衛産業等の運用実態に留意しつつ、その機能を一元的に集約する可能性も含め、調査結果につき一定のポータビリティ性（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であること。例えば、政府職員が政府内の異動や政府から民間事業者等への異動を経ても結果が有効、あるいは、民間事業者等において、他の所管行政機関や契約にも当該調査結果が有効であること等が含まれ得る。）が確保されるよう、また、その適正な水準が維持されるよう、政府全体で統一的な対応を行っていくことが望ましい。また、こうした検討に当たっては、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も踏まえることが必要である。

（３）産業保全（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。
- この点、例えば、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）において、民間企業等の非政府組織が遵守すべき事項が包括的に規定されており、その中には物的保全に関する規定や、民間企業等の非政府組織のガバナンスにおける「外国による所有、管理又は影響（FOCI：Foreign Ownership, Control or Influence)」を管理する規定のほか、サイバーセキュリティに関する規定等もあることから、こうした制度も参考にしながら検討を深めることが必要である。

（４）プライバシー等との関係

- 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。その際、信頼性の確認のために収集された情報の管理が適切になされることは必須である。

・ 制度の検討に当たっては、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、信頼性の確認のための調査とプライバシーの関係や従業者の処遇への影響の考慮を含めた労働法令との関係を十分踏まえ、適切な形で整理を行うことが必要である。

（５）情報保全を適切に実施するための官民の体制整備

・ 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、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。

・ 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。また、実際の保全措置を講ずるに当たっては、適切な情報保全の観点から専用の区画や施設を設ける必要がある。

・ 民間事業者等においても、同様の区画や施設を設ける必要があり、民間事業者等にとっては少なからぬ負担となる。こうした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　その他

（１）ＣＩ以外の重要な情報の取扱い

・ 上記のとおり、セキュリティ・クリアランス制度の在り方を検討していく上では、主たる対象はＣＩであることが前提であるが、同時に、ＣＩ以外の重要な情報にも何らかの形で情報保全措置を講ずることが必要ではないかと考えられる。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などが挙げられる。

・ これらの情報の取扱いについては、米国等の主要国においても取組に差があるが、情報の重要性等を考慮すれば、必要に応じ、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も検討を進める必要があると考えられる。

・ 特に、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。

・　その上で、民間事業者等として必要性がある場合に、民間事業者等自身が必要に応じ自主的な調査を含む情報保全措置を講ずる必要性も指摘されている。検討の結果、環境整備を行う場合には、特にプライバシーや労働法令との関係も十分踏まえ、民間事業者等任せにせず、政府が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。

・　上記の取組を進める上で、公文書管理に係る諸制度のみならず、原子炉等規制法、営業秘密制度（不正競争防止法）、特許出願非公開制度や輸出管理制度等の既存の関連制度との関係も踏まえつつ、望ましい情報保全の在り方を検討していくことが必要である。

（２）信頼性の確認に係る理解の促進

・　諸外国では、信頼性の確認を受けることで社会での活躍の幅が広がるものと認識されているとの声も聞こえている。こうした認識に鑑み、処遇面も含め、このような信頼性の確認に係る理解の醸成に努めることが重要である。

（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
	小柴 満信	経済同友会 幹事
	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
	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

経済安全保障の観点からの情報保全の強化の必要性

□ 経済安全保障推進法の附帯決議や国家安全保障戦略を踏まえ、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た検討を進める必要。

経済安全保障推進法の附帯決議

衆議院内閣委員会（令和4年4月6日）

十四　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こと**。

参議院内閣委員会（令和4年5月10日）

二十一　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こと**。

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）

Ⅵ 我が国が優先する戦略的なアプローチ

2 戦略的なアプローチとそれを構成する主な方策

⑸ 自主的な経済的繁栄を実現するための経済安全保障政策の促進

エ　（前略）また、**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た検討を進める**。

いわゆる「セキュリティ・クリアランス」の概要

□ いわゆる「セキュリティ・クリアランス」とは、**国家における情報保全措置の一環**として、**①政府が保有する安全保障上重要な情報を指定**することを前提に、②当該情報に**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の者）**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**アクセス権を付与**する**制度**。**③特別の情報管理ルールを定め、当該情報を漏洩した場合には厳罰を科すことが通例**。

