

【対談】
グローバルサプライチェーンでの重要情報保護を強化するための新しい取組とは
素材スライド集

2025年12月22日

合同会社三笠ポリシーアドバイザリ 代表社員 三笠 武則
(営業秘密保護推進研究会 事務局長)



Copyright @ APPTras All Rights Reserved.

本日の対談の論点：

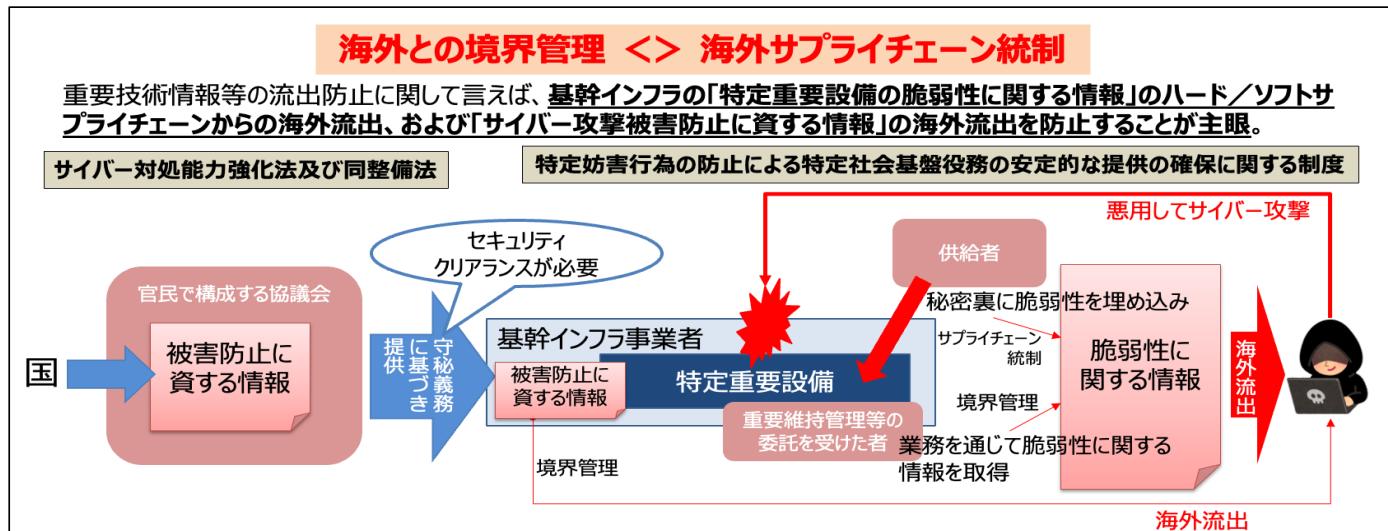
1. 本日紹介した国の制度の重点ポイントはどちら？ 海外との境界管理 vs 海外サプライチェーン統制
2. 重要秘密流出の脅威類型とは？
3. 従来の営業秘密管理の枠を超えて、流出防止を強化すべき民間保有の重要秘密とは？
4. 物理的セキュリティの再点検
5. 民間企業は経済安保推進法やセキュリティクリアランス制度の保護アプローチの何を参考にすべきか？

