TOKIO MARINE NICHIDO
リスクマネジメント最前線
2013 | No.23

増大する技術情報流出リスクとその対策

技術情報流出は、自社の従業員及び退職者、取引先、ハッキング・盗聴といった外部からの不正アクセス等の様々な経路で発生し、そのリスクを完全に回避することは難しい。本稿では、流出時の法的保護の観点も含め、技術情報を適切に秘密管理する体制の構築について解説する。

1. 技術情報流出防止の重要性

（1）技術情報流出リスクの増大

製造業や情報産業などの多くの企業において、研究開発活動を通して誕生した独自技術は、魅力ある製品やサービスを生み、他社との差別化を実現し、市場における競争力の源となる非常に重要な資産である。もし、これらのうち企業秘密とすべき技術に関する情報が流出して競合他社に利用された場合、企業の競争力は毀損され、当該技術の開発に見合ったリターンを得ることができない事態となる。また、軍事転用可能な技術に関する情報が海外に漏れた場合には、企業の信頼は失墜し、国家の安全保障さえも脅かされてしまう。

現在、グローバル化の進展や新興国の急速な経済発展を受けた国際的な企業間競争の激化、技術やノウハウを知りうる人材の国境を超えた流動化、IT 技術の発展により大容量データの持出しが可能になったこと等を背景として、国内だけでなく国外への技術情報の流出も含めて、そのリスクは高まってきていると言われている。

（2）企業における対策の重要性

技術情報流出リスクの増大に伴い、個々の企業についても対策強化が重要となってきているが、技術情報は無形資産であるため有形資産と比較して管理が難しい。技術情報が流出した場合、直接情報を入手した者に加え、間接的に知り得た者も活用できる可能性があるため、二次的・三次的に影響が拡大する恐れがある。さらに、秘密管理しているからこそ意味のある技術情報については、一旦流出して公知のものとなってしまえば、その価値を回復することは難しい。

技術情報の保護手法としては、特許化と秘匿化の 2 つがある。特許化には排他的独占権を獲得できるという利点があるものの、一定期間経過後には内容が公開されてしまう。一方、企業内で秘匿化する場合、その試みが成功すれば技術情報はほぼ永続的に秘密管理される。ただし、不正な漏洩等があっても法的救済を十分に受けられない恐れがある。

これまで、日本の製造業等では限られた範囲で技術情報を秘密管理する手法が多くとられてきたが、現在の国際社会ではオープン・イノベーションが強く推進されており、このような動きに乗り遅れないためには、企業として市場における他社との相互利益と自社の持続的成長の両方を確保すべく、特許等の知的財産関連法の保護の下で開示すべき技術情報と秘密管理すべき技術情報を戦略的に判別した上で、流出防止の対策を実施していくことが必要だと考えられる。

2. 政府における技術情報流出防止の取組み

技術情報の流出により、国内企業が競争力を失うことで経済発展が妨げられ、時に国家の安全保障さえも脅かされるという観点から、経済産業省では技術情報流出防止に向けた取組みを進めている。

■表 1　営業秘密保護に係る法改正等

年	改正等の内容
1990	「営業秘密」の不正取得・使用・開示行為に対する民事保護規定創設
2003	「営業秘密侵害罪」創設により違法性の高い営業秘密侵害行為に刑事罰導入
2005	「営業秘密侵害罪」罰則強化 →国内処罰規定、退職者処罰規定、法人処罰規定導入等
2009	「営業秘密侵害罪」罰則強化 →従業者等による営業秘密の領得自体への刑事罰導入等
2011	刑事訴訟等の過程で営業秘密内容が保護されるための手続き導入

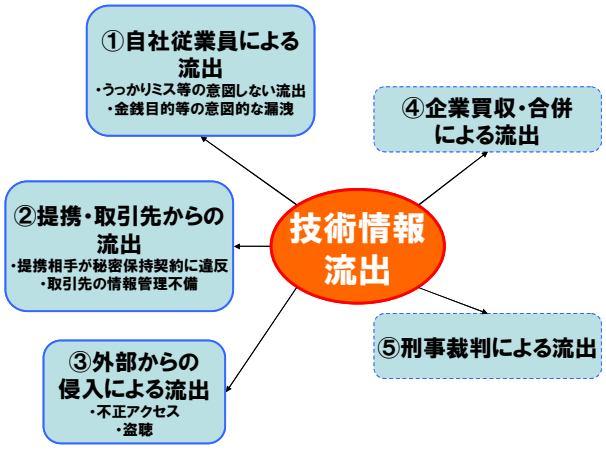
出典：「近事の技術流出事例への対処と技術流出の実態調査について」（経済産業省）より弊社作成

