営業秘密保護推進研究会（APPTraS）
第21回連続オープンセミナー：サプライチェーンセキュリティと経済安全保障
Part 2「経済安全保障制度への対応とグローバルサプライチェーンの保護」

セキュリティクリアランス制度に対応するための企業実務の解説

2025年12月22日

森・濱田松本法律事務所 外国法共同事業 弁護士
慶應義塾大学大学院 政策・メディア研究科 特任准教授（非常勤）
蔦　大輔

MORI HAMADA

Lawyer Profile

パートナー

蔦　大輔

Daisuke Tsuta

東京弁護士会所属

慶應義塾大学大学院政策・メディア研究科 特任准教授

一般社団法人日本シーサート協議会（NCA）専門委員

サイバーセキュリティ法制学会理事

Direct 03-6266-8769
Mail daisuke.tsuta@morihamada.com

MORI HAMADA

主要取扱分野

サイバーセキュリティ、個人情報保護、IT・ICT

- サイバー攻撃の予防、攻撃を受けた後の対応に関する助言、サポート、従業員による内部不正対応
- 個人情報保護・データ利活用、オンラインサービスのサポート
- サイバーセキュリティに深く関わる経済安全保障分野においても各種サポートを行う（クリアランス・インフラ防護など）
- 年間の講演実施数（セミナー、社内研修込み）40～50

著作・論文

- 『クロスセクター・サイバーセキュリティ法』（2025年、編著）
- 「サイバーセキュリティ法の羅針盤」（有斐閣Online連載、2025年～）
- 『企業情報管理実務マニュアル［第2版］』（2025年、共著）
- 『明日話したくなる個人情報のはなし』（2025年、共著）
- 『類型別　不正・不祥事への初動対応』（2024年、共著）
- 『情報刑法I　サイバーセキュリティ関連犯罪』（2022年、共著）
- 『60分でわかる！改正個人情報保護法超入門』（2022年、共著）
- 『事例に学ぶサイバーセキュリティ』（2020年、共著）

その他、著書・論文・講演多数

経歴

京都大学法学部卒業、神戸大学法科大学院修了

財務省近畿財務局、総務省行政管理局、内閣官房内閣サイバーセキュリティセンター（NISC・現国家サイバー統括室）にて任期付公務員として執務（2014年～2020年）

主な活動

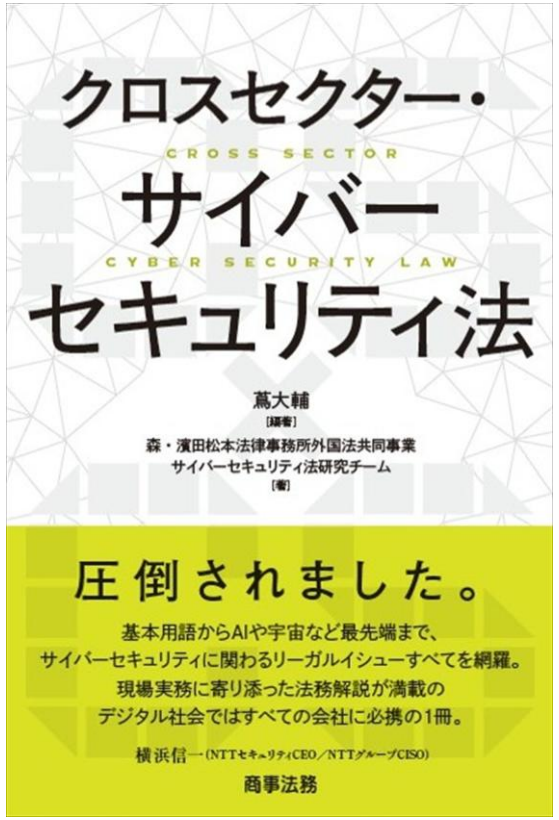
2016年 情報ネットワーク法学会理事（～2020年）
2022年 サイバーセキュリティ協議会 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会 委員
2022年 警察庁 サイバー被害の潜在化防止に向けた検討会 委員
2023年 経済産業省 サイバー攻撃による被害に関する情報共有の促進に向けた検討会 委員
2023年 サイバーセキュリティ法制学会理事
2023年 警察庁 キャッシュレス社会の安全・安心の確保に関する検討会　委員
2024年 総務省サイバーセキュリティタスクフォース ICTサイバーセキュリティ政策分科会 構成員
2024年 総務省 ICTサービスの利用環境の整備に関する研究会利用者情報に関するワーキンググループ オブザーバー
2025年 日本弁護士連合会 情報セキュリティワーキンググループ 委員

受賞歴等

令和6年度 サイバーセキュリティに関する総務大臣奨励賞受賞
The Legal 500 Asia Pacific 2025のTMT部門　Next Generation Partners
The Best Lawyers in Japan（2026 edition）Information Technology Law

【PR】2025年10月20日発売:「クロスセクター・サイバーセキュリティ法」

- 多様な専門分野を有するMori Hamadaの弁護士の叡智を結集(著者総勢60名超)
- サイバーセキュリティと様々な法分野をクロスさせて実務上の論点を解説



法律(総論)	会社法	ディスクロージャー	個人情報保護	知的財産・営業秘密	競争法・独禁法
労働法	システム開発	弁護士実務	刑事法	危機管理	M&A
外為法	セキュリティ・クリアランス	インフラ・サイバー安全保障	金融規制全般	保険法・サイバー保険	エネルギーインフラ(電気)
通信インフラ	データセンター	医療・医療機器	モビリティ	航空・船舶	クラウド
IoT	EC・クレジット	防災	AI	メタバース	宇宙
Fintech	DFFT	アジア法	中国法	EU法	アメリカ法
イスラエル法					

アジェンダ

1. セキュリティ・クリアランスとは

2. 重要経済安保情報保護活用法の概説

3. 他の経済安全保障関連法令とクリアランスの活用可能性

セキュリティ・クリアランスとは

1

MORI HAMADA

セキュリティ・クリアランスとは

- **セキュリティ・クリアランス制度**：国家における情報保全措置
  - 安全保障上重要な情報（**Classified Information／CI**）を指定
  - 情報にアクセスする必要がある者に対して**政府による調査を実施、信頼性を確認**してアクセスを認める
  - 情報管理ルールを定め、**漏えい時には厳しい罰則**