1. 本日紹介した国の制度の重点ポイントはどちら？

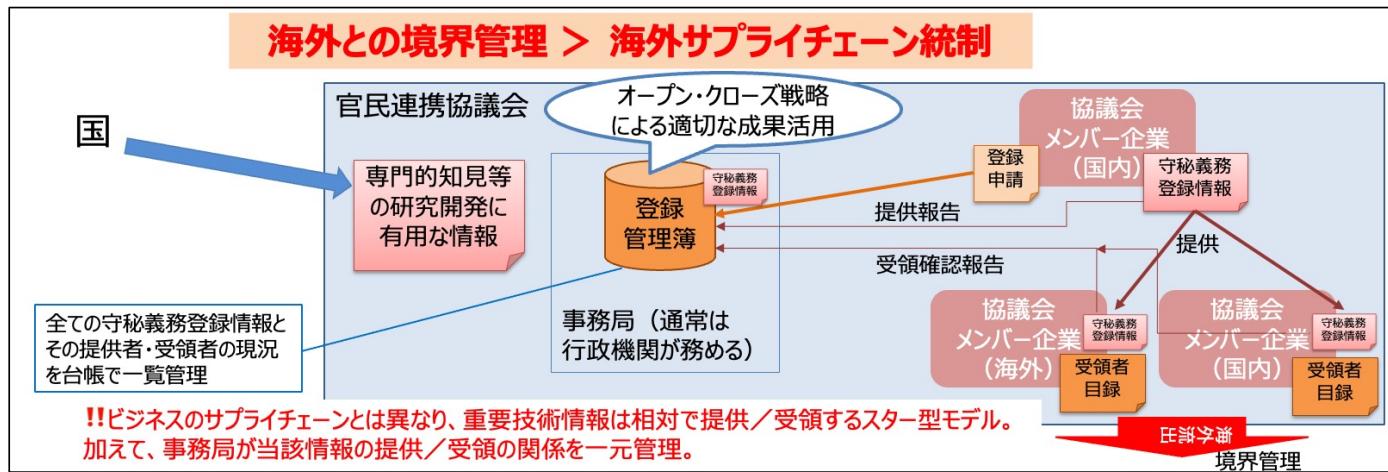
海外との境界管理 vs 海外サプライチェーン統制

経済安全保障推進法における重要技術情報保護の主眼とは

特定妨害行為の防止による
特定社会基盤役務の安定的な
提供の確保に関する制度



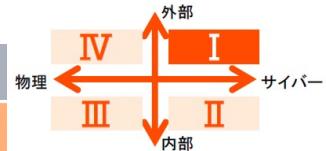
特定重要技術の研究開発の
促進及びその成果の適切な
活用に関する制度



2. 重要秘密流出の脅威類型とは？

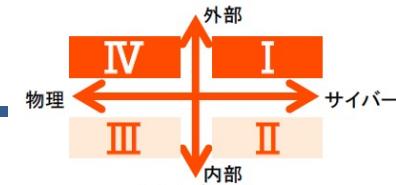
脅威の4類型～サイバー領域と物理領域の双方から迫るリスク

■ サイバー領域と物理領域という2つの視点から脅威を体系化し、「脅威の4類型」としてその全体像を整理します。



(出典) 橋 了道 「重要技術情報漏えいの脅威類型と持つべきリスク認識」

第I類型 vs 第IV類型 (外部の視点)

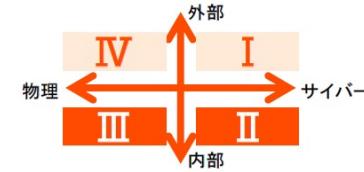


- 第I類型は“インターネット越しの見えない侵入者”で、検知と可視化で守り、第IV類型は“目の前にいる訪問者”で、見せない・触れさせない管理で守ります。
- 経路は違っても、どちらも境界線の“ゆるみ”を突いてくるという点は同じです。

観点	第I類型:外部侵入型サイバー脅威	第IV類型:外部接触型物理脅威
攻撃者の姿	目では見えない相手(インターネット越しの侵入者)	目で見える相手(訪問者・業務委託・研究協力者)
侵入の方法	ネットワーク経由 (脆弱性・マルウェア・認証情報の窃取)	契約・業務・取材・見学を装った物理的接触
狙われる対象	サーバ・システム・データベース	設備・工程・研究内容・試作品・紙媒体の図面等
検知難度	デジタルログの解析で特定可能だが、巧妙化が進んでいる	行動の痕跡が残りにくく、発覚は事後の場合が多い
防御手段	セキュリティ監視・検知・ログ分析・アクセス制御	入退室管理・撮影制限・情報非開示・エスコート徹底
考え方	見えない相手→監視・検知(“見える化”)で防ぐ	見える相手→情報を秘匿・制限(“見せない”)で防ぐ

(出典) 橋 了道 「重要技術情報漏えいの脅威類型と持るべきリスク認識」

第Ⅱ類型 vs 第Ⅲ類型 (内部の視点)



- 第Ⅱ類型と第Ⅲ類型は、どちらも“内部から始まる脅威”です。
- 第Ⅱ類型はITシステム上のログで追跡ができますが、第Ⅲ類型は人の行動を見ないと防げません。
つまり、情報セキュリティ部門だけでは完結しない領域であると言えます。

