特　集

企業における営業秘密保護

――グローバル・コンプライアンスの視点から取るべきプロセスの探求――

矢　倉　信　介*

抄　録　企業において長年蓄積されてきた営業秘密は，企業における競争力の源泉となっている。しかしながら，オープン・イノベーションの発展，人材の流動化，さらには情報管理のIT化によって，営業秘密は流出の危険に晒されており，企業における営業秘密管理に向けた対策構築はもはや急務である。秘密情報管理について完璧なマニュアルは存在しない。本書はまず自社の現状把握からスタートし，予防対策及び有事対応における当該企業にとってオーダーメイドとも言えるプロセス（対策）を導き出すべきことを提言し，その要点について概説した。営業秘密を管理するにあたり，マネジメントを先頭に，知財部，法務部等の各部門，さらには弁護士やITベンダー等の外部専門家との協働も不可欠であり，究極的に，営業秘密保護対策は，企業におけるコンプライアンスの一環として取り扱われるべきなのである。

目　次

1.　はじめに
2.　営業秘密流出の現状
　2. 1　人材を通じた流出
　2. 2　取引に伴う流出
　2. 3　情報管理のIT化に起因する流出
3.　具体的対策～ベスト・プロセスの探求～
　3. 1　出発点：自社における現状把握
　3. 2　営業秘密管理体制の構築（予防段階）
　3. 3　秘密情報の流出発生時の対応（有事）
　3. 4　紛争解決の現場からのフィードバック
4.　結びにかえて

1．はじめに

企業において長年蓄積されてきた技術情報やノウハウ等の秘密情報は，競争力の源泉であり，マーケットにおける優位性を獲得する上で極めて重要である。ビジネスのグローバル化が著しく進む中，企業にとって自社の競争力を向上させるためには，自社技術を適切に管理するとともに，外部の技術やノウハウを積極的に取り入れ，新たな価値を創造していくことが求められ，その目的で実施した資本・事業提携及びライセンス等により，自社の秘密情報の流出の機会は以前にも増している。さらに，人材の流動化とともに，非正規雇用を含む人材の雇用形態も多様化し，人材の移動過程において企業の秘密情報が流出している事実が存在する。また，情報管理体制のIT化に伴い，秘密情報の管理も従前の紙等の媒体を用いたものから，コンピューター，ネットワーク等のIT技術に依存する度合いが高まっており，かかるIT技術の脆弱性をついた流出事案が後を絶たない。

我が国の政府も，秘密情報管理についての指針や技術流出防止に向けたマニュアル等を公表する等，秘密情報の保護に関する啓蒙活動に力を入れている。しかしながら，企業担当者からは「自社が実施している対策の実効性の感触がない」との声が聞かれ，一様に手探り状態であ

* 弁護士・ニューヨーク州弁護士・弁理士
Shinsuke YAKURA

る。その原因として，営業秘密の流出を阻止する「完全なマニュアル」を模索しようとする姿勢が根底にあるのではなかろうか。

企業における営業秘密保護は，知財部や法務部，人事部，さらには経営企画やIT部門を含む担い手により，企業を「横断して」実行されなければならない。その陣頭指揮は経営を指揮する役員を含むマネジメントが担う必要がある。しかるに，営業秘密保護は，企業における知的財産マネジメント[1)]，さらには，コンプライアンス対策の一環として捉えられなければ，実効性のあるものとはならない。

本書では，それら営業秘密保護の担い手がとるべきプロセスとは何かについて，グローバル・コンプライアンスの視点から探求するものである。

2．営業秘密流出の現状

営業秘密流出の経路は，大きく分けて①人材を通じた流出，②社外との取引に伴う流出，及び③秘密管理のIT化に起因する流出に分類される（もちろん，①ないし③の類型の複合形態も存在する。とりわけIT技術の利用については，ほぼすべての流出事案に共通して関連するものと言える。）。

2．1　人材を通じた流出

人材を通じた営業秘密の流出事例としては，元従業員が秘密情報を不正に持ち出し，転職先等で当該情報を不正利用する事案が典型例である。そのような事案に関し，我が国の裁判実務上は，競業避止義務の有効性及び存否や営業秘密の秘密管理性等の論点との関連で多くの事案が取り扱われており，かかる裁判例の研究成果も多く存在する。

近年，我が国の企業にとって極めて大きな関心を集めたものとして，日本の大手製鉄会社が韓国の大手製鉄会社を相手に東京地方裁判所において訴訟提起した事案がある[2)]。

この事案で，日本の大手製鉄会社は，電力インフラの変圧器等に使用する鉄鋼製品の製造技術が，同社の研究職従事者を含む複数の元従業員を通じて，競業会社である韓国の大手製鉄会社により盗用されたとして，不正競争防止法に基づく営業秘密侵害を理由に，約1,000億円の損害賠償の支払請求と，対象製品の製造販売の差止を求めた。これに対して，韓国の大手製鉄会社は，東京地方裁判所における答弁として，原告の主張する「営業秘密」は公知技術を含むものであって保護に値しないことのほか，そもそも「盗取」の事実は存在しない旨反論した。さらに，被告は，手続的な戦略として，本件はそもそも日本に国際裁判管轄は存在せず，却下されるべき旨の本案前の答弁を提出するとともに，韓国において債務不存在確認訴訟を提起したことである。このように，日本と韓国の双方の裁判所に同一案件が係属している状況では，様々な問題が生じ得ることとなる。例えば，仮に韓国の裁判所が日本の裁判所よりも先に債務不存在を確認した判決を出した場合の帰趨が問題となる。この点につき，韓国裁判所の判決に日本の裁判所が法律上拘束されることはないが，仮に，日本において原告勝訴の確定判決が存在する場合において，韓国の裁判所で当該日本の判決を執行する際に重大な問題が生じ得よう。

