

技術流出対策ガイドンス

第2版

経済産業省
貿易経済安全保障局 技術調査・流出対策室

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

第0章 はじめに

本ガイダンスの目的

- 技術優位性は、経済安全保障上の観点から、我が国の自律性・不可欠性を維持、強化していく上で、最も不可欠な要素である。また、産業界にとっても、国際競争を勝ち抜き、利益を得ていくための基盤である。これは諸外国においても同様であり、近年、大国間の競争が激しさを増す等国際情勢が不安定化する中で、各国は、大規模な研究開発プロジェクトをはじめとする支援措置や、デュアルユース技術に対する管理強化措置等、技術を巡る施策を強化している
- その中で、国家が主体となって、他国の企業が保有する優れた技術を獲得しようとする動きも加速している。経済産業省が産業界に行ったヒアリングでは、多くの企業から技術流出リスクに直面しているとの声が聞かれる。同時に、役務提供としての技術移転、人材の流出、買収、技術情報の不正取得・開示等多様なケースで技術流出が生じており、その手法も巧妙化しているため、具体的にどのように対処すべきか悩む声も多い。産業界の保有する優れた技術の流出は、我が国の経済安全保障上も深刻な問題であり、産業界自身にとっても大きな経済的損失をもたらすため、官民いずれにおいても、技術流出対策の強化は急務である
- 経済産業省では、外為法に基づき、産業構造審議会安全保障貿易管理小委員会中間報告（令和6年4月）において指摘された技術管理強化のための官民対話スキームを導入する等、規制的手法の強化にも取り組んでいる。しかしながら、技術流出の経路の多様化や手法の巧妙化が常に進んでいる状況において、全ての技術流出リスクに対し、規制的手法によって対処することは現実的ではない。「国が決めた規制さえ遵守していれば良い」と考えている企業は、直ちにこの認識を捨て、自己の利益や信頼を守る観点から、自主的に取組を強化していく必要がある
- 経済のグローバル化が進む現在において、企業の成長にとって、海外の様々な地域における拠点設置、多様で優秀な人材の活用、優れた海外企業との提携等に戦略的に取り組むことが重要である。技術流出を過度におそれ、委縮しては、激しい国際競争を生き残ることはできない。同時に、グローバル市場での成長に伴って高まる技術流出のリスクにも、適切に対処していくことが必要である。技術流出対策は、企業にとって単なるコストではなく、企業活動における将来的なコスト・損失を軽減し、持続的な企業経営を目指す上で必要な投資と認識すべきである（経済安全保障リスクに関して経営者等が認識すべき原則については、経済安全保障経営ガイドライン（第1.0版）も参照）
- 具体的にどのような技術流出対策を行えばよいかは、各企業の置かれた状況や取引の形態によっても様々であり、画一的な正解は存在しない。これが、上述のヒアリングにおける各企業の悩みにもつながっており、ビジネスの過度な委縮をもたらすことも懸念される。このような問題の解決の一助とするため、本ガイダンスでは、想定される様々なビジネスシーンに応じ、どのような技術流出リスクが存在するかを整理し、各企業の好事例等も含め、有効と考えられる技術流出対策を整理し、選択肢として提示する

本ガイドス策定に当たってのスタンス

● 本ガイドスに記載する対策は企業に対する義務付けではない

- 本ガイドスは、あくまで自主的な技術流出対策の選択肢を提示するものであり、外為法を遵守するための義務事項や、営業秘密として保護されるための要件の解説等を行わない
- したがって、本ガイドスに記載した対策を義務付けるものではなく、技術流出の防止という本ガイドスの目的を達成するために、各企業が独自の手法で取り組むことを妨げるものでもない。むしろ、各企業のビジネスに応じて創意工夫を凝らして効果的な技術流出対策を実践することが期待される

● 官民対話に活用する

- 外為法に基づく技術管理対話スキームを含め、技術流出対策を強化するために官民で対話する際に、本ガイドスを参照しながら議論、相談を進める

● 企業に対して完璧を求めない（完璧な技術流出対策は存在しない）

- 完璧な技術流出対策は存在せず、どれだけ対策を講じても技術流出を完全に防ぐことはできない
- したがって、各企業は、技術流出を予防することの重要性を認識した上で、本ガイドスに過剰に依存せず、最大限の努力をするという前提の下で本ガイドスを活用する
- 特に中小企業にとっては、全ての対策を講じることは、リソース面から限界がある。取り組める対策から確実に実行していくことが望ましい

● 本ガイドスは見直し・拡張されていくものである

- 第1版としては、①外為法に基づく技術管理対話スキームが対象とする生産拠点の海外進出に伴う技術流出と、②産業界においても重要課題と認識されている人を通じた技術流出に焦点を当てた
- 第2版としては、第1版の内容をアップデートするとともに、他企業等に対する技術提供を伴う取引として、③共同研究と、④すり合わせに伴う技術流出に焦点を当てた
- また、研究成果の公開を前提とする競争的研究費のうち、一定の研究開発プログラムについては、内閣府主催の「研究セキュリティと研究インテグリティの確保に関する有識者会議」が取りまとめた「研究セキュリティの確保に関する取組のための手順書」に示すリスクマネジメントを実施する必要があるため、参考までに、本ガイドスとの対応関係についても、参考資料としてまとめている
- 完璧な技術流出対策が存在しない以上、本ガイドスは一度策定して完成するものではない。経済産業省では、各企業による独自の好事例の取り込み等、随時アップデートを図っていく

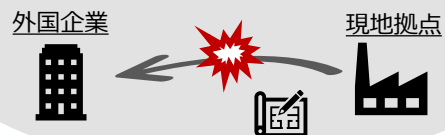
技術流出の経路と本ガイダンス構成の全体像

- 技術流出の経路は、役職員等による営業秘密の持ち出しや、転職等に伴う技術者の社外流出、海外の生産拠点からの流出、共同研究やすり合わせ等における取引相手方からの流出等、多種多様である。また、近時は、国家が主体となって、他国の企業が保有する優れた技術を獲得しようとする動きも加速している
- 事業内容や技術戦略を踏まえて特に管理すべき技術が何か、いかなる流出経路に注意すべきかを見極め、優先順位付けすることが重要

<技術流出の様々な経路（例）>

第2章にて解説

生産拠点の海外進出に伴う技術流出



完全子会社や合併会社の設立、現地企業への製造委託等、様々な手法があるが、現地拠点のガバナンス確保や情報管理が不十分なために、生産技術が流出するケースがある

第3章にて解説

人を通じた技術流出



役職員等が、接待含む不適切な接触等を契機に技術を漏えいしたり、競合他社が、技術獲得を目的に技術者を引き抜くようなケースがある

第4章にて解説

共同研究に伴う技術流出



研究パートナーである企業・大学等や研究参加者の情報管理が不十分であったり、他の企業や大学等との共同研究に流用され、技術流出に至るケースがある

第5章にて解説

すり合わせに伴う技術流出



サプライチェーンの上流・下流に位置する調達元や顧客、またサプライチェーンの外に属する製造装置の調達先等と、仕様調整に係るすり合わせを通じ、自社の技術情報が流出するケースがある

第1章にて解説

各経路に対する共通する対策として、経営層によるリーダーシップと、技術流出対策に関する組織体制の構築、重点的に守るべき技術の特定・評価が重要である

本ガイドスの構成（細目）

第0章 はじめに

- 1 本ガイドスの目的等
- 2 技術流出の経路と本ガイドスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
 - ① 経営層によるリーダーシップとアクション
 - ② 司令塔となる部署の設置
- 2 重点的に守るべき技術の特定・評価
 - ① 重要技術の位置づけを評価
 - ② 自社の競争力の源泉となるコア技術の特定
 - ③ 技術の特徴等に応じた適切な知的財産戦略
 - ④ 営業秘密管理の徹底

第2章 生産拠点の海外進出に伴う技術流出への対策

0 技術流出事例

1 計画前・計画段階において取り組むべき事項

- ① 日本社内の情報管理体制の整備
- ② 相手国の制度の確認
- ③ 相手国の技術的関心の確認
- ④ 相手国の労働法制・慣習・雇用情勢等の確認
- ⑤ 情報管理体制等に関する取引先のデューデリジェンス（DD）の実施
- ⑥ ステークホルダーに対する事前説明

2 契約締結時に取り組むべき事項

- ① 提供する技術の内容等の明確化
- ② 技術情報の取扱いに係る遵守事項の明確化
- ③ 事情変更が生じた場合の対応の明確化
- ④ 契約終了後の手続の明確化
- ⑤ （合弁契約の場合）ガバナンスの確保

3 海外事業の実施段階において取り組むべき事項

- ① 段階的な技術提供
- ② 情報のブラックボックス化
- ③ 技術情報提供後の情報管理の徹底
- ④ 製造設備のメンテナンス管理の徹底

4 撤退・契約終了時に取り組むべき事項

- ① 撤退計画に対応した適切な情報管理の徹底
- ② 製造設備の適切な管理・処分
- ③ 撤退後のフォローアップ

5 その他の取組事項

- ① 海外の研究開発拠点に対する管理の徹底

第3章 人を通じた技術流出への対策

0 技術流出事例

1 技術流出を防ぐために未然に取り組むべき事項

- (1) ルール面での対応
 - ① 情報管理に関するルールの整備・運用の徹底
 - ② 情報管理状況の監査と重要プロジェクトの配置等への反映
- (2) 人事面での対応
 - ③ 情報管理に関する定期的・階層的な研修の実施
 - ④ 法令上必要な事項の採用時確認
 - ⑤ 重要技術を扱う部署への配属に際しての確認
 - ⑥ 副業等を通じた情報流出の防止
 - ⑦ 競業禁止義務契約の適切な活用
- (3) システム面での対応
 - ⑧ アクセスコントロールの徹底
 - ⑨ 退職時のアクセス制限
 - ⑩ デバイスの管理・利用ルールの徹底
 - ⑪ ソフトウェアやSNS等の利用ルールの徹底
 - ⑫ 技術流出に繋がるおそれのある行為の検知・警告

(4) オペレーション面での対応

- ⑬ 工程の細分化・全体工程を知る役職員の限定
- ⑭ 海外出張や赴任時の情報管理
- ⑮ 展示会等を契機とする部外者との接触への対応

2 技術流出した場合に取り組むべき事項

- ① 違反に対する毅然とした対応
- ② 再発防止策の策定・徹底

3 技術者の流出に対して取り組むべき事項

- ① イノベーションを生み続ける（技術の陳腐化の加速）
- ② 優秀な技術者の流出防止
- ③ 退職者との良好な関係の構築

本ガイダンスの構成（細目）

第4章 共同研究に伴う技術流出への対策

0 技術流出事例

1 計画段階において取り組むべき事項

- (1) リスクマネジメントプロセスの導入
 - ① リスクマネジメントプロセスの導入
- (2) 自社における研究体制の確認
 - ② 共同研究に従事する役職員の決定
- (3) テーマ選定における取組事項
 - ③ 技術の重要性を踏まえたリスク評価と研究テーマ選定
- (4) パートナー選定における取組事項
 - ④ パートナー候補のDDの徹底（相手国の観点）
 - ⑤ パートナー候補のDDの徹底（組織の観点）
 - ⑥ パートナー候補のDDの徹底（関与する個人の観点）

2 契約締結時に取り組むべき事項

- ① 事前のNDA締結と段階的な情報開示、NDA締結前の特許出願
- ② 自社の契約書ひな型の活用とリスクに応じた契約条件設定
- ③ 共同研究の目的・テーマの範囲の画定
- ④ 研究参加メンバーや情報の取扱方法の明確化
- ⑤ 提供する技術情報の範囲と、知的財産の帰属等の明確化
- ⑥ 秘密保持義務・競業禁止義務の設定
- ⑦ モニタリング条項の設定と実施による情報管理の確認
- ⑧ 共同研究先の業績悪化・資本変動等に備えた解除事由等の設定
- ⑨ 非公開範囲の設定や、成果公開時の事前承諾手続等の明確化
- ⑩ 契約終了後の情報返却・削除義務の明確化と履行確認
- ⑪ 国外訴訟・法制度リスクへの備え

3 共同研究の実施段階において取り組むべき事項

- ① 研究計画等における情報の利用・管理ルールの明確化
- ② 相手方への情報管理体制強化要請とモニタリングの実施
- ③ 情報アクセス制限と物理的セキュリティ強化による漏えい防止
- ④ 委託先・クラウド利用時の情報管理の徹底
- ⑤ 堅牢なセキュリティ対策の導入や、外部ツールの利用制限の検討
- ⑥ セキュリティ担当者の配置とサイバー防御態勢の強化
- ⑦ 技術流出発生時のインシデント対応計画と対応体制の整備

4 研究終了時に取り組むべき事項

- ① 終了後のモニタリングと文書等の適切な管理
- ② 技術情報やサンプルの返還・廃棄の徹底

第5章 すり合わせに伴う技術流出への対策

0 技術流出事例

1 取引開始前に取り組むべき事項

- ① 取引先のリスク評価を行う
- ② 取引開始前の情報提供の範囲の限定

2 契約締結時に取り組むべき事項

- ① 秘密保持義務・情報の取扱方法等の規定
- ② 資本変動等に備えた解除事由等の設定

3 サプライチェーンの中との連携において取り組むべき事項

- ① サプライチェーンの上流（仕入れ先）に対する情報提供範囲の制限
- ② サプライチェーンの下流（顧客等）に対する情報提供範囲の制限

4 サプライチェーンの外との連携において取り組むべき事項

- ① サプライチェーン外（製造装置メーカー等）との連携時の情報提供制限
- ② サプライチェーン外との連携時における情報管理状況の確認

(参考) 研究セキュリティの確保に関する取組のための手順書について

第1章

各章で共通する技術流出対策

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

1. ① 経営層によるリーダーシップとアクション

- **経済安全保障リスク (技術流出リスクを含む) への対応**は、短期的には対応コストが先行し得るものの、中長期的に損失を抑えるために重要であるが、時に短期的な利潤最大化に相反する経営判断や、大きな経営戦略の変更を伴う可能性もあることから、現場の担当者に判断を委ねることは適切ではない。経済安全保障への対応を重要な経営事項として位置付け、**経営者等自らがリーダーシップを発揮して、自社のリスクに応じた対策の推進を主導する必要がある**。その際、激しい国際競争を生き残っていくことと経済安全保障を両立させるためには、**自社に関わる経済安全保障リスクに過度に萎縮することなく、リスクを適切に把握し対応**することが求められる
- 企業においては、自社の技術優位性・不可欠性を確保するため、中長期的成長の観点からイノベーション創出のための研究開発投資や事業投資等を行うことは言うまでもないが、**自社のコアとなる技術等の喪失・流出を防止するために対策を講じることはますます重要**になっている。このため、本ガイダンスの活用にあたって、まずは「**経済安全保障経営ガイドライン**」(*)を参照しながら、**経営層のリーダーシップの下、全社的な体制を構築の上、取組を進める**

(※) 経済産業省「経済安全保障経営ガイドライン」(https://www.meti.go.jp/policy/economy/economic_security/260123_guideline.pdf)を参照

経営意識

- ✓ 優位性を持つコア技術が海外に流出した場合、他国のキャッチアップが急速に進み、**自社のみならず我が国の産業・技術基盤に影響を及ぼす可能性がある (リスク)**
- ✓ 取引先からの流出リスクも認識し、取引先の技術等の管理体制についても考慮
- ✓ **自社のコア技術や取引先の技術情報等の流出対策は、企業価値向上に貢献し得る (機会)**
- ✓ **自社のコア技術等の管理**が、自社の優位性・不可欠性の確保に直結する**経営課題**である

経営戦略の立案

- ✓ **継続的なイノベーション**を図り、現在のコア技術等がコモディティ化した後も新たな不可欠性の創出を目指す
- ✓ 自社のみならず業界全体の不可欠性確保の観点から、技術等の協調領域を見極めた上で、**業界全体や政府が育成するプロジェクト等に参画することも有用**
- ✓ **攻めの経営戦略を立案する際に、コア技術等の喪失・流出リスクの把握や、流出対策の必要性を検討**
- ✓ **買収や資本提携等を通じてノウハウや技術が流出するリスクも考慮し、上場の是非を含めた資本政策を検討**

体制整備/ ステークホルダーとの対話

- ✓ 技術流出対策を、経営企画・人事・法務等**間接部門も含めた全社的な取組**とし、**横断的な連携体制を整備**
- ✓ 技術者コミュニティの活性化や退職者との良好な関係構築等の**企業風土づくり**も重視。**待遇向上や働きやすい環境整備**も重要
- ✓ 技術流出対策や管理体制について、株主・金融機関・取引先等の**主要ステークホルダーに平時から説明し、理解を得る**

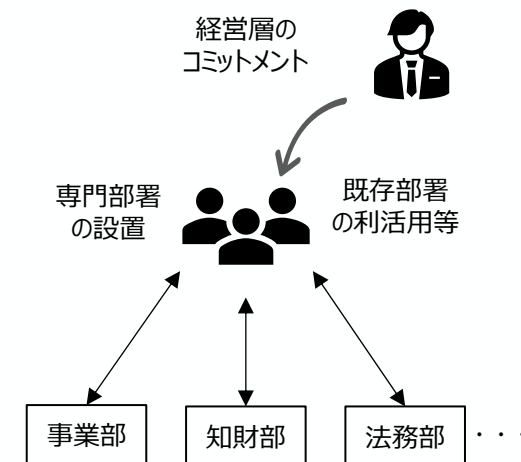
1. ② 司令塔となる部署の設置

- 技術流出対策の強化には、現場の判断に任せきりにするのではなく、**組織横断的な対応が不可欠**
- 関係部署がそれぞれの担当所掌で責任を果たすとともに、既存部署の利活用や機能の拡大、専任部署の新設も含め、技術流出対策の**司令塔となる部署を設置し、部署間を連携させ、全社的な対策を講じることが重要**

対応策の例

① 司令塔となる部署の設置

- 生産拠点の海外進出や共同研究等の具体的な取引や事業遂行では、その計画段階から撤退に至るまで、長期にわたり、事業部門や研究開発部門、管理部門（法務・知財・人事等）をはじめとする多くの部署が関与するが、技術流出リスクの評価がなされないままに進行することを防ぐため、こうした取引に係る情報を収集・管理する体制を整備することが重要である。また、人を通じた技術流出対策においても、役職員が社内ルールに反して研究内容の公表等を行っていないか確認するため、役職員の論文や出版物、副業等の状況に関する情報を収集・管理するとともに、人事部・法務部・情報システム部等複数の部署が連携して実施する必要がある
- そこで、迅速に全社的な対策を講じるため、既存部署（経営管理部門、リスク管理部門、技術統括部門等）の利活用や機能の拡大、専任部署の新設も含め、技術流出対策の司令塔となる組織横断的な部署を設置する
- 部署の設置については、企業の置かれた状況を踏まえて、適切な方法を検討すべきである。例えば、企業グループに属している企業の場合には、グループ全体の所掌範囲等を踏まえて、親会社において部署を設置するのが適切なケースもある。また、本社が海外にある企業の場合には、日本法人に専任部署を設置する必要性等を慎重に検討すべきケースもある
- 各部署から管理職級のメンバーを参画させる等して、専門部署の判断を現場まで徹底させる。また、取引の検討・決裁手続に専門部署を関与させ、手続面からも、その判断が軽視されないようにする
- 重要技術の流出等の緊急事態が発生した場合における連絡・対応についても、専門部署が必要に応じて関与する



※ さらに具体的な民間の好事例については、同「経済安全保障上の課題への対応（民間ベストプラクティス集）—第2.0版— I 経済安全保障上の課題に対応するための組織体制の構築」（https://www.meti.go.jp/policy/economy/economic_security/best_practice2.0.pdf）も参照

② 経営層のコミットメント

- 短期的な利益を求めると、技術流出対策の重要性が矮小化されるおそれがある。専門部署に司令塔としての強いリーダーシップを与え、その判断が尊重されるよう、トップ経営層が関与することが重要

(参考) サイバーセキュリティについて

- 様々なビジネスの現場において、ITの利活用は企業の収益性向上に不可欠なものとなっている一方で、企業が保有する**重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化している。**
- また、サプライチェーンを介したサイバーセキュリティ関連被害の拡大を踏まえた、**サプライチェーン全体を通じた対策の推進の必要性も高まっている。**
- このため、**経営者のリーダーシップの下で、サイバーセキュリティ対策を推進することが重要**である。経済産業省の策定した「**サイバーセキュリティ経営ガイドライン**」では、サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「3原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部（CISO等）に指示すべき「重要10項目」をまとめているため、**参考にされたい。**

(※) 経済産業省「サイバーセキュリティ経営ガイドライン」(https://www.meti.go.jp/policy/netsecurity/mng_guide.htmlを参照)

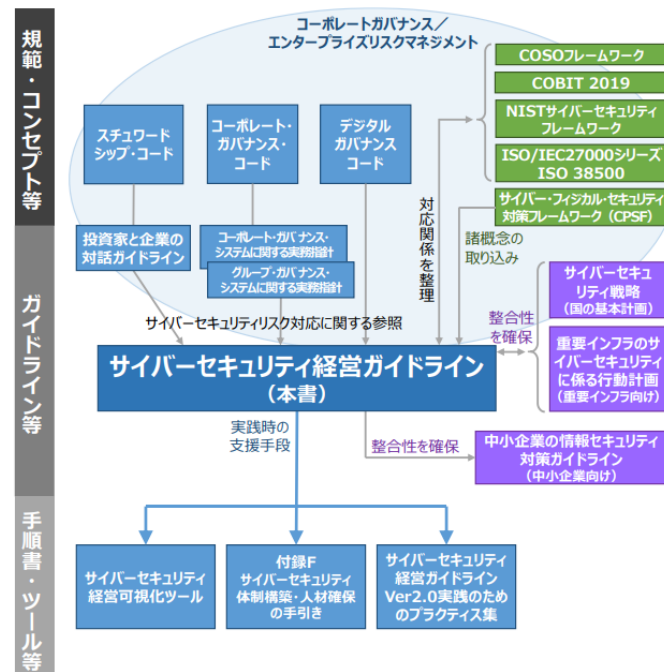
サイバーセキュリティ経営ガイドライン（抜粋）

経営者が認識すべき3原則

- ① 経営者は、サイバーセキュリティリスクが自社のリスクマネジメントにおける重要課題であることを認識し、自らのリーダーシップのもとで対策を進めることが必要
- ② サイバーセキュリティ確保に関する責務を全うするには、自社のみならず、国内外の拠点、ビジネスパートナーや委託先等、サプライチェーン全体にわたるサイバーセキュリティ対策への目配りが必要
- ③ 平時及び緊急時のいずれにおいても、サイバーセキュリティ対策を実施するためには、関係者との積極的なコミュニケーションが必要

サイバーセキュリティ経営の重要10項目

- 指示1 サイバーセキュリティリスクの認識、組織全体での対応方針の策定
- 指示2 サイバーセキュリティリスク管理体制の構築
- 指示3 サイバーセキュリティ対策のための資源（予算、人材等）確保
- 指示4 サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
- 指示5 サイバーセキュリティリスクに効果的に対応する仕組みの構築
- 指示6 PDCA サイクルによるサイバーセキュリティ対策の継続的改善
- 指示7 インシデント発生時の緊急対応体制の整備
- 指示8 インシデントによる被害に備えた事業継続・復旧体制の整備
- 指示9 ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
- 指示10 サイバーセキュリティに関する情報の収集、共有及び開示の促進



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項
- 4 その他の取組事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

2. ① 重要技術の位置づけを評価

- 戦略的に自社の技術を育て、効果的・効率的に技術流出対策を講じるためにも、自社に関わる様々な技術の重要性について、経営戦略等を踏まえながら、評価を行うことが重要。また、技術の重要性や位置づけは、国内外の技術動向等に伴い変化していくことから、評価を適宜見直すことも重要
- 具体的には、①**自社の競争力の源泉となるコア技術**を明確にするとともに、自社の技術が、②**軍事転用懸念のある安全保障上の重要技術**や③**経済安全保障に関わる重要技術**に該当するかどうかを評価し、社内での情報管理に反映させていく必要がある
- また、**破壊的技術革新が進む領域**に関しては、現在、自社が保有していない技術について、海外との共同研究等も通じ、**自社の技術優位性を磨きあげながら、同時に防衛策（技術流出対策）を講じていく必要がある**。このため、④**自社が保有しておらず、獲得をしたい技術**も評価しておく

対応策の例

- 技術の重要性に応じ、技術管理に際しての基本的な考え方を構築することが必要である。重要性の評価に当たっては、以下の4領域における位置付けを整理することが重要である

① 競争力の源泉となるコア技術

- 競争力に直結する技術であるため、権利化・秘匿化の観点も意識しつつ（p21参照）、社内管理に万全を期すとともに、技術保有者の把握や適切な処遇等による対策が必要
- ②・③に位置付けられる技術もあるため、海外移転等を進める場合には、必要に応じて経済産業省や所管省庁に相談することも有用

② 安全保障上の重要技術（軍事転用懸念のある技術）

- 外為法上のリスト規制技術に該当する場合等、我が国の安全保障に影響を与える可能性があるもの。外為法において求められる該非判定等をあわせ、特に慎重な対応が必要

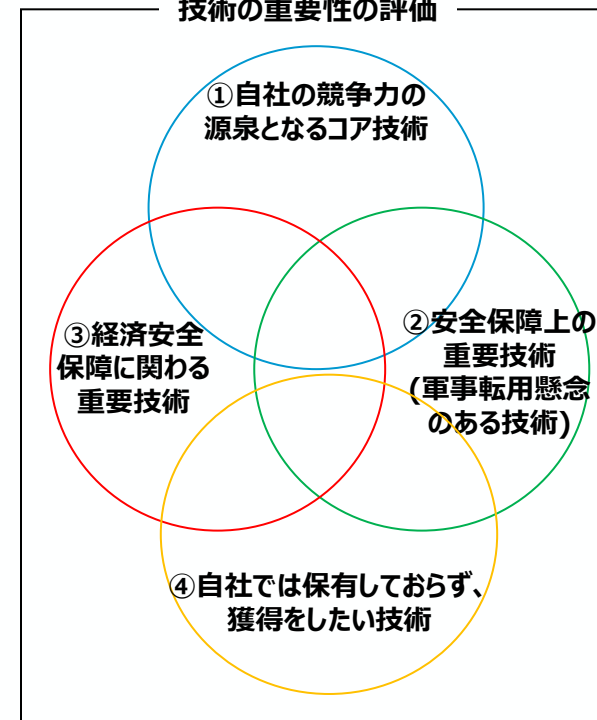
③ 経済安全保障に関わる重要技術

- わが国の経済活動の自律性や不可欠性を確保するために重要な技術。諸外国の獲得対象となっている可能性もあり、第三国からの制裁や取引停止等の関係でも注意を要する。一社の技術流出等の問題が我が国の産業・技術基盤、ひいては国力に影響を与える可能性がある

④ 自社では保有しておらず獲得をしたい技術

- 技術流出対策とイノベーションのバランスをとりながら、共同研究等を通じて、積極的に技術の創出・獲得に取り組む。相手先との関係で、レピュテーションリスクや第三国の法令抵触リスクへの配慮が必要

技術の重要性の評価



2. ② 自社の競争力の源泉となるコア技術の特定

- 企業の研究開発等の活動を通じて生み出す技術情報は膨大であり、その重要度・機微度にも差がある。このため、技術流出を防止するためには、**技術の重要度に応じたメリハリのある対策が肝要**
- 例えば、企業グループ内における技術提供や生産拠点の海外進出等の技術提供を伴う取引を検討する際に、どの範囲で技術提供するかは、経営戦略上の重要な判断。**輸出管理の対象技術に留まらず、自社の競争力上重要な技術（コア技術）を安易に海外に移転しない。**経営戦略上、**海外に移転すると判断する場合も、技術流出対策の一層の徹底が必要。**流出対策に自信が持てないまま**短期的な利益を追求すると、長期的には競争力を失うこと**に繋がりがねない
- いずれの方針を取るにしても、**正しくコア技術を特定することが前提。**これを誤れば、**意図しない技術流出を招き、ビジネスを毀損してしまうおそれもある**

対応策の例

① 自社の競争力の源泉が何であるかを改めて確認する

- 自社の製品のどのような点が市場において評価されているかを確認する。その上で、当該競争力がいかなる要素技術によって実現しているかを分析し、コア技術として特定
- 当該プロセスに、現場の技術者も関与させることで、組織全体の意識啓発も期待できる

② 技術の優位性・重要性を確認する

- 輸出管理の対象であるかに関わらず、優位性や重要性が高いコア技術は、特に狙われやすいことを認識する
- 特定されたコア技術が、他国の企業等において既に保有されている技術あるいは容易に開発されうる技術であるか否かを確認する。併せて、市場における将来性やサプライチェーン上の重要性・不可欠性（チョークポイントをなす唯一無二の技術か）を確認する。また、自社が当該技術を有するに至る経緯（投下した労力や費用、技術開発に至る研究開発活動の独創性等）の確認も有用である

③ 技術が、どの様に存在しているか（形態）を確認する

- コア技術が、どこに、どの様な形態で存在するかにより、自ずと管理手法も変化してくる。技術は、設計図面や配合比率データのようにモノやデータに記載・記録されているケースに限られず、技術者の経験ノウハウのように目に見えないケース、カスタマイズした製造装置に化体しているケース等がある。
- 特に、コア技術が、ソフトウェアやデータ等の無体物として存在している場合には、複製が容易かつ追跡が困難であること、拡散可能性が高く、一度流出した場合に回収することが困難であること等を踏まえて、適切に管理する必要がある。
- コア技術の存在する形態に応じた情報管理を講じるとともに、当該技術を体得している役職員や、その技術に接する立場にある役職員の範囲や地位等も確認することが重要である。その際、当該役職員の特許・論文・所属学会・共同研究関係等の情報も活用して、技術との関係性（キーパーソンかどうか）を継続的に評価することも重要である。

(参考) 安全保障に関連する技術の確認①

- 外為法に基づくリスト規制技術と官民対話スキームの対象技術
 - 外国為替令別表1～15項に定める技術
 - ※「貨物・技術のマトリクス表」(https://www.meti.go.jp/policy/anpo/matrix_intro.html)も参照。
 - 貿易関係貿易外取引等に関する省令第十条第三項の規定に基づく重要管理対象技術(<https://www.meti.go.jp/policy/anpo/anpo08.html>を参照)
 - ※ 外為法では、必要な許可を取得しないで、規制対象である貨物の輸出や技術の提供を行った場合など、法令の規定に違反した場合に、「刑事罰」や「行政制裁」が科されるほか、行政指導である「警告」や「経緯書・報告書の提出」などがある。安全保障貿易管理の概要については、以下を参照。
<https://www.meti.go.jp/policy/anpo/gaiyou.html>
- 対内直接投資審査制度における事前届出の対象となる業種を営んでいる場合には、当該業種に係る技術(https://www.mof.go.jp/policy/international_policy/gaitame_kawase/fdi/index.htmを参照)
- 経済安全保障推進法に基づく、特許出願非公開制度における保全審査の対象となる特定技術分野（公にすることにより外部から行われる行為によって国家及び国民の安全を損なうおそれが大きい発明が含まれ得る技術）(https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/patent.htmlを参照)
- 防衛装備庁「防衛技術指針2023」で示された、将来の防衛力強化に向けて重点的に研究開発を進めるべき12の重要技術分野
①無人化・自律化、②新たなプラットフォームの活用、③新たなエネルギーの活用、④新機能素材・新製造手法、⑤センシング技術、⑥コンピューティング技術、⑦「見えなかったもの」を見える化する技術、⑧架空情報を現実のように見せる技術、⑨未来予測と判断能力強化、⑩ネットワーク技術、⑪サイバー防衛技術、⑫認知能力の強化
(<https://www.mod.go.jp/atla/guideline2023/technical/index.html>を参照)

(参考) 安全保障に関連する技術の確認②

- 米国輸出管理規則（EAR : Export Administration Regulations）で対象とされる技術（CCL（Commerce Control List））

(<https://www.bis.gov/regulations/ear>を参照)

※なお、日本企業であっても、EAR対象技術の開示が、再輸出・みなし再輸出として規制される可能性がある点には留意する。

(https://www.jetro.go.jp/ext_images/world/security_trade_control/pdf/guide/202401_v2.pdfを参照)

- 米国 対外投資規制で対象とされる技術（半導体・マイクロエレクトロニクス、量子情報技術、人工知能）

(<https://home.treasury.gov/news/press-releases/jy2687>を参照)

- EU デュアルユース規制で対象とされる技術（デュアルユース品目リスト（Annex I））

(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202402547を参照（2024年改正））

(参考) 経済安全保障に関連する技術の確認①

経済安全保障の観点からは、国家の自律性、不可欠性に関する技術については、詳細に特定することで広く各国の関心対象となり得るため、特定することは困難であるが、その外延を把握するためには、以下のようなソースを参照することが有益

- 経済安全保障推進法第7条に規定する特定重要物資

(https://www.cao.go.jp/keizai_anken_hosho/suishinhou/supply_chain/supply_chain.htmlを参照)

- 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及び経済安全保障重要技術育成プログラム (K Program)において支援対象とする重要技術 (中長期的に我が国が国際社会において確固たる地位を確保し続ける上で不可欠な要素となる先端的な重要技術)

(https://www.cao.go.jp/keizai_anken_hosho/suishinhou/doc/kihonshishin3.pdfを参照)

(https://www8.cao.go.jp/cstp/anken_anshin/kprogram.htmlを参照)

- 重要経済安保情報保護活用法第2条第4項第2号に規定する重要経済基盤に関する革新的な技術に該当しうる情報でもある重要経済基盤を防護するための革新的技術 (例えば、基盤公共役務の提供や重要物資の供給網を支える施設・設備等を防護するための革新的なサイバーセキュリティ技術等) (https://www.cao.go.jp/keizai_anken_hosho/hogokatsuyou/hogokatsuyou.htmlを参照)

- 重要技術領域

第7期科学技術・イノベーション基本計画において、我が国における重要技術領域として、新興・基盤技術領域と国家戦略技術領域の2領域を設定している。(<https://www8.cao.go.jp/cstp/kihonkeikaku/index7.html>を参照)

- 新興・基盤技術領域

総合的な安全保障などの動向・情勢や日本の科学技術の立ち位置も踏まえつつ、急速に発展しつつあり、将来の日本の科学技術をけん引するような潜在力を有する新興技術や基盤技術の領域

- 国家戦略技術領域

将来の日本の自律性・不可欠性の確保、将来性のある成長産業の創出を進めることを目指し、一気通貫支援によって科学と産業を結び付け、関連する人的・物的資源を国内に確保していくことを目指すべき技術領域

新興・基盤技術領域

- ① 造船
- ② 航空
- ③ デジタル・サイバーセキュリティ
- ④ 農業・林業・水産 (フードテックを含む。)
- ⑤ 資源・エネルギー安全保障・GX
- ⑥ 防災・国土強靱化
- ⑦ 先端医療
- ⑧ 製造・マテリアル (重要鉱物・部素材)
- ⑨ モビリティ・輸送・港湾ロジスティクス (物流)
- ⑩ 海洋
- ⑪ 防衛産業

国家戦略技術領域

- ⑫ AI・先端ロボット
- ⑬ 量子
- ⑭ 半導体・通信
- ⑮ バイオ・ヘルスケア
- ⑯ フュージョンエネルギー
- ⑰ 宇宙

（参考）経済安全保障に関連する技術の確認②

- EUが選定した経済安全保障のための重要技術分野（Economic Security Strategy）

技術セキュリティと技術流出に関するリスクを評価する対象となる10の重要技術のリストを選定。

①先端半導体技術、②人工知能技術、③量子技術、④バイオ技術、⑤先端接続性、ナビゲーション、デジタル技術、⑥先端センサー技術、⑦宇宙、推進技術、⑧エネルギー技術、⑨ロボット工学、自律システム、⑩先端材料、製造、リサイクル技術（中でも①～④は最も深刻な技術漏えいリスクがあるとされた）

（https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_enを参照）

- 米国大統領府科学技術政策局が発表した重要・新興技術（critical and emerging technologies : CETs）

先進コンピューティング、先進工学材料、先進ガスタービンエンジン技術、高度かつネットワーク化されたセンシングとシグネチャ管理、先進製造、人工知能、バイオテクノロジー、クリーンエネルギーの生産と貯蔵、データプライバシー・データセキュリティ・サイバーセキュリティ技術、指向性エネルギー、高度に自動化された自律・無人システムとロボティクス、ヒューマンマシンインターフェース、極超音速、統合通信・ネットワーク技術、測位・航法・タイミング技術、量子情報および実現技術、半導体およびマイクロエレクトロニクス、宇宙技術・システム

（<https://bidenwhitehouse.archives.gov/ostp/news-updates/2024/02/12/critical-and-emerging-technologies-list-2024-update/>を参照）

2. ③ 技術の特徴等に応じた適切な知的財産戦略

- 技術情報を秘匿・ブラックボックス化し、徹底して流出対策を強化するクローズ戦略と並び、特許等による知的財産（知財）権の獲得や、プラットフォームを獲得するといった戦略も重要
- クローズ戦略と戦略のいずれを取るかは経営戦略上の判断であるが、技術特性や競合他社の開発動向等を踏まえて判断しなければ、守るべき技術を誤って流出させてしまうおそれがある

対応策の例

① 権利化・秘匿化の適切な選択基準を持つ

- 権利化・秘匿化のメリット・デメリットを理解し、選択の判断基準を社内で整理する
- 一般的には、組成・形状等侵害を発見しやすい場合は権利化し、製法のノウハウ等侵害が発見しにくい場合は秘匿化するケースが多い。また、競合他社との技術格差が大きくなく、短い期間でキャッチアップされると考える場合は、権利化するケースが多い。一方で、競合他社のキャッチアップに時間を要することが見込まれる場合や、製品のライフサイクル等に鑑みて、特許権の存続期間よりも長く技術を保護したい場合等は、秘匿化するケースもある
- 特許出願する場合は、ターゲットとする市場や製造委託先の国等も踏まえた、出願国の適切な選択も重要
- 経済安全保障推進法に基づく、特許出願非公開制度の対象となる特定技術分野については、同制度に基づく保全審査や保全指定が行われうる点には留意が必要である。必要に応じて、外国出願禁止の事前確認制度の利用も検討する

② 職務発明者や競合他社による特許化への対応

- 社内技術者の職務発明の成果がコア技術になる場合も多いが、技術者が退職後に自ら特許出願する場合もある。退職後の扱いも含め、職務発明規程を整備し、自社が特許を受ける権利を取得することが必要。また、特許法の定めに沿った相当の利益の付与も必要（p100参照）
- 特許を取得した技術について他社による権利侵害が判明した場合は、迅速に法的措置を講じることが重要
- 流出した技術について他社が特許出願する場合もある。事実実験公正証書を作成する等して先使用権を主張立証するための証拠化を行うことも検討に値する

③ 特許明細書等の記載の工夫

- 特許出願時の書類は公表されるため、秘匿化すべき関連技術がある場合には、明細書に記載しない等の工夫をする。また、特許出願する技術についても、出願前に情報が流出しないよう秘匿化を徹底する

④ 秘密管理の徹底

- 秘匿化を選択した場合は、不正競争防止法の保護を受けられるよう、営業秘密管理を徹底する
- 他方、同法による保護は事後的な被害回復にとどまるケースもあるため、営業秘密管理として求められる事項に留まらず、本ガイダンス等も参考としつつ、可能な限りの流出対策を講じることが重要

※下記資料も参照されたい。

- ・特許庁「特許出願非公開制度について」
<https://www.jpo.go.jp/system/patent/shutugan/hikokai/index.html>
- ・特許庁「中小企業向け職務発明規程ひな形」
https://www.jpo.go.jp/system/patent/shutugan/shokumu/shokumu_cyusyou.html
- ・特許庁「先使用権制度事例集」
<https://www.jpo.go.jp/system/patent/gaiyo/senshiyo/index.html>
- ・経済産業省「営業秘密管理指針」
<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

2. ④ 営業秘密管理の徹底

- 自社の重要技術のうち、特許取得せず、オープンにもしない重要技術については、**営業秘密管理を徹底する**
- 仮に流出した場合に、不正競争防止法に基づく対応を講じることができるよう、**必要最低限の前提として、営業秘密として法的保護を受けるために必要な水準の秘密管理措置を行う必要がある**

対応策の例

① 秘密管理性が認められるような情報管理を行う

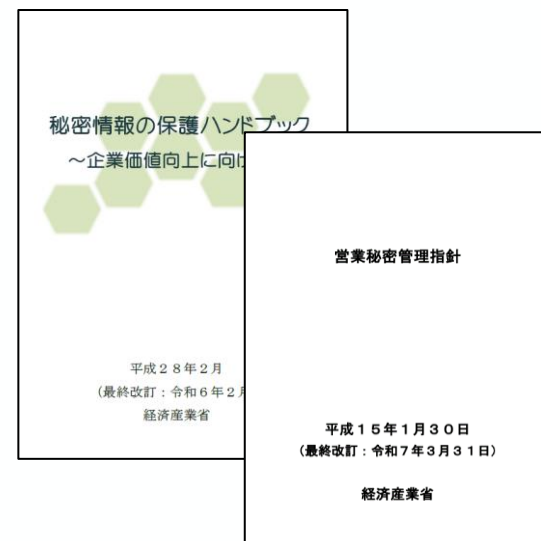
- 営業秘密として法的保護を受けるためには、適正な営業秘密管理が行われていることが前提となる。その上で、従業員等に対して、組織として営業秘密管理を行っている意思を明確に示すとともに、従業員等がその意思を認識できる状態を確保する必要がある
- 秘匿化すべき重要な技術が、技術者の経験やノウハウ等の目に見えない形で存在する場合、営業秘密として保護するためには、原則として、その内容を可視化することが必要となる。しかし、必ずしも内容そのものが可視化されていなくとも、当該情報の範囲・カテゴリーを口頭や書面で伝達することで、従業員の認識可能性を確保できると考えられるケースもある。

② 秘密情報の分類を行う

- また、技術流出を防止するためには、法的保護を受けるために必要となる最低限の水準を超えた技術流出対策を講じることが重要。その前提として、秘匿化する技術情報について、メリハリを受けた管理を講じることができるよう、情報の内容・性質やその評価の高低等に応じ、秘密情報を同様の管理水準であると考えられるものごとに分類することが重要（極秘・部外秘・社外秘等）

③ 立証を意識してセキュリティシステム等を導入する

- 仮に技術流出が発生した場合、秘密管理措置が講じられていることを前提に、毅然とした対応をとることが重要
- 訴訟等となった場合には、営業秘密侵害等の要件を立証する必要がある。秘密管理措置の実施にあたっては、後日の訴訟等における立証を見据えて、客観的な証拠保全が可能な情報セキュリティシステム等の導入も検討する。
- また、書面化・証拠化の際には、公証制度やタイムスタンプの利用等を検討するとともに、弁護士や弁理士等の専門家の助言を得ることも有用



※本ガイダンスでは、不正競争防止法上の秘密管理措置の内容に関する具体的な解説は行わない。不正競争防止法による保護を受けるために必要となる最低限の水準の対策を示す「営業秘密管理指針」や、様々な対策例を紹介する「秘密情報の保護ハンドブック ～企業価値向上にむけて～」も参照されたい

<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

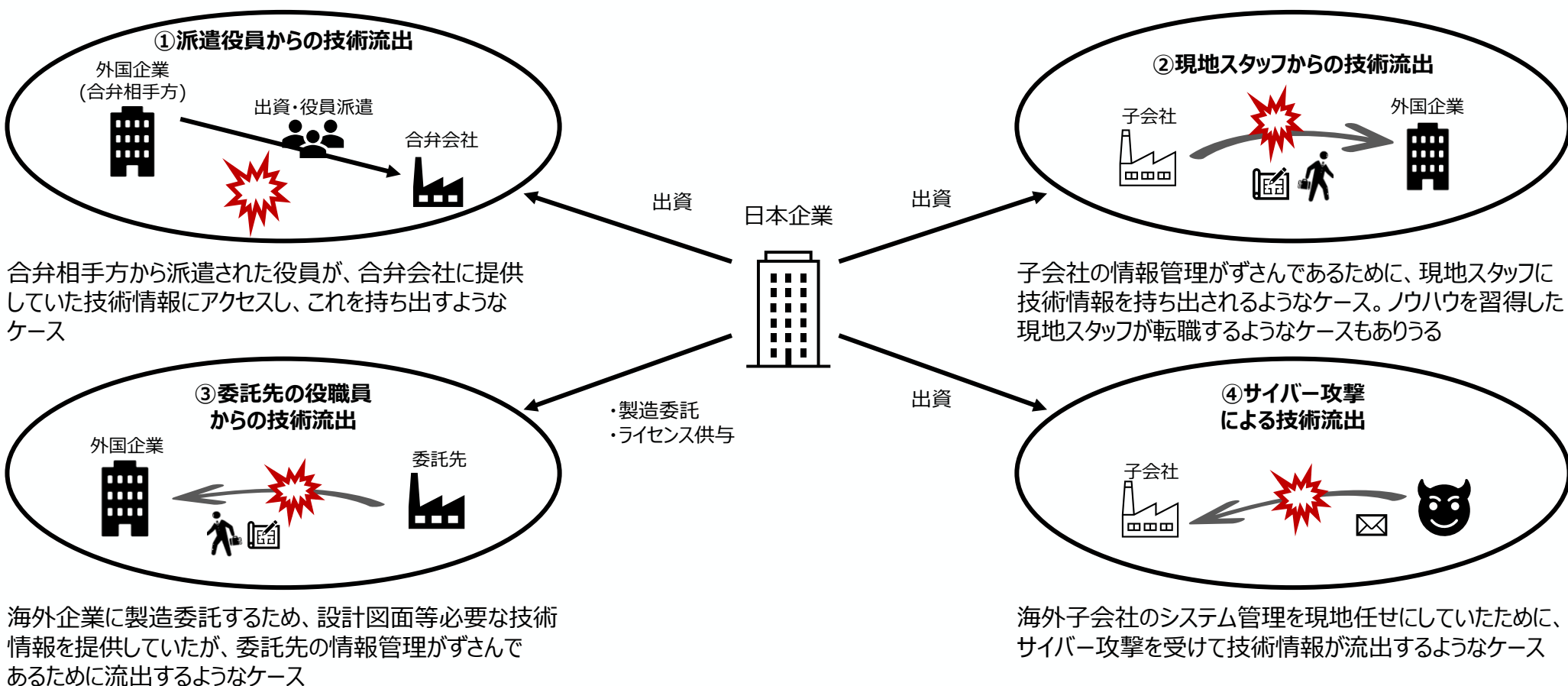
第2章

生産拠点を海外進出に伴う技術流出への対策

第2章が想定する技術流出のケース

- 第2章では、日本企業が、海外拠点での生産及び製品開発を行う場合を想定した技術流出対策を記載している。典型的には、子会社や現地企業との協力による合併会社を設置するケースや、現地企業に対して生産委託・ライセンス供与等を行う場合を想定している

<生産拠点の海外進出に伴う技術流出ケース (例)>



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
 - 1 計画前・計画段階において取り組むべき事項
 - 2 契約締結時に取り組むべき事項
 - 3 海外事業の実施段階において取り組むべき事項
 - 4 撤退・契約終了時に取り組むべき事項
 - 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
 - 1 技術流出を防ぐために未然に取り組むべき事項
 - 2 技術流出した場合に取り組むべき事項
 - 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
 - 1 計画段階において取り組むべき事項
 - 2 契約締結時に取り組むべき事項
 - 3 共同研究の実施段階において取り組むべき事項
 - 4 研究終了時に取り組むべき事項

