資料

# 事務局説明資料

令和５年11月20日
内閣官房

# 第７回会議の議論の整理（主なポイント）

## １．新たなセキュリティ・クリアランス制度の骨格

### （１）情報指定の在り方

- 「政府が外部から受領した情報については、秘密指定の効果は原保有者には及ばない」とあるので、**民間事業者が保有する情報には対象を広げないということを改めて明記すべき。**
- 「秘密指定の効果は原保有者には及ばない」という考え方に異論はないが、民間企業から政府に共有されて、なんらか付加価値がついたような場合には、対象となり得る。**どういう形で民間に提供された場合には秘密指定の効果が及ぶのかを明確にしないと、誤解に基づく反対意見も出てくるおそれがある。**
- アメリカの大統領令では、政府による指定だけでは機密指定すべき情報を網羅することができないことから、機密指定権を持たない者が、機密指定を必要とする情報を自ら創出し、秘密保全対象情報であると判断した場合には、**行政機関に速やかにその旨を通知する義務を課し、**この通知を受けた行政機関は30日以内に当該情報を機密指定するか否かを決定すると規定している。
- 必要最小限の情報を必要最低限の期間に限って指定するという抑制的な方針の下で運用されている特定秘密保護法とは一線を画し、**中間論点整理にあるとおり柔軟かつ機動的にやっていくという基本方針が必要。**
- 特定秘密保護法にも、貨物の輸出入禁止のように経済安保上の情報が挙がっている。**経済官庁が本当に守らなければいけない情報として指定していかないと、民間まで意識が高まっていかない。**
- 運用基準に該当すれば指定されるはずということだが、基準においても各行政機関の長が裁量性を持っている。**経済官庁において、特定秘密の指定が全くされていないのは、由々しき問題。特定秘密保護法の運用として改善すべき。**
- **本制度の対象とする情報については、国民の知る権利や事後的な検証についても検討が必要**ではないか。
- 技術革新が激しく、地政学的リスクも日々変化し、生成技術やデジタル技術といった様々な技術が日々革新されていることを踏まえると、これらの情報が重要情報か否かを審査する者には技術に関するリテラシーが必要。

# 第７回会議の議論の整理（主なポイント）

## １．新たなセキュリティ・クリアランス制度の骨格

### （２）調査とプライバシー・従業員との関係

- **民間事業者がセキュリティ・クリアランスを受けることに対する事前の労使協議と、セキュリティ・クリアランスの運用や対象業務などの労使協定締結を法律で義務付けておく必要。**
- 信頼性調査への同意拒否や調査結果を理由とする不合理な配置転換など、**労働者への不利益取扱いの禁止については、罰則を含め、あらかじめ法で規定をしておくべき。**
- **現実問題として、全ての取扱事業者に対して事前の労使協議や労使協定の締結を義務付けることは難しいのではないか。**どこまで義務付けるべきなのかといった議論も必要。
- 米国の原子力事業者は、労働組合の代表による労働安全衛生チェックが労働協約の中に含まれている関係で、秘密管理区画の中に入るために、労働組合の代表者もセキュリティ・クリアランスが必要とされ、組合も合意している。日本でも、同じようなことになる可能性については留意したほうが良い。

### （３）FCL、FOCI

- 外国に通用する制度を前提にするのであれば、**FOCI（Foreign Ownership, Control, or Influence）の適用等についても検討すべき**ではないか。
- 防衛産業保全政策に関する説明を受けたときに、**法人クリアランスにおいて、取締役会議長とCEOに相当する方に対する個人のセキュリティ・クリアランス**が入っていなかった。

# 第７回会議の議論の整理（主なポイント）

## １．新たなセキュリティ・クリアランス制度の骨格

### （４）セキュリティ・クリアランスの対象範囲

- CIに触れることになる企業の会計監査を行う監査法人や、サイバーセキュリティ監査を行う法人、法律事務所、特許事務所、環境監査を行う法人などもクリアランスの対象になると思われる。
- 現状の特許出願非公開制度には、人的クリアランスの要素はない。
- サイバー関連情報を利用する基幹インフラ事業者には、セキュリティ・クリアランスの対象とするよう義務として規制すべきではないか。
- 基幹インフラ事業者に別途義務化が必要という認識はなかったので慎重に検討すべき。中間論点整理の「政府からCIの共有を受ける意思を示した」という表現は重要。

