〈日本知財学会誌〉Vol. 11 No. 2―2014 : 24-31

技術秘密情報の流出防止対策―企業の現場から―

山本崇晶（住友電気工業株式会社法務部長）

How to Protect Technical Trade Secret for Companies

Takaaki Yamamoto
General Manager, Legal Department, Sumitomo Electric Industries, Ltd.

【要旨】 技術秘密情報の流出を防止するため，企業は，物理的秘密管理，情報管理ルールの制定，守秘義務契約など，さまざまな取り組みを行なっている．技術秘密情報管理活動の実効性を上げるためには，流出リスクの発生可能性や想定される損害等を評価し，取り組みを改善してゆく必要がある．また，技術秘密情報の流出が現実に発生した場合の不正競争防止法の執行については，(1)秘密管理性の要件，(2)刑事告訴受理の条件，(3)民事訴訟での証拠開示手続きにつき，工夫や改善が望まれる．本稿は，企業の法務担当者としての考察を述べる．

【キーワード】 技術秘密情報　　流出防止　　実効性向上　　不正競争防止法

【Abstract】 In order to protect technical trade secret from leakage, companies have a variety of measures, such as physical security measures, rules of information security, and confidentiality agreements. To make such measures more effective, such measures shall be improved through assessment of risks of leakage and damage likely to suffer. With respect to enforcement of Unfair Competition Prevention Law in case of technical trade secret leakage, improvement shall be made on (1)"measures to be taken to keep confidentiality" requirement, (2)requirements for filing of criminal complaint, and (3)discovery of evidence in civil procedure. This article addresses the thoughts of one in-house legal counsel on the above subjects.

【KEYWORDS】 technical trade secret　　leakage prevention　　improvement of effectiveness　　unfair competition prevention law

1. はじめに

筆者は，住友電気工業株式会社法務部に 20 年超在籍し，法務問題を扱ってきた．本稿では，いわゆる営業秘密，その中でも技術情報に焦点を当てる．自社が秘密としている技術情報（以下，技術秘密情報）が意に反して流出することを防止するための取り組みのなかで考察してきたことを紹介する．また，不幸にして技術秘密情報が流出した場合に，被害を最小限に止めるために手を打つ際にぶつかる問題にも触れる．それらは，原材料や部品を，客先メーカに販売する部材メーカ，しかもある程度規模の大きい企業の立場を想定して考察したものである．

なお，本稿の意見は，住友電気工業株式会社の意見ではなく，筆者個人の意見であることをお断りしておく．

2. 技術秘密情報の管理

技術秘密情報の管理のあり方は，各企業の実情により異なってくる．製品や技術の内容，製造ライン

ISSN 1349-421X

やサプライチェーンの組み立て，事業規模，業務の進め方，管理思想などにより，管理の仕組みはさまざまになる．各企業にて工夫し，試行錯誤を重ねる必要がある．一般的にどうあるべきかは，経済産業省が発表した「営業秘密管理指針」（平成 15（2003）年 1 月 30 日発行，最終改訂平成 25（2013）年 8 月 16 日）が参考になる．

「営業秘密管理指針」は，営業秘密が，不正競争防止法の下で保護されるための要件を充足するための「秘密としての管理」の水準を示すことを第一義的目的として，営業秘密に対するアクセス制限や秘密であることの客観的認識可能性の実施策を紹介し，企業組織としての管理の仕方を，物理的管理，技術的管理，人的管理の各側面から，具体的な例を挙げて示している．また，組織的な営業秘密管理の進め方として，営業秘密の把握，管理方針の整備，責任者の設置，教育や周知，モニタリングや監査などの，ベストプラクティスを示している．いずれの点についても，日本の裁判例を踏まえつつ，具体的な方策を網羅的に，かつ，一般的なものと高度なものと段階わけをして紹介し説明していて，各企業が営業秘密管理体制を構築していくのに参考にしやすい．さらに，実際に営業秘密の管理を導入する手順についても述べてあり，至れり尽くせりの感がある．実際に，多くの企業が「営業秘密管理指針」に沿った取り組みを整えていると推測する．