観点	第Ⅱ類型: 内部関与型サイバー脅威	第Ⅲ類型: 内部起点型物理脅威
経路	デジタル(システム・クラウド)	物理(現場・紙・試作品・設備)
検知手段	ログ・アラート・システム監視	監視カメラ・通報・在庫管理
発生形態	サイバーインシデント・設定ミス	現場・研究所・製造ラインへの侵入
検知難度	中(デジタル記録あり)	高(行動監視に依存)
対応主体	IT・情報セキュリティ部門	総務・人事・製造・研究管理部門
再発防止策	権限管理・システム監査	入退室管理・持込持出制限・教育

(出典) 橋 了道「重要技術情報漏えいの脅威類型と持つべきリスク認識」

3. 従来の営業秘密管理の枠を超えて、 流出防止を強化すべき民間保有の重要秘密とは？

重要経済基盤保護情報該当性の定義（詳細）

第1号 外部から行われる行為から重要経済基盤を保護するための措置又はこれに関する計画若しくは研究	① 外部から行われる行為から基盤公共役務の提供体制を保護するための措置 又はこれに関する計画若しくは研究のうち、以下に掲げる事項に関するもの	ア 基盤公共役務 を提供する事業者及び行政機関の 施設・設備等の安全確保 に関する措置 a 施設・設備等の導入及び維持管理等に係る 規制・制度 に関して 行政機関が行う審査・監督等の措置 b 施設・設備等に対する 外部からの物理攻撃、サイバー攻撃 その他の役務の提供に支障を与える行為に 対応するための措置 c 施設・設備等に係るその他の安全確保に係る措置（a及びbに掲げるものを除く。） イ 基盤公共役務を提供する 事業者の経営 や、事業者及び行政機関が保有する 技術、知識、データ、人員等 の役務の安定的な提供を行う体制を維持するために必要とするその他の 経営資源 に対し 外部から行われる行為 からの 保護措置
	② 外部から行われる行為から重要物資の供給網を保護するための措置 又はこれに関する計画若しくは研究のうち、以下に掲げる事項に関するもの	ア 外部から行われる輸出入規制、不公正な貿易政策、国際物流網の封鎖等 の行為による 重要物資の供給途絶や供給不足、国内生産基盤の弱体化等 に 対応するための措置 イ 重要物資の供給網に関わる事業者及び行政機関の 施設・設備等の安全確保 に関する措置 a 施設・設備等に対する 外部からの物理攻撃、サイバー攻撃 その他の重要物資の安定供給に支障を与える行為に 対応するための措置 b 施設・設備等に係るその他の安全確保に係る措置（aに掲げるものを除く。） ウ 重要物資の供給網に関わる 事業者の経営 や、事業者及び行政機関が保有する 技術、知識、データ、人員等 の物資の安定提供を行う体制を維持するために必要とするその他の 経営資源 に対し 外部から行われる行為 からの 保護措置
第2号 重要経済基盤の脆弱性、重要経済基盤に関する革新的な技術その他の重要経済基盤に関する重要な情報であって安全保障に関するもの	① 重要経済基盤の脆弱性 に関する情報であって安全保障に関するもの	ア 基盤公共役務の提供体制の脆弱性 に関する情報であって安全保障に関するものうち、以下に掲げる事項に関するもの a 基盤公共役務を提供する事業者及び行政機関の 施設・設備等の脆弱性 に関する情報 b 基盤公共役務を提供する 事業者の経営 や、事業者及び行政機関が保有する 技術、知識、データ、人員等 の役務の安定的な提供を行う体制を維持するために必要とするその他の 経営資源に関する脆弱性 に関する情報 イ 重要物資の供給網の 脆弱性 に関する情報であって安全保障に関するものうち、以下に掲げる事項に関するもの a 重要物資の外部依存度、非代替性、供給途絶時の影響の詳細等につき 調査・分析等 により得られた情報 b 重要物資の供給網に関わる事業者及び行政機関の 施設・設備等の脆弱性 に関する情報 c 重要物資の供給網に関わる 事業者の経営 や、事業者及び行政機関が保有する 技術、知識、データ、人員等 、物資の安定供給を行う体制を維持するために必要とするその他の 経営資源に関する脆弱性 に関する情報
② 重要経済基盤に関する革新的な技術 に関する情報であって安全保障に関するもののうち、以下に掲げる事項に関するもの	ア 重要経済基盤 に関する革新的な技術の 国際共同研究開発 において、 外国の政府等から提供 され、当該外国において本法による保護措置に相当する措置が講じられている情報 イ 重要経済基盤に関する革新的な技術で 我が国が技術優位性を持つ分野 （これから技術優位性を確保しようとする分野も含む。）に関する 研究・調査・分析・審査等 により得られた情報 ウ 重要経済基盤を 防護 するための革新的技術に関する情報	
③ その他の重要経済基盤に関する重要な情報 であって安全保障に関するもの		
第3号 第1号の措置に関し収集した外国の政府又は国際機関からの情報	外部から行われる行為から重要経済基盤を保護するための措置又はこれに関する計画若しくは研究に關し収集した 外国の政府又は国際機関からの情報 であって、当該外国の政府又は国際機関において本法による保護措置に相当する措置が講じられている情報（当該情報を分析して得られた情報を含む。）	4
第4号 第2号及び第3号に掲げる 情報の収集整理又はその能力 に関する情報	第2号及び第3号に掲げる 情報の収集整理又はその能力 に関する情報	9