- **CIの機微度による分類**：概ね3段階に分類
  - ① トップ・シークレット（Top Secret）
  - ② シークレット（Secret）
  - ③ コンフィデンシャル（Confidential）
  - ※CIに至らない機微度だが一定の保全措置が必要な情報（Controlled Unclassified Information／CUI）は、制度の対象外

日本におけるセキュリティ・クリアランス制度

■ 特定秘密保護法

- ➢ 防衛、外交、特定有害活動の防止、テロリズムの防止の4分野に限定
- ➢ 対象は基本的に公務員

■ 経済安全保障版セキュリティ・クリアランス

- ➢ 上記4分野に限らず、**経済安全保障上重要な情報**の保全の必要性
- ➢ 加えて、企業からのニーズ
  - ✓ 海外政府からCIの共有を受ける必要があるプロジェクトに参加できない（**諸外国に通用する制度**の必要性）
  - ✓ 海外ビジネス・国際共同開発においても、セキュリティ・クリアランス保有者がいないために海外企業からCUIの共有を受ける際に制約がある（「**信頼できる証**」としての事実上の効用）
  - ✓ 政府・諸外国が保有しているインシデント情報に民間事業者がアクセスできれば、**サイバーセキュリティの向上**につながる

重要経済安保情報保護活用法の概説

2

重要経済安保情報保護活用法（重要経済安保情報の保護及び活用に関する法律）

2024年5月17日公布（令和6年法律第27号）、2025年5月16日施行

■ 情報の保全指定

➢ 行政機関の長が3つの要件を満たす情報を**重要経済安保情報**と**指定**

①重要経済基盤保護情報該当性　②非公知性　③秘匿の必要性

- ✓ **サイバー関連情報**：サイバー脅威・対策等に関する情報
- ✓ **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

■ 適合事業者への提供（FCL）

- **適合事業者**との秘密保持契約に基づき重要経済安保情報を提供可
- 適合事業者の基準は政令で定める（**Facility Security Clearance／FCL**）