3. 問題意識―いかに実効性を高めるか

3.1. 管理に伴う問題点

情報管理ルールの制定と実施は，リスク発生の予防のために行なうものであるが，ともすればルールを守ることが自己目的化してしまう．また，社内の業務監査で不備を指摘されなければ，それでよしとされることとなりやすい．競争法コンプライアンスなど，他の種類のリスクの予防のための取り組みも，同様の傾向を持つ．類似の取り組みがたくさんあり，それぞれルールの制定・遵守，自己点検・報告と監査に追われ，「管理疲れ」をもたらす．本来なすべき事業活動に割くリソースを奪われては，本末転倒となる．できるだけメリハリをつけて，コスト効率を上げる，実効性を上げる，という視点で，取り組みを設計し，見直すことが必要となる．

3.2. 管理の実効性とは何か―管理目的との関係

ここで，「管理の実効性」とは何か．管理活動に，実効性のあるものと，実効性のないものとあるとすれば，それはどこに現れるのか．言いかえれば，管理の実効性は，何によって測ることができるのか．

管理の実効性を考える場合には，管理の目的が何かを考慮する必要がある．ここでは，①実際に技術秘密情報の流出を防止すること，②技術秘密情報の流出があった場合に法的な保護を受けることができるようにすること，そして，①②により，③実際に技術秘密情報の流出による経済的損失を最小化すること，であると想定する．そして，運営にあたっては，これらの目的を達成しているか，達成度を何で見るか，達成効率を上げるためにはどうしたらよいか，を常に考えることとなる．ここで，①の技術秘密情報流出の流出予防と，②の法的保護の確保（秘密管理性の要件の充足）との，どちらを重く見るかで，取り組みのあり方が少し変わってくるのではないかと思う．

②に重点を置けば，どちらかというと，制度をきちんとつくり，きちんと運用することに目が向きやすいのではないか．裁判の場で組織としての管理の粗さや関連するルールが必ずしも守られていないことが指摘され法的保護が否定されるおそれがあれば，それをつぶしておくことに重点が置かれるであろう．それに対し，①の技術秘密情報の流出の予防そのものに重点を置くのであれば，重要な技術秘密情報に限ってはしっかり流出の予防がされていれば，全体の管理の粗さにはある程度目をつぶることもあるだろう．

3.3. 管理の実効性をどう考えるか―実践的な考え方

最終的な目的が，③技術秘密情報の意図せざる流出による経済的損失を最小化するということにあると考え，予想される経済的損失との関係で管理レベルを調整することが合理的と考えるのであれば，②よりも①に重点を置いて考える方が理に適うであろう．特に，②については，仮に管理を厳格に実施し

ていたとしても，現在の日本の法制度とその運用の元では，現実化した経済的損失を回復し，最小化するというのは，必ずしも容易ではない．感覚的ではあるが，①実質的な流出予防に重点を置く方が実践的と思う．

とすれば，技術秘密情報の実際の流出やその現実のリスクの発生の有無や頻度，発現したリスクの重大性や内容が，管理の実効性を評価する指標となろう．そして，重大なリスクが現実に発生する可能性の高いところを重点的に管理する，というのが管理の実効性を高める基本だろう．ある日，技術秘密情報の流出が発覚した場合，その流出が発生した原因や，発生したことに気づくのに時間がかかった原因などを分析し，それまでの管理の取り組みを評価して，再発防止策を考えることになる．発覚した流出事象が，全くノーマークであった場合は，実効性に問題があったということになろう．

以上を前提に，技術秘密情報管理の取り組みの制度を設計し運営に持ち込む事務担当者の立場で，実効性のある技術秘密情報管理の仕組みをつくる，あるいは，既にある管理の仕組みをより実効性のあるものに改善する，という想定で，以下に，諸側面ごとに，考えるべき事項や考え方を整理してみる．