（出典）内閣府「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概要」

● 特定重要技術の定義

「先端的技術」：「将来の」国民生活及び経済活動の維持にとって重要なものとなり得る先端的な技術

「特定重要技術」：「先端的技術」のうち①～③のいずれかに該当するもの（複数該当もあり得る）

①【当該技術を外部に不当に利用された場合】において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの
⇒当該技術の適正な管理が必要

②【当該技術の研究開発に用いられる情報が外部に不当に利用された場合】において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの
⇒研究開発に関する情報の適正な管理や、守秘義務の求めが必要

③【当該技術を用いた物資又は役務を外部に依存することで外部から行われる行為によってこれらを安定的に利用できなくなった場合】において、国家及び国民の安全を損なう事態を生ずるおそれがあるもの
⇒我が国が国際社会における自律性、優位性、ひいては不可欠性を確保・維持する必要

⇒ 特定重要技術の研究開発等を図るため、国は、以下の措置を講ずるよう努める

- **必要な情報の提供**：協議会等における、専門的知見など研究開発に有用な情報の提供
- **資金の確保**：指定基金を活用した研究開発等の強力な支援
- **人材の養成及び資質の向上**：協議会、指定基金、調査研究等を通じた、関連の人材の養成と資質の向上
- **その他**：協議会等における、成果の適切な活用に資する取組

※ 特定重要技術の性質上、安全保障貿易管理への適切な対応や研究インテグリティの自律的な確保に向けた取組に十分配慮が必要

● 調査研究を実施する技術領域

⇒ 以下の技術領域を参考にしつつ、柔軟に実施

- | | | | |
|--------------------|-------------------|---------------------|-----------------|
| ○バイオ技術 | ○データ科学・分析・蓄積・運用技術 | ○脳コンピュータ・インターフェース技術 | ○海洋関連技術 |
| ○医療・公衆衛生技術（ゲノム学含む） | ○先端エンジニアリング・製造技術 | ○先端エネルギー・蓄エネルギー技術 | ○輸送技術 |
| ○人工知能・機械学習技術 | ○ロボット工学 | ○高度情報通信・ネットワーク技術 | ○極超音速 |
| ○先端コンピューティング技術 | ○量子情報科学 | ○サイバーセキュリティ技術 | ○化学・生物・放射性物質及び核 |
| ○マイクロプロセッサ・半導体技術 | ○先端監視・測位・センサー技術 | ○宇宙関連技術 | ○先端材料科学 |

※令和3・4年度内閣府委託事業における広範囲調査の対象領域

● 指定基金を用いて研究開発等を実施する技術領域

⇒ 経済安全保障重要技術育成プログラムの「研究開発ビジョン」において示される技術

3

（出典）内閣府「特定重要技術の研究開発の促進及びその成果の適切な活用に関する基本指針」

サイバー対処能力強化法及び同整備法

情報共有・対策のための協議会の設置（強化法第9章）

- 内閣総理大臣は、サイバー攻撃による被害の防止のため、重要電子計算機を使用する者等（あらかじめ同意を得た者に限る。）を構成員とする協議会を設置し、構成員に対し、守秘義務を伴う被害防止に資する情報を共有するとともに、必要な資料提出等を求めることができることとする（サイバーセキュリティ協議会を廃止し、強化・新設）。 (第45条)
- 内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置
- 協議会には、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える
- 構成員に対しては、守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能