技術情報の保護に関わる法制度としては、事業者間の公正な競争を確保することを目的とした不正競争防止法がある。同法では技術情報も含めた営業秘密の不正取得等を禁止しているが、その罰則に当たる営業秘密侵害罪の構成要件が厳格すぎること等から、これまで十分に活用されてこなかった。また、仮に要件を満たして起訴できた場合にも刑事裁判の公開原則により秘密が公開されてしまう恐れもあった。そのため、経済産業省では実際の流出事例や企業の管理実態を踏まえ、営業秘密侵害罪が技術情報等の営業秘密流出の抑止力となるよう、営業秘密保護に係る法制度の改正等を進めている（表 1）。

この他にも、「技術流出防止指針」（企業の海外展開等で発生しうる技術流出について、その対策等を提示したガイドライン）・「営業秘密管理指針」（適切な営業秘密管理のためのガイドライン）の策定、技術流出に関する実態調査の実施等、企業が技術情報流出防止に取り組む上で有用と考えられる情報も発信している。また、安全保障に関わる機微な技術情報については、外国為替及び外国貿易法（以下、外為法）による規制強化等の取組みが進められている。

3. 技術情報流出の実態

先に述べたように技術情報の保護手法には特許化と秘匿化の 2 つがあるが、以降は個々の企業での対策が特に重要となる「秘密管理されている技術情報」にスポットを当てて、流出の傾向及び実施すべき対策を整理していく。



■図 1　技術情報の流出経路

出典：「技術情報等の適正な管理の在り方に関する研究会報告書」（経済産業省）より弊社作成

図 1 は技術情報の主な流出経路をまとめたものである。「①自社従業員による流出」については、メール誤送信や PC の置き忘れ、私用パソコンにコピーしたデータのファイル交換ソフトを介した流出等の意図しない流出と、金銭目的での競合他社への情報の売り渡し等の悪意のある意図的な漏洩が挙げられる。秘密保持契約の要求が不十分といった理由から、退職者に対する牽制とならず、転職先で情報を漏らすケースも含まれる。「②提携・取引先からの流出」には、取引先企業の情報管理体制の不備から図らずも情報が流出してしまうケースや、提携先企業が意図的に秘密保持契約に違反して技術情報を流用するケース等がある。「③外部からの侵入による流出」は、外部者からの情報システムへの不正アクセスや盗聴によって情報が流出する場合である。

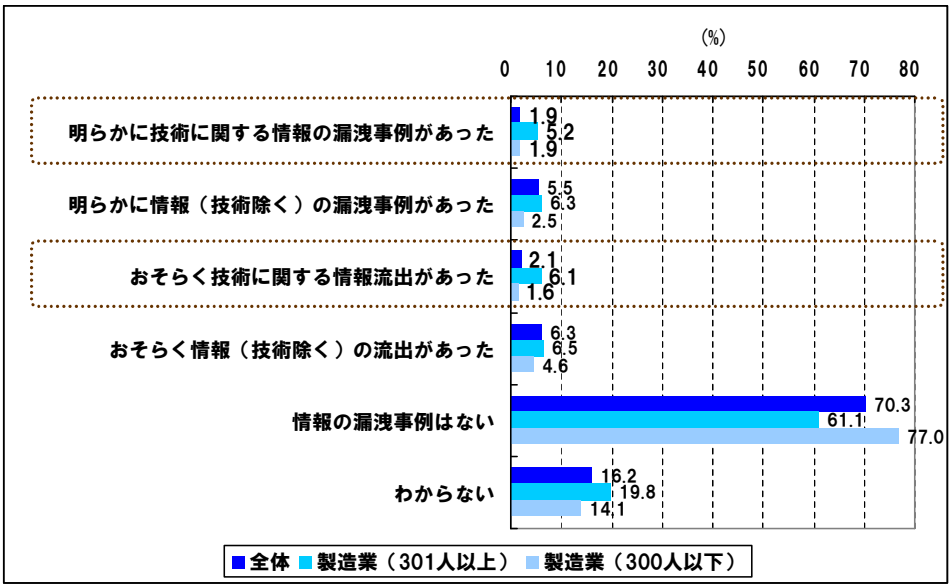
「④企業買収・合併による流出」は、相手企業に技術情報が流出したとしても、買収・合併後も当該技術情報を利用した企業活動が継続可能という点から、必ずしも流出元の企業に悪影響のみを及ぼすものではないと考えられる。ただし、リストラや業界再編を受けた買収や合併、事業切り離し、新会社設立等の動きの中で、当事者となる企業間の情報管理レベルの違いにより、第三者に技術情報が流出してしまう可能性もある。また、買収により安全保障に関わる技術が海外に流出するという事態は回避しなくてはならないため、軍事転用の可能性が高い技術を保有する製造業の外資規制対象への追加等、外為法の改正が行われている。