### （５）罰則

- **罰則を法令で規定するのであれば、既存の制度との整合性が必要。**
- Top Secret、Secretについては特定秘密保護法と同じ水準で良いと思うが、Confidentialまで同じであるべきかは議論の余地がある。区分に応じて変える余地も残しておいた方が良い。
- 新制度の罰則が10年や５年となった場合、特定秘密のConfidential級には国家公務員法の１年の罰則しか及ばないということになり、均衡がとれない。

# 第７回会議の議論の整理（主なポイント）

## ２．対象情報の範囲

### （１）経済安保上重要な情報の候補

- 「国家及び国民の安全を支える経済的な基盤の保護に関する情報」の**「基盤」という用語が何を指すのかが不明瞭。**どういう意味で使われているのか、どれほど広い概念を持った言葉として使われるのかについて整理が必要。
- 「経済的な基盤」の中には、経済安全保障推進法の支援対象になっていない食料安全保障やエネルギー安全保障も含まれるであろうから、**どこまでのスコープで考えるのかについて検討が必要。**
- 「経済的な基盤の保護に関する情報」であって、漏えいすれば国家及び国民の安全に一定の支障を与えるおそれがあるいうものということであれば、例えば、AI技術や半導体技術の中でも、それが何らかの形で漏えいすると国家及び国民の安全に支障があると考えられる場合には、おそらく定義には含まれるのであろう。
- **サイバーの脅威情報や被害情報はむしろ公開して対策に努めてもらったほうが効果的だという指摘もある**中で、本当に情報指定するのか。
- 重要情報であることの基準の一つとして、プロの諜報員や工作員を動員して不正をしてでも取得したいということだと思うので、**悪意ある人や国からの不正なアクセスが増えてきている、といった情報もあると、制度の必要性が積極的に理解できるようになると思う。**
- 資料５ページは、**あくまでも重要な情報の候補であり、必ずしもすべてが秘密指定されるわけではない。**
- 諸外国がクリアランスの対象としている情報の範囲と重要情報の候補には、余りにもギャップがあると思う。
- 規制制度関連情報については、経済安全保障推進法のように経済安全保障自体を目的にしているような法律以外でも、**例えば、個別の業法でも一部の情報が安全保障に関わることもあるものについても、拾えるような丹念な作業が必要。**

# 第７回会議の議論の整理（主なポイント）

## ２．対象情報の範囲

### （２）CUI（Controlled Unclassified Information）、民間事業者が保有している情報

- **「経済的な基盤の保護」に関する情報の中には、国が保有するものだけではなく、民間が保有するものもあるはず。**民間企業に対する指針を与えるような規定を盛り込んでいくべきではないか。
- **法律の中に、CUIを保護していくというプログラム規定のようなものを設けた上で、それに向けて政府の努力義務規定のようなものを設け、それを根拠にして、政府がガイドラインを作っていくというような手法もあり得る。**
- CUIに関して、守るべき情報であるということをガイドラインで示すことはある程度可能だとしても、**それをどうやって守るのか。**クリアランスの対象情報を特定するという側面と、それをどうやって守るのかという側面をどのようにして担保していくのかが重要。
- **アメリカでは、CUIも、人的スクリーニングということで、少なくとも犯罪情報と財務情報をチェックしなければならず**、同様のことを我が国で実現するためには、ガイドラインでは無理で法定が必要。この点は、サイバーセキュリティ成熟度モデル（CMMC）2.0の適用に際しても重要。
- 民間事業者が保有している情報は、**政府に提供された情報で、かつ、秘密保持契約の締結等の形式要件を満たしたものがセキュリティ・クリアランスの適用となり、そうでないもの（CUI）はガイドラインの適用になる、といったように分けて説明をすべき。**
- 中間論点整理を踏まえ、**CIをまず議論してからCUIについても手当てを考えるという順番**にすべき。