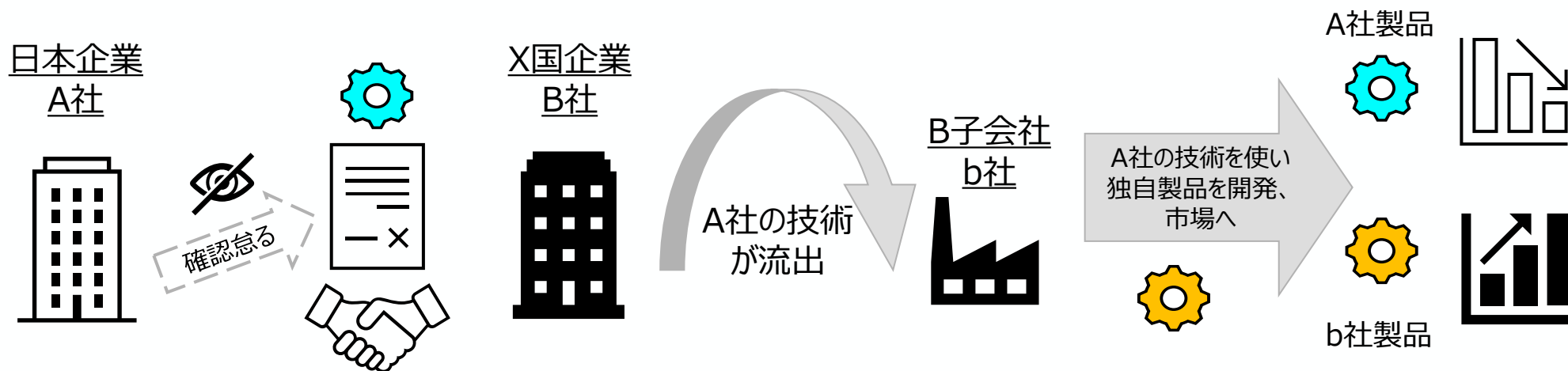
第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
 - 1 取引開始前に取り組むべき事項
 - 2 契約締結時に取り組むべき事項
 - 3 サプライチェーンの中との連携において取り組むべき事項
 - 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

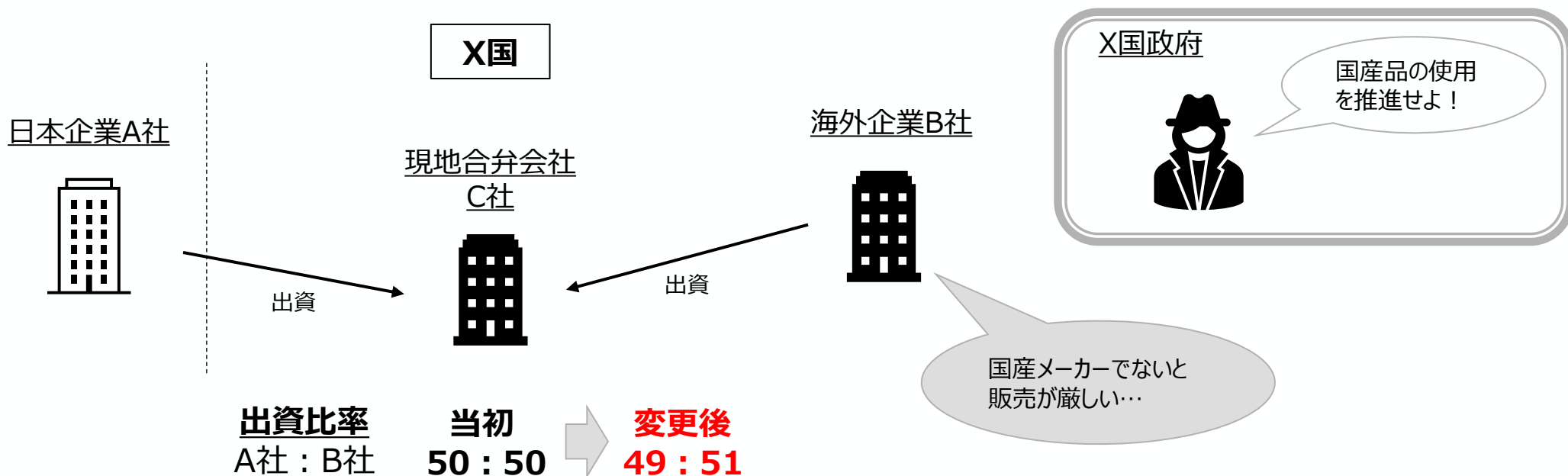
Case1: ライセンス契約先からの技術流出

- 日本の中堅企業A社は、X国企業のB社に対する技術供与のライセンス契約を締結した
- しかし、A社は国際展開に不慣れだったため、B社が説明するX国の法制度や商慣行を鵜呑みにし、**契約内容の精査を怠った**。また、B社に対する監視を含め、**技術流出対策については特段の対応を行っていなかった**
- 数ヶ月後、B社の子会社であるb社が、**A社の技術を使用し、独自製品を開発していることが発覚**。A社は抗議したが、**B社は「契約の範囲内」と主張**
- **A社は瞬く間にシェアを奪われ、契約解除を進めたが、法的手段を講じても既に取り返しが見つからない状況**になってしまった



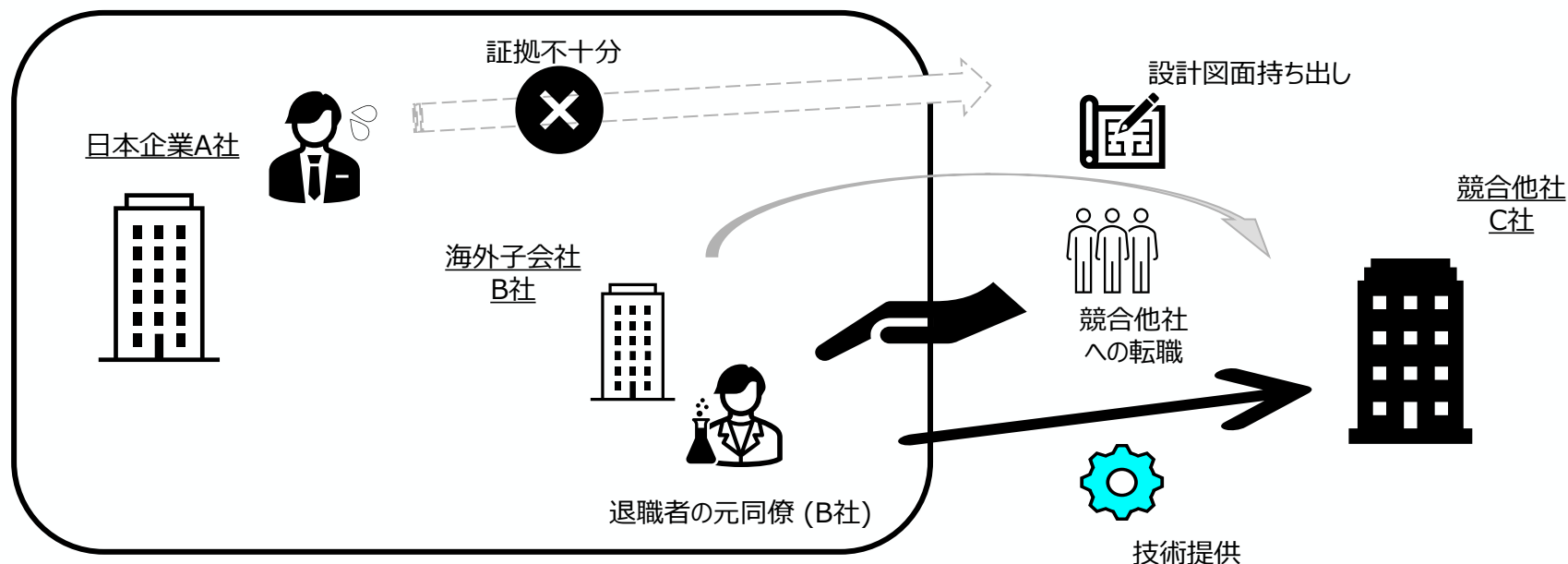
Case2: 合併会社設立後、出資比率の変更に伴う技術流出

- **日本企業A社**は、**X国企業B社**から誘致を受け、**現地製造のための合併会社C社**を設立。C社に対する**出資比率**は、**A社とB社が50%ずつ**であり、**A社からC社に製造技術を提供**
- C社の生産開始後、突如としてB社から、「政府の国産化推進の指導もあり、国産メーカーでなければ顧客への販売が不利になる。B社の出資比率を過半にしなければ、外国メーカーとして扱われる。」と通告され、**出資比率の変更を求められた**
- A社は、既にC社に対する多額の投資を行っていたため、撤退という選択は困難であった。最終的に、**経営の主導権をB社に譲るとの判断**をせざるを得なくなった



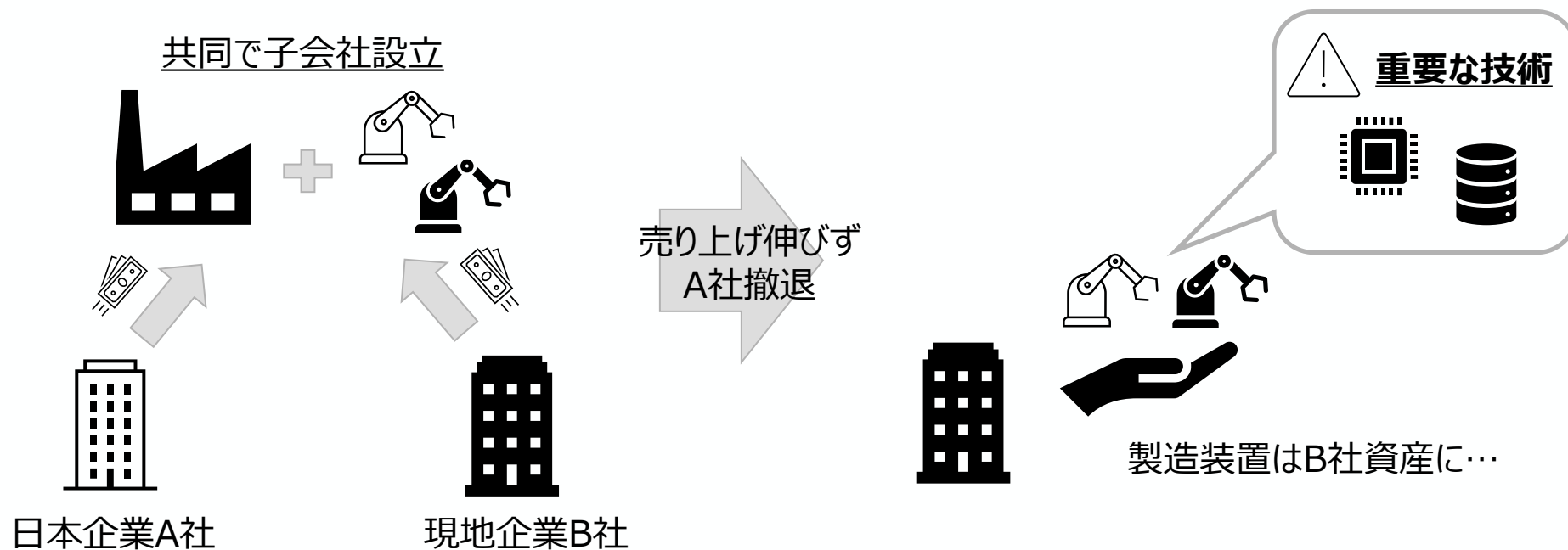
Case3: 海外子会社の従業員からの流出

- 日本企業A社は、海外製造のために、**現地子会社のB社を設立**し、順調に売り上げを伸ばしていた
- ある時期を境に、**B社の従業員の退職が相次ぎ、多くが現地の競合他社C社へ転職**するという事態が発生。その後、**C社は、B社の類似製品を量産**するようになった
- 原因を調査したところ、転職者の一部が、退職時に、**B社から設計図面を持ち出していた**ことが判明。また、退職後も**B社の元同僚をそそのかして、継続的に技術情報を提供**させていたことも発覚
- A社は当該国の不正競争防止法に基づく訴訟提起を検討したが、そもそも**営業秘密管理がずさん**だったために、訴訟は困難との結論になった



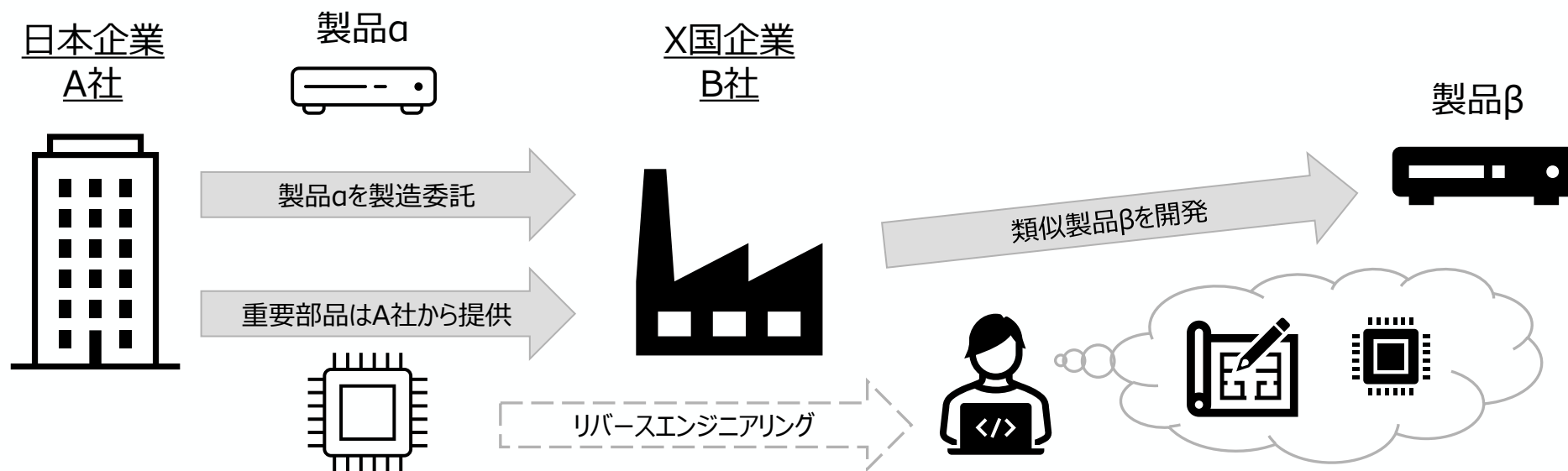
Case4: 撤退時の技術管理不足による流出

- 日本企業A社は、海外の取引先から現地生産を強く求められていたが、**新規拠点を立ち上げる投資余力がなかった**
- この中で、**現地企業Bから、設備投資に係る費用を負担するとの提案**があり、B社と共同で子会社を設立することとなった
- その後、思うように販売実績が伸びず、A社は撤退を決意。撤退にあたり、**重要な技術が化体されている製造装置を廃棄しようとしたが、出資時にB社の資産となっていたために廃棄することができず、B社が当該装置を引き継いで使用することとなった**



Case5: 製造委託先からの技術流出

- 日本企業A社は、製造コストを下げるため、**X国企業B社に製品αの製造を委託**することを決めた
- 技術流出には特に注意し、**製品のコアとなる重要な素材や部品はA社から提供**することにし、最終加工及び組立のみを委託することにした
- しかし、数ヶ月後、**より安価な類似製品βにより、X国のシェアが奪われ始めた**。販売元を調べると製造委託先のB社であった。A社はB社に抗議したが、B社は「**独自開発品である**」と主張した
- B社は、A社から提供された**部品をリバースエンジニアリング**し、類似品の製造を行うだけの技術を手に入れていた



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

1. ① 日本社内の情報管理体制の整備

- そもそも、日本の本社において適切な情報管理体制が構築できていなければ、海外拠点における**管理も望めない**。本社が主導し、グローバル展開を意識した社内規程等を整備する必要がある
- また、規程を整備しても、役職員に周知され、実行されなければ意味がない。**社内教育を徹底した**上で、役職員に対して**確認や誓約等を求め、定期的に更新していくことも重要**
- さらに、監査等を通じて、**社内での実施状況を継続的にモニタリング**するとともに、**違反事例や他社の最新の取組に関する情報を収集し、規程や研修内容等に反映させていくことも有益である**

対応策の例

① 情報管理規程を整備する

- 本社において、海外拠点を含む全社スタンダードとしての情報管理規程を整備する。拠点や業務により特殊事情がある場合、追加規程を設ける
- 近年は、生成AIの活用等も進展しており、AIを利用する際のルールを追加する等、業務のあり方の変化に合わせて不断の見直しも必要

② 教育・研修及び確認を行う

- 全拠点において、役職員に対し、最新の社内規程に基づく定期的な教育・研修を実施する。拠点に出入りする業者等技術情報に関わる全ての関係者を対象とすることが望ましい
- 教育・研修の実施後は、内容を理解したことの確認プロセスを設けるとともに、規程を遵守することについて、誓約等を求め、更新していく

③ 最新情報を常に反映していく

- ルールは常に見直しが必要。違反事例があった場合は勿論、他社の好取組等も含め、社内規程や研修内容等を不断に見直ししていくことが必要



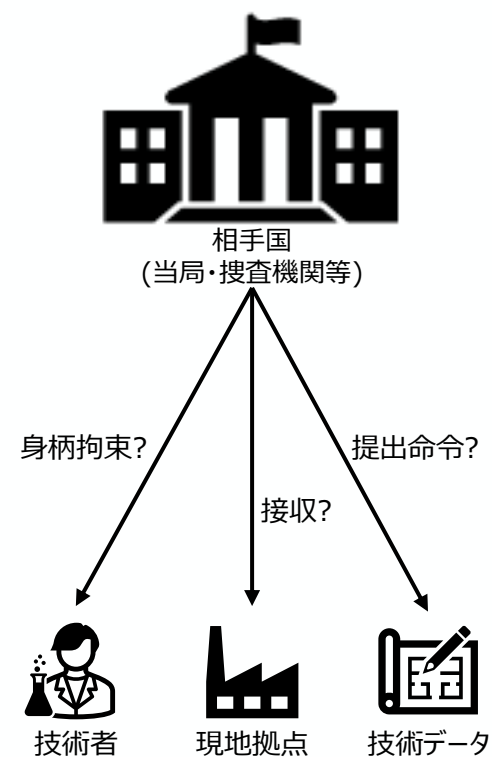
1. ② 相手国の制度の確認

- 国によっては、安全法令、環境法令、競争法令等を根拠に、**技術情報の開示**を求められることがある。また、政治的混乱の際に、**現地拠点の土地や設備を接收**される場合もある
- 技術移転しようとする相手の国が**どのような制度を持ち、運用しているか**、**地政学リスクがどの程度あるか**等について、事前に精査することが重要

対応策の例

① 相手国の制度を確認し、リスクを分析する

- 運用実態を含め、以下のような技術流出につながる相手国政府の制度を確認する。専門知識を要するため弁護士等の活用も検討する。中小企業等自社だけでの対応が困難なケースでは、業界団体や公的機関等の提供する情報も参考にする。迷う場合には、経済産業省等への相談も検討する。
 - ✓ 安全規制、環境規制、競争法関連の許認可・審査プロセス等において、公的機関に対する技術データ等の提出が求められる可能性があるか
 - ✓ 有事等に、施設や設備が差し押さえられる可能性があるか
 - ✓ 技術者を拘束される可能性があるか
 - ✓ 自国企業を優遇するような契約条件を強制される可能性があるか
 - ✓ 外資比率が高い場合に補助や調達等で不利に扱われる可能性があるか
 - ✓ 現地で訴訟になった際に設計図面等の提出が義務づけられる、または訴訟記録として公開される可能性があるか
 - ✓ 外国政府等による情報収集活動に協力する義務を課す法令等が存在するか



② 現地情勢や法制度以外のルール・慣行も確認する

- 現地の情勢や地政学リスクに関する情報、法制度ではないものの技術流出に繋がりうる取引慣行等も収集する。駐在員や現地コンサル企業等を活用する。業界内の情報共有や、公的機関等が提供する情報も有効である
- なお、相手国の法令等によっては、現地での情報収集が困難な場合もあるため、留意が必要

1. ③ 相手国の技術的関心の確認

- 経済安全保障の重要性が高まる中、各国が、国産化や技術優位性の強化を目指している。相手国政府が、**国産化等を強く主導する技術分野**では、技術流出リスクが高まるおそれがある
- 移転しようとする技術が、**相手国の政策**にどのように位置づけられているか、補助制度等**具体的な施策**の実施状況を含め精査することが重要

対応策の例

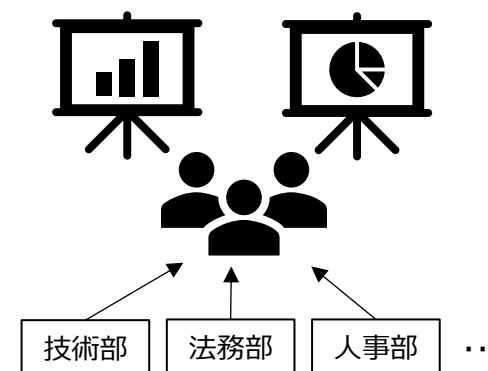
① 社内横断的な情報収集・分析体制を整備する

- 相手国の産業政策等を、各事業部門が単独で、その都度確認することは困難かつ非効率。また、生産拠点の海外進出に関するプロジェクトが、複数の事業部門で同時進行する場合もある
- そのため、社内横断的に、主要各国の技術的関心について情報収集・分析を行う体制を整備する (p12参照)

② 公的機関等との連携を通じた相手国・取引先の情報収集

- 自社のみで収集できる情報には限界があるため、業界団体や公的機関等との連携や、経済産業省への相談等により、相手国の産業政策に関する情報を継続的に収集・分析する
- 取引先と相手国政府との関係性についても確認を行う。特に、資本関係、公的支援の有無等、政府からの支配関係に留意する。その手法として、HP等の公開情報、取引先のデューデリジェンス (DD)(p36参照)のほか、公的機関等とも連携して情報を収集する (この際、重要経済安保情報に指定されるような情報の提供が有効と政府が判断し、企業としても、セキュリティ・クリアランス制度が有益と判断した場合は、同制度の活用も検討する)

社内横断的な
技術的関心の情報収集・分析



業界団体・公的機関との連携、
経済産業省への相談



1. ④ 相手国の労働法制・慣習・雇用情勢等の確認

- 海外では、労働法制や慣習、賃金体系、技術者の流動性等が日本とは異なる。こうした労働環境の違いを正しく理解し、現地に即した経営を行わなければ、法令違反のおそれのみならず、**現地スタッフの不満や技術管理に関する認識の相違**に起因し、意図しない技術流出が生じるおそれもある
- こうした違いを正しく把握するための情報収集を行うとともに、**相手国の制度や文化に合った適切な教育や意思疎通**を図る必要がある

対応策の例

① 相手国の労働法制等の確認

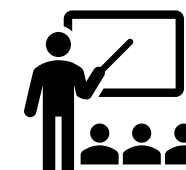
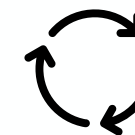
- 相手国の労働法制や労働慣習、労働市場の動向について事前に調査する。特に、労働法制については法令遵守の観点から確実に把握・理解することが必須。必要に応じて現地法令に詳しい専門家やコンサルタントも活用し、最新の情報収集に努める



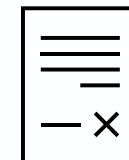
制度に関する調査・分析

② 相手国の労働慣習等を社内規程や研修等に反映する

- 技術流出リスクへの対応の観点からは、労働法制の遵守だけでは不十分。日本本社で使用している教育・研修プログラムについて、現地の文化や労働慣習を考慮してカスタマイズすべき点がないか確認し、反映する
- 雇用契約や社内規程に、技術流出対策に関する具体的なポリシーを明文化し、従業員にその意義を理解させる。流出時の責任やペナルティを明記することで、意識を高める
- 日本ならば常識、当たり前であることも、他国では通用しないことが多い。技術情報の重要性や取扱手順等、初歩から具体的に説明する



研修の実施



契約内容への明文化

③ 相手国の雇用情勢も考慮して、移転する技術の範囲を見極める

- 転職率が高い国では、現地スタッフの転職による技術流出の可能性が相対的に高いため、移転する技術の範囲について慎重に判断する

1. ⑤ 情報管理体制等に関する取引先のデューディリジェンス (DD) の実施

- 合併相手方や、製造委託先等について、技術流出の懸念がないか丁寧な確認が必要
- **情報管理体制に不備がある場合や、財務状況に不安がある場合等は、役職員や関係会社を通じた技術流出のおそれがある。特に、情報管理体制が自社と同等の水準以上か確認する**
- 自社の重要技術に関わる取引を行う以上、取引先との企業規模の差等に躊躇することなく、**対等なパートナーとして情報提供、説明を求めていくことが必要**

対応策の例

① 情報管理に関するDD

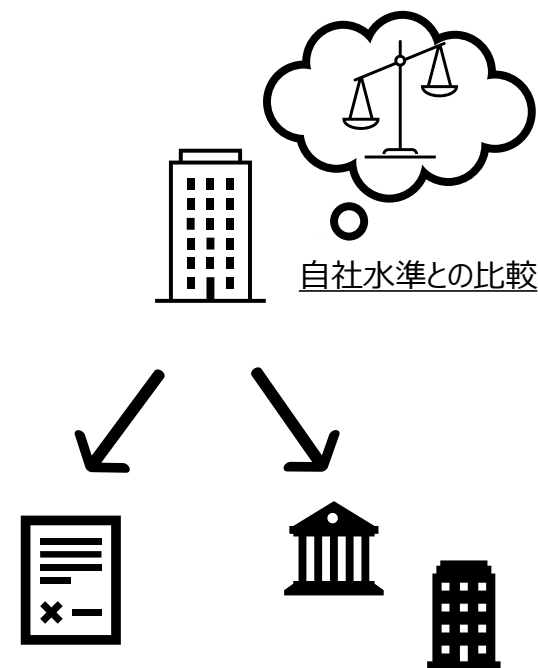
- MoU (基本合意書) やNDA (秘密保持契約) を締結のうえ、弁護士等の専門家も活用しつつ、取引先のヒアリングや現地確認によって、以下のような点を確認
 - ✓ 情報管理に関する社内規程の整備状況
 - ✓ 情報管理に関する責任部門の設置状況
 - ✓ 役職員への教育・研修状況
 - ✓ 物理的・技術的な情報管理体制の状況 (アクセス制御等)
 - ✓ 過去の情報流出事案の有無・内容
 - ✓ 不適切な管理を検知するための施策の有無 (モニタリング等)

② 財務やコンプライアンス遵守の状況に関するDD

- 取引先や関係企業の財務健全性やコンプライアンス遵守状況についても、弁護士等の専門家も活用しつつ、リスク評価を実施する

③ 情報管理がずさんな相手方とは取引を行わない

- 相手が自社の水準に達していない場合には、必要な情報管理体制の整備を要請し、財務状況等のチェック 体制整備が完了してから契約する



自社水準との比較

財務状況等のチェック

専門家等の活用

1. ⑥ ステークホルダーに対する事前説明

- 生産拠点の海外進出は、経営状況に与える影響も大きく、仮に技術が流出した場合には、**経済的な不利益は甚大**である
- 自社の出資・融資元や取引先等、**主要なステークホルダーに対して、技術流出リスクと対策状況を含め、丁寧な説明を行うことが重要**

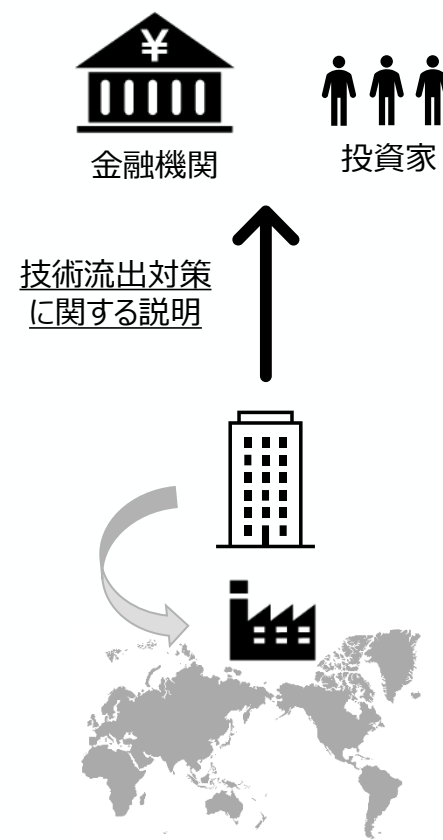
対応策の例

① 契約内容等の確認

- 投資家や金融機関等と締結している投資契約・ローン契約の内容によっては、契約上、海外技術移転を伴う取引に事前承諾が必要となっているケースもあるため、まずは契約内容を確認する
- 仮に契約上の定めがない場合であっても、海外技術移転の規模や移転技術の重要度によっては、当該技術の流出が企業価値の毀損に直結することから、投資家や金融機関等に対して事前に説明する

② 技術流出対策に関する丁寧な説明

- 投資家等からの流出もあり得ることから、当該技術の秘匿性には留意しつつ、技術流出リスクと流出対策について、丁寧に説明する
- 場合によっては、ステークホルダーが技術流出リスクに関する情報を有している場合もある。説明にとどまらず、ステークホルダーとの対話内容を考慮した技術流出対策を講じることも重要
- なお、投資家や金融機関への情報共有に当たっては、ステークホルダー間の公平性の観点から、各投資家等との契約、法令・上場ルール等に反しないよう留意する



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

2. ① 提供する技術の内容等の明確化

- 当初の想定範囲を超える技術情報の提供を求められた場合に拒否できるよう、**提供する技術情報の範囲・内容を吟味し、契約書で明確化**することが重要
- また、実務担当者が、技術情報の提供可否等を正確に判断できるよう、**社内ガイドライン等の整備**も重要

対応策の例

① NDAの確実な締結

- 契約交渉が開始する前に確実にNDAを締結する。NDAについては、いかなる目的で、どのような情報を提供するか、可能な限り限定する
- 最終契約の締結までは、事業の実現可能性を検討するために必要最低限の技術情報しか提供しない

② 技術の重要度に応じた契約審査

- 提供する技術情報の重要性が高い場合（他企業との技術格差が高い等）、一層厳格な契約審査を行う

③ 提供範囲の明確化

- 事業部門・法務部門・コア技術の特定を担う部門（経済安全保障の担当部門等）が連携し、必要最低限の技術情報の範囲を画定し、契約書において明確化する

④ 提供方法の明確化

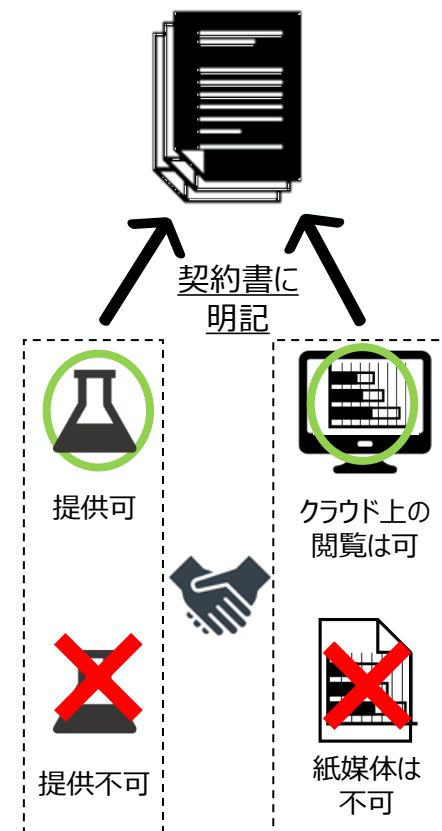
- イレギュラーな提供方法を許容すると技術流出の可能性が高まる。提供方法（いかなる媒体に記録するか等）も契約書に明確化する

⑤ 提供範囲や提供方法を変更する場合の対応

- 取引遂行の過程で、当初定めた範囲を超える情報提供の必要性等が生じた場合は、新たに契約を締結する

⑥ 実務者向けのガイドラインの策定

- 技術や取引ごとに、社内用のガイドライン等を策定し、技術の提供可否や提供方法について、実務担当者が正確に判断できる体制を整備する



2. ② 技術情報の取扱いに係る遵守事項の明確化

- 取引先が無断でサブライセンス、リバースエンジニアリング等をした場合、技術流出リスクが高まる
- **技術情報の重要度・機微度に応じ、取扱主体や取扱方法を限定し、異なる取扱いを禁止することが重要**
- 合併相手方やライセンシーに対しては、提供技術が重要であるからこそ、徹底した流出対策が必要であることを伝え、**契約交渉において安易に妥協しないことも重要**
- 同時に、契約が必ずしも遵守されないリスクを常に意識する。契約内容だけでなく、その実施にも注意が必要

対応策の例

① 取扱主体の限定

- 技術情報の取扱責任者と、情報の重要度・機微度に応じて、アクセス可能な役職員の範囲（拠点・部門・社員ID等で特定）を明確に定める
- メンバーが変動する場合は、事前の書面承諾がない限りアクセス権限の付与を禁じる

② 取扱い方法の限定

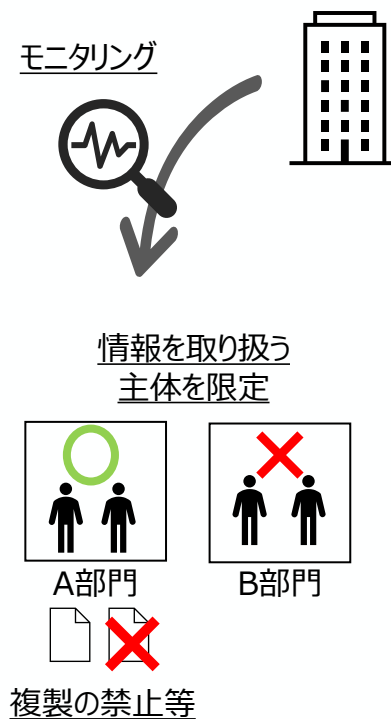
- 取引先DDで確認した情報管理体制を踏まえて、技術情報の重要度・機微度やその提供方法に応じて、行うべき管理方法を明確化する（例：図面の複製禁止、製造装置の移設禁止等）
- また、目的外利用のほか、サブライセンス、再委託、リバースエンジニアリング等の技術流出に繋がりうる行為については、事前承諾事項や禁止事項とする
- 海外製造委託に伴って技術指導を行う場合や、合併会社に従業員を派遣する場合、委託先・合併相手方に対して、自社の従業員に対する引き抜き行為を禁止する

③ 情報管理体制の維持

- 取引先DDで確認した情報管理体制の維持を遵守事項として定める
- 情報管理体制の変更・緩和については、事前通知事項や解除事由として定める

④ 監査条項を規定

- 遵守事項が適切に履行されているかをモニタリングするため、書面による報告の義務付けや生産拠点への立入りを可能とする条項等、監査に関する条項を定める



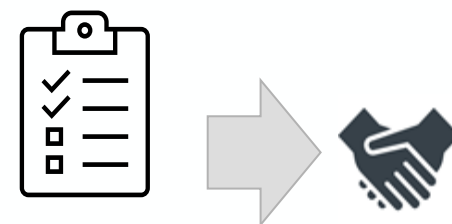
2. ③ 事情変更が生じた場合の対応の明確化

- 取引先が情報管理体制を緩和したり、新たに競合しうる製品の製造を開始した場合等、契約後に事情が変わる場合には、技術流出リスクが高まる可能性がある
- そのため、リスクとなりうる**事情変更を事前に把握する手段とその対応策を明確化**することが重要

対応策の例

① 事前承諾事項・通知事項・解除事由として規定

- 取引先による下記事項の決定は、計画段階で評価した技術流出リスクに影響する可能性があるため、解除事由として定め、場合によっては事前承諾を義務付ける
 - ✓ 経営権の変動を伴う株式の発行等（競合他社に対する第三者割当て、事業譲渡、会社分割等）（CoC: Change of Control）
 - ✓ 自社と競合する事業への進出・競合する新製品の開発
 - ✓ 取引先DDで確認した情報管理体制等の変更
 - ✓ 信用状態の悪化
 - ✓ 相手国政府に対する、提供する技術と関係する補助金の交付申請
- 下記事項の発生も技術流出リスクに影響する可能性があるため、解除事由として定め、通知を義務付ける。また、技術情報の提供を直ちに中止・回収することも規定する
 - ✓ 相手国当局による技術情報に係る報告徴求命令や立入検査
 - ✓ 技術流出のおそれにつながるような相手国の制度の変更（p33参照）
 - ✓ 経営権の変動を伴う市場での株式取得等（CoC）



解除事由として規定



② 免責条項を規定

- 日本や相手国、第三国の規制や、社会情勢の変化に伴い、日本からの技術情報の提供が困難になった場合に、債務不履行を構成しないような免責条項を設ける

2. ④ 契約終了後の手続の明確化

- 契約終了後に、技術情報が記載・記録された文書・電子媒体やカスタマイズされた製造装置が第三者が流出することで、技術流出につながる可能性がある
- 契約終了事由は様々であり、終了時に新たな合意を行うことが困難なケースも多いため、**あらかじめ契約終了後の処分手続を明確に定めておくことが重要**
- その上で、契約書は円滑な処分のための準備に過ぎず、**撤退時に確実に履行することが重要**

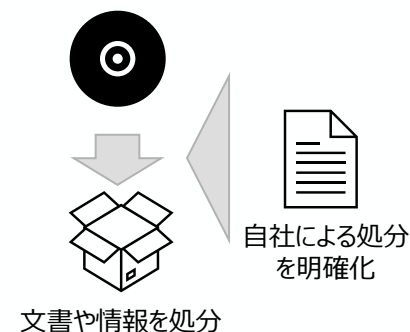
対応策の例

① 自社による記録媒体の処分を明確化

- 契約期間中に取引先の記録媒体に記録せざるを得ない場合は、契約終了と同時に、権利を放棄させ、自社の処分に服する旨定める

② 処分手続の可視化

- 技術情報が記載された文書等については自ら処分するのが望ましいが、取引先において処分する場合であっても、処分事業者の選定を自ら行うことができるようにする



③ 守秘義務の存続

- 処分漏れ等の理由で、取引先に技術情報が残ってしまう場合も存在するため、存続条項に守秘義務条項を含めること等を通じて、契約終了後も、守秘義務を存続させる



④ 非公開の紛争解決手続の利用について規定

- 仮に紛争になった場合、技術情報が記載された文書等が証拠提出されると、訴訟記録として公開されるリスクがあるため、非公開の紛争解決手続を利用できるよう、仲裁条項等を定めることも有用

2. ⑤ (合併契約の場合) ガバナンスの確保

- 海外企業と合併会社を設立する場合、そのガバナンスを確保しなければ、合併事業を通じて技術が流出する可能性がある
- 合併契約において、**技術移転を伴う取引に係る意思決定権を確保するとともに、技術流出のおそれが生じた場合に、合併事業を解消**できるようにすることが重要

対応策の例

① 出資比率の確保・維持

- まず、合併相手方が自由に株式を譲渡しないよう、譲渡制限付き株式とする
- 合併相手方に経営権が支配されないよう、資本比率の過半数を確保する
- 現地での便益を目的に出資比率の変更を迫られた場合であっても、議決権のない株式を発行する等の対応も含め、合併相手方が過半数を保有しないように注意する（潜在株や黄金株も保有させない）

② 役員指名権の確保

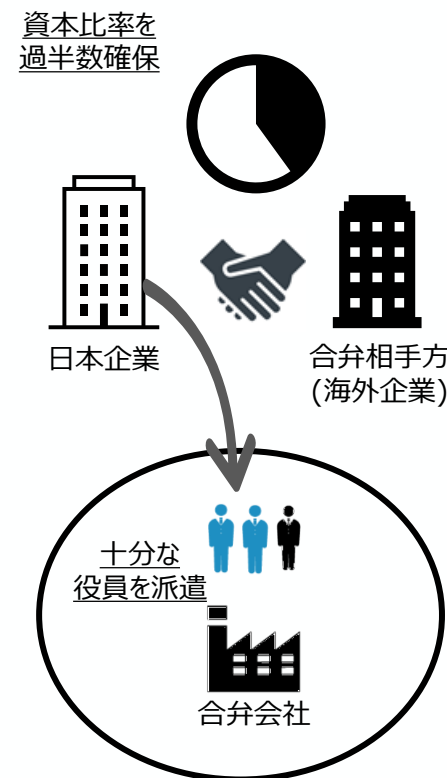
- 技術流出のおそれがある取引が秘密裏に行われないう、十分な人数の役員を派遣する権利を確保する
- 仮に出資比率が過半数でない場合であっても、出資比率に応じた人数の役員指名権を確保する。そのうえで、契約や定款において、役員選任議案等の決議要件を加重することも有用（特別決議とする等）

③ 技術流出のおそれのある行為を拒否権事由・事前承諾事項として規定

- 合併会社から海外企業への技術移転取引や、合併相手方との契約締結、情報管理規程の改廃、技術者の引き抜き等は、合併会社からの技術流出に繋がる可能性があるため、拒否権事由として定める

④ 合併解消の条件・解消時の技術情報の取扱い

- 合併相手方の契約違反によって技術流出のおそれが生じた場合に、速やかに合併事業を解消できるよう、準拠法に留意の上、解消条件（コールオプション／プットオプションの行使、解除権の行使等）を定める
- また、自社の技術をライセンス契約等によって提供する場合は、ライセンス契約の解除事由や、提供した技術情報の処分等についても定める
- なお、合併会社に対して、重要技術を有する技術者を派遣している場合、契約終了後、当該技術者が合併相手方から引き抜かれる可能性もある。各国の競争法や規制当局の判断等にも留意したうえで、一定の期間、合併相手方に対して、技術者の引き抜きを制限することも検討する



第0章 はじめに

- 1 本ガイドンスの目的等
- 2 技術流出の経路と本ガイドンスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項**
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

3. ① 段階的な技術提供

- 最初から広範囲な技術情報を提供すると、結果として必要のない技術情報まで提供してしまうおそれがある。進捗に応じて事業計画が変更される可能性を視野に入れ、**事業計画の進展と連動した段階的な情報提供を行うことが重要**である
- また、国際情勢の変化等、他律的な理由により、事業計画が停止する可能性もある。**慣習的に契約期間を定めるのではなく、個別の取引ごとに、短期/長期のいずれが自社に有利であるかを見極め、交渉していくことが有効**

対応策の例

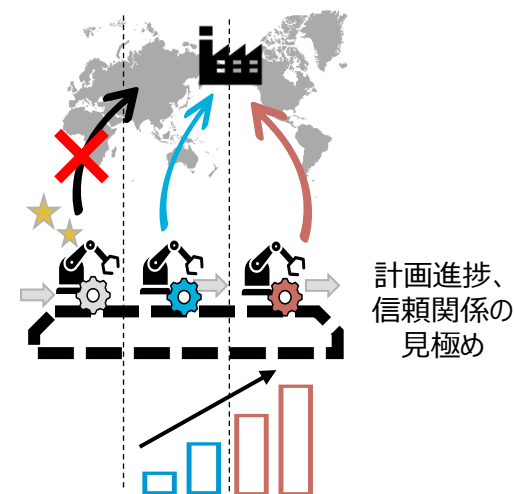
① 段階的な技術提供

- 技術情報を段階的に提供し、必要性に応じて情報の開示を制限する
- 例えば、初期段階では基本的な情報のみを提供し、事業計画の進捗や信頼関係の構築を見極めながら重要な情報を開示するといった対応が考えられる
- また、製造委託等に伴い、技術者を現地に派遣して技術指導を行う場合、あらかじめ、回答してもよい範囲を明確化する

② 契約期間の見極め

- 長期的な契約は、経済合理性の観点から有効な場合がある一方、撤退等事情変更への対応が難しくなるリスクがある。このため、例えば、契約期間を半年や1年間等の短期間で設定し、都度更新するといった工夫をする
- 自動更新条項についても注意が必要。更新手続の形骸化を防ぐため、更新時には、契約期間中の監査結果等を踏まえた契約審査を実施する等の対応が有効。結果に応じて、条項の追加等を含めた契約の変更も検討する
- 契約期間の経過後も技術情報の提供が続くような事態を防止するため、法務部門と事業部門が適切に連携し、確実な契約管理を行う

段階的な技術提供



契約期間の見極め



3. ② 情報のブラックボックス化

- 現地への情報提供は、事業計画の遂行に必須な範囲に留め、**事業計画の遂行に不必要な情報は、可能な限り秘匿することが重要**
- 技術そのものに関する情報は当然であるが、例えば、部品等の調達元等、**周辺情報についても技術流出の端緒となり得ることを意識し、注意することが必要**

対応策の例

① 生産・製造工程や原材料等のコードネーム化

- 社内での会話や資料に記載された、生産プロセス、原材料等の名称が知られることで、技術流出の端緒となる場合がある
- こういった重要な固有名詞をコードネーム化し、日常的にはその名称でやり取りをすることで、情報の漏えいを防止することができる
- 実際の名称とコードネームの対応関係は、一部の責任者のみが把握する等、情報の共有範囲を限定する

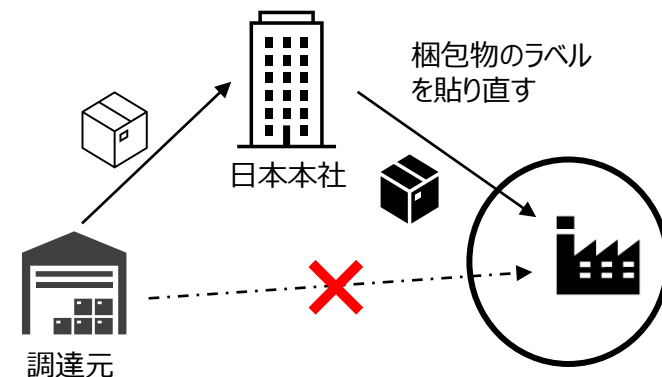
コードネーム化のイメージ



② 図面の使い分け

- 海外拠点に設計図面を送る場合、本来の図面のほか、機密性が高い情報を削除した図面を作り、分けて管理する

調達元の秘匿



③ 調達元の秘匿

- 部品等の調達元が知られることで、当該調達元に技術獲得のアプローチが行われる場合がある。調達元とは、擦り合わせのために技術情報を共有しているケースもあるため、注意が必要
- 各種資料には調達元を記載しない、調達元企業の名称で納入しない(梱包の印刷等も企業名がないものを使用する)といった工夫をする

3. ③ 技術情報提供後の情報管理の徹底

- 現地での情報の管理が不十分であれば、情報漏えいや情報の不正使用のリスクが高まる。現地拠点に対し、情報管理の体制の構築を求めるとともに、対応状況を監査することが必要

対応策の例

① 情報セキュリティ体制の構築

- 技術情報の保存、アクセス、共有、削除等に関する明確なポリシーを策定し、従業員に周知徹底する

② アクセス権限の管理

- 重要情報へのアクセス権限を厳格に管理し、必要な従業員にのみ情報を提供する。また定期的にアクセス権限を見直す

③ 提供する情報をリスト等で管理

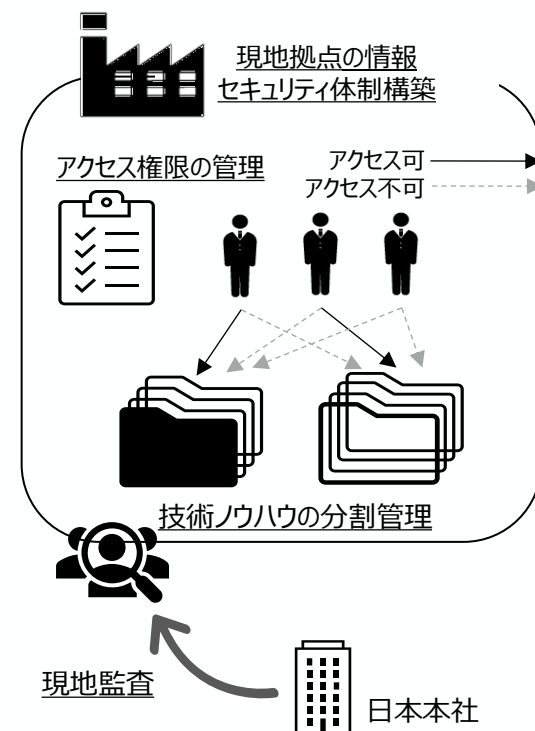
- 事業実施段階における適切な情報管理はもちろん、撤退時の確実な処分を可能とするために、提供した情報の内容・時期・方法等について、リスト等により管理する。文書として配布する場合には、管理番号を付して配布先や部数を限定して管理することも有用