①情報指定

政府が保有する安全保障上重要な情報を指定

②調査を実施して信頼性確認（「アクセス権(セキュリティ・クリアランス)」を付与）

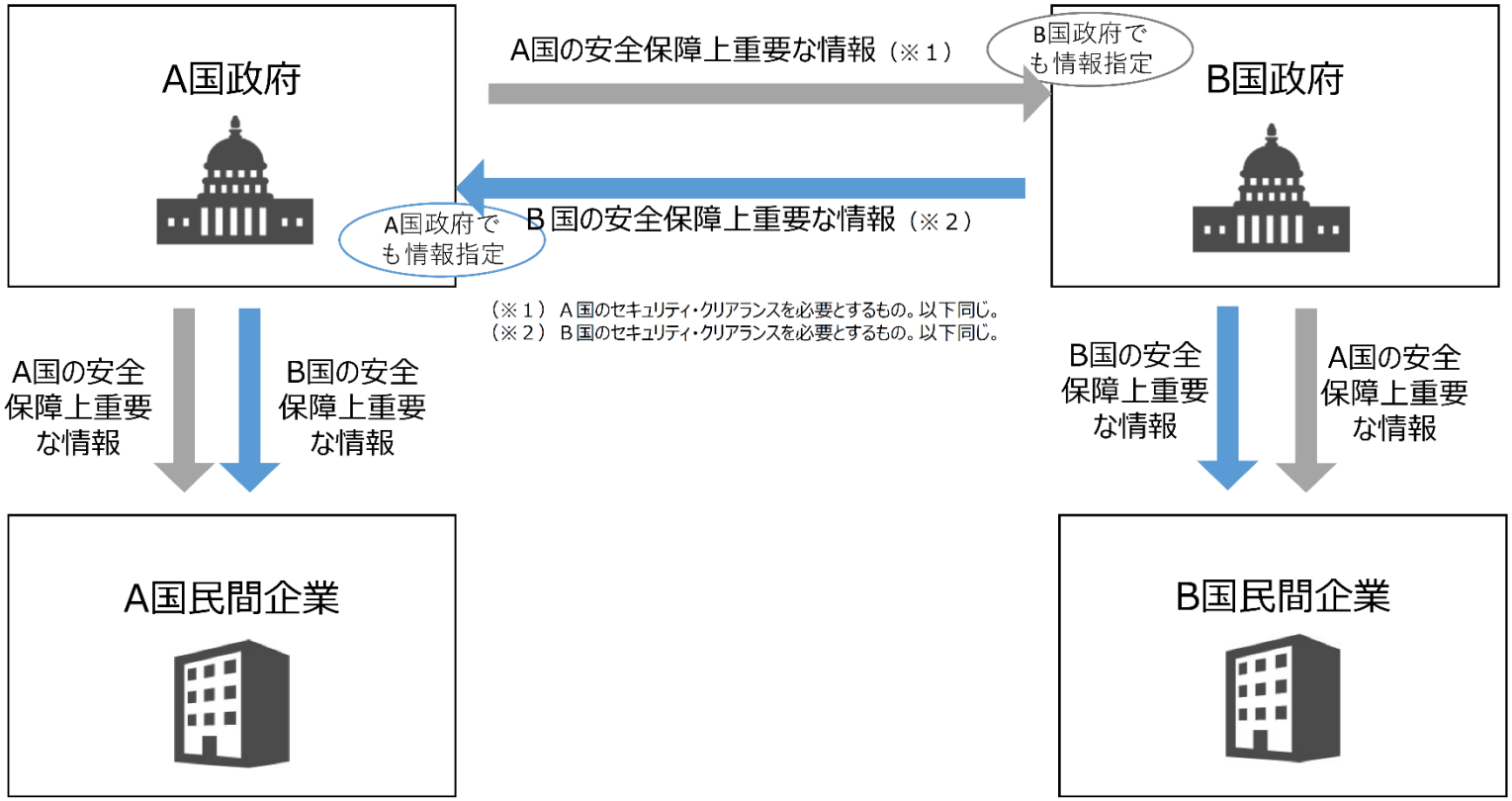
指定された情報にアクセスしようとする者（基本的に自国民が対象）

③情報漏えい時の厳罰を含む特別の情報管理ルール

これらと併せて、
民間事業者に政府から情報が共有される場合には、民間施設の保全体制を確認（施設クリアランス）

セキュリティ・クリアランスと安全保障上重要な情報のやりとりのイメージ

- 政府が保有する安全保障上重要な情報へのアクセス権（セキュリティ・クリアランス）は、基本的には自国民を対象に付与される。
- 外国政府の安全保障上重要な情報にアクセスするためには、自国政府を通じて行う必要がある。
  ※国によっては制度の差異あり。



