企業経営と営業秘密管理

弁護士　中務尚子

１．なぜ営業秘密管理か

自社の情報が漏洩し、長年に渡って積み上げられた技術が競業会社の手に渡り、短期間で競業品が市場に出回ってしまうという事件が後を絶ちません。最近では、新日鐵住金が韓国のポスコ社を訴えた営業秘密漏えい事件（平成２７年９月に和解）、あるいは東芝が韓国のＳＫハイニックス社を訴えた営業秘密漏えい事件（平成２６年１２月に和解）などの大型案件が顕在化し、世間の耳目を集めました。現在、最も問題視されているのは、日本企業の重要な製造技術が海外からねらわれ、従業員を介在してやすやすと外国企業に流出してしまうという現実です。

このような技術流出は、日本企業ひいては日本産業の発展を著しく阻害するため、官と民が連携して、強い危機感をもって対応すべき問題と認識されています。平成２６年９月、経済産業省の産業構造審議会知的財産分科会に営業秘密の保護・活用に関する小委員会が設置され、営業秘密の保護強化、不正競争防止法の改正、営業秘密管理指針の改訂などについて、内容の濃い活発な議論がなされました。平成２７年２月にはそのとりまとめが発表され、不正競争防止法の改正に至っています。

企業から技術や情報が漏洩してしまう原因には様々なものがあります。相手企業が自社従業員のうちキーとなる人物を見定めて巧妙に接触、結局、その従業員を介して不正に漏れたというケースが多く見られますが、他方で、深く考えることなく安易に自社の情報を第三者に渡してしまい取り返しがつかなくなったというケースもあります。

知的資産である技術やノウハウは、企業の経営戦略において、収益を生み出す源であり、他社と自社を差別する競争力という意味で代え難い価値を有しています。自社の技術や情報を適切に守り、知的資産の不正な流出を防ぐため、情報管理の重要性を強く認識し社内で実効性のある管理体制を構築することが肝要です。

２．営業秘密保護の法的枠組み

営業秘密を保護するための法的枠組みには、主として不正競防止法によるものと契約によるものが考えられます。

不正競争防止法は、営業秘密の不正取得や不正開示などの行為を不正競争行為としており（不正競争防止法２条１項４号から１０号）、万一、自社の営業秘密が侵害される場合には、不正競争防止法に基づく差止めや損害賠償等の権利行使ができます。

契約による保護とは、取引先や従業員との間で秘密保持契約などの契約を締結することによるものであり、不正競争防止法上の営業秘密に該当しない情報についても保護を図ることができます。

不正競争防止法において、情報は、秘密管理性、有用性、非公知性の３つの要件を満たす場合に営業秘密として保護されます（２条６項）。秘密管理性とは、その文言どおり、「その情報が秘密として管理されていること」です。有用性とは、その情報が客観的にみてその企業の事業活動に有用な情報であること、非公知性とは、その情報が一般的に知られていないか容易に知ることができないことです。

これら３つの要件のうち、実際の事例においては「秘密管理性」の有無が問題となる場合が多く、裁判例において、ある情報が秘密管理性を満たすというためには、その情報にアクセスできる者が制限されていること（アクセス制限の存在）とその情報にアクセスした者にその情報が営業秘密であることが認識できるようにされていること（認識可能性の存在）の２つが主なポイントとされています。

３．情報管理のための視点

企業が自社の情報を管理するにあたって、いくつかの視点を持つことが重要です。

例えば、不正競争防止法にいう秘密管理性要件を満たし、法的な保護を受けることができるための管理レベルと、現場において、個々の技術情報の性質や重要度等より、自社の技術流出を現実に防止するために必要な事実上の管理レベルは異なります。そうすると、あくまで不正競争防止法上の保護を受けることができる管理レベルを基礎としたうえ、現実の技術流出防止のためにいかなる措置が必要かを考えることになります。より高度な管理を要する種類の情報もありますし、海外からのサイバー攻撃に備えなければならないような特殊なケースもあるでしょう。

次に注意すべきなのは、経済産業省による指針の内容と裁判所による判断内容が必ずしも一致しないという点です。

経済産業省による「営業秘密管理指針」は、平成１５年１月３０日に制定、何度か改訂が重ねられ、平成２７年１月２８日に全面改訂されました。従前の指針は、情報管理水準として一般的な管理方法と高度な管理方法の２つを区別した非常に多様な例を示しており、実際に何をすればよいのかが捉えにくいといった指摘がありました。

平成２７年の全面改訂後の指針は、営業秘密管理について、「営業秘密保有企業の秘密管理意思が、具体的状況に応じた経済合理的な秘密管理措置によって従業員に明確に示され、結果として従業員が当該秘密管理意思を容易に認識できることが必要」と述べたうえ、１）秘密情報と一般情報