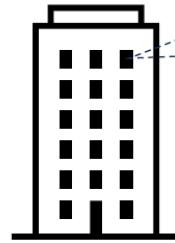
（出典）NCO「サイバー対処能力強化法及び同整備法について」

4. 物理的セキュリティの再点検

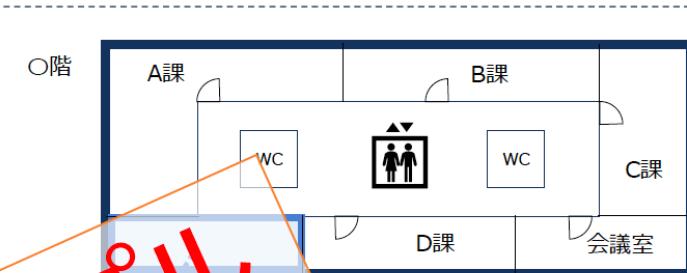
重要経済安保情報取扱区画のイメージ（1/2）

① 社屋

適切な入場制限措置
例：社員証等による認証



② 区画



② 重要経済安保情報取扱区画

天井、壁、床：容易に破壊されないうな鉄筋コンクリート又は頑丈な不燃性素材を用いる。

出入口：原則1カ所（複数箇所とする場合は不適意に開閉可能とならない）。常夜灯の設置（緊急時に照明が確保できる）

窓：窓がない部屋が推奨。仮に設置されている場合は、窓の強度を補強し警戒装置を含め容易に破壊侵入されないようにし、外部から盗み見られないよう遮蔽措置を講じる（ブラインドを常時閉めるなど）

開口部：ダクト、天窓等の開口部に不法侵入、盗見、盗聴のおそれがある場合には、金網や鉄格子を取り付ける。

① 部外からのアクセス制限

執務室を含む社屋の入出場時に社員証等による認証がなされるなど、入場を制限。
(アクセスの制限がない場合は、建物の敷地全体を金網等で囲んだ上で、適切な入場制限措置を講じること。)

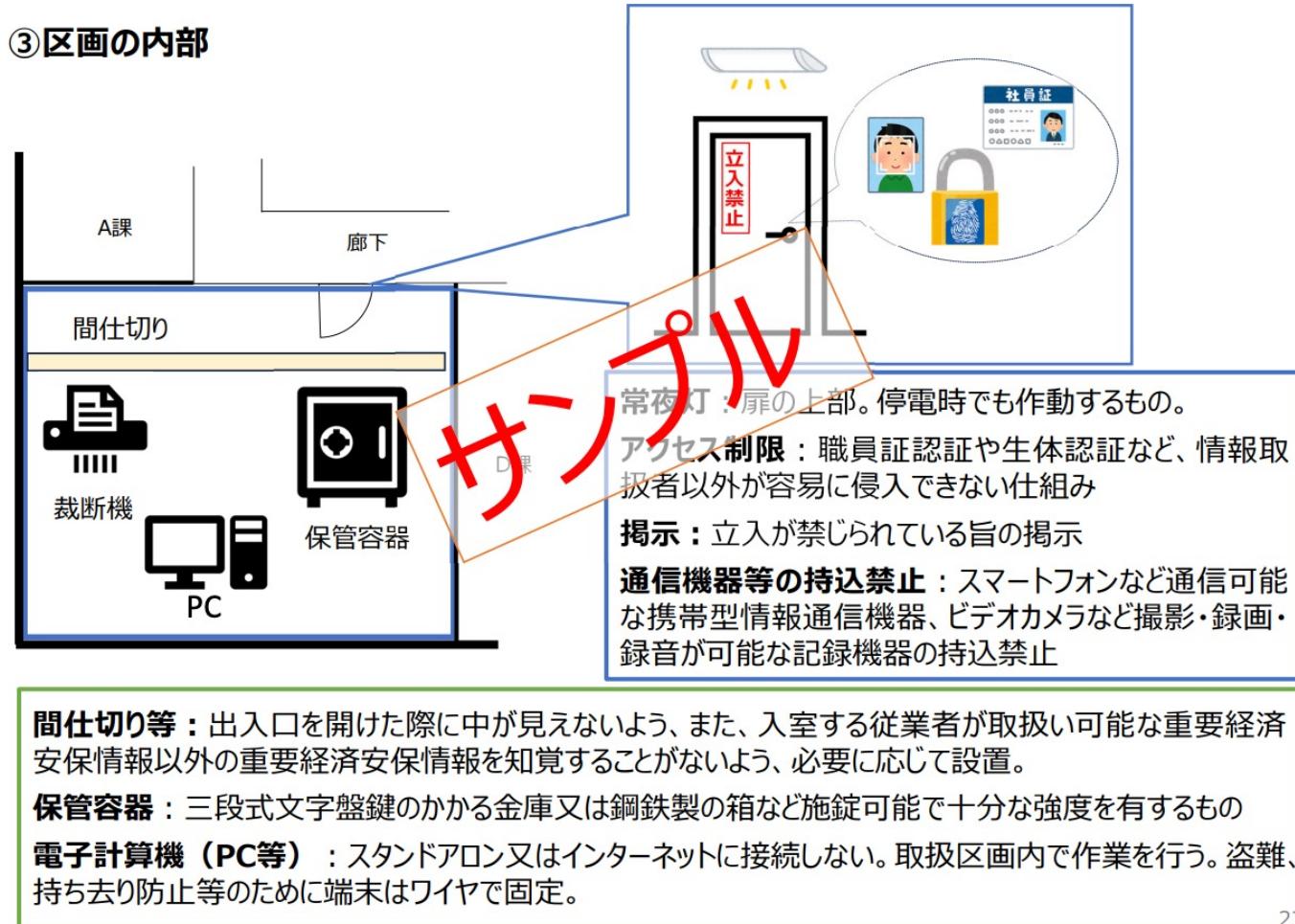
(出典) 内閣府「(適合事業者において重要経済安保情報の取扱いが見込まれる従業者向け)