「⑤刑事裁判による流出」については、前述のように 2011 年に訴訟過程における営業秘密保護の手続きが整備されている（図 1）。

以上のことから、企業が優先的に対策を講じるべきは①・②・③の「人」を通じた技術情報の流出であると考えられる。2012 年度に経済産業省が実施した調査[1]では、過去 5 年間に人を通じた営業秘密（技

[1] 経済産業省「営業秘密の管理実態に関するアンケート」

術に関する情報）の漏洩が、明らかにもしくはおそらくあったと回答した企業は全体の 4.0%、技術情報の重要性が高い製造業、特に従業員数 301 人以上の企業においては 11.3%となっている（図 2）。

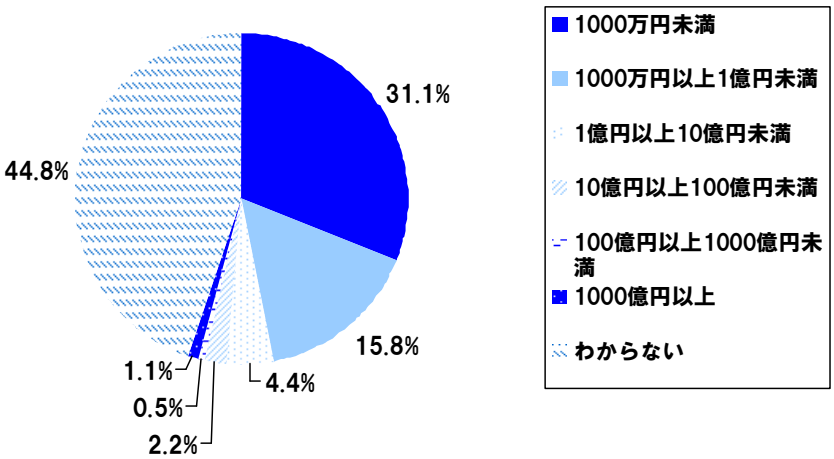


■図 2　人を通じた営業秘密の漏洩実態（全体及び製造業）

出典：「「営業秘密の管理実態に関するアンケート」調査結果（確報版）」（経済産業省, 2012 年）より弊社作成

※全体：n=2969、製造業(301 人以上)：n=555、製造業(300 人以下)：n=566

また、技術情報以外の営業秘密も対象となっているが、漏洩による損害についての問いに対しては、企業によって「1000 億円以上」（1.1%）という回答も見られた（図 3）。10 億円以上の損害が生じていると回答したのは全て製造業の企業であった。