④ 技術ノウハウの分割管理

- 技術ノウハウを分割管理し、全ての情報が一カ所に集約されないようにする

⑤ 技術情報の取扱いに係る遵守事項の現地監査等

- 情報セキュリティに関する事項を含め、技術情報の取扱いに係る遵守事項が徹底されているかどうか、必要に応じて現地で対応状況を確認する。また、現地監査に加えて、取引先による特許出願状況をモニタリングすることも有用



※中国、ベトナム、タイ、韓国、シンガポール、インドネシア、インド及びメキシコにおける営業秘密管理については、下記HP掲載の各マニュアルも参照されたい。
 ・経済産業省「営業秘密～営業秘密を守り活用する～」
<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

3. ④ 製造設備のメンテナンス管理の徹底

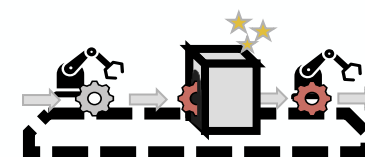
- 製造設備には、設備メーカーとの擦り合わせや自社内でのカスタマイズを通じて、**様々なノウハウが化体している場合がある**。また、製造設備の種類、配置や稼働方法、どのメーカーの設備を利用しているかといった情報そのものが機微な場合もある
- 現地企業による保守・メンテナンスは、設備のカスタマイズ等の技術情報に触れる機会にもなり得るため、**リバースエンジニアリング等による技術流出リスクが高い**。製造設備のメンテナンス等によって技術流出のリスクがある場合には、自社または日系メーカーによる対応が重要。メンテナンス業者等の第三者の工場立ち入り時は特に注意が必要
- このような取組は、製造設備や各種機器を海外販売する際の、リバースエンジニアリング対策にも重要。

対応策の例

① 製造設備に関する機微情報の範囲の確認

- 現地拠点で稼働する製造設備について、どこに自社のノウハウに関係する機微情報が存在するかを確認する。この際、スペックや部品等個々の製造設備に関する情報に限らず、以下のような観点から、広く確認することが必要
 - ✓ スペック・部品：当該設備がどのような性能を持ち、どのような部品を用いているか。特に、市販の汎用品ではなく、設備メーカーとの擦り合わせや自社内でのカスタマイズを行っている場合は機微度が高い
 - ✓ 設備の種類、配置、稼働方法：どの工程に、どのような種類の設備を、どのように配置し、どのように稼働しているかといった情報が、品質やコストに直結する機微情報となる場合がある
 - ✓ 設備メーカー：技術獲得を目指す競合他社が、製造設備メーカーにアプローチを試みることも多いため、どのメーカーの設備を使用しているかが機微情報となる場合がある

製造設備に関する
機微情報の範囲を確認



② 信頼できるメンテナンス体制の確保

- 設備のメンテナンスは、極力、日本の本社や設備メーカーから派遣された技術者が実施することが、技術流出防止の観点から有効である。他方、現地企業に協力を求めざるを得ないケースもある。その場合は、以下のような取組を徹底する
 - ✓ 信頼できる企業であるかの確認
 - ✓ 必要なエリア以外の立入や、電子デバイス等の持ち込み制限
 - ✓ 隣接するプロセスや装置（企業ロゴ等を含む）の秘匿
 - ✓ 特に重要な保守部品の内製化や正規品の日本からの送付
 - ✓ メンテナンス現場への立ち合い



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

4. ① 撤退計画に対応した適切な情報管理の徹底

- 海外拠点から撤退をする場合、現地従業員が競合他社へ転職すること等を通じ、技術情報の漏えいリスクが高まる
- 重要情報へのアクセス制限や、撤退に伴う情報の取扱いに関するポリシーを作成する等、情報漏えいリスクを低減することが必要

対応策の例

① 社内ポリシーを整備する

- 撤退に伴う情報の取り扱いに関する社内での明確なポリシー（情報の保存方法や共有設定等）を設定し、従業員に対して周知する

② アクセス権限を再設定する

- 撤退に伴い業務を縮小する中で、重要情報へのアクセス権限を再設定し、不要な従業員のアクセスを制限する。
- たとえば、事業撤退に当たっては、本社や親会社、政府当局、顧客等との調整業務等は残る一方で、営業や製造に関する業務は段階的に縮小・終了することとなり、海外拠点において技術情報を利用する必要性も低下する。このように、撤退計画の遂行に当たって必要最小限の業務を特定した上で、当該業務に必要な情報以外はアクセスを停止し、当該必要な情報にアクセスできるメンバーも限定・特定することが重要である。

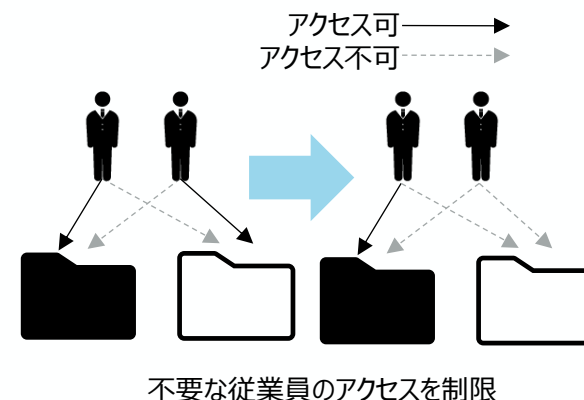
③ 監視を強化する

- 技術情報の持ち出しリスクが高まるため、不自然なデータのダウンロードが行われていないか等のチェックを強化する

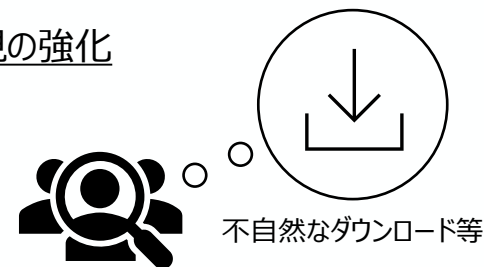
④ 契約内容の確認・見直しを行う

- 撤退に際して、退職後の情報漏えいに対する責任を明確にする等、現地従業員や関係者との秘密保持契約の内容を再確認し、必要に応じて契約内容の見直しを行う

アクセス権限の再設定



監視の強化



4. ② 製造設備の適切な管理・処分

- 製造設備は、培ったノウハウによりカスタマイズしているケースがあり、このような装置が**競合他社に転売**されたり、**リバースエンジニアリング**されることを通じて、技術が流出するケースがある
- コア技術が化体した製造設備については、撤退時に適切に**返却**または**廃棄**されるよう具体的な手続きを定めるとともに、**確実な実施**を図ることが必要

対応策の例

① 設備の機微度の確認

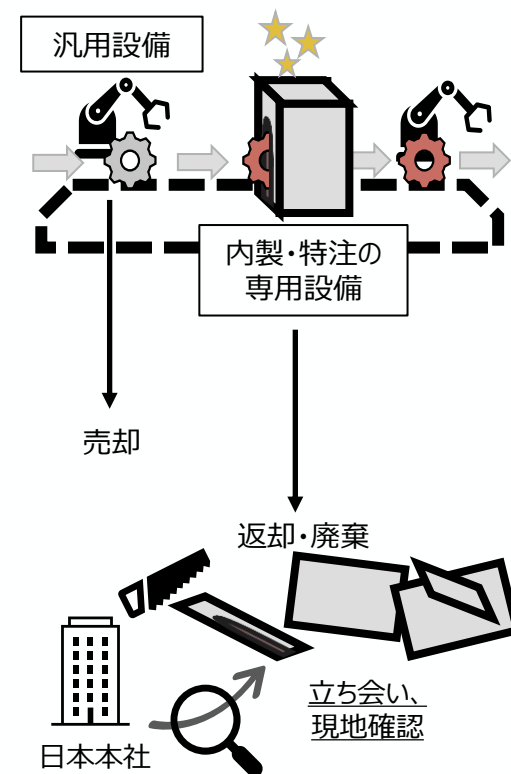
- コア技術が化体し技術流出に繋がりうる設備がどれか特定する
- ア) 汎用設備をそのまま使用している場合、イ) 汎用設備だが設定値等を独自調整している場合、ウ) 専用設備として内製や特注している場合、といったカテゴリに整理すると分かりやすい

② どのような処分を行うかの意思決定

- コア技術が化体していると考える設備については、返却や廃棄の対象とする
- 汎用品をそのまま使用している場合や、設定値等を初期設定に戻すことができる場合等は売却の対象とする

③ 実施確認

- 決められた処分を確実に行う。特に、廃棄については、廃棄事業者に一任するのではなく、取引実績や情報管理体制等を調査して慎重に選定した上で、立ち会い・現地確認まで行う等自社の責任で実施する



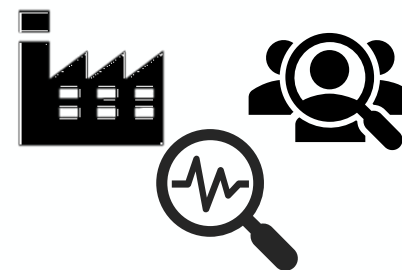
4. ③ 撤退後のフォローアップ

- 撤退後は、**現地の体制が縮小・喪失するため、技術流出による問題が生じても気づきにくい**といった課題がある。定期的に現地の状況を**モニタリング調査**したり、現地での取引先との**コミュニケーションを継続**することで信頼関係を維持し、情報収集に努めることが必要
- その上で、問題を把握した場合は、**迅速かつ毅然とした対応**を図ることが必要

対応策の例

① 現地のモニタリングを実施する

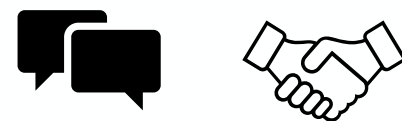
- 現地の競合他社が類似製品の開発・販売を開始していないか、現地スタッフがどのようなところに転職しているか、提供した技術に関連する特許が現地に出願されていないか等、技術流出につながりうる動向について、定期的に調査する



現地のモニタリング

② 取引先との信頼関係の維持

- 現地の取引先とのコミュニケーションを維持し、信頼関係を保つ
- これにより、現地動向に関する様々な情報をリアルタイムで入手しやすくなるとともに、取引先による不正な行為の抑止にもつながる



コミュニケーション、信頼関係の維持

③ 不正行為に対する毅然とした対応

- 守秘義務等の契約や法令に違反する行為を把握した場合は、訴訟等を含め、迅速かつ毅然と対応する
- その後の同様の行為に対する抑止につながるほか、技術流出による実被害を最小限にとどめることにもつながる



訴訟を含めた対応

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

5. ① 海外の研究開発拠点に対する管理の徹底

- 海外に研究開発拠点を持つ企業では、**海外拠点間で直接技術移転**が行われるケースが存在する
- 日本から海外拠点への技術移転に際しては、本社によるガバナンスが効きやすい一方、**海外拠点間の技術移転については管理が行き届かず、意図しない技術流出や外為法等のコンプライアンス違反が生じるおそれもある**
- コア技術を持つ海外の研究開発拠点については、日本国内と同様の管理を徹底するほか、**本社への報告等ガバナンスが効く仕組み**を構築しておくことが重要

対応策の例

① 日本国内と同等の管理

- コア技術を持つ海外拠点を特定した上で、以下の点も考慮して、日本国内と同等の管理体制を整備する
 - ✓ 海外拠点で開発した技術の日本本社での一元管理
 - ✓ 重要度に応じた、海外拠点で取り扱う技術のランク付け
 - ✓ 技術の重要度に応じた、システム上のアクセスコントロールの実施
- 情報管理研修やコンプライアンス教育等も、日本国内と同様に徹底する



日本国内同様の
研修の実施

日常的なコミュニケーション

② 日本本社への報告等

- コア技術を持つ海外拠点に対し、日常的なコミュニケーションを徹底するほか、技術移転については本社に報告し、指示や承認を受ける仕組みを構築する
- なお、海外拠点から日本本社への技術提供については、現地の輸出管理制度の遵守に留意する



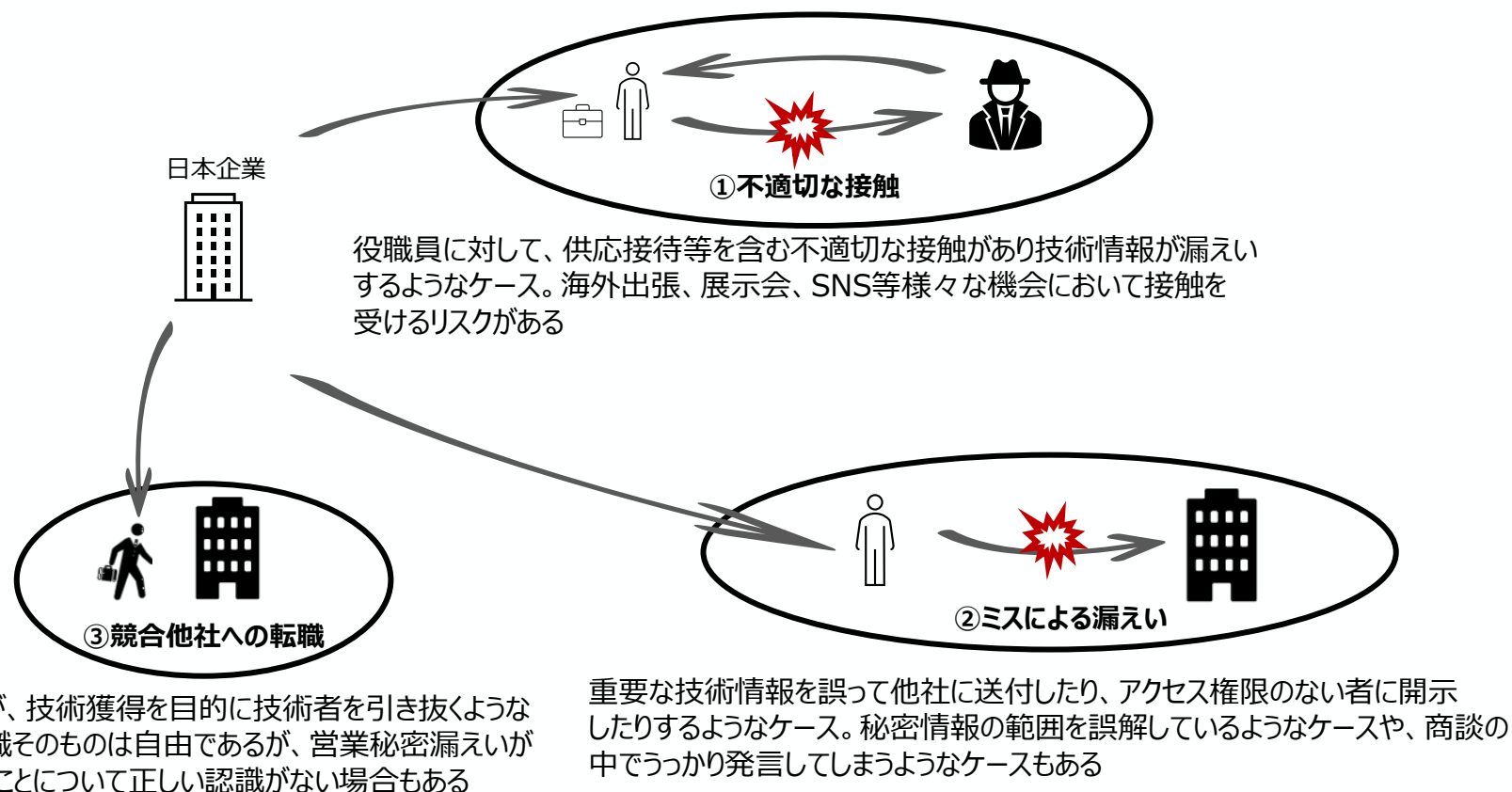
第3章

人を通じた技術流出への対策

第3章が想定する技術流出のケース

- 第3章では、役職員による技術情報の持ち出し（不正の目的に限られない）による技術流出への対策や、優秀な技術者の転職によって技術優位性を失うような場合への対策を記載している。なお、いわゆる正社員（管理職含む）に限った議論ではなく、役員、派遣従業員、出向者、退職者等、広く自社の技術情報に関わる人物を想定している

<人を通じた技術流出ケース（例）>



「人を通じた技術流出対策」に関する基本的認識

- 企業活動においては業務遂行のため、日常的に多数の役職員が様々な技術情報を取り扱っている。そのため、意図的か否かによらず、技術流出事案には、何らかの形で企業内の役職員が関係しているケースが多く、**人を通じた技術流出対策は、企業規模や業態を問わず、重要である**。また、海外拠点への技術移転や共同研究に伴う技術流出についても、海外拠点や共同研究先の役職員や研究者を通じて技術が流出するケースが多く、本章は、こうした様々なビジネスシーンにおいても参照されたい。
- そして、技術情報を取り扱う者はいわゆる**正社員（管理職含む）に限られず、雇用関係にない役員、派遣従業員、出向者、業務委託先のフリーランス**等も含まれる。そのため、人を通じた技術流出対策を考える際には、**勤務形態を問わず広く企業内で技術情報を取り扱う者を通じた技術流出を念頭に置く必要がある**。そこで、本章では、こうした様々な企業内ステークホルダーを念頭に、「役職員」という語を用いている
- 技術情報の形態やその取扱方法は、業界や個別の企業・部署に応じて千差万別であるものの、本章のうち、「**1. 技術流出を未然に防ぐために取り組むべき事項**」については、概ね、①**ルール面での対応**（社内規程の整備等）、②**人事面での対応**（社内研修等）、③**システム面での対応**（アクセスコントロール等）、④**現場のオペレーション面での対応**（製造工程における人員配置等）、の4段階で整理して記載する
- ただ、いずれの対応についても、**守るべき技術の重要性や自社の規模等に応じて、メリハリを付けた対応を講じることが重要**である。p5に記載のとおり、全ての対策を講じることが、リソース面から限界があるケースもあるため、**取り組める対策から確実に実行していくことが望ましい**

第0章 はじめに

- 1 本ガイドンスの目的等
- 2 技術流出の経路と本ガイドンスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

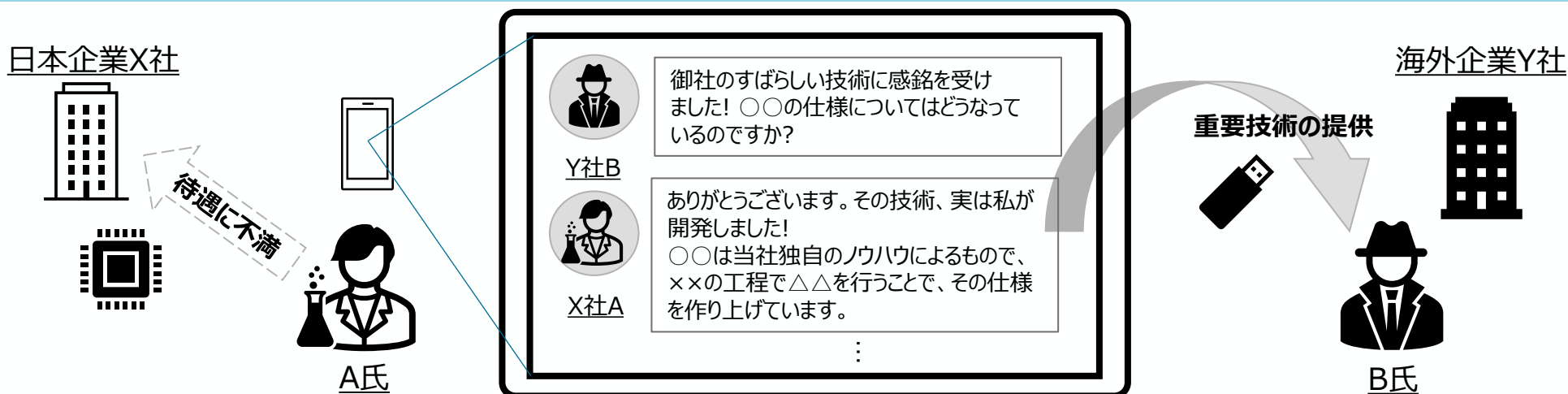
第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

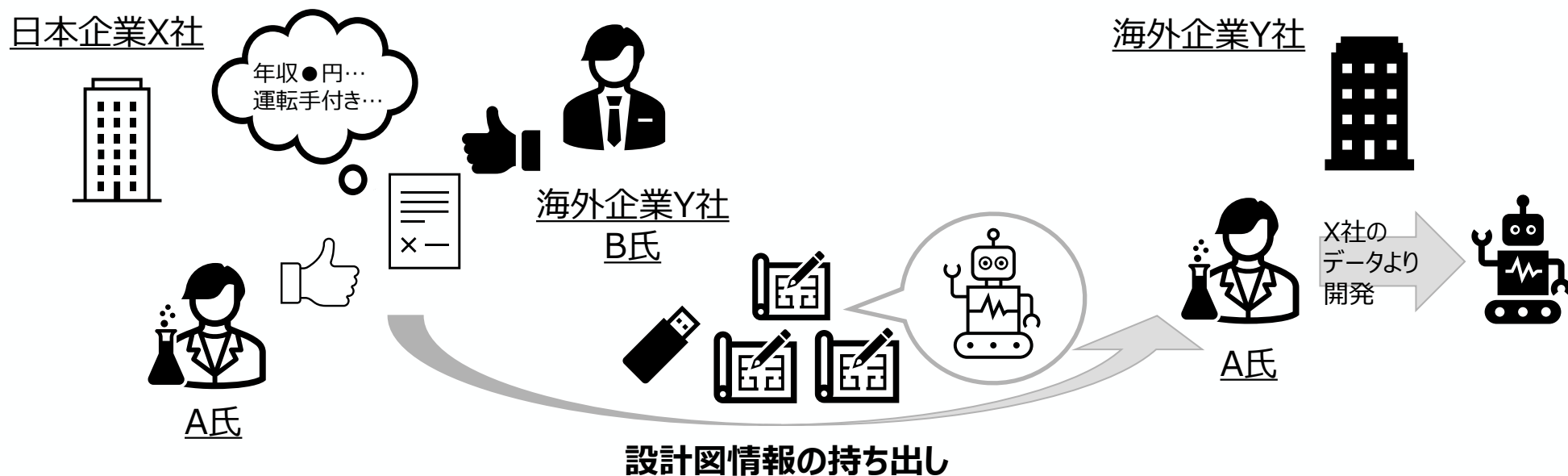
Case1: SNSでのやりとりを通じた技術流出

- 日本企業X社の社員であるA氏は、X社の主力製品の開発に携わる優秀な技術者であった
- ある日、本名で登録していたSNSを通じて、海外企業Y社のB氏から、自社製品の技術に関する質問が送られてきた。自らが開発した技術であったため、興味を持たれたことに嬉しくなってしまう、ついつい非公開としている情報まで提供してしまった
- B氏とのやりとりはその後も継続。自社での待遇に不満を持ち、自分の評価を高めたいと考えたA氏は、Y社の情報と引き換えという条件で更に重要技術を手渡したが、Y社から情報が送られてくることはなかった
- A氏の行動を不審に思った同僚がX社内で報告・相談したことにより、Y社への機密情報流出が発覚。A氏は、悪質な情報漏えいに関与したとして懲戒解雇の処分を受けるとともに、刑事告訴され、懲役刑及び罰金刑を科せられることとなった



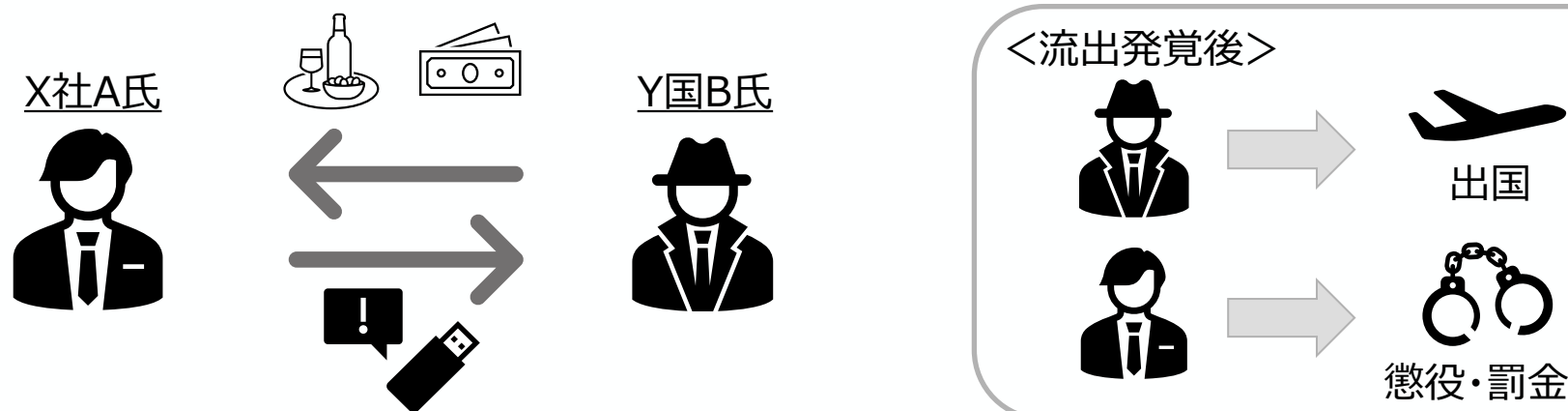
Case2: 役員の転職を契機とする技術流出

- 日本企業X社の役員であったA氏は、X社において製品開発に従事
- ある日、業務で知り合った海外企業Y社のB氏から、転職を持ちかけられた。A氏は、提示された待遇に魅力を感じ、翌年度からY社に転職することを決意
- A氏は、転職前に、Y社での活用も見越して、自身が関係した大量の設計図情報をUSBメモリに保存して持ち出した。A氏の転職後、Y社は、A氏が持ち出した情報を元に、X社と競合する製品を開発し、マーケットシェアを伸ばしていった
- X社の内部監査において、A氏のデータの持ち出しが発覚。A氏は、刑事告訴され、懲役刑及び罰金刑を科せられることとなった



Case3: 産業スパイの接触を通じた技術流出

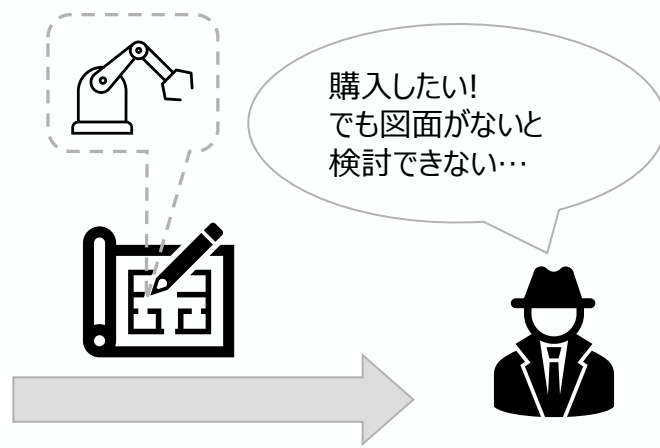
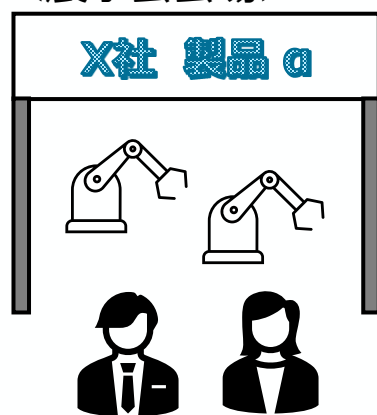
- **日本企業X社の社員A氏**が、レストランで食事をしていたところ、隣のテーブルにいた**Y国政府機関の職員B氏**に話しかけられた。日本のビジネス事情にも詳しいB氏との会話は弾み、その後も頻繁に会うようになった
- 親しくなって数ヶ月がたった頃、**B氏がX社の重要プロジェクトについて関心を示し、A氏に関連する情報を求めてきた**。求められた情報は公開情報であったため、A氏は気軽に情報を提供した
- B氏の要求は**次第にエスカレートし、X社の重要な技術情報の提供を求められた**。A氏はプロジェクトを監督する立場であり、当該情報を容易に入手することができた。それまでに**食事や金品を受け取っていた**こともあり、A氏は断ることができず、情報を提供してしまった
- その後、情報流出が発覚し、**A氏は懲役刑及び罰金刑を科せられることとなった**。一方、**B氏は出国**してしまい、不正競争防止法違反で送検されたのみであった



Case4: 展示会への出展を契機とした技術流出

- 日本企業X社は、主力製品の営業のため、海外で開催される展示会に出展した。X社の製品は海外でも人気が高く、様々な企業から声をかけられたが、その中で、**現地企業Y社から「御社の製品αの購入を検討したい」との商談を持ちかけられた**
- パンフレットを使って製品説明をしたものの、Y社から「**購入したいが、当社の製造ラインで使用できるか不安。製品αの詳細な設計図面を見せてもらえないか**」という要望があった
- 新たな販路が獲得できると期待し、**求められるがまま、設計図面のコピーを渡してしまった**。しかしながら、その後、**Y社からの連絡は途絶え**、販路も拡大することができないまま1年が経過した
- X社が別の商談のため現地を訪問した際、**製品αと類似するY社製品βが安価で出回っていたことが発覚**。**販路を拡大するどころか、既存の売上シェアも奪われる**状況となった

<展示会会場>



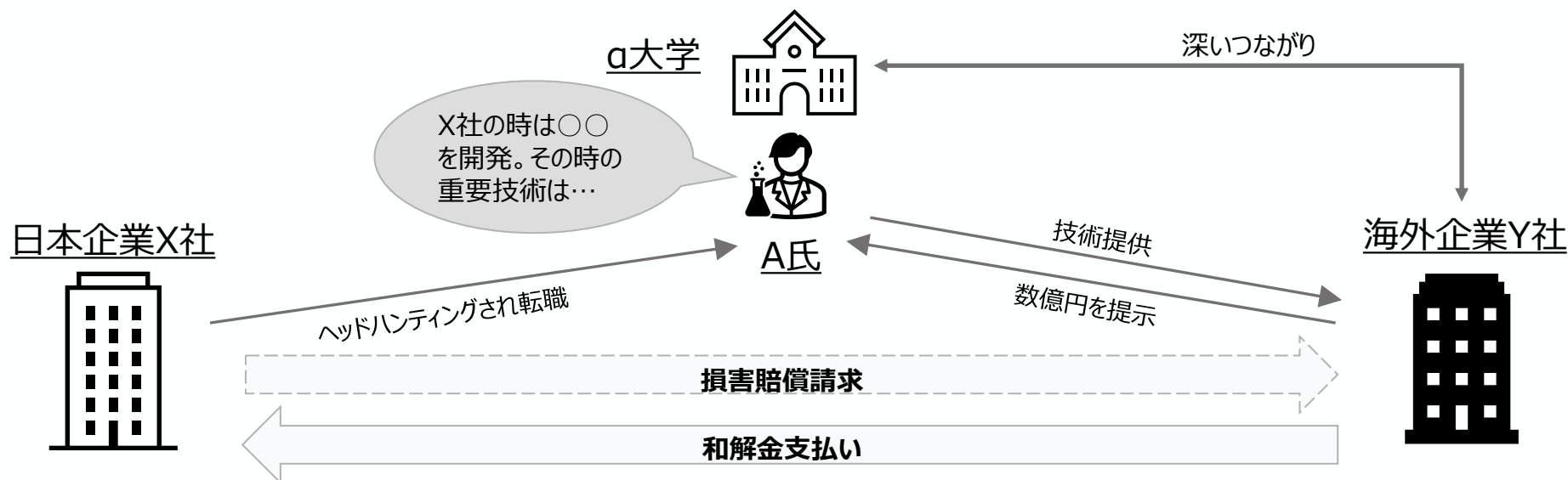
Y社

<1年後>



Case5: 従業員による営業秘密の不正開示に伴う流出

- 日本企業X社のA氏は、ある製品の研究開発に関わる技術者であったが、社内で他の技術者に対して劣等感を感じており、研究へのモチベーションを失いつつあった
- ある日、海外企業Y社と繋がりの深い現地のa大学に客員教授としてヘッドハンティングされた。待遇にも魅力を感じ、X社から転職することを決意
- A氏は、a大学での講演等を通じて、X社の製品開発に係る技術情報を開示するとともに、Y社から数億円の額を提示され、技術情報を提供していたことが発覚した
- X社内では、公になれば企業イメージの低下にも繋がると懸念する声もあったが、最終的に毅然とした対応を取るべきと判断。Y社及びA氏に対して、損害賠償を求める訴訟を提起し、最終的に金銭の支払いにより和解した



第0章 はじめに

- 1 本ガイドンスの目的等
- 2 技術流出の経路と本ガイドンスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

1. ① 情報管理に関するルールの整備・運用の徹底

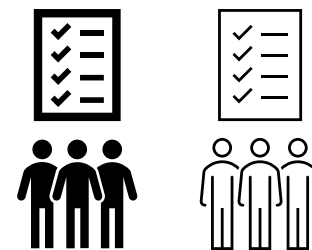
- 人を通じた技術流出は、いわゆる**正社員（管理職含む）に限った課題ではない**。技術流出対策を講じる上では、雇用関係にない**役員や派遣従業員、出向者、業務委託先のフリーランス等を含め、勤務形態を問わず広く役職員を通じた技術流出を念頭に置く必要がある**
- そのため、**就業規則のほか、雇用契約、委任契約、出向契約、業務委託契約等において技術流出の防止について定めることが重要である**
- また、社内規程に基づく情報管理体制を実効的に運用させるため、**関係部署の連携も重要である**

対応策の例

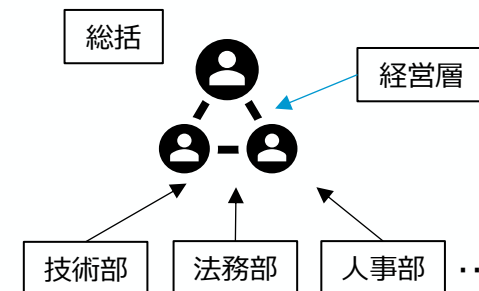
① 情報管理規程を整備するほか、雇用契約等の個別の契約でも対応する

- 広く技術情報に接する役職員を対象に情報管理規程を整備する。最新情報の反映等、規程の内容を不断に見直すことも重要である
- 職種や勤務形態によっては適用される社内規程が異なる場合もある。自社における雇用等の状況を踏まえて、広く全ての役職員が技術情報に関する守秘義務等を負うよう規程が整備されているか、雇用契約等の個別契約に必要な定めがあるか、留意する
- 規程の形骸化を防ぐためには、実際に技術情報を扱う現場の意見を踏まえた内容にすることが重要。規程を整備・改定する際には、現場から意見募集することも有用である

情報管理規程の整備



関連部署の連携



② 規程の整備に終始せず、実効的な運用を徹底する

- 事業部に限らず、情報システム部・人事部・法務部・知財部・監査部等の関係部署が連携し、研修の実施・懸念事案への対応・規程の改定等を組織的・機動的に実施する
- 必要に応じて、各部署の司令塔となる部署を設置することも有用 (p12参照)
- 関係部署の連携においては経営層が関与し、技術流出対策が重要な経営課題であることを全社的に認識させる

1. ② 情報管理状況の監査と重要プロジェクトの配置等への反映

- 社内規程に基づく情報管理を徹底するためには、**定期的に監査を行い**、管理状況を把握する必要がある。監査結果は継続的に記録し、**社内規程や研修内容等に反映させる等**、PDCAを意識し、**情報管理体制の改善に常に取り組む**
- 組織的な情報管理体制の改善にとどまらず、**個別の人事配置（重要プロジェクトへの配置等）**を検討する際にも、**役職員の情報管理意識を確認し、反映させることも重要**

対応策の例

① 社内規程に基づく情報管理状況の監査

- 社内規程に基づく適切な情報管理を行っているかについて、定期的に監査し、必要に応じて不定期な監査も実施する
- 監査結果は経営陣に報告し、必要に応じて社内規程や研修内容を更新する等、監査それ自体に終始することなく、情報管理体制のブラッシュアップや社内の意識醸成に活用する

② 人事配置における情報管理意識の確認・反映

- 情報管理を適切に行うことも個々の役職員の重要なスキルの一つと捉える。重要技術に関与する職務や、今後の重要技術に繋がる研究開発プロジェクトへの配置を検討する際に、情報流出に繋がる非違行為状況や学習テスト等の結果も考慮・反映する
- また、上記の重要プロジェクト等に配置される役職員は、これまでより重要度・機微度が高い技術情報に接することとなる。このため、情報管理意識を改めて喚起するために、退職後を含む厳格な秘密保持義務を遵守する必要性を説明し、同意を得ることを前提とする。必要に応じ、追加的な遵守事項を定める



1. ③ 情報管理に関する定期的・階層的な研修の実施

- 情報管理規程は整備して終わりではなく、**役職員が確実に遵守してこそ意味がある**
- また、事業の実態や技術進展等を踏まえ、情報管理規程は不断に見直すべきもの。役職員が常に最新のルールを理解できるよう、**定期的な研修や学習ツール等で学ぶ機会を持たせることが必要である**
- 職位や所属部署ごとに注意すべき内容は異なる。画一的な内容ではなく、**対象者の立場に応じたきめ細かい研修内容**としていくことが重要である

対応策の例

① 役職員に対する研修の実施

- 全社的な情報管理意識を醸成することが重要。以下の点を意識した研修プログラムを策定した上で、定期的な研修を行う。また、研修の都度、就業規則に従い秘密保持義務を遵守することを誓約書の提出等により明示的に確認することは、秘密保持の重要性に関する意識啓発の観点からも有用である
 - ✓ 情報管理規程の趣旨や違反した場合に生じる事態が理解できるような内容にする
 - ✓ 最新事例や身近な流出事例を盛り込む等、受講者が他人事と思わないような内容とする。実施方法についても、対面実施を組み合わせる等の工夫をする
 - ✓ 遵守事項に関する平板な説明に終始せずロールプレイ等を活用する
 - ✓ 職務内容やポジションに応じた階層的な研修メニューを用意する
- 技術流出対策の重要性について、トップメッセージを随時発する等して、全社的な情報管理意識の醸成を図る
- 必要に応じて、専門家や政府関係者に依頼し、実際の流出事例を交えた研修を行うことも検討する



定期的な研修で常に最新のルールを理解



最新事例、身近な流出事例



ロールプレイ等



トップメッセージの発信



立場に応じた研修

派遣従業員 出向者

② 派遣従業員等に対する研修の実施

- 情報管理研修の必要性は、役員や正社員に限らない
- 派遣従業員や取引先等からの出向者等、自社の技術情報に触れる可能性のある者についても、同様に研修を実施する

1. ④ 法令上必要な事項の採用時確認

- 自社技術が外為法に基づく輸出管理の対象に該当しうる場合、**外為法違反が生じないよう確認が必要**。特に、**非居住者や特定類型に当たる居住者に対する技術提供は、みなし輸出管理の対象になることに注意が必要**
- 中途採用した者が、転職元企業の営業秘密を持ち込んだ場合、自社が営業秘密侵害に問われるリスクがある。そのような法令遵守意識の低い者の雇い入れは、将来的に自社の技術流出に繋がる可能性もある
- そのため、採用後に意図せず関係法令に違反することがないように、**外為法に基づく居住者該当性等、法令遵守の観点から必要な事項について、あらかじめ確認することが必要**

対応策の例

① 法令遵守のために必要な事項を採用時に確認する

- 外為法遵守の観点から、リスト規制やキャッチオール規制に該当する可能性のある技術提供が行われうる業務に従事する予定の者を採用する場合には、特定類型の該当性を確認する（特定類型の該当性の判断に係るガイドラインを参照）。
- また、重要技術を扱う職種に従事する労働者の採用選考にあたり、応募者の採用選考時に、技術流出防止に関連した確認の一環として、国籍を確認する場合については、以下の厚生労働省のHPを参照。
（厚生労働省HP「公正な採用選考をめざして よくある質問」 <https://kouseisaiyou.mhlw.go.jp/question.html>）
- 参考までに、労働施策の総合的な推進並びに労働者の雇用の安定及び職業生活の充実等に関する法律に基づき、外国人を雇用する事業主に対し、外国人の雇入れと離職の際に、氏名、在留資格、在留期間その他の法令に基づく必要事項を在留カード等により確認し、外国人雇用状況の届出を行うことが義務づけられているため、法令違反が生じないよう留意する

・経済産業省「外国為替及び外国貿易法第25条第1項及び外国為替令第17条第2項の規定に基づき許可を要する技術を提供する取引又は行為について 別紙1-3 特定類型の該当性の判断に係るガイドライン」
https://www.meti.go.jp/policy/anpo/law_document/tutatu/t10kaisei/e_kimu_tutatu.pdf

・厚生労働省「外国人雇用状況の届出について」
https://www.mhlw.go.jp/stf/seisaku_unitsuite/bunya/koyou_roudou/koyou/gaikokujin/todokede/index.html

② 他社の営業秘密を持ち込まないよう転職採用時に注意する

- 採用した転職者が、転職元企業の技術情報を持ち込んだ場合、意図せず営業秘密侵害を問われることがある。面接等を通じて、転職元企業や業務内容、情報管理に関する意識等を確認し、営業秘密の持ち込みを防ぐことも重要である。

厚生労働省HP（公正な採用選考をめざして よくある質問（事業主の方へ））（抜粋）

Q 重要技術を扱う職種に従事する労働者の採用選考にあたり、応募者の採用選考時に、技術流出防止に関連した確認の一環として、国籍を確認してもよいのでしょうか。

A 採用選考時には、適性・能力に基づいた判断基準による公正な採用選考を行うことが求められており、国籍を含めた応募者本人の責任によらない事項を把握することは就職差別につながるおそれがあります。ただし、特別な職業上の必要性があるなど、把握すべき内容について個別に合理性、必要性がある場合には、必ずしも把握することが不適切ではない場合があるものと考えられます。

1. ⑤ 重要技術を扱う部署への配属に際しての確認

- 自社が保有する重要技術（第1章「2. ① 重要技術の位置づけを評価」の①～③に該当する技術）については適切な秘密管理が必要である。秘密管理の内容としては、通常、技術情報を取り扱う役職員の個別事情によらず、統一的にシステム面やオペレーション面の措置が講じられるケースが多い。しかし、**秘密管理の高度な必要性が認められる技術情報（特に②・③に該当する技術）に限っては、当該情報を取り扱う部署・ポジションへの配属に際して、配属候補者の個別事情を考慮し、業務上知った技術情報を漏えいするおそれを評価（適性の確認）すべき場合もある。**なお、ここでいう適性の確認は、重要経済安保情報保護活用法における「適性評価」とは異なる
- もっとも、適性の確認に当たってはプライバシー情報を収集することとなるため、**高度な必要性が認められる場合に限るとともに、対象者の理解を得ることに努め、技術流出防止の目的を達するために必要かつ合理的な範囲で、情報収集すべきである**
- また、**重要技術等の秘密管理を目的とした評価は、業務を行った際に重要技術等を漏らすおそれがないことについての評価であり、人事評価又は業務遂行その他の能力の実証を行うものではなく、人事評価や人事考課、解雇、懲戒処分、不利益な配置の変更等のために評価結果を利用等してはならない（目的外利用等の禁止）**
- さらに、関係法令に違反しないことが前提となる。例えば、適性の確認の実施や評価結果を踏まえた対応については、**労働基準法第3条が定める労働条件についての差別的取扱とならないようにすることが必要。**また、評価に用いる情報には、個人情報が含まれることから、その取扱いに際しては、**個人情報保護法の規定を遵守する必要がある**、取得の際における利用目的の特定・明示、要配慮個人情報の取得に係る本人の同意取得等が求められる
- また、適性の確認の実施については、本人に対して**丁寧に同意を得るプロセスを確保**することが重要。なお、その際、重要経済安保情報保護活用法に基づく適性評価でない場合は、その旨を明確に本人伝達することが必要である。理解を得るためのプロセスにおいては、実施について同意が得られなかった場合や、評価の結果、重要技術等の取扱いの業務を行った場合にこれを漏らすおそれがないと認められなかった場合、予定されていた結果として、**重要技術等へのアクセスが必要となる業務には従事できないこと、重要技術等の取扱いの業務が予定されないポストに配置換となること等があることについて、理解を得るための工夫が必要**（※対象とする情報が異なるため、必ずしも参考になるとは限らないが、例えば、重要経済安保情報保護活用法の運用基準においては、適性評価の不同意書や告知書にこれらの内容を予め確認する内容が含まれている）
- 重要技術等を取り扱っていなかった部署が、組織再編や外部環境の変動等に応じて、重要技術等を取り扱うこととなるケースも存在する。そのような場合にも、部署内に配属されている役職員等に技術情報の漏えいのおそれがないか、改めて点検することが重要である

1. ⑤ 重要技術を扱う部署への配属に際しての確認

対応策の例

適性の確認が必要となる技術情報

- 適性の確認は対象者のプライバシー情報を収集・利用する必要があるほか、対象者の理解を得る必要があり、実施にも多大なコストを要することから、**通常システムの対策では十分とはいえない高度な必要性を、丁寧に検討することが重要**。例えば、①**法令遵守のために必要なケース**や、②**技術の重要性** (第1章「2. ① 重要技術の位置づけを評価」の②・③に該当する技術を参照) に照らし、**他国に流出した場合の損失が甚大なケース** (例えば、**第三国からの制裁等を受ける可能性がある場合や、我が国の産業・技術基盤を毀損する可能性がある場合**) が考えられる
- 法令遵守のために必要なケース (①) としては、例えば、**技術の内容によって、海外の輸出管理法令等の遵守の観点から、特定の国籍の従業員への情報提供が制約されるケースが存在する**。このような場合、**自社の法令遵守の観点から必要な対応を行うために、対象技術の共有が必要となる部署への配属に当たって、必要に応じて対象者の国籍を確認することも考えられる**。また、海外の取引先から、当該取引先の法令遵守の観点から、特定の国籍の従業員への情報提供を制約するよう要請されるケースも存在する。このような場合についても、法令遵守の観点から必要な対応を行うために、対象技術の共有が必要となる部署への配属に当たって、必要に応じて対象者の国籍を確認することが考えられる
- **自社のリスク管理の観点 (②) からは、技術流出した場合に被る損失を考慮することが重要である**。特に、自社が被る損失 (レピュテーションリスクも含む) に限らず、**技術が海外に流出した場合、他国のキャッチアップが急速に進み、将来的に自社のみならず我が国業界全体の優位性・不可欠性の喪失につながる可能性についても考慮した上で、必要性を吟味することが考えられる**
- また、技術流出時の損失の程度のみならず、**技術流出の蓋然性を検討することも有用である**。例えば、**他国の獲得関心の対象となっている技術かどうか**について、**政策文書や補助金・対内投資誘致の動向等を分析し、技術の位置付け (国産化が志向されているか等) を確認することが考えられる**。自社のみでは収集可能な情報に限りがあることから、必要に応じて、業界団体や公的機関、経済産業省等に相談することも検討する

1. ⑤ 重要技術を扱う部署への配属に際しての確認

対応策の例

対象となる役職員の理解

- 適性の確認を行うに当たっては、対象となる**役職員（以下「対象者」）の理解を得ることが重要**となる
- その際には、
 - 重要技術等が流出した場合には、**自社の短期的な経済的損失のみならず、他社による急速なキャッチアップ・過剰供給等の結果として自社の経営において中長期的かつ甚大な不利益が生じる可能性があること**、
 - さらに軍事転用懸念のある安全保障上の重要技術の場合には、**軍事転用された場合に、国際社会の平和及び安全に影響を与える可能性があり、自社にとっても深刻なレピュテーションリスクにつながる**こと、
 - また、経済安全保障上の重要技術の場合には、特に海外に流出した場合、他国のキャッチアップが急速に進み、将来的に自社のみならず我が国業界全体の優位性・不可欠性の喪失につながり、ひいては**我が国の産業・技術基盤に影響を及ぼす可能性がある**こと
 - このため、流出したものに対しては**毅然とした不正競争防止法上の責任追及をせざるをえない**こと、
 - 他方で、**事後的な責任追及のみでは回復困難な利益がある**こと
 - **後述する外国政府の情報収集活動に協力する義務を法的に負っている対象者については、自社に負う守秘義務との間で、二者択一を迫られるリスクがある**こと
- 等、**こうした対応の必要性を、丁寧に説明**することが重要
- 適性の確認の実務が円滑に進むよう、労使も含めて様々なステークホルダーと対話することに努めることも重要である