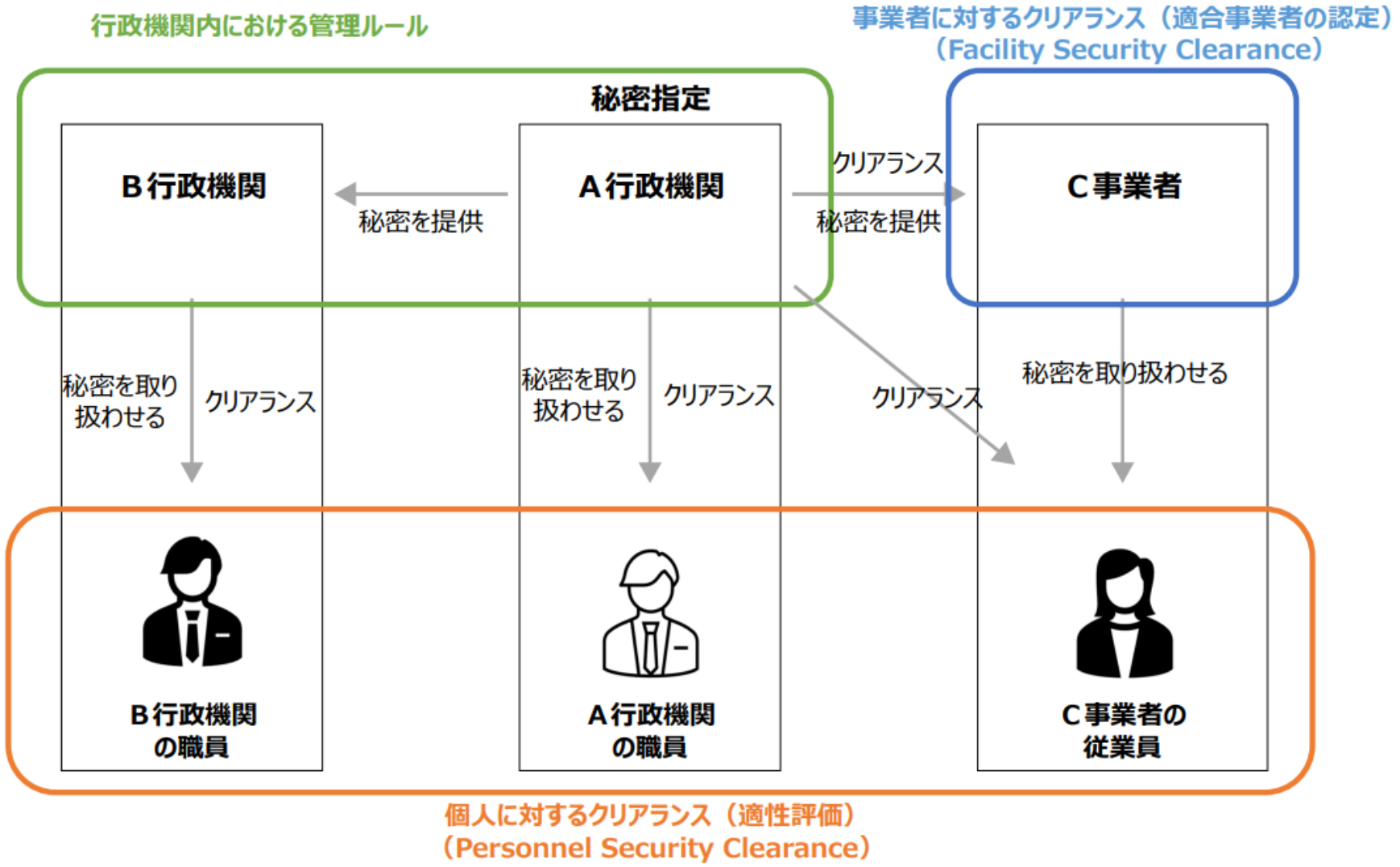
■ 取扱者の適性評価（PCL）

- 重要経済安保情報の取扱いは、適性評価（**Personnel Security Clearance／PCL**）をクリアした者に限定

重要経済安保情報保護活用法に関する関連ドキュメント等

法律	・重要経済安保情報の保護及び活用に関する法律
政令（施行令）	・重要経済安保情報の保護及び活用に関する法律施行令 各行政機関が定める内部ルール（規程）に関する事項、情報の保護措置、適合事業者に関する基準等について定める
運用基準	・重要経済安保情報の指定及びその解除、適性評価の実施並びに適合事業者の認定に関し、統一的な運用を図るための基準 名称のとおりの事項を定める運用基準。2025年1月閣議決定
ガイドライン（行政機関編）	行政機関において法運用に関わるものの理解を助けることを目的とするガイドライン。別添として適合事業者との契約書ひな形（2025年5月）
ガイドライン（適合事業者編）	事業者において法運用に関わる者の理解を助けることを目的とするガイドライン。各種ひな形も別添資料として添付（2025年5月）
適性評価に関するQ&A	適性評価を受ける予定がある者やその関係者向けのQ&A（2025年5月）
重要経済安保情報保護規程	各行政機関が重要経済安保情報を保護するために施行令11条に基づき策定する規程

重要経済安保情報の提供の流れと管理ルールのイメージ

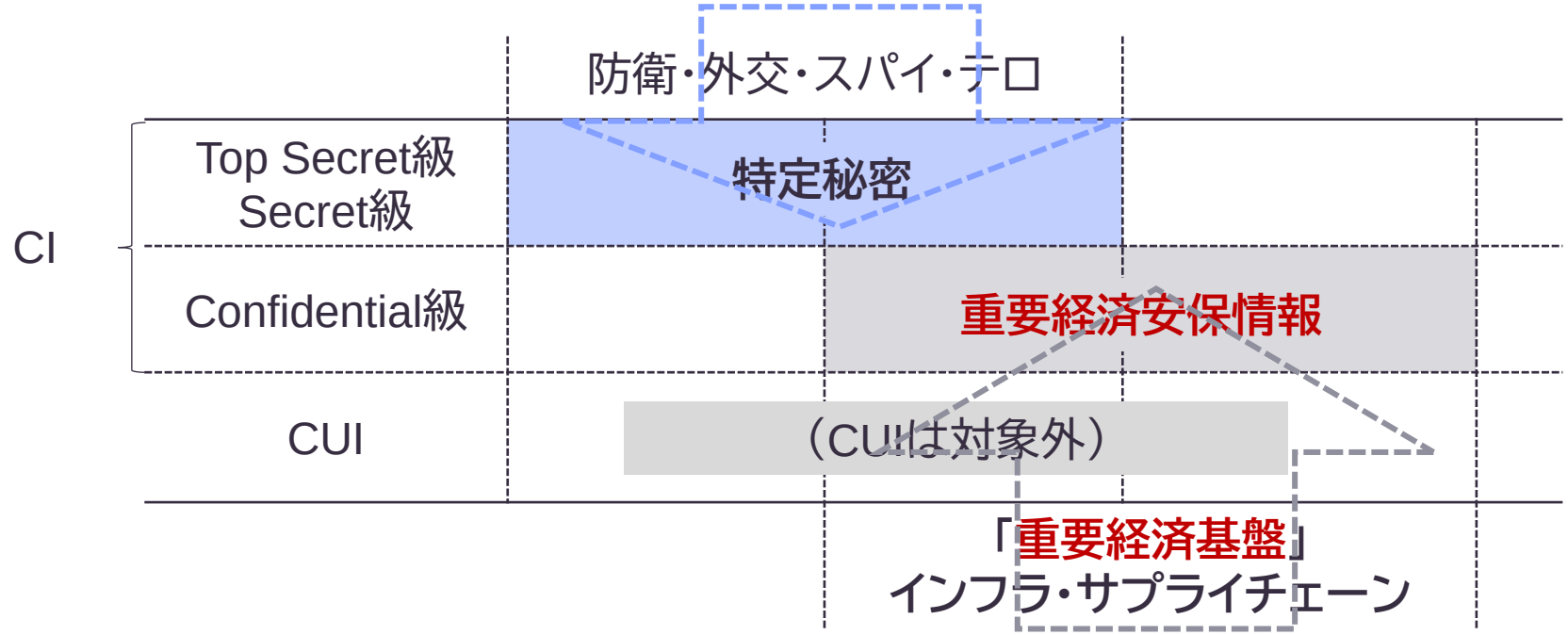


出典：内閣府参考資料
「適性評価と重要経済安保情報の提供の流れ」
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_hyouka.pdf

特定秘密保護法と新法の比較

	特定秘密保護法	重要経済安保情報保護活用法
指定対象情報	● 防衛 ● 外交 ● 特定有害活動の防止 ● テロリズムの防止 いずれも政府が保有する情報が対象	● 重要なインフラ ● 重要物資のサプライチェーン （重要経済基盤保護情報）
情報の機微度	● **Top Secret、Secret**級に相当 （漏えいが我が国の安全保障に**著しい支障**）	● **Confidential級**に相当 （漏えいが我が国の安全保障に**支障**）
情報の取扱主体	● 行政機関における取扱制限（公務員の適性評価）を想定 ※民間事業者への提供も一応可能	● 民間事業者への提供＋取扱制限（従事者の適性評価）を想定
適性評価有効期間	● 5年	● 10年

指定の対象となる情報のイメージ



＜参考＞特定秘密保護法の特定秘密カテゴリの拡大？

■ 特定秘密保護法に関する運用基準の改訂

※12月上旬：日経等で特定秘密に経済安保追加という旨の報道

- 特定秘密保護法に関する運用基準の改定案が2025年11月にパブコメ
- 重要経済安保情報保護活用法との整合性の確保のための改訂

> 「**重要経済基盤保護情報に該当する情報のうち**、(1)に示した事項の細目に該当し、(2)の非公知性の要件も満たすものであって、(3)の特段の秘匿の必要性の要件に照らし、**その漏えいがわが国の安全保障に著しい影響を与えるおそれが**あるものについては、同法第3条第1項に規定する重要経済安保情報ではなく特定秘密として指定すること」

