

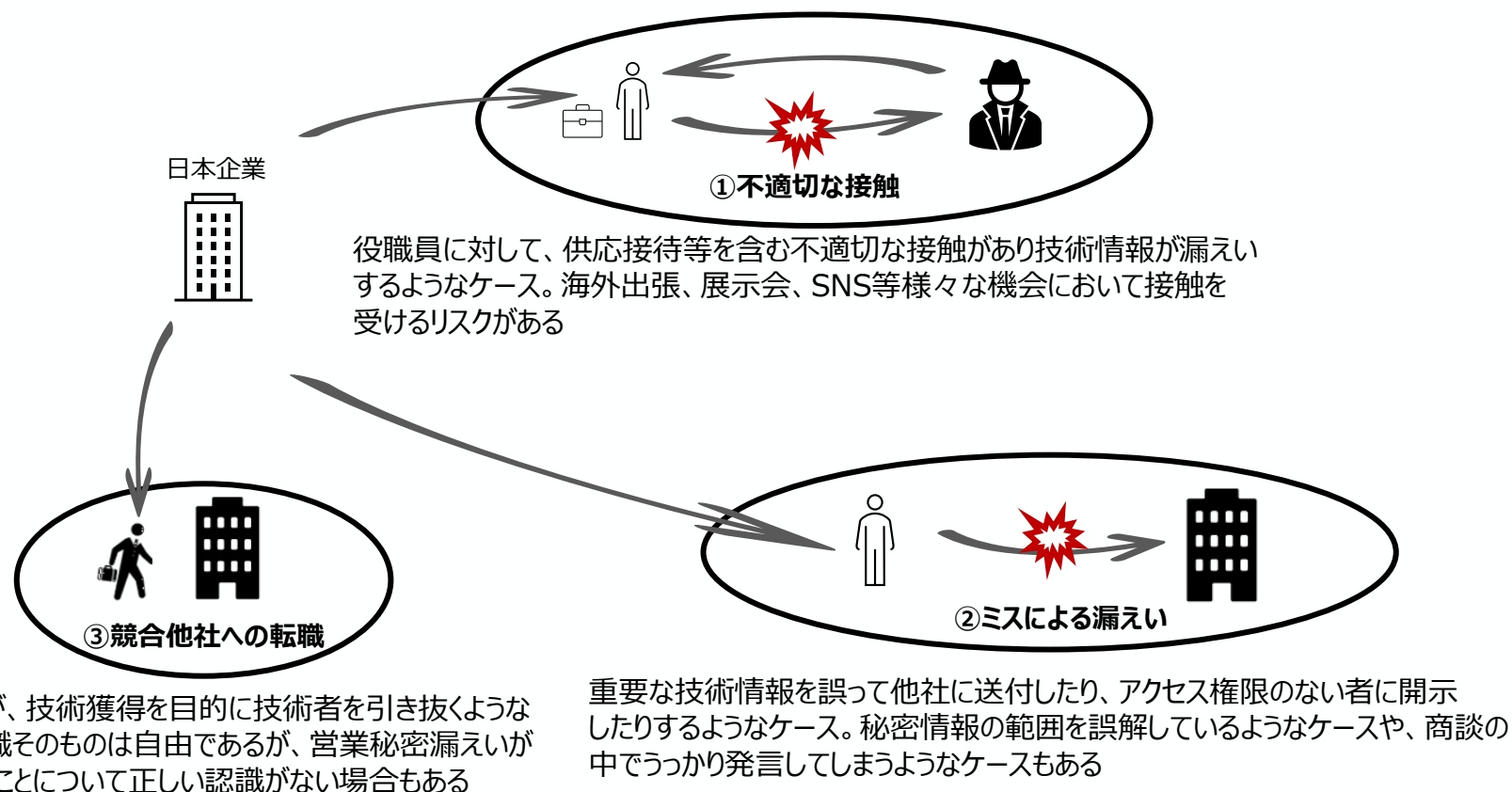
第3章

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

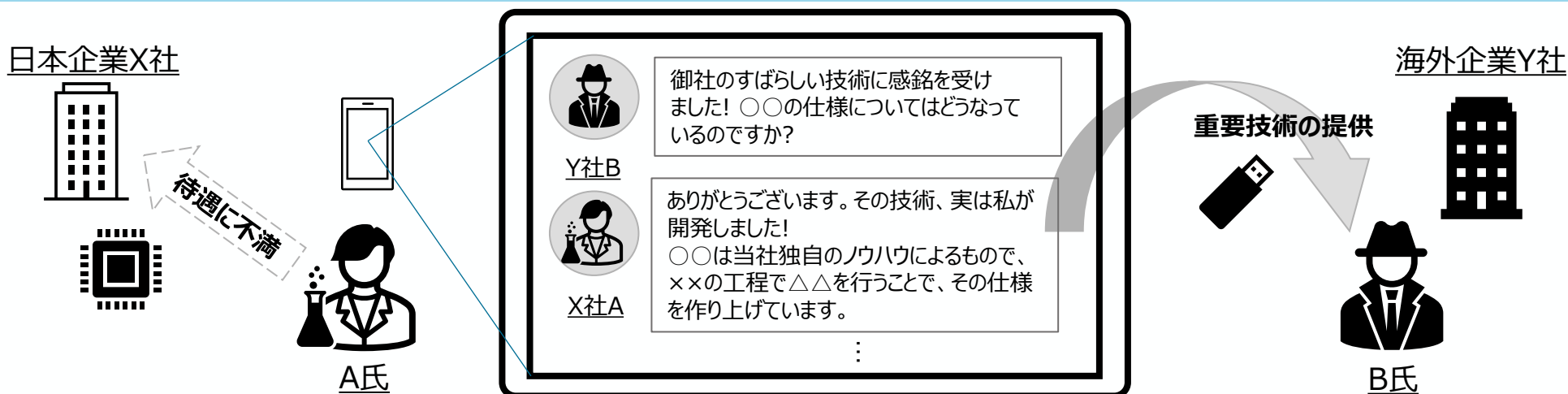
第5章 すり合わせに伴う技術流出への対策

- 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

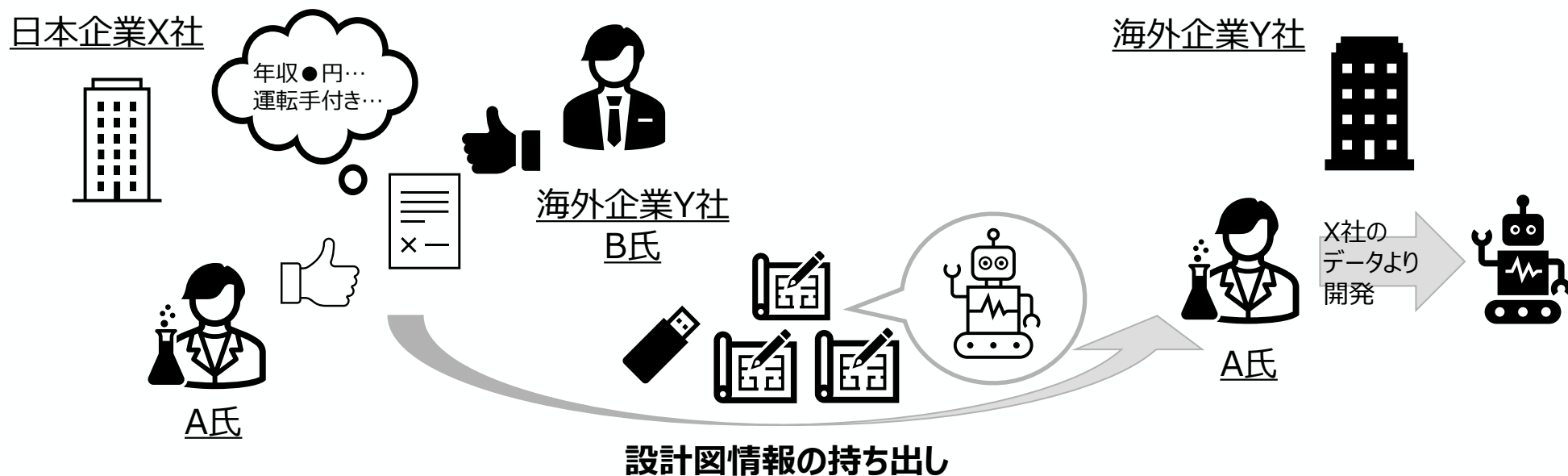
Case1: SNSでのやりとりを通じた技術流出