諸外国における情報保全制度の比較（セキュリティ・クリアランス制度等①）

		アメリカ	イギリス	ドイツ	フランス	カナダ	オーストラリア
根拠		大統領令第13526号 等	政府セキュリティ基準 等	連邦保安審査に関する機密事項の保護に関する法律、秘密情報保護一般行政規則 等	防衛法典、国防秘密保護に関する省庁間一般通達第1300号 等	セキュリティポリシー、セキュリティマネジメントの指針 等	保護的保全方針枠組み 等
情報区分	クリアランス対象情報（注1） Top Secret級	**Top Secret** 不当な開示が国家安全保障に著しく深刻な損害を与えると合理的に予想し得るもの	**Top Secret** 英国又は同盟国の国家安全保障を直接支え、又は脅かす著しく機微な情報であって、あらゆる脅威からの保護に係る極めて高度な保証を要するもの	**Streng Geheim** 許可のない者が知ることで国又は州の存立又は死活的利益を危険に晒し得るもの	**Très Secret** 漏洩又はアクセスが防衛及び国家安全保障に著しく深刻な結果をもたらし得るもの	**Top Secret** 不当な開示が国益に著しく深刻な損害を与えると合理的に予想し得るもの	**Top Secret** 機密性が損なわれることにより国益、我が国の組織又は個人に著しく深刻な損害を与えると予想し得るもの
	Secret級	**Secret** 不当な開示が国家安全保障に重大な損害を与えると合理的に予想し得るもの	**Secret** 非常に機微な情報であって強力な組織犯罪集団や国家主体等の高度な能力を有する脅威からの保護を要するもの ※ 2014年に見直し（以前は**Confidential**の区分が存在）	**Geheim** 許可のない者が知ることで国又は州の安全保障を危険に晒し、又はその利益に重大な損害を与え得るもの	**Secret** 漏洩又はアクセスが防衛及び国家安全保障に損害を与え得るもの ※ 2021年に見直し（以前は**Confidentiel Défense**の区分が存在）	**Secret** 不当な開示が国益に重大な損害を与えると合理的に予想し得るもの	**Secret** 機密性が損なわれることにより国益、我が国の組織又は個人に重大な損害を与えると予想し得るもの
	Confidential級	**Confidential** 不当な開示が国家安全保障に損害を与えると合理的に予想し得るもの		**VS-Vertraulich** 許可のない者が知ることで国又は州の利益に害を及ぼし得るもの		**Confidential** 不当な開示が国益に限定的又は中程度の損害を与えると合理的に予想し得るもの	**Protected** 機密性が損なわれることにより国益、我が国の組織又は個人に損害を与えることが予想し得るもの
	その他取扱注意情報（注2）	**Controlled Unclassified Information**	**Official-Sensitive**	**VS-Nur Für Den Dienstgebrauch**	**Diffusion Restreinte**	**Protected**	**Official-Sensitive**
クリアランス対象情報の範囲・分野		①軍事計画・兵器システム又は軍の運用 ②外国政府情報 ③インテリジェンス活動・情報源・方法又は暗号 ④機密情報源を含む連邦政府の外交関係又は対外活動 ⑤国家安全保障に関連する科学的・技術的・経済的事項 ⑥核物質又は核施設の防護策のための政府プログラム ⑦国家安全保障に関連するシステム・設備・インフラ・プロジェクト・計画・防護サービスの脆弱性又は能力 ⑧大量破壊兵器の開発等	Top Secretの漏洩は次をもたらす／脅かす。 ①広範な人命損失 ②英国又は友好国の国内治安 ③国際的な緊張 ④英国又は同盟国の軍隊の有効性又は安全性 ⑤友好国との関係 ⑥安全保障活動又は諜報活動の継続的な有効性 ⑦英国経済への長期的な損害 ⑧重大な組織犯罪を捜査又は起訴する能力 ※Secretにも同様の類型あり	公共の利益のため、特に連邦又は州の福祉を保護するために秘匿する必要のある事実、物又は知見	「国防秘密」（政治、軍事、外交、科学、経済、産業等の分野で用いられる）	各省の判断により個々に情報の分類及び指定を実施	対象情報の漏洩は次の事項を脅かす。 ①個人の安全等 ②政府組織の能力、資産、法執行・政策遂行能力等 ③国の経済 ④国のインフラ ⑤国際関係 ⑥治安・国防・インテリジェンス活動
同情報指定権限者		大統領、副大統領、大統領が指名した行政機関の長、委任された政府職員が指定	各省庁・部局が、クリアランス対象情報に関する政策を執行し、指定	部局又はその被授権者が指定	大統領、首相、大臣等が指定の条件を定める当該条件に従い作成者が指定	各省が分類及び指定	機関を代表して情報を生成又は準備することに責任を有する者が指定