の合理的区分と２）営業秘密であることを明らかにする措置があればよいとしています。すっきりとわかりやすい内容になりました。例えば紙媒体の情報の場合、その情報が一般情報から区分されたうえで「マル秘」と表示すればよいとされており、従前の指針に比べ要件が緩やかになった印象を与えます。ただし、指針は行政によるガイドラインであり、不正競争防止法の解釈や事案ごとの判断をするのはあくまで裁判所です。指針が裁判所を拘束するものではありませんので、これまで同様、裁判例における判断基準をきちんと認識しておくべきです。

３つめの視点としては、不正競争防止法の法人への罰則が強化されていますので、自社の技術や情報を守るという本来の視点以外に、第三者の秘密情報をうっかり不正に取得してしまわないという視点、第三者の秘密情報を適正に取得した場合であっても、自社の情報と第三者の秘密情報を区別して管理し、これらを混在させないための視点があげられます。例えば、中途採用者の面接の際のインタビュー等は、その者が前職において接した秘密情報を取得しないことを意識した内容にすべきです。

４つめとして、情報管理体制は企業経営に資するものでなければ意味がありませんので、自社の営業秘密管理について、各部署が連携した戦略的あるいは多角的な視点を持つことが重要です。

４．裁判例にみる判断基準

これまで営業秘密が問題となった過去の裁判例においては、例えば世界的にも稀少な技術情報などのように不正取得された情報の重要性が高い場合や、不正取得の態様が悪質である場合、あるいは企業規模が小さい場合などには、秘密管理性の要件を緩やかに認定される傾向があります。ただし事案によっては救済的な意味会いがある場合もありますので注意が必要です。裁判例の判断基準は必ずしも一貫しているわけではなくケースバイケースであることを認識すべきでしょう。

また、営業秘密の侵害案件では、原告は、その情報の漏えい経路を明らかにし、侵害者に責任追及する証拠が必要となりますが、侵害者による不正取得や不正開示の立証には相当な困難が伴います。

平成２７年の不正競争防止法改正により、被告による使用に関する推定規定が新設され（５条の２）、民事訴訟において、原告が、被告が営業秘密を不正取得したこと、及び、当該営業秘密が物の生産方法に係わるものであることを立証した場合には、被告による営業秘密の使用を推定することとされました。これまで原告において被告による秘密情報の使用を立証することは非常に難しかったのですから原告の立証が相当軽減されたわけです。しかしながら情報の漏洩経路、すなわち被告による不正取得や不正開示の立証に依然として困難が伴うことに変わりありません。

したがって、自社の情報管理体制を検討するにあたっては、上記のような不正取得等の立証の困難性を認識しておくことも重要です。電磁的ファイルに技術的措置を施したり、コンピューター上のファイルへのアクセス記録とその記録の保存が有用です。加えて過去の裁判例のうち不正取得等の立証に奏功した事案を分析してみる、自社の情報の漏洩ルートを具体的に想定して対策を検討することなどが考えられます。

５．具体的な管理のポイント

営業秘密の管理は、まずもって「秘密情報の特定」です。自社の強みとなる知的資産を把握のうえ、その資産を構成する個々の情報を抽出し、そのなかからオープンにせず秘匿すべき情報を特定することになります。ただし、あれもこれもと広範な情報を安易に秘密指定してしまいますと、その情報に多くの人がアクセスすることになるのですから、必然的にアクセス制限が緩くなってしまい、その情報が秘密であると認識できることができなくなって、かえって秘密管理性が失われるリスクが生じることに気をつけてください。

次に、特定した秘密情報について、秘密性の度合いによる分類をなし、秘密である旨の表示をします。

そして企業の規模、情報の重要性、利用頻度などに応じて最も合理的な管理方法を選択します。分離保管等による秘密情報と一般情報との区別、マル秘などの秘密表示、パスワード等によるアクセス制限が必要と考えられます。そして、例えば対象となる重要情報にどうしても数多くの従業員が頻繁にアクセスする必要がある場合には、従業員との間で対象を明確にした秘密保持契約を締結する、外部からのアクセス制限を強くするなどについて検討を加えることになります。

ところで、営業秘密管理は、いったん体制ができればそれでよいというものではなく、定期的な見直しが必要となります。時間の経過とともに秘密情報の一部が公知情報となることは多々見られ、そうなれば、せっかくの特定や区別が意味を失うのです。そのような場合には一般情報と秘密情報が混在することとなって区別が曖昧となり、秘密管理性が失われるリスクが生じることに注意してください。

６．おわりに

情報管理にあたっては、自社の技術を守るという意識を企業全体で共有し、現場の技術者や営業の担当者が安易な考えを持たぬようにし、中長期的な防衛を考えてください。

日本には、素晴らしいモノづくりの技術、ノウハウ、長年にわたって積み上げてきた情報があるのに、ガードが低いことが多々見られます。自社

の重要技術や情報を不正に流出させないことは、まさに企業のリスク管理の一つです。企業の技術情報は、多数の技術者の努力の結果生み出されます。完璧な管理体制を敷くことは現実的ではなく、流出予防には限界があるのです。そのような現実を認識したうえで、自社の情報を適切に管理し、自社の重要な資産である技術、情報を適正に守り抜いてください。