- 特定秘密保護法の別表（防衛、外交、特定有害活動防止、テロリズム防止）を改正するものではないため、純粋に「特定秘密に経済安保を追加」というわけではない
- 解釈上特定秘密の範囲を経済安保関連情報に広げやすくすることが狙い？

自社保有情報が保全指定されると自由に扱えなくなる？

■ よくある誤解

- 自社保有の情報／政府に渡した情報が秘密指定されると自由に使えなくなる？

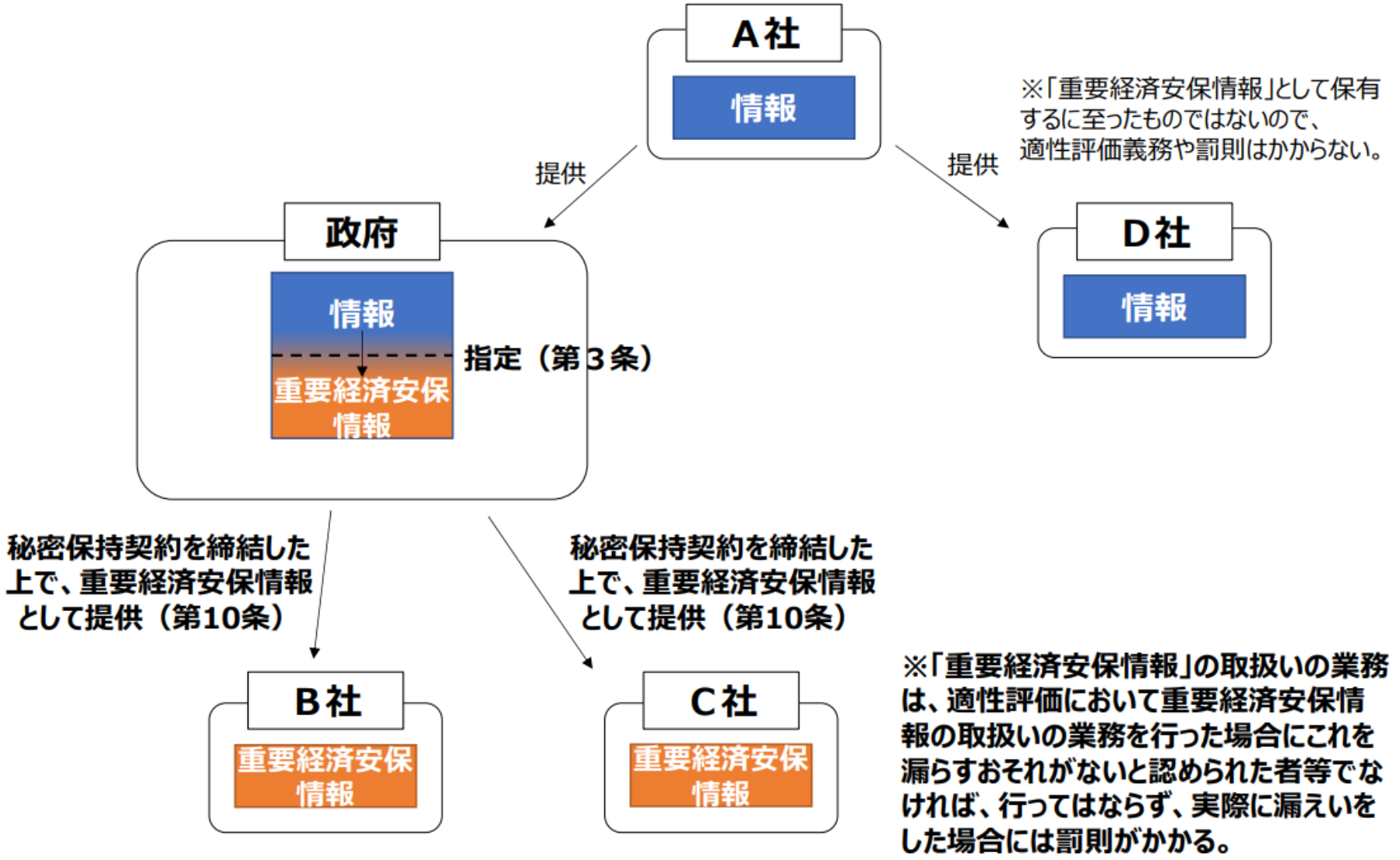
■ 民間保有の情報は基本的に対象外

- 保全指定の対象は、政府が保有する情報である
- 事業者等から提供された情報も、①重要経済基盤保護情報該当性、②非公知性、③秘匿の必要性の3つの要件を満たすなら保全指定自体は否定されないが、特に、②と③の関係で、**事業者等から提供された情報を単に重要経済安保情報に指定するだけでは、当該情報を提供した事業者等に法の規定は及ばない**（運用基準8頁）