1. ⑤ 重要技術を扱う部署への配属に際しての確認

対応策の例

情報収集の範囲

- 適性の確認において取得する情報の範囲については、実施する必要性との関係で、必要かつ合理的なものにすべきである。実際には、**配属部署・ポジションで扱う技術の内容や重要性、当該部署等を取り巻く環境によって異なるため、状況を踏まえた個別の検討**を行っていく必要があるが、以下の項目については、海外への技術流出リスクを評価する上で、一般的に確認することが有用な項目と考えられる。なお、いずれの項目についても、一事のみをもって配属の可否を判断できるケースは稀であり、他の項目や、対象者の業務遂行能力や過去の実績等も踏まえつつ、**総合的・客観的に評価することが重要**

① 社内における情報管理状況

- まず、自社における情報管理の状況について確認すべきである。内部監査の結果 (p66) や、研修の受講状況等 (p67)、日頃接している上長等へのヒアリングを通じて、日常的な情報管理に関する意識を確認する
- また、社内における情報管理状況については、配属時の検討に限らず日常的に確認することも重要である

② 外国政府の情報収集活動に協力する法的義務 (インテリジェンス活動協力義務) を負っているか

- インテリジェンス活動協力義務に関しては、対象者の個人的な意図に関わらず、昨今では**外国政府が自国民に情報収集活動に協力するよう法的義務を課す事例が見受けられる**ことから、外国政府等から情報収集活動への協力義務を負わされていることがないか、具体的には、**かかる義務の根拠法令の有無や内容を含め、いかなる要件が定められているかを確認**することが重要。そして、その要件への該当性を判断するために、必要な範囲で情報収集を行う
- また、法令に限らず、**外国政府・企業等との契約によって協力義務を課されているケースもありうる**ことから、**そうした契約関係にないことをあらかじめ誓約させる**ことも重要である。また、インテリジェンス活動協力義務を課するような国への渡航歴の申告を求めるとも考えられる

③ 外国政府等との関係 (反復的な連絡の有無や、外国政府機関からの給付・免除の有無等)

- ②のような法的義務ではないものの、外国政府等からの働き掛けを受けた場合に協力せざるを得ない関係になっていないかを評価する観点から、確認することが有用である。基本的には、かかる関係の有無の申告を求めるとか、関係にないことの誓約を求めるとも考えられる

1. ⑤ 重要技術を扱う部署への配属に際しての確認

対応策の例

情報収集の範囲 (続)

- ④ 情報取扱に関する前科を有しているか
 - 例えば、不正競争防止法上の営業秘密侵害罪、刑法上の秘密漏示罪、個人情報保護法上の個人情報データベース等不正提供罪等があり得る。ただし、前科は、個人情報保護法上の要配慮個人情報に該当するため (同法第2条第3項)、取得に際しては対象者の同意を得る必要がある点に留意する (同法第20条第2項)
- ⑤ 過去に情報取扱に関する非違歴があるか
 - 使用が禁止されている記録媒体への情報保存や、必要な手続を経ない文書の複写、職務に関連した事項をインターネット上のサイトに公表したりする等して、社内規程等に違反し、職業上の懲戒処分や懲戒処分には至らない上司からの指導監督上の措置 (訓告、厳重注意等) を受けたことがあるかを確認する
 - 自社における非違歴に留まらず、対象者の同意を得た上で、過去に在籍した企業等に対して、非違歴の有無に関する情報提供を求めることも有用である
- また、保護する情報の対象が異なるため、**必ずしもすべての項目について適用することは適切ではないが、重要経済安保情報保護活用法**の下で、国から共有を受けた情報を漏らすおそれがないことを確認する**適性評価の項目** (p76,77参照) を参考とすることも一案として、技術の重要度や企業において確認することが可能かどうか等を検証した上で、重要な項目を確認することも有用
- 対象者から収集する情報は基本的に個人情報に当たることから、個人情報の保護に関する法律の遵守が必要となる。例えば、
 - 取得時における利用目的の特定及び明示等 (法17条1項、21条2項)
 - 要配慮個人情報を取得する場合の本人同意の取得 (法20条2項)
 - 取得したデータについての安全管理措置 (法23条)が必要となる。

また、不正な手段による取得 (法20条1項)、本人同意なく利用目的外で利用すること (法18条1項)、不適正利用 (違法又は不当な行為を助長し、又は誘発するおそれがある方法による利用) が禁止されていること (法19条) に留意する必要がある。

個人情報の取扱いについて同意を得るに当たっては、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければならない (個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン (通則編)」2-16)。

なお、要配慮個人情報に該当しない個人情報を取得する場合については、同法上は同意取得の義務は生じないが、対象者の理解を得ることが重要であるから、そのような情報であっても、収集する必要性を真摯に説明した上で、同意を得て取得することが重要である。

1. ⑤ 重要技術を扱う部署への配属に際しての確認

対応策の例

評価結果の利用（配属の可否の判断）

- 適性の確認の実施や評価結果を踏まえた対応については、労働基準法第3条（※）に違反しないようにすることが必要
 - ※ 労働基準法第3条では、労働者の国籍、信条又は社会的身分を理由として、労働条件について差別的取扱をすることを禁止している。この場合の「理由として」とは、労働者の国籍、信条又は社会的身分が差別的取扱の決定的原因になっていると判断される場合をいい、労働者の国籍、信条又は社会的身分が差別的取扱の決定的原因に当たるかは、業務上の必要性等も踏まえて、その差別的取扱が行われた際の一切の事情を勘案した上で総合的に判断されるものである
- また、前述した外国政府の情報収集活動に協力する義務を課す法令が適用される可能性がある場合、配置において恣意的・主観的な判断を避けるために、社内規程等に従って、かような法令の制定状況やその最新の内容を定期的に確認するとともに、その法令が定める要件への該当性を判断するために必要十分な情報のみを根拠に、配属の可否を客観的に判断することが重要となる

【その他結果の取扱いに関する留意事項】

- **人事評価や人事考課、解雇、懲戒処分、不利益な配置の変更等のために評価結果を利用等してはならない。**例えば、評価結果を考慮して、解雇、減給、降格、懲戒処分、自宅待機命令、不利益な配置の変更、労働契約内容の変更の強要、昇進若しくは昇格の人事考課において不利益な評価を行うこと、又は専ら雑務に従事させる等就業環境を害することは厳に慎むべきである
- また、適性の確認の実施に際しては、評価実施部門とは別に、相談等を受ける窓口を設置・活用を検討すべきである。当該窓口においては、対象者が適性の確認の実施に当たって提供した個人情報の前記の目的外で利用されたと考える場合の相談等を受理することが想定される

個人情報保護に関する法律

(利用目的の特定)

第十七条 個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

(利用目的による制限)

第十八条 個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

(不適正な利用の禁止)

第十九条 個人情報取扱事業者は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

(適正な取得)

第二十条 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

2 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

(取得に際しての利用目的の通知等)

第二十一条 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

(安全管理措置)

第二十三条 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

労働基準法

(均等待遇)

第三条 使用者は、労働者の国籍、信条又は社会的身分を理由として、賃金、労働時間その他の労働条件について、差別的取扱をしてはならない。

重要経済安保情報の保護及び活用に関する法律

第十二条

2 適性評価は、適性評価の対象となる者（以下「評価対象者」という。）について、次に掲げる事項についての調査（以下この条及び第十六条第一項において「適性評価調査」という。）を行い、その結果に基づき実施するものとする。

一 重要経済基盤毀損活動（重要経済基盤に関する公になっていない情報のうちその漏えいが我が国の安全 保障に支障を与えるおそれがあるものを取得するための活動その他の活動であって、外国の利益を図る目的で行われ、かつ、重要経済基盤に関して我が国及び国民の安全を著しく害し、又は害するおそれのあるもの並びに重要経済基盤に支障を生じさせるための活動であって、政治上その他の主義主張に基づき、国家若しくは他人を当該主義主張に従わせ、又は社会に不安若しくは恐怖を与える目的で行われるものをいう。）との関係に関する事項（評価対象者の家族（配偶者（婚姻の届出をしていないが、事実上婚姻関係と同様の事情にある者を含む。以下この号において同じ。））、父母、子及び兄弟姉妹並びにこれらの者以外の配偶者の父母及び子をいう。以下この号において同じ。）及び同居人（家族を除く。）の氏名、生年 月日、国籍（過去に有していた国籍を含む。）及び住所を含む。）

二 犯罪及び懲戒の経歴に関する事項

三 情報の取扱いに係る非違の経歴に関する事項

四 薬物の濫用及び影響に関する事項

五 精神疾患に関する事項

六 飲酒についての節度に関する事項

七 信用状態その他の経済的な状況に関する事項

(参考) 重要経済安保情報保護活用法における適性評価の例

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の策定について (運用基準)¹

・ 適性評価の実施に当たってのお知らせ (告知書) 適性評価で調査する事項 (p.50-52)

2 適性評価で調査する事項

適性評価においては、重要経済安保情報保護活用法に定められた次に掲げる事項について調査します。

なお、以下に記載する事項に該当する事実があるからといって、重要経済安保情報を漏らすおそれがないと認められないと直ちに判断されるものではありません。

(1) 重要経済基盤毀損活動 (注) との関係に関する事項

重要経済基盤毀損活動を行ったことがある、あるいは、支援したことがあるか、重要経済基盤毀損活動を行う団体のメンバーだったことがある、あるいは、現在メンバーであるか、こうした団体を支援したことがある、あるいは、現在支援しているか、外国との関係を含め、こうした団体からの働き掛けを受けた場合に協力せざるを得ない関係になっていないかについて調査します。

なお、外国との関係があることをもって、重要経済基盤毀損活動との関係があると直ちに判断されるものではありません。

また、あなたの家族や同居人についても、その氏名、生年月日、国籍及び住所に限り調査します。このことを家族や同居人にお知らせいただいても差し支えありません。この調査は、あなたに対する外国の情報機関等からの働き掛けの有無を確認する上での参考とするためであり、これらの事項以外の事項について調査することはありません。

(2) 犯罪及び懲戒の経歴に関する事項

過去に罪を犯し、有罪の判決 (執行猶予が付いているものも含みます。) を受けたことがあるか、又は職業上の懲戒処分を受けたことがあるかについて調査します。

(3) 情報の取扱いに係る非違の経歴に関する事項

使用してはならないとされている記録媒体に情報を保存したり、必要な手続を経ずに文書を複製したり、職務に関連した事項をインターネット上のサイトに公表したりするなどして、文書やシステムの管理に関する規則等に違反し、職業上の懲戒処分や懲戒処分には至らない上司からの指導監督上の措置 (訓告、厳重注意等) を受けたことがあるかについて調査します。

(4) 薬物の濫用及び影響に関する事項

所持や使用等が禁止されている薬物を所持したり使用したりしたことがあるかや、疾病の治療のための薬物を用量を著しく超えて服用したことがあるかについて調査します。

(5) 精神疾患に関する事項

アルコール依存症、統合失調症などの精神疾患により自己の行為の是非を判別し、若しくはその判別に従って行動する能力を失わせ、又は著しく低下させる症状を呈しているかについて調査します。

なお、精神疾患に関し、治療やカウンセリングを受けたことがあるとの事実をもって、重要経済安保情報を漏らすおそれがないと認められないと直ちに判断されることはありません。必要な場合には、医療機関等に照会した上で、具体的な症状や治療の経過、再発の可能性等を踏まえ、重要経済安保情報を漏らすおそれがないかどうか判断されます。

(6) 飲酒についての節度に関する事項

飲酒を原因として、けんかなどのトラブルを引き起こしたり、業務上の支障を生じさせたりしたことがあるかについて調査します。

(7) 信用状態その他の経済的な状況に関する事項

住宅、車両及び耐久消費財の購入並びに教育といった一般的な目的とは異なる借入れがあるか、金銭債務の不履行があるか、自己の資力に照らし不相当な金銭消費があるかなど、経済的な状況について調査します。

(注) 「重要経済基盤毀損活動」とは、公になっていない情報のうちその漏えいが我が国の安全保障に支障を与えるおそれがあるものを取得するための活動その他の活動であって、外国の利益を図る目的で行われ、かつ、重要経済基盤に関して我が国及び国民の安全を著しく害し、又は害するおそれのあるもの (重要経済安保情報を標的としたいわゆるスパイ活動等) や、重要経済基盤に支障を生じさせるための活動であって、政治上その他の主義主張に基づき、国家若しくは他人を当該主義主張に従わせ、又は社会に不安若しくは恐怖を与える目的で行われるもの (重要経済基盤を標的とするいわゆるテロリズム) を指します。スパイ活動等において取得の対象となる情報としては、重要経済基盤に関し政府の保有する情報で我が国及び国民の安全を確保する観点から保護すべきものが想定される他、政府が関知するに至っている民間保有の機微な情報でその漏えいが我が国及び国民の安全の確保に支障を与えるおそれがあるもの (例えば、我が国における重要物資のサプライチェーン上の脆弱性に関する情報) も含まれます。

¹https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/kijun.pdf

(参考) 重要経済安保情報保護活用法における適性評価の例

重要経済安保情報保護活用法の運用に関するガイドライン（適合事業者編）（第1版）¹

2 目的外利用等の禁止（2）適性評価に関する個人情報の利用及び提供の制限（目的外利用の禁止）

なお、以下は上記の「目的外利用」に関する具体例である。

- 適性があるとは認められなかった者について、予定していた重要経済安保情報の取扱いの業務を行わせないことについては、そもそも本法が予定していることであり、「目的外利用」に当たらないと解釈される。
- 適合事業者において、重要経済安保情報の取扱いの業務を行わせる前提で採用又は採用内定した場合において、当該者につき適性があるとは認められなかったときは、採用又は採用内定の当初の目的を達成できないことになる。この場合において、当該者の採用や採用内定の取消をすることは本法との関係で問題になるものではないが、最終的に当該取消が可能であるか否かは、司法において個別具体的に判断されることになる。
- 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については、重要経済安保情報の取扱いの業務の難易度とそれに対する遂行能力、当該業務を遂行する上で当該従業者が負う業務上の責任などを全体として評価した結果であり、適性があると認められ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と解釈される。

適性評価に関するQ&A（第1版）²

<評価>（6ページ）

Q19. 以下のような事情がある者は、適性が認められないと判断されますか。

- ・外国籍である場合や、外国籍の者と結婚している場合、外国籍の者や外国との関係が深い場合
- ・外国の金融機関の口座や外国の不動産を保有している場合

A. 外国との関係が深いことなどのみをもって、直ちに適性があると認められないと判断されるわけではなく、個別具体的な事情を考慮して総合的に判断されます。

¹ https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/jigyousyagl.pdf

² https://www.cao.go.jp/keizai_anzen_hosho/hogokatsuyou/doc/tekiseihyoukaqa.pdf

(参考) 海外における適性評価の例 [1/3]

米国「National Security Adjudicative Guidelines」(国家情報長官室 (ODNI)) [仮訳]

目的¹	<ul style="list-style-type: none">機密情報へのアクセス、または機密性の高い地位に就く資格を初回または継続的に必要とするすべての対象者に対して、単一かつ共通の審査判断基準を定めるもの
考え方²	<ul style="list-style-type: none">審査プロセスとは、当該人物の人生の十分な期間にわたり、その人の複数の変数 (行動・背景等) を慎重に天秤にかける検討である。これを“Whole-Person Concept (全人格評価)”と呼ぶ。過去・現在、好ましい情報も不利な情報も含め、利用可能で信頼できるあらゆる情報を考慮して、国家安全保障に関する資格の適格性を判断する
具体的な考慮要素 (詳細次頁)	<ul style="list-style-type: none">忠誠心外国の影響外国の優先性的行動個人の行動財務状況アルコール摂取薬物との関わり心理状態犯罪行為機密情報取扱い外部活動IT利用

1. <https://www.odni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>

2. <https://www.cdse.edu/Portals/124/Documents/jobaid/personnel/National-Security-Adjudication.pdf>

(参考) 海外における適性評価の例 [2/3]**各考慮要素の詳細 (同ガイドライン Appendix A) [仮訳]**

項目	想定する懸念
忠誠心	個人は、米国に対して疑いのない忠誠心を持っていなければならない。忠誠に疑念があれば、機密情報を守る意思そのものが疑われる。
外国の影響	個人の直系家族が米国市民でない場合、または強要を受ける可能性がある場合、安全保障上のリスクが生じ得る。これらの状況は外国からの影響を受ける可能性を生み、その結果として機密情報が漏えいするおそれがある。また、他国の市民との接触や他国における財政的利害関係も、個人が強要・搾取・圧力に対して脆弱となる可能性がある場合、安全保障上の判断において重要となる。
外国の優先	個人が、米国よりも外国を優先するような行動を示す場合、その者は米国の利益にとって有害となる情報を提供したり、判断を下したりする傾向を有する可能性がある。
性的行動	性的行動が、犯罪行為を伴う場合、人格または情緒の障害を示す場合、個人を強要・搾取・脅迫にさらす可能性がある場合、あるいは判断力や慎重さの欠如を反映している場合には、安全保障上の懸念事項となる。ただし、性的指向や性的嗜好は、安全保障クリアランスの適格性を判断する際の根拠または失格理由として用いてはならない。
個人の行動	疑わしい判断、不信頼性、信頼性の欠如、率直さの欠如、不誠実さ、または規則や規制に従う意思の欠如を伴う行為は、その人物が機密情報を適切に保護しない可能性を示すものである。通常、以下の事由は、不利なクリアランス処分、またはクリアランス適格性に関する手続きの行政的終了につながる (略)
財務状況	財政的に過度の負債や支出を抱えている個人は、資金を得るために違法行為に関与せざるを得なくなるリスクがある。また、説明のつかない裕福さは、金銭的利益を伴う犯罪行為の収益と関連していることが多い。
アルコール摂取	過度のアルコール消費は、疑わしい判断、不信頼性、衝動の抑制の失敗を招くことが多く、不注意による機密情報の不正開示のリスクを高めるものである。

(参考) 海外における適性評価の例 [3/3]**各考慮要素の詳細 (同ガイドライン Appendix A) [仮訳] (続き)**

項目	想定する懸念
薬物との関わり	薬物に対する不適切または違法な関与は、個人が機密情報を保護する意思または能力に関して疑問を生じさせるものである。薬物乱用または薬物依存は、社会的または職業的機能を損ない、機密情報の不正開示のリスクを高める可能性がある。(略)
心理状態	情緒的、精神的、または人格上の障害は、個人の心理的・社会的・職業上の機能に重大な欠損を生じさせ得る。これらの障害は、判断力、信頼性、あるいは安定性に欠陥があることを示す可能性があるため、安全保障上の懸念事項となる。潜在的な失格要因や軽減要因を十分かつ適切に評価するためには、政府に雇用されているか、政府が受け入れまたは承認した資格を持つ精神保健専門家（例：臨床心理士または精神科医）を利用するべきであり、特に当該個人の精神保健提供者との協議において重要である。
犯罪行為	犯罪行為の履歴または繰り返しは、その人物の判断力、信頼性、および誠実性に疑念を生じさせるものである。
機密情報取扱い	安全保障規則に従わないことは、個人の誠実性、意思、および機密情報を保護する能力に疑念を生じさせるものである。
外部活動	特定の種類の外部雇用や活動への関与が、個人の安全保障上の責務と競合し、機密情報の不正開示のリスクを高める可能性がある場合、それは安全保障上の懸念事項となる。
IT利用	情報技術システムに関する規則、手順、指針、または規制に従わないことは、個人の誠実性、意思、および機密性を要するシステム、ネットワーク、情報を適切に保護する能力について、安全保障上の懸念を生じさせる可能性がある。情報技術システムとは、機密情報または敏感な情報の通信、伝送、処理、操作、保存に使用されるすべての関連機器を含むものである。

1. ⑥ 副業等を通じた情報流出の防止

- 近年、働き方の多様化やスポットコンサルの普及等が進んでいるが、このような副業・兼業を通じて技術情報を漏えいするケースも存在
- そのため、社内規程で**副業・兼業のルールを明確化**するとともに、**研修等により周知・徹底**する

対応策の例

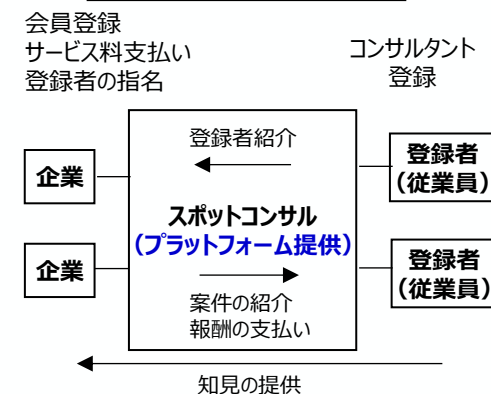
① 副業・兼業ルールの明確化・届出手続の徹底

- 労働時間以外の時間をどう利用するかは原則として従業員の自由だが、副業・兼業が、会社の秘密漏えいや、競業による利益侵害、信用毀損等に繋がるおそれのある場合、制限する必要性は高い
- 従業員の副業・兼業からの技術流出を防止するため、労使でも話し合い、就業規則等において、副業・兼業する場合の事前届出を義務付ける
- 副業・兼業の可否については、必要に応じて上長も関与し、以下の点を考慮して検討する
 - ✓ 当該従業員が重要な技術情報に触れる職務に従事しているか、過去に従事していたか
 - ✓ 今後、自社の重要な技術情報を取扱いが発生するか
 - ✓ 副業・兼業と自社事業の間に競合関係・取引関係その他の技術流出の動機・機会に繋がりうる関係がないか
- 人事異動を検討する際は、当該役職員の副業・兼業の有無や内容も考慮する。異動により競業又は情報漏えいのおそれが生じる場合、業務範囲の見直し等を含め、慎重に判断する

② スポットコンサルのチェック

- スポットコンサル会社のプラットフォームに自社従業員が登録していないか定期的な見回り等を通じて確認する
- 副業・兼業ルールに違反する場合や、情報漏えいのおそれがある場合は、本人に対する指導を行う。また、就業規則違反の事例が散見される場合は、スポットコンサル会社にも協力を要請する

スポットコンサルの仕組み



※社内規程で副業・兼業のルールを明確化するには、厚生労働省が策定した「副業・兼業の促進に関するガイドライン」も参照されたい(厚生労働省HPからダウンロード可能)
<https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/0000192188.html>

参考裁判例

- 大阪地判平成27年8月3日（平成25年（ワ）3282号）

【事案概要】

ある会社（本業先）の統括本部長であった元従業員が、在職中に、本業先と競合する会社を設立し、本業先の顧客に対して競合事業に関する営業行為を行ったことから、本業先が当該元従業員に対して、損害賠償を求めた事案。なお、本業先の就業規則には在職中の兼業許可制が定められていた一方で、当該元従業員は、退職時の秘密保持・競業避止に関する誓約書の提出を拒否していた。

判決では、当該元従業員の在職中の競業行為について、会社の許可を得ずに兼業を行ったものとして、上記の就業規則の違反による債務不履行が認められた。

【判決抜粋】

（前略）労働時間以外の時間をどのように利用するかは、本来労働者の自由であるから、兼職は労働者の自由であるのが原則である。他方、労働者は、使用者に対し、労働契約上、労働時間外においても誠実義務を負っており、兼職についても一定の制約があることは免れない。したがって、兼職許可制は、使用者の正当な利益を確保する限度で有効であると解すべきであるから、兼職の態様や期間等からみて本来の業務に支障を生じさせる可能性がある兼職や、競業他社で就労したり役員に就任したりするなど企業秩序を著しく乱すような兼職のみが許可制違反に該当するというべきである。（後略）

- 福岡地判昭和59年1月20日（昭和56年（モ）3103号）

【事案概要】

タクシー会社に勤務する運転手が、父親が経営する新聞販売店の配達業務等への従事を理由になされた懲戒解雇の効力を争った事案。

判決では、兼業による企業秩序への侵害の程度や労務提供への支障の状況を考慮し、一部の時期の兼業は就業規則上禁止される兼業には該当しないが、それ以外の時期の兼業は就業規則上禁止される兼業に該当するとされた上で、懲戒解雇については後者の限度で懲戒処分事由は認められるものの、労働者の受ける不利益が著しく大きいとして解雇権の濫用に当たり無効とされた。

【判決抜粋】

（前略）兼職禁止規定の適用にあたっては、一般に、労働者は労働契約に定められた時間、場所において、契約に定められた労働を提供する義務があるが、時間外においては、特約なき限り他の者のために働いてはならない義務はないこと、債務者会社の右就業規則においては、兼職禁止規定違反の制裁は、懲戒解雇という重い処分のみとされていることなどに照らすと、右兼職禁止規定に違反するのは、会社の企業秩序を乱し、会社に対する労務の提供に格別の支障を来たす程度のものであることを要すると解すべきである。（後略）

※その他の裁判例については、「副業・兼業の促進に関するガイドライン」パンフレットも参照されたい。（前ページの厚生労働省HPからダウンロード可能）

1. ⑦ 競業避止義務契約の適切な活用

- 役職員の退職後の技術流出を防止するため、就業規則や退職時の誓約書において、**役職員が退職後に競合他社で業務を行うことを制限する規定（競業避止義務）**を導入することは重要
- 競業避止義務は、**職業選択の自由の制約となり得るため、その有効性について訴訟で争われる場合がある。企業側の守るべき利益を保全するために必要な限度の制約とする必要がある**

対応策の例

競業避止義務の有効性について、以下で詳細な分析が行われているため、必要に応じて参照いただきたい
<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/honpen.pdf>

- **競業避止義務の有効性をめぐる訴訟では、当該義務の内容が、企業の守るべき利益を保全するという目的に照らし、合理的な範囲に留まっているかという観点で判断される**
 - ✓ 従業員の地位：企業が守るべき秘密情報に真に接しているか
 - ✓ 転職先の地域的な限定：事業内容に鑑みて地理的な制限を付す必要はないか（付すことで役職員への制約を軽減できるか）
 - ✓ 競業避止義務の存続期間：企業の利益と労働者の不利益を考慮して、合理的な期間が設定されているか
 - ✓ 禁止される競業行為の範囲：競業企業への転職を一般的・抽象的に禁止するのではなく、業務内容や職種等で制限を付しているか
 - ✓ 代償措置が講じられているか：高額な賃金や割増退職金の支払い等が行われているか
- **上記を踏まえ、経済安全保障の観点から高まる技術流出リスクへの対応として、以下の視点を考慮し、競業避止義務契約の内容を検討することが重要**
 - ✓ 企業側の守るべき利益を保全するという目的に照らし、自社の重要技術、とりわけ競争力の源泉となる技術（p15参照）を扱っていた人物かどうかを丁寧に検討する
 - ✓ 当該重要技術が経済安全保障上も重要である（優位性・不可欠性がある）場合、技術格差の大きい他国が技術的獲得に関心を有していることがある。そのような場合、当該国に技術が流出するとキャッチアップの契機となり、わが国の経済安全保障に影響を与える可能性があるため、当該国又は当該国企業（子会社を含む）での競業を一定期間制限する必要性は高い
 - ✓ 重要技術を取り扱う部署の役職員は然るべく処遇すべきであるが、離職に当たり競業避止義務を課す場合にも、相応の代償措置を講じることが重要
- なお、外国拠点の役職員や外国籍の役職員と締結する競業避止義務契約については、当該外国の法令等が適用される可能性もあるため、この点には留意を要する

(参考) モデル条項

- 競業禁止義務の定め方については、就業規則に規定を設ける事例と、個別の誓約書に規定を設ける事例がある。それぞれのモデル条項について、以下のとおり。
- 経済産業省「秘密情報の保護ハンドブック～企業価値の向上に向けて～ 参考資料 5 競業禁止義務契約の有効性」において指摘されているとおり、就業規則に規定を設け、かつ、規定した内容と異なる内容の個別の誓約書を結ぶことについては、就業規則に定める基準に達しない労働条件を定める契約の効果を無効とする労働契約法12条との関係が問題となる。このため、実務上は、**就業規則には「従業員は在職中及び退職後6ヶ月間、会社と競合する他社に就職及び競合する事業を営むことを禁止する」というような原則的な規定を設けておき、加えて、就業規則に、例えば「ただし、会社が従業員と個別に競業禁止義務について契約を締結した場合には、当該契約によるものとする」というように、個別合意をした場合には個別合意を優先する旨規定しておけば、労働契約法12条の問題は生じず、規則の周知効果を狙うという観点からも記載をしておくべきである。**

就業規則の規定例

(競業禁止義務)

第〇〇条

従業員は在職中及び退職後 6 ヶ月間、会社と競合する他社に就職及び競合する事業を営むことを禁止する。ただし、会社が従業員と個別に競業禁止義務について契約を締結した場合には、当該契約によるものとする

個別合意の例 (誓約書の例)

貴社を退職するにあたり、退職後1年間、貴社からの許諾がない限り、次の行為をしないことを誓約いたします。

- 1) 貴社で従事した〇〇の開発に係る職務を通じて得た経験や知見が貴社にとって重要な企業秘密ないしノウハウであることに鑑み、当該開発及びこれに類する開発に係る職務を、貴社の競合他社 (競業する新会社を設立した場合にはこれを含む。以下、同じ。) において行いません
- 2) 貴社で従事した〇〇に係る開発及びこれに類する開発に係る職務を、貴社の競合他社から契約の形態を問わず、受注ないし請け負うことはいたしません

※経済産業省「秘密情報の保護ハンドブック～企業価値の向上に向けて～参考資料 5 競業禁止義務契約の有効性」 (<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>) を参照 (p219～)

1. ⑧ アクセスコントロールの徹底

- **Need-to-Know**の原則を徹底し、**当該技術情報を知る必要性のある役職員にのみアクセス権を設定することが重要である**。配属における適性の確認（p69～）と同様に、配属におけるポストと、それに紐付く技術情報へのアクセス権を明確にしておくことが重要である
- また、アクセス権の見直しも重要であり、**人事異動や転職・退職等に伴って即時にアクセス権を再設定することも重要である**

対応策の例

① アクセス権限の設定に関するルールの明確化

- 情報管理規程等において秘密情報の分類（極秘・社外秘等）を設定した上で（p22参照）、技術の重要度に応じたランク付けや、ランクに応じたアクセス権限の設定を、どのような手順で誰が行うかを明確にしておくことが重要

② アクセスできる人員の限定

- 技術情報の秘匿性によっては、必要に応じて適性の確認の結果も踏まえつつ（p69～参照）、アクセスできる人員を必要最小限に絞り込むことが重要となる
- また、人事異動や転職等に伴い迅速にアクセス権が変更できるよう、人事部門との情報共有を密に行う体制を構築することも重要。退職予定者については、必要に応じて、次ページのとおり、退職前からアクセス権限を制限することも重要である
- さらに、例えば、アクセス権限を持たない役員等が、その地位を利用して、一般の従業員に重要情報の開示を要求し外部へ持ち出すようなケースもあるため、注意が必要である

③ アクセス方法の限定

- 技術情報が電子データとして存在するか、書類等に記録されているかによって変わりうるが、他の情報と区別して管理し、アクセス方法を限定することが重要である
- 近年リモートワークが一般化しているが、セキュアな環境で作業しないケースもあり得ることから、重要な技術情報へのアクセス制限を含め、ルールを定める

④ 権限範囲・期間の限定

- 情報の重要度に応じて、印刷用権限（管理者向け）と閲覧用権限（作業向け）を区別して付与する等、従業員ごとにアクセス可能な範囲を設定することも重要
- 恒常的にアクセス可能とすべき情報と、そうでないものが存在するケースもある。重要な技術情報については、利用期間も考慮の上、アクセス可能期間を定めて、期間を経過した時点で管理者以外のアクセスを制限することも有用

※本対策と関連して、より詳細な対策については、「秘密情報の保護ハンドブック ～企業価値向上にむけて～」3-4 具体的な情報漏えい対策例 (1) 従業員等に向けた対策のうち「①「接近の制御」に資する対策」も参照されたい

（経済産業省HP: <https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>）

1. ⑨ 退職時のアクセス制限

- 退職者から技術流出するケースでは、退職直前に重要なファイルをダウンロード等される場合もある。このため、退職予定者については、**アクセス権限の解除や業務範囲の限定**により、重要な技術情報へのアクセスを制限することが重要
- また、退職予定者に対しては、**他の役職員よりも厳格に、情報アクセスのログ取得や**（退職の申し出よりも前のログも含めた）**分析**を行い、**情報流出の予兆を退職前に検知、対処**することが重要

対応策の例

①重要情報へのアクセスを制限する

- 退職を申告した役職員の業務を、引継ぎ等のために必要最低限の範囲に限定し、データアクセス権限やセキュリティエリアへの入室権限を解除する

②退職予定者について、より厳格なアクセスログ取得・分析を行う

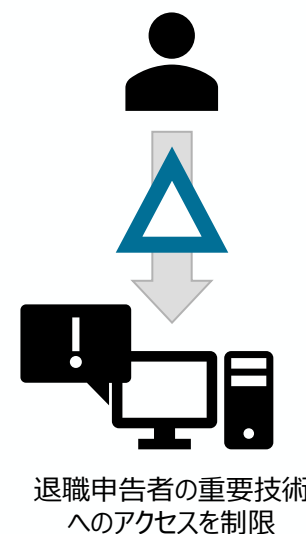
- 当該役職員の職種等に応じて、直近アクセスした技術情報の内容、外部へのメール送信の履歴等を、必要に応じて数ヶ月遡り、警戒度を高めてチェックする。情報流出の予兆があれば、退職前にヒアリング等を実施する

③貸与物品等を確実に返却させる

- 退職予定日まで、PC等の会社の貸与物品や、図面・マニュアル等の文書を返却させる

④退職後の秘密保持義務と違反した場合の対応に関する説明を行う

- 退職前に面談し、就業規則や在職中の誓約書等により退職後の秘密保持義務を課していることを前提に、注意喚起のため、改めて技術情報の重要性や秘密保持義務の内容、違反した場合に法的措置を講じる旨を明確に説明する



退職申告者の重要技術へのアクセスを制限

※技術流出防止の観点からは、退職後も秘密保持義務を課することが必要。その際、誓約書等によって同義務を定める場合においても、退職者の職業選択の自由や営業の自由を不当に制限することのないよう注意が必要である。裁判例の中には、「その秘密の性質・範囲、価値、当事者（労働者）の退職前の地位に照らし、合理性が認められるときは、公序良俗に反せず無効とはいえない」としたものがある。一方、保護対象となる機密事項の定義も例示もない誓約書に基づく退職後の秘密保持義務について、「予測可能性を著しく害し、退職後の行動を不当に制限する効果をもたらすものであって不合理である」とした裁判例もある（次ページの参考裁判例を参照）。いずれにせよ、日常的な営業秘密管理の徹底が前提となることを理解する必要がある

参考裁判例

○ 東京地判平成14年8月30日（平成13年（ワ）21277号）

【事案概要】

転職元企業が、同業他社に転職した元従業員に対して、在職中に担当した顧客への営業活動が、在職中に提出された誓約書に基づく退職後の秘密保持義務及び競業禁止義務に違反するとして、損害賠償を求めた事案。

判決では、誓約書の定める秘密保持義務は合理性を有するもので、有効とされた。

【判決抜粋】

（前略）このような退職後の秘密保持義務を広く容認するときは、労働者の職業選択又は営業の自由を不当に制限することになるけれども、使用者にとって営業秘密が重要な価値を有し、労働契約終了後も一定の範囲で営業秘密保持義務を存続させることが、労働契約関係を成立、維持させる上で不可欠の前提でもあるから、労働契約関係にある当事者において、労働契約終了後も一定の範囲で秘密保持義務を負担させる旨の合意は、その秘密の性質・範囲、価値、当事者（労働者）の退職前の地位に照らし、合理性が認められるときは、公序良俗に反せず無効とはいえないと解するのが相当である。（後略）

○ 東京地判平成20年11月26日（平成20年（ワ）853号）

【事案概要】

転職元企業が、同業他社に転職した元従業員に対して、在職中に得た商品の仕入先情報の利用が、在職中に提出された誓約書に基づく退職後の秘密保持義務及び競業禁止義務に違反するとして、損害賠償を求めた事案。なお、当該元従業員が提出した誓約書は2通あり、それぞれ次の条項が定められていた。判決では、当該仕入先情報は、誓約書に定める秘密保持義務の対象に当たらないとされた。

- ・「業務上知り得た会社の機密事項、工業所有権、著作権及びノウハウ等の知的所有権は、在職中はもちろん退職後にも他に一切漏らさないこと。」
- ・「私は、貴社を退職後も、機密情報を自ら使用せず、又、他に開示いたしません。」

【判決抜粋】

（前略）従業員が退職した後においては、その職業選択の自由が保障されるべきであるから、契約上の秘密保持義務の範囲については、その義務を課すのが合理的であるといえる内容に限定して解釈するのが相当である・・・秘密保持の対象となる本件機密事項等についての具体的な定義はなく、その例示すら挙げられておらず・・・いかなる情報が本件各秘密合意によって保護の対象となる本件機密事項等に当たるのかは不明といわざるを得ない。しかも、前記(1)で検討したとおり、原告の従業員は、本件仕入先情報が外部に漏らすことの許されない営業秘密として保護されているということを認識できるような状況に置かれていたとはいえないのである。このような事情に照らせば・・・本件仕入先情報が本件機密事項等に該当するとして、それについての秘密保持義務を負わせることは、予測可能性を著しく害し、退職後の行動を不当に制限する結果をもたらすものであって、不合理であるといわざるを得ない。したがって、本件仕入先情報が秘密保持義務の対象となる本件機密事項等に該当すると認めることはできない。（後略）

1. ⑩ デバイスの管理・利用ルール of 徹底

- 多くの技術情報は電子ファイルとして存在しており、PC・スマートフォン等の電子デバイスによって取り扱われるケースが多い
- そのため、**役職員が使用するデバイスを会社が適切に管理することが重要である**

対応策の例

① 業務用デバイスは会社が所有・貸与する

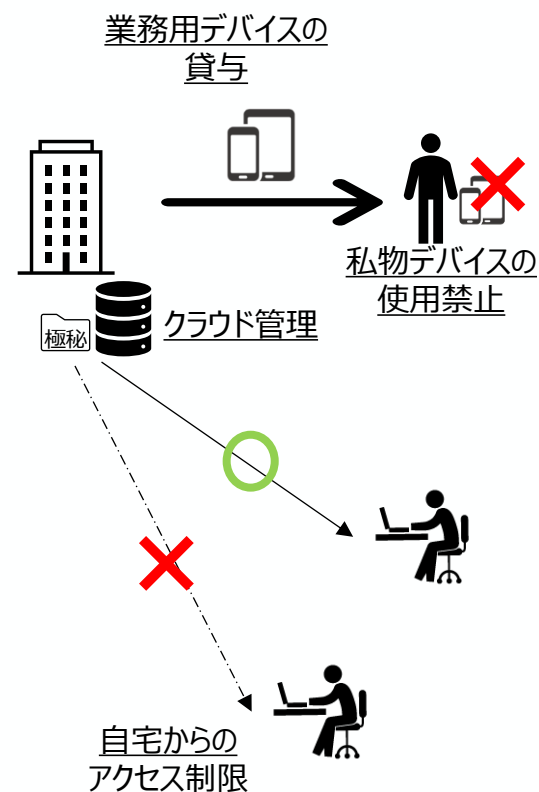
- 業務用デバイスは、会社が所有・支給することで、その管理・利用方法や退職時の返却について、会社の指示に従う必要のある仕組みとする。特に、私的な海外旅行等業務外の渡航の際には、持参を禁止する等のルールを整備し、運用を徹底する（その他海外渡航の際の注意点はp93参照）
- 私物デバイスを使用せざるを得ない場合、情報管理部門等の承認やデバイス登録を条件とし、廃棄・処分時のルールも明確化する
- 異動時には、他部門に技術情報を持ち出せないよう、デバイスの交換やアクセス制限等を行う
- 業務用デバイスにログインする際には、生体認証等を含め、セキュリティを強化する

② デバイスの紛失・盗難に備える

- デバイスの紛失・盗難に備えて、リモートでのデータ消去、遮断等ができるようにする
- クラウド管理により、デバイスへのデータ保存そのものを制限するような方法も有効

③ USBメモリ等へのコピーを禁止・制限する

- 技術情報を業務用デバイス外で保存しないよう、USBメモリ等へのコピーを禁止する（USBポートのブロック等）
- 業務上の必要性がある場合には、情報管理部門等の承認を条件とし、会社所有のUSBメモリ等へのコピーに限定する



1. ⑪ ソフトウェアやSNS等の利用ルールの徹底

- 検索エンジンや生成AI等を業務のために利用するケースが増加。しかし、こうしたサービスの提供事業者等が、ユーザーの入力した情報を保有する場合もあり、技術流出に繋がる可能性がある
- そのため、重要な技術に関する情報は生成AIのプロンプトに入力しない等、**利用方法やルールを明確にすることが重要**
- また、**SNS等の利用に関しても、技術流出を防ぐ観点から利用ルールを策定**する。また、SNS等を通じた**不審なアプローチについて、会社へ報告する仕組み**も構築することも有効

対応策の例

①社内ポリシーでソフトウェアの利用方法を定める

- 業務用デバイスへのソフトウェアのインストールは許可制とし、情報セキュリティに疑いのあるソフトウェアについては、インストールできないようにする
- 生成AI、翻訳サイト、検索エンジン等のツールについては業務に資するものもある。利用を禁止するだけでなく、契約においてデータの利用に制限をかける、利用に当たっての社内ルールを策定する（懸念のあるツールがあればネガティブリストを作成する）等の対策により、可能な限りセキュアな環境を構築することも重要

インストールの
許可制

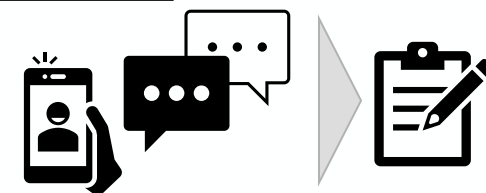
情報の機微度に応じた
生成AI等への入力禁止



②SNS等の利用ルールについても定める

- SNS等による情報流出を防止するため、SNS等の利用ルールを策定し、社内規程に盛り込む。研修等を通じ、役職員へ周知徹底を行う
- 公開されている情報に自社情報が含まれていないか定期的な見回り等を通じて確認をする
- SNS等を通じて、情報提供等を求める不審なアプローチを受けた場合には、上司や専用窓口等への報告を求める

SNS利用ルール



※AI活用に関しては、AI事業者ガイドラインも参照されたい。特に、「AI事業者ガイドライン（第1.2版）別添」においては、AIによるリスクの一つとして、機密情報の流出が挙げられているため（p20）、必要に応じて参照されたい。

https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20260331_report.html

1. ⑫ 技術流出に繋がるおそれのある行為の検知・警告

- 意図的な技術流出が生じる前には、大量の印刷やデータダウンロード等、通常とは異なる行動を伴うケースが多いため、**技術流出に繋がるおそれのある行為を検知するシステムを整備**することが有効
- また、具体的な検知方法は明かさないうにつつ、技術流出に繋がるおそれのある行為を**組織的に検知していることを周知・警告**することで、不適切な行動の抑止にもつながる

対応策の例

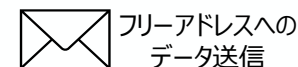
① 技術流出に繋がるおそれのある行為を検知するための体制を整備する

- 意図的なケースを含め、技術流出に繋がるおそれのある行為（大量のファイルの印刷やダウンロード、深夜・休日の頻繁なアクセス、フリーアドレスへのデータ送信等）については、システム上の検知が可能なものも多い。必要に応じて外部のセキュリティシステム等を導入し、平時よりこうした行為を事前検知できる体制を整備する
- また、システム対応以外でも、技術流出に繋がるおそれのある行為に関する通報窓口を設置することも有効
- 不適切な行為を検知した場合、上長への通知や本人へのヒアリング等により事実確認する

技術流出に繋がる
おそれのある行為を検知



大量のファイル印刷、ダウンロード



フリーアドレスへの
データ送信

② 技術流出に繋がるおそれのある行為を検知していることを周知・警告する

- 組織的に検知システム等を設けていることを周知し、抑止につなげる
- また、社内研修等において、技術流出をした場合には懲戒処分や訴訟等の対象になり得る（割に合わない行為である）ことを周知する

検知の周知・警告



③ 技術流出に繋がるおそれのある行為を技術的に不可能にする

- 技術情報の重要度・機微度によっては、技術的な設定により印刷やメール送信を禁止する

※会社が管理する社内ネットワークシステムについては、業務上必要な範囲を超えた利用を就業規則において制限することが重要である。一方で、社内ネットワークシステムの監視・調査には、プライバシー保護の観点から注意が必要である。「監視の目的、手段及びその態様等を総合考慮し、監視される側に生じた不利益とを比較衡量の上、社会通念上相当な範囲を逸脱した監視がなされた場合に限り、プライバシー権の侵害となる」とした裁判例がある。企業の運営上必要かつ合理的なものであり、労働者の人格や自由に対する行きすぎた支配や拘束とならないよう注意が必要である。（次ページの参考裁判例を参照）

参考裁判例

- 東京地判平成13年12月3日（平成12年（ワ）12081号・平成12年（ワ）16791号）

【事案概要】

ある従業員の上司が、当該従業員が誤送信したメールを受信したこと等をきっかけに、自らをセクシュアル・ハラスメント行為で告発しようとしている動きを察知し、当該従業員の業務メールを監視していたことについて、当該従業員が、プライバシー侵害を理由に損害賠償を求めた事案。

判決では、当該業務メールの閲覧・監視行為について、プライバシー侵害には当たらないとされた。

【判決抜粋】

（前略）このような状況のもとで、従業員が社内ネットワークシステムを用いて電子メールを私的に使用する場合に期待し得るプライバシーの保護の範囲は、通常の電話装置における場合よりも相当程度低減されることを甘受すべきであり、職務上従業員の電子メールの私的使用を監視するような責任ある立場にない者が監視した場合、あるいは、責任ある立場にある者でも、これを監視する職務上の合理的必要性が全くないのに専ら個人的な好奇心等から監視した場合あるいは社内の管理部署その他の社内の第三者に対して監視の事実を秘匿したまま個人の恣意に基づく手段方法により監視した場合など、監視の目的、手段及びその態様等を総合考慮し、監視される側に生じた不利益とを比較衡量の上、社会通念上相当な範囲を逸脱した監視がなされた場合に限り、プライバシー権の侵害となると解するのが相当である。（後略）

- 東京地判平成14年2月26日（平成12年（ワ）11282号）

【事案概要】

ある従業員に対して誹謗中傷メールが送信された事案の調査に際して、会社が、調査対象者の業務用パソコンおよび業務メールの内容を調査したことについて、当該調査対象者が、プライバシー侵害を理由に損害賠償等を求めた事案。

判決では、当該調査について、プライバシー侵害には当たらないとされた。

【判決抜粋】

（前略）企業は、具体的な規則を定めるまでもなく当然のこととして、企業秩序を維持確保するため、具体的に労働者に指示、命令することができ、また、企業秩序に違反する行為があった場合には、その違反行為の内容、態様、程度等を明らかにして、乱された企業秩序の回復に必要な業務上の指示、命令を発し、又は違反者に対し制裁として懲戒処分を行うため、事実関係の調査をすることができる。しかしながら、上記調査や命令も、それが企業の円滑な運営上必要かつ合理的なものであること、その方法態様が労働者の人格や自由に対する行きすぎた支配や拘束ではないことを要し、調査等の必要性を欠いたり、調査の態様等が社会的に許容しうる限界を超えていると認められる場合には労働者の精神的自由を侵害した違法な行為として不法行為を構成することがある。（後略）

1. ⑬ 工程の細分化・全体工程を知る役職員の限定

- 生産プロセスの全体工程等、コア技術の全容を知る役職員を起点に技術流出が生じた場合、そのダメージも甚大なものとなる
- 被害を最小限に留めるため、**研究開発・製造工程を細分化し、各担当者が知り得る情報を限定する**。同時に、全体工程を知る役職員は一定数必要であるため、**全体工程を知る役職員を限定し、組織的に把握することが重要**