# 論点

□ 経済安全保障上の重要情報に対し、下記のそれぞれの事項について、

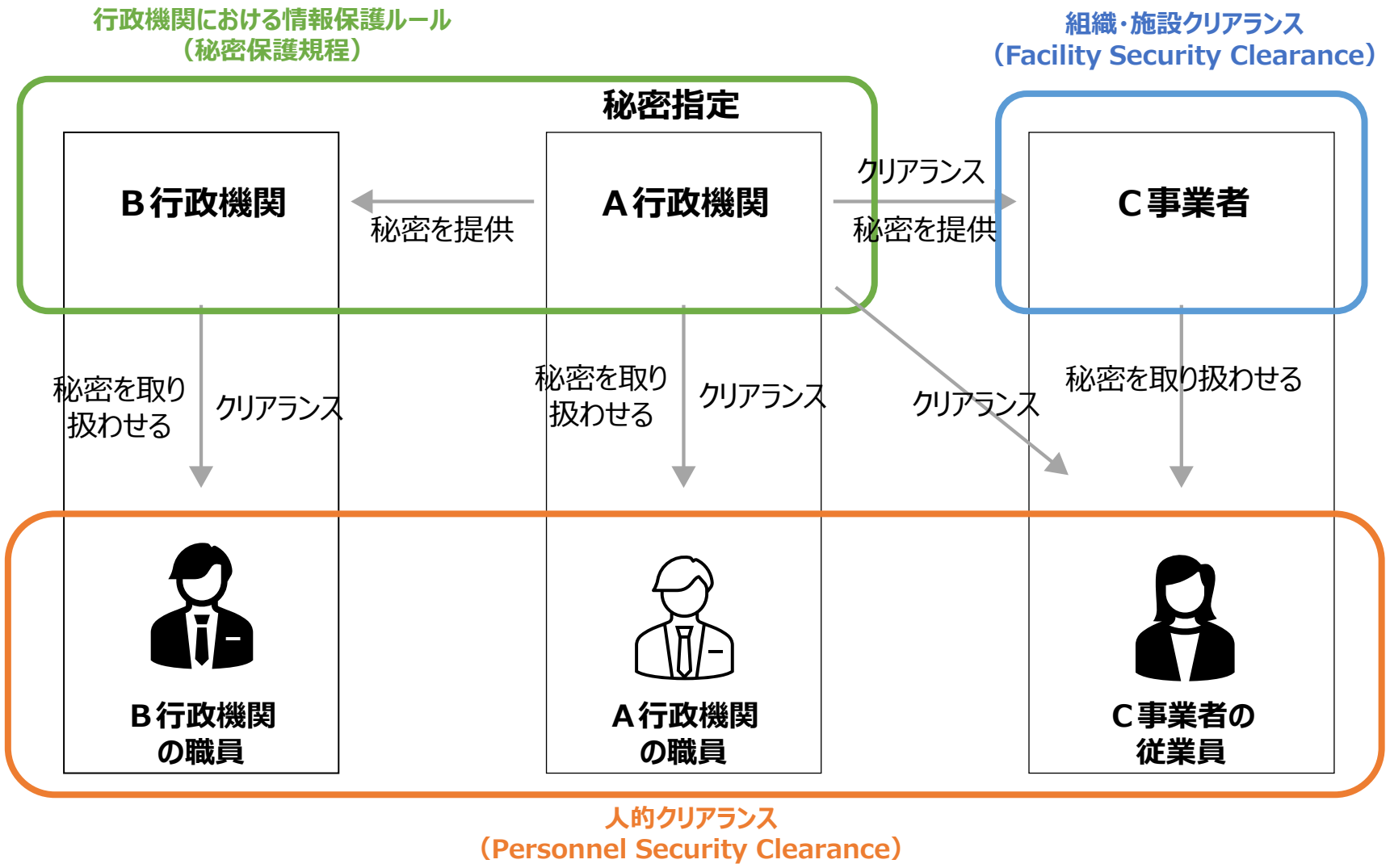
・Top Secret／Secret級の情報においては、特定秘密保護法と同レベルの取扱いとすることで良いか？

