

# セキュリティクリアランス制度に対する要望

2023年3月14日

# 1. 基本的立場

## ■国の保有する防衛関連の機密情報（Classified Information：以下「CI」）の民間開示を拡大する制度見直し（セキュリティークリアランス制度：以下「SC制度」）を要望

- 現時点では日本政府との関係で、防衛関連の個別のプロジェクトごとにCIの開示を受けているが、この手続きは契約ごとに行わざるを得ない。
- また、契約ごとの対応となるので、長い目で見たSCホルダー育成という視点から見てもマイナス。
- 外国政府も参画した国際共同開発プロジェクトにおいて、相手国政府のCIへのアクセスを得ようとすると、さらに手続きが必要となり多大の時間を要している。
- デュアルユース品の共同開発過程では当社には限られた技術情報しか開示されず、プロジェクトに参加する全当事者にとって不便。

## ■防衛以外の官民の国際共同開発案件においても日本企業が円滑に当該プロジェクトに参加するにはSC制度が必要

- デュアルユース分野における国際会議・学会等ではSC保有者のみが参加する発表の場があるが、こうした場に参加できないなど、デュアルユース品の国際共同開発に支障が出る可能性を危惧。
- 防衛以外の分野におけるSC制度については先行各国の情報保全・SC制度運用を精査し、防衛以外の戦略分野に関するSC制度が具体化することを期待。

# 2. SC制度の効果として期待すること

## 米国の状況

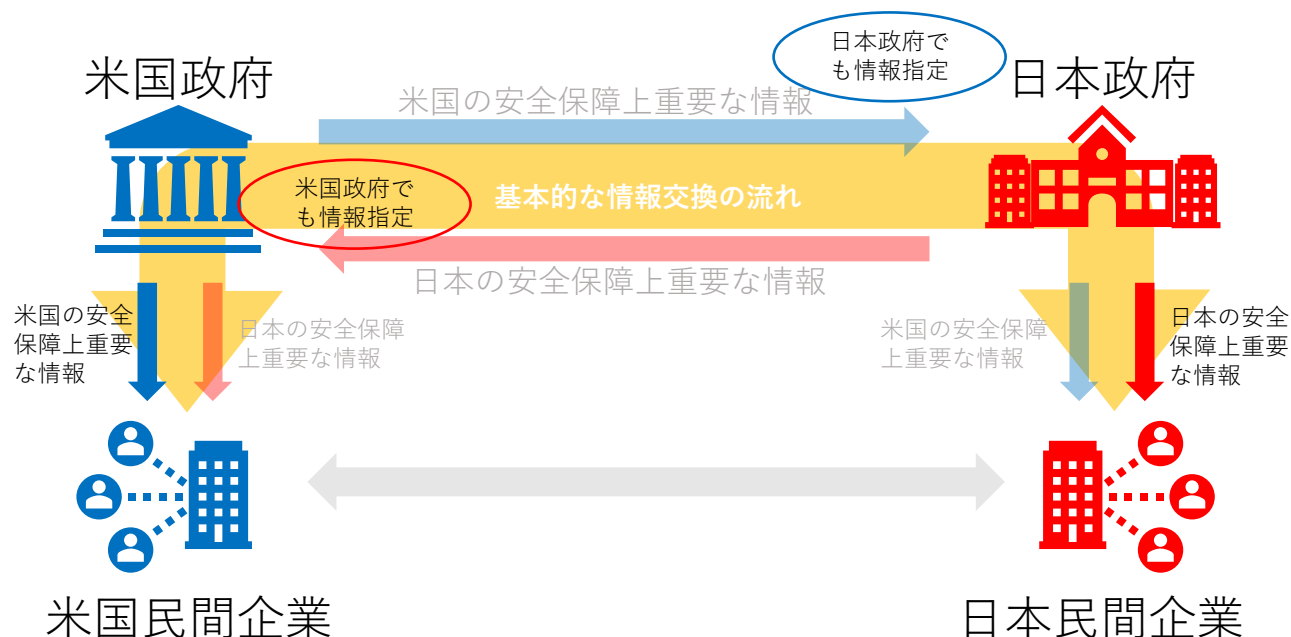
CIの範囲：8分野

- ①軍事 ②外国政府
- ③インテリジェンス④情報源
- ⑤安保関係科学技術/経済
- ⑥核関連 ⑦基幹インフラ
- ⑧大量破壊兵器

SCホルダー(\*)

- 政府：290万人 (68%)
- 民間：103万人 (24%)
- 不明：32万人 (7%)

\*：2019年10月1日時点



## 日本の現状

特定秘密の指定範囲：4分野のみ

- ①防衛 ②外交
- ③スパイ ④テロ

SCホルダー(※)

- 政府：13万人 (97%)
- 民間：3,444人 (3%)

※：3月9日読賣新聞より

で示す政府保有のCIに対する民間サイドの基本的なアクセスルートを構築する

高度な技術分野での官民国際共同開発においては、で示す通り、直接日米が専門的会話をできる運用環境の確立を望む

CIの範囲を、国の保有する安保関連科学技術/経済・基幹インフラにまで拡大すれば、官民共同の次世代技術・インフラ技術開発においても同様の効果が期待される。

# 3. 制度設計に当たっての要望

- SC付与の審査基準の明確化（人と施設に関する情報保全義務の内容明確化）
- SC対象となる人物のバックグラウンド調査は国が実施
- 政府の一元的窓口の設置（審査の一本化）
- 契約単位の適合事業者・従業者指定から、資格要件に基づいた有期の指定に変更
- SCの有効期間、失効要件、違反時の罰則の明確化
- 制度の周知徹底を通じた官民双方の「情報保全」能力の向上

## ■ SCの対象となる政府保有CIにとどまらない「情報保全関連制度の鳥瞰的な整理」

- 政府保有のCIのみならず企業が保有する情報の中には、外為法（みなし技術輸出規制などが典型例）や原子炉等規制法に基づき従業員の情報へのアクセスを規制する法令がある。
- また、企業が不正競争防止法に基づき保有する営業秘密の保護を図るためには、一定の情報管理が必要となる。
- SC制度、個別規制法、不正競争防止法などで要請される情報保全の方策に関して、関連する政府担当部署は複数あるが、企業の視点から見れば、特定情報に関する従業員のアクセス権の制限を労働法制上の要請との整合性を図りながら導入し、全情報の管理体系を確立する必要がある。
- 政府サイドの情報保全制度に関する考え方を明確に提示してもらいたい。

