2023 年 6 月 16 日

セキュリティ・クリアランスに関する議論の最新動向
ー中間論点整理の公表を踏まえてー

森・濱田松本法律事務所
弁護士　宮岡 邦生
TEL. 03 6266 8738
kunio.miyaoka@mhm-global.com

Ⅰ. はじめに

政府は、2023 年 6 月 6 日、日本における「セキュリティ・クリアランス」制度の整備に向けた有識者会議の中間論点整理を公表しました（内閣官房ウェブサイト、本文）。

セキュリティ・クリアランスとは、一般に、政府が保有する安全保障上重要な情報を秘密情報に指定した上で、情報にアクセスする必要がある者に対し、政府による信頼性調査を実施した上で、アクセス資格（クリアランス）を付与する制度をいいます。

米国をはじめとする主要国では既に本格的なセキュリティ・クリアランス制度が導入されているところ、日本にも関係する法制度は存在するものの、諸外国と比較すると限定的な手当てにとどまっていました。しかし、昨今の経済安全保障への意識の高まりや産業界の声を受け、改めて、主要国と平仄を合わせた本格的なセキュリティ・クリアランス制度の導入に向けた機運が高まっており、中間論点整理はそうした動きの一環と位置付けられます。

本ニュースレターでは、まずⅡ. で、セキュリティ・クリアランスとは何かについて、諸外国における制度の整備状況も含めて簡単に概観した後、Ⅲ. で日本における既存の情報保全制度である特定秘密保護法について復習した上で、Ⅳ. で有識者会議設置の経緯を含む議論の状況を、Ⅴ. で今回公表された中間論点整理のポイントをそれぞれ解説します。

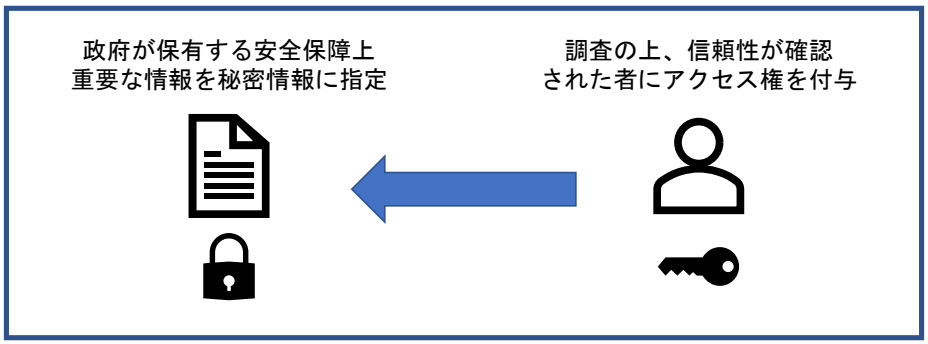
Ⅱ. セキュリティ・クリアランスとは何か

セキュリティ・クリアランスには必ずしも公式な定義や要件があるわけではありませんが、一般的には、国家における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秘密情報（Classified Information、「CI」と呼ばれます。）に指定した上で、

②情報にアクセスする必要がある者[1]に対し、調査を調査を実施した上でアクセス資格（クリアランス）を付与することを中核とする制度をいいます。

こうした情報保全制度は、米国のほか英国、ドイツ、フランス、カナダ、オーストラリアといった主要国で導入されており、クリアランス保有者の数は、米国の場合には民間人を含めて 400 万人以上、その他の主要国でも数十万人以上にのぼるとされます。

＜セキュリティ・クリアランス制度のイメージ＞



セキュリティ・クリアランス制度の対象となる秘密情報（CI、上記①）の種類・範囲は国によって異なりますが、典型的には、軍事、外交、国内治安、諜報（インテリジェンス）、科学技術、インフラの脆弱性にかかわる情報など、国家安全保障（ないしは経済安全保障）に影響を与えうる情報全般がカバーされます。CI は、さらに、その機微度に応じて、トップシークレット、シークレット、コンフィデンシャル（米国の場合）といった複数の段階に分類され、段階に応じて異なるアクセス資格が用意されることが一般的です。

＜秘密情報のイメージ（米国の場合[2]）＞

秘密情報への指定対象となる事項	秘密情報の機微度
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インテリジェンスに関する活動、情報源、方法又は暗号 ④米国の外交関係又は対外活動（秘密情報源を含む） ⑤国家安全保障に関連する科学的・技術的・経済的事項 ⑥核物質又は各施設の防護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、生産又は使用	**Top Secret** 不当な開示が国家安全保障に例外的に深刻な損害を与えると合理的に予想しうるもの **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うるもの **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うるもの