- 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



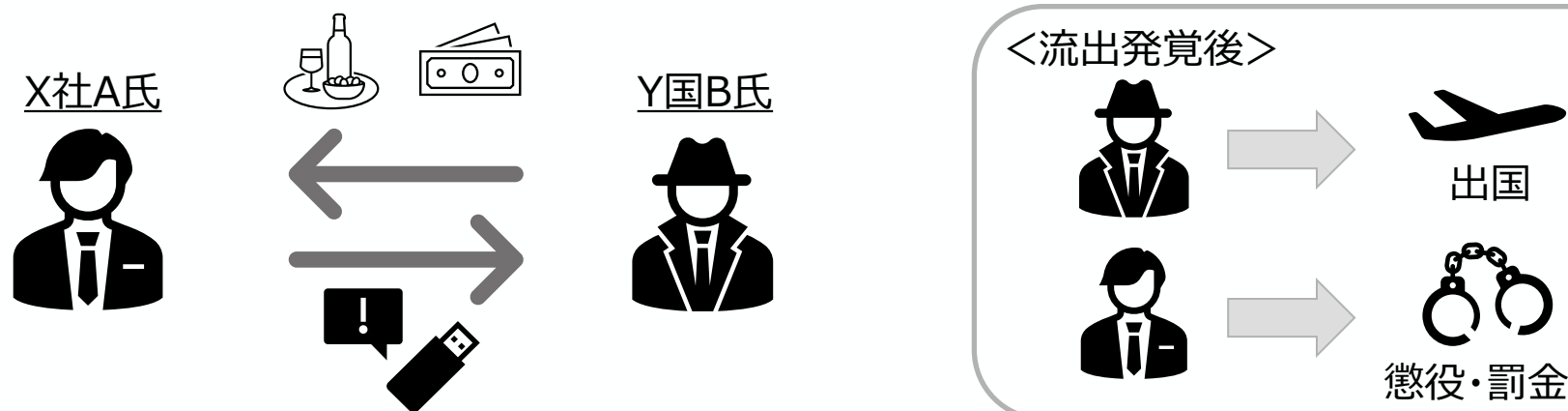
Case2: 役員の転職を契機とする技術流出

- 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

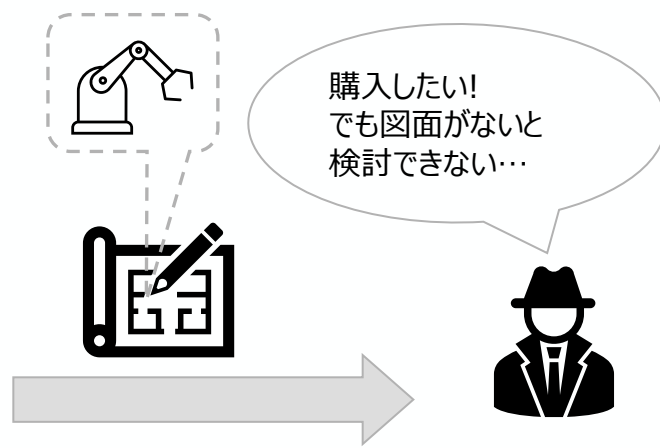
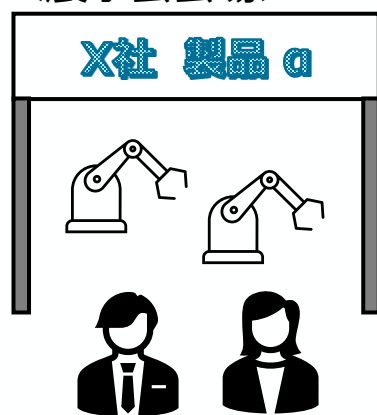
- **日本企業X社の社員A氏**が、レストランで食事をしていたところ、隣のテーブルにいた**Y国政府機関の職員B氏**に話しかけられた。日本のビジネス事情にも詳しいB氏との会話は弾み、その後も頻繁に会うようになった
- 親しくなって数ヶ月がたった頃、**B氏がX社の重要プロジェクトについて関心を示し、A氏に関連する情報を求めてきた**。求められた情報は公開情報であったため、A氏は気軽に情報を提供した
- B氏の要求は**次第にエスカレートし、X社の重要な技術情報の提供を求められた**。A氏はプロジェクトを監督する立場であり、当該情報を容易に入手することができた。それまでに**食事や金品を受け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