教育資料ひな型」

22

重要経済安保情報取扱区画のイメージ（2/2）

③区画の内部



(出典) 内閣府「(適合事業者において重要経済安保情報の取扱いが見込まれる従業者向け) 教育資料ひな型」

- 重要経済安保情報は、適性があると認められた者のみがアクセスできる措置（生体認証等）が講じられた、スタンドアローン又はインターネットに接続していない（※）、契約行政機関の承認を得たパソコン等で取り扱うこと。



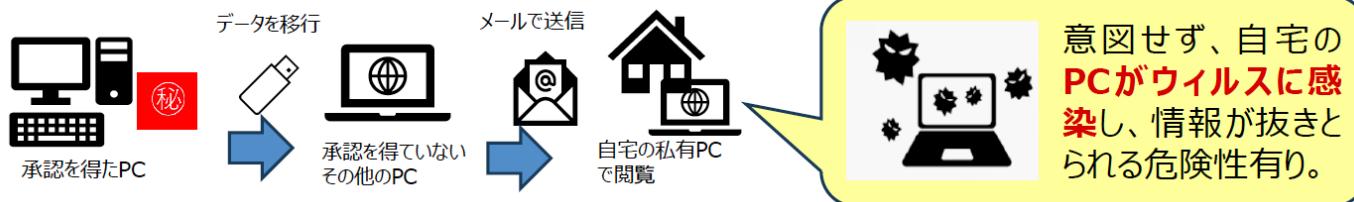
※インターネットやWi-Fiへの接続は不可。



- } ✓ 重要経済安保情報を記録するデータをUSB等に記録する場合には、暗号化を行うなどの保護措置が必要。（安全が確保されていないUSB等は使用しない。）
- ✓ 重要経済安保情報を含むデータのUSB等への書き出し口及び印刷ログを保存。

※重要経済安保情報の不適切な取扱い例

- ・重要経済安保情報の取扱が認められていないパソコンに同情報に該当するデータを移行した。
- ・当該データをメールで私有パソコンに送信し、自宅で閲覧した。



(出典) 内閣府「(適合事業者において重要経済安保情報の取扱いが見込まれる従業者向け) 教育資料ひな型」

■ 経済安全保障推進法

➤ 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保：

- 契約により、設備の製造・開発環境にアクセス可能な要員を物理的（入退室管理等）かつ論理的（データやシステム等へのアクセス制御）に適切に制限することを確認している
- 委託の相手方及び再委託先の相手方等が保有している設計書や設備等の情報について、…要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データやシステムへのアクセス防御）に適切に制限することを確認している。
- 委託の相手方及び再委託の相手方等が重要維持管理等の実施環境において、…要員を物理的（監視カメラ等の入退室管理等）かつ論理的（データやシステム等へのアクセス制御）に制限することを確認している