4. リスクの分析・評価

4.1. 全般

まず，技術秘密情報の流出について，自社にどのようなリスクがあるのかを認識し，評価する．出発点として，自社の過去の技術秘密情報の流出事例を集めて，分析する．法的紛争となったものや実損の発生したものから，ヒヤリ事例まで，できるだけ集める．問題となった情報の内容，取得・保有関係，管理状況，流出に至った経緯，関与者，発覚の経緯，発覚後問題解決に至るまでの経緯，発生した損害とその算定根拠など，事実関係をできるだけ詳しく調べる．情報流出問題が発生すれば必ずしかるべき部門に報告がなされ，調査され，内容が記録される仕組みがあり，記録が整理されていれば，それを見ることから始めればいい．しかし，現実には，労働災害や品質事故と異なり情報事故が網羅的に記録・整理されている会社は多くはないのではないかと推測する．そういう場合に事案を掘り出し整理するのは容易ではない．事業部門・営業部門内の管理部門の経験者や，法務，総務・人事，知財部門などの者から聴き取りを行なったり，業務記録をひっくり返して，事例を探し当てることとなる．丁寧に調べれば，結構な数あるのではないかと思う．

また，自社と業態の似ている企業で過去に起こった技術秘密情報の流出問題を集めて研究してみる．メディア上の情報だけで相当数になる．また，裁判例を読み，証拠を裁判所で閲覧する．日本国内のみならず国外の事例も研究する．経済産業省の「営業秘密管理基準」やその関連の資料にも相当数の事例が紹介されている．

併せて，技術秘密情報の保護についての各国の法制度やその運用も整理して頭に入れる．同テーマを扱った，経済産業省の委託研究の報告書が参考になる．

これらを通じて，自社の，どういう技術秘密情報が，どういう経路で，どういうところに流出し，自社にどういう損失を発生せるのか，といったことのイメージを掴むのが，出発点となる．

4.2. 問題となる技術秘密情報

まず，自社に問題となる技術秘密情報にどのようなものがあるかは，過去にリスクの発生した事例を検討したり，経済産業省による事例紹介を見れば，だいたいの見当はつく．

研究・開発活動に関するものでは，研究テーマや研究計画，研究の結果得られたデータ，進捗状況等，多くのものが重要な技術秘密情報となろう．設計・製造においては，製品の設計図面，設備図面，製造条件の管理データなどが重要であることが多いだろう．製造に使用される原料や部材の購入仕様書も技術秘密情報として重要であろう．特に製造設備や製造技術についての情報は，守秘にしておく必要性が極めて高いことが多いであろう．製品の設計図など，製品そのものの情報は，市場で入手し分析すれば分かることが多いので，秘密にするより特許権等の出願をして内容を公開して独占権を得る途を選ぶことが多い．一方，製造条件は，特許権等の出願はせず

ノウハウとして秘密に保持することで，その価値を維持することが比較的多かろう．

いずれにしても，自社のどのような技術秘密情報が重要であるかは，研究・開発や製造の現場が一番よく知っている．どういう技術情報が競業事業者に知られていない故に自社が競争上優位に立てているのか，何を知られると競争上自社がダメージを受けることとなるのか，逆に競争事業者のどんな技術秘密情報を知ることができれば攻撃の手がかりを掴むことができそうなのか，などは，実際に事業をしている現場が一番よく知っている．そして，現場にとっては，重要な技術秘密情報が何かということより，いかにしてその流出を防止するかという方法論が一番の関心となる．

一方，現場が比較的気づきにくい技術秘密情報もある．設備の形状や工場でのレイアウトは，自らの目に常にさらされているものであり，特段の研修や教育を受けなければ，それ自体の技術情報としての価値を理解していない場合もある．また，工程内で発生した不良品は，技術秘密情報を含んでいることもあるが，廃棄されるものであるから，秘密技術情報としての価値を理解されないことがある．

共同研究・開発活動等の過程で他社から開示を受けた技術秘密情報も，自社の情報と勘違いして取り扱うことで，流出させてしまうことがある．つまり，自社の情報と同様に扱い，特許出願することで開示したり，学会発表してしまうことがある．

また，工程内で発生した不良品が客先の新製品の設計に合わせて設計された部品である場合，不良品そのものの流出が，客先にとっての技術秘密情報を開示することになる場合もある．

いずれにしても，現場がその重要性に気づきにくいような技術秘密情報は，特段の注意喚起や教育・研修を行なうなど，その管理に工夫が要求される．

4.3. 流出によるダメージ

次に，技術秘密情報が意図せずして流出した場合のリスクの現れ方，つまり自社がどういうダメージを被るかも整理しておく．想定されるダメージの大きさは，関係する技術秘密情報の重要性につながり，管理レベルの設定に結びつくからである．