[1] 基本的には自然人が対象ですが、施設や法人を対象とする制度もあります。本レターでは、基本的に自然人を対象としたものにフォーカスします。
[2] 大統領令 13526 号（2009 年 12 月 29 日）「機密指定された国家安全保障情報（Classified National Security Information）」による。

資格付与の対象者（上記②）については、政府職員のほか、必要に応じて民間企業の従業員にも資格が与えられます。例えば米国の場合、官民の比率は 7：3 程度といわれています。資格付与の前提となる適性評価にあたっては、例えば以下のような事情について、総合的な調査・評価が行われます。

＜適性評価における考慮要素（米国の例[3]）＞

① 米国への忠誠心	⑧ 薬物等への依存・濫用
② 外国からの影響	⑨ 精神状態
③ 外国を好む傾向	⑩ 犯罪歴
④ 性行動	⑪ 保護された情報の取扱い
⑤ 個人的な行動	⑫ 本業以外の活動
⑥ 経済的な状況	⑬ 情報技術の利用
⑦ アルコール消費	

セキュリティ・クリアランス制度の下での CI の提供に際しては、対象者がアクセス資格（クリアランス）を有することに加え、当該情報を知る必要性（Need-to-Know）が要求されることが通常です。また、保全措置の対象となる CI を漏洩した者には厳しい刑事罰が科されます。

なお、セキュリティ・クリアランス制度の対象は原則として CI に限定されますが、諸外国では、政府保有情報のうち、CI に指定するほど機微ではないものの相応の厳格な管理が必要と考えられる情報や、民間事業者等が保有している情報のうち国として保全が必要が考えられる情報について、「CUI」（Controlled Unclassified Information）[4]といった名称の下で、セキュリティ・クリアランスよりも緩やかな保全措置が導入されている例もあります。

Ⅲ. 日本における既存の制度：特定秘密保護法

日本の情報保全制度としては、2013 年に成立した特定秘密の保護に関する法律（以下「特定秘密保護法」といいます。）が挙げられます。

この法律は、①安全保障に関する一定の情報であって公になっていない情報のうち、安全保障の観点から特に秘匿の必要があるものについて、行政機関の長（大臣等）が情報を「特定秘密」に指定した上で、②適性評価をクリアした者のみに取扱いを認めることを可能にするという仕組みを定めています。政府が保有する安全保障上重要な情報を機密情報に指定した上で、一定の基準を満たした者にのみアクセスを認めるという意味では、情報保全制度の一種と位置付けることができます。一方で、主要国におけるセキュリティ・クリアランス等の情報保全制度と比べると、（ア）特定秘密の指定対象となる

[3] Security Executive Agent Directive 4 – National Security Adjudicative Guidelines
[4] 大統領令 13556（2010 年 11 月 4 日）「管理された非機密情報（Controlled Unclassified Information）」も参照。例えば、米国では、米国立標準技術研究所（NIST）が策定した情報セキュリティ基準である SP800-171 が、CUI の保護に関するフレームワークを定めており、これを受けて我が国においても、防衛省が、SP800-171 と同水準の管理策を盛り込んだ防衛産業サイバーセキュリティ基準を 2022 年 3 月に整備しています。

事項が限定されている点、（イ）保全措置の対象が「特定秘密」という 1 類型のみで機微度に応じた段階が設けられておらず、主要国で CI に分類される情報のうち比較的機微度の高い情報[5]のみを対象としている点などが異なっています。

1. 特定秘密への指定対象となる事項

特定秘密保護法に基づく秘密指定の対象となる事項（上記①）は、法律の別表で以下の 4 類型に分けて指定されています。行政機関の長は、これらの事項に関する情報であって公になっていないもののうち、その漏えいが我が国の安全保障に著しい支障を与えるおそれがあるため、特に秘匿することが必要であるものを特定秘密に指定することができます（3 条）。