この事案が示すように，グローバルに事業展開する企業における人材を通じた営業秘密の流用は容易に国境を超えることから，営業秘密流用に関する有事対応においても，グローバルな視点から最善策を導き出す必要がある。情報の非公知性が法的保護の源泉である営業秘密にとって，少しでも適切な対応が遅れれば，当該情報はたちまち公知情報となり，企業にとって取り返しのつかない事態に陥る。

2. 2　取引に伴う流出

営業秘密流出の第二の類型として，社外との取引の過程で発生し得る流出がある。冒頭で述べたとおり，グローバル・マーケットにおける競争上の優位性を獲得する目的から，他社との資本・業務提携やライセンスを積極的に実行する企業も多い。かかる契約交渉ないしは取引の過程で，自社の重要な技術情報やノウハウ等が相手方に開示されるケースも存在する。一旦交渉に入っても，双方の意向が一致しない結果，最終契約の締結に至らない場合もある。また，契約そのものが後に解除される等により提携関係が解消される場合もある。仮に，提携関係を解消した相手方の手元に開示済みの技術情報やノウハウ等に関する情報が何らの制限なく残るとすれば，自社にとって大きな損害が発生する。

そのような事態を回避するため，一般的に，企業間で資本・業務提携交渉を入る前に，秘密情報の開示及び使用の制限を目的として，「非開示契約」（Non disclosure agreement）や「秘密保持契約」（Confidentiality agreement）が締結される。しかしながら，これらの契約を締結した場合であっても，後に秘密情報の取り扱い等を巡って紛争が発生することも多い。

前述の人材を通じた流出類型と比較して，取引に伴う流出類型については，我が国における裁判例が少ない[3)]。近時の事例として，通信事業者間の資本・業務提携に向けた交渉過程で開示された情報について，不正競争防止法における営業秘密としての保護を受けるかどうか争われた事案がある[4)]。この事案では，最終的に，当初目標としていた資本・業務提携の最終合意に至らず，交渉終了に伴い原告から提供された資料は原告に返還されたが，原告は，当該開示資料が被告により不正に開示され，使用された等を理由に，不正競争防止法等[5)]に基づく損害賠償請求訴訟を提起した。原審である東京地方裁判所は，不正競争防止法上の「営業秘密」の要件[6)]のうち，「非公知性」を否定するとともに，その他の要件である「秘密管理性」についても，原告主張の管理方法が実際に行われていたと認めるに足りる証拠はないとして，「営業秘密」の要件充足を否定した。その控訴審である知財高裁も，控訴人の請求をすべて棄却した。本事案では，不正競争防止法に基づく請求のほか，債務不履行に基づく請求を含む，原告の請求すべてが棄却された。

取引を通じた流出類型においては，取引相手方に対して，何を，どのように開示するか，さらには，契約書に相手方の義務としてどこまで落とし込めるか，相手方をどのようにモニタリングし，義務違反行為をどのように特定，立証するか等，当該類型に特有の問題が存在する。

2. 3　情報管理のIT化に起因する流出

近年の情報流出事案を見ると，IT技術を通じた流出がそのほとんどを占める。IT技術を用いた情報管理により，紙媒体を用いた情報管理に要するスペースは大幅に減少し，管理作業の効率化，管理コストの削減に大きく寄与している。しかしながら，IT技術により管理されるべき情報が無体物化したことにより，情報の流出行為そのものが，外部から判別しにくくなった。すなわち，情報の不正取得者にとっては，情報管理のIT化により，不正取得行為を隠密裏に遂行することが可能となった。企業にとっては，従前どおりの方法で情報の不正取得行為を正確に捕捉することは困難である。

例えば，従業員による，インターネット上のメール機能を利用した秘密情報の不正取得事例は後を絶たない。さらには，USBメモリ等の携帯式ハードディスクを用いた不正取得行為，ひいては，秘密情報が入っているPC本体を盗取するといったケースも存在する。

2007年に発生した日本の自動車部品メーカー

の元従業員が自動車関連図面を大量にダウンロードした会社のパソコンを無断で持ちだして検挙された事案[7]や，2012年に発生した日本の大手工作機械メーカーの元従業員が工作機械の図面情報等を不正にダウンロードし私物のハードディスクに複製して検挙された事案[8]は，いずれもIT技術を通じた流出事案であった。

また，近時は，インターネットウィルスを用いた遠隔操作による情報流出のリスクも高まっている。これらのリスクは，企業にとって多大なメリットをもたらした情報管理のIT化に伴う負の副産物というべきものであり，加えて，企業におけるITシステムのアップデートの遅れや暗号化対策の未整備，さらには，モニタリングルールの未整備ないし未実施等が流出を助長する結果となっている[9]。

さらに，留意すべきは，デジタル情報に特有の性質に基づく脆弱性である。例えば，従業員によりファイルデータが不正取得された後に，関連データが削除された場合を取り上げてみる。削除直後であれば，元のデータが未だ実在する可能性が高いが，不正取得事実が発覚後，社員等によりPCが不用意に操作されることにより，ファイルのデータが実在する領域が上書きされ，元データが永久に喪失してしまう可能性がある。

情報流出発覚後の第一歩は迅速な証拠の保全であるが，かかる証拠の保全も，ここで述べたようなデジタル情報特有の性質を十分に理解した上で実施することが不可欠である。この点において，ITに関する最新の専門的知見を有する外部ITベンダーを積極的に活用することは重要である。

3．具体的対策～ベスト・プロセスの探求～

3. 1　出発点：自社における現状把握

企業において具体的対策を講ずる上で出発点となるのは，秘密情報の管理に関する自社の現状を，いち早く正確に把握することである。具体的には，前述した情報流出の要因たる３類型（すなわち，人材を通じた流出，取引による流出及びIT化に伴う流出の３類型）を考慮した以下の項目について，具体的に把握することが必要である。