■ 例外となり得るケース

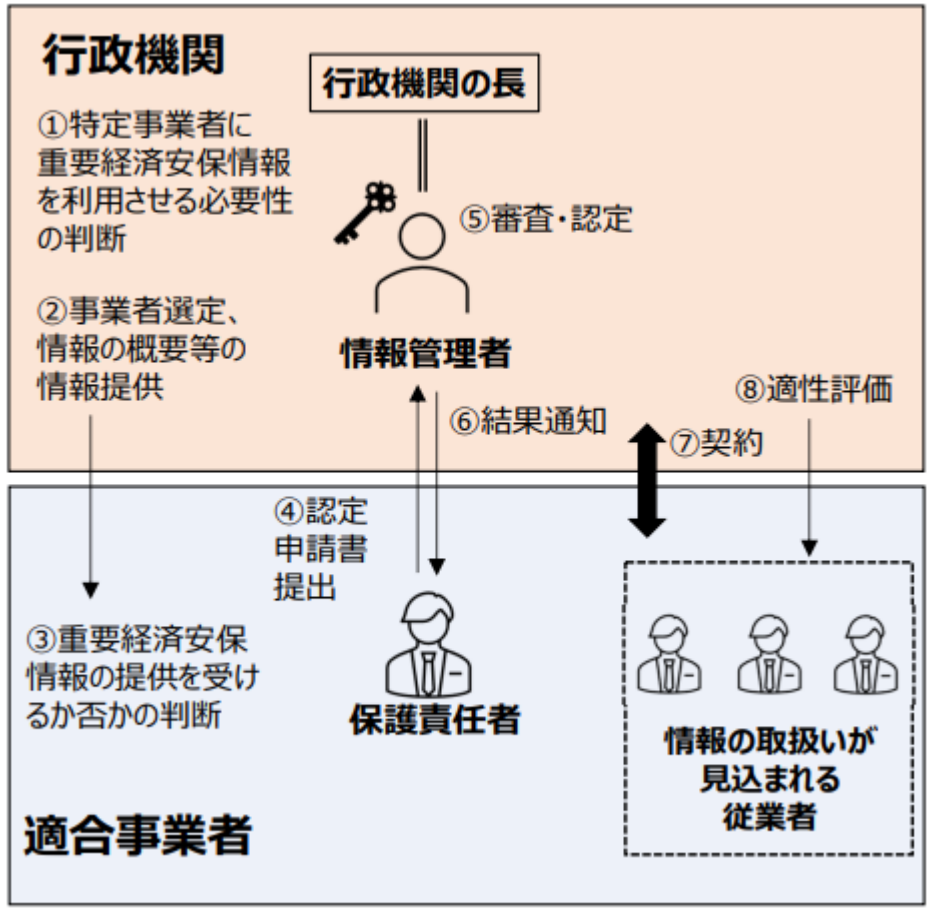
- 法10条2項：行政機関から民間事業者への調査研究の委託の成果物（委託とは関係ない独自の調査研究、どうは対象外）
- 革新的技術に関する情報のうち、**民間企業や研究機関が独自に保有している技術情報そのものではなく、行政機関が自ら分析し、または企画立案を加える**ことで生成した情報

「重要経済安保情報」として保有に至ったかどうかがポイント



出典：内閣府参考資料 「適性評価と重要経済安保情報の提供の流れ」
https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/sankou_hyouka.pdf

適合事業者認定：事業者のクリアランス（FCL）



■ 事業者の選定（2パターン）

1. **提供する場合**（元々政府で保有する情報を提供）
2. **保有させる場合**（調査研究の実施により重要経済安保情報の発生が見込まれる場合）

※事業者の同意がなければ、調査研究等の結果を重要経済安保情報に指定できない

■ 適合事業者の認定

- 認定申請書には、**申請者に関する事項（株主、役員情報を含む）、保護責任者に関する事項、情報保全に係る規程、教育に関する事項、重要経済安保情報を取り扱う場所に関する事項**を記載
- **外国からの影響**などの様々な考慮要素からの総合判断により、**行政機関の長**が適合事業者かどうかを認定する
- 適合事業者と認められない場合には理由も通知する

事業者が規程に定めるべき事項

■ 重要経済安保情報の管理に必要なものとして規程に定めるべき事項の例

※ガイドライン（適合事業者編）に規程のひな形（別添1）あり

- ✓ 重要経済安保情報の保護の全体の責任を有する者（**保護責任者**）の指名基準・指名手続
- ✓ 重要経済安保情報の保護に関する業務を管理する者（**業務管理者**）の指名基準・指名手続、職務内容
- ✓ 従業者に対する重要経済安保情報の保護に関する**教育の実施内容**及び方法
- ✓ 重要経済安保情報の保護のために必要な施設**設備の設置**に係る手続
- ✓ 重要経済安保情報の**取扱いの業務を行う従業者の範囲**の決定基準及び決定手続
- ✓ 重要経済安保情報を**取り扱うために使用する電子計算機の使用の制限**に係る手続及び方法

  ※規程ひな形（電子計算機の使用の制限）
  第30条 重要経済安保情報を記録する電磁的記録は、**スタンドアローンの電子計算機又はインターネットに接続していない電子計算機**であって、かつ、適性があると認められた者のみがアクセスできる措置が講じられたものとして、契約行政機関が認めたもののみで取り扱うものとする
- ✓ 重要経済安保情報の漏えいのおそれがある緊急事態に際しての文書等の廃棄に係る手続及び方法
- ✓ 重要経済安保情報文書等の紛失その他の事故が生じた場合における被害防止措置の手続及び方法

FCLに関する留意点

■ 適合事業者認定申請書に、役員情報と株主情報の提供が必要

- 役員：**氏名、生年月日、国籍等、帰化歴の有無**の記載が必要であり、**身分証の添付**も必要
- 株主：議決権の5％を超を直接保有する者の記載が必要。資産管理信託会社が株主となっている場合、**「真の株主」の情報**を行政機関から求められる
- 役員全員が適性評価を受ける必要まではないが、情報を取り扱うのであれば必要
- 様々な場面で「国籍」が求められる