・Confidential級の情報においても、特定秘密保護法に準じた取扱いとすることで良いか？

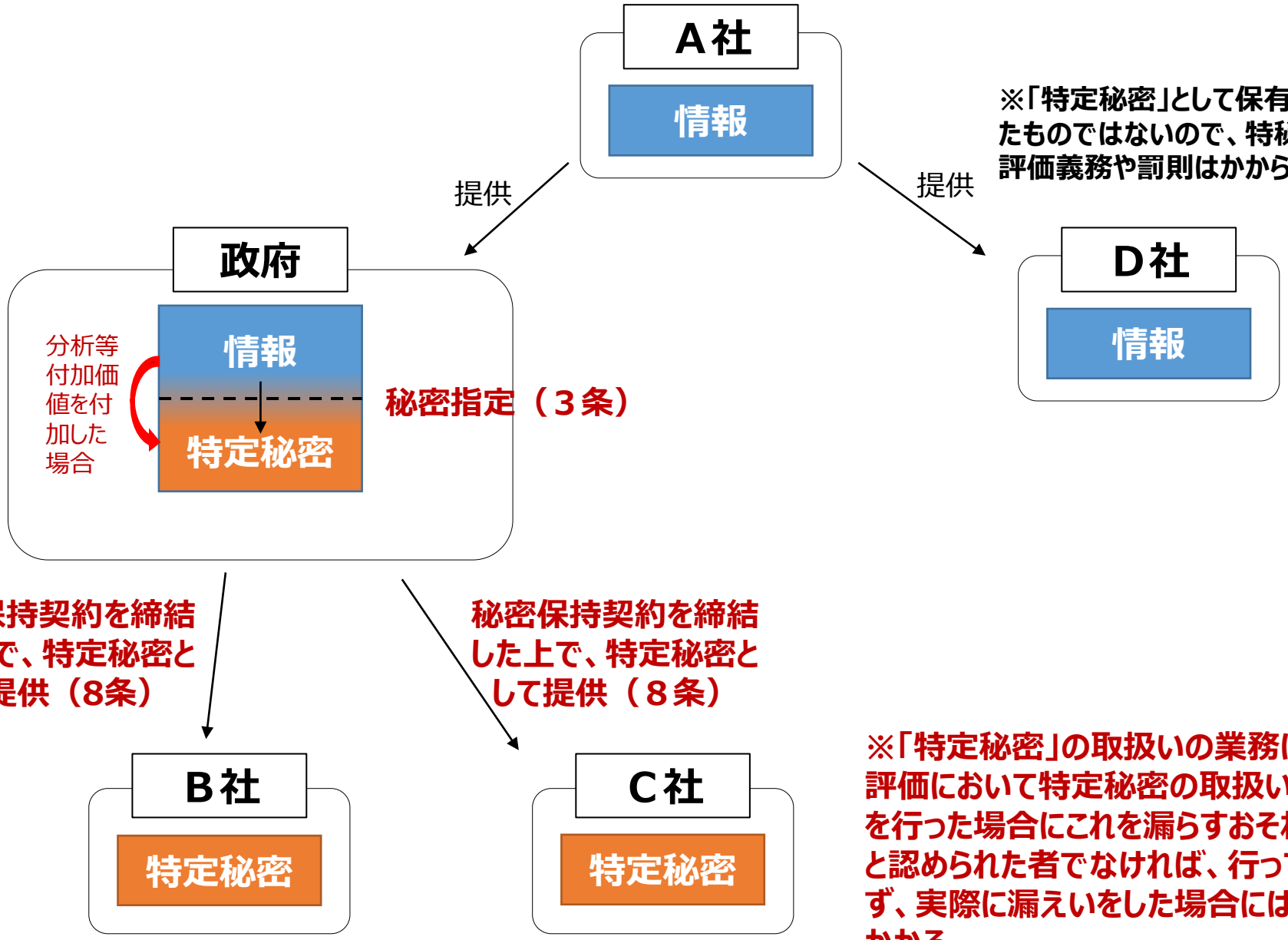
- **事業者に対する信頼性確認**
- **個人に対する信頼性確認**
- **漏洩等に対する罰則**