① 技術情報，ノウハウ，顧客情報等の流出を阻止すべき情報の存在，価値，重要度
② 技術情報，ノウハウ，顧客情報等に関係する業務に従事していた従業員の特定
③ 技術情報，ノウハウ，顧客情報等の管理体制の内容，アクセス制限の有無とその内容，モニタリング体制の内容等
④ 取引（資本・業務提携，ライセンス等）に関連して提供，開示された技術情報，ノウハウ，顧客情報等の特定及び提供，開示の具体的内容
⑤ 契約における手当の現状把握
　○労働関連契約（競業禁止，勧誘禁止，秘密保持等），就業規則
　○個別合意書面（個別の従業員が差し入れた誓約書含む）
　○取引（資本・業務提携，ライセンス等）に関連して締結した契約（競業禁止，秘密保持等）
　○上記契約の執行状況の確認（締結しただけになっていないか）
⑥ 契約外における手当の現状把握（特許出願等権利化の状況，IT技術の整備状況，企業内における従業員トレーニングの実施状況を含む）

⑦ 上記項目に基づく確認内容を踏まえた具体的アクションの必要性についての分析・検討

このように，秘密情報管理についての現状把握に際して検討すべきポイントから，企業における営業秘密保護の担い手が，知財部や法務部のみならず，人事部，経営企画部さらにはIT部門の協力も不可欠となることがわかる。加えて，取引（資本・業務提携やライセンス等）に関する具体的内容については，ビジネスを具体的に担っている事業部との協力も必要になる場合もある。会社の組織を横断的にコントロールするため，マネージメントレベルの積極的関与が必要とされる理由がここにある。

さらに，実務的に重要となるのが，現状把握の具体的方法である。現状把握の結果得られる内容は，必ずしも「これで万全」と言えるものであるとは限らない。むしろ，企業の秘密管理にとって「不十分」な部分を露呈するものであることが多く，これがひとたび紛争の相手方の手元に渡れば,「営業秘密」の要件としての「秘密管理性」を欠く証拠として利用されかねない。訴訟が日本のみで提起される場合はもとより，米国のように強制的証拠開示制度（ディスカバリー）が存在する民事訴訟制度のもとでは，ディスカバリーの手続で相手方への開示対象となる可能性がある。秘密情報の管理状況に関する現状確認の結果（不利なもの）が訴訟を通じて相手方の手に渡るのを可及的に回避するため，現状把握レポートの作成及び報告の過程において，弁護士・依頼者間秘匿特権（Attorney Client Privilege）を積極的に活用することが望ましい[10]。米国法のもとでの弁護士・依頼者間秘匿特権は，依頼者から弁護士に対して，又は弁護士から依頼者に対して伝えられた秘密を保護するためのものであり，秘匿特権による保護を受けるためには，弁護士と依頼者間のコミュニケーションのうち，秘匿特権のある者の間で内密に行われたものであり，法的支援又は助言を求めるためのものであることを要する[11]。なお，電子メール・チェーンのCCに弁護士を入れさえすれば弁護士・依頼者間秘匿特権による保護の対象となると考えるのは正確ではない。弁護士・依頼者間秘匿特権による保護を受ける可能性を高めるための方策としては，営業秘密の流出現状調査を，企業における「営業秘密の流出対策」の一環として取り扱うとともに，当該対策を依頼した外部弁護士の指示に基づき，当該弁護士から法的助言を受ける目的で調査することとし，当該調査報告の結果についても，当該弁護士に宛てた報告書という形式をとることが考えられる。同時に，これら一連の経緯を証拠化するため，調査依頼は弁護士名義で出すとともに，報告書の中にも「弁護士からの指示に基づき，弁護士の法的助言を受ける目的で」と明記しておくのが得策である。

自社における秘密情報管理の現状が確認できた場合，次のステップは，①平常時（流出発生前）における予防段階としての，営業秘密管理体制の構築及び見直しと，②営業秘密の流出が確認された場合における具体的な紛争対応である。

3. 2　営業秘密管理体制の構築（予防段階）

(1) 営業秘密管理に要求される水準

企業における営業秘密管理の究極的な目的は，企業における重要な経営資源たる秘密情報の保護である。企業の秘密情報が裁判所による救済手段を得るためには，当該秘密情報そのもの及び当該秘密情報の管理の内容が，法令上ないし判例上要求されている基準を充足している必要がある。

我が国において「営業秘密」の保護を担う重要な法律は，不正競争防止法である。同法において法的保護を享受するためには，「営業秘密」の要件の一つである秘密管理性を充足しなけれ

ばならない。我が国の判例上，かかる秘密管理性を充足するためには，①対象情報にアクセスできる者の制限（アクセス制限）と，②対象情報にアクセスした者に，それが秘密であると認識できること（客観的認識可能性）の２つの要素を充足する必要があると考えられている。いかなる場合に秘密管理性が肯定されるかは，これら２要素をどのように解釈するかによるが，この点について，我が国の裁判例は，要求する管理の程度について時代とともにその解釈を変遷させてきている。主な解釈の相違は，要求される管理の水準について，情報の性質，保有形態，さらには，対象企業の規模等を積極的に考慮するか（相対的に考えるという意味で相対説と言われる。），それとも，それらを考慮することなく一律に，客観的に考えるかという点である（客観説）。裁判例を見ると，一時期客観説に傾いた時期も存在したが（その原因としては，営業秘密について刑事罰が拡大強化され，秘密管理性も「刑事罰を課せるほど」のものを要求する雰囲気が生まれたことによると考えられる。），現在は，やや相対説的な考え方に傾いていると考えることも可能である[12]。

もちろん，裁判例の動向については今後も注視していく必要があるが，企業としては，上記に述べた「現状」を踏まえ，事業規模や情報の性質や価値に鑑みた対策を「ベスト・エフォート（最善の努力）」として実践するしかない。裁判例の動向に過度に敏感になる結果，継続的且つ安定的な対応策が取れなくなってしまっては本末転倒である。