まずは，技術秘密情報が競争事業者の手に渡り，自社のビジネスを失ってしまうリスクがある．また，ビジネスを失うことはなくても，製品の市場価格が下がり，収益性を落とすことがある．特に，製造設備についての技術秘密情報が流出し，設備メーカが設備一式を製造できるようになれば，そこから設備を購入すれば競争事業者が製品を製造できるようになってしまう可能性もある．その競争事業者の市場シェアが小さくても，製造設備についての開発費がかかっていない分低い価格設定が可能となり，自社も競争上やむを得ず価格を下げることになれば全体として大きなダメージを被ることになる．

また，技術秘密情報を入手した競争事業者が，その情報をベースにした発明をし特許権等を出願した場合には，当該技術秘密情報が公開されるばかりか，当該競争事業者が特許権を行使し，自社が事業の差し止めを受けたり損害賠償を求められるというリスクも出てくる．

さらに，他社から開示を受けた技術秘密情報を流出させてしまった場合は，当該他社から損害賠償を請求されたり社会的信用を失う，などのリスクが発生する．

そして，これらのリスクは，技術秘密情報が競争事業者の手に渡ることで自社の競争力の源泉を喪失する，一旦流出すると取り返しのつかないことになる（事後的な措置では被害の回復が困難である），などの特徴を持つ．

4.4. 流出経路

さらに，技術秘密情報が流出する場合の経路としてどのようなものがあるかを整理する．流出を防止する対策をどうするかは，流出経路ごとに大きく変わってくるため，流出経路の分析は重要になる．

流出経路には，だれが流出させたかという面（流出主体の問題）と，どうやって流出させたか（技術的な面）とがある．

4.4.1. 流出主体

流出主体には，自社との関係で，①各種取引先（客先，技術提携先，共同開発・研究の相手先，製造委託・外注先，原材料仕入先など，各種の契約関係にある），②役員や従業員（委任契約や雇用契約関係

にある），③それ以外の第三者（契約関係にない）があり，それぞれ流出させる動機や流出態様が異なる．

まずは①各種取引先であるが，自社との関係でさまざまである．

客先が，自社が納入している部材の設計図面を競争事業者に開示して同一の部材を製造させ，セカンドソースを確保する，ということがある．設計図面には公差その他製造方法やコストに関わる秘密技術情報が盛り込まれていることがあり，それが意図せずして流出する可能性がある．

客先が，自社が納入しようとしている部材のサンプルを，特性データ等の技術秘密情報を付けて，評価してもらう目的で提供したところ，当該情報をベースに「発明」をなし特許出願する，ということがある．出願内容が公開され，自社の技術秘密情報が流出してしまう．

原料の購入先や部材の製造委託先が，当該原料の購入仕様書の内容や部材の製造条件等を，自社の競争事業者に対し，原料の売り込みや製造受託の申し入れに際して開示してしまうと，自社の技術秘密情報の流出となる．

②技術秘密情報の流出主体として最も多いのは，役員・元役員や従業員・元従業員（以下，従業員等）である．従業員等は，社内の技術秘密情報に常時触れているか，触れようと思えばその思いを遂げやすい立場にある．自社の中での自分の将来に見切りをつけ，自社の貴重な技術秘密情報を手土産に転職活動をしたり，それをもとに独立し起業しようとすることがある．また，貴重な技術秘密情報を買いたいとアプローチしてくる第三者がいる場合，金銭的欲求から技術秘密情報の持ち出し，売却をすることもある．持ち出そうと思えばできる環境があり，持ち出す誘惑があるので，特に退職に際し従業員等が技術秘密情報を持ち出す例は後を絶たない．

これらに対し，③第三者については，夜陰に乗じて施設に忍び込み，あるいはハッキングの技術を駆使して直接に技術秘密情報を取得するという場合の他，従業員等を唆して技術秘密情報を持ち出させる，あるいは任用・雇用して技術秘密情報を開示させるなど，間接的に技術秘密情報を取得する場合がある．

4.4.2. 流出形態

流出形態としては，紙にコピーして持ち出す，USB メモリなど物理的な媒体に記録して持ち出す，写真撮影して持ち出す，メモをとって持ち出す他，ネットワーク経由で送出する（させる）などの方法がある．

