第１章
各章で共通する技術流出対策

目次

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当たって、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

具体的な技術流出対策については、本ガイダンスを活用する

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

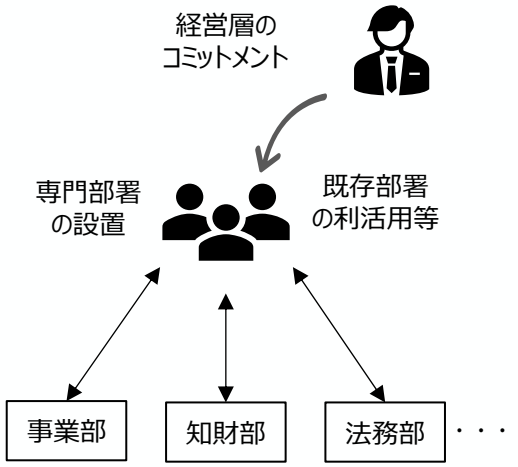
対応策の例

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

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



※ 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

(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）

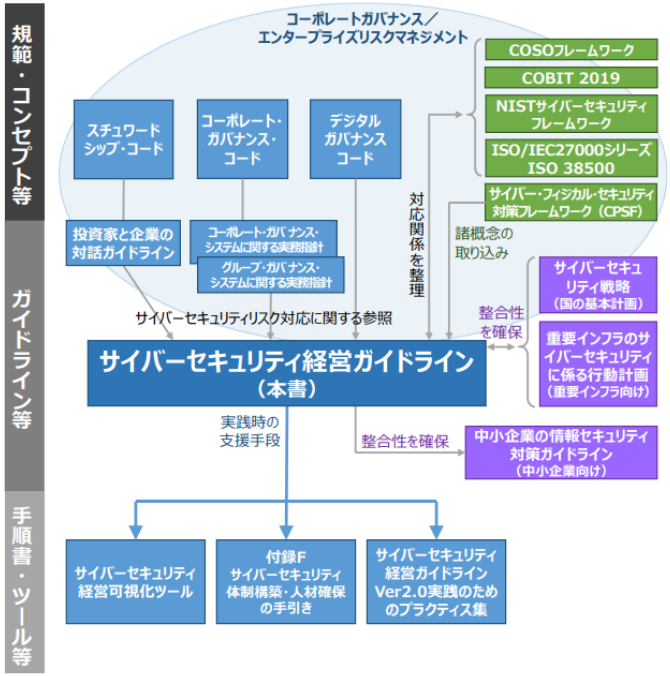
サイバーセキュリティ経営ガイドライン（抜粋）

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



目次

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も評価し、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**も評価をしておく

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**

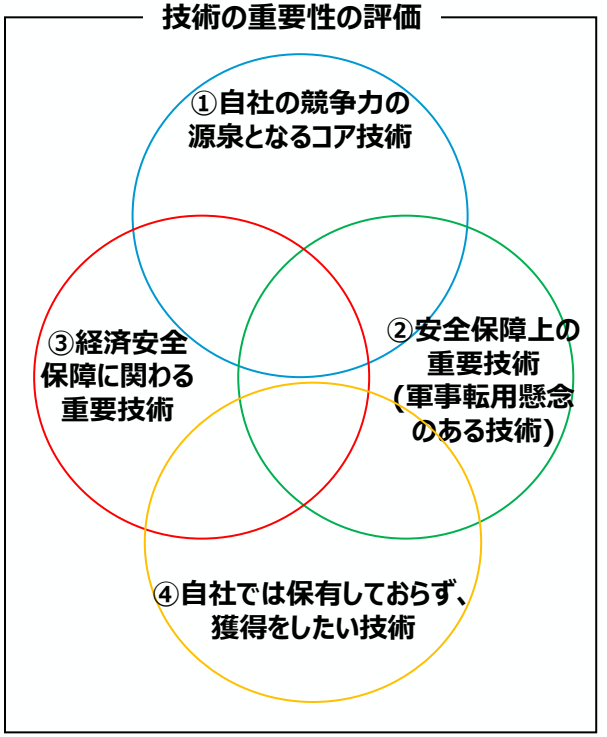
自社保有技術

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



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**ことに繋がりかねない
- 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る形では存在しないケース、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サイバー防御技術、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_anzen_hosho/suishinhou/supply_chain/supply_chain.htmlを参照）

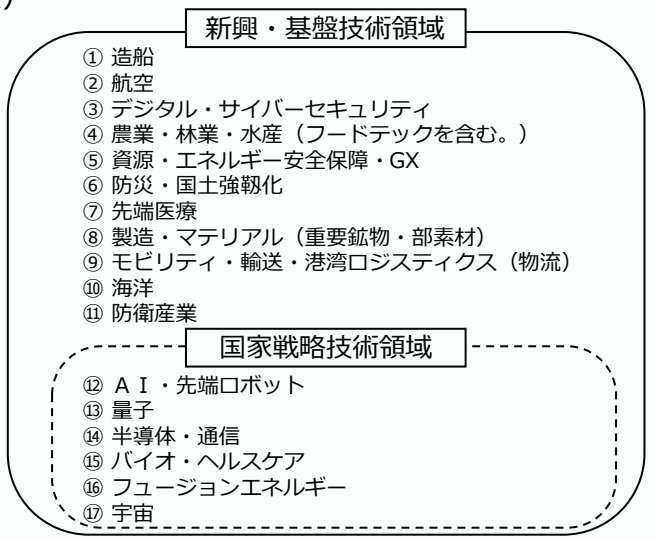
- 特定重要技術の研究開発の促進及びその成果の適切な活用に関する基本指針及び経済安全保障重要技術育成プログラム (K Program)において支援対象とする重要技術（中長期的に我が国が国際社会において確固たる地位を確保し続ける上で不可欠な要素となる先端的な重要技術）
（https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/doc/kihonshishin3.pdfを参照）
（https://www8.cao.go.jp/cstp/anzen_anshin/kprogram.htmlを参照）

- 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_anzen_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



（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