以上は，適用法が日本法である場合を前提としているが，これに対して，外国法[13]が適用される場合，当該外国法が営業秘密保護のために要求する水準に合致した管理体制である必要がある。当該外国法の要求水準について事前に把握しておくことが望ましい。

(2) 営業秘密管理における視点

営業秘密管理体制の構築に際して重要な視点として，「モノ」の管理（物的管理）と「ヒト」の管理（人的管理）がある。また，双方を有機的に結合し，営業秘密管理を実効化あらしめるものとして，「組織的」管理がある。企業における営業秘密管理体制の構築に際して，このように分類をすることは，管理体制の構築に必要な対策項目の漏れを防ぎ，実効性のある管理を実現する上で有益である[14]。

また，営業秘密管理の主体として，第一次的には当該企業がある。企業内部における担い手として，前述のとおり，役員等のマネジメントによる陣頭指揮のもと，知財部，法務部，人事部，経営企画部さらにはIT部門が有機的に結合した協働体制が必要不可欠である。さらには，前述した弁護士・依頼者間秘匿特権の確保のためには外部弁護士との協働も重要となるほか，ITについて専門的な知見を携え，必要なリソースを提供する外部ITベンダー[15]も，営業秘密管理における重要な担い手である。

もちろん，営業秘密管理のため，どこまでコストをかけられるかという問題もある。この点については，対象企業においてどれだけ価値ある営業秘密が存在し，流出の危険に晒されているかという点にも大きく関連する。営業秘密が，一旦盗取され又は公知になると価値は喪失してしまう性質を有することに鑑みれば，少なくとも，企業が重要な営業秘密を保有し，それがマーケットにおける競争力確保の源泉となっているような場合，一定範囲でのコスト負担は，自社の競争力獲得に向けた真のコスト・エフィシェンシー実現にむしろ寄与するものである。

(3) 営業秘密としての保有か特許出願か

営業秘密としての保護と特許化による保護のそれぞれにメリットとデメリットが存在する。企業の開発部門により生み出された新規技術に

ついて，特許として公開し，譲渡可能な排他的独占権を獲得すべきか，他社へ公開することなく，自社の事業遂行において営業秘密として秘匿しながら保有すべきか，慎重な判断が必要となる。

特許化ではなく営業秘密として保有すべきとの判断をした以上，直ちに，法的保護を受けるために必要な秘密管理の措置をとる必要があるが，未だ判断がつかない時点においても，将来において営業秘密としての保護を受ける可能性がある技術情報については，営業秘密に準じた管理を行う必要がある。

(4) 営業秘密の特定

営業秘密管理の大前提として，対象となる秘密情報の範囲を明確に特定しておく必要がある。そうすることで，管理すべき範囲が明確になり，本来管理の対象外である情報への混入及びそれに伴う管理体制の欠如という事態を回避することが可能となる。

このように，秘密情報の外縁部分を明確化することは，自社情報と他社情報との区別化につながる。これにより，他社の秘密情報が自社の情報に混入することで，近時問題となっている自社情報を使用する際の足かせとなる事態（いわゆる情報のコンタミネーションないしは汚染の問題）を回避することに役立つ。

(5) 物的管理

物的管理のポイントは，秘密情報の存在形態を確認の上，当該形態に見合った適切な管理を行うことである。

秘密情報の存在形態としては，従来からの紙媒体のほか，電子データ，電子機器のほか，秘密情報が具現化されたものとしての試作品や金型などが含まれる[16)]。

それぞれの秘密情報の存在形態に応じて，秘密管理性の要件充足に向けた管理体制作りが重要である。これらの秘密情報へのアクセスを制限し，秘密情報であることについて外部から客観的に認識可能な程度に明確に記載することは不可欠である。例えば，秘密情報の存在形態がデジタル情報であれば，パスワード化，暗号化により利用制限を設けることができる。その場合の利用者IDやパスワード，さらには暗号については適切に管理される必要であり，秘密情報へのアクセスの有無，時間，用途等を含め，適時にログを取っておく必要がある。万が一秘密情報の流出が発生した場合でも，即時に対処するための証拠作りをしているとの視点が重要である。

その他，営業秘密が保管されている場所についての入退室情報や来客について，履歴やログをとっておくことも非常に重要となり，その過程では，企業におけるIT部門のほか，外部ITベンダーとの協働体制が重要となる。

(6) 人的管理

企業の役員や従業員は，契約書における具体的な条項がなくとも，委任契約ないしは雇用契約に基づき，信義則上の忠実義務や秘密保持義務を負うと理解されている。しかしながら，適切な秘密管理の観点からは，対象者に自らが負う義務について明確に認識させ，秘密保持義務違反の発生を未然に回避するためにも，対象者の役職や地位に応じて，雇用契約や就業規則さらには個別の誓約書の形式で，制限の内容を具体的に規定し，締結する必要がある。そうすることで，万が一秘密情報が従業員等により不正に持ちだされた場合においても，雇用契約や就業規則を，締結済みの「証拠として」直ちに裁判所に提出し，より迅速に差止等の救済手段を申し立てることが可能となる。

競業避止義務についても，基本的には同じことが言えるが，退職者の競業避止義務については，憲法上の職業選択の自由との関係で合理的

範囲内でのみ認められると解されている[17]。競業避止義務の合理性判断基準に，代償措置の内容がある。代償措置に相当するものとして，退職金制限条項と連動させるという取り決めが考えられ，実務上も多く利用されている。

なお，適用法令として日本法以外も考えられる場合，契約準拠法の相違から競業避止義務違反の許容範囲の相違にも留意すべきである。例えば，カリフォルニア州法の適用がある場合，競業避止義務を定める条項そのものが原則として無効と解されている。ことクロスボーダーでの対策が必要な事案においては，弁護士等の外部専門家のアドバイスを受けることをお勧めする。