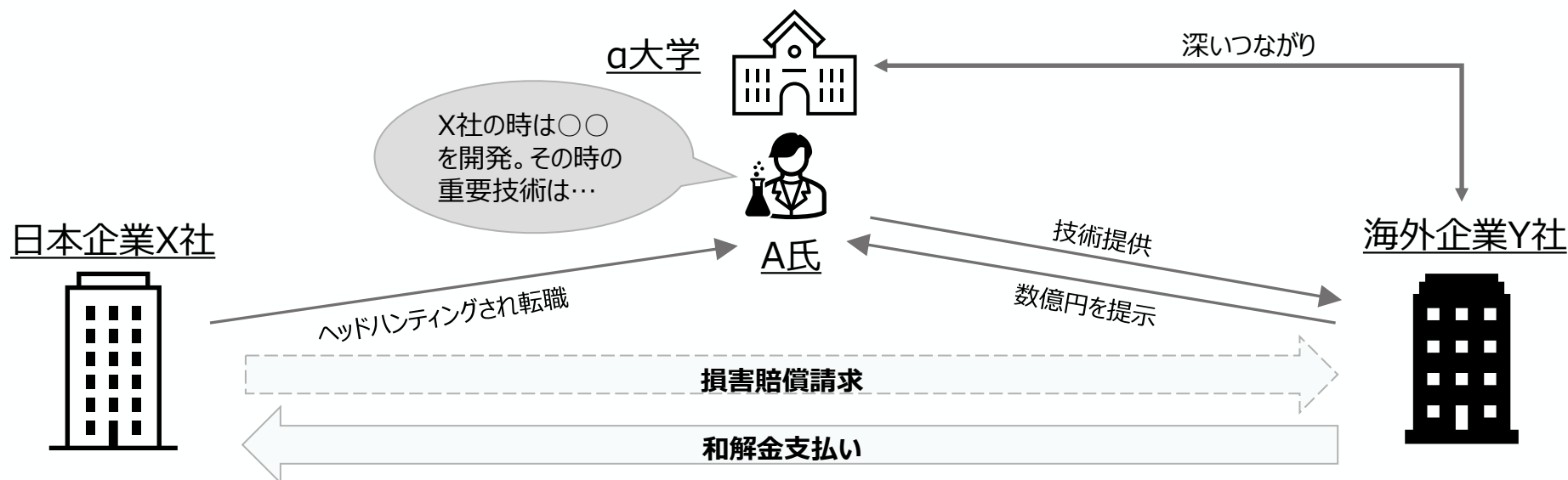
Y社

<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

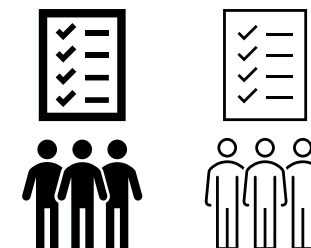
- 人を通じた技術流出は、いわゆる**正社員（管理職含む）に限った課題ではない**。技術流出対策を講じる上では、雇用関係にない**役員や派遣従業員、出向者、業務委託先のフリーランス等を含め、勤務形態を問わず広く役職員を通じた技術流出を念頭に置く必要がある**
- そのため、**就業規則のほか、雇用契約、委任契約、出向契約、業務委託契約等において技術流出の防止について定めることが重要である**
- また、社内規程に基づく情報管理体制を実効的に運用させるため、**関係部署の連携も重要である**

対応策の例

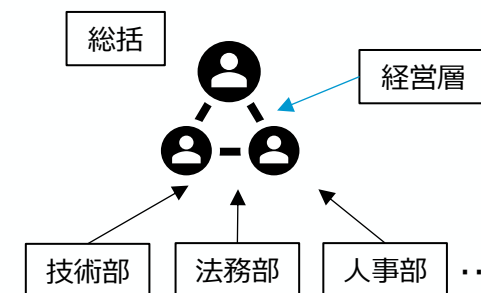
① 情報管理規程を整備するほか、雇用契約等の個別の契約でも対応する

- 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



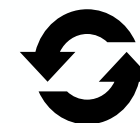
1. ③ 情報管理に関する定期的・階層的な研修の実施

- 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



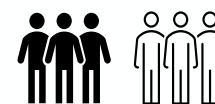
最新事例、身近な流出事例



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

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。

・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

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られることも考えられる

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たり、関係にないことの誓約を求められることが考えられる

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

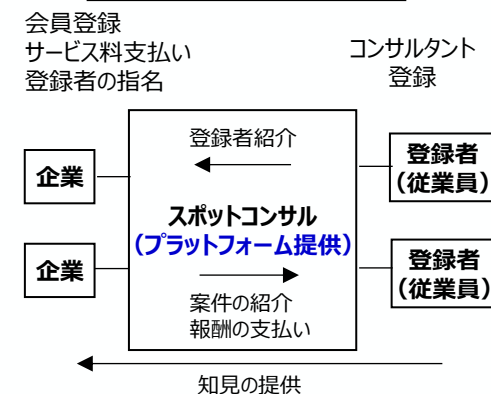
① 副業・兼業ルールの明確化・届出手続の徹底

- 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を制限することも重要である
- さらに、例えば、アクセス権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