対応策の例

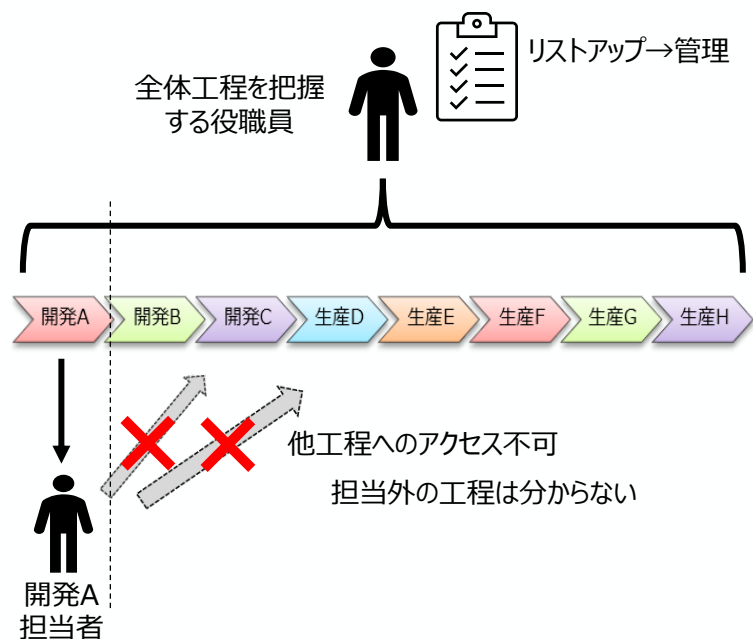
① 工程を細分化し、各担当者が知り得る情報を限定する

- 重要なノウハウやコア技術が用いられる製造プロセスについては、製造拠点や原料調達先を分散させ、広く一般の担当者レベルでは全体工程を把握できないようにする
- 製造拠点の分散が難しい場合は、工程ごとに管理区域を設定し、人員配置や入退室・アクセス権限の設定等によって、管理上の細分化を実現する (アクセス権限の設定についてはp85も参照)
- 各工程の担当者間で品質向上等のためにコミュニケーションをとる必要がある場合には、全体工程を知る限られた役職員がハブの役割を果たす等の対応を講じて、情報のやりとりに注意する

② 全体工程を知る役職員を限定・把握する

- 全体工程を知る役職員を、その必要性がある者に限定したうえで、会社側でリストアップして把握する
- 当該役職員については、給与面を含めて責任に見合う処遇を行う (p100参照)。また、当該役職員への不審なアプローチ等がないか重点的に把握する

工程細分化とリストアップのイメージ



1. ⑭ 海外出張や赴任時の情報管理

- 海外に出張・赴任する役職員が、国内と異なる環境で、意図せずに情報を流出してしまうケースがある。**アクセス権限の設定やデバイス管理**等に留意が必要

対応策の例

① アクセス権限を再設定する

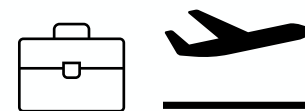
- 海外に赴任した役職員が、引き続き、日本国内のシステムにアクセスできる場合、当該役職員の使用するデバイスを経由して技術情報が漏えいするケースがある
- 人事異動に伴うアクセス権限のリアルタイムの更新は、日常的にも重要な対策であるが、海外赴任者については特に注意する

② デバイスの持参ルールを定める

- 海外出張時に、業務用デバイスを海外に持参する際のルールを定める
- 外国の法制度等の内容(p33参照)も踏まえて、技術流出リスクが高いと判断した地域に出張する場合には、日頃利用しているデバイスの持参を禁止したり、情報管理部門の承認を必要とするといった対応が考えられる
- また、業務上の必要性がある場合は、コア技術の情報にアクセスできない出張用デバイスを用意することや、紛失時に日本からのデータ消去やアクセスブロックが可能な設定を行う等の対応が考えられる
- 通常の出張とは異なる長期出張や海外赴任に当たっては、新しい業務用デバイスを貸与する。また、私的旅行等業務外の渡航の際には、業務用デバイスの持参を禁止する等のルールを整備する

③ カウンターインテリジェンスに関する研修の実施

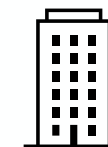
- Case3で示した技術流出事例のとおり、技術を獲得するために、役職員に対して様々な働きかけ・諜報活動（盗聴、窃取、協力者からの情報収集等）が行われる可能性がある。特に、海外出張者や赴任者等はそういったリスクが高いため、こうした諜報による情報漏えいその他の被害の防止（いわゆるカウンターインテリジェンス）に関する研修を実施する



コア技術にアクセスできない
業務用デバイス



日本からの
データ消去、
アクセスブロック



日本本社

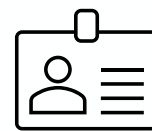
1. ⑮ 展示会等を契機とする部外者との接触への対応

- 展示会や学会等はビジネス拡大の機会となる一方で、競合他社等が自社の優秀な技術者に接触する機会でもあり、技術者の流出につながるケースも存在する
- また、技術者としての実力をアピールするため、必要以上の情報を公表してしまう場合もある。資料の事前確認や、第三者から接触があった場合の対応方法等を決めておく等、技術流出リスクを低減するための取組を行う必要がある

対応策の例

① 技術者個人の連絡先を教えない

- 展示会等への出展は重要な営業機会である一方で、必ずしも身元がはっきりとしない不特定多数の参加者と接触する場でもあることから、商談に見せかけた不審なアプローチの契機となるおそれがある
- 会社のビジネスとは無関係な、技術者個人に対する不審なアプローチが進まないよう、展示会専用の業務メールアドレスを記載した名刺を用意する等して、展示会に出席する技術者個人の連絡先が安易に知られないようにする



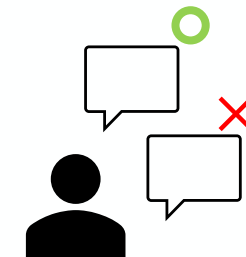
- ✗ 個人の連絡先
- 展示会専用の連絡先 (窓口等)

② 接触があった場合の会社への報告

- 他社からリクルート等の接触があった場合には、会社に報告することを奨励する
- 業務用メールについて、特定のアドレスからリクルートメールを受信しないように設定する

③ 技術的な質問に対する回答可能な範囲を明確にルール化する

- 公開している情報のみに限定する、組織的な確認プロセスをルール化する等、必要以上の情報を不用意に回答することがないように留意する



○ 回答範囲の明確なルール化

④ 展示会等で公表する資料や展示品を事前確認する

- パンフレットやプロモーション映像、展示品の事前確認を徹底する。(例：①PR映像の映り込みの確認、②配布資料の提供先を限定、③ノウハウが関連する部品を展示品に組み込まない等)

第0章 はじめに

- 1 本ガイドンスの目的等
- 2 技術流出の経路と本ガイドンスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

2. ① 違反に対する毅然とした対応

- 重要技術を適切に**営業秘密管理**していることを前提に、漏えいには**毅然とした対応**をとることが必要
- 事案が公となった場合のレピュテーションリスクをおそれ、不正競争防止法に基づく刑事告発を躊躇し、内々に処理する企業も多い。しかしながら、同法に基づく毅然とした対応は、**営業秘密管理を日常的に行っていることの証左**であり、取引先や顧客、株主等の**ステークホルダーからの信頼向上**に資するものである
- また、社内に対しては、**次の漏えい事案の抑止**にもつながるほか、当該技術を生み出すために**努力を積み重ねてきた他の多くの役職員に報いる視点**からも重要である

対応策の例

① 迅速な調査と対応

- 技術流出の疑いが生じた場合には、迅速に事案調査を実施し、事実関係を確認する

② 法的措置を含む厳正な処分

- 役職員から技術流出した場合には、就業規則に基づく懲戒処分のみならず、不正競争防止法に基づく民事上の責任や、雇用契約や誓約書等に基づく債務不履行責任を追及する。また、同法に基づく刑事上の責任を追及するため、警察への相談や捜査協力も行う
- 技術の重要度や訴訟等のコストを考慮して、どこまでの措置を講じるかはケースバイケースだが、レピュテーションリスクの回避のみを意識し、甘い対応で内々に処理しようとする姿勢は望ましくない
- なお、令和5年の不正競争防止法改正により、国内において管理されている日本企業の営業秘密の侵害が国外で発生した場合に、日本の裁判所で同法に基づき訴訟提起できる旨が明確化されている



技術流出の疑いが生じた場合、迅速に調査を実施

③ 公表や説明の実施

- 事案について、社内外に対する適切な形での公表・説明を検討する
- ステークホルダーに対しては、日常的に適切な営業秘密管理を行っている事実を強調し、信頼向上に努める。同時に、自社の取引先等が同様の対応をした場合には、責任を追及するのみならず、適正に評価する
- 役職員に対しては、社内研修等で丁寧に説明し、意識向上と今後の抑止につなげる。また、営業秘密の漏えいは、他の役職員の努力を無にする行為であり、組織としての姿勢を示していくことが重要である



法的措置を含め厳正に処分する

※技術が流出した場合には、被害を最小限に抑えるために、速やかな対応を講じることが重要となる。漏えい事案への対応については、前掲「秘密情報の保護ハンドブック～企業価値向上にむけて～」Jp147以降を参照されたい。(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>)

2. ② 再発防止策の策定・徹底

- 同様の漏えい事案が発生することを防止するためには、当該事案の原因を分析し、その**根本的な要因を明確にする必要がある**
- その上で、**再発防止策を策定**し、社内研修や監査にも反映させ、**重点的にチェック**することで対策を徹底することが重要

対応策の例

①原因分析を実施する

- 漏えい事案の原因を詳細に分析し、どういった点について問題があったのか、管理体制や社内教育の不足がなかったのか等について検討する



②社内規程の見直しと再発防止策の策定

- 社内規程やポリシーを外部の弁護士等に確認してもらい、規程整備・体制構築を行う
- また、漏えい事案の原因分析に基づいて、情報管理体制の見直しや、従業員への教育プログラムの強化等についての具体的な再発防止策を策定する



③研修や定期監査の実施

- 策定した再発防止策を基に、全ての役職員を対象とする研修を定期的実施し、流出防止や情報セキュリティの重要性を再確認させるとともに、定期的な監査を実施し、再発防止策が適切に実行されているか確認する



定期的な
研修



監査の実施

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

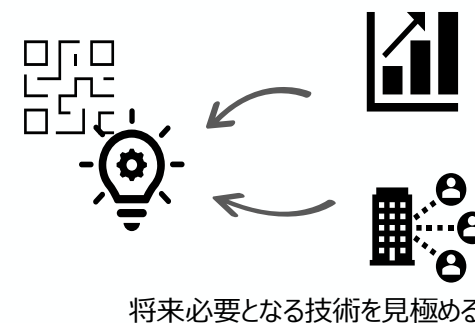
3. ① イノベーションを生み続ける (技術の陳腐化の加速)

- 対策を講じることで技術流出の時間を遅らせることはできるが、**技術流出を完全に止めることはできない**。また、技術が流出しなくとも、**競合他社は常にキャッチアップのための努力を続けている**
- このため、**イノベーションを生み続け、流出した技術が速やかに陳腐化するような状況を作ることが、最大の技術流出対策**である (Run Faster)

対応策の例

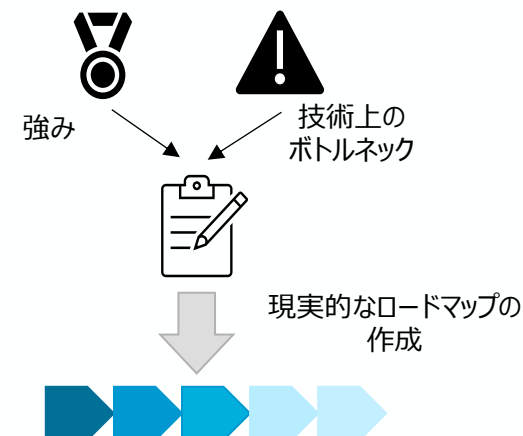
① 将来必要となる技術の見極め

- 足元の市場のみならず、競合他社の伸長や数年先の市場動向を見据え、将来のビジネスの中核を担う有望な技術を見極める。その際、安易な楽観論に陥ることなく、自社の経営状況や技術開発力を冷静に判断する



② 技術開発から実装までを見据えた計画の策定

- 現状における自社の強みや経営資源の制約、技術上のボトルネックを認識した上で、実装までの現実的なロードマップを作成し、リソースを投入する



3. ② 優秀な技術者の流出防止

- 優秀な技術者が他社に転職した場合、営業秘密漏えいの有無に関わらず、転職先企業の技術力が向上し、自社の競争優位性が損なわれるリスクがある
- **コア技術に繋がりうる優秀な技術者が誰であるかを、技術と紐付けてリスト化する等して特定・把握し、ふさわしい職位・給与等で処遇したり、表彰制度等によってモチベーションを向上することが重要**

対応策の例

① 優秀な技術者の待遇を向上させる

- コア技術に直結するような優秀な技術者については、例えば役員又はそれに準ずる適切な職位に昇進・昇格させ、インセンティブ報酬の対象としたり、給与等の金銭的な処遇を向上させる
- また、給与以外に、技術者としてのキャリアアップに資するような機会の提供も検討する（留学に係る金銭的な支援等）



② 技術者のモチベーションの維持・向上を図る

- 優秀な技術者については、金銭的な処遇の向上のみならず、社内表彰制度の導入や、役員級の技術系職位の設置、職務発明規程に基づく相当の利益の設計を工夫すること等により、モチベーションの維持・向上を図る
- 自社でのキャリアアップに魅力を感じることができるよう、社内の技術者コミュニティの活性化や、短期的利益に直結しない研究開発を重んじる企業カルチャーを醸成する



③ 熟練技術者の流出を防止する仕組みを作る

- コア技術に直結する熟練技術者が定年によって社外に流出しないよう、定年延長や再雇用制度を導入する。その際、その能力等に応じた適切な処遇についても十分留意する
- また、顧問やコンサルタントとしての関与等を通じて、持続的な関係を構築する



3. ③ 退職者との良好な関係の構築

- 退職した技術者が、海外の競合他社等に技術顧問として雇用され、自社の競争優位性が損なわれるケースも存在する
- **退職者と優良な関係を構築しておくことが、こういった動きの抑止につながる。また、退職者の動向を把握することで、技術流出リスクを未然に検知するきっかけとなる場合もある**

対応策の例

① 退職者と良好な関係を構築することの重要性を浸透させる

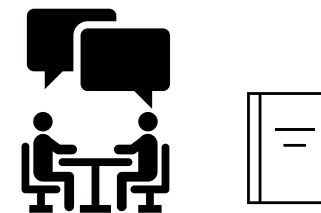
- 中途・定年を問わず、退職者と良好な関係を構築し、自社と心理的に近い距離感を持つことが、技術流出対策の観点からも重要であるという考えを、全社的に浸透させる



良好な関係の重要性

② OB・OG会等を通じて定期的にコミュニケーションを図る

- OB・OG会や退職者向けの広報誌等を通じて、実例を交えつつ、技術流出に関する注意喚起を行う
- 拠点・部門・入社年次等のより緊密なコミュニティとの関係性も重視し、退職した技術者の近況を把握することで、技術流出のおそれが生じていないか確認することも有用
- 特に、コロナ禍等を通じて退職者とのコミュニケーションが希薄化してしまった企業も、退職者とのコミュニティの再構築を検討する



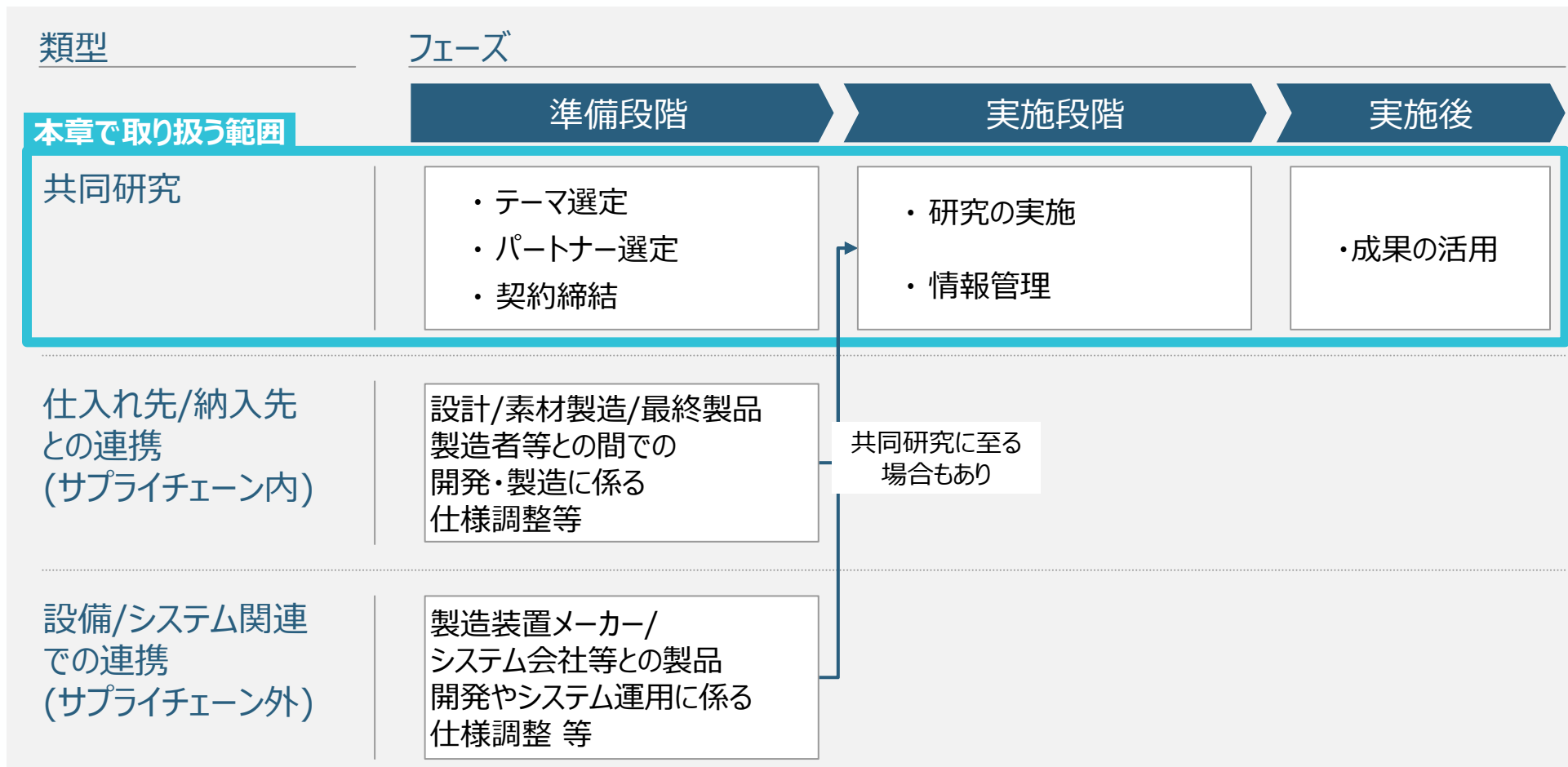
定期的なコミュニケーション

第4章

共同研究に伴う技術流出への対策

本章で取り扱う範囲

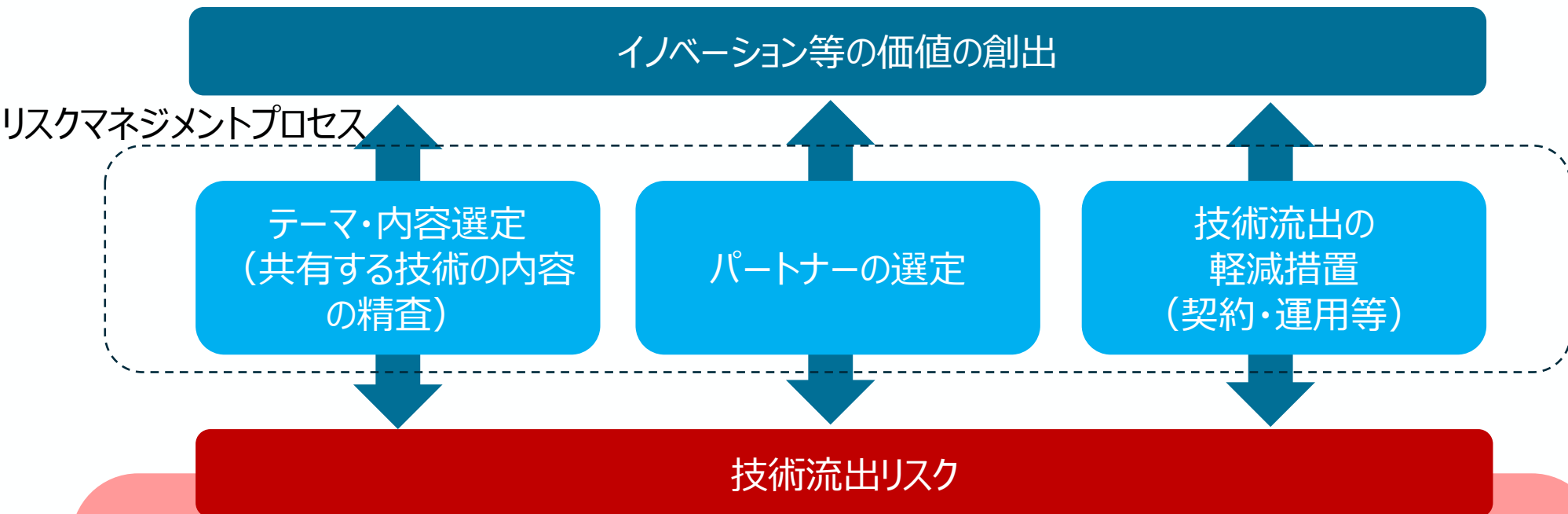
- 企業が他の企業や大学等と連携する場合、技術流出リスクが想定される主な事例としては、①**共同研究**と、②**サプライチェーンの中での連携**/③**サプライチェーンの外との連携**が挙げられる
- 本章では、①**共同研究のリスクと対策**を取り扱う



「共同研究に伴う技術流出への対策」に関する基本的認識

- **イノベーション実現には、外部からの知識の積極的な獲得や、その効果的な取り込みが重要**
 - 個別企業の人材や研究開発基盤だけではなく、異なる国や組織との共同研究により、知識・技術の伝搬を促し、企業のイノベーションを推進していくことが必要
- **また、経済安全保障の観点でも、国際的な共同研究開発の強化が必要**
 - 民間企業等が先端技術分野においてイノベーション力を発揮し、我が国の「技術優位性」を磨き上げ、「不可欠性」まで強化することは重要な課題
 - 我が国の国内での研究開発力を高めていくだけでなく、特に技術的な課題がある領域では、海外の知見を積極的に取り込むことが重要
- **一方、共同研究では、他の組織・他国との技術の共有が想定され、技術流出リスクが高い。このため、テーマ・内容、パートナー等に応じ、適切なマネジメントが重要**
- **特にパートナーは、組織体制や目的、遵守する法令等、特性が多種多様であり、留意が必要**
 - 組織の規模・体制の相違 (例: 大企業/中小企業)
 - ガバナンス/研究目的や従事者の特性の相違 (例: 企業と大学・国立研究機関)
 - 遵守すべき法令や慣習の相違 (例: 外国企業や大学)
 - その他、共同研究に関わる協力会社 (装置メーカーや資材メーカー等) や試験機関 (公的共同利用施設等) についても考慮が必要な場合がある
 - 相手国によっては、外交・安全保障を意識した対応が必要になるケースもありうる

「共同研究に伴う技術流出への対策」に関する基本的認識



【準備段階】

- 機微なテーマを選定し扱うことによる特に重要な技術の流出
- 事前協議・交渉段階での不用意なやり取りによる流出
- 内部関係者による不正持ち出し

【実施段階】

- 相手方の内部関係者による技術の不正な持ち出し
- 相手方による情報の不正利用 (目的外利用等) / 不注意による流出
- 第三者が相手方の情報を窃取することによる流出
- 相手方の資本構成の変更や業績悪化等を通じた流出

- 知的財産の取扱いが不明確であることに起因する流出
- 不利な法制度/管轄での訴訟対応

【実施後段階】

- セキュリティ不備による漏えい (サイバー攻撃による流出も含む)
- 委託先等からの二次漏えい
- 相手方による共同成果の独占利用・不正利用
- 相手方による予期せぬ成果の公開による技術流出
- 相手方の情報処分の不備による流出

共同研究における技術流出リスクの全体像

- 共同研究では、実施前・実施段階・実施後の各段階に、様々な技術流出が生じるリスクがある

共同研究のフェーズ 各フェーズで発生しうる技術流出リスク

相手方の悪意による技術流出

当方又は相手方の偶発・過失による技術流出

フェーズ	サブフェーズ	技術流出リスク	
		相手方の悪意による技術流出	当方又は相手方の偶発・過失による技術流出
準備段階	テーマ選定	機微なテーマを選定し扱うことによる特に重要な情報の流出	
	パートナー選定	信頼性の低い相手方を選定したことに起因する流出	事前協議・交渉段階での不用意なやり取りによる流出 Case1
	契約検討/契約締結	※契約内容は、実施段階・実施後段階のリスクを意識した上で検討・締結する必要	
実施段階	研究の実施	相手方による情報の不正利用 (目的外の利用等)	相手方の不注意による流出
		相手方の内部関係者による不正な持ち出し Case2,3	第三者が相手方の情報を窃取することによる流出
			相手方の資本構成の変更や、業績悪化・破綻等を通じた流出
		知的財産の取扱いが不明確であることに起因する、相手方による意図しない情報利用	不利な法制度/管轄での訴訟対応
実施後段階	情報セキュリティ体制		セキュリティ不備による漏えい (サイバー攻撃による流出も含む)
			相手方の委託先等からの二次漏えい
	成果活用	相手方による共同成果の独占利用・不正利用	相手方による予期せぬ成果公開による流出
		相手方の情報処分の不備に起因する流出 Case4	

共同研究における技術流出リスクとその対応の全体像

- リスクに応じ、契約での規定やモニタリング等、必要な対策を実施していく必要がある

共同研究のフェーズ

各フェーズで発生しうる技術流出リスク

各リスクへの対策 (まとめ)

悪意による技術流出

偶発・過失による技術流出

情報管理体制

テーマ選定

機微なテーマを選定し扱うことによる特に重要情報の流出

準備段階

パートナー選定

信頼性の低い相手方を選定したことによる流出
事前協議・交渉段階での不用意なやり取りによる流出

契約検討/
契約締結

契約内容は、実施段階・実施後段階のリスクを意識した上で検討・締結する必要

実施段階

研究の実施

相手方による情報の不正利用 (目的外の利用等)
相手方の内部関係者による不正な持ち出し
相手方の不注意による情報の漏えい
第三者が相手方の情報を窃取することによる流出
資本構成の変更や業績悪化等を通じた流出
知財取扱の不明確に起因する相手方の意図せぬ情報利用
不利な法制度/管轄での訴訟対応

情報セキュリティ

セキュリティ不備による漏えい (サイバー攻撃による流出も含む)
相手方の委託先等からの二次漏えい

実施後

成果活用

相手方による共同成果の独占利用・不正利用
相手方による予期せぬ成果公開による流出
相手方の情報処分の不備に起因する流出

リスクマネジメントプロセスの導入、重要技術の定義/見直し

技術の重要性を踏まえたリスク評価とテーマ選定 (コア技術の除外等)

パートナー候補のDD徹底 (国・組織・個人の観点)

検討段階でのNDA締結/相手方の体制や段階に応じた開示/NDA締結前の特許出願

契約内容の検討

- ・ 自社ひな形の活用、研究目的の明確化、研究参加メンバーの特定、情報管理体制構築、目的外利用等の禁止、提供技術の範囲や方法の明確化、知的財産の帰属の明確化、秘密保持義務・競業避止義務、監査条項の規定、CoC条項の設定、成果の公開に係る手続等の明確化、準拠法・管轄の選択、情報返却・削除義務

秘密保持義務/競業避止義務の設定

情報管理体制の構築/運用の継続的な要請、モニタリングの実施

解除条項の挿入 (資本関係変更時等)

知財/ノウハウ取扱明確化

中立的な国際ルールでの準拠法の設定

システム対応等 情報セキュリティ体制の構築

再委託含めた実施体制報告/確認

研究終了後のモニタリングと文書等の適切な管理

研究終了時の技術情報やサンプルの返還・廃棄の徹底

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

0 技術流出事例

- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

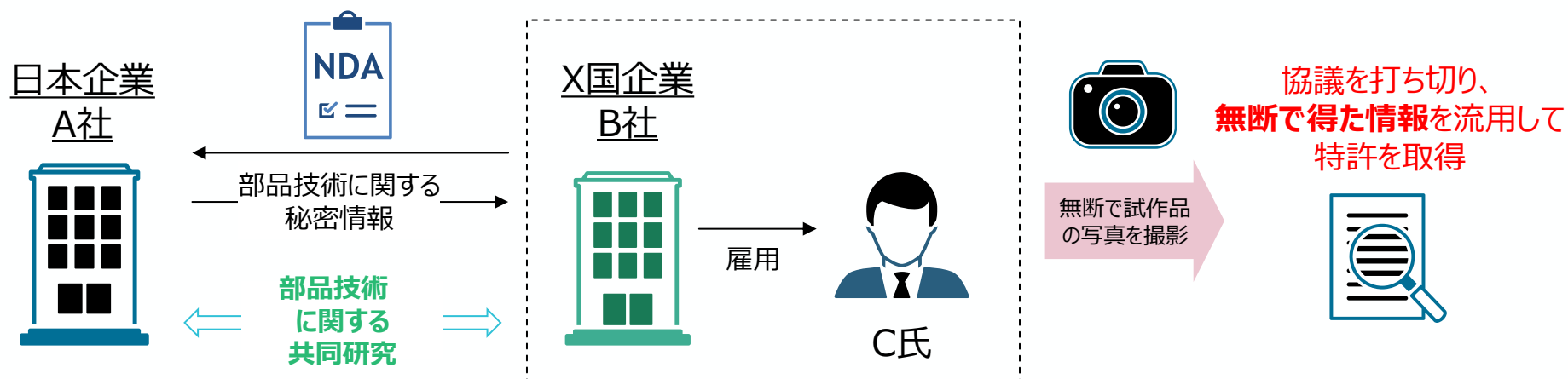
0 技術流出事例

- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

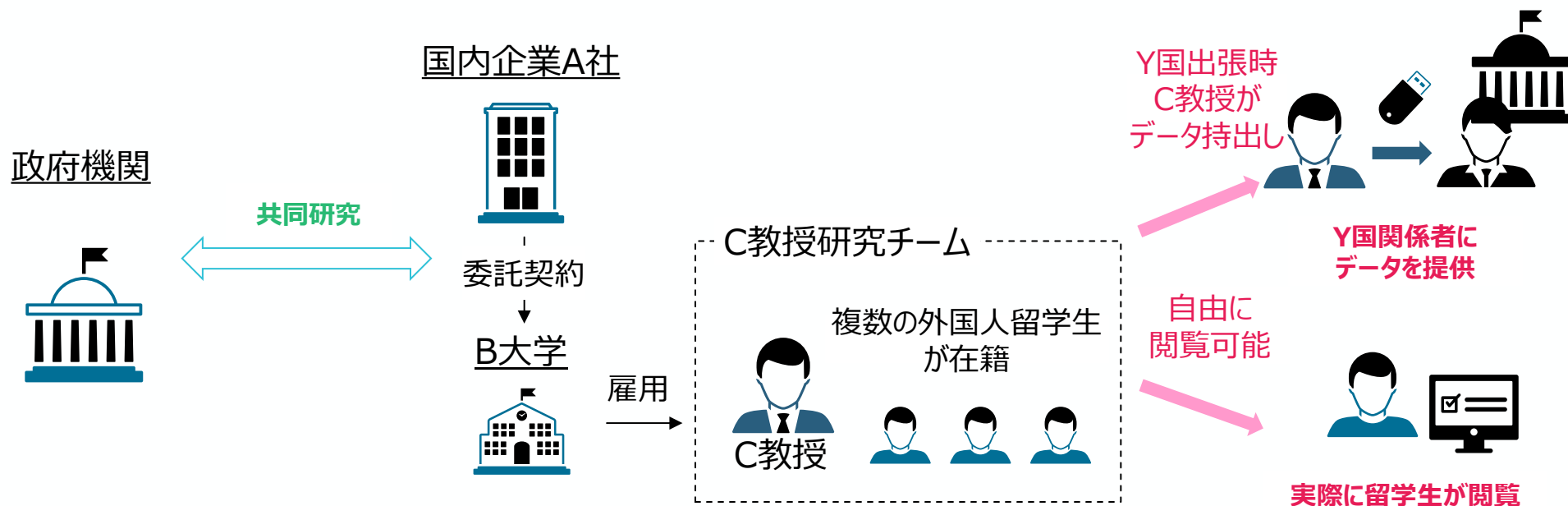
Case1: 共同研究の事前協議の際の技術流出

- 日本企業A社は、開発した技術の商業化を目的として、部品技術に関する共同研究の実施に向け、X国のB社と秘密保持契約 (NDA) を締結したうえで、事前協議を実施。A社が試作品をB社に提示した際、B社の技術責任者C氏が無断で当該試作品を写真撮影した
- 協議を打ち切った数か月後、B社は試作品の写真から得た情報を流用し、部品技術に関する特許を出願。その後数年かけて特許を複数件取得した
- A社は、B社に対して訴訟を提起し、B社が取得した特許権の移転を求めるとともに、秘密保持義務違反に基づく損害賠償請求を行った



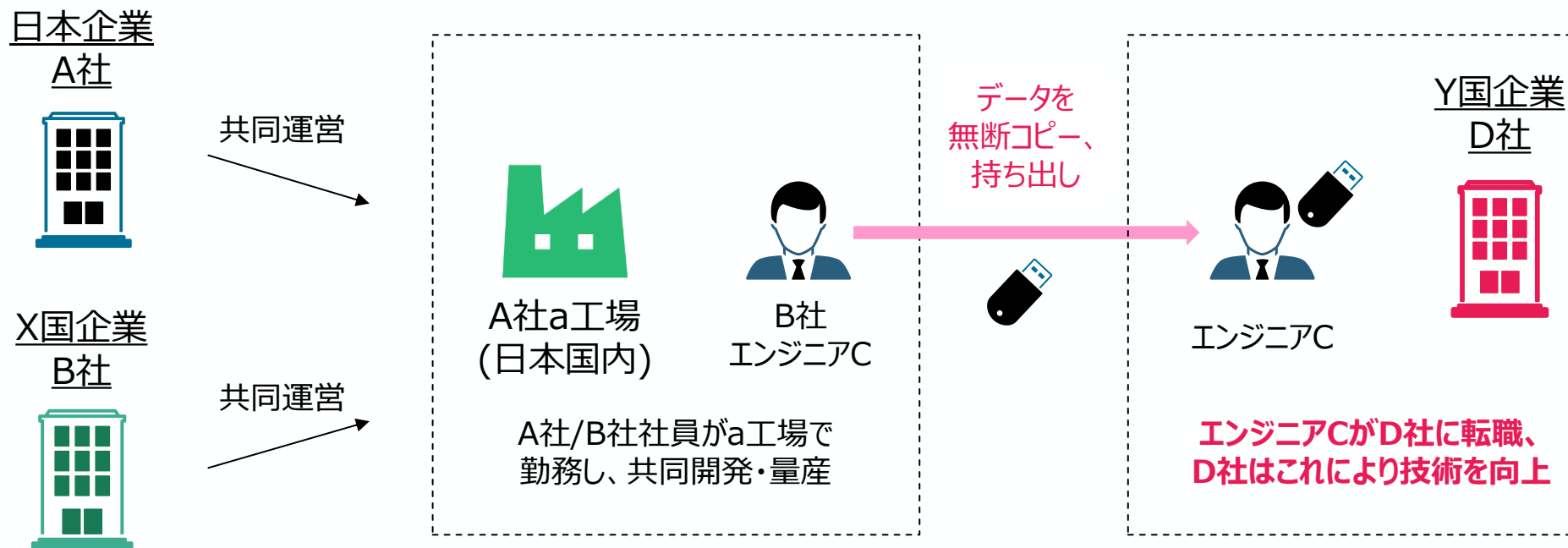
Case2: 内部関係者の不正持ち出しによる技術流出

- 政府機関と国内企業A社、A社委託先のB大学の3機関は**共同研究を実施**。当該共同研究に係る技術はデュアルユースの観点から**輸出管理の対象になり得るものだった**
- B大学のC教授の研究チームにおいて、**外国人留学生を含む所属学生が関連する技術データを自由に閲覧可能な状態**になっており、**留学生が実際にデータを閲覧していた**
- C教授自身も、研究データを所持して**海外Y国に渡航し、Y国にデータを提供していた**
- 大学職員が、上記研究室の状況を認識し、当局に通報。**C教授はY国出張からの帰国時にPCを押収され、その後輸出管理法令の違反等により、有罪判決を受けた**



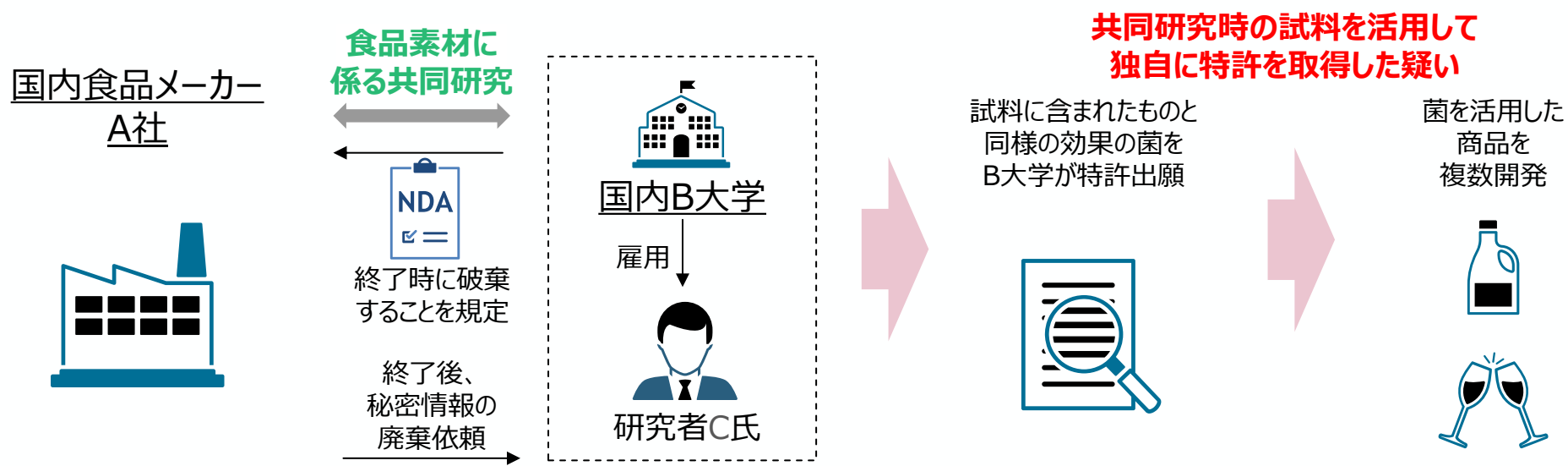
Case3: 内部関係者の不正持ち出しによる技術流出

- 日本企業A社とX国海外企業B社は、半導体に関する技術の共同開発で包括的に連携
- 包括連携の枠組みの中で、国内に所在するA社のa工場に、B社技術者も勤務していた。B社日本法人に勤務していたエンジニアCが、A社の研究データを無断でコピーした。その後、当該エンジニアはA社競合のY国D社に転職し、持ち出した技術情報を流用した
- この結果、D社の同分野での開発が急速に進展。A社経営層も不審に感じ、B社と共同で調査を実施したところ、エンジニアCによる流出が発覚した



Case4: 共同研究終了時の情報処分不備による技術流出

- 国内食品メーカーA社は国内B大学との共同研究にあたり、B大学のC氏に特殊効果を持つ細胞を含む試料等を提供。契約終了後の試料・情報の返還・廃棄等について規定したNDAを締結
- その後、A社はプロジェクトから撤退し、秘密情報の廃棄にC氏も応じた
- 数年後、B大学が同様の効果を持つ菌を特許出願し、以降、菌を活用した商品を複数開発
- A社が外部に解析を依頼し、B大学の菌が自社と同一であると判断。C氏は上記の情報を継続して保有/活用し、その後の特許出願に不正利用した疑いがある。B大学にその旨を問い合わせたが、大学側から納得のいく説明はなく、その後、A社はB大学を提訴した



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

1. ① リスクマネジメントプロセスの導入

- 共同研究に際しては、**自社の重要技術を開示する場合も想定されるため、共同研究の実施国、実施相手、実施に関与する個人の観点から、①リスクを把握するための調査（デューディリジェンス（DD））を行った上で、②把握したリスクの評価（共同研究を通じた技術流出リスク等の評価）を行い、③技術流出の可能性を低減させるための措置を講じる必要がある。**また、これらの措置が適切に運用されているかの**フォローアップ**を行い、**必要に応じて改善措置を講じるとともに、今後の社内での検討に反映させていくことが重要**
- その前提として、**社内での実施体制構築**、共同研究先に開示する技術情報の重要性の事前評価や秘密保持を確保した上での相手方との事前調整等の**一連のプロセスを、社内の業務フローに組み込む必要がある**

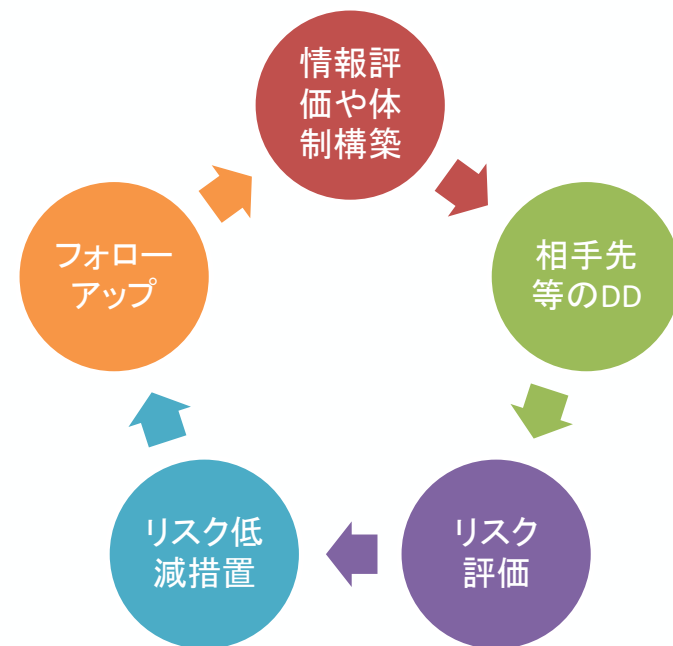
対応策の例

① 共同研究を行う際の一連のプロセスを社内ルール化し、業務フローに組込む

- ✓ 実施に伴う社内での確認体制や確認フローの構築
- ✓ 技術の重要性を踏まえた共同研究テーマの選定
- ✓ 共同研究パートナー候補のDD（国・組織・個人の観点）
- ✓ NDAを締結した上での相手方との事前調整
- ✓ 契約や運用面でのリスク軽減措置の実施
- ✓ フォローアップの実施
- ✓ 実施中の事業や社内ルール等への反映を徹底

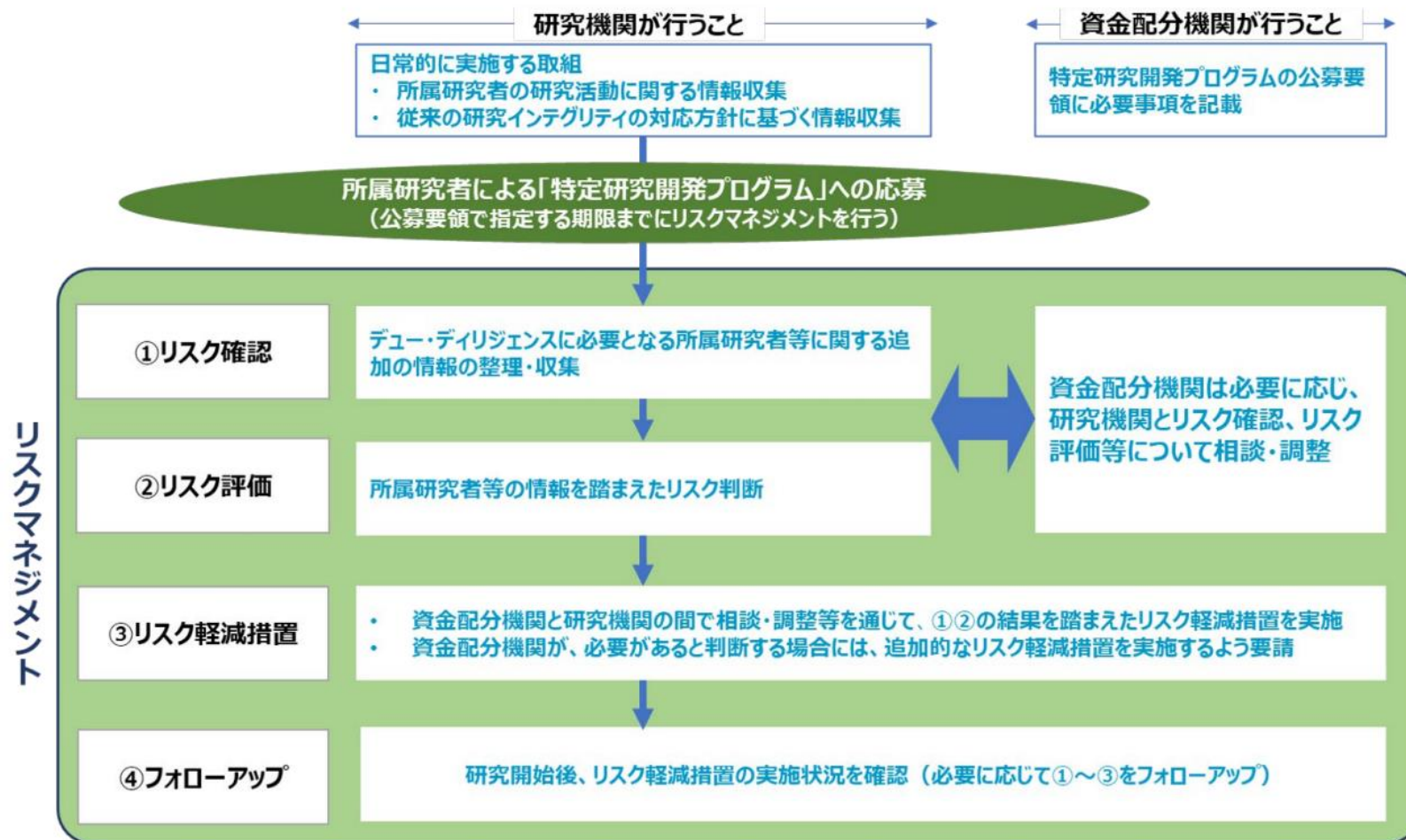
② 社内の担当部署が実施部門の要請を踏まえてDD等を行う体制を構築

- ✓ 社内体制等によるものの、チェック&バランスの観点から、研究実施部門と異なる部署が関与・実施することも考えられる



(参考) 手順書における研究セキュリティ確保のためのリスクマネジメント手順

- 手順書は、①研究成果の公開を前提とする競争的研究費のうち、②「重要技術領域リスト」に該当する技術を含む可能性があるものであって、③経済安全保障の観点から特に技術流出の防止が必要であるとして当該競争的研究費を所管する府省が資金配分機関と相談の上で指定する研究開発プログラム（特定研究開発プログラム）を対象に、政府、資金配分機関、研究機関及び研究者が実施すべきリスクマネジメントとして「最低限実施すべき措置」と「実施することが望ましい措置」を示している



※ 手順書p7より抜粋
 (<https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha.html>)