より高いレベルでの契約内容の順守を促すため，従業員を対象に，情報セキュリティ教育のためのセミナーや外部専門家をまじえたトレーニングセッションの実施は有益である。これら契約の締結及びセミナーないしはトレーニングセッションの実施そのものが，秘密管理性を確保するための証拠となる。

(7) 組織的管理

物的管理，人的管理を実効性あるものにするために，組織的な管理によって補完する。多くの流出事案は，人を通じて行なわれるものであるから，出来る限り「ヒト」に依存しない管理体制を構築していこうとするのが，最近の傾向であろう。但し，究極的に，秘密情報の不正取得をしようと意思決定するのは「ヒト」そのものである。したがって，「ヒト」についての管理を怠ることは，会社における営業秘密の管理体制そのものを否定することになる。

まず，組織的管理の一つとして，物的管理及び人的管理の履行状況について定期的にモニタリングする必要がある。モニタリングの過程で，ログデータ等から，秘密情報の流出の予兆となるべき事象を把握することも可能となり，早期に法的手続を開始することが可能となる。

内部監査の実施も有効であり，監査結果に基づき，改善すべき点があれば改善し，以後の物的管理及び人的管理の具体的内容としてフィードバックが図られるべきである。

(8) 取引に伴う流出事案について

取引（資本・業務提携ないしライセンス等）に伴う営業秘密の流出類型の予防段階における管理としては，基本的には，上記に述べた内容が妥当する。すなわち，秘密情報の特定ができていることを前提に，契約書（合弁契約書やライセンス契約書）において秘密情報の取り扱いや使用制限等に関する条項を明確に規定し，その履行状況の適切なモニタリング（相手方による関連特許の出願や相手方製品の詳細監視を含む）の実施が重要である。

3. 3 秘密情報の流出発生時の対応（有事）

(1) 流出発生時（紛争発生時）の段階的対応

秘密情報の流出が発生した場合における対応については，①流出の疑いが発覚した直後から具体的な紛争解決手続の遂行に向けた戦略を構築する段階である「戦略構築段階」と，②策定された戦略に基づき紛争を遂行する「紛争遂行段階」に分けて検討すべきである。そうすることで，それぞれの段階に応じたベストの対応を取ることが可能となり，具体的な対応策について「漏れ」が発生するのを可及的に防ぐことができる。

(2) 戦略構築段階

1）流出及び紛争の実態の把握

被害発生を回避するため，すでに述べた定期的なモニタリングやアクセスログの確認を通じて，流出を未然に防止することが重要となる。その上で，重要技術情報を把握しているキーパーソンたる従業員が退職する場合，退職前インタビューを通じて，その者が現実に秘密情報に

触れていたか，また当該情報を「持ち出し」そうかについて感触を得ることを試みてみることも検討に値する。例えば，退職時における秘密保持や競業禁止を目的とした誓約書へのサインを求め，それを頑なに拒否してきたような場合には，当該従業員に対する監視の目をさらに強めることができる。流出を試みる者も人間であり，流出についての何かしらのサイン（兆候）が存在する場合もあり得るのである。さらには，当該インタビューにより故意に流出を企てていた者も翻意する可能性もあろう。いずれにせよ，このようなインタビューはメリットこそあれ特段デメリットは見当たらない。

戦略構築のスタートラインは，対象となる営業秘密を特定するとともに，流出の事実を確認するとともに証拠の確保を行う。その上で，法律上の請求にかかる要件充足の分析である。ここでも，企業としては，法律事務所やITベンダーといった外部専門家間の協働作業が重要となる。

想定されるプロセスは，以下のとおりである。

①営業秘密の特定

どのような情報が流出したのか，それは法的に保護を受けるだけの内実を具備しているのかについて分析する。なお，「営業秘密」として法的保護を受けるかについては，適用法上の要件如何に関連する。事案が日本国内にとどまる場合，不正競争防止法上の「営業秘密」として認められるかという点が問題となるが，事案が国境をまたぐ場合，関連国の営業秘密保護法規に基づく要件充足について確認することも必要となる。

特に問題となるのが「秘密管理性」の要件充足性であり，対象となる営業秘密がどのように管理されてきたかについて，客観的な証拠を確保する必要がある。前述した予防段階において，この点についてケアされていれば（弁護士・依頼者間秘匿特権が付与されていればなおよい），有事段階に至っても対応がスムーズであろう。

②流出の事実確認及び証拠の確保

確認すべき事実として，秘密情報の持ち出しの事実，さらには，競業他社とのやりとり，他の従業員に対する勧誘の事実等がある。

確保すべき証拠として，紙媒体によるハードコピーのほか，電子データ，さらには社内外の証人候補や関係者に対する事情聴取の結果得られる陳述が存在する。なお，関係者へ事情聴取する場合でも，その対象者の選別，実施主体や場所等については，十分慎重に検討する必要がある。

また，対象となる秘密情報へのアクセスログを保全，確保しておく必要がある。デジタルデータについてはフォレンジックによりログを保全し，すでに削除されたデータの復元作業を行う。そのため外部のITベンダーとの協働が必要となり，外部弁護士の指示のもと，外部弁護士に報告する形で実施すれば，弁護士・依頼者間秘匿特権を確保することにも寄与する。なお，前述のとおり，デジタルデータの脆弱性の問題から，フォレンジックによる証拠確保は，流出の兆候発覚後直ちに実施する必要がある。

なお，関係者へのインタビューや従業員のPCやEメールを確認する際は，各国の労働法規やプライバシー関連法との抵触もあり得るので，事案が国境をまたぐ場合には特に注意が必要である。

米国の民事訴訟制度に見られる広汎なディスカバリー制度がない日本の民事訴訟制度のもとでは，とりわけ，相手方の侵害行為の具体的態様についての証拠を得るのが困難な場合が多い。民事訴訟法第234条に基づく証拠保全手続の利用を検討できるものの，証拠保全決定に基づく証拠調べは，あくまでも相手方の任意の協力に基づくものであり，相手方が断固として協力を拒否することも想定できる。相手方の任意の協力が得られない場合には，文書提示命令や