5. 流出防止のための方策

流出防止のための方策は，流出主体や流出形態により異なる．流出形態がネットワーク経由の場合には，情報セキュリティ対策が中心となる．それ以外の場合につき，流出主体ごとに分けて整理する．

5.1. 各種取引先

客先，仕入先，共同開発研究相手，製造委託・外注先等に技術秘密情報を開示する際には，当該情報についての守秘義務（第三者への開示や目的外の使用の禁止）を定めた契約を相手方と事前に取り交わしておくことが最低限必要になる．契約形態としては，守秘契約（Non-Disclosure Agreement や Confidentiality Agreement）の他に，情報の開示の根拠となる契約（売買契約，製造委託契約，共同開発契約等）に守秘義務を定める場合がある．

守秘契約を交わした上で，どういう情報をどういうタイミングで開示するかを注意深くコントロールすることも重要である．例えば，客先の要請に応じて，部材の設計図面を競争事業者に開示せざるを得ない場合，当該図面上に製造条件や製造技術に関係するような情報があれば除去し，必要最低限な情報に絞る等である．また，重要な製造設備の製作委託にあたっては，設備を分割して複数のメーカに発注し，設備の全体像をできるだけ見せないようにするやりかたもある．

また，情報の開示を定める契約の中に，守秘義務条項のみならず，目的外使用をしていないかを監査する権利を設定しておくことで，情報の無断使用に対する抑止力を確保する場合がある．

管理という点では，開示する情報に秘密情報である旨を表示することの励行や，情報を口頭で開示した場合に後日書面化し守秘対象であることを確認す

ることなど，実務上煩わしいことを面倒くさがらずに実施するということが重要となる．

また，自社が情報の開示を受ける場合には，開示を受ける以前から自社で有していた技術情報について，守秘義務の対象外であることを立証できるように保有していた技術情報を保管しておく工夫が重要となる．

5.2. 従業員等

5.2.1. 頭の中にある情報

従業員等による技術秘密情報の流出については，そもそも流出を止めることが法的に認められうる種類の情報かどうかという問題がある．例えば，転職者が，頭の中にある情報を転職先で開示したり使用したりするのを止めうるのかという問題である．この問題について大まかにいうと，自社に特有の製造技術や製品を開発した場合の特殊性の高い技術秘密情報は法的にも流出を阻止できる可能性があるが，その分野で開発や製造を行なうためのベースとなる一般的な知識，スキルやノウハウは，特別な合意の無い限り，法的には流出を止めることができない可能性が高い．そのような技術秘密情報の流出を防止する方策としては，十分な処遇をしてその技術秘密情報を身につけている役員・社員を自社に引き留めたり，十分な経済的手当を継続してその役員・社員に当該情報を退職後も開示・使用しない旨の合意を取り付ける必要がある．

5.2.2. 悪意の無い場合

法的にも流出を止めることが認められうる技術的秘密情報につき，従業員等による流出を防止する方策については，当該従業員等が，それは自社の保有する情報であって「自分のもの」ではないことについて百も承知している場合（悪意をもって流出させる場合）と，それと知らずに行なう場合（悪意の無い場合）とがある．

悪意の無い場合としては，そもそも技術秘密情報ではないと思っていた場合や，他社に対して守秘義務を負う情報とは思っていなかった場合がある．これらについては，秘密情報管理の基本，つまり，それが技術秘密情報であることを明確に表示し，技術秘密情報の扱いについての教育を行なう等して周知をしっかりとすることが一番の対策であろう．また，過失による流出を防ぐようなフェールセーフの仕組みを作ること（情報機器にセキュリティを施す等）や，忘れないように注意を喚起する仕組みを作ること（サーバにアクセスするたびに注意書きが表示される）も有効であろう．

また，従業員等に対して，委任契約や雇用契約の中で，守秘義務を明確に定めておくことは，注意喚起の意味も含めて基本的に重要なことである．具体的には，任用や入社の際の誓約書や就業規則で守秘義務を明記しておく，退任・退職の際に守秘の誓約書や，「会社の情報は全て返還した」旨を表明する書面を徴求するなどが有効である．