# 重要情報の主な流れとそれに対する保護ルールのイメージ

□ 重要情報を保護するルールとして、行政機関内での管理・保護を規定する秘密保護規程、事業者に対する組織・施設クリアランス、個人に対する人的クリアランス、がある。



# 【参考】民間提供情報を特定秘密に指定した場合にその効果が及ぶ範囲



# 【参考】特定秘密の指定の効果が及ぶ場合と及ばない場合

## 1）民間事業者が自ら作成した情報の場合

民間が保有している民生技術等の情報は原則として特定秘密の対象にはならない。
契約に基づき武器等の試験を行わせる場合等、例外的な場合に限られる。

政府 ⇔（「特定秘密」であることを明示／秘密保持契約）⇔ 民間事業者（例：契約に基づく装備品の性能試験の数値）→ **及ぶ**

政府（政府とのやりとりなし）→ 民間事業者（例：企業の独自開発による製品の数値）→ **及ばない**

## 2）民間事業者が政府から提供を受けた情報の場合

政府 ⇔（「特定秘密」であることを明示／秘密保持契約）⇔ 民間事業者（例：特定秘密に指定している装備品の性能）→ **及ぶ**

政府 →（非特定秘密）→ 民間事業者（例：公知の装備品の性能）→ **及ばない**

## 3）民間事業者が他の民間事業者から提供を受けた情報の場合

民間事業者 →（非特定秘密）→ 民間事業者（例：企業の独自開発によるエンジンの数値）→ **及ばない**

※　政府によって秘密指定された情報は他社に提供することはできず、他社から提供を受けた時点でそれは秘密指定された情報ではない。

# 【参考】行政機関における特定秘密の保護ルール

□ 特定秘密保護法では、各行政機関において、特定秘密保護規程を作成した上で、秘密の保護に当たることになっている。

■特定秘密保護規程の概要

第１章　総則
　― 特定秘密管理者・保全責任者の指名、保全教育の実施

第２章　特定秘密の指定等
　― 秘密の指定、指定期間の延長、解除

第３章　特定秘密の取扱いの業務
　― アクセス管理、立入・機器持ち込み制限、保管容器、施設設備、電子機器使用制限、作成、運搬、管理、伝達、保管、廃棄、検査

第４章　特定秘密の指定等が法等に従っていないと認めたときの措置

第５章　他の行政機関に対する特定秘密の提供

第６章　適合事業者への特定秘密の提供
　― 適合性審査、秘密の保護にかかる契約

第７章　その他公益上の必要による特定秘密の提供を受けた者による保護措置

第８章　適性評価
　― 実施責任者・担当者の指名、候補者・適性が認められた者の名簿の作成、苦情処理

第９章　通報窓口

第10章　雑則

（出典）各省庁の秘密保護規程を基に、事務局にて作成

# 【参考】特定秘密保護法における適合事業者の基準

□ 特定秘密保護法における適合事業者とは、特定秘密の保護のために必要な施設設備を設置していることを含む下記の基準に適合する事業者であることとされている。

■基準の主な内容（特定秘密の保護に関する法律施行令第13条）

次の措置の実施に関する**規程を定めており**、かつ、当該規程に従ってこれらの措置を講ずることにより**特定秘密を適切に保護することができると認められること**。

- 業務管理者の指名
- 必要な施設設備の設置
- 特定秘密取扱場所への立入り及び機器持ち込みの制限
- 使用する電子計算機の制限
- 作成、運搬、交付、保管、廃棄等の制限
- 業務の状況の検査
- 紛失その他の事故発生時の被害防止措置
- 従業者に対する教育
- 特定秘密の取扱いの業務を行わせる従業者の範囲の決定

など

# 【参考】海外の制度概要（施設クリアランス）

| | アメリカ | イギリス※1 | ドイツ | フランス |
|---|---|---|---|---|
| 概要 | ○ 事業者が秘密情報の保管を行うには主管官庁※による施設クリアランス認定※が必要<br>※ 国により、施設クリアランス認定を行う主管官庁は異なる。<br>※ 国により、施設クリアランスに相当する制度の名称は異なる。 | | | |
| 物的保護要件 | ○ 建物構造の保全措置（例：外壁、扉、窓、警報装置 等）<br>○ 情報管理上の措置（例：不正アクセス防止措置 等）<br>○ その他 | | | |
| 組織的要件の例（外国による影響等（FOCI）） | ○ 施設クリアランス付与にあたり、対象事業者の経営陣(例：国籍等の人定事項)、出資元の外国資本等の保全上の影響を考慮※2<br>○ その上で、ＦＯＣＩの影響がある場合でも、一定の緩和措置を講じた上で施設クリアランスを付与する場合あり | ○ 施設クリアランス付与にあたり、対象事業者の経営陣(例：国籍等の人定事項)、出資元の外国資本等の保全上の影響を考慮<br>○ 取締役の少なくとも50%がイギリスに居住し、かつ、イギリス国籍であること | ○ 施設クリアランス付与にあたり、対象事業者の経営陣(例：国籍等の人定事項)、出資元の外国資本等の保全上の影響を考慮 | ○ 施設クリアランス付与にあたり、対象事業者の経営陣(例：国籍等の人定事項)、出資元の外国資本等の保全上の影響を考慮 |
| 要件を満たさなくなった場合の措置等 | ○ 施設クリアランスの抹消等 | | | |