検証物提示命令の発令に向けた働きかけを裁判所に行うことも検討されるべきであろう。

③法律上の請求にかかる要件充足の分析

請求の根拠については，適用される法律上の実体的規定によるところとなる。日本において典型的な救済措置として，不正競争防止法に基づく救済措置がある。これらを実際に請求できるかどうかを検討するため，まず，不正競争防止法第２条第１項第４号ないし第９号に列挙されている行為（不正競争行為）[18]の存否を，上記②によって確認された事実に照らし分析する。その上で，同法上の救済措置，すなわち，差止請求（３条），損害賠償請求（４条ないし９条）及び信用回復措置の請求（14条）が認められるかどうかについて，獲得した証拠の内容，証拠価値に照らして分析する。また，同法上，一定の行為類型には刑事罰の適用もあることから（営業秘密侵害罪）[19]，被害者たる企業としては，告訴等の手段の積極的活用も考慮すべきである。

不正競争防止法に基づく請求のほか，具体的事実関係によっては，従業員との個別契約（秘密保持義務，競業避止義務等）違反に基づく差止や損害賠償請求，さらには，不法行為に基づく損害賠償請求も考えられる。戦略策定段階では，漏れのないよう，可能性のあるあらゆる請求権について分析を行うことが肝要である。

事案が国境をまたぎ，適用され得る法律も１つの国の法律に限られない場合，適用され得る法律の実体上の救済手段も多岐にわたる。その場合，各管轄におけるそれぞれの救済手段の実効性，速さ，費用等を総合考慮することで，最善のアクション・プランを構築すべきである。

④訴訟ホールド（Litigation Hold）について

とりわけ米国が管轄地となり得る紛争が発生した場合，（米国等における）ディスカバリー手続の準備として，訴訟の対象となる事案に関連するあらゆる情報を，そのままの状態で保存する必要がある。そこで，当該保存の必要性について，各関連文書保持者に対して的確に通知する必要がある。それが訴訟ホールド（Litigation Hold）と呼ばれるものである。

訴訟ホールドの不手際により，訴訟上不利な立場に追い込まれた例も実在することを肝に銘じておくべきである[20]。適時に（訴訟の可能性があると判断された時点），訴訟ホールド通知を関係各社に発行することを怠ってはならない。

２）紛争解決の場所及び紛争解決の手段の選択

どこ（どの国や地域）で，どのような手続を，いつ，誰に対して開始するかという点については，あらゆる選択肢を洗い出した上で，費用対効果を考えながら，当該事案を前提として（獲得できた証拠を考慮して）企業にとって最良の戦略を導き出す[21]。とりわけ，国境をまたぐ流出事案の場合，戦略上の選択肢の幅も広がるのみならず，検討対象国の歴史や地方保護主義の弊害，相手方企業に対する評価等，考慮すべき要素も多い。

①実体法における保護の内容

具体的な手続を開始させる場所については，それぞれの適用法のもとで，営業秘密がどのような保護を受けるかという点も，他の選択肢との比較を行う上で重要なファクターとなる。

②ディスカバリーを利用するのが得策か

流出の被害者たる企業が退職者や相手先企業に対して権利行使を検討しているが，手持ち証拠に乏しい場合，米国のディスカバリー制度を利用し，先方から有利な手持ち証拠を出させることも検討に値する。

③紛争解決方法

警告書の送付，交渉，訴訟の提起，仲裁や調停等の代替的紛争解決手続（ADR）等，紛争解決手段の選択は極めて重要なプロセスである。具体的事案を前提に，実際に手続をシミュレートすることにより，紛争解決方法をより実践的に選択する必要がある。例えば，営業秘密

が絡む事案であれば，原則として公開される裁判所での裁判よりも，手続について秘密性が保たれ，且つ専門的知識を有する仲裁人を選任できる仲裁手続に親和性がある事案もあるだろう。但し，事案が国境をまたぐ場合，上記紛争解決方法については，管轄としてあり得る国においてそれぞれの手続を開始するとすればどのように進行するか，という観点からのシミュレートが必要である。クロスボーダーリティゲーションに対する高度のマネジメントスキルと経験が問われる。当該分野における専門家との協働が必須と言える。

④保全措置の利用可能性

米国では，暫定的保全措置命令という制度があり，申し立てから短期間で，暫定的な差止を申し立てることが可能である。営業秘密の盗取等が米国でのビジネスに与える影響次第では，利用価値のある制度であると言える。

また，国境を超えて複数の国が関連する事案においては，実際のところ，費用対効果についての慎重な吟味は必要であるものの，複数の管轄地全てで同時に差止を求めることも検討に値する。

⑤行政手続の利用[22)]

中国においては，行政手続の利用により，迅速，簡易かつ比較的低コストにて行政上の命令を得られるメリットがある。その半面，我が国の裁判手続のように，手続において予測可能性や安定性があるとは言い難い。行政手続の利用も慎重に選択する必要がある。

⑥刑事手続の利用

刑事告訴は，公権力による捜査活動につながる可能性があり，とくに相手方の手元にある有力な証拠の取得による事案の全面解決が期待できることもある。しかしながら，よほど営業秘密としての管理が確実でありかつ不正取得の事実が明らかな事案でない限り，告訴状が受理されることを容易に期待できない。また，事案を刑事事件とすることで，世間の目に触れる可能性も高くなることから，企業のレピュテーション管理を難しくすることもある。したがって，刑事手続の利用についても，そのメリットとデメリットとを慎重に考慮する必要がある。