＜特定秘密への指定対象となる事項＞

第 1 号（防衛に関する事項）	第 2 号（外交に関する事項）
イ 自衛隊の運用又はこれに関する見積もり若しくは計画若しくは研究 ロ 防衛に関し収集した電波情報、画像情報その他の重要な情報 ハ ロに掲げる情報の収集整理又はその能力 ニ 防衛力の整備に関する見積もり若しくは計画又は研究 ホ 武器、弾薬、航空機その他の防衛の用に供する物の種類又は数量 ヘ 防衛の用に供する通信網の構成又は通信の方法 ト 防衛の用に供する暗号 チ 武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの仕様、性能又は使用方法 リ 武器、弾薬、航空機その他の防衛の用に供する物又はこれらの物の研究開発段階のものの製作、検査、修理又は試験の方法 ヌ 防衛の用に供する施設の設計、性能又は内部の用途	イ 外国の政府又は国際機関との交渉又は協力の方針又は内容のうち、国民の生命及び身体の保護、領域の保全その他の安全保障に関する重要なもの ロ 安全保障のために我が国が実施する貨物の輸出若しくは輸入の禁止その他の措置又はその方針 ハ 安全保障に関し収集した国民の生命及び身体の保護、領域の保全若しくは国際社会の平和と安全に関する重要な情報又は条約その他の国際約束に基づき保護することが必要な情報 ニ ハに掲げる情報の収集整理又はその能力 ホ 外務省本省と在外公館との間の通信その他の外交の用に供する暗号
第 3 号（特定有害活動の防止に関する事項）	**第 4 号（テロリズムの防止に関する事項）**
イ 特定有害活動の防止のための措置又はこれに関する計画若しくは研究 ロ 特定有害活動の防止に関し収集した国民の生命及び身体の保護に関する重要な情報又は外国の政府若しくは国際機関からの情報 ハ ロに掲げる情報の収集整理又はその能力 ニ 特定有害活動の防止の用に供する暗号	イ テロリズムの防止のための措置又はこれに関する計画若しくは研究 ロ テロリズムの防止に関し収集した国民の生命及び身体の保護に関する重要な情報又は外国の政府若しくは国際機関からの情報 ハ ロに掲げる情報の収集整理又はその能力 ニ テロリズムの防止の用に供する暗号

特定秘密の有効期間は上限 5 年で、更新が可能です。指定の有効期間は通算 30 年を超えることができないとされていますが、我が国及び国民の安全を確保するためにやむを得ない理由を示して内閣の承認を得た場合に限り、通算 30 年を超えて延長することができます。ただし、この場合であっても、暗号や人的情報源等を除き、通算 60 年を超えて延長することはできないとされています（4 条）。

[5] 「特定秘密」は、概ね米国における Top Secret と Secret の機微度に対応するといわれています（例えば、2023 年 4 月 25 日開催の第 5 回有識者会議議事要旨参照）。

2. 特定秘密の取扱いの業務を行うことができる者

特定秘密を取り扱える者（上記②）は、次の者に限られます（11、12、15 条）。

- 特定秘密の取扱いの業務を行うことが見込まれる行政機関の職員若しくは適合事業者の従業者又は都道府県警察の職員のうち、
- 行政機関の長（都道府県警察の職員の場合は、警察本部長）が行う適性評価を通じて特定秘密を漏らすおそれがないと認められた者

適性評価の調査事項は以下の項目とされています（12 条 2 項 1～7 号）。

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

適性評価のための調査は、（ア）評価対象者本人への質問や面接、（イ）上司・同僚等への質問や人事管理情報による確認、（ウ）公務所又は公私の団体への照会などの方法により行われます（12 条 4 項、運用基準[6]）。調査の実施にあたっては、プライバシー等の観点から、評価対象者の事前同意が必要とされており、また、評価のために取得した個人情報等の目的外利用の禁止が定められています（16 条）。適性評価の結果は本人に通知されます（13 条）。

3. 特定秘密の提供

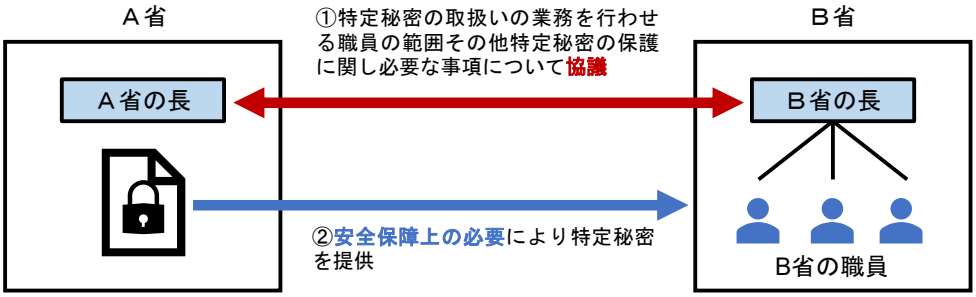
特定秘密を保有する行政機関の長は、一定の要件の下で、①他の行政機関や②一定の要件を満たした民間事業者（適合事業者[7]）に対し、特定秘密の提供を行うことができます。