競争事業者への転職を禁ずることは，職業選択の自由との関係で限界があり，転職しないような処遇を用意することが基本となろう．定年退職の場合，秘密情報へのアクセスが高かった者については，一定期間，顧問契約や嘱託契約を締結してつなぐという方途もあるだろう．

5.2.3. 悪意のある場合

これに対し，確信犯的な技術秘密情報の持ち出しへの対抗策は難しい．

技術秘密情報にアクセスできる人をできるだけ限定したり，技術秘密情報の所在を分散させ全体像を把握できる人をできるだけ限定するようにすること等により，情報流出の可能性をできるだけ減らすという方策が基本的に重要であろう．

また，悪意のある場合の技術秘密情報の流出に対し重い刑事罰等が定められており，実際に厳しく処罰されていて，そのことを，研修，教育等で周知・宣伝することは，目に見える形で管理をしっかりすること（施錠，監視カメラの設置，アクセスログの点検等）と相俟って，確信犯的情報流出に対する抑止効果を期待できると思われる．

5.3. それ以外の第三者

契約関係にない第三者による技術秘密情報の盗みだしについては，防犯カメラの設置，施設への入出門管理，写真撮影や録音のできる機器の持ち込みの禁止などにより，技術秘密情報の流出につながる事象を物理的に制限することが中心となろう．情報通

信ネットワークを経由しての盗み出しは，ハッキング対策等，情報セキュリティの技術的方策が中心となるだろう．

6. リスクの拡大防止・被害回復

6.1. 全般

種々の予防策にもかかわらず，不幸にして技術秘密情報の流出が発生した場合（正確には，現実に流出した可能性があると思われる場合）には，自社の損失をできるだけ小さい範囲にとどめることと，現実化した被害の回復をすることが重要になってくる．損失をできるだけ小さい範囲にとどめるためには，まず，技術秘密情報の流出の可能性をできるだけ早い段階で察知し，それに応じた行動を素早くとることが必要である．

6.2. 情報流出の早期察知

早い段階で覚知するためにはどうしたらよいか．技術秘密情報の流出に気づく端緒としては，インターネットを検索していて自社の技術秘密情報が開示されていたのを見つけた場合，特許公報に自社の技術秘密情報が記載されていたのに気付いた場合，競争事業者から自社の技術秘密情報を使用した可能性のある製品が出された場合などがある．いずれも，技術秘密情報の流出から時間がたってから偶然知ったというケースが多いのではないか．

自社の技術秘密情報に関して定期的にインターネット上の検索を行なったり，重要な技術秘密情報にアクセスしていた従業員の転職先を調査したり，転職先の会社の事業活動や特許出願活動をマークすることで，技術秘密情報の流出を比較的早期に察知できる可能性があると思われる．

6.3. 流出の拡大阻止や被害回復に向けた行動

技術秘密情報の流出の可能性を察知したら何ができるか．技術的秘密情報を持っている元従業員の転職先が判明した場合には，転職先に直ちに警告状を出し，当該元従業員は技術秘密情報につき守秘義務を負っているので十分注意されたいと注意を喚起し牽制する．また，具体的な事業活動で当該技術秘密情報を使用している可能性が窺えれば，使用されているのであれば直ちにやめられたい旨の通告をする．

さらに，技術秘密情報の実施の蓋然性が高いとなれば，その差し止めを求め，実施によって被った損害の賠償を求めることになる．このために具体的にどういう方法をとることができるかは，関連する国の法制度にかかっている．日本法では，不正競争防止法に基づく，使用差止請求や損害賠償請求，さらには刑事処分を求めることが中心となろう．

7. 法的保護を求める場合

7.1. 全般

不正競争防止法に規定される，使用の差止めや損害の賠償を相手方に求めたり，相手方に対する刑事処罰を求めたりするには，捜査機関や裁判所に動いていただかねばならない．動いていただくよう関係機関に求めるためには，当方に，①相手方による営業秘密の取得や秘密が実施されていること等を主張し，②それをある程度証明できる証拠を集めることが求められる．

それぞれ，それなりに困難の伴うことであり，特に証拠の収集はハードルが高い．以下に，民事的救済を求める場合や，刑事処罰を求める場合に，ハードルと感じることを述べる．