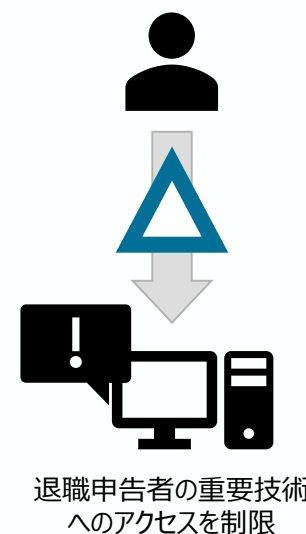
- 当該役職員の職種等に応じて、直近アクセスした技術情報の内容、外部へのメール送信の履歴等を、必要に応じて数ヶ月遡り、警戒度を高めてチェックする。情報流出の予兆があれば、退職前にヒアリング等を実施する

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

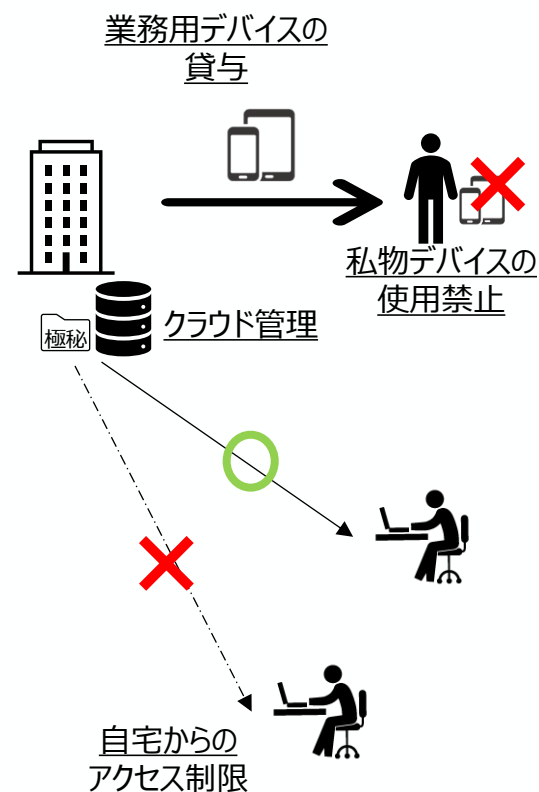
- 業務用デバイスは、会社が所有・支給することで、その管理・利用方法や退職時の返却について、会社の指示に従う必要のある仕組みとする。特に、私的な海外旅行等業務外の渡航の際には、持参を禁止する等のルールを整備し、運用を徹底する（その他海外渡航の際の注意点はp93参照）
- 私物デバイスを使用せざるを得ない場合、情報管理部門等の承認やデバイス登録を条件とし、廃棄・処分時のルールも明確化する
- 異動時には、他部門に技術情報を持ち出せないよう、デバイスの交換やアクセス制限等を行う
- 業務用デバイスにログインする際には、生体認証等を含め、セキュリティを強化する

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



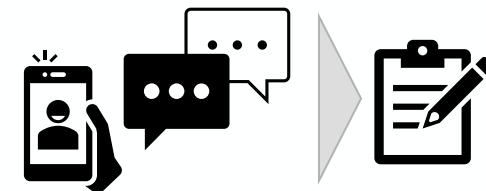
業務用デバイス



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ようにしつつ、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