➤ 特定重要技術の研究開発の促進及びその成果の適切な活用

- 守秘義務登録情報へのアクセス制限及びアクセスログの記録等が行われるように設定された情報端末等を用いる

■ セキュリティクリアランス制度（審査項目）

➤ 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

5. 民間企業は経済安保推進法やセキュリティクリアランス制度の保護アプローチの何を参考にすべきか？

信頼できるステークホルダー間のスター型の重要情報共有モデル

● 守秘義務登録情報の登録(第13条)、取扱い(第14条)、提供(第15条)、受領者からの告知(第16条)

〈守秘義務登録情報の登録・提供フロー〉

1. 提供者は、協議会において法62条7項の守秘義務の対象として扱う情報について、事務局に登録申請 (13条2項)
2. 事務局は、上記申請を受けたとき、守秘義務登録情報として登録して管理 (13条1・4項)
3. 守秘義務登録情報の提供者は、提供する他の構成員等に対し、求め受領確認し、確認がされた後に直接提供 (15条1項)
4. 事務局は、協議会内における守秘義務登録情報の共有状況を管理 (14条2項)

※登録・共有・管理手続きの詳細は情報管理規程に規定

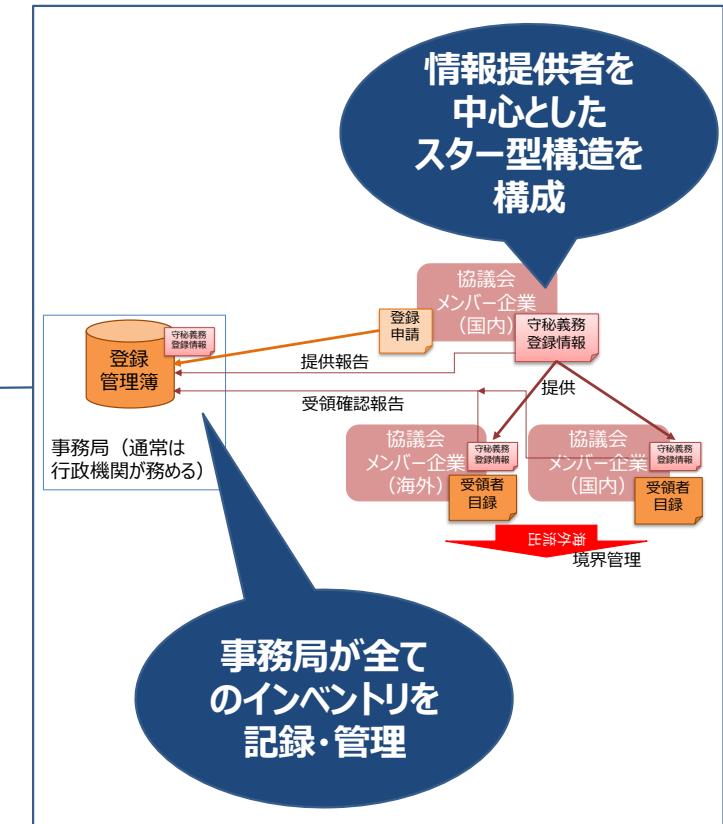
〈守秘義務登録情報の取扱い〉

- ✓ 登録申請時に明示すべき内容 (13条3項)
 - 情報の概要
 - 守秘義務の存続期間 (必要な限度にとどめるよう努める)
 - 情報を共有しようとする構成員等の範囲
- ✓ 未登録の情報は、守秘義務の対象として取扱うことはできない (13条5項)
- ✓ 提供の事前確認時に明示すべき内容 (15条2項)
 - 情報の概要
 - 守秘義務の存続期間 (必要な限度にとどめるよう努める)
 - 情報を共有する構成員等の範囲
 - 守秘義務対象の情報の範囲 (必要な限度にとどめるよう努める)
- ✓ 守秘義務登録情報の提供者が適当と認めた者 (構成員等に限る) の範囲内でのみ共有し、それ以外の者に開示してはならない (14条1項)
- ✓ 取扱いに係るその他事項は、情報管理規程で定める (14条3項)

※破棄や提供者への引き渡し後も守秘義務は継続

〈法人における取扱い〉 (14条1項)