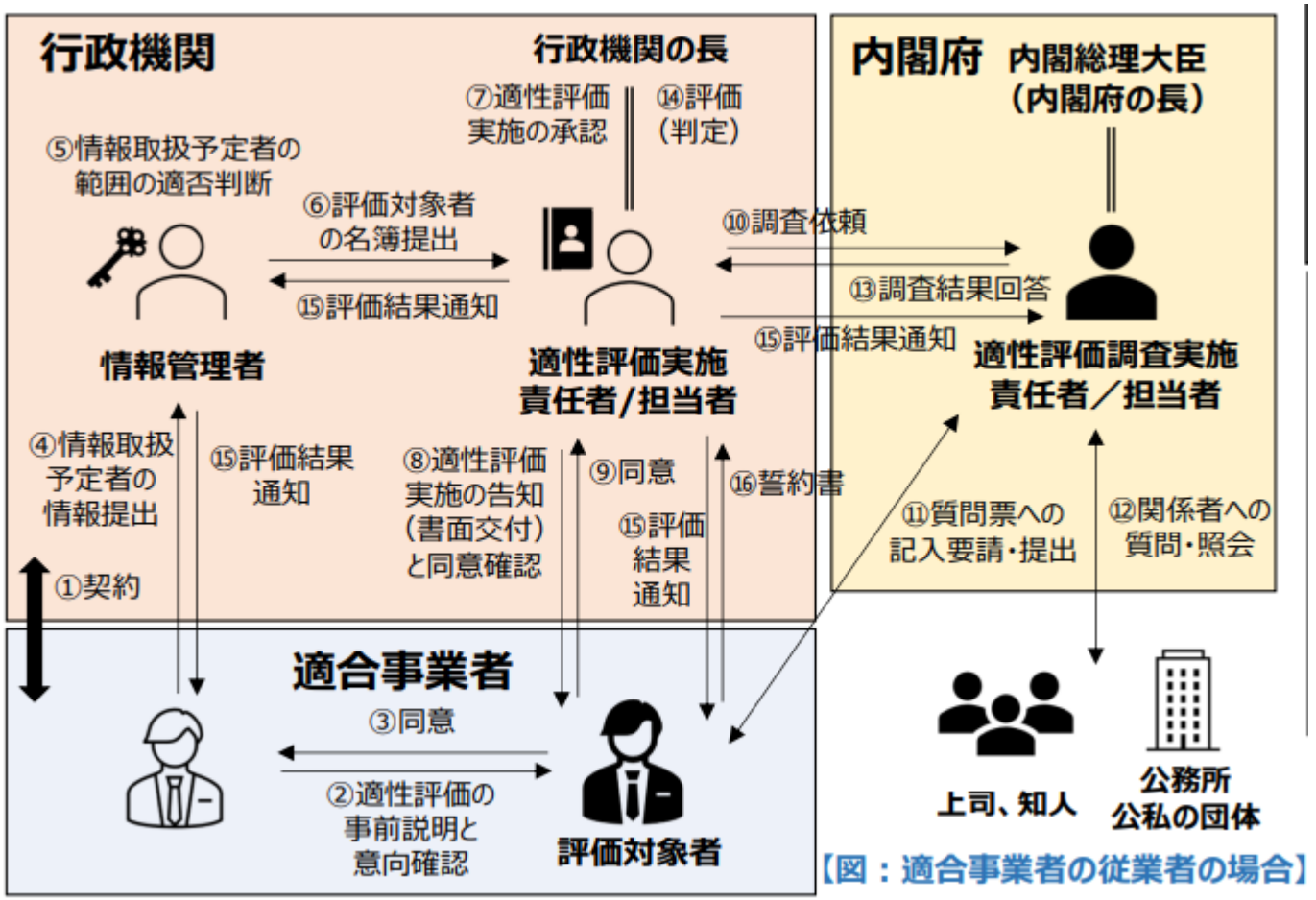
■ 教育資料の作成・添付

- 重要経済安保情報を保護するために必要な知識を的確に習得するための**教育資料の作成及び実施**が必要、認定申請の際に提出も必要（適合事業者GLに教育資料ひな形あり）

■ 施設設備の整備

- 厳格な物理的・技術的安全管理措置が必要
- **データで扱う場合はスタンドアローンで扱う必要**

適性評価：情報を取り扱う個人のクリアランス（PCL）



【図：適合事業者の従業者の場合】

■ 適性評価の基本的な考え方

1. 基本的人権の尊重
2. プライバシー保護
3. 法定調査事項以外の調査の禁止
4. 適性評価結果の目的外利用禁止

■ 適性評価の流れ

- 評価対象者の同意を前提に、内閣府による一元的調査結果に基づき行政機関が認定

適性評価における調査事項等

■ 調査事項（法12条2項）

① **重要経済基盤毀損活動**との関係に関する事項
　✓家族及び同居人の氏名、生年月日、国籍及び住所を含む
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

※②～⑦は特定秘密保護法における適性評価と同じ項目

※**重要経済基盤毀損活動**とは、(a)非公開の重要経済基盤に関する情報を外国の利益を図る目的で取得する活動、(b)政治上その他の主義主張に基づき、社会に不安若しくは恐怖を与える目的で重要経済基盤に支障を生じさせる活動等

■ 評価の視点

a. 情報を適正に管理できるか
b. 規範を遵守して行動できるか
c. 職務に対して誠実に取り組めるか
d. 情報を漏らす活動に関与しないか
e. 自己を律して行動できるか
f. 漏えいの働きかけを受けた場合に応じるおそれが高い状態にないか
g. 職務の遂行に必要な注意力を有するか

■ 対象行動に関する考慮要素

調査事項に関する**対象行動**があった場合、その性質、重大性、関与の程度、背景、頻度、時期、当時の年齢、再発防止可能性など

適性評価の結果

■ 適性評価結果の通知（法13条）

- 適性評価の結果は、**評価対象者**に通知＋適合事業者の従業者の場合には、**適合事業者**にも通知
- 対象者により評価に必要な時間が大きく変わりうるため、結果を通知するまでの**期間制限はなし**
- 結果については、苦情の申出が可能（法14条）

  ＝法令上の手続としての**不服申立は想定されていない**

■ 適性評価に関する個人情報の目的外利用・提供の制限（法16条）

- 行政機関の長は、評価対象者が同意しなかったこと、適性評価の結果及び調査で取得する個人情報は、重要経済安保情報の保護以外の目的で利用・提供してはならない
- 適性評価結果の通知を受けた適合事業者等は、重要経済安保情報の保護以外の目的で通知の内容を利用・提供してはならない

  →**不利益取扱いの禁止**

PCLに関する留意点

■ 個人が積極的に適性評価を受けに行くことの可否

- **重要経済安保情報を受領する（保有する）必要性がある適合事業者の従事者であることが前提**であるため、それと無関係に適性評価を求めるというフローはない

■ 適性評価の結果の利用

- **適性評価は人事評価や業務遂行能力を実証するものではない**

  →適性評価の結果を考慮した**解雇、言及、降格、懲戒処分などは目的外利用として禁止**
- **適合事業者において、適性があると認められた者を対象に手当を支給**することは、従事者が負う責任等を全体として評価した結果、適性評価を受けた事実そのものが評価対象ではないという前提で**目的外利用には当たらない**（適合事業者ガイドライン）