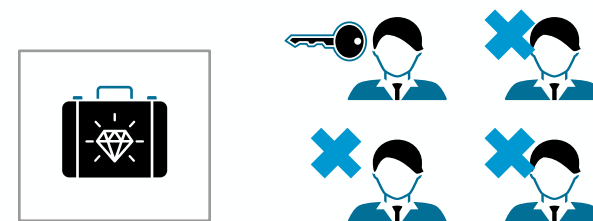
1. ② 共同研究に従事する役職員の決定

- 共同研究の内容によっては、**流出時の損失が大きい重要技術を取り扱うケース**がある。また、共同研究の相手方からも、**信頼できる担当者のみ従事させるべきとの要請が行われる場合**もある
- このため、技術の重要性によっては、必要に応じて、**共同研究に従事するメンバーの候補者を選定し、その適性を事前に確認した上で決定していくことも重要**（必要に応じ、**適性の確認** (p69～) を実施する）

対応策の例

- **例えば、技術の重要度に応じて、以下の項目を確認することが考えられる**
 - 社内における情報管理状況（社内研修の受講状況等）
 - 居住性や特定類型該当性（外為法上の規制技術（キャッチオール含む）の取扱いが発生しうる場合）
 - 外国政府等との契約又は外国の法令その他これに類するものにより、当該政府等による情報収集活動に協力する義務を負っていないか
 - 上記契約関係の確認のために、研究費や奨学金等の給付も含めた契約関係の有無
 - 過去に上記法令を有するような外国政府やその支配を受ける企業に在職していたか、当該国への渡航歴
 - 外国政府や外国企業、外国企業の支配を受ける企業、外国大学等との副業・兼業等の有無
 - 情報取扱いに関する非違歴や前科の有無

共同研究に関与する役職員を限定



職員について確認すべき事項

- 情報管理スキル/非違歴の確認
- 外為法上の規制に関する確認
- 外国政府との関係性
 - 金銭関係、外国企業在籍情報 等

(参考) 手順書が求める研究セキュリティ確保のために確認すべき項目

- **手順書においては、特定研究開発プログラム（p115参照）の全体責任者や研究参画者等について、以下に掲げる事項を自己申告させた上で確認し、DDを実施することを求めている。** DDは、基本的に、自己申告による情報、ソース等各研究代表機関が通常把握しうる情報を用いて実施することとされている

- ① 学歴（必要に応じて指導教官等の情報を含む。）
- ② 研究経歴・職歴
- ③ 研究費の取得歴
- ④ 研究費以外の支援等の取得歴
- ⑤ 発表論文における筆頭著者、責任著者及び共著者
- ⑥ 特許の出願状況（共同発明者及び共同出願人の情報を含む。）
- ⑦ 外国の人材採用プログラムへの参加歴
- ⑧ 指針に基づく処分歴
- ⑨ リストへの掲載の有無
- ⑩ リスト掲載機関への所属の有無
- ⑪ リスト掲載機関に所属する研究者との関係（共同研究・受託研究の実施、共著論文の執筆・公表及び学会等における連名の口頭発表の実績をいう。）の有無
- ⑫ 安全保障貿易管理における「非居住者」（一時帰国しその滞在期間が6月未満の日本人等）又は「特定類型」（日本の大学の教授であり外国の大学と雇用契約を締結し教授職を兼職している者、外国政府から留学資金を得ている留学生、外国の人材採用プログラムに参加し多額の研究資金や生活費の提供を受けている研究者等）への該当性
- ⑬ その他資金配分機関がデュー・ディリジェンスの実施に当たり必要と認める事項

※ 手順書p18より抜粋

(<https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha.html>)

1. ③ 技術の重要性を踏まえたリスク評価と研究テーマ選定

- 技術流出対策を考える上で、重要技術の位置付けの評価 (p15) が重要であることは、共同研究についても同様である。具体的には、自社が保有している技術に関しては、①**自社の競争力の源泉となるコア技術**、②**軍事転用懸念のある安全保障上の重要技術**、③**経済安全保障に関わる重要技術**に該当するかどうかを評価することが必要である。また、共同研究のポイントとして、破壊的技術革新が進む領域において行われる共同研究については、④**自社が現在保有していない技術の獲得・開発**に意義があるケースもあるところ、そうしたケースにおいては、**自社の技術優位性を磨きあげながら、同時に防衛策 (技術流出対策) を講じていく必要がある**
- こうした技術の**重要性の評価**を踏まえて、計画中の研究テーマに係る技術が**流出した場合に想定されるリスク**を検討した上で、共同研究先のDDを実施し、計画中の共同研究における**技術流出リスク (流出した場合の損失とその可能性)**を把握・評価する。そして、**評価したリスクと、共同研究によって創出される価値の較量**を行った上で、研究の実施可否 (必要に応じて研究テーマの見直し) やリスク軽減措置の内容等を決定する
- リスクの評価に当たっては、共同研究先に提供する技術情報が、通常、**共同研究先の管理下に置かれることとなるため**、自社管理と比べて、**情報のコントロールが困難となるケースが多いことを認識**する。本ガイダンスに記載のとおり、リスク軽減措置として、契約上の対策や実施段階におけるオペレーション上の対策はあり得るが、**技術流出を完璧に防ぐことは困難であることから、共同研究先による情報管理をコントロールすることの難しさを十分認識した上で、研究テーマを設定することが重要である**

① 競争力の源泉となるコア技術

- 競争力に直結する技術であるため、権利化・秘匿化の観点も意識しつつ、社内管理に万全を期すとともに、技術保有者の把握や適切な処遇等による対策が必要。
- ②・③に位置付けられる技術もあるため、海外移転等を進める場合には、必要に応じて経済産業省や所管省庁に相談することも有用。

② 安全保障上の重要技術 (軍事転用懸念のある技術)

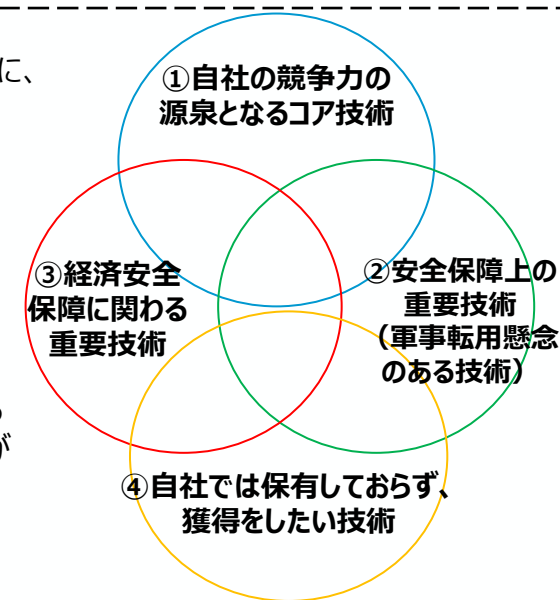
- 外為法上のリスト規制技術に該当する場合等、我が国の安全保障に影響を与える可能性があるため、特に慎重な対応が必要。

③ 経済安全保障に関わる重要技術

- わが国の経済活動の自律性や不可欠性を確保するために重要な技術。諸外国の獲得対象となっている可能性もあり、第三国からの制裁や取引停止等の関係でも注意を要する。一社の技術流出等の問題が我が国の産業・技術基盤、ひいては国力に影響を与える可能性がある。

④ 自社では保有しておらず獲得をしたい技術

- 技術流出対策とイノベーションのバランスをとりながら、共同研究等を通じて、積極的に技術の創出・獲得に取り組む。相手先との関係で、レピュテーションリスクや第三国の法令抵触リスクへの配慮が必要。



自社
保有
技術

1. ③ 技術の重要性を踏まえたリスク評価と研究テーマ選定

対応策の例

① 研究テーマの機微性・流出時のリスクの評価

- 共同研究のテーマ選定時に、前ページにおける技術の位置付けを踏まえて、その機微性を評価する。特に、軍事転用懸念のある安全保障上の重要技術 (②) や、経済安全保障に関わる重要技術 (③) に該当しないか丁寧に検討する。技術の機微性を踏まえて、流出時のリスク (法令違反による罰則、自社の競争優位性の喪失・競合企業のキャッチアップ等) を評価する
- その際、安全保障上の重要技術を中心に、外為法や海外の輸出管理法令の規制を受ける可能性を検討した上で、研究テーマを選定することが必要である。また、国際共同研究の場合には、共同研究の成果を日本や第三国に移転する際に、相手国の法令上、移転が阻害される可能性がないか事前に把握し、移転が不許可となる可能性が存在する場合には、テーマ設定の段階からリスク回避を図る必要がある。国の観点からのDDについてはp120も参照
- また、防衛関連契約等に基づき、他国から機密性が高い情報を提供されている場合には、当該契約等に基づいて義務付けられているセキュリティ基準等に抵触しないよう留意を要する



テーマ選定時に
技術の重要性を評価する



リスクを評価する



テーマ・リスクに応じた
対応を行い、リスクを最小化

② 研究テーマの見直しの検討

- 流出時のリスク評価を踏まえ、相手側との信頼度も考慮の上、適切なテーマを選定する。例えば、過去の取引実績のみに依拠することは適切ではないものの、特に初めて共同研究を行う相手方とは、周辺技術等の無難なテーマを設定することが考えられる。詳細はパートナー候補のDD (p120～) を参照
- 信頼感の醸成を踏まえ、徐々に重要度の高い技術を含むテーマに移行することもあり得る

③ 過度に萎縮しない

- 経済安全保障に関わる重要領域に関するテーマであっても、自社が保有しない技術を持つ企業との共同研究では、技術流出リスクは限定的なケースもありうる。レピュテーションリスクも踏まえた経営判断により決定されるものではあるが、パートナー候補のDD等を適切に行い、リスク軽減措置を講じた上で、過度に萎縮せずイノベーションを目指すことも重要

1. ④ パートナー候補のDDの徹底（相手国の観点）

- 外国企業や研究機関等との**国際共同研究**の場合、相手企業等の所在国において、**法令に基づき政府への情報開示を求められたり、現地での商慣習により想定とは異なる情報管理が行われる可能性があるため、技術流出リスクが高まる可能性がある**
- このため、相手国における関連法制や商慣習について事前に確認しておくことが重要。その際、**輸出管理における区分や政府による民間事業者が保有する情報への強制的アクセスを可能とする法令の有無、いわゆる第一国出願義務の有無等を、国ごとの属性を踏まえることも有益**

対応策の例

① 国際共同研究の場合、相手国の法制度や属性・情勢等を確認し、リスクを分析する

- 日本とは異なる法令や慣習の影響を受けるため、国によっては、客観的・典型的に技術流出リスクが高まる可能性がある。例えば、以下のような点を確認する。専門知識を要するため弁護士等の活用も検討する。中小企業等自社だけでの対応が困難なケースでは、業界団体や公的機関等の提供する情報も参考に（p33も参照）。
 - ✓ 相手国において研究開発・発明を行うような場合に、共同研究の成果を日本又は第三国に移転することについて、相手国の輸出管理法令の適用があるか
 - ✓ 共同研究の成果について、第一国出願義務や知的財産権の帰属・活用等について、特許法等の知的財産法上、どのような制限を受けるか
 - ✓ 外国政府等による情報収集活動に協力する義務を課す法令を有する国か
 - ✓ 政府による強制情報アクセスが行われる可能性がある国か
- また、相手国の属性として、輸出管理上の区分や国連制裁等の対象となっているか等を確認することも重要である。

パートナー候補のDDの実施
(国際共同研究の場合)



② 相手国の情勢等についても確認する

- 共同研究の進捗確認等のために役職員が現地出張する場合は、情勢や規制法、他社の情報インシデントの有無等の確認も重要。例えば、以下のような点を確認することが有用
 - ✓ 海外安全情報による治安情勢等の政治社会情勢等
 - ✓ 当局によって不透明かつ予見不可能な形で解釈される可能性があるスパイ行為に係る規制法の有無
 - ✓ 他社で出張者が持参した端末から情報漏えいが発生していないか

制裁対象国等の確認

国連安保理や米国等の制裁対象国との共同研究を行う場合には、法令遵守の観点から問題であるため、事前の確認が必要。

【国連安保理の制裁対象リスト】

<https://main.un.org/securitycouncil/en/sanctions/information>

【米国財務省の対象リスト】

<https://ofac.treasury.gov/sanctions-programs-and-country-information>

輸出管理を厳格に行っている国に該当しないかの確認

国際レジームの下で、輸出管理を厳格に行っている**以下の国以外**との共同研究を行う場合には、流出時に軍事転用等が行われるリスクも高く、実施に際し注意を要する。

合計27カ国：アルゼンチン、オーストラリア、オーストリア、ベルギー、ブルガリア、カナダ、チェコ、デンマーク、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、アイルランド、イタリア、大韓民国、ルクセンブルグ、オランダ、ニュージーランド、ノルウェー、ポーランド、ポルトガル、スペイン、スウェーデン、スイス、英国、アメリカ合衆国

最新の情報は、経産省のHP等で確認されたい。<https://www.meti.go.jp/policy/anpo/qanda13.html>

いわゆる第一国出願制度を設けている国に該当しないかの確認

安全保障上の理由により、自国で行われた発明や自国民による出願について、国内法令により外国出願に制限を設けている国も存在する。最新の情報は別途確認されたいが、以下の情報が参考となる。

- ・独立行政法人工業所有権情報・研修館「新興国等知財情報データベース」<https://www.globalipdb.inpit.go.jp/country/>
- ・世界知的所有権機関（WIPO）「国際出願と国家安全保障に関する考慮事項」https://www.wipo.int/pct/ja/texts/nat_sec.html

政府による民間事業者が保有する情報へのアクセスが行われる可能性がある国の確認

現地法令により、政府による民間事業者等が保有する情報へのアクセスが可能となる場合、共同研究相手先に開示した情報が流出するリスクが存在する。法令の改廃や運用状況等を適時に入手していく必要がある。このような情報を提供するソースや事業者は多岐に亘るが、個人情報保護委員会の以下のサイトを確認することも有益。

<https://www.ppc.go.jp/enforcement/infoprovision/laws/>

1. ⑤ パートナー候補のDDの徹底 (組織の観点)

- 前記のとおり、共同研究に伴い提供する技術情報は、共同研究のパートナーにおいて管理されることから、**企業 (大企業・中小企業等)、大学・研究機関の別等、パートナーの特性**により、技術流出のリスクが異なる
- このリスクを評価するため、扱う技術の重要性等を踏まえつつ、**DD**を行い、法令遵守の観点 (安全保障貿易管理等) に限らず、**懸念主体との資本・人的関係を確認**するとともに、競合の有無や共同研究に関連するテーマの**特許出願の有無等を把握**し、必要に応じ、リスクの軽減措置を講じることが重要
- もっとも、例えばM & A取引におけるDDとは異なり、あくまで自社の技術情報の流出防止が目的であることから、共同研究の過程で提供する**技術情報の重要性・機微性 (p118参照)**や、**相手方の特性 (業種、上場/非上場、国内/海外等)**を考慮の上、**コスト等も踏まえて確認項目を調整することも重要**である

対応策の例

- 相手方の特性によりリスクが異なる点に留意しつつ、ソース調査に加えて、技術の重要度や、共同研究の検討に至った経緯、NDA締結段階で感じる怪しさ等も踏まえて、必要に応じてヒアリング・資料開示を通じ、確認を行う。外国のパートナーとの実施の場合、前述の「相手国の観点」も踏まえた検討が必要

(相手方の特性によらず確認すべき事項)

- 各国制裁リスト等への掲載有無
- 過去の法令違反・訴訟・不正事例・情報インシデントの有無
- (外為法上の規制技術を提供する場合には) 居住者該当性
- 外国政府等による情報収集活動に協力する義務の有無 (当該義務を直接的に負っていないと、当該義務を負うものや当該義務を課す外国政府等が、以下のような関係を有しているかも確認する)
 - 議決権、株式数又は出資金の額の 50%以上を占めているか
 - 役員又は役員で代表権を有するものの 1/3 以上を占めているか (外国政府等又は情報収集義務者に指名・任命された者も含む)
 - 拒否権付株式 (黄金株) を保有しているか
- 情報管理に係る規程や教育計画の有無・内容 (特に、他者から提供を受けた情報に係る管理状況については、責任者へのヒアリング等によって丁寧に確認する)
- 同一又は密接に関連する技術領域において、外国政府等による情報収集活動に協力する義務を負うものを行う共同研究や技術提携等の有無、存在する場合には計画中の共同研究と実施拠点や担当部署等が共通していないか

DDの実施 (全般)



チェック項目
(共通)

- 制裁リストの掲載
- 過去の法令違反
- 研究セキュリティのための取組

⋮



チェック項目
(企業)

- 設立時期
- 役員構成
- 株主構成
- 事業・研究開発実績財務状況

⋮

1. ⑤ パートナー候補のDDの徹底（組織の観点）

対応策の例

- 特に、相手方が企業の場合には、懸念主体との資本・人的関係等を確認する観点から下記項目のチェックが有用である。もっとも、自社のみで収集できる情報には限界があるため、必要に応じて公的機関等との連携や経済産業省への相談等により、情報を収集・分析することも有用

（確認すべき事項）

① 株主構成（最終親会社含む）、潜在株式の有無・内容・保有者

- ・ 技術獲得を図る主体が株主に含まれる場合には、当該株主が、共同研究の相手方を通じて技術が流出するリスクが高まる。特に、前述の通り、情報収集協力義務を有するものが株主等に含まれていないかを確認することが重要。
- ・ 発行済み株式や新株予約権等の数・内容等は商業登記により確認できるが、株主の属性等については、公開されていないケースが多い。上場会社であれば、開示書類等により大株主の状況等を確認できる場合もあるほか、非上場会社については、HP等の公表情報により直近の資金調達の状況を確認することや、必要に応じて、上記義務を有するような株主が主要株主に含まれていないか等をヒアリングをすることが考えられる。

② 役員構成

- ・ 役員自らが情報収集協力義務を負う場合のほか、当該義務を負う主体と密接な関係を有する場合にも、技術流出リスクは高まる。HPや商業登記、有価証券報告書等の公開情報の確認に加えて、ヒアリング等により、略歴や兼職状況（他国企業の役員等への就任状況等）を含めて確認する。その際は、企業規模等によるが、当該役員の所掌範囲が、計画中の共同研究や関連する事業領域を含む可能性があるか（自社が提供する技術情報にアクセスする権限の有無やアクセスする可能性の程度）も確認する。

③ 設立時期、事業・研究開発実績、財務状況、主要顧客

- ・ 前述した制裁リスト等に掲載されている主体が、非掲載の法人等を介して、技術獲得を図るケースも存在する。共同研究先の設立時期や事業・研究開発実績を確認することが重要だが、それらの情報のみで判断することなく、設立間もない企業と共同研究を行う場合には、設立の経緯や設立者のバックグラウンド等を、公表情報や業界内のレピュテーション、ヒアリング（日頃のコミュニケーション等も含む）等を通じて丁寧に確認することが重要である。また、共同研究に至る経緯も重要であり、相手方から持ちかけられた共同研究の場合は、相手方の具体的な研究開発実績等について、より慎重に確認する。
- ・ また、技術獲得を図る主体が、出資ではなく貸付け等によって、事実上の支配関係を構築し、技術獲得の拠点とするケースも存在する。このため、公開情報のみによって確認することは難しい情報もあるが、財務状況や主要な債権者等を確認することも有用である。

④ 知的財産権の取得・実施状況（当該知財の開発経緯含む）

- ・ 前述の研究開発実績と同様、特許情報プラットフォーム等を利用した知的財産権（特許権・実用新案権等）の取得・実施状況の確認も重要である。
- ・ また、相手方の共同研究や技術提携の実績についても、必要に応じて確認することが有用である。具体的には、過去に、制裁リスト等に掲載されている懸念主体との研究歴等の有無、情報管理や成果利用をめぐる紛争事案の有無等を公表情報や業界のレピュテーション等を通じて確認することが考えられる。

⑤ 情報インシデントや不競法違反（営業秘密関連）等の有無

- ・ 過去に情報漏えい事案がないか、所属する役職員等による営業秘密の持ち出し事案がないか等を確認する。なお、漏えい事案の有無のみを確認・評価することは妥当ではなく、毅然とした対応を講じているか、適切な再発防止策を講じているかが重要である点に留意する。情報セキュリティに関する認証制度（p174参照）の取得状況等も参考になる。

1. ⑤ パートナー候補のDDの徹底 (組織の観点)

対応策の例

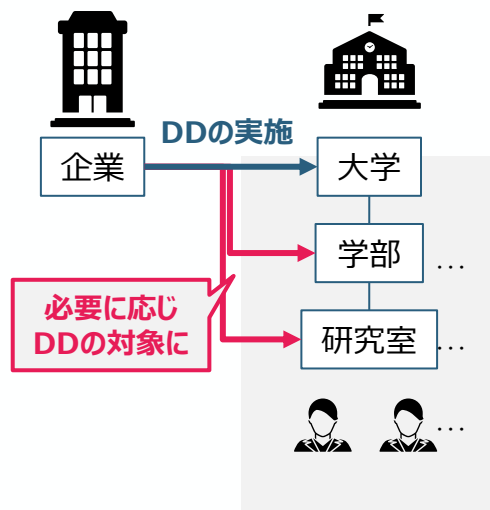
- 相手方が大学等の場合であっても、情報管理に関するガバナンスが機能しているかを確認することが重要である。組織として共通する基準や体制がなければ、各研究者等による個別判断によることとなり、情報漏えいのリスクが高いため、大学等との共同研究においても、組織の観点からのDDを実施することが重要となる

DDの対象の設定

- 大学は、共同研究の成果の事業化・利益獲得に対する考え方や組織のガバナンスのあり方が、企業とは異なるケースが多いことを認識することが重要である。例えば、総合大学か、国内の大学か等、大学に応じて事情は異なるが、一般に、学部や研究室は、企業における部署等と比べて独立性の高い運用がなされているケースが多い。このため、「大学」のみをDDの対象として位置付けてしまうと、考慮すべきリスク項目の見落とし、あるいは過度なリスク評価に繋がるおそれがある。また、DDを踏まえて評価したリスクについては、契約上の対応によって軽減を図ることが考えられるが、契約上の義務を負う契約主体が、大学法人となるかを確認・考慮する必要もある
- このため、ケースバイケースではあるが、DDの対象としての「組織」を大学全体にのみ設定するのではなく、学部や研究室をDDの対象としての「組織」と位置付けることも含めて、DDの対象となる「組織」をどのように設定するかが重要となる (総合大学か、国内大学か等にもよるが、大学全体/学部・研究室単位と、複合的に確認すべきケースもある)。なお、共同研究に参画する研究者個人に関するDDについては、p127参照

確認項目

- 相手方の特性によらず確認すべき事項 (p122) のほか、最低限リスクマネジメントの状況や学内・研究室内における情報管理の体制等を確認することが重要である。具体的には、経済産業省「大学における秘密情報の保護ハンドブック」¹や、イノベーション促進産学官対話会議事務局「産学官連携による共同研究強化のためのガイドライン (3-2-2-2)技術流出防止マネジメント (営業秘密管理)」²等が参考となる。また、大学におけるリスクマネジメントのあり方については、特に、共同研究のテーマが重要技術領域リスト (手順書参照) に該当する場合には、経済安全保障の観点から研究セキュリティの確保が必要となる技術領域に当たりうるため、相手方と連携し、丁寧に確認することが重要である。研究成果の公開を前提とする競争的研究費のうち特定のプログラムを対象にしたものであるため (p115参照)、企業との共同研究において馴染まない事項も含まれる点には留意を要するが、必要に応じて、「研究セキュリティの確保に関する取組のための手順書」³に沿った評価と適切なリスクマネジメントの実施状況を確認することが重要である (例:「日常的に実施する取組」として実施が求められている情報管理体制の整備状況や、研究インテグリティのチェックリストに基づく情報の申告状況等)
- 確認に当たっては、企業との共同研究への関与の度合いにもよるものの、教授等の共同研究責任者のほか、必要に応じて、情報管理に関して学内で担当している部局に確認することも一案 (秘密情報の管理に係る学内体制については、次ページも参照)。また、各大学が産学連携に関するウェブサイト等で公表している情報を確認することも有用



1: 経済産業省「大学における秘密情報の保護ハンドブック」

(https://www.meti.go.jp/policy/innovation/corp/himitsujoho/161012_himitsujoho.pdf)

2: イノベーション促進産学官対話会議事務局「産学官連携による共同研究強化のためのガイドライン」

(https://warp.ndl.go.jp/info:ndljp/pid/13982561/www.mext.go.jp/a_menu/kagaku/taiwa/1380912.htm)

3: 研究セキュリティと研究インテグリティ確保に関する有識者会議「研究セキュリティの確保に関する取組のための手順書」

(<https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha.html>)

(参考) 大学における秘密情報の保護ハンドブック

- 大学を読み手として想定し、①保有する情報の把握・評価、秘密情報の決定、②秘密情報の分類、情報漏えい対策の選択及びそのルール化、③秘密情報の管理に係る学内体制のあり方、④秘密情報管理における学生等の扱い、について記載されている

①保有する情報の把握・評価、秘密情報の決定

これまでに秘密情報を区別して管理するための規程等や体制を整備してこなかった大学を念頭に、自学が保有する情報から秘密情報を決定するまでのステップを紹介

- (1) 大学が保有する情報（紙媒体、電子データ、ノウハウ等）の全体像の把握
- (2) 保有情報の評価
例) 漏えい時の社会的信用低下による共同研究件数の減少等の観点
- (3) 評価の高低に基づく秘密情報の決定

③秘密情報の管理に係る学内体制のあり方

学内体制の整備における基本的な考え方を示しつつ、考えられる学内体制の参考例を提示

- 例)「秘密情報管理委員会」
(責任者は、副学長や担当理事等)

部局名(例)	情報管理に関して学内で担当している役割
総務課	・法人文書管理(台帳管理等)
人事課	・教職員を対象とする教育の実施 ・違反を犯した教職員の処分
産学連携本部	・学外機関との秘密保持契約等の雛形整備
情報基盤センター	・学内情報システムとネットワークの管理 ・学内セキュリティポリシーに基づく運用
学内CSIRT	・学内情報セキュリティインシデントへの対応
その他各部局	・自部署で管理する情報の保守

②秘密情報の分類、情報漏えい対策の選択及びそのルール化

- ・秘密情報の分類例の説明
- ・大学における5つの漏えい対策とその目的の説明
例) 接近の制御、持ち出しの困難化等
- ・秘密情報の取扱方法に関するルール化の考え方
 - (1) 大学全体に共通する一定の統一的なルール
 - (2) 部署・研究室等の単位ごとの個別対策の策定

④秘密情報管理における学生等の扱い

学生等に対しどのような秘密保持の遵守等を求めることが望まれるかといった点について説明

- 例) 学内研究活動や学外機関等が関与する共同研究等へ学生等を参加させる場合
- (1) 研究活動への学生等の参加の是非の検討
(学生のメリットと義務のバランスで検討)
 - (2) 秘密保持の遵守等を求める方法の検討
(イ) 学生等を対象とした通則等での指示
(ロ) 秘密保持に関する誓約書の提出

(参考) 輸出管理上の懸念主体等の確認

輸出管理上の懸念主体となっていないか、国連・外国政府による制裁対象となっていないか等、可能な限り公的機関のウェブサイト等を通じて確認を行う。

【経産省：外国ユーザーリスト】

<https://www.meti.go.jp/policy/anpo/law00.html#userlist>

【財務省：経済制裁等対象リスト】

https://www.mof.go.jp/policy/international_policy/gaitame_kawase/gaitame/economic_sanctions/list.html

【米国商務省：統合スクリーニングリスト】

<https://www.trade.gov/consolidated-screening-list>

【国際連合 安全保障理事会 統合リスト】

<https://main.un.org/securitycouncil/en/content/un-sc-consolidated-list>

なお、手順書のうち、「(参考) デュー・ディリジェンスに用いる情報の収集について」の下記記載も、参考にされたい。

(参考) デュー・ディリジェンスに用いる情報の収集について

デュー・ディリジェンスに用いる情報は、以下に例示するツールを用いて収集することが考えられる。その他のインターネット等で公開されている情報も参照可能であるが、当該情報の信頼性や正確性を慎重に確認することが必要である。また、デュー・ディリジェンスの実施に際し、情報の信頼性などの判断が困難な場合は、適宜、相談窓口、資金配分機関等に相談することが望ましい。

- ・学術論文データベース (Web of Science、Scopus等)
- ・ポータルサイト (Google Scholar等)
- ・研究データベース (e-Rad、科研費データベース、researchmap等)
- ・知的財産データベース (特許情報プラットフォームJ-PlatPat等)
- ・経済産業省の外国ユーザーリスト
- ・米国の統合スクリーニングリスト

なお、これらのツールを用いて収集した情報だけでは十分なデュー・ディリジェンスの実施が困難な場合は、企業が提供する情報分析ツールや企業への委託調査を活用することも考えられる。

1. ⑥ パートナー候補のDDの徹底（関与する個人の観点）

- 組織単位での体制の確認に加え、人からの技術流出リスクを低減する観点から、必要に応じ、共同研究に参加するメンバーについても、共同研究先の協力を得て、個人単位のDDを実施することが重要。DDの結果を踏まえ、重要技術に関する情報のアクセス管理を検討する。

対応策の例

- 組織としてはリスクが高いと評価されない場合であっても、共同研究に伴い提供する技術情報を管理・利用するのは共同研究に参加する研究者になるため、共同研究参加者から流出する可能性があることを、まず認識する。その上で、共同研究で扱う情報の重要度や性質に応じ、共同研究先の協力を得て、確認作業を行う

（確認すべき事項）

共通して確認する事項の例

- 外国政府等により情報収集活動への協力義務の有無
本項目に限らないが、共同研究先に所属する者から直接的にエビデンス等を確認できない場合も多いため、契約上、共同研究先に対して確認・表明保証を求めることも一案
- 情報取扱に関する非違歴・懲戒歴や前科
なお、前科は、個人情報保護法上の「要配慮個人情報」に該当するため、取得には本人同意が必要になるほか、仮に第三者提供に該当する場合には、提供に関する本人同意も必要
- 居住者該当性や特定類型該当性
共同研究先が本邦法人の場合も、共同研究契約や研究計画書等に、当該共同研究に参加するメンバーを明記した上で、共同研究先において居住者該当性や特定類型該当性を確認する

アカデミアとの研究の場合に確認する事項の例

- 研究インテグリティのチェックリスト(*)において確認された項目
- 「研究セキュリティの観点から確認すべき情報」を参照（右を参照）
- 雇用関係のない参加者（学生等）の有無

再掲

研究セキュリティ確保のために確認すべき項目

- ① 学歴（必要に応じて指導教官等の情報を含む。）
- ② 研究経歴・職歴
- ③ 研究費の取得歴
- ④ 研究費以外の支援等の取得歴
- ⑤ 発表論文における筆頭著者、責任著者及び共著者
- ⑥ 特許の出願状況（共同発明者及び共同出願人の情報を含む。）
- ⑦ 外国の人材採用プログラムへの参加歴
- ⑧ 指針に基づく処分歴
- ⑨ リストへの掲載の有無
- ⑩ リスト掲載機関への所属の有無
- ⑪ リスト掲載機関に所属する研究者との関係（共同研究・受託研究の実施、共著論文の執筆・公表及び学会等における連名の口頭発表の実績をいう。）の有無
- ⑫ 安全保障貿易管理における「非居住者」（一時帰国しその滞在期間が6月未満の日本人等）又は「特定類型」（日本の大学の教授であり外国の大学と雇用契約を締結し教授職を兼職している者、外国政府から留学資金を得ている留学生、外国の人材採用プログラムに参加し多額の研究資金や生活費の提供を受けている研究者等）への該当性
- ⑬ その他資金配分機関がデュー・デリジェンスの実施に当たり必要と認める事項

※ 研究者向け「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト（雛形）」(令和3年12月17日版)
<https://www.8.cao.go.jp/cstp/kokusaiteki/integrity/checklist1.pdf>

(参考) 研究インテグリティとは

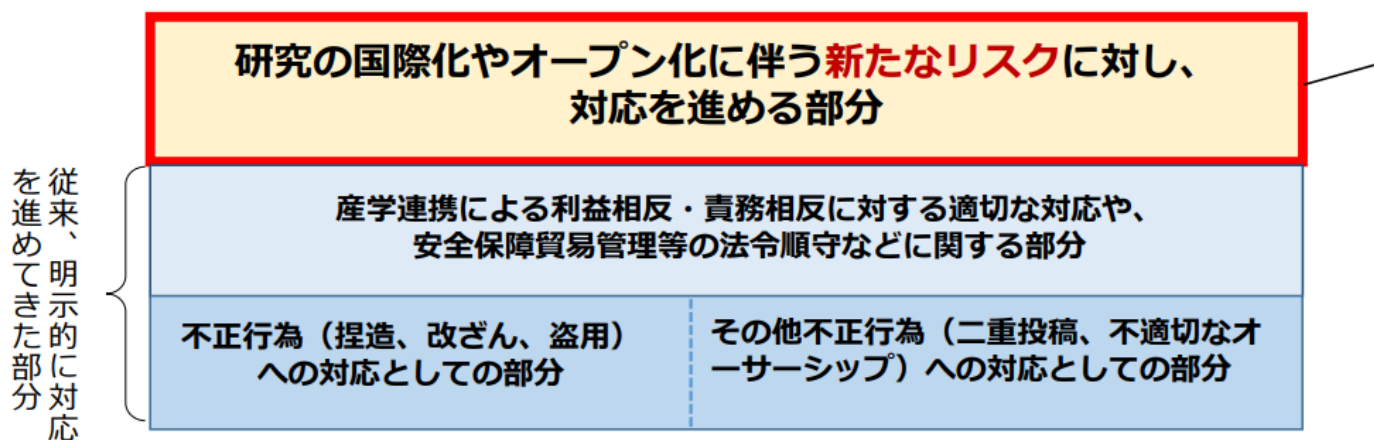
新たに求められる研究の健全性・公正性（研究インテグリティ）について

背景・課題

- 我が国の科学技術・イノベーションの創出・振興のためには、多様な相手との国際共同研究を推進していく必要。他方、研究活動の国際化等の進展に伴う新たなリスク※により、意図せざる技術流出に陥る危険性が指摘。
※研究成果を独占しようとする不当な共同研究契約などを契約してしまうリスク等
- こうした新しいリスクに対応しつつ、必要な国際協力等を進めていくためには、研究の健全性・公正性（研究インテグリティ）を確保し、国際的に信頼性のある研究環境を構築する必要。
- このような背景の下、令和3年4月に政府としての対応方針を決定。

リスク軽減の観点から新たに確保が求められる研究インテグリティ

新たに求められる部分
 （研究活動の透明性を確保し、説明責任を果たすといった、研究者や研究組織としての「規範」）



➡ **大学・研究者自身に対するレピュテーションリスクの観点からも研究インテグリティの確保に自ら取り組んでいただくことが重要**

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

2. ① 事前のNDA締結と段階的な情報開示、NDA締結前の特許出願

- パートナー選定の前後から、一定の情報を相互に提供し、共同研究の実施可能性を検討するケースが多い。また、協議段階にもかかわらず、本来は共同研究契約の締結後に共有すべき情報が提供される等して、より踏み込んだ議論に移行するケースも少なくない
- そのため、**情報流出**や**知的財産**についてトラブルが生じるリスクを防ぐため、**事前協議段階**での相手方との情報共有や交渉の際に、**NDAを確実に締結**するとともに、**必要に応じて特許出願**や**相手方の体制確認**等を行う

対応策の例

① 秘密保持契約 (NDA) の早期締結

- 自社から情報を提供する前 (打合せ前等) に、確実に秘密保持契約を締結する。例えば、目的外利用・第三者への情報開示・再委託・複製の禁止、提供資料/試料の取扱範囲、情報返却/破棄の条項を設定することが考えられる
- また、共同研究契約の締結前に試料等を提供する場合には、その内容や重要性等に応じて、分析等の禁止のほか、使用場所や使用期間等を具体的に定めておく必要がないか、慎重に検討する
- 秘密保持義務については、残存条項として、少なくとも提供した情報が陳腐化するまでの期間等を考慮した上で、契約終了後も一定期間は存続させることが重要

② NDA締結前における情報の提供制限や特許出願

- NDA締結前は機密機微情報を提供せず、基本的には公開情報に限定する。非公開情報を提供するのであればNDAの締結を前提とする
- NDA締結後に知財トラブルになる可能性がある場合、必要に応じ、自社技術の特許を事前に出願することも検討する

③ 相手方の体制に応じた情報開示の徹底

- 相手方のDDが未実施の場合にも、機微情報の開示・提供は行わない。DD実施後も、当初から全ての情報を開示せず、必要最低限の範囲で段階的に情報を提供することが重要
- また、デジタル権利管理 (DRM) ツールを活用し、事後に相手側で閲覧不能等とする、相手方の体制が不十分な場合は是正を求め、是正されない場合は研究を開始しない等の対策も重要

事前のNDA
締結



段階的な情報開示
DRMツール等の
活用



事前の特許出願



※ NDAのひな型については、特許庁のイノベーションポータルサイトも参照

(https://www.jpo.go.jp/support/general/open-innovation-portal/document/index/ma-v2_2-nda_chikujouari.pdf)

2. ② 自社の契約書ひな型の活用とリスクに応じた契約条件設定

- 相手方の提示するドラフトで安易に契約すると、相手方に有利な契約となり、自社の技術流出リスクが高まる可能性がある
- 契約交渉等の個別事情によるところは大きいものの、**必要以上に相手方に有利な契約に応諾しないよう、自社の契約書ひな型**を用意しその使用を目指すことや、契約交渉において譲歩すべきでない範囲を確認しておくことが重要。契約交渉においては、**情報の重要度や相手方のリスクの大きさ**を考慮し、それらに応じた**追加等修正**を行うことが重要

対応策の例

① 可能であれば、自社の契約書ひな型の利用を徹底する

- 必要以上に相手方に配慮した契約書に応諾することのないよう、各種リスクに対応可能な自社契約書ひな型を用意し、その内容に沿った契約の締結を目指す
 - ✓ 守秘義務や目的外使用の禁止、及び第三者提供の制限
 - ✓ 成果の帰属・利用権の明確化、違反時の罰則 等

② 相手方のリスクに応じて条項を追加する

- 共同研究先のDDの結果等（p120～）を踏まえつつ、相手方が受ける規制や、相手方の拠点がどの国に所在しているか等を基にリスク判断
- 追加条項は、表明保証条項や、人を通じた技術流出を防止するための条項（引き抜き禁止等）等が考えられる

③ 譲歩できない範囲を事前に明確にしておく

- 契約交渉等の結果として、自社のひな型に基づいて契約締結できない場合もあるため、技術流出対策の観点から譲歩できない範囲を、技術の重要性も踏まえつつ、あらかじめ明確にしておく
- 仮に相手方のひな型をベースとする場合でも、条項を追加する

各種リスクや情報の重要度に応じた契約書ひな形の用意



- 守秘義務や取扱者の明確化
- 成果の帰属
- 違反時の罰則
- ⋮



必要に応じて条項の追加を実施

追加条項

- 表明保証条項
- 人材の引き抜き禁止
- ⋮

※ 共同研究契約のひな型についても、特許庁のイノベーションポータルサイトも参照。

https://www.jpo.go.jp/support/general/open-innovation-portal/document/index/ma-v2_2-kyoudou_chikujouari.pdf

※ 「秘密情報の保護ハンドブック ～企業価値向上にむけて～」掲載の共同研究開発契約書のひな形も参照されたい（p202～）

<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

2. ③ 共同研究の目的・テーマの範囲の画定

- 契約上定められた**共同研究の目的やテーマの定義や範囲は、本節で記載する契約上の対策の多くに影響する**
- そのため、共同研究の目的やテーマを契約上定めることが重要となるが、**その範囲については、慎重な検討を要する**

対応策の例

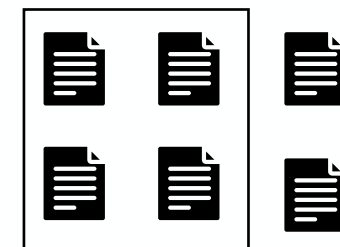
① 目的やテーマを契約時点であらかじめ明らかにしておく

- 契約締結に至るまでに当事者間で認識を共有した共同研究の目的やテーマを、正確かつある程度具体的に定めることが必要となる
- ただし、目的やテーマを狭く規定してしまうと、本来は適用したい情報について秘密保持義務が及ばなくなるケースや、本来禁止したい範囲の競業行為を禁止できない等の弊害が生じる可能性がある（それぞれの義務については、p135～参照）。また、共同研究の過程で一定の変更等が発生した場合に、何度も契約書の修正が必要になりかねない
- このため、司令塔となる部署と関係部署（知財部・法務部 等）が連携し、必要に応じて弁護士等の外部専門家にも相談の上で、ある程度の幅を持った適切な記載にすることが重要となる
- その上で、秘密保持条項や競業避止条項等を規定し、いかなる技術情報や競業行為が契約の適用を受けるかについて相互に認識を共有し、契約範囲外の技術流出を防ぐことが重要である

共同研究の目的・範囲の定義



目的の定義



範囲の定義

※ 共同研究のテーマ及び目的に関する規定のモデル条項や、テーマの抽象度や広狭に関する考え方等については、前述の特許庁のイノベーションポータルサイトに掲載された共同研究開発契約のモデル条項にも詳細に説明されているため、参照されたい。

(https://www.jpo.go.jp/support/general/open-innovation-portal/document/index/ma-v2_2-kyoudou_chikujouari.pdf)

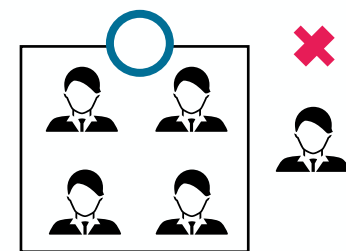
2. ④ 研究参加メンバーや情報の取扱方法の明確化

- 不正な持ち出しや関係ない者によるアクセスを防ぐため、関与する個人の観点からのDDの結果（p127参照）も踏まえて、**自社が共同研究先の誰に技術情報を提供しているか（誰の取扱いを認めているか）を、契約書や研究計画書等において、氏名等とともに明確にすることが重要**である
- また、参加メンバーに加えて、**取扱方法や情報の利用範囲を限定し、異なる取扱いを禁止することが重要**

対応策の例

① 参加メンバーの限定・明確化

- 共同研究契約や付随する研究計画書・名簿等において、研究参加者を氏名等により特定し、記載がない者には情報を取り扱わないことを明確に定める
- また、研究参加者に異動が生じる場合には、通知を求めるとともに、事前の書面承諾がない限り、新たな研究参加者には技術情報を取り扱わないことを定めることも重要である
- 技術の重要性等によっては、各参加者から個別に秘密保持義務に係る誓約書の提出を求めることも考えられる。特に、大学との共同研究の場合、研究体制に学生が含まれるケースもあるが、通常、学生は大学に雇用等されておらず、秘密保持義務を含めた就業規則等の適用を受けないため、注意が必要となる。契約上の対応策としては、秘密保持義務や損害賠償条項、成果の帰属等について定めた誓約書の提出を求めることが考えられる。提出を行わない学生については、共同研究への関与を認めないことや、大学が雇用して（リサーチアシスタント（RA）等）、賃金を支払い、雇用契約を締結することが考えられる
- また、研究室における研究参加メンバーとそれ以外との間の情報遮断が不十分なケースもあるため、技術の重要性やパートナーDDの結果も踏まえて、研究室内の非参加メンバーからも個別に秘密保持義務に係る誓約書の提出を求めることが考えられる



参加メンバーの特定



ログの追跡

※ その他学生等の取扱いに関しては、「大学における秘密情報の保護ハンドブック」第5章 秘密情報管理における学生等の扱いも参照。
https://www.meti.go.jp/policy/innovation_corp/himitsujoho.html

② 情報の取扱方法の明確化・第三者への委託の制限

- 情報の流出を防ぐため、情報の取扱区域の限定、アクセスの管理・制限、アクセスやダウンロードに関するログの取得・管理等を行う旨定め、意図しない経路や取扱いのトレーサビリティを担保する
- 共同研究の目的や双方の役割等について可能な限り明確に定めた上で、目的外での情報利用の禁止、事前の書面承諾のない持ち出しや解析、第三者への業務委託の原則禁止等を定める。また、違反時に共同研究の停止や損害賠償請求ができるよう条項化する

2. ⑤ 提供する技術情報の範囲と、知的財産の帰属等の明確化

- 必要以上に技術情報を提供することのないよう、契約上の手当として、共同研究の実施において提供すべき技術情報の範囲や提供方法をあらかじめ明確に規定することが重要である
- また、相手方が共同研究に関わる技術を単独で特許化・利用することを防ぐために、契約において、**成果物や知的財産の帰属と利用権についてあらかじめ明記**することが重要である

対応策の例

①バックグラウンドIP/フォアグラウンドIPの区分

- 前提として、共同研究契約以前から保有していた技術情報（バックグラウンドIP）を特定した上で、共同研究により創出される技術（フォアグラウンドIP）と適切に区分することが、情報のコンタミネーションを防ぐ観点から重要である
- 共同研究に伴い提供するバックグラウンドIPについては、必要に応じて、共同研究開始前に単独で特許を出願するほか、公証制度等を利用し、共同研究前から既に保有していたことの証拠化を図ることが考えられる。こうした対策の考え方や、管理を怠った場合のリスク等については、特許庁のイノベーションポータルサイトに掲載された共同研究開発契約のモデル条項（2条（定義）や6条（情報の開示）等）を参照されたい

※ 特許庁のイノベーションポータルサイトご参照 (https://www.jpo.go.jp/support/general/open-innovation-portal/document/index/ma-v2_2-kyoudou_chikujouari.pdf)

②提供する技術範囲・提供方法の明確化

- NDA締結段階に限らず（p130参照）、共同研究の実施段階においても、提供する技術情報を必要十分な範囲に限ることが重要である。契約上、提供範囲を限定・明確化する、自社の裁量の範囲とする等して必要のない範囲まで提供義務を負わないようにする
- また、提供した技術情報をもれなく確認するためにも、提供方法（特定のサーバやフォルダ上での提供に限る等）を明確化することも重要である

③成果物・知的財産権の帰属や利用権の明記

- 共同研究により創出される知的財産を円滑に利用するとともに、技術流出を含めて、知的財産に関する紛争を防止する観点から、契約書に成果物・知的財産の帰属と利用権を明記することが重要である
- 知的財産権の帰属の決め方には様々なパターンがあるが、相手方単独での特許化・利用、無断での第三者への共有を防止する観点からは、自社の単独帰属又は当事者間での共有を選択することが望ましい

2. ⑥ 秘密保持義務・競業避止義務の設定

- 共同研究の相手方やその内部関係者が、共同研究に係る**技術情報を不正に持ち出すリスク**や、他の研究テーマに流用されるリスクが存在するため、**秘密保持義務**や流用の制限・競業避止義務を定めることが重要

対応策の例

① 秘密保持義務の規定

- 共同研究契約の締結前にNDAを締結している場合であっても (p130参照)、共同研究の実施フェーズでは、NDA段階よりも機微な技術情報が提供されるため、共同研究契約においても、秘密保持条項を定めることが重要
- 秘密情報の定義 (共同研究の成果の扱い含む) に関する検討を要する場合もあるが、義務の内容としては、NDAと同様、第三者への情報開示・再委託・複製の禁止、提供資料/試料の取扱範囲、試料の分析等の禁止、情報返却/破棄等を盛り込むことが考えられる。また、共同研究期間中に限らず、終了後一定期間の存続について定めることも重要。なお、委託を認める場合であっても、委託先企業等への秘密保持義務を徹底させる
- また、不公正な取引方法に該当しないよう、公正取引委員会「共同研究開発に関する独占禁止法上の指針」(以下「共同研究開発ガイドライン」という) にも留意しつつ、提供した技術情報が共同研究テーマ以外に流用されることを制限することも重要である (以下参照)。経済安全保障の観点から行おうとする自社の行為と独占禁止法との関係について、不明な点等があれば、公正取引委員会への相談も検討する