①については、特定秘密を保有する行政機関（A 省）の長は、他の行政機関（B 省）が我が国の安全保障に関する事務のうち法律の別表に掲げる事項に係るものを遂行するために必要があると認められるときに、他の行政機関に対して特定秘密を提供することができるとされています（6 条）。特定秘密の取扱いの業務を行わせる職員の範囲その他の特定秘密の保護に関し必要な事項については、あらかじめ、関係する行政機関の長の間で協議が行われます。提供先の行政機関（B 省）の長は、協議に従い、特定秘密の適切な保護のために必要な措置を講じた上で、職員に当該特定秘密の取扱

[6] 特定秘密の指定及びその解除並びに適性評価の実施に関し統一的な運用を図るための基準
[7] 物件の製造又は役務の提供を業とする者で、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その他政令で定める基準に適合するものをいいます（5 条 4 項）。

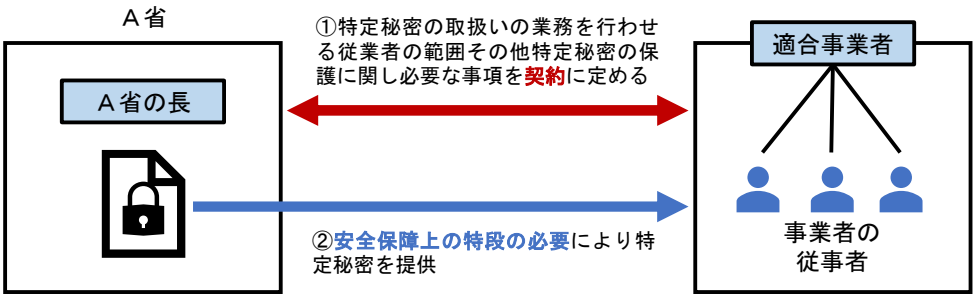
いの業務を行わせることとなります。

＜他の行政機関への特定秘密の提供＞



②については、特定秘密を保有する行政機関の長は、その所掌事務のうち法律の別表に掲げる事項に係るものを遂行するために、適合事業者に特定秘密を利用させる特段の必要があると認めたときには、特定秘密の提供を行うことができるとされています（8 条）。特定秘密を取り扱う従業員の範囲等については、行政機関と適合事業者の間の契約によって定められます。

＜適合事業者への特定秘密の提供＞



上記のほかに行政機関が保有する特定秘密の外部への提供が行われる場合として、例えば、行政機関の長は、安全保障上の必要が認められるときは、外国の政府又は国際機関に対し、特定秘密保護法に基づく措置に相当する情報保全措置が講じられていることを要件として、特定秘密を提供することができることとされています（9 条）。

4. 罰則

特定秘密を漏洩した者に対しては厳しい罰則が規定されています。

例えば、特定秘密を取り扱うことを業務とする者による情報漏洩については、故意の場合には 10 年以下の懲役（又は情状により 10 年以下の懲役及び 1,000 万円以下の罰金）に、過失の場合には 2 年以下の禁錮又は 50 万円以下の罰金に処されます（23 条）。

Ⅳ. 新たな制度の導入に向けた議論の状況と有識者会議の設置

1. 経済安全保障分野も含めた情報保全のあり方に関する議論

以上のように、特定秘密保護法は、情報保全制度の一種である一方で、秘密指定の範囲が防衛、外交、特定有害活動の防止、テロリズム防止の 4 分野のみとされていること、秘密情報の段階が比較的機微度の高い 1 段階のみに限定されていることなど、主要国の制度と比較すると限定的なものにとどまっています。

実際の運用を見ても、これまでに特定秘密に指定された情報は「防衛に関する事項」（別表第 1 号）に集中しており[8]、特定秘密の指定を行う官庁についても、防衛省、内閣官房、警察庁、外務省などが大半で、経済関係官庁による指定はほとんどありません[9]。また、日本で特定秘密の取扱いの業務を行うことができる者は約 13 万人いるものの、その比率は官が 97%、民が 3%で[10]、米国などと比較すると、民間の資格者が少ない状況です。

こうした中、近年のいわゆる「経済安全保障」[11]への関心の高まりも背景として、先端技術分野における優位性確保なども視野に、日本でも、主要国並みのセキュリティ・クリアランス制度を整備し、情報保全を一層強化する必要性が指摘されるようになりました。2022 年 5 月に成立した経済安全保障推進法では、セキュリティ・クリアランスに関する制度の導入自体は見送られましたが、衆議院及び参議院各内閣委員会における附帯決議で、「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」ことが明記されました[12]。さらに、2022 年 12 月に閣議決定された国家安全保障戦略でも、「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」方針が示されています。

---

[8] 内閣府が公表している各行政機関における特定秘密の指定状況の一覧表（令和 4 年 12 月末現在）によれば、行政機関全体で指定されている特定秘密の件数は 702 件あり、そのうち 420 件（60%）が防衛に関する事項で、399 件（57%）が防衛省による指定となっています。