⑦メディアの活用

営業秘密流出の被害者となることで，当該企業のレピュテーション低下のリスクが存在する。そこで，仮に，営業秘密の被害者として報道されても，それを打ち消す形で，訴訟提起の事実を積極的に公表することで，レピュテーションリスクを回避することが可能になる事案もあり得よう。メディアを積極的且つプロアクティブに使うことも検討に値する。

⑧債務不存在確認訴訟の提起

前述のとおり，日本の大手製鉄会社が東京地方裁判所に対して韓国大手製鉄会社を訴えたのに対して，被告たる韓国大手製鉄会社は，韓国において債務不存在確認訴訟を提起した。かかる事実は，日本の大手製鉄会社の日本における訴訟戦略に少なからず影響を与えたものと考えられる。当職の経験でも，営業秘密の不正取得に関して相手方（米国企業）との交渉が収束しなかった事案で，先手を打って日本において債務不存在確認訴訟を提起して，有利な和解に導いた例もある。管轄等の問題はあるが，とりわけ被告企業にとって十分検討価値のある選択肢である。

(3) 紛争遂行段階

戦略構築が完了した場合，あとは構築済みの戦略にしたがって，具体的な紛争解決手続を遂行する。手続の進行の都度，既存の戦略に不備はないか，変更を要する点はないかについて，積極的に分析し，誤りは直ちに修正する。交渉ないしは訴訟手続の遂行過程において，相手方から具体的な反論や証拠が提出される。例えば，退職従業員による秘密情報の流用事案等におい

ては，被告となった元従業員が原告会社に対して悪意を抱いている別の退職従業員から会社の秘密管理体制に批判的な陳述書を取り付けて裁判所に提出することもある。そのような場合，相手方から出された反論及び証拠について，「客観的に」かつ慎重にその内容を精査し，自らの主張及び論拠に与える影響について正確に分析する必要がある。当該分析結果に基づき，自らの主張の論拠に不足する部分があれば「直ちに」，追加の証拠（書証ないし人証）で補強する必要がある。また，交渉や裁判手続遂行の過程で相手方から出された証拠を精査することにより，当初は判明していなかった秘密情報の開示先や使用場所が判明することもある。そのような場合には，直ちに，判明した開示先を被告ないし交渉の相手方に追加することや，新たな手続（他国での仮処分等）の開始も積極的に検討する必要があろう。戦略構築段階で構築した戦略は，構築時点での「ベスト・ジャッジメント」に他ならない。紛争そのものは，相手方の出方や裁判所等の紛争解決機関，さらにはメディアの動向にも左右され得るまさに「生き物」である。紛争遂行に携わる者（会社及び弁護士を含む外部専門家のチーム）は，そのような紛争の性質をふまえ，そのような時々刻々と変化し得る紛争への柔軟な対応が求められる。

営業秘密に関する紛争の「終結」ないし「出口」としては，裁判所による判決及び判決に基づく執行という手段もあるが，判決そのものに不服がある相手方から任意の履行を期待しにくく，また，対象国によっては執行が困難という問題が生じ得る等，必ずしも最良の結果を出すとは限らない。「判決」や「執行」というドラスティックな手段ではなく，相手方への任意の履行の確保を期待し，裁判等の手続コストをより軽減する目的から，営業秘密に関する紛争は，裁判等の手続の開始後でも和解により終結させることも多い。また，和解で終結させることで，判決内で詳細な事実関係が記載されることにより，生じ得るレピュテーション・リスクを軽減させることも可能となる。自社に有利な和解に持ち込むためには，相手方にも裁判所にも，自社の主張は「強い」ということを強く印象づけることが不可欠である。そのためには戦略構築段階における事前準備が極めて重要となることは言うまでもない。また，裁判手続を開始した場合には，手続当初の段階で，いかに裁判官を味方に付けるかが，自社に有利な和解を導くための鍵となる。そのためには，証拠に基づく丁寧な主張を，書面をもって行うことは最低限必要であるし，さらには手続の初期の段階で，裁判官との直接の面談を申し込み，とりわけ「営業秘密」について裁判官に理解してもらうため，図表を効果的に使用した資料を用いたプレゼンテーションを行うことも有効であろう。

3. 4　紛争解決の現場からのフィードバック

予防段階において，粛々と秘密情報の管理を進めていても，いざ紛争が発生してみてはじめて，証拠上不足している部分，ログの取り方等において改善の余地がある部分が発生する。このような紛争解決の現場から出た「生の声」は，よりよい秘密情報の管理体制を構築する上で極めて有用であり，予防段階での秘密管理体制への効果的なフィードバックが期待される。

4．結びにかえて

結局のところ，秘密情報管理について完璧なマニュアルは存在しない。まずは自社の現状把握からスタートし，予防対策及び有事対応における当該企業にとってオーダーメイドとも言えるプロセス（対策）を導き出すのが目的である。そのためには，マネジメントを先頭に，知財部，法務部等の各部門，さらには外部専門家との協働も不可欠である。その点において，秘密情報の管理は企業のコンプライアンス対策と多くの

共通項を有する。まさに，営業秘密保護対策は，コンプライアンスの一環として取り扱われるべきなのである。

注　記

1）経済産業省の知的財産管理指針や知的財産戦略本部が発行している知財推進計画では，知的財産戦略と経営戦略と研究開発戦略とが三位一体となったグローバルな企業戦略が必須である旨指摘する。さらに，「数を競う単純な権利取得・確保ではなく，事業構想や研究開発段階から多次元的な知財マネジメントを適切に行い，自ら仕掛けることも必要」である旨指摘されている（知財推進計画2012年版６頁）。かかる考え方については，その効果が実感しにくいこと，失敗した点を見極めることが難しいこと等の理由により，実効性の点で難しいとの評価もある（中原裕彦「企業の営業秘密管理と知的財産マネジメント」NBL No.975，11頁以下参照）。

2）日本経済新聞　電子版2012年11月22日付記事，同2012年10月25日付記事，2013年４月23日付記事及び同2013年４月24日付記事並びにSankei Biz 2013年４月27日付記事等参照。