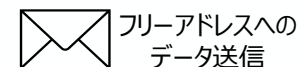
① 技術流出に繋がるおそれのある行為を検知するための体制を整備する

- 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

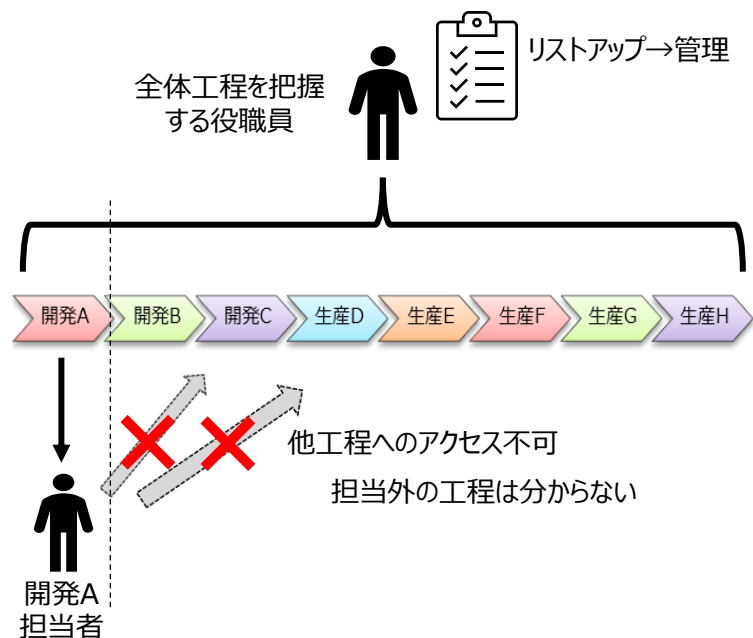
① 工程を細分化し、各担当者が知り得る情報を限定する

- 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

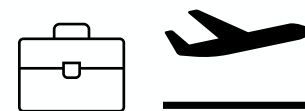
- 海外に赴任した役職員が、引き続き、日本国内のシステムにアクセスできる場合、当該役職員の使用するデバイスを経由して技術情報が漏えいするケースがある
- 人事異動に伴うアクセス権限のリアルタイムの更新は、日常的にも重要な対策であるが、海外赴任者については特に注意する

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

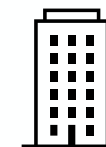
- Case3で示した技術流出事例のとおり、技術を獲得するために、役職員に対して様々な働きかけ・諜報活動（盗聴、窃取、協力者からの情報収集等）が行われる可能性がある。特に、海外出張者や赴任者等はそういったリスクが高いため、こうした諜報による情報漏えいその他の被害の防止（いわゆるカウンターインテリジェンス）に関する研修を実施する



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

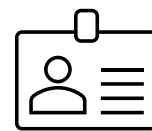
1. ⑮ 展示会等を契機とする部外者との接触への対応

- 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



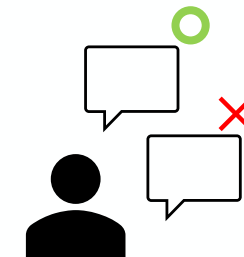
- ✗ 個人の連絡先
- 展示会専用の連絡先 (窓口等)

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

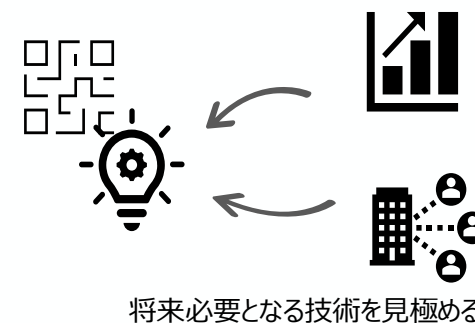
3. ① イノベーションを生き続ける（技術の陳腐化の加速）

- 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き続け、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

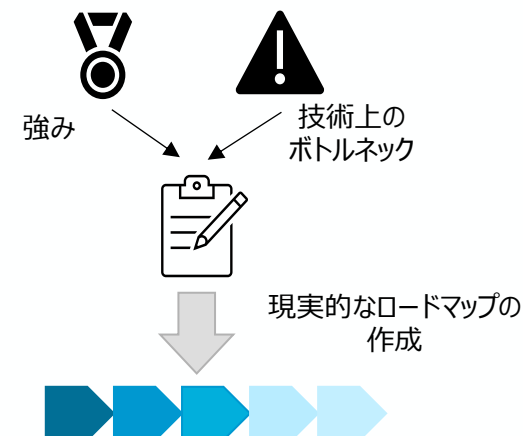
① 将来必要となる技術の見極め

- 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

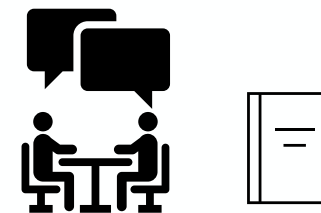
- 中途・定年を問わず、退職者と良好な関係を構築し、自社と心理的に近い距離感を持つことが、技術流出対策の観点からも重要であるという考えを、全社的に浸透させる



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