[9] 上記一覧表によれば、令和 4 年 12 月末現在で特定秘密に指定されている 702 件のうち総務省による指定が 11 件、財務省が 0 件、経済産業省が 4 件となっています。

[10] 「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」（2022 年 6 月 7 日）によれば、2021 年年末時点で、官が 130,853 人（うち防衛省が 122,282 人）、民が 3,444 人となっています。

[11] 経済安全保障という用語については、必ずしも国際的な定義が確立されているわけではありませんが、2022 年 12 月 16 日に閣議決定された日本の国家安全保障戦略では、「我が国の平和と安全や経済的な繁栄等の国益を経済上の措置を講じ確保すること」と定義されています。また、経済安全保障推進法 2 条に基づいて策定された「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基本的な方針」（2022 年 9 月 30 日閣議決定）では、経済安全保障の要素として、「自律性の確保」、「優位性ひいては不可欠性の獲得・維持・強化」、「国際秩序の維持・強化」の 3 つが挙げられています。

[12] 2022 年 6 月 7 日に閣議決定された「経済財政運営と改革の基本方針 2022」（骨太方針 2022）にも同様の方針が盛り込まれています。

2. 有識者会議の設置

このような動きを踏まえ、2023 年 2 月 14 日に開催された第 4 回経済安全保障推進会議で、岸田総理大臣から、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て、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 年程度を目途に、可能な限り速やかに検討作業を進めるようにとの指示がなされました。これを受けて、2023 年 2 月 21 日付で、経済安全保障担当大臣の下に「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」が設置されました。

有識者会議は、経済団体、学会、法律家などから選ばれた 12 名のメンバーから成り、2023 年 2 月 22 日以降、同年 5 月 29 日までに合計 6 回の会議が開催されています。

今般公表された中間論点整理は、これらの会議における議論を踏まえ、2023 年 6 月 6 日に公表されたものです。

Ⅴ. 中間論点整理のポイント

中間論点整理は本文 8 頁の簡潔な内容ですが、①セキュリティ・クリアランス制度に関する必要性、②新たな制度の方向性、③具体的な方向性、④その他――について、制度の導入に向けた論点や課題が箇条書き的に列挙されています。

以下、簡単に内容を紹介（要約）します。

1. セキュリティ・クリアランス制度に関する必要性

（1）国としてのセキュリティ・クリアランス制度の必要性

- 安全保障の概念が経済・技術の分野にも大きく拡大し、軍事技術・非軍事技術の境目も曖昧となる中、経済安全保障分野において、我が国の情報保全の更なる強化を図る必要がある。
- 特定秘密保護法では、政府が特定秘密に指定できる情報が防衛、外交、特定有害活動、テロの 4 分野に限定されているところ、経済安全保障上重要な情報について、経済関係省庁や、防衛産業を超えた民間における情報保全強化が必要。
- 情報保全の強化は、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協力を推進し、ひいては、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。

（2）企業からのニーズ

- 企業からは、同盟国等の政府調達等において相手から十分な情報が得られない、情報開示に時間がかかる、政府主催か否かを問わず特定の会議に参加できない

といった困難がある。国際的に通用する制度や国際的な枠組みがあれば、状況が変わったのではないかとの声。

- 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。このような制度においては、情報保全全般が主要国との間でも認められるものでなくてはならない。

2. 新たな制度の方向性

（1）基本的な考え方

- 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 について、アクセスする必要がある者に対して、政府による信頼性確認を行った上でアクセスを認めるという制度である。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あり方を検討していく上でも、情報保全の主たる対象は CI であることが前提になる。
- 政府から民間事業者等に CI が共有される場合には、民間事業者等の従業者及び情報保全体制（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）同盟国・同志国との連携

- 新たに設けられる制度は、米国のほか、欧州等の主要な同志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、そこを目指すことが重要。
- これら同志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、これらの国の制度を踏まえて検討を進めるとともに、同志国との間の国際的な枠組みについても検討を進めていくべき。

（3）政府横断的・分野横断的な制度の検討

- 新しい制度の検討にあたっては、特定秘密保護法をはじめとする既存の情報保全制度や、情報公開法、公文書管理法等の他法令との整合性に留意する。

3. 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の指定は、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ことが基本。
- 特定秘密保護法の 4 分野と同様又はそれに準ずるものとして、例えば、経済制裁に関する分析関連情報、経済安全保障上の規制制度の審査関連情報、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などを念頭に、厳格に管理すべき経済安全保障上の情報の範囲について検討を深める。