■ 重要経済安保情報の取扱いが想定される従業員

- 重要経済安保情報を取り扱うという条件で採用されることになる求職者についても、「重要経済安保情報を取り扱うことが見込まれる者」として採用・内定前から適性評価を開始しうる

FCL・PCLを受けたことの発信

■ 適合事業者である事を対外的に表明すること（適合事業者ガイドライン）

- 適合事業者に認定された事業者が、自らが適合事業者であることを、対外的に公表し、又は第三者に開示していくことについては、**法的に禁止されている行為ではない。**他方、一般論として言えば、当該事業者が重要経済安保情報を取り扱っていることを表明していることになるため、それを契機に、当該事業者が**情報漏えいの働き掛けを受ける対象となり得る**点に十分留意する必要があると考えられる。

■ 適性評価を受けたことの発信（適性評価Q&A)

- 評価対象者が自身の結果について共有する行為は**本法によって禁止されてはいません。**ただし、適性があると認められ、重要経済安保情報の取扱いの業務を行う場合、**諜報活動の標的となる可能性があるため、情報保全の観点から慎重であることが望ましく**、留意が必要です。

- その他、当然ながら労働者としての守秘義務や内部規程違反となる可能性もありうる

他の経済安全保障関連法令とクリアランスの活用可能性

3

サイバーセキュリティに関連する経済安全保障法制の動向

法令等	概要
経済安全保障推進法	• 2022年成立、4つの施策からなるオムニバス法令 • 基幹インフラに関する審査制度（2024年運用開始） 正式名：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法律
重要経済安保情報保護活用法	• 2024年成立、経済安全保障版セキュリティ・クリアランス法 • 2025年5月16日施行 正式名：重要経済安保情報の保護及び活用に関する法律
サイバー対処能力強化法及び同整備法	• 2025年5月16日成立、国家安全保障戦略に基づく能動的サイバー防御 • 官民連携、通信情報利用、アクセス・無害化、体制整備 正式名：重要電子計算機に対する不正な行為による被害の防止に関する法律・同法律の施行に伴う関係法律の整備等に関する法律
国家サイバー統括室発足 （National Cybersecurity Office: **NCO**）	• 2025年7月1日、内閣官房内閣サイバーセキュリティセンター（NISC）を改組する形で内閣官房国家サイバー統括室として発足 サイバー対処能力強化法整備法の一部施行、内閣官房組織令改正

サイバー対処能力強化法及び同整備法の概要

①官民連携（インシデント報告等）、**②通信情報の利用**、**③アクセス・無害化**措置、**④組織・体制整備**

➢ 主要な措置（抜粋）は以下のとおり

①官民連携

- **基幹インフラ事業者による**特定の電子計算機（組込みプログラムを含む）の届出義務・**インシデント報告義務**
- 情報共有・対策の**協議会**設置
  サイバーセキュリティ協議会の改組
- **脆弱性対応強化**
  通信情報利用と合わせて、分析情報・脆弱性情報の提供

②通信情報の利用

- **基幹インフラ事業者との協定（同意）**に基づく通信情報取得
- 同意によらない通信情報取得
- 意思疎通の本質ではない情報（機械的情報）の選別、他の情報消去
- 取得した通信情報の厳格な取扱い
- 独立機関（**サイバー通信情報監理委員会**）による事前審査・継続検査