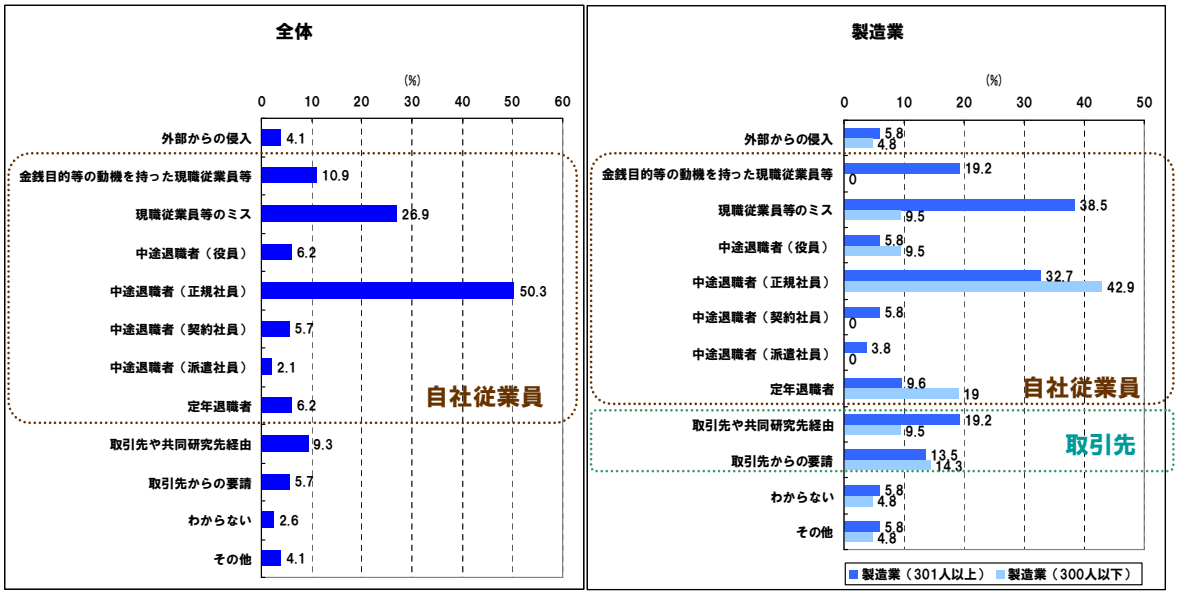


■図 3　人を通じた営業秘密の漏洩による推定被害額

出典：「近事の技術流出事例への対処と技術流出の実態調査について」（経済産業省, 2012 年）より弊社作成

※n=183、複数回流出の場合は合計額。

同調査によれば、営業秘密の漏洩者として全体で最も多かったのは「中途退職者（正規社員）」（50.3%）であり、次いで「現職従業員等のミス」（26.9%）、「金銭目的等の動機を持った現職従業員等」（10.9%）となっている（図 4）。製造業について見ると、従業員数 301 人以上では「現職従業員等のミス」・「中途退職者（正規社員）」・「金銭目的の動機を持った現職従業員等」・「取引先や共同研究先経由」、従業員数 300 人以下では「中途退職者（正規社員）」・「定年退職者」・「取引先からの要請」が上位に挙がっている。全体結果と比較すると、製造業では取引先との回答が多くなっている。



■図 4　営業秘密の漏洩者（全体及び製造業）

出典：「「営業秘密の管理実態に関するアンケート」調査結果（確報版）」（経済産業省, 2012 年）より弊社作成

※全体：n=193、製造業（301 人以上）：n=52、製造業（300 人以下）：n=21

4. 企業が実施すべき対策

ここでは、企業が技術情報流出防止のために実施すべき対策のポイントとして、経済産業省が策定した「営業秘密管理指針」を参考に、技術情報が営業秘密に該当するための要件と情報管理の概要について説明する。「営業秘密管理指針」は、不正競争防止法の改正に伴い改訂が重ねられていることに加え、具体的な管理策や判例を紹介することで、企業における実効的な営業秘密管理を促すものとなっている。同指針に基づいた管理を実行することで、技術情報の流出予防につながるだけでなく、流出時に法的保護を受けられる可能性も高まると考えられる。

（1）営業秘密の定義と民事・刑事的保護

企業が主観的に企業秘密であると主張したとしても、それが定められた営業秘密に当たらなければ、法的保護を受けることはできない。不正競争防止法では保護の対象となる「営業秘密」を表 2 の要件を満たす技術上、営業上の情報としている。

営業秘密に該当すると認められた場合には民事的保護を受けられるので、不正に取得・使用・開示された際、営業上の利益の侵害に対する差止めと損害賠償、営業上の信用回復に必要な措置を求めること

ができる。

さらに、不正に利益を得る、企業に損害を加えるといった目的による悪質なケースについては、営業秘密侵害罪が適用されて刑事罰の対象となる。また、日本国内で管理される営業秘密であれば、その不正使用・開示が国外で行われたとしても処罰の対象となる。民事・刑事いずれについても、訴訟において営業秘密が保護されるよう秘密保持命令等の特別措置が導入されている。