- 国際的には情報の機微度に応じて複層的に管理がなされている点に留意し、現在の特定秘密における単層構造から複層構造化について検討する。

（2）信頼性の確認（評価）とそのための調査

- 特定秘密保護法の下で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が、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。
- 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。
- 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、調査については、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）が確保されるよう政府全体で統一的な対応を行っていくことを検討する。

（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ところ、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や従業者であって、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。
- この点について、例えば米国における国家産業保全計画（NISP: National Industrial Security Program）及びその運用マニュアル（NISPOM: National Industrial Security Program Operating Manual）なども参考にしながら検討を深める。

（4）プライバシー等との関係

- 新しい制度の下での信頼性の確認のための調査は、CI へのアクセスを必要とする者の任意の了解の下で行われることが大前提になり、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も必須。
- 制度の検討にあたっては、信頼性の確認を受ける対象者が広がり得ることや、企業で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、プライバシーと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について整理する。

（5）情報保全を適切に実施するための官民の体制整備

- 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、情報保全を適切に実施するため必要な体制整備や、適切な情報保全のための専用の区画や施設を設けるといった対応を行う必要がある。
- 民間事業者等にとっては少なからぬ負担となるため、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。

4. その他

（1）CI 以外の重要な情報の取扱い

- セキュリティ・クリアランス制度の主たる対象は CI であるが、それ以外にも、CI に指定するほどの機微度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について、一定の保全措置を講ずる必要性について検討を進める必要がある。
- 民間事業者等が保有している情報について、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ところ、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が必要。
- 公文書管理に係る諸制度、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、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検討していく必要。

（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と認識されているとの声もある。処遇面も含め、信頼性の確認に係る理解の醸成に努めることが重要。

Ⅵ. まとめ

中間論点整理は、あくまで有識者会議の議論を踏まえ、今後議論を深めるべき論点を列挙したものであり、今後、セキュリティ・クリアランスについて具体的にどのような法整備が行われるのかは必ずしも明らかではなく、今後の議論の進展を待つ必要があります。

もっとも、中間論点整理で示唆された考え方を総合すると、今後の法整備のあり方としては、①特定秘密保護法が対象とする防衛・外交といった分野だけでなく、非軍事部

門・先端技術分野などを含む経済安全保障上重要な情報を保全するための制度とすること、②米国をはじめとする主要国との連携も視野に、これら主要国のセキュリティ・クリアランス制度と平仄を合わせた制度とすること、③法整備の対象は政府が保有する CI とすること（ただし、CUI など CI 以外の重要な情報についても、一定の保全措置が必要かどうかを検討）が構想されているように見受けられます。

セミナー情報

- セミナー　『「ビジネスと人権」分野別連続ウェビナー（全 10 回シリーズ）第 1 回「人権×危機管理」』
  - 視聴期間　2023 年 4 月 12 日（水）～2023 年 10 月 31 日（火）配信
  - 講師　梅津 英明、御代田 有恒、上田 優介、仲谷 佳奈子
  - 主催　森・濱田松本法律事務所

- セミナー　『「ビジネスと人権」分野別連続ウェビナー（全 10 回シリーズ）第 2 回「人権×独禁法：公正取引委員会グリーンガイドラインからの示唆」』
  - 視聴期間　2023 年 5 月 11 日（木）～2023 年 10 月 31 日（火）配信
  - 講師　高宮 雄介、田中 亜樹、筑井 翔太、木村 信太郎
  - 主催　森・濱田松本法律事務所

- セミナー　『「ビジネスと人権」分野別連続ウェビナー（全 10 回シリーズ）第 3 回「人権×不動産」』
  - 視聴期間　2023 年 5 月 26 日（金）～2023 年 10 月 31 日（火）配信
  - 講師　田中 亜樹、白井 俊太郎、上田 優介
  - 主催　森・濱田松本法律事務所

- セミナー　『ブロックチェーンゲームの法的論点』
  - 開催日時　2023 年 6 月 20 日（火）14:00～14:30
  - 講師　増田 雅史
  - 主催　KPMG／あずさ監査法人

- セミナー　『FP が知っておくべき Web3・NFT・メタバース』
  - 開催日時　2023 年 6 月 23 日（金）19:00～20:00
  - 講師　増田 雅史
  - 主催　ファイナンシャル・プランナー三田会

- セミナー　『web3 国家戦略の現在と未来～「web3 ホワイトペーパー」ドラフトメンバーを迎えて』
  - 開催日時　2023 年 6 月 29 日（木）17:00～18:00
  - 講師　増田 雅史
  - 主催　IVS KYOTO 実行委員会