※1 特に国防省との契約時の規定を掲載

※2 公開されている申告フォーム（SF328）に、発行済み株式の5%以上を外国人が保有しているか、外国企業の10%以上の持ち分を保有しているか、取締役会メンバー等に外国人がいるか等の質問項目あり。申告フォームに該当項目がある場合には、FOCI下にあるといえるか、FOCIのリスクが許容範囲内か、リスク低減措置が取られるか、という観点からリスク評価を実施

# 【参考】特定秘密保護法における適性評価

□ 特定秘密保護法における適性評価の手続やその内容は下記のとおり。

## ■手続

評価対象者への告知
評価対象者の同意
→ 調査 →
特定秘密の取扱の業務を行った場合にこれを漏らすおそれがないことについての評価（適性評価）
→ 評価対象者に結果を通知

（評価対象者による適性評価に関する苦情）

## ■調査

**【調査事項】**

① 特定有害活動及びテロリズムとの関係に関する事項
② 犯罪及び懲戒の経歴に関する事項
③ 情報の取扱いに係る非違の経歴に関する事項
④ 薬物の濫用及び影響に関する事項
⑤ 精神疾患に関する事項
⑥ 飲酒についての節度に関する事項
⑦ 信用状態その他の経済的な状況に関する事項

※①には、家族（配偶者・父母・子・兄弟姉妹、配偶者の父母及び子）及び同居人の氏名・生年月日・国籍・住所を含む

**【調査方法】** ※行政機関の長が実施

○本人による質問票の提出
○上司等の本人をよく知る者による調査票の提出
○（必要に応じ）旅券の写し等

↓ 疑問が生じた場合

○上司、同僚その他知人への質問
○人事管理情報による確認
○本人に対する面接

↓ 引き続き疑問が解消されない場合

○公務所・公私の団体への照会

## ■留意事項

①適性評価の実施について同意しなかったこと、②適性評価の結果、③適性評価の実施に当たって取得する個人情報、について、国家公務員法上の懲戒の事由等に該当する疑いがある場合を除き、特定秘密の保護の目的外での利用及び提供を禁止。

# 【参考】罰則

■ 情報の漏洩等に対する罰則を定めている主な法律は以下のとおり。

| | 行為 | 取扱にかかる法律での PCL/FCL規定の有無 | 罰則 |
|---|---|---|---|
| **不正競争防止法** | 現職の役員又は従業者が、図利加害目的で、営業秘密の管理に係る任務に背き、営業秘密を使用又は開示 | × | 10年以下／2,000万円以下 |
| **特定秘密保護法** | 特定秘密の取扱いの業務に従事する者が、その業務により知得した特定秘密を漏洩 | ○ | 10年以下／1,000万円以下 |
| **マイナンバー法** | 個人番号利用事務等に従事する者又は従事していた者が、正当な理由なく、特定個人情報ファイルを提供 | × | 4年以下／200万円以下 |
| | 個人番号利用事務等に従事する者又は従事していた者が、その業務に関して知り得た個人番号を自己若しくは第三者の不正な利益を図る目的で提供 | × | 3年以下／150万円以下 |
| **衛星リモセン法** | 衛星リモートセンシング記録保有者が、公益上の必要や非常事態への対応等により行う場合以外で、衛星リモートセンシング記録を提供 | × | 3年以下／100万円以下 |
| **貸金業法<br>割賦販売法** | 指定信用情報機関の役員若しくは職員又はこれらの職にあった者が、信用情報提供等業務に関して知り得た秘密を漏洩 | × | 2年以下／300万円以下 |
| **原子炉等規制法** | 原子力事業者等及びその従業者並びにこれらの者であった者が、正当な理由がなく、業務上知ることのできた特定核燃料物質の防護に関する秘密を漏洩 | △ | 1年以下／100万円以下 |
| **国家公務員法<br>自衛隊法** | 職員／隊員が、職務上知ることのできた秘密を漏洩 | × | 1年以下／50万円以下 |
| **防衛生産<br>基盤強化法** | 装備品等秘密の取扱いの業務に従事する従業者が、その業務に関して知り得た装備品等秘密を漏洩 | × | 1年以下／50万円以下 |