共同研究開発ガイドライン第2の2 (抜粋)

(1) 共同研究開発の実施に関する事項

ア 原則として不公正な取引方法に該当しないと認められる事項

- ② 共同研究開発のために必要な技術等 (知見、データ等を含む。以下同じ。) の情報 (共同研究開発の過程で得られたものを含む。以下同じ。) を参加者間で開示する義務を課すこと
- ③ ②で他の参加者から開示された技術等の情報に関する秘密を保持する義務を課すこと
- ④ ②の技術等の情報以外に共同研究開発に関して他の参加者から得た情報のうち特に秘密とされているもの (共同研究開発の実施自体が秘密とされている場合を含む。) の秘密を保持する義務を課すこと
- ⑥ ②で他の参加者から開示された技術等を共同研究開発のテーマ (共同研究開発の対象範囲をいう。以下同じ。) 以外に流用することを制限すること ((1)イ①の場合を除く。)

イ 不公正な取引方法に該当するおそれがある事項

- ① 技術等の流用防止のために必要な範囲を超えて、共同研究開発に際して他の参加者から開示された技術等を共同研究開発以外のテーマに使用することを制限すること ((1)ア⑥参照)
 - 開示された技術等をそのまま流用するのではなく、それから着想を得て全く別の技術を開発することまで制限するような場合には、当該研究開発活動の制限は、技術等の流用防止のために必要な範囲を超えて参加者の事業活動を不当に拘束するものであり、公正な競争を阻害するおそれがあるものと考えられる (一般指定第一二項 (拘束条件付取引))

※ 公正取引委員会「共同研究開発に関する独占禁止法上の指針」第2 共同研究開発の実施に伴う取決めに対する独占禁止法の適用について」も参照。

(<https://www.jftc.go.jp/dk/guideline/unyoukijun/kyodokenkyu.html>)

※ 関連して、「経済安全保障と独占禁止法に関する事例集」(令和7年11月20日 公正取引委員会・経済産業省・国土交通省) の事例⑮ (他社との共同研究開発の制限) も参照。

(https://www.jftc.go.jp/houdou/pressrelease/2025/nov/251120_economic.security.html)

2. ⑥ 秘密保持義務・競業避止義務の設定

対応策の例

② 競業避止義務の規定

- 共同研究に伴い共同研究先やその参加メンバーに蓄積するノウハウの流出を防ぐためには、秘密保持義務を課すだけでなく、一定の競業避止義務を課すことも有効となる。他方で、必要な範囲を超えて広く研究開発活動を制限すると、不公正な取引に該当するおそれがあることから、前記と同じく、共同研究開発ガイドラインを踏まえて、適切な契約条項を定めることが重要である
- 具体的には、特定した研究参加メンバー（p133参照）について、研究開発終了後の合理的な期間、競合企業との研究開発業務に従事することを禁止することが考えられる（次ページの参考事例も参照）。また、必要な場合には、研究開発終了後の合理的期間に限り、同一又は極めて密接に関連するテーマに関する第三者との研究開発を制限することが考えられる。その他、転職後の関係者の引き抜き禁止や、現地法人での役職兼務禁止等を定めることも考えられる
- 経済安全保障の観点から行おうとする自社の行為と独占禁止法との関係について、不明な点等があれば、公正取引委員会への相談も検討する

共同研究開発ガイドライン第2の2（抜粋）

(1) 共同研究開発の実施に関する事項

ア 原則として不公正な取引方法に該当しないと認められる事項

- 共同研究開発のテーマと同一のテーマの独自の又は第三者との研究開発を共同研究開発実施期間中について制限すること
- 共同研究開発の成果について争いが生じることを防止するため又は参加者を共同研究開発に専念させるために必要と認められる場合に、共同研究開発のテーマと極めて密接に関連するテーマの第三者との研究開発を共同研究開発実施期間中について制限すること（(1)ウ①参照）
- 共同研究開発の成果について争いが生じることを防止するため又は参加者を共同研究開発に専念させるために必要と認められる場合に、共同研究開発終了後の合理的期間に限り、共同研究開発のテーマと同一又は極めて密接に関連するテーマの第三者との研究開発を制限すること（(1)ウ①及び②参照）
 - 共同研究開発終了後についての研究開発の制限は、基本的に必要とは認められず、参加者の研究開発活動を不当に拘束するものであるため、公正競争阻害性が強いものと考えられる（(1)ウ①及び②参照）。ただし、共同研究開発終了後の合理的期間に限り、同一又は極めて密接に関連するテーマの第三者との研究開発を制限することは、背信行為の防止又は権利の帰属の確定のために必要と認められる場合には、原則として公正競争阻害性がないものと考えられる。
- 参加者を共同研究開発に専念させるために必要と認められる場合に、共同研究開発実施期間中において、共同研究開発の目的とする技術と同種の技術を他から導入することを制限すること（(1)イ②の場合を除く。）

イ 不公正な取引方法に該当するおそれがある事項

- 共同研究開発の実施のために必要な範囲を超えて、共同研究開発の目的とする技術と同種の技術を他から導入することを制限すること（(1)ア⑩参照）
 - 参加者が共同研究開発に関係する知見、成果等に関する権利を放棄する等して共同研究開発から離脱し、他から優れた技術を導入することを希望する場合にまでそれを認めないといった制限は、共同研究開発の実施のために必要な範囲を超えて参加者の事業活動を不当に拘束するものであり、このような事項は、競合する技術を保有する事業者の取引機会を奪い又は参加者の技術選択の自由を奪うものであって、公正な競争を阻害するおそれがあるものと考えられる（一般指定第一項（排他条件付取引）又は第二項（拘束条件付取引））。

ウ 不公正な取引方法に該当するおそれが強い事項

- 共同研究開発のテーマ以外のテーマの研究開発を制限すること（(1)ア⑧及び⑨の場合を除く。）
- 共同研究開発のテーマと同一のテーマの研究開発を共同研究開発終了後について制限すること（(1)ア⑨の場合を除く。）
 - 上記①及び②のような事項は、参加者の研究開発活動を不当に拘束するものであって、公正競争阻害性が強いものと考えられる（一般指定第二項（拘束条件付取引））。

参考事例

○ 「独占禁止法に関する相談事例集（平成23年度）」事例5 <https://www.jftc.go.jp/dk/soudanjirei/h24/h23nendomokuji/h23nendo05.html>

【相談要旨】

- (1) X社は、電子機器Aのメーカーである。
- (2) Y社は、ソフトウェアBの開発事業者である。
- (3) 電子機器Aを作動させるためにはソフトウェアBをインストールする必要がある。ソフトウェアBは特殊なものではなく、これを開発できる技術者は多数存在し、また、そのような技術者を多数有する事業者もY社をはじめ多数存在する。
- (4) X社とY社は、電子機器AにインストールするためのソフトウェアBの共同研究開発を行うことを検討しているところ、その際、開発に係るノウハウの流出を防ぐため、守秘義務契約を締結することとした。しかしながら、ソフトウェアBの開発のノウハウは開発担当者個人に蓄積されるため、X社は、守秘義務契約だけではノウハウの流出を防止することはできないと考え、Y社に対し、開発期間中及び開発終了後3年間に限定し、本件開発に携わったY社の技術者（以下「担当技術者」という。）を、電子機器AのメーカーのうちX社と特に競合する者（このような者は3社存在する。）の開発業務に従事させることを禁止する内容の契約を締結することを検討している。
- (5) ソフトウェアBの共同研究開発においては、当事者間において、開発終了後3年から5年程度の期間に限って、同一のテーマの第三者との研究開発を禁止することが業界内で一般的とされている。
このようなX社の取組は、独占禁止法上問題ないか。

【独占禁止法上の考え方】

- (1) 共同研究開発終了後についての研究開発の制限は、基本的に必要とは認められず、参加者の研究開発活動を不当に拘束するものであるため、公正競争阻害性が強いものと考えられる。ただし、共同研究開発終了後の合理的期間に限って、同一又は極めて密接に関連するテーマの第三者との研究開発を制限することは、背信行為の防止又は権利の帰属の確定のために必要と認められる場合には、原則として公正競争阻害性はないものと考えられる（共同研究開発ガイドライン第2-2（1）ア(9)）。
- (2) 本件は、共同研究開発を行うに当たり、X社がY社に対し、担当技術者の共同研究開発終了後の研究開発を制限するものであるところ
ア 担当技術者が、X社の協力を得て取得したノウハウを用いて他社との開発を行うという背信行為を防止するものであり、その目的自体は正当なものであること
イ （ア） 守秘義務契約だけでノウハウの流出を防止することは容易でないこと
（イ） 担当技術者のみを対象としており必要最小限の制限と考えられること
（ウ） 本件制限の期間は業界内で一般的とされている期間の中で最も短いものを選択していること
から、制限の内容について不合理なものとはいえないこと
ウ 本件制限は、担当技術者が電子機器AのメーカーのうちX社と特に競合する3社の開発業務に従事させることを禁止するのみであって、例えば、Y社が、担当技術者以外の自社の技術者に従事させて当該3社と共同研究開発を行うこと、Y社が応用技術を開発して3社に営業活動を行うこと、3社以外の電子機器Aのメーカーの開発業務に従事させること等は禁止されておらず、ソフトウェアBの技術市場及び製品市場への影響は軽微であること
から、独占禁止法上問題となるものではない。

【回答の要旨】

X社が、Y社と共同研究開発を行うに当たり、Y社に対し、開発期間中及び開発終了後3年間、担当技術者を同一テーマの開発業務に従事させることを禁止することは、独占禁止法上問題となるものではない。

2. ⑦ モニタリング条項の設定と実施による情報管理の確認

- 特に機微な情報を取り扱う共同研究においては、**相手方が契約に従って適切に情報管理を行っているか確認**するため、契約時に**対面及び書面での監査/モニタリング**に関する条項を盛り込み、定期的又は必要に応じて監査やモニタリングを実施することが重要

対応策の例

① モニタリングに関する条項の規定

- 技術情報が契約に従って適切に管理されているかを確認するため、契約上、モニタリング条項を盛り込むことが有用である。確認の方法は、確認項目によってケースバイケースではあるが、例えば以下が考えられる

対面にて確認することが望ましい事項

- ✓ 情報の保管・管理場所の確認や、貸与物やサンプルの状況の確認等を行う

書面にて確認する事項

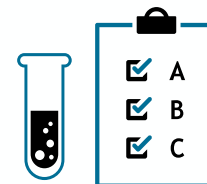
- ✓ 情報へのアクセス権限の設定やログの管理状況、研究への関与メンバーの変更の有無、情報の第三者への共有の有無、成果の公表予定の有無等を確認する

② モニタリング結果を踏まえた是正

- モニタリングの結果を踏まえ、相手方に対して契約に定めた情報管理を行うよう是正を求めることが重要である
- 是正に応じない場合や見込まれない場合については、解除事由に含める等して、契約を解除することができるようにする

監査/モニタリング条項の設定

対面での確認



確認事項

- 保管・管理状況
- 貸与物やサンプルの状況
- ⋮

書面での確認



確認事項

- アクセス権限・ログ
- 情報取り扱い状況 (名簿 等)
- 第三者共有の有無
- ⋮

状況に応じて是正

2. ⑧ 共同研究先の業績悪化・資本変動等に備えた解除事由等の設定

- 共同研究先の業績悪化や破綻、資本構成の変化等の契約後の事情変更により、技術流出リスクが高まる可能性がある
- このリスクを最小化するため、相手方の資本構成を含め、DDの段階で確認した事項が大きく変化する際に、それを事前に把握する手段とその対応策を明確化することが重要

対応策の例

① 事前承諾・通知事項・解除事由として規定

- 合併や事業譲渡、経営権の変動を伴う株式の発行等については、パートナーDD (p122～参照) において確認した相手方の資本構成等に大きく変化を生じるものであるから、事前承諾又は事前通知を求める
- その上で、懸念のある主体が、新たな株主になること等により、技術情報にアクセスする可能性が生じる場合には、共同研究契約を解除することができるよう、解除事由として定めることが考えられる
- また、資本構成等の変更に限らず、例えば以下のように、事前のDDで確認した重要な事項の変動については、解除事由等として規定することが考えられる
 - ✓ 経営状況の悪化
 - ✓ 外国での多額の研究費の申請
 - ✓ 制裁リスト等への追加 等

解除事由として想定される主な事項

資本構成 (支配者) の変更

経営状況の悪化



外国での多額の研究費の申請



② 解除後のデータ返却等の規定・実行

- 共同研究契約を解除するだけでは技術流出リスクは軽減できないため、相手側に提供したデータやサンプルの返却や破棄に関する条項を盛り込むとともに (p141参照)、確実に実行することが重要

2. ⑨ 非公開範囲の設定や、成果公開時の事前承諾手続等の明確化

- 特に共同研究の相手方が大学等の場合、学会や論文等における公表を望むケースが多いが、自社として秘匿化を望む場合や研究成果に新規性が認められる場合には、**学会や論文等で発表されることで、意図せず関連する技術情報が明らかにされてしまうリスク**がある
- これを回避するため、**提供した技術情報の秘匿化・非公開期間の設定**や、**成果を公表する際の事前通知のルール**を設定することが重要である

対応策の例

① 非公開範囲・非公開期間の規定

- 特に、自社から提供した秘匿化すべき技術情報（ノウハウ含む）については、契約上、特許出願時の公表書類に記載しない旨規定する
- 特許出願に限らず、情報が陳腐化する期間等も考慮の上で、非公開期間を設定し、その間の公表を禁止することも重要である

② 成果の公表に係る手続の明確化

- 研究成果を公表する場合には、共同研究期間中及び共同研究期間後のいずれであっても、公表内容について、共同研究先の事前の書面承諾を必要とする旨定めることが重要である。また、承諾が必要となる旨のみならず、公表内容の確認に要する期間について、契約締結段階で当事者双方の認識を共有したうえで、公表予定日の何日前までに承諾の請求をすべきか、契約上明確に定めることも重要となる
- 仮に、事前承諾を要件とできない場合であっても、自社のあずかり知らない範囲で成果が公表されることを防ぐため、公表内容について、時間的余裕をもって事前通知を求めるべきである

③ 成果確認会等における認識の共有

- また、成果の内容や利用・公表等に関する双方の認識を把握しておくために、共同研究の終了前に、研究成果の取扱いを確認するセッションを設け、成果の帰属や、今後の公開予定/特許出願予定について協議する旨を定めることも重要
- 成果確認会においては、提供した技術情報の廃棄証明書（p141参照）、アクセス権限の削除ログ、第三者共有記録等の情報管理に関する文書を整理することも有用である

提供情報の秘匿化・非公開期間の設定



提供した情報は
非公開を要求



契約期間後の
非公表期間を設定

公表前の事前照会・承諾、予定の確認



公開予定の確認
(論文/学会等)

報告会での成果の確認



アウトプット

- 成果確定書
- 返還・消去証明書
- 権限削除ログ
- 第三者への共有記録

2. ⑩ 契約終了後の情報返却・削除義務の明確化と履行確認

- 共同研究に際して提供したデータやサンプル等が相手方に残っていると、これが原因となり、技術が流出するリスクが存在する
- 情報の返却や削除の義務を明記し、違反時には責任を追及できるよう、NDAや共同研究契約において担保することや、運用面でも、実際に削除等がなされたか確認することが重要である

対応策の例

① 契約終了後の返却・削除義務の規定

- NDAや共同研究契約において、契約終了後、共同研究過程で提供したデータやサンプル等の返却を定めることが重要。返却が原則ではあるものの、情報の形態等により返却が困難な場合も想定して、削除・廃棄を義務付け、削除・廃棄証明書の提出を求めることが考えられる
 - ✓ 貸与機材やサンプルはシリアル番号をつけて管理・回収
 - ✓ 自社の情報プラットフォームを用いる場合はアクセスを遮断

② 返却義務等の履行確認

- 共同研究契約に定めた手続きに従って、返却・処分等を確実に行うことが重要。特に、廃棄については、相手方や廃棄事業者に一任するのではなく、取引実績や情報管理体制等を調査して慎重に選定した上で、立ち会い・現地確認まで行う等自社の責任で実施する
- 相手方が違反した場合は、損害賠償条項等により、責任を追及することも考えられる。また、仮に技術情報が流出するおそれがある場合には差止請求を行うことができる旨を契約に明記することも重要

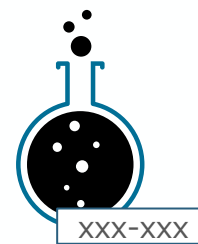
終了時のデータ削除・返却・アクセス遮断



データ削除/
返却



アクセス遮断



シリアル番号
での管理

終了時に履行状況を確認

2. ⑪ 国外訴訟・法制度リスクへの備え

- 共同研究契約に関連して紛争が生じた際に、自社に**不利な法制度・裁判管轄での訴訟**とならないように、事前に**準拠法を日本法または中立的な国際ルールに決定**しておくことが重要
- 相手国の法制度・判例への理解不足による不利な契約となることを防ぐために、**専門家のレビュー**を受けることも有用

対応策の例

①適切な紛争解決手続の規定

- 国際共同研究の場合には特に注意を要するが、準拠法を日本法や中立的な国際ルールに定めることが重要である
- 裁判手続による解決を想定している場合には、裁判管轄を日本の裁判所に定めることが考えられるが、裁判の場合、技術情報が記載された文書等が証拠提出された場合に訴訟記録として公開されるリスクがあるため、非公開の紛争解決手続を利用できるよう、仲裁条項等を定めることも有用。仲裁機関についても、ケースバイケースではあるが、日本の仲裁機関か、外国であっても、中立的な第三国の仲裁機関を指定することが望ましい

②専門家のレビュー依頼の検討

- ケースバイケースではあるが、契約条項の検討に当たっては、法令や判例等の過去の事例を考慮する必要があるほか、国際共同研究契約のように外国の法制度や判例も考慮すべき場合も存在する。必要に応じて、契約内容について、弁護士等の専門家の確認を受けることも検討する
 - ✓ 競争禁止義務の有効性
 - ✓ パートナーDD (p122～参照) の結果も踏まえた契約条項の規定
 - ✓ 成果の帰属や利用・公表に関する規定の適切性
 - ✓ 相手方の契約違反時の手当の検討

準拠法の設定



日本



中立的な
ルール

専門家によるレビュー



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

3. ① 研究計画等における情報の利用・管理ルールの特明確化

- 契約上の措置のみでは、共同研究の相手方による提供した試料の持ち出しや情報の不適切利用による技術流出リスクの軽減は難しい。このため、実施段階の対策・工夫により、技術流出を防止することが重要となる
- 研究従事者が適切な情報管理を行うことができるよう、契約書だけではなく研究計画や実施規約を作成し、情報等の区分管理、情報等の持ち出し検知・追跡の仕組みの導入、違反時における対応の特明記等を行うことが必要

対応策の例

① 研究計画や実験規約の作成・確認

- 研究計画書・実験規約を作成し、データを取り扱う情報システムや試料やサンプル等を取り扱う施設・設備等に関する管理・利用指針、データや試料等の取扱手順等を明文化し、研究に参加する各研究者に署名させ、遵守を求める

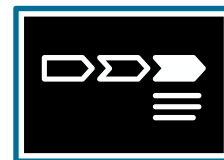
② 試料等の持ち出し時にアラートが鳴る仕組みの導入

- 相手方に提供した技術情報について、その形態（電子データか否か等）に応じて、物理的又は情報システムの的に区分して厳格に管理する。例えば、試料や専用装置に持ち出し検知タグやGPSトラッカーを取り付け、持ち出された場合にアラートが出る仕組みを導入することも考えられる
- デジタル情報については、自社デバイスの貸与や自社クラウドでの取扱いを求め、データに電子透かしやアクセス履歴が残るソフトを用いて、利用の証跡を残すことも一案である

③ 違反発覚時の対応の特明記

- 契約書上、研究計画に従って情報管理を行うことの義務付けや、違反時には共同研究の解除や損害賠償請求が可能であることを特明記する。その上で、これらの点について、研究参加者にも説明し、理解を得る

研究計画の作成・遵守



スケジュールの作成



遵守事項の特明確化

情報管理の特整備



区分管理の特徹底



自社クラウドの活用/
ログの追跡の特実施

3. ② 相手方への情報管理体制強化要請とモニタリングの実施

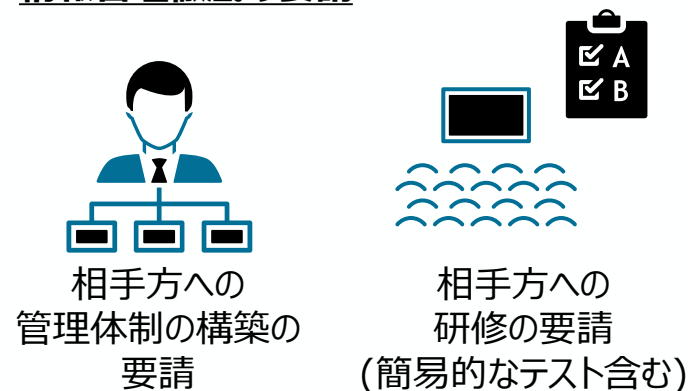
- 相手方の情報管理体制や意識が不十分な場合、**ヒューマンエラーによる技術流出に加え、第三者による情報窃取のリスクも高まる**
- このため相手方に対し、**厳格な情報管理体制の構築や従業員等への研修等を通じた意識啓発**を求めるとともに、必要に応じ、**モニタリング**を実施し、取組状況等の確認を行うことが重要である

対応策の例

① 契約締結時に求めた情報管理を徹底させる

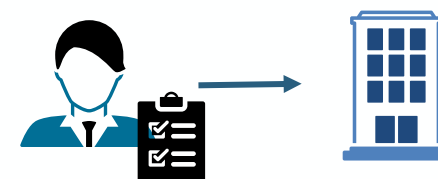
- 契約上、情報の取扱者を限定するとともに、情報の取扱区域の限定やアクセスの管理・制限等の情報の取扱いを明確化しておくことが重要である (p133参照)
- その上で、契約に基づき、実施段階における情報管理の徹底を求める。必要に応じて、相手方の研究メンバーに対する研修や説明会等の機会を用意し、情報管理の重要性・必要となる情報管理に関する説明のほか、定期的に簡易テストの実施を行う等の対策も有用である。その際、相手方の体制が不十分であったり、自社の是正要求が遵守されない場合等は、共同研究の停止もあり得ること、技術流出した場合には損害賠償請求を行う可能性があること等についても説明する

情報管理徹底の要請



② 情報管理状況についてモニタリングを実施する

- 契約上、モニタリング条項を規定した上で (p138参照)、技術情報が契約に従って適切に管理されているか、定期的にモニタリングやヒアリングを行うことが重要である
- 現地確認が難しい場合は、契約内容等が実際に履行されているか、書面報告を求める等の対応により、確認することが考えられる



モニタリングの実施

3. ③ 情報アクセス制限と物理的セキュリティ強化による漏えい防止

- 相手方が真摯に体制を構築していたとしても、**セキュリティの不備**がある場合、**技術情報が漏えい**するリスクは存在する
- これを防止するため、共同研究における**情報アクセス**や**持ち出し**を最小限に制限し、**権限の管理**や**監視体制**・**物理的セキュリティ**を強化することが重要である

対応策の例

① アクセスコントロールの実施

- 相手方に提供した技術情報が、相手方のサーバーや研究参加メンバーのデバイスに保存・管理されると、自社のコントロールを及ぼすことは困難となる。このため、必要に応じて、自社が管理権限を有するプラットフォーム上で情報を共有し、以下のような技術的な対策を講じることが有用
 - ✓ 必要最小限に絞った権限者のみがアクセス可能とする
 - ✓ 閲覧・編集・ダウンロード等の権限等を詳細に設定し、情報の拡散を防止する
 - ✓ 特に機微なデータは、専用の閲覧端末でのみ閲覧させる
 - ✓ アクセスログを常時監視し、異常な閲覧やダウンロード等があれば、即座に検知・遮断する仕組みを整備する

アクセス/情報持出の制限



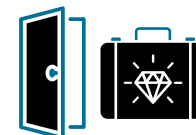
外部への持ち出しを技術的に遮断



異常なダウンロードや閲覧の通知

② 物理的なセキュリティの強化

- 新規設備が必要になる場合もあるためケースバイケースではあるが、自社が提供したサンプルや重要な技術が化体している装置等を用いた研究の場合は、相手方に建屋や専用の施設・設備での区分管理や立入者の限定・入退室ログ管理を求める。可能であれば、自社の厳重なセキュリティ環境下で研究することも考えられる



施設への立ち入りの制限

3. ④ 委託先・クラウド利用時の情報管理の徹底

- 技術情報の流出は、共同研究の相手方に限らず、**委託先を含む全関係者**から生じる可能性があることを認識する
- 委託等について、契約上の条件を課すことも重要であるが (p133参照)、オペレーションにおいても、**情報管理体制全体を可視化し**、不備があった際には**是正を促す**ことで、委託先等からの流出を防ぐことが重要である
- また、契約終了時には、**委託先を含め資料の返却・消去**を徹底し、**残存リスクを最小化**することも重要である

対応策の例

①委託の原則禁止と、事前承認時のDD

- 共同研究の過程で、業務の一部を相手方から第三者に委託するケースもあるが、委託先における情報管理をコントロールすることは困難であり、まず契約において、原則禁止や事前の書面承認を義務化することが重要 (p133参照)
- 承認するかどうかを判断する場合には、必要に応じて、相手方の協力を得て、委託先のパートナーDDを実施し (p120～参照)、技術流出リスクを評価することが重要となる

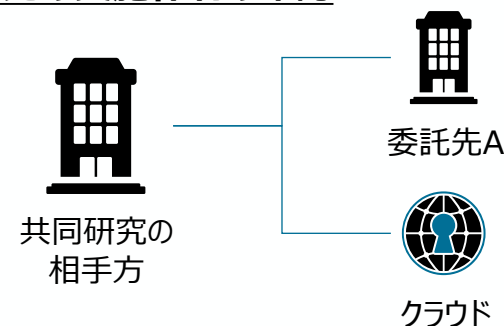
②委託先の情報管理体制の確認

- そもそも委託先に対しては、自社が共同研究の相手方に提供した情報を共有しない、又は取扱者を限定することが重要である。どうしても情報共有が必要な場合は、委託先のDD (管理体制の確認含む) の結果も踏まえて、共有する情報を厳に特定・限定することが重要となる
- 委託先に対しても、共同研究契約において相手方が負担している義務と同等の義務を課した上で、委託先における情報管理の状況 (クラウドの利用状況含む) について、必要に応じて、報告を求め、監査も実施する。万一不備があった際は、是正を促す

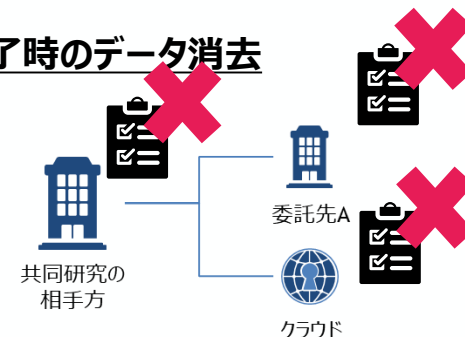
③契約終了時の資料やデータの返却・消去の徹底

- 契約終了時は、委託先も含めて資料やデータが返却・消去されたことを確認し、契約終了後の残存リスクを最小化する

委託先の実施体制の確認



契約終了時のデータ消去



3. ⑤ 堅牢なセキュリティ対策の導入や、外部ツールの利用制限の検討

- あわせて、研究に関するデータを厳重に保護するため、ネットワークや施設に**堅牢なセキュリティ対策**を講じることが重要である
- また、**外部の事業者が管理・提供するツールの利用**に当たっては、**安全性を検証**した上で、リスクに応じて、セキュアな環境の構築や、利用の制限を検討することが重要である

対応策の例

① 堅牢なセキュリティ対策を導入する

- 重要技術に関する研究データを扱うようなPCやネットワークには、堅牢なセキュリティ対策の導入を検討する。特に機密性の高いデータは暗号化しつつ、社外からアクセスできない閉域網やオフライン環境で管理することも有用である。
- 必要に応じて、共同研究者についても、多要素認証等により認証を厳格化することを検討する。
- 重要技術を取り扱っている施設への入退室管理を厳格化し、仮に部外者が立ち入る場合は、関連する情報の遮蔽措置等を講じることも有用。

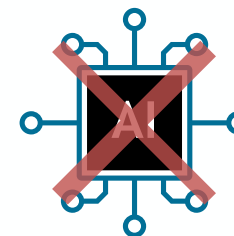
② 外部の事業者が管理・提供するツールの利用方法の制限を検討する

- 外部の事業者が管理・提供するツールについては、第三者への情報漏えいにつながるリスクがないか、安全性を評価することが重要である。リスクが高い場合には、機密性の高い研究においては、技術流出につながる利用を行わないことも考えられる。
- 他方で、研究において取り扱う技術情報の重要性等を踏まえつつ、契約においてデータの利用に制限をかける、利用に当たっての社内ルールを策定する（例えば、懸念のあるツールがあればネガティブリストを作成する）等の対策を講じた上で、可能な限りセキュアな環境を構築することも考えられる

堅牢なセキュリティ対策の導入



ネットワークやPC・データ等は
オフライン環境等の堅牢な環境で保護する



**流出につながるリスクがある外部ツール
については、利用を制限することも検討**

3. ⑥ セキュリティ担当者の配置とサイバー防御態勢の強化

- 特に重要性の高い技術情報を取り扱う共同研究では、高度なセキュリティ水準を確保すべきケースも存在する。**専門の担当者**の設置や、**プロジェクト単位**でセキュリティ管理を徹底することが有効である
- また、**最新の脅威への対策やフィッシング対策訓練等**を通じて、**サイバー防御態勢を強化**し、技術流出リスクを最小化することが重要である

対応策の例

①プロジェクト毎にセキュリティ担当者を配置し、管理を徹底する

- 特に重要性の高い技術情報を取り扱う共同研究では、プロジェクト毎にセキュリティ担当者を置き、情報管理体制を整備することも有効である。また、整備した管理体制を定期的に確認し、最新の脅威情報を共有するとともに、必要に応じて情報管理体制のブラッシュアップを図ることも重要である。
- 重要な技術情報については、データの暗号化や、アクセスログ等の常時監視を行い、漏えいした際に即時に状況を把握できるような対策も有用である。

②サイバー防御態勢の確認及び強化のために訓練を実施する

- 共同研究を実施する過程で技術情報の授受を行う場合に、情報共有のためのプラットフォームを用いるケースもある。そのようなケースでは、たとえば、共有リンクの有効期限やパスワードの設定等により、誤転送リスクを低減することも考えられる。
- 必要に応じて、定期的な脆弱性診断の実施や定期的なバックアップの実施等により、防御態勢の確認・強化を図ることも有用。また、研究従事者へのフィッシング対策訓練を実施することも有用。

専門のセキュリティ担当者の配置



専門担当者の配置による
体制等の確認



暗号化/
常時監視

サイバー防御態勢の構築/訓練の実施



共有リンクの
有効期限/パスワードの設定



バックアップ



訓練の実施

3. ⑦ 技術流出発生時のインシデント対応計画と対応体制の整備

- 万が一、技術流出が生じた場合には、**被害を最小限にすることが重要である。**
- このため、アクセスログの記録・確認等により、**技術流出が発生していないか把握できる体制を整えるとともに、インシデント発生時の計画をあらかじめ策定することで、技術流出の懸念が生じた際、速やかに対処できるようにすることが重要である**

対応策の例

① インシデント対応計画や適切な連絡・対応体制を整備する

- 自社プラットフォーム又は相手方システムにおいて、管理者がアクセス/送受信ログを確認し、不審ダウンロードや大量送信を監視する
- 漏えいが疑われる場合に、速やかに関係者に連絡し、被害拡大を防ぐ初動を取れるようにインシデント対応計画を整備する
- 技術流出のおそれが生じた場合に、相手方に速やかに報告を求め、適切な連絡・対応を講じることができる体制を整備する

状況の常時把握とインシデントへの対応



被害拡大を防ぐため、レポートラインや初動を含めた対応計画を双方で用意する



- インシデント（懸念含む）発生時の報告先
- 対応チェックリスト等

※技術が流出した場合には、被害を最小限に抑えるために、速やかな対応を講じることが重要となる。漏えい事案への対応については、前掲「秘密情報の保護ハンドブック～企業価値向上にむけて～」p147以降を参照されたい。

(<https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>)

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

4. ① 終了後のモニタリングと文書等の適切な管理

- 共同研究期間が終了した後も、**成果の独占・不正利用**や、**知的財産に係る紛争**が生じるリスクが存在する
- これを防ぐため、**研究終了後も定期的なモニタリングを実施**することが有用である。また、必要に応じて、**権利関係の明確化**を行うとともに、**訴訟等に備えて、文書や記録を適切に管理**することも重要である

対応策の例

① 研究終了後も相手方の動向をモニタリングする

- 知的財産権の帰属等について、契約上、どのように定めているかにもよるが（p134参照）、相手方が独自に特許出願や製品化等を行っていないか確認するため、成果報告会等の機会を利用して、定期的なコミュニケーションを継続することも有用である
- 相手方の特許出願状況や論文発表、プレスリリース等を定期的にチェックし、公開情報を通じて不正な利用等がないか確認することも重要である

事後のモニタリング



定期的な
コミュニケーション



相手方の動向の
注視

**権利帰属が明確でない成果は
速やかに再度協議**

② 不明確な成果帰属がある場合は、追加の合意形成を図る

- 原則として、成果の帰属については契約段階において事前に合意し、契約上も明確に定めておくべきだが（p134参照）、権利帰属が明確でない成果が生じた場合にも、速やかに協議を行い、合意形成を図ることが重要である
 - ✓ 「xxについて、特許出願は共同で行い、権利は共有する」
 - ✓ 「第三者にライセンスする場合は、相手方と事前協議する」等



訴訟時に備え、平時からエビデンスを蓄積



実験ノート



実験データ

③ 適切に記録管理等を行う

- 相手方が成果を不正に利用する場合もあり得るため、訴訟等に備え、日頃からエビデンスとなる文書や記録（実験ノート、データ等）を適切に管理することも重要である

4. ② 技術情報やサンプルの返還・廃棄の徹底

- 共同研究中に提供した技術情報が、研究終了後も相手方に残存すると、**不正利用**や**情報流出のリスク**が高まる。このため、**提供した情報の返還・消去**や、**データのアクセス権の解除**を確実に実施することが重要である
- また、サンプルを提供している場合には、確実に**期限内の返還**を求めることも重要である

対応策の例

① 共同研究終了時の技術情報等の返還・消去を徹底する

- まずは、共同研究契約等において、契約終了後のデータ等の返却・廃棄等を義務付けることが重要である（p141参照）。
- その上で、共同研究終了時には、相手方任せにするのではなく、技術情報等の返却・廃棄を明確に求めることが重要である。特に、廃棄を求める場合には、廃棄証明書の提出を求めることも有用である
- 共同研究中の情報のやり取りについて、情報共有プラットフォームを活用している場合は、その閉鎖や、相手方に付与したアクセス権の解除等を実施することが重要である

② 提供したサンプルの返還を徹底する

- 共同研究の過程で相手方にサンプルを提供した場合は、研究終了後の不正利用を防止するため、契約に定めた上で（p141参照）、期限を設けて確実な返還を求めることが重要である
- サンプルの内容や形状等にもよるが、契約に違反するようなリバースエンジニアリングがなされていないかを確認するため、返還時の状態を確認・記録しておくことも重要である

研究終了時の技術情報の返還・消去

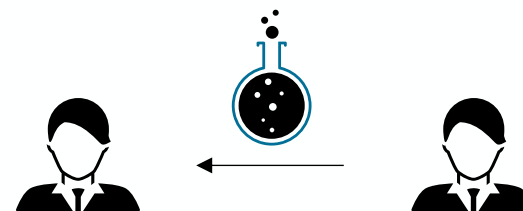


データの消去/処分



情報共有プラットフォームの
閉鎖・アクセス権消去

提供したサンプルの確実な返還



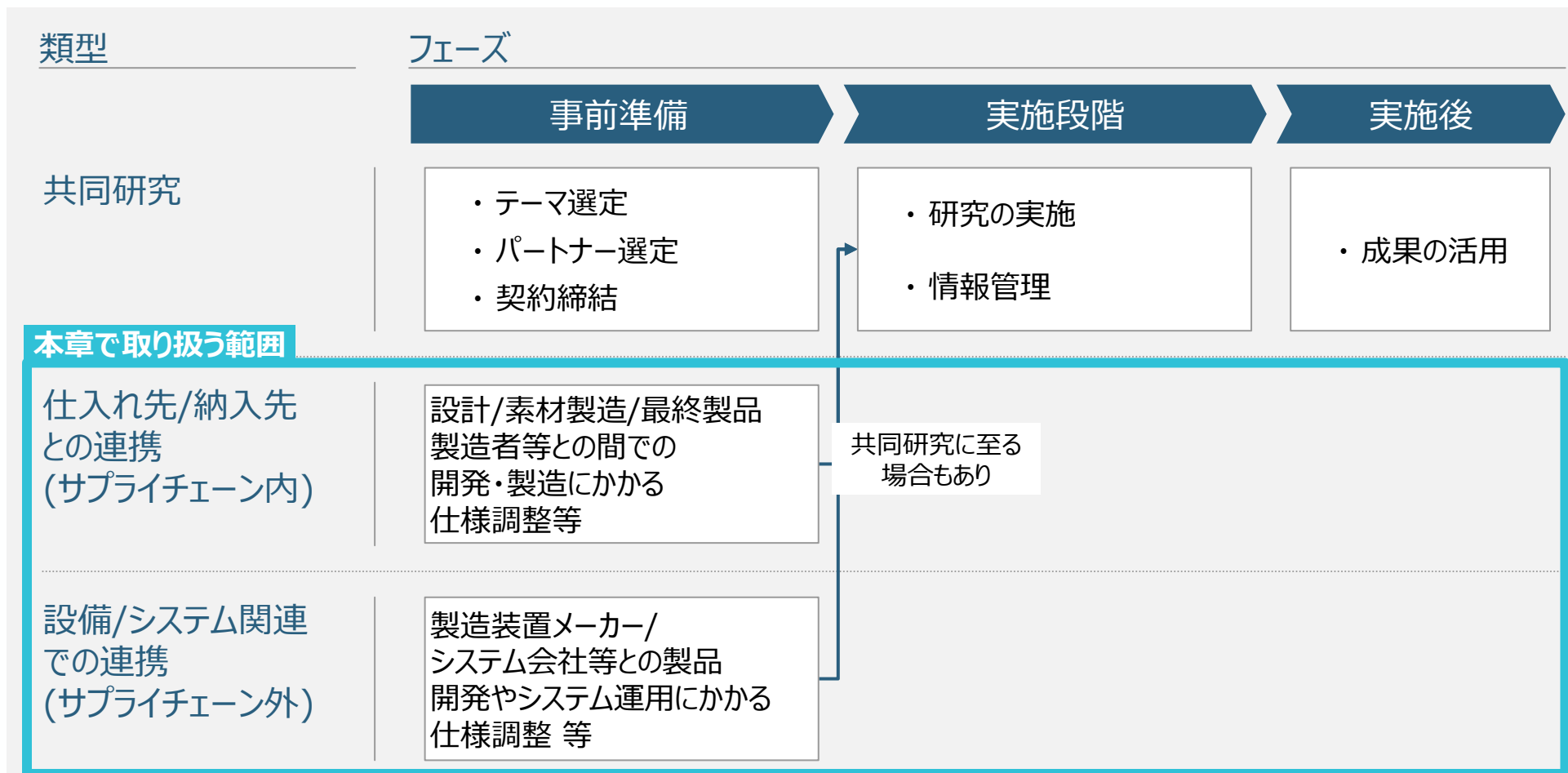
期間内の返還の要請
(返却物の確認)

第5章

すり合わせに伴う技術流出への対策

本章で取り扱う範囲

- 他者との連携において技術流出リスクが想定される事例のうち、本章では、②**サプライチェーンの中でのすり合わせ**と、③**サプライチェーンの外でのすり合わせのリスクと対策**を取り扱う

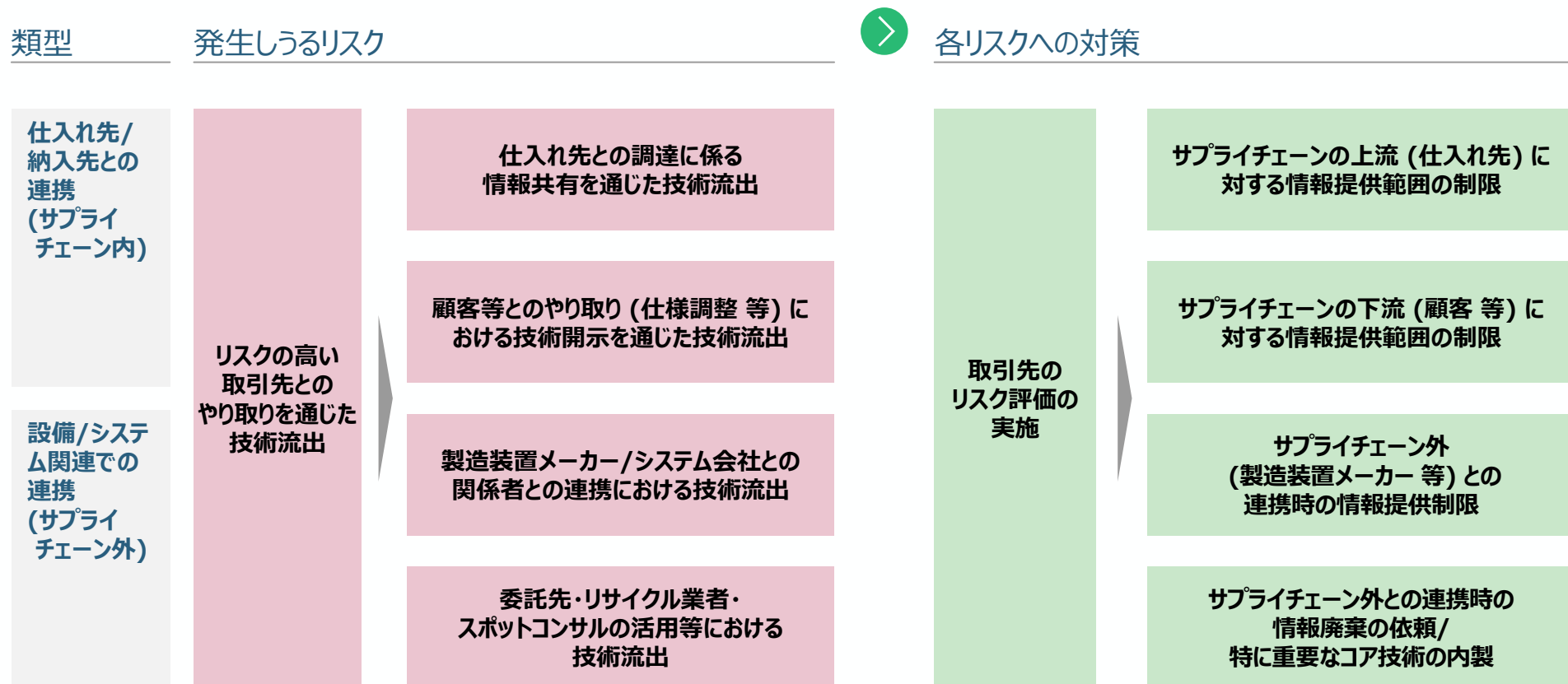


「すり合わせに伴う技術流出への対策」に関する基本的認識

- **製品性能や品質最大化には、個々の部品調達に関わる組織間での最適化に向けた相互調整（いわゆる「すり合わせ」）が極めて重要**
 - これは、伝統的に企業とサプライヤーの緊密な連携によって他国には真似が出来ない品質を生み出してきた我が国製造業の「お家芸」の分野（※）
 - （※）「すり合わせ」の対局の概念として、標準化によって、外部の生産機能を水平分業させ、コストを大幅に下げる「組み合わせ」がある。細かい技術に関するやりとりが無い分、参入障壁が低く、標準品の大量生産に向けた手法といわれている
- **「すり合わせ」は、必ずしも長年にわたり緊密な関係を築いてきた企業に限られず、グローバルにその対象が拡大。更に、国が経済安全保障の観点で、市場アクセスを人質にしつつ、自律性、すなわち現地企業からの調達比率を高める要請で競っている分野も見受けられる**
- **我が国企業も当該国での市場アクセスの確保のため、この要請に応じ「すり合わせ」の対象を外国企業（現地企業）に広げざるを得ないことも考えられる**
- **このようにサプライチェーンのパートナーの多様化は不可避の一方、「すり合わせ」においては、営業秘密を含め、さまざまな技術情報の共有が行われることから、技術流出のリスクが高い**
 - 例えば、すり合わせで共有された技術情報を使って自社の技術力を高めたり、製造する部品のラインナップを拡大する等の行為が行われるリスクがある
- **このため、共同研究と同様、パートナーや「すり合わせ」の内容等に応じ、適切なリスク軽減措置を組み合わせしていくというマネジメントが必要である**

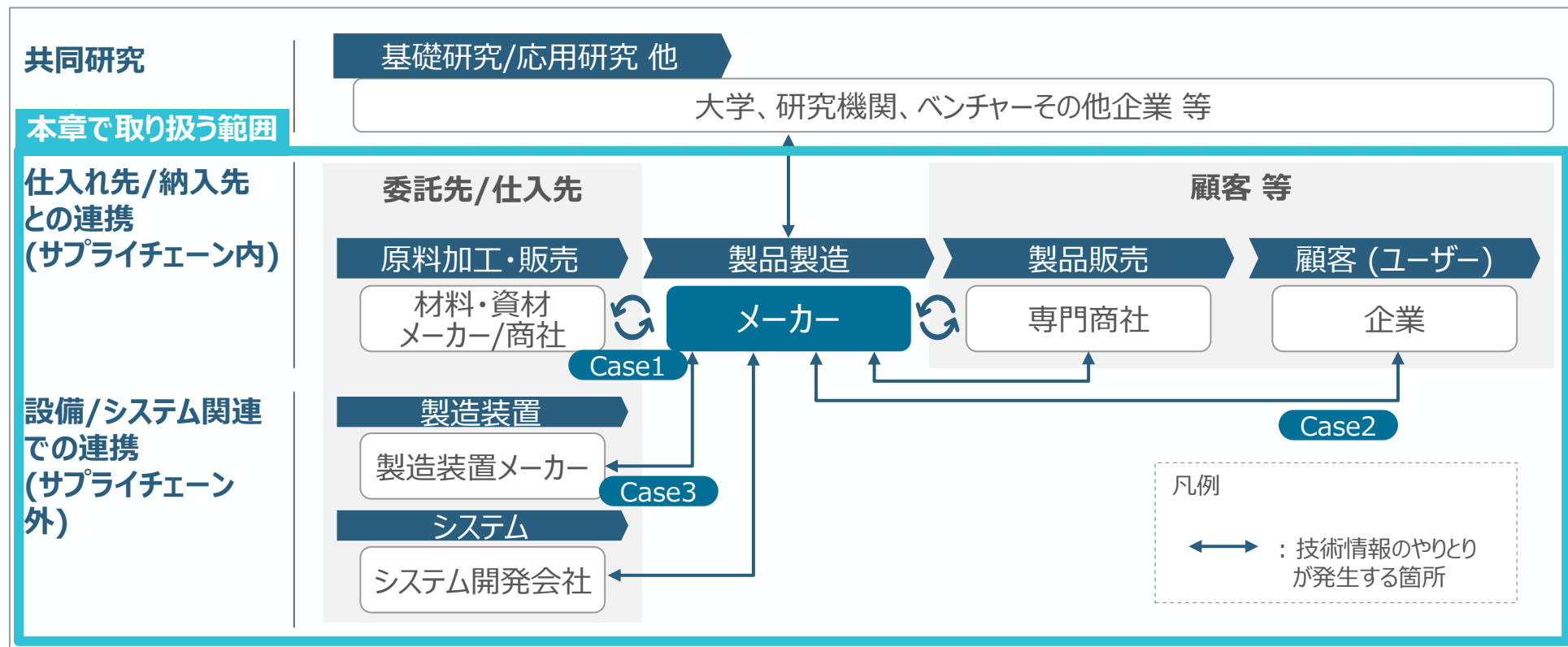
すり合わせに伴う技術流出リスクとその対策の全体像

- 企業が保有する技術は、サプライチェーンの中（仕入れ先（上流）や顧客（下流）等）や、サプライチェーンの外（製造装置メーカー等）とのすり合わせ等の場面でも流出するリスクがある
- このため、まずは取引先のリスクを評価した上で、各相手方に対し、**情報提供を制限する等、対策を講じていく必要がある**