- セミナー　『【オンライン／会場】実務担当者のための日本・グローバルの個人情報保護規制入門講座』
  - 開催日時　2023 年 6 月 30 日（金）14:00～17:00
  - 講師　田中 浩之
  - 主催　一般社団法人企業研究会

- セミナー　『ChatGPT を含む生成系（ジェネレーティブ）AI 活用の法務実務～利用態様を踏まえた整理～』
  - 開催日時　2023 年 7 月 3 日（月）10:00～12:00
  - 講師　田中 浩之
  - 主催　株式会社金融財務研究会

- セミナー　『コンテンツビジネス法務の視点からみる AI、メタバース、web3』
  - 開催日時　2023 年 7 月 6 日（木）15:00～16:40
  - 講師　増田 雅史
  - 主催　一般社団法人 キャラクターブランド、ライセンス協会、一般社団法人 CiP 協議会、一般社団法人 日本オンラインゲーム協会、一般社団法人 日本動画協会

- セミナー　『第 5173 回金融ファクシミリ新聞社セミナー「安全保障貿易管理の基本と実務の最新動向～外為法・米国 EAR の基礎から最先端の動きまで体系的に解説～」』
  - 開催日時　2023 年 7 月 7 日（金）9:30～11:30
  - 講師　宮岡 邦生
  - 主催　株式会社 FN コミュニケーションズ

- セミナー　『Web3・NFT・メタバースの法律実務と政策動向～『NFT の教科書』『NFT ホワイトペーパー』で著名な第一人者による解説～』
  - 開催日時　2023 年 7 月 18 日（火）13:30～15:30
  - 講師　増田 雅史
  - 主催　JPI（日本計画研究所）

- セミナー　『企業における ChatGPT を含む生成系（ジェネレーティブ）AI 活用の法務実務』
  開催日時　2023 年 7 月 26 日（水）14:00～16:00
  講師　田中 浩之
  主催　一般社団法人企業研究会

- セミナー　『インターネットビジネスの法律関係総論 アプリビジネスを例として』
  開催日時　2023 年 7 月 31 日（月）18:20～19:35
  講師　増田 雅史
  主催　筑波大学大学院 人文社会ビジネス科学学術院 ビジネス科学研究群

- セミナー　『第二東京弁護士会研修「インバウンド実務入門（外為法編）」』
  開催日時　2023 年 7 月 31 日（月）18:00～20:00
  講師　大川 信太郎
  主催　第二東京弁護士会 国際委員会

- セミナー　『第 5175 回金融ファクシミリ新聞社セミナー「ランサムウェアの脅威と被害時の対応に関する法律実務」』
  開催日時　2023 年 8 月 2 日（水）13:30～15:30
  講師　蔦 大輔
  主催　株式会社 FN コミュニケーションズ

- セミナー　『第 5181 回金融ファクシミリ新聞社セミナー「ChatGPT 等の「Generative AI」を金融機関が活用する際の法律留意点～大規模言語モデル・画像生成 AI 等、有効活用のポイント～」』
  開催日時　2023 年 8 月 10 日（木）13:30～15:30
  講師　田中 浩之
  主催　株式会社 FN コミュニケーションズ

- セミナー　『Web3・NFT・メタバース』
  開催日時　2023 年 9 月 11 日（月）19:45～21:00
  講師　増田 雅史
  主催　筑波大学大学院 人文社会ビジネス科学学術院 ビジネス科学研究群

文献情報

- 論文　「外為法に基づく半導体製造装置等に関する輸出管理の強化と実務上の対応」
  掲載誌　NBL No.1241
  著者　大川 信太郎、瀧山 侑莉花

- 論文　「Japan - Cookies & Similar Technologies」
  掲載誌　OneTrust DataGuidance 2023 年度版
  著者　岡田 淳

- 論文　「私法上の法律関係に即した課税論から国税庁「NFT に関する税務上の取扱いについて」を読み解く」
  掲載誌　NBL No.1242
  著者　大石 篤史、増田 雅史、原田 昂、間所 光洋（共著）

- 論文　「The Financial Technology Law Review Sixth Edition - Japan Chapter」
  掲載誌　The Financial Technology Law Review Sixth Edition
  著者　岡田 淳、堀 天子、飯島 隆博（共著）

- 論文　「企業法務最前線〈第 255 回〉メタバースについて」
  掲載誌　月刊監査役 749 号
  著者　増田 雅史

- 本　『ChatGPT の法律』（2023 年 6 月刊）
  出版社　株式会社中央経済社
  著者　田中 浩之（共著）

- 論文　「「対話で学ぶ」「知らなきゃ困る」グローバル個人情報保護規制（4）各国の個人情報保護規制の概要②（中国）」
  掲載誌　会社法務 A2Z 2023 年 2 月号
  著者　田中 浩之、蔦 大輔、北山 昇、塩崎 耕平