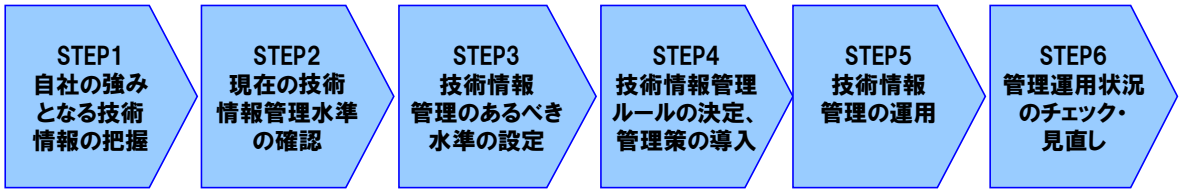
■表 2　営業秘密の要件

①秘密管理性	■事業者によって秘密として管理されていることが客観的に認識される（以下のような管理をしている）ことが必要。 ・　情報にアクセスできる者を特定している ・　情報にアクセスしたものが、その情報を秘密だと認識できる状態にある □事業者が秘密として管理していれば、記憶して持ち出された情報、従業員が体得したノウハウも営業秘密に該当。（ただし管理の難しい個人の技能等は営業秘密とはなりにくい。）
②有用性	■事業活動に有用であることが客観的に認識されることが必要。 □将来の事業に活用できる情報や、「ある手法が役立たない」といった間接的に有用となる失敗情報にも有用性は認められる。 □公序良俗に反する情報は有用性がないと判断される。
③非公知性	■保有者の管理下以外では一般に入手できない状態にあることが必要。 □一般に入手可能な書物等に掲載されている場合、非公知性は認められない。 □複数の人物が知っていても、守秘義務が課される等一般に知られていなければ非公知性があると考えられる。

出典：「営業秘密管理指針（2011 年 12 月改訂版）」（経済産業省）より弊社作成

（2）技術情報の管理

技術情報を営業秘密として適切に管理するためには、図 5 に示す手順を参考に体制を構築することが有効だと考えられる。



■図 5　技術情報管理体制の構築手順

出典：「営業秘密管理指針（2011 年 12 月改訂版）」（経済産業省）より弊社作成

STEP4 で導入する管理策としては、媒体の施錠保管や保管場所への入退室制限（物理的管理）、ウィルス対策ソフト導入やアクセスログの取得・チェック（技術的管理）、従業員への教育・研修や取引先との秘密保持契約の締結（人的管理）等が挙げられる。

技術情報に限らず営業秘密を管理する上で最も重要なことは、構築した管理体制が実効性を持って機

能することである。例えば、書類のラベリング等の管理策が形式的な場合や、技術情報の内容を精査せずに部署単位等のおおまかなアクセス制限に止まっている場合には、営業秘密としての保護を受けられなくなってしまう恐れもある。実際に、立入り禁止と表示した場所への入退室が自由であった、施錠管理されていなかったといった理由から、営業秘密の要件である秘密管理性が否定された判例もある。そのため、STEP6 で管理策の実施状況やルールの遵守状況をチェックし、必要に応じた見直しを行うことには大きな意味があると言える。

前述の経済産業省の調査では、営業秘密の主たる流出経路として退職者も含めた自社従業員が挙がっていることから、人的管理を十分に実施していくことも重要となる。どの技術情報が営業秘密に該当し、どのような取扱いが求められているのか、自らに課せられた守秘義務はどのような内容なのかを周知徹底し、従業員の意識を高めていくことが大切である。また、退職者に秘密保持を要求したいと考える場合には、不正競争防止法による法的保護を受けることも視野に入れ、退職時にも、できる限り秘密保持契約を締結して退職者の義務を明確化しておくことも必要となる。

なお、技術情報の管理においては、全ての情報に対して高度な管理策を導入する必要があるわけではない。情報流出のリスク（影響度や頻度等）を見極め、管理策導入により業務効率や従業員の士気の著しい低下が起きないかといった点も考慮しながら、企業の実態に見合った管理を進めていくことが望ましい。

5. おわりに

企業が成長を続けていく上で、技術、ノウハウ、図面等の技術情報は欠かすことのできない重要な資産であるが、それらは形を持たないために、どのような技術情報を保有しているのか十分に把握・整理できていない、適切な管理が行われていないといったケースも少なくないと考えられる。

技術情報流出のリスクが高まっている現在の状況は、企業が自社の技術情報及びその管理体制を見直し、対策強化に取組む好機だと捉えることもできる。その取組みが技術情報流出防止だけでなく、見落としていた新たな資産の発掘につながる可能性もある。

本稿が、技術情報の保護に関心を抱く方々に有用な情報を提供できるものとなれば幸いである。

（2013 年 5 月 21 日発行）

東京海上日動リスクコンサルティング株式会社
ビジネスリスク事業部 ビジネスリスク第一グループ
〒100-0005 東京都千代田区丸の内 1-2-1 東京海上日動ビル新館 8 階
Tel.03-5288-6712
http://www.tokiorisk.co.jp/