企業をとりまく想定される技術流出の経路（メーカーの場合）

- 企業の保有技術は、先述の「共同研究」に加え、サプライチェーンの中（仕入れ先や顧客等）や、サプライチェーンの外（製造装置メーカー等）とのすり合わせでも流出するリスクがある



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

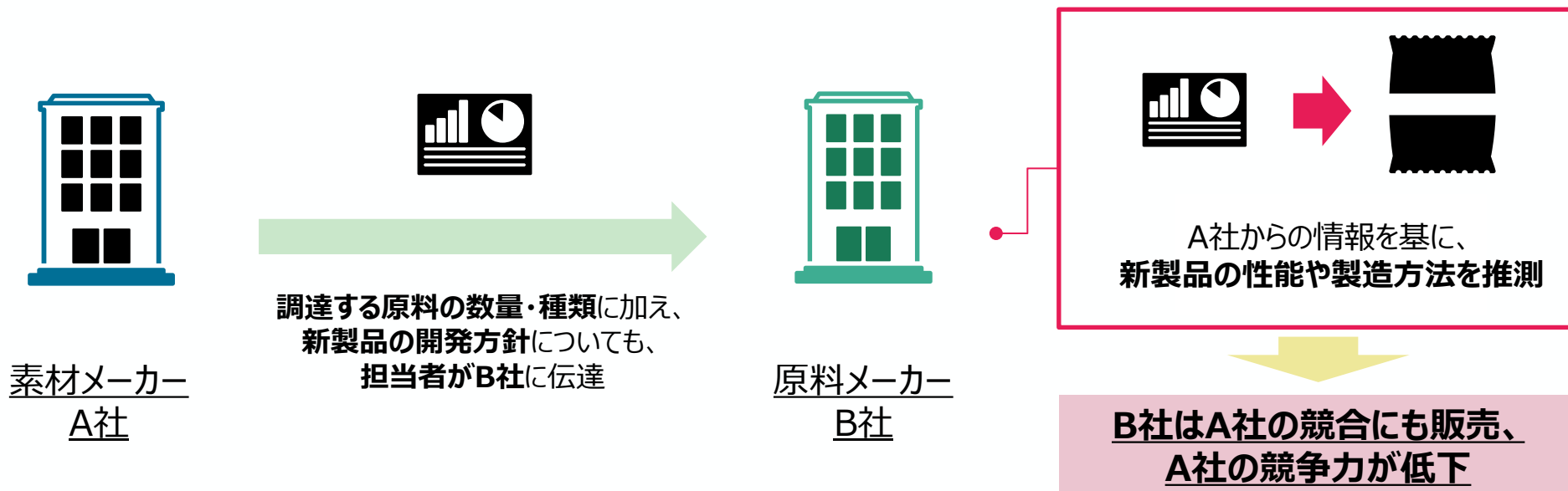
第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

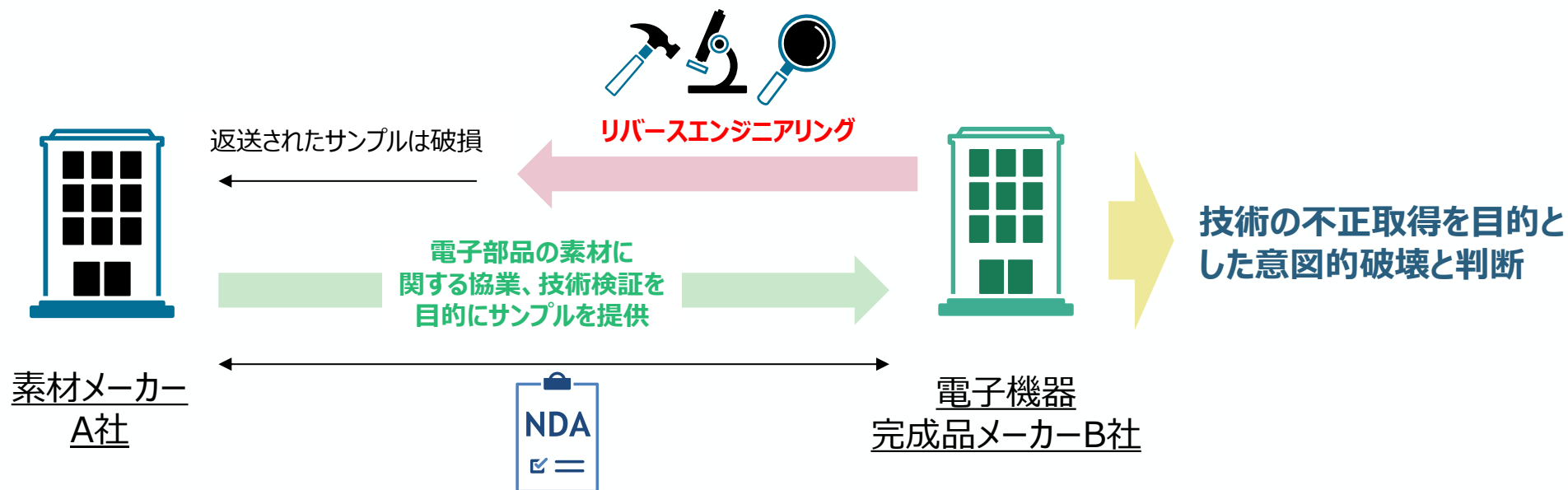
Case1: 原料メーカー（仕入れ先）からの技術流出

- 日本の素材メーカーA社は、部素材の性能向上に向けた開発に際し、当該部素材の原料の国内唯一の供給元であるメーカーB社に対して原料を発注。その際、A社の担当者が、**自社の新製品の開発方針を必要以上にB社担当者に明らかにした。**
- B社はこの情報を基に、**A社新製品の性能や製造方法を推測**。自社の原料を販売する際、この情報をA社の複数の競合他社にも提示し、販路を拡大した。
- A社はその後、**競合他社が自社と同様の新製品を投入していることを認識**。しかし、B社からの情報漏えいを立証するための確たる証拠がなく、**法的責任を追及することができなかった。**



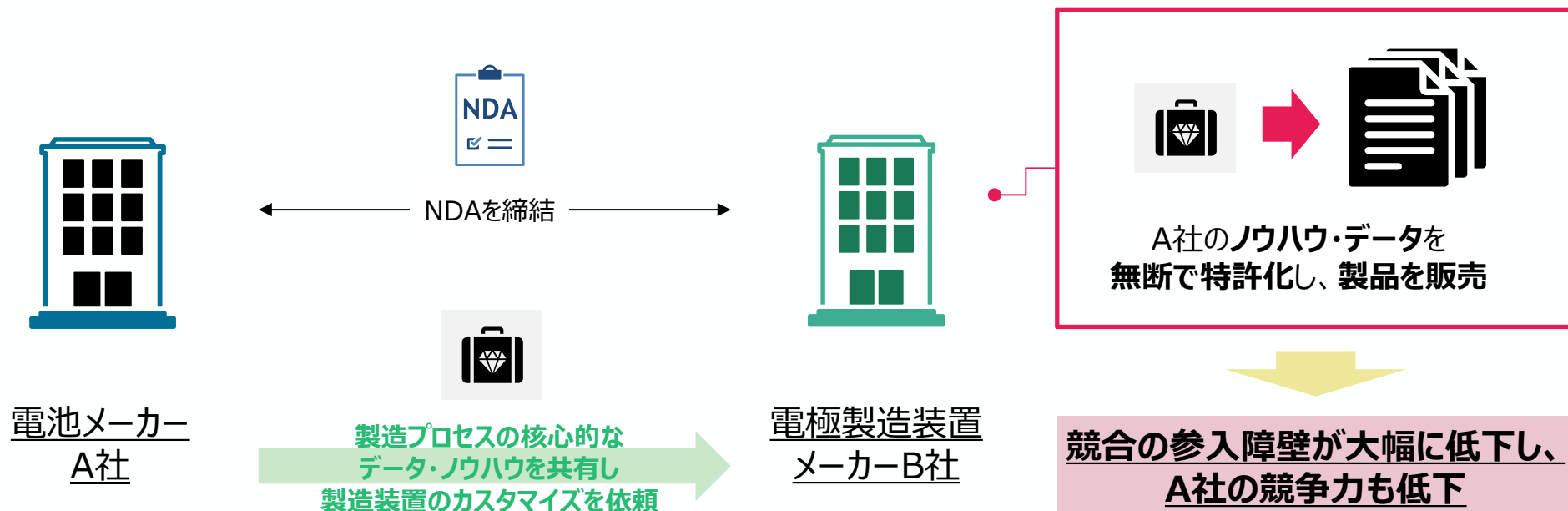
Case2: 顧客へのサンプル提供の際の技術流出

- **素材メーカーA社**は、自社の先端的な部素材技術を、**海外の電子機器完成品メーカーのB社**にライセンス提供することも視野に、NDAを締結したうえで、**サンプルを送付した**。
- B社に送付したサンプルは、**返却期日をはるかに超過したのち、破損・欠損した状態**で返却。
- A社は、B社が**リバースエンジニアリング**を目的として意図的に破壊したと判断。
- A社はこの出来事により、**製品技術や商業機会の喪失が生じ得ると懸念し、事件後、政府機関との連携を強化し、自社の情報セキュリティ体制や知財戦略を見直した**。



Case3: 製造装置メーカーからの技術流出

- 電池メーカーA社は、電極製造装置メーカーB社とNDAを締結した上で、製造プロセスの核心的なデータ・ノウハウをB社に対して共有し、電極量産装置のカスタマイズを依頼、B社は同装置を開発し、A社に対して納入した。
- これに留まらず、B社は、A社から提供されたデータ・ノウハウを目的外に使用し、独自に特許を出願、A社の競合他社に対して販売した。
- A社は、B社による特許出願に伴う公開によって、ノウハウによる事業優位性を喪失し、競合の参入障壁が大幅に低下、自社の競争力も大幅に低下した。



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

1. ① 取引先のリスク評価を行う

- 技術情報の提供を伴うような取引先については、通常、提供した技術情報が当該取引先において管理されることとなるから、あらかじめ、通常行われる信用状況の評価だけでなく、**技術流出リスクの観点から評価**を行う
- 特に、新規の取引先については、会社の事業内容や経営状況、役員構成等の一般的に入手可能な情報収集に加え、可能であれば、トップの人柄や業界内でのレピュテーションや他企業との取引実績、他の企業との間で技術の取扱いをめぐる訴訟の状況等を確認する。また、重要な技術情報の提供を伴う重要取引先については、日頃から定期的に確認することも重要である
- その上で、当該企業が自社の重要技術の獲得に関心があると思われる場合や、情報管理体制等に不十分な点がある場合等、**リスクが高いと思われる場合には、取引を回避する、あるいは取引内容を見直す**等の対応を行う
- もっとも、例えばM&A取引におけるDDとは異なり、あくまで自社の技術情報の流出防止が目的であること、リスクに応じて濃淡をつけなければ対象となる取引数が膨大になる可能性があること等に鑑みて、すり合わせの過程で提供する**技術情報の重要性・機微性（p15参照）**や、**相手方の特性（業種、上場/非上場、国内/海外等）**を考慮の上、**コスト等も踏まえて確認項目を調整する必要がある**

対応策の例

- 本取組の前提として、サプライチェーン戦略において、生産のリードタイムやコスト削減といった観点に加えて、技術提供の有無・可能性や、提供技術の重要性（p15参照）を考慮することも検討する
- その上で、取引の内容（単なる売買に留まるか等）や提供可能性のある技術情報の重要性を吟味し、必要に応じたリスク評価を行う。リスク評価の実施において収集する情報例としては、以下が考えられる。その他、取引類型が異なるため、そのまま適用することが適当ではないものの、必要に応じて、共同研究におけるパートナーDDの項目（p122～）も参照されたい
 - **事業内容**：類似の事業があり、自社に技術優位性がある場合、技術獲得される可能性
 - **経営状況**：経営状況が芳しくない場合、自社の競合他社に買収される可能性や、短期的な利益獲得を目的とした技術の不正な取得が行われる可能性
 - **トップの人柄/意識等**：会社のトップ（社長）の人柄や考え方、契約遵守意識によって、技術流出リスクが高くなる可能性
 - **役員構成**：外国政府等による情報活動への協力義務を課せられている役員がいる場合、他国に技術を移転される可能性
 - **レピュテーション・訴訟状況**：過去に技術の取扱いに問題のあった企業については、適切な再発防止策が講じられていない限り、同様の問題が発生する可能性

1. ② 取引開始前の情報提供の範囲の限定

- 取引に入る前の商談や設備等の導入を検討する段階において、フィージビリティスタディーの観点から、自社の技術情報を一定程度提供するケースがある
- あらかじめ、NDAを締結した上で、自社における情報管理のランク付け等を踏まえつつ、提供範囲を明確化し、必要最低限の情報しか提供しないことが重要である

対応策の例

① NDAの締結

- 新規取引に向けた商談等において、技術情報を提供する可能性があるのであれば、あらかじめNDAを締結した上で、技術情報を提供することが必要である

事前のNDA締結



② 提供可能な範囲の限定・明確化

- 商談や設備等の導入検討におけるコミュニケーションの過程で、うっかり重要な技術情報を口頭説明又は開示してしまうケースが少なくない
- あらかじめ、社内において、取引先のリスク評価の結果等も踏まえつつ、取引開始前に提供可能な技術情報の範囲を明確にしておくことが重要である。また、提供する技術情報についても、固有名詞のコードネーム化や不必要な部分に関するブラックボックス化等の対策も検討する
- さらに、明確化した提供範囲を、実際に商談等に出席する担当者に対しても説明することも重要である

コードネーム化のイメージ



従業員

ここで扱っている原材料は「001」です



本当は「A」という原材料

③ 段階的な技術提供

- 取引開始前においても、信頼関係の構築を見極めながら必要な情報を開示するという対応が考えられる

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

2. ① 秘密保持義務・情報の取扱方法等の規定

- 日常的に行われる「すり合わせ」について、その都度契約が締結されるケースは少なく、取引先との間で締結された取引基本契約によって規律されるケースが多い。当該基本契約の名称等（売買基本契約等）にとられることなく、相互調整のために技術情報の授受が行われる可能性があるのであれば、**秘密保持義務を規定することが重要**である

対応策の例

① 秘密保持義務の規定

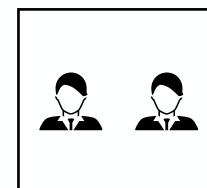
- すり合わせを伴う取引に係る基本契約はケースバイケースであるが（売買基本契約、加工委託基本契約等）、仕様調整やカスタマイズといった相互の調整に伴い、自社から取引先に対して技術情報を提供する可能性があるのであれば、必要に応じて、基本契約に以下のような秘密保持義務を定めることが重要である

目的外利用の禁止／第三者への提供禁止／複製の禁止／情報返却・破棄等

- また、重要な技術情報を提供する場合には、必要に応じて、個別にNDAを締結することも重要である。特に、自社において営業秘密として管理している技術情報（p22参照）を共有する場合には、秘密管理性の有無が法人（具体的には管理単位）ごとに判断されることも踏まえて、営業秘密を特定したNDAの締結等により、自社の秘密管理意思を明確に示すことが重要である（営業秘密を企業内外で共有する場合の秘密管理性の考え方については、経済産業省「営業秘密管理指針」を参照）

※経済産業省「営業秘密管理指針」参照 (<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>)

秘密保持義務



第三者への提供禁止
承諾なき委託の禁止



義務の設定

秘密保持、
目的外利用禁止

② 情報の取扱方法の明確化

- 仕様調整やカスタマイズといった相互の調整に伴い、取引先が業務委託を行うケースもありうる。技術の重要性を踏まえつつ、業務委託先を把握するための条項を盛り込むことも重要である。例えば、事前承認や事前通知等を求めることがありうる

2. ② 資本変動等に備えた解除事由等の設定

- 取引先の業績悪化や破綻、資本構成の変化等の契約後の事情変更により、技術流出リスクが高まる可能性がある
- 取引の内容や提供する可能性のある技術情報の重要性等を踏まえたケースバイケースの判断が重要となるが、相手方の資本構成が大きく変動する場合等について、**事前に把握する手段とその対応策を明確化**することも検討する

対応策の例

①事前承諾・通知事項・解除事由として規定

- 取引の内容や提供する技術情報の重要性等によっては、合併や事業譲渡、経営権の変動を伴う株式移転等について、事前承諾又は事前通知を求めることも有用である
- その上で、懸念のある主体が、新たな株主になること等により、技術情報にアクセスする可能性が生じる場合には、契約を解除することができるよう、解除事由として定めることも考えられる
- また、取引内容等にもよるが、資本構成の変更等に限らず、以下のような技術流出リスクに影響を与える重要な事項の変動については、解除事由等として規定することが考えられる
 - ✓ 経営状況の悪化
 - ✓ 外国での多額の研究費の申請
 - ✓ 制裁リスト等への追加 等

解除事由として想定される主な事項

資本構成（支配者）の変更

経営状況の悪化



外国での多額の研究費の申請



②解除後のデータ返却等の規定・実行

- 契約を解除するだけでは技術流出リスクは軽減できないため、相手側に提供したデータやサンプルの返却や破棄に関する条項を盛り込むとともに、確実に実行することも重要

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

3. ① サプライチェーンの上流（仕入れ先）に対する情報提供範囲の制限

- サプライチェーンにおける上流（原料・素材等の仕入れ先）と調達等についてやり取りする際、その情報から、自社の製品開発の方針や技術情報が推測されるリスクがある。これを回避するため、仕入れ先に提供する情報は、可能な限り限定する
- また、仕入れ先に提供する情報が営業秘密に該当する場合や、営業秘密が推測される可能性がある場合には、技術情報を提供する前にNDAを締結する等、情報の保護措置を検討する
- 他国からの要請等を背景に、不合理な情報開示が求められた場合には、安易に応じず、経済産業省への相談も検討する

対応策の例

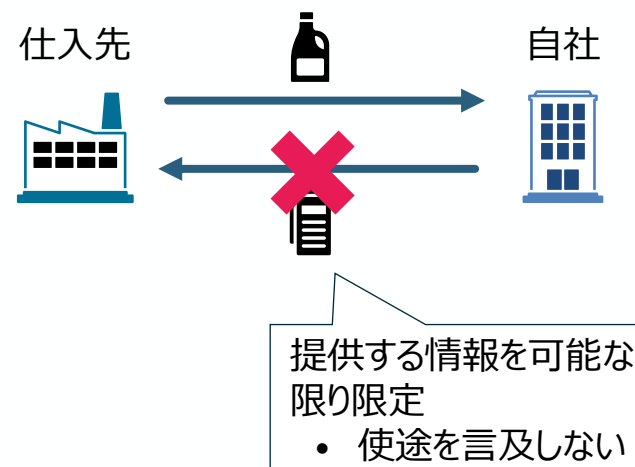
①仕入れ先等に対して提供する情報の限定

- 自社の事業に必要な原料・素材等を調達する際、自社から一定の技術情報を提供するケースもあるが、必要以上の情報を提供すると、自社技術に関する情報や関心、自社の製品開発の方向性を相手方に推測され、競争に流用されるリスクがある。このため、提供する情報を、可能な限り必要最低限の範囲に限定することが重要である（どれを提供し、提供しないか、事前に明確にする）
- その際、相手方の他の取引先（他国の競合企業の有無等）や、事業規模等を踏まえたリスクに応じ、提供する情報の範囲を限定する。また、調達する原料・素材等の具体的な用途については、言及しないことも重要である
- なお、情報を受領する仕入れ等の立場からも、必要以上の情報を受領してしまうと、漏えいリスク・管理コストが生じるため、かかる対応は重要となる

②外国政府等からの要請に基づく情報開示要求に適切に対応する

- 原材料の仕入れ先等から、外国政府からの要請等を背景に、技術やサプライチェーンに関する情報の開示を求められた場合は、その要求の合理性を確認する。不当な内容と思われる場合には、安易に応じず、経済産業省への相談も検討する

仕入れ先に対する提供情報の限定



3. ② サプライチェーンの下流（顧客等）に対する情報提供範囲の制限

- 上流と同様に、**下流（顧客等）**に対しても、**仕様調整の場面等**において技術等の情報を開示するケースがあるが、意図しない技術流出リスクに備えるため、**情報提供の範囲を限定**することが重要
- また、リバースエンジニアリングによる技術流出を防ぐため、コア技術が含まれる部分については**ブラックボックス化**を検討する。営業秘密を提供せざるを得ない場合には、必要に応じてNDAを締結する等の秘密管理も重要

対応策の例

①顧客に対しても、自社から提供する情報を限定する

- 顧客は相対的に立場が強いことが多いが、情報開示を求められた場合も含め、できる限り情報を提供しないよう努める。追加的に技術情報を提供せざるを得ない場合や改善等のためにある程度共有が必要な場合も、提供する情報を選別し、また、説明・表現を工夫するとともに、ノウハウや製造条件等は秘匿し、固有名詞はコード化する。また、サンプルを提供した場合は、回収を徹底することも重要
- こうした対策を行うに当たって、あらかじめ、提供可能な範囲でも、技術情報の粒度に応じたランク分けを行っておくことが有用である。その際、営業担当者任せにせず、提供する技術情報の内容や粒度について、事前に社内で整理することが重要
- また、顧客からの要望で工程監査を受け入れる際、事前に可否を検討し、更に具体的な内容を事前に取り決めるよう徹底する

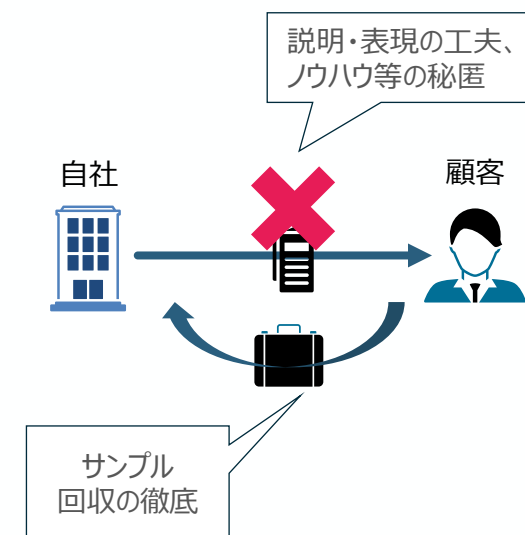
②提供情報に関する秘密管理の徹底

- 情報提供が必要な場合も、個別にNDAを締結し、相手方に秘密情報であることが分かる表示をすることが必要。可能なら監査・訪問等により契約遵守状況を確認する
- また、海外法人とのすり合わせの際は、自社の現地法人の社員に厳格なアクセスコントロールを実施することが重要（本社出向者への限定等）

③外国政府等からの要請に基づく情報開示要求に適切に対応する

- 原材料の仕入れ先等から、外国政府からの要請等を背景に、技術やサプライチェーンに関する情報の開示を求められた場合は、その要求の合理性を確認する。不当な内容と思われる場合には、安易に応じず、経済産業省への相談も検討する

顧客に対する情報提供の実施



第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

4. ① サプライチェーン外（製造装置メーカー等）との連携時の情報提供制限

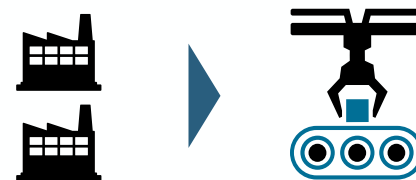
- 製造装置メーカーやシステム会社等、サプライチェーンの外の関係者と連携する際にも、仕様調整や発注等を通じて提供した技術情報が、意図せず流出するリスクがある
- このため、契約において**秘密保持条項**を設けることに加え、**提供する情報の限定**や**調達先の分散**等の対策を行うことが重要である。また、**重要なコア技術が製造装置等に化体するケースでは、内製することも検討する。**

対応策の例

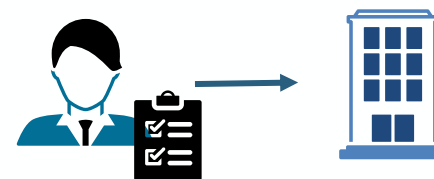
① 装置メーカー等の外部企業等へ提供する情報の限定

- 自社開発方針やノウハウの流出を防ぐために、仕様調整等の際に提供する情報を必要最低限の範囲で限定したり、調達を分散することが考えられる（一社に依存せず可能な限り複数から部品を調達し、個々の部品の用途が分からないようにする等）
- 装置を使用するに当たり、改造やカスタマイズが必要となる場合には、極力自社で改造等を行い、操業条件の漏えいを防ぐことが重要。修理やメンテナンスのためにメーカーに出す際は、購入時のカタログスペックに戻すことも重要
- 仮に自社の情報を提供する際は、これを開示する範囲（従業員、受託事業者等）と責任の所在を明確にする

一か所に情報が集中しないよう、出す情報を限定し、分散調達を行う



カスタマイズを含む製造委託を実施する際は、秘密保持義務を盛り込みつつ、情報提供を工夫



(段階的な情報提供/モニタリングの実施)

② カスタマイズ含めた製造委託を実施する際の留意点

- 契約に秘密保持条項を盛り込むとともに、例えば以下のとおり、自社からの情報提供を工夫する
 - ✓ 段階的な技術提供の実施
 - ✓ 情報セキュリティ体制構築の依頼、現地モニタリング
 - ✓ 装置納品後の情報破棄の確実な実施 等

③ 極めて重要なコア技術については内製する

- 競争力に特に大きな影響を与える重要なコア技術が、製造装置やそのカスタマイズ等に化体するケースも存在する。コスト等も踏まえた判断が必要となるが、重要性等に応じて、内製することも検討する。

4. ② サプライチェーン外との連携時における情報管理状況の確認

- 取引先に対し、可能であれば**情報管理に関する第三者認証の取得を促す**等、情報管理がしっかりと行われていることを確認する
- また、**サプライチェーン外においては、リサイクル業者やコンサルなど様々な取引先が関係することとなるが、技術情報の提供・開示を伴う取引については、提供・開示する事項を限定することが重要である。**

対応策の例

① 情報管理の実施状況を確認する

- サプライチェーン外との連携に限られないが、取引先に対して、情報管理者の選任、情報の取扱いに関する社内規程の有無、社内研修の実施状況、漏えい発生時の対応等の情報管理体制の状況を確認し、適切な体制の構築を依頼することも重要である
- こうした情報管理に関する取組事項を満たしているか確認する場合、第三者認証制度（例えば、技術情報管理認証制度（TICS）等）を活用し、取引先に認証の取得を促すことも検討する

② 取引内容に応じて、提供・開示する事項を限定する

- 外部のリサイクル事業者等に委託して技術情報を処分するケースもあるが、情報の重要性等を考慮して、委託の可否を判断する。また、廃棄時の記録保存や、場合によっては立ち会い等を検討することも有用。
- 企業がコンサルサービスを利用して様々なアドバイスを受けるケースがあるが、その過程で自社の技術情報を提供する場合には、その必要性を吟味して、提供・開示する情報の範囲に留意する。

技術情報管理認証制度

【制度概要】



※技術情報管理認証制度（TICS）は、産業競争力強化法に基づき政府が運用する制度。企業は認証機関の指導・助言を受けつつ、対策に取り組み、その状況が客観的に審査・認証される。詳細は経済産業省HP (https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/) を参照。

第0章 はじめに

- 1 本ガイドランスの目的等
- 2 技術流出の経路と本ガイドランスの構成

第1章 各章で共通する技術流出対策

- 1 組織体制の構築・リスクマネジメント
- 2 重点的に守るべき技術の特定・評価

第2章 生産拠点の海外進出に伴う技術流出への対策

- 0 技術流出事例
- 1 計画前・計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 海外事業の実施段階において取り組むべき事項
- 4 撤退・契約終了時に取り組むべき事項
- 5 その他の取組事項

第3章 人を通じた技術流出への対策

- 0 技術流出事例
- 1 技術流出を防ぐために未然に取り組むべき事項
- 2 技術流出した場合に取り組むべき事項
- 3 技術者の流出に対して取り組むべき事項

第4章 共同研究に伴う技術流出への対策

- 0 技術流出事例
- 1 計画段階において取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 共同研究の実施段階において取り組むべき事項
- 4 研究終了時に取り組むべき事項

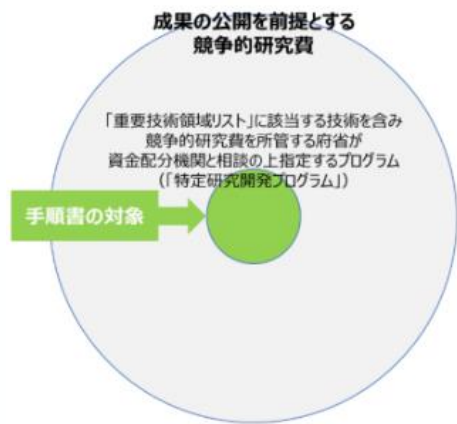
第5章 すり合わせに伴う技術流出への対策

- 0 技術流出事例
- 1 取引開始前に取り組むべき事項
- 2 契約締結時に取り組むべき事項
- 3 サプライチェーンの中との連携において取り組むべき事項
- 4 サプライチェーンの外との連携において取り組むべき事項

(参考) 研究セキュリティの確保に関する取組のための手順書について

(参考) 研究セキュリティの確保に関する取組のための手順書について

- 研究セキュリティと研究インテグリティの確保に関する有識者会議は、研究セキュリティの確保に関する取組を構築するため、2025年12月に「**研究セキュリティの確保に関する取組のための手順書**」を取りまとめている（以下「**手順書**」という）
※ 詳細について、内閣府HP (<https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha.html>) 参照
- **手順書の対象は、①研究成果の公開を前提とする競争的研究費のうち、②「重要技術領域リスト」に該当する技術を含む可能性があるものであって、③経済安全保障の観点から特に技術流出の防止が必要であるとして、当該競争的研究費を所管する府省が資金配分機関と相談の上で指定する研究開発プログラム（以下「特定研究開発プログラム」という）**であり、政府、資金配分機関、研究機関及び研究者が実施すべきリスクマネジメントとして、「最低限実施すべき措置」と「実施することが望ましい措置」を示している
- このため、**企業が研究代表機関又は共同研究機関となる場合**においても、特定研究開発プログラムに応募する際に**手順書が求めるリスクマネジメントの実施が必要**となる。手順書は、大学や研究機関等を念頭に置いて策定されているため、研究機関が企業である場合におけるリスクマネジメントの実施に当たっては、**必要に応じて、本ガイダンスの内容を参照されたい**
- もっとも、本ガイダンスは、生産拠点の海外進出等のビジネスも取り上げているほか、手順書が示す「最低限実施すべき措置」や「実施することが望ましい措置」を超えた対応策も記載しているため、**手順書の適用を受ける企業が、本ガイダンスの記載事項を全て遵守することまでは必要でない**
- そこで、企業の便宜のために、**手順書の要求事項について、関連する本ガイダンスの箇所を示す**。なお、手順書の適用を受ける企業においては、手順書の内容を確認されたい



研究セキュリティ

国家及び経済の安全を脅かすリスクから研究活動を守るため、研究機関や研究者に求める認識や行動。国や研究機関において守るべきと判断した研究活動を対象とする
(補足説明) 国家又は経済安全保障を害する研究開発成果等の不当利用、重要技術の流出、研究インテグリティの毀損等のリスクから研究活動を保護すること

リスクマネジメント

研究セキュリティを確保するため、組織として、重要技術が流出する等のリスクを確認・評価し、必要に応じて、事案発生時における損失・毀損等を抑制するために必要なリスク軽減措置をあらかじめ実施すること。リスクマネジメントには、リスク確認とリスク評価（デュー・ディリジェンスを含む）、リスク軽減措置及びフォローアップの一連の活動が含まれる

(参考) 研究セキュリティの確保に関する取組のための手順書について

<手順書が求めるリスクマネジメント>

3-1 日常的に実施する取組

(1) 所属研究者の研究活動に関する情報の収集

研究機関は、研究インテグリティのチェックリストに基づき研究者から申告される情報を収集することが必要である。また、所属研究者の論文投稿、雑誌等への掲載、出版物など研究成果に関する情報及び発明・特許等の知的財産に関する情報を収集することが望ましい。

(2) 情報管理体制の整備

研究機関は、所属研究者が特定研究開発プログラムに応募する場合又はその予定がある場合は、適切にリスクマネジメントを実施できるよう、リスクマネジメントに必要な情報を管理する体制を整備することが必要である。その際、研究インテグリティのチェックリストに基づき研究者から申告された情報に加え、特定研究開発プログラムへの応募に当たり必要な情報などリスクマネジメントに関する情報を、関係部署が連携して収集し、それらを一元的に管理する体制を整備することが望ましい。

(3) データ等の管理に関する情報の収集

研究機関は、以下の①から③に掲げる情報を収集することが望ましい。

- ①「公的資金による研究データの管理・利活用に関する基本的な考え方」（令和3年12月17日統合イノベーション戦略推進会議）に基づき作成されたデータマネジメントプラン（以下「DMP」という。）に関する情報
- ②当該研究機関における情報システムの管理に関する情報
- ③当該研究機関における各種施設・設備等の管理に関する情報

(4) その他の取組

研究機関は、研究インテグリティのチェックリストについて、その運用状況等を踏まえ見直すことが必要である。また、所属研究者が特定研究開発プログラムに応募する又はその予定がある場合は、所属研究者等に対して、研究セキュリティの確保に関する研修受講を奨励することが望ましい。

3-2 特定研究開発プログラムへの応募における取組

研究機関は、所属研究者が特定研究開発プログラムに応募する場合、資金配分機関が公募要領で定める期限までに、本手順書に基づくリスクマネジメントを実施することが必要となる。そのため、研究機関は、特定研究開発プログラムへの応募時において、リスクマネジメントの実施体制の整備に向けて準備することが望ましい。その際、以下の①から③までに掲げる事項に留意することが考えられる。

- ①特定研究開発プログラムの運営に関与する者の指名
- ②特定研究開発プログラムの運営に関与する者による守秘義務の遵守の徹底
- ③重要技術の流出などの緊急事態が発生した場合の連絡・対応に係る体制の整備

● 研究者から申告される情報（p182参照）は、**外国の機関等との連携・契約・物品提供等に関する事項**であり、企業で勤務する**従業員にとっては副業・兼業に当たるケース**も多いため、**第3章「1. ⑥副業等を通じた情報流出の防止」を参照**

● 技術流出対策に必要な情報の収集・管理を行うための体制整備については、**第1章「1. ①経営層によるリーダーシップとアクション」・「1. ②司令塔となる部署の設置」を参照**

● 研究過程におけるデータの取得・管理・活用等の情報管理に関する計画書やルールについては、**第4章「3. ①研究計画等における情報の利用・管理ルールの明確化」を参照**

● 運用状況等を踏まえた情報管理の見直しについては、**第3章「1. ②情報管理状況の監査と重要プロジェクトの配置等への反映」を参照**

● ①・②については個別のプログラムごとに様々であるが、③については、**日常的な取組の一環として第1章「1. ②司令塔となる部署の設置」を参照**

(参考) 研究セキュリティの確保に関する取組のための手順書について

<手順書が求めるリスクマネジメント>

3-3 資金配分機関が公募要領で定める期限までに実施する取組 (リスク確認・リスク評価)

(1) 研究代表機関が実施するリスク確認・リスク評価

(i) PI、研究代表機関に所属する研究参画者及び Co-PI について

研究代表機関は、PI、当該研究代表機関に所属する研究参画者及び Co-PI について、以下の①から⑬までに掲げる事項に関する情報（③から⑬まで、⑩及び⑪に関する情報は、応募する日の属する年度を含めた過去3年分とする。）を自己申告させた上で確認し、デュー・デiligenceを実施することが必要である。研究代表機関は、デュー・デiligenceの結果を踏まえ、適宜、資金配分機関と相談・調整しつつ、実施するリスク軽減措置の内容を検討することが必要である。デュー・デiligenceは、自己申告による情報、ソースの情報など各研究代表機関が通常把握し得る情報を用いて実施することとするが、必要な情報が得られない等の理由により十分な実施が困難な者については、必要に応じてリスク軽減措置を実施することが望ましい。

- ①学歴（必要に応じて指導教官等の情報を含む。）
- ②研究経歴・職歴
- ③研究費の取得歴
- ④研究費以外の支援等の取得歴
- ⑤発表論文における筆頭著者、責任著者及び共著者
- ⑥特許の出願状況（共同発明者及び共同出願人の情報を含む。）
- ⑦外国の人材採用プログラムへの参加歴
- ⑧指針に基づく処分歴
- ⑨リストへの掲載の有無
- ⑩リスト掲載機関への所属の有無
- ⑪リスト掲載機関に所属する研究者との関係（共同研究・受託研究の実施、共著論文の執筆・公表及び学会等における連名の口頭発表の実績をいう。）の有無
- ⑫安全保障貿易管理における「非居住者」（一時帰国しその滞在期間が6月未満の日本人等）又は「特定類型」（日本の大学の教授であり外国の大学と雇用契約を締結し教授職を兼職している者、外国政府から留学資金を得ている留学生、外国の人材採用プログラムに参加し多額の研究資金や生活費の提供を受けている研究者等）への該当性
- ⑬その他資金配分機関がデュー・デiligenceの実施に当たり必要と認める事項

(ii) 特定研究開発プログラムにより行う研究に関するデータ等の管理について

研究代表機関は、以下の①から④までに掲げる事項の適切性を確認することが望ましい。

- ①特定研究開発プログラムにより行う研究に関する DMP
- ②特定研究開発プログラムにより行う研究の過程で発生する電磁的な形態により管理できないもの（試料等）の管理方針
- ③特定研究開発プログラムにより行う研究において使用される情報システム（PI が管理するものを含む。）の管理方針
- ④特定研究開発プログラムにより行う研究において使用される施設・設備等（建屋、居室、実験室、実験装置等）の管理方針

- 研究に従事する従業員のリスク確認等については、**第4章「1. ② 共同研究に従事する役職員の決定」**を参照
- また、共同研究先の研究者のDDについては、**第4章「1. ⑥ パートナー候補のDDの徹底（関与する個人の観点）」**を参照

- 研究過程におけるデータの取得・管理・活用等の情報管理に関する計画書やルールについては、**第4章「3. ① 研究計画等における情報の利用・管理ルールの明確化」**を参照

<手順書が求めるリスクマネジメント>

3-3 資金配分機関が公募要領で定める期限までに実施する取組 (リスク確認・リスク評価)

(1) 研究代表機関が実施するリスク確認・リスク評価

(iii) 共同研究機関について

研究代表機関は、共同研究機関（我が国の大学、大学共同利用機関、高等専門学校、国立研究開発法人及び公設試験研究機関以外の機関に限る。）について、以下の①から④までに掲げる事項に関する情報を自己申告させた上で確認し、デュー・ディリジェンスを実施することが望ましい。

- ①共同研究を行う目的
- ②共同研究の対象分野における実績（応募する日の属する年度を含めた過去3年分）
- ③財務状況、（共同研究機関が企業である場合は）資本構成
- ④リストへの掲載の有無

(iv) 特定研究開発プログラムにより行う研究に対して支援を行う個人・機関について

研究代表機関は、特定研究開発プログラムにより行う研究に対して助成、寄附、物品の提供等の支援を行う個人・機関（国、地方公共団体など公的機関を除く。以下「支援者」という。）について、以下の①から⑤までに掲げる事項に関する情報を確認し、デュー・ディリジェンスを実施することが望ましい。


- ①支援の内容
- ②支援の目的及び支援の条件
- ③財務状況、（支援者が企業である場合は）資本構成
- ④リストへの掲載の有無
- ⑤（支援者が個人である場合は）リスト掲載機関への所属の有無

(v) その他

研究代表機関は、共同研究機関その他個人・機関との間で締結する共同研究契約その他契約・協定について、協力の内容、研究データ等へのアクセス、発明・特許等の知的財産の取扱い及び守秘義務の内容の適切性を確認することが必要である。

- 
- 共同研究先のDDについては、第4章「1. ⑤ パートナー候補のDDの徹底（組織）」を参照

- 
- 共同研究先のDDについては、第4章「1. ⑤ パートナー候補のDDの徹底（組織）」を参照

- 
- 共同研究契約について確認すべき事項については、第4章「2. 契約締結時に取り組むべき事項」の各項目を参照

(参考) 研究セキュリティの確保に関する取組のための手順書について

3-3 資金配分機関が公募要領で定める期限までに実施する取組（リスク確認・リスク評価）

(2) 共同研究機関が実施するリスク確認・リスク評価

(i) Co-PI 及び共同研究機関に所属する研究参画者について

共同研究機関は、Co-PI 及び当該共同研究機関に所属する研究参画者について、上記(1)(i)に掲げる事項に関する情報を自己申告させた上で確認し、デュー・デシリジェンスを実施することが必要である。デュー・デシリジェンスは、自己申告による情報、ソースの情報など各共同研究機関が通常把握し得る情報を用いて実施することとするが、必要な情報が得られない等の理由により十分な実施が困難な者については、必要に応じてリスク軽減措置を実施することが望ましい。

(ii) 特定研究開発プログラムにより行う研究に関するデータ等の管理について

共同研究機関は、上記(1)(ii)に掲げる事項(1)(ii)③において「PI」とあるのは、「Co-PI」と読み替えるものとする。)の適切性を確認することが望ましい。

(iii) その他

共同研究機関は、研究代表機関その他個人・機関との間で締結する共同研究契約その他契約・協定について、協力の内容、研究データ等へのアクセス、発明・特許等の知的財産の取扱い及び守秘義務の内容の適切性を確認することが必要である。

3-4 リスク軽減措置

研究機関は、リスク確認・リスク評価の結果を踏まえ、リスク軽減措置を実施することが必要であり、また、資金配分機関から追加的なリスク軽減措置の実施を要請された場合は、適切に対応することが必要である。研究機関が実施するリスク軽減措置は、以下に例示するものが考えられるところであり、リスクの程度に応じた合理的な措置であれば足りる。

- ・施設・設備へのアクセス権限の管理
- ・オフキャンパス等の研究場所の確保
- ・取り扱う情報の機微性に応じたミーティング等への参加者の考慮
- ・(研究参画者が学生の場合などにおいて)雇用契約を締結することによるガバナンスの強化
- ・研修の受講による研究セキュリティに関するリテラシーの向上・研究データ等の情報へのアクセス権限の管理
- ・サイバー攻撃への対策の強化

- 研究に従事する者のリスク確認等については、**第4章「1. ② 共同研究に従事する役職員の決定」**を参照

- 研究過程におけるデータの取得・管理・活用等の情報管理に関する計画書やルールについては、**第4章「3. ① 研究計画等における情報の利用・管理ルールの明確化」**を参照

- 共同研究契約について確認すべき事項については、**第4章「2. 契約締結時に取り組むべき事項」**の各項目を参照

- 共同研究契約におけるリスク軽減措置については、**第4章「2. 契約締結時に取り組むべき事項」**及び**「5. 共同研究の実施段階において取り組むべき事項」**の各項目を参照


3-5 特定研究開発プログラムにより行う研究の開始後の取組（フォローアップ）

研究機関は、特定研究開発プログラムにより行う研究の開始後、適宜、リスク軽減措置の実施状況等を確認し、その結果を踏まえた取組を実施することが必要である。

特定研究開発プログラムにより行う研究の進展に応じ、研究参画者を追加する場合は、当該研究参画者についてデュー・ディリジェンスを実施する必要がある。研究参画者を新規に採用する場合は、採用に係る公募の段階で、候補者からデュー・ディリジェンスに用いる情報を収集することが望ましい。

研究者から申告された情報に誤りが発覚した場合は、研究機関はその旨を速やかに資金配分機関に報告するとともに、修正された情報に基づき、改めてデュー・ディリジェンスを実施することが必要である。

また、特定研究開発プログラムにより行う研究の実施を通じて蓄積されるリスクマネジメントに関する知見や経験を踏まえたヒヤリハット事例・好事例については、関係行政機関、資金配分機関等の求めに応じて提供することが望ましい。

- 
- いずれの取組についても、基本的には適宜実施状況を確認することが重要である。例えば、**自社における研究であれば、第3章「1. ② 情報管理状況の監査と重要プロジェクトの配置等への反映」を、共同研究の場合には第4章「3. ② 相手方への情報管理体制強化要請とモニタリングの実施」を参照**

研究者向け

研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト(雛形)

1. 全般的な事項

- 外国の機関・大学等との共同研究や交流等（資金、施設・設備・機器等の物品、人材の受け入れを含む。）に伴う、利益相反・責務相反が適切に管理されないリスク、技術流出・情報流出につながるリスク、信頼の低下リスク（※）等のリスク（以下単に「リスク」という。）に留意するとともに、リスクが懸念される場合には所属機関の担当部署に相談等をしていますか？

※ 例えば、研究公募への応募において、研究者が、海外では制限が講じられている外国機関との共同研究の情報を提出しなかったことにより、虚偽記載や利益相反を疑われるような事態になり、本人の信頼が低下するリスク

- 研究活動の透明性の確保に係る情報（職歴・研究経歴、現在の全ての所属機関・役職（兼業や、外国の人材登用プログラムへの参加、雇用契約のない名誉教授等を含む。）、外部機関から受けている各種の支援）について、所属機関の規程等に基づき、担当部署に適切な報告等を行っていますか？

2. 外国の機関・大学等との連携・契約や、外国からの報酬・物品の提供に係る手続きに関する事項

- 外国の機関・大学等との連携・契約において覚書（Memorandum of Understanding: MOU）等の書面を交わす際、所属機関の規程等に基づき担当部署に確認や判断を求めるなど、適切な手続きを経ていますか？

✓ 書面を提示していますか？

✓ 連携・契約における自らの機関及び相手方の参加メンバーの情報を提示していますか？

- 外国の機関・大学等から補助金や助成金・報酬（※）・物品の提供を受ける際、所属機関に報告等を行っていますか？また、上述のリスクが懸念されるようになった場合に、所属機関の担当部署に相談等をしていますか？

※ 報酬：奨励金、兼務の給与、賞金、贈答品、寄附金、出張費、講演料、執筆料等

- 外国の機関・大学等と長期間にわたって連携・契約している場合、相手方の参加メンバーや共同で行う研究内容に変化がないかを確認し、実質的な変更があった場合に所属機関の担当部署に報告等していますか？また、上述のリスクが懸念されるようになった場合に、所属機関の担当部署に相談等をしていますか？

- 外国の機関・大学等との書面を交わさない連携や報酬・物品の提供の無い連携を行う場合であっても、リスクがあり得ることを認識していますか？また、リスクが懸念されるようになった場合に、所属機関の担当部署に相談等をしていますか？

- 特定の外国に長期の出張や高頻度な出張を行う場合、必要に応じて所属機関の担当部署に報告等していますか？また、リスクが懸念されるようになった場合に、所属機関の担当部署に相談等をしていますか？

- 外国の機関・大学等と共同で行う研究の過程において、我が国の安全保障や経済・社会に悪影響を及ぼす等の共同研究の目的外使用をされるリスクがあり得ることに留意し、技術情報を提供する際の事前確認や技術情報の管理を適切に行っていますか？また、当該リスクが懸念されるようになった場合に、所属機関の担当部署に相談等をしていますか？

3. 外国の機関・大学等との連携・契約の相手方に関する事項

- 外国の機関・大学等と連携・契約する場合、その組織や相手方の参加メンバーについての情報、連携・契約の目的を確認していますか？

研究者向け「研究の国際化、オープン化に伴う新たなリスクに対するチェックリスト(雛形)」(令和3年12月17日版)

<https://www8.cao.go.jp/cstp/kokusaiteki/integrity/checklist1.pdf>