- 論文　「2023 Global Legislative Predictions」
  掲載誌　International Association of Privacy Professionals
  著者　田中 浩之（共著）

NEWS

➢ 札幌オフィス開設のお知らせ

今般、当事務所は、札幌オフィスを開設することといたしましたので、お知らせいたします。

当事務所は、現在、北海道の案件につきましても、東京をはじめとする国内各拠点においてリーガル・サポートを提供しておりますが、企業法務を中心とした分野において、より近接した拠点からのサポートを期待するとの声をいただいておりました。当事務所は、このようなご要望・ご期待にお応えして、きめ細やかなサポートを行うべく、今般、北海道札幌市に新たな拠点を設けることといたしました。

札幌オフィスには、M&A、会社法関連業務、スタートアップ等において豊富な経験を有するパートナーである立石 光宏 弁護士及びアソシエイト弁護士が所属いたします。

札幌オフィスは、他の国内拠点（東京、大阪、名古屋、福岡及び高松）及び海外拠点（北京・上海・シンガポール・バンコク・ヤンゴン・ホーチミン・ハノイ・ジャカルタオフィス及び2023年秋の業務開始を予定しておりますニューヨークオフィス）、並びにその他の国の提携法律事務所等と密に連携をとりながら、M&A・スタートアップ・事業承継・危機管理・ファイナンス・訴訟・事業再生・クロスボーダー取引をはじめとする幅広い分野において最先端のリーガル・サポートを提供し、北海道の経済発展に微力ながら寄与して参る所存です。

札幌オフィスの開設については、開設に必要となる諸手続を経た上、2023 年 9 月又は 10 月のスタートを目指しております。開設日・開設場所等の詳細が決まりましたら、改めてお知らせいたします。

※札幌オフィスは、弁護士法人森・濱田松本法律事務所の従事務所として開設する予定です。

➢ Benchmark Litigation Asia-Pacific 2023 において高い評価を得ました

Benchmark Litigation Asia-Pacific 2023 年版において、当事務所及び当事務所のバンコクオフィス（Chandler MHM Limited）が全ての分野において高い評価を受けました。さらに当事務所の 4 名の弁護士が高い評価を受けております。

詳細は Benchmark Litigation のウェブサイトに掲載されております。

分野

・JAPAN
- Commercial and transactions
- Intellectual property
- International arbitration
- White collar crime

・THAILAND
- Commercial and transactions
- Intellectual property
- Trade and customs
- Government and regulatory
- Labor and employment

弁護士

・JAPAN
- Commercial and transactions
  Litigation Star：関戸 麦
- Intellectual property
  Litigation Star：三好 豊
- White collar crime
  Future Star：山内 洋嗣

・THAILAND
- Commercial and transactions
  Litigation Star：ナティー・シーラチャルァン

➢ Benchmark Litigation Asia-Pacific Awards 2023 にて受賞しました

Benchmark Litigation Asia-Pacific Awards 2023 の JURISDICTIONAL AWARDS において、当事務所は JAPAN FIRM OF THE YEAR を受賞しました。
詳細は Benchmark Litigation のウェブサイトに掲載されております。

➢ ALB Japan Law Awards 2023 にて受賞しました

トムソン・ロイターグループの国際的法律雑誌である ALB（Asian Legal Business）による ALB Japan Law Awards 2023 において、当事務所は以下のカテゴリーにて受賞しました。

LAW FIRM CATEGORIES

・Japan Law Firm of the Year
・Japan Deal Firm of the Year

・Banking and Financial Services Law Firm of the Year
・Capital Markets Law Firm of the Year
・Investment Fund Law Firm of the Year
・Regulatory and Compliance Law Firm of the Year
・Restructuring and Insolvency Law Firm of the Year
・Technology, Media and Telecommunications Law Firm of the Year

DEAL CATEGORIES

・Debt Market Deal of the Year
- Bain Capital's Tender Offer for Hitachi Metals
・Equity Market Deal of the Year
- SBI Sumishin Net Bank's Global IPO

・M&A Deal of the Year (Premium)
- KKR Acquisition of Mitsubishi Corp UBS Realty
・Technology, Media and Telecommunications Deal of the Year
- Hitachi Disposition of Hitachi Metals

詳細は、ALB ウェブサイトのリンクをご覧下さい。

（当事務所に関するお問い合せ）
森・濱田松本法律事務所　広報担当
mhm_info@mhm-global.com
03-6212-8330
www.mhmjapan.com