守秘義務登録情報の取扱いは、構成員等である役職員に限る



(出典) 三笠 武則「経済安全保障推進法における重要経済安保情報等の保護対策の骨子」

経済安全保障推進法

特定社会基盤役務の安定的な供給の確保に関する制度では、特定重要設備の導入・維持管理等の委託をしようとする際に事前に国に届出を行い、審査を受ける

- 設備導入や委託が特定妨害行為の手段として使用されるおそれがあるかの審査にあたり、我が国の外部にある主体から強い影響を受けているかを考慮

＜設備供給者・維持管理等委託先・再委託先の届出事項＞

- …住所・設立準拠法
- 議決権の5%以上を直接に保有する者
- 役員の…国籍等
- 外国政府等との取引が売上高の25%以上を占める場合、外国政府等の名称等
- 設備の製造場所の所在地

ほぼ共通の事項

セキュリティクリアランス制度

＜適合事業者の認定における考慮要素＞

- 株主や役員の状況に照らして、事業者の意思決定に関して外国の所有、支配又は影響がないと認められるかどうか

申請事項：

- ✓ …住所・設立準拠法
- ✓ 議決権の5%以上を直接に保有する者
- ✓ 役員の…国籍等
- ✓ 外国政府等との取引が売上高の50%以上を占める場合、外国政府等の名称等
- ✓ 設備の製造場所の所在地

＜適性評価（従業員）における考慮要素＞

- 基本事項（…国籍、帰化歴、…）
- 家族・同居人の氏名等（…国籍、帰化歴等）
- 重要経済基盤毀損活動との関係（重要経済基盤毀損活動との関係、外国政府等との関係、来日外国人への援助等、影響のある外国人との関係、外国政府の職員等からの依頼や誘い、外国の金融機関の口座の保有、外国の不動産の保有、外国政府機関からの給付や免除、外国政府が発行した旅券の保有、海外への居住または渡航）

(出典) 内閣府「経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について」
「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概要」

セキュリティクリアランス制度の適性評価における質問票の項目

本人に対する質問票：

1. 基本事項（氏名、生年月日、国籍、帰化歴、過去10年以内の職歴（勤務期間と離職理由を含む）、過去10年以内の学歴（在籍期間と中退の理由を含む）等）
2. 家族・同居人の氏名等（氏名、生年月日、国籍、帰化歴等）
3. 重要経済基盤毀損活動との関係（重要経済基盤毀損活動との関係、外国政府等との関係、来日外国人への援助等、影響のある外国人との関係、外国政府の職員等からの依頼や誘い、外国の金融機関の口座の保有、外国の不動産の保有、外国政府機関からの給付や免除、外国政府が発行した旅券の保有、海外への居住または渡航）
4. 犯罪および懲戒の経歴（犯罪経歴、懲戒処分）
5. 情報の取扱いに係る非違の経歴
6. 薬物の濫用および影響（違法所持・使用等、有機溶剤の濫用等、薬物の用量超過）
7. 精神疾患
8. 飲酒についての節度（飲酒を原因とするトラブル等）
9. 信用状態その他の経済的な状況（借入れ、滞納、自己破産、クレジットカードの使用停止、民事執行、差押え）
10. その他適性評価手続のために必要な情報（過去の適性評価の経歴）

評価対象者の上司等に対する調査票：

1. 重要経済基盤毀損活動との関係①
重要経済基盤毀損活動を実施又は支援したか
上記活動を行う団体のメンバーである／だったか
同団体を支援している／したことがあるか
2. 重要経済基盤毀損活動との関係②
業務以外で繰り返し連絡を取ったり、会ったりしている外国政府関係者や外国人がいるか
3. 犯罪および懲戒の経歴があるか
4. 情報の取扱いに係る非違の経歴があるか
5. 薬物の濫用および影響が認められるか
6. 精神疾患が認められるか
7. 飲酒についての節度（飲酒を原因とするトラブル等）があるか
8. 信用状態その他の経済的な状況
借入れ、金銭債務不履行、自己の資力に照らして不相応な金銭消費があるか／あったか
9. その他適性評価手続のために必要な情報（過去の適性評価の経歴）

（出典）内閣府「質問票（適性評価）」「調査票（適性評価）」

本資料の内容についてのお問い合わせは下記までお願いします。

合同会社三笠ポリシー・アドバイザリ 代表社員
営業秘密保護推進研究会 事務局長 三笠 武則

(e-mail) takenori.mikasa@mikasa-pa.jp