※ 通信情報は官民連携にも利用

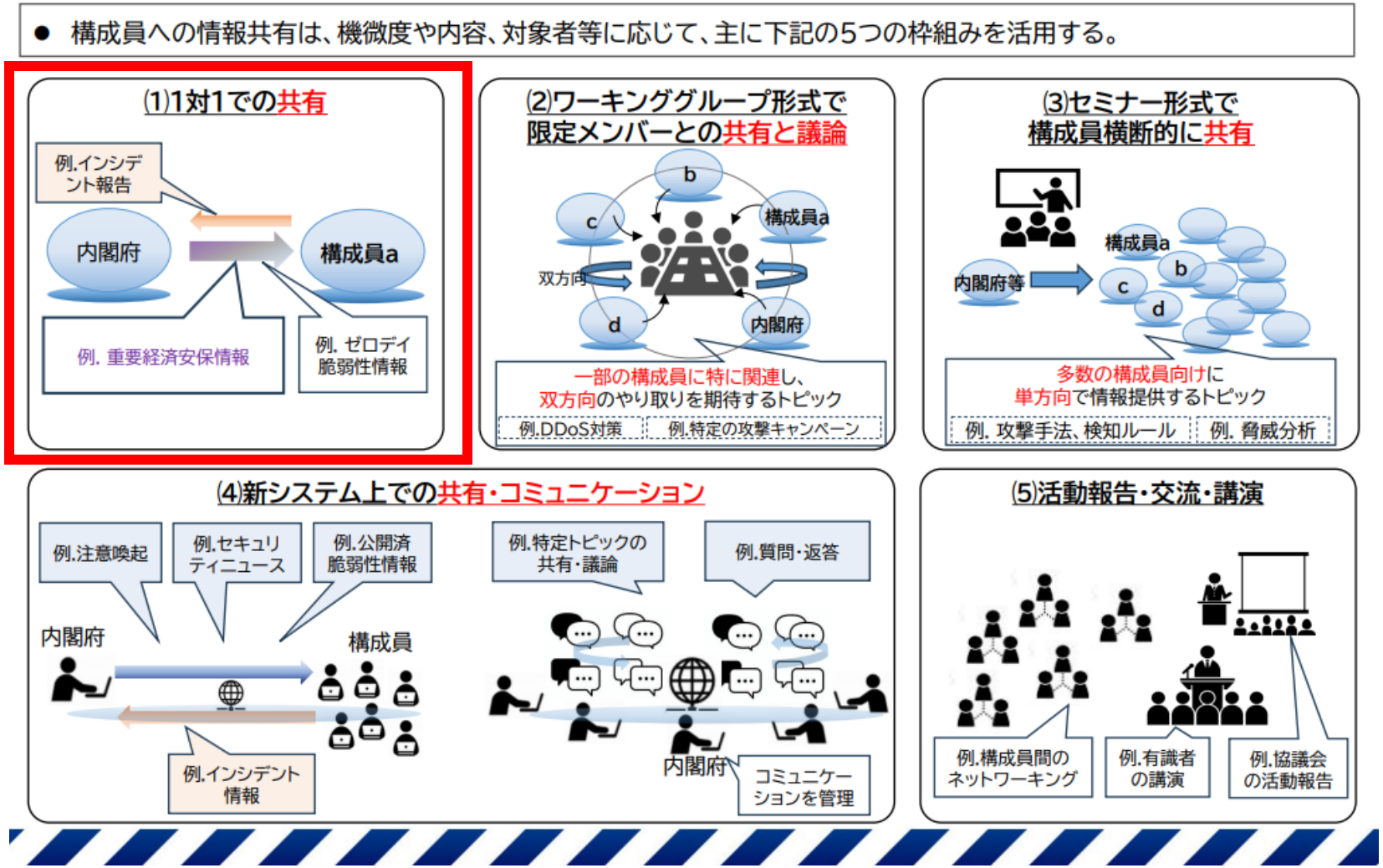
③アクセス・無害化

- サイバー攻撃による重大な危害防止のための、警察・自衛隊による無害化措置（①攻撃に利用されているサーバへのログイン、②インストールされているプログラムを確認、③攻撃に使えないよう無害化）
- 措置の実施にはサイバー通信情報監理委員会の事前承認が必要

④組織・体制整備

- サイバーセキュリティ戦略本部強化：**重要インフラ事業者**等のセキュリティ確保に関する国の基準作成を所掌事務に追加
- **内閣サイバー官**の設置、**サイバー通信情報監理委員会**の設置（NISC改組は政令改正で実施→R7.7.1国家サイバー統括室）

協議会における情報共有（検討中の案）



■ 新協議会

- サイバー対処能力強化法に基づく官民連携のための協議会
- **1対1での情報共有の際に、重要経済安保情報の共有を想定**か

出典：サイバー対処能力強化法の施行等に関する有識者会議第4回会合(2025年12月8日)資料5https://www.cyber.go.jp/pdf/council/cyber_anzen_hosyo/cyber_anzen_hosyo-04shiryo05.pdf

2026年経済安全保障法制の動向

■ 経済安全保障推進法改正の方向性

- 2025年11月に改正の方向性について報道、経済安全保障法制に関する有識者会議がリブート
- 2025年12月16日の会議で資料公開

1	サプライチェーン強靭化	➢ 海底ケーブル敷設等の「役務」（サービス）についても財政援助 ➢ 安定供給に支障が生じるおそれがある場合の措置
2	**基幹インフラ**	➢ 基幹インフラに「医療」分野を追加 ➢ 手続の運用改善（法律、基本方針、政省令の見直し）
3	重要な海外事業展開支援**（新設）**	➢ 重要事業（報道では造船や高速通信）などの海外展開を支援
4	調査研究の推進・官民連携	➢ 指定基金に関する規定の整備 ➢ 総合的な経済安全保障**シンクタンク、官民協議会**
5	**データセキュリティ（新設）**	➢ 安全保障上重要なデータ（個人に関する機微なデータ、基幹インフラサービスの安定的提供に必要なデータ）の防護 ➢ データセンター・クラウド上のデータ防護

○ データセキュリティについて以下の２つの観点で検討を進めてはどうか。

① **安全保障上重要な個人データ（ゲノムデータ、金融情報等）を取り扱う者**に関する措置

② 大量のデータの保存・処理を行う**データセンター・クラウドサービスを提供する者**に関する措置

データ取扱事業者

① 安全保障上重要な個人データの防護

安全保障上重要な個人データの取扱事業者

提供（売買等）→ 第三者

解析依頼 → ゲノム解析事業者

情報システムの導入 → 情報システムベンダー（オンプレ/クラウド）


ゲノムデータ・医療情報


金融情報


位置情報


生体認証情報

データの保存・処理

② データセンター・クラウドサービス上のデータの防護

ベンダー等

サーバ導入等 → **クラウド事業者**

電源導入等 → **データセンター事業者**

※ 上記①②とは別途、基幹インフラ役務の安定的な提供に必要なデータの防護については、既存の基幹インフラ制度の運用改善等を検討。

経済安全保障推進法改正：データセキュリティ制度の新設

■ 安全保障上重要なデータの防護

- **個人に関する機微データ（ゲノムデータ、位置情報、生体認証情報、金融情報、医療情報）**が漏えい等した場合に、特定の個人に対する影響力行使等に利用されるリスク
- データ提供、データの保存・処理を行う情報システムの契約、ゲノムデータの解析依頼を規制対象？
- 防護のための具体的な措置は不明だが、**一定のデータについて一定の行為を原則禁止？**
- 米国データセキュリティプログラムを参考か

■ データセンター・クラウド上のデータ防護

- データセンター、クラウドにおける**情報の漏えいや滅失を防ぐための措置（安全管理措置義務？）**
- 日本国内の**データセンターの設置状況等を把握するための措置（届出義務？）**
- 規制対象となる「データセンター」事業者とは

CUIはどうなったか？

CUIについてはセキュリティクリアランスの対象外

- 民間保有のCUIは、営業秘密として自主管理が基本となる
- ただし、海外ビジネス・国際共同開発において、セキュリティ・クリアランスがCUIを共有する条件（「**信頼できる証**」）とされる場面がある
- 法案成立時の附帯決議に、「民間事業者等が保有している情報であって国として経済安全保障の観点から保護が必要と考えられる最先端技術情報等について、民間事業者が必要となる対応をとれるような環境整備を検討すること」とあったが…？
- 2025年5月に、経済産業省より「技術流出対策ガイダンス第1版」が公開されているが、CUIやセキュリティ・クリアランスに関連すると思われる記述は特に見受けられない

ご清聴ありがとうございました

森・濱田松本法律事務所外国法共同事業
弁護士　蔦　大輔　Daisuke TSUTA
Tel　03-6266-8769
E-mail　daisuke.tsuta@morihamada.com

オンライン名刺