（備考）2023年３月時点の政府ＨＰ等を基にした事務局まとめ。各国制度は現在進行形で変更されているものがあり、また、全ての情報が公開されている訳ではない等から、上記が最新とは必ずしも限らない。
（注１）アメリカにおけるＣＩ（Classified Information）に相当する情報。
（注２）取扱いのためＣＩ相当のいわゆる「クリアランス」までは要しないが、取扱いに注意すべき情報として、一定の保全措置や調査が必要とされ得るもの。

諸外国における情報保全制度の比較（セキュリティ・クリアランス制度等②）

		アメリカ	イギリス	ドイツ	フランス	カナダ	オーストラリア
根拠		大統領令第13526号、第12968号、保全行政責任者指令６号　等	英国政府人的保全管理　等	連邦保安審査に関する前提及び手続並びに機密事項の保護に関する法律　等	防衛法典、国防秘密保護に関する省庁間一般通達第1300号　等	セキュリティスクリーニング基準　等	保護的保全方針枠組み　等
クリアランス付与の対象者		原則として、米国市民である政府職員、契約事業者、ライセンシー、認定資格保有者、政府機関からの助成金受領者	クリアランス対象情報へのアクセスを必要とする一定の役職に就く者 ※全ての公務員・軍所属者・政府の臨時職員・政府請負業者は基礎的調査基準（BPSS）に基づく調査に服する	安保上機微な活動を行うことを託される者 ※クリアランス対象情報へのアクセス権を有する又はアクセスし得る者、国際機関のクリアランス対象情報へのアクセス権を有する又はアクセスし得る者　等	クリアランス対象情報へのアクセスを必要とする役職を特定する一覧表に掲げられた役職に就く者	連邦政府内の役職者及び政府のセンシティブ情報を共有する必要のあるその他の個人 ※その他の個人：政府と一定の契約・臨時採用等の手続きを経た者	原則として、公務員採用要件を満たし、クリアランス対象情報へのアクセスを必要とする職務に就くこととなるオーストラリア国民
	民間人	政府との契約等によりクリアランス対象情報に触れる場合、民間人にもクリアランスが付与され得る					
クリアランスの種類	区分	① **Top Secret** へのアクセス資格 ② **Secret** へのアクセス資格 ③ **Confidential** へのアクセス資格	①**Top Secret**へのアクセス資格（Developed Vetting） ②**Top Secret**への限定的アクセス及び**Secret**へのアクセス資格（Security Check） ※上記のほか、**Secret**への限定的アクセス及びその他公文書全般へのアクセス資格であるBPSS、テロ関係及び空港関係ポストに関するアクセス資格があり、一定の調査が要求される	① **Streng Geheim** へのアクセス資格 ② **Geheim** へのアクセス資格 ③ **VS-Vertraulich** へのアクセス資格	① **Très Secret** へのアクセス資格 ② **Secret** へのアクセス資格	① **Top Secret** へのアクセス資格 ② **Secret**及び **Confidential** へのアクセス資格 ※**Secret**レベルと **Confidential**レベルで資格上の区別なし ※上記のほか、Protectedへのアクセス資格であるReliability Statusがあり、一定の調査が要求される	① **Top Secret** へのアクセス資格 ② **Secret** へのアクセス資格 ③ **Protected** へのアクセス資格
	有効期間	①５年又は6年 ②10年 ③15年 （注）	①7年 ②10年 ※BPSS：更新不要 ※テロ関係ポストに関する適性評価：10年 ※空港関係ポストに関する適性評価５年	原則10年 ※５年後に申告書再提出	①５年 ②７年 ※上記は調査機関による評価の有効期間 これを上限としてクリアランスの有効期間を決定	①５年 ②10年 ※Reliability Status：10年	①7年 ②10年 ③15年

（備考）2023年３月時点の政府ＨＰ等を基にした事務局まとめ。各国制度は現在進行形で変更されているものがあり、また、全ての情報が公開されている訳ではない等から、上記が最新とは必ずしも限らない。
（注）アメリカでは、有効期間の変更や、区分間での統一が現在進行形で議論されている。また、2018年より有効期限に関わらず政府内データベース等を用いた継続調査が一部実施されており、将来的には政府全体で実施予定。

情報の区分（イメージ）

	政府由来情報 （政府保有・民間へ共有）	民間由来情報 （民間保有）
CI(Classified Information)レベル	A （Top Secret、Secret、Confidential）	D
CIレベル未満の要保護情報	B	E
その他の情報	C	F