7.2. 民事的救済を求める場合

7.2.1. 秘密管理性

使用の差止めや，損害賠償を請求しそれが認められるためには，まず，営業秘密であること，つまり，問題となる情報が，「秘密管理性」「有用性」「非公知性」の要件を充足することを主張し立証することが求められる．これらの主張・立証をどの程度厳格に求めるかで，不正競争防止法の規定の実効性は左右される．「有用性」は損害の発生からある程度推定することはできようし，「非公知性」は相手方に公知であることの主張や立証を促し判断することで，実際的な結論に至ることができると思う．問題は「秘密管理性」であり，これを余りに厳格に求めると，救済される場合が限定され過ぎるように思う．

そもそも，問題となる技術秘密情報が，流出させた者にとって「自分のもの」ではなく，他人である企業の保有するものである場合に，それを流出させたり勝手に実施する行為は，企業の財産の侵害にあたるだろう．それを，「秘密として十分管理されていなかった」からといって不問にするというのには違和感を覚える．企業の管理実態よりも，流出させた側にその技術秘密情報を開示したり使用したりする正当な権原があるかどうかが問題の核心なのではないか．

7.2.2. 証拠の確保

また，問題となる技術秘密情報が相手によって流出されたことや，相手方または第三者の元で実施されていることを，事実として正確に掴み，証拠も入手して立証するのは，至難のことである．米国の民事訴訟手続においては，いわゆる証拠開示手続き（Discovery）があり，裁判所の命令を背景にして，双方当事者の手持ち証拠が全面的に開示されること，それを少なくとも双方の代理人弁護士は全て見ることができることをベースに，立証活動や和解協議がなされる．コストはかかるが，少なくとも「どうせばれることはないだろう」という前提に立つことができないという点は，評価できると思う．出るところに出たら開示される（隠すと不利益を受ける）という前提は，技術秘密情報の取得や無断使用に対する抑止力としても大きいのではないかと思う．

7.3. 刑事処罰を求める場合

7.3.1. 刑事告訴の受理

技術秘密情報を流出させたと推定される相手方に対する処罰感情からというよりも，自社では事実関係の調査に限界があるとして，警察や検察に刑事告訴を行ない，公権力による捜査を求めることがある．しかし，告訴状が受理され警察や検察に実際に捜査を開始していただくために，告訴人の側でどの程度の事実を調査し証拠を集めておくことが求められるのか必ずしも明確でない．現実には，退職者が技術秘密情報を持ち出して中国の企業に持ち込んだと思しき場合でも，退職者の現在の所在地も，中国企業での情報使用の実態も，告訴人側ではなかなかつかめない．ただ，その退職者が技術秘密情報を持ち出した痕跡は明確にある，という場合，公機関に捜査を進めていただく他に手の打ちようがない．告訴受理のハードルがあまりに高いと，法律の目的が遂げられ難くなる可能性がある．

7.3.2. 秘密管理性

また，「営業秘密」の要件である有用性や秘密管理性の要件をあまり厳格に扱うことは，有体物の窃盗等の場合とのバランス上，違和感を覚える．有体物であれば，仮に価値が低かろうとも所有者に無断で持ち出せば窃盗罪になるし，仮に所有者の占有を離れていたとしても，勝手に自分のものとすれば占有離脱物横領罪に問われる．また他人の財物の価値を失わせれば器物損壊罪となる．技術秘密情報に物理的形状は無いが，企業のものと知って，あるいは自分のものではないと知りつつ第三者が流出させ技術秘密情報の価値を毀損させても，「秘密管理性」に欠けているので犯罪とはならないというのは，いかにもバランスを欠くように感じられる．処罰されるべきなのは，技術秘密情報の管理活動への侵害ではなく，技術秘密情報の価値を毀損する行為であろう．その情報が「自分のもの」ではないと承知していながら，開示したり使用する行為は，本来の情報保有者の管理の如何にかかわらず処罰されうるという考え方は，成り立たないものだろうか．

8. 結語

以上，技術秘密情報の流出防止に取り組む現場の目から，より実効性のある取り組みとするために，日常考察している事項を述べた．不断のリスク分析・評価や，実態に即した改善を重ねることなど，至極当たり前のことを述べたにとどまる．また，法制度の運用について，雑駁な感想を述べたが，なにがしかの参考になれば幸いである．