3）例えば，資本提携の交渉過程において開示された秘密情報の不正開示等について争われた事案に，東京地方裁判所平成18年３月30日判決（判時1958号115頁）がある。この事案では，不正開示の事実が認められないとして原告の訴えは棄却された。

4）東京地方裁判所平成24年６月１日，知財高裁平成24年12月12日。

5）本件において，原告は，不正競争防止法に基づく請求のほか，不法行為及び債務不履行に基づく主張も行ったが，いずれも裁判所によって否定されている。

6）「営業秘密」について，不正競争防止法第２条第６項は，以下のとおり規定する。

　この法律において「営業秘密」とは，秘密として管理されている生産方法，販売方法その他の事業活動に有用な技術上又は営業上の情報であって，公然と知られていないものをいう。

7）時事通信2007年３月16日付配信記事。

8）日本経済新聞　電子版　2012年４月18日付記事，同2012年５月９日付記事参照。

9）警察庁が民間企業及び教育機関等を対象に実施した「不正アクセス行為対策等の実態調査」（平成23年度版）によれば，「情報セキュリティ対策の必要性を感じているか」との質問に，「必要性を感じている」と回答した者が96.8％にのぼった。しかしながら，自社システムの脆弱性について事実１回も検査したことがない者は74.6％にのぼっている。さらに，「報道やセキュリティベンダーから提供される情報を基に，自社システムの変更や防御措置を講ずるなどの対策を実施」した企業は50.4％に過ぎず，45.3％の者は「実施していない」と回答している。かかる調査結果からも，民間企業等における情報セキュリティ対策は，未だ発展途上にあると言えよう。

10）弁護士・依頼者間秘匿特権の戦略的活用については，高取芳宏著「企業間紛争解決の鉄則20」の49頁以下（鉄則６）が詳しい。

11）弁護士・依頼者間秘匿特権は，米国のみならず，英国等においてもコモンローによって認められているが，ここでは，米国法のもとでの秘匿特権について言及した。

12）この点についての研究成果として，田村善之著「営業秘密の不正利用行為をめぐる裁判例の動向と法的な課題」パテントVol.66，No.6がある。田村教授によると，裁判例の動向として，平成15年に経済産業省により「営業秘密管理指針」が出される直前くらいまでは，管理の程度を比較的緩やかに解されていた時代が長く続いていたが，当該指針の発表後から，次第に厳格に解する判例が続き，平成20年頃，再度緩やかな方向に揺り戻しがあったと分析されている。

13）例えば，米国では，営業秘密はもともと各州のコモンローによって保護されてきたが，州ごとの不均衡を除去する目的で，統一営業秘密法（Uniform Trade Secrets Act, UTSA）が制定され，これを基にした法律が全米の大半の州で制定されている。また，営業秘密の刑事面からの保護については，1996年制定の連邦経済スパイ法が規律している。その他，適用法令として，2012年制定の営業秘密の不正取得に関する明確化法，同年制定の外国及び経済スパイ罰則強化法，さらには，合衆国法典第19編第1337条（第337条）がある。なお，統一営業秘密法に基づく法律の制定を行っていないニューヨーク州及びマサチューセッツ州等では，州のコモンローが適用法と

なる。

さらに中国において，営業秘密は，1993年に制定された反不正当競争法と民法通則における不法行為に関する条項に基づく保護を受ける。

14) 経済産業省が作成した「営業秘密管理指針」（平成15年１月30日　最終改訂平成25年８月16日）及び日本知的財産協会フェアトレード委員会が作成した「秘密情報マネジメントハンドブック」（2013年６月）においても，秘密情報の管理においてかかる分類が用いられており，我が国における多くの企業がかかる分類を採用しているものと考えられる。

15) 外部ITベンダーについては，秘密情報流出確認にかかるモニタリングやログ収集，さらには流出発覚の際のフォレンジックの実施等，予防段階から紛争発生段階に至るまで，企業活動に継続的に関わっていくことになる。したがって，外部ITベンダーの選定は慎重に行うべきであり，具体的には，複数の外部ITベンダーから選出する手続（通常Beauty Contestと呼ばれる）を経ることをお勧めする。

16) 日本知的財産協会フェアトレード委員会が作成した「秘密情報マネジメントハンドブック」(2013年６月）18頁以下参照。

17) 合理的であるかどうかは，一般的に，制限の期間，場所的範囲，制限の対象となる職種の範囲，代償措置の有無等が基準として判断される（フォセコ・ジャパン・リミテッド事件　奈良地裁昭和45年10月23日）。

18) 不正競争防止法第２条第１項第４号ないし第９号における各行為類型は下記のとおり。

①窃取等不正取得（４号）
②不正取得者からの転得者（５号）
③不正取得にかかる事後的悪意者（６号）
④信義則違反（７号）
⑤不正開示者からの転得者（８号）
⑥不正開示にかかる事後的悪意者（９号）

19) 不正競争防止法第21条１項１号ないし７号

20) 2011年９月14日に判決が下されたDuPont v. Kolon Industriesの事案で，裁判所は，米国での裁判の直前に，Kolon社が（Litigation Noticeの不手際から）営業秘密の窃取事実に関するEメール等を破棄したと認定し，Kolon社に対して対象技術を今後20年間世界のあらゆる場所で使用してはならない旨判示するとともに，懲罰的賠償部分を上乗せし，合計９億ドル以上の損害賠償を命じた。

21) 参考として，前掲注10）が詳しい（鉄則７，８，９，10及び11参照）。

22) 本件をはじめ，コンプライアンス関連事案では，民事手続，刑事手続，行政手続，メディア対応の４つの側面から検討すると，取るべき手段についての漏れがなくなる。この点については，前掲注10）に言及がある（鉄則５）。

（原稿受領日　2014年１月14日）