営業秘密官民フォーラムメールマガジン掲載コラム　第49回

営業秘密漏洩の早期発見

弁護士知財ネット
弁護士　　松本　幸太

１　はじめに

自社の営業秘密を守るには、適切な営業秘密管理体制をとり、情報漏洩を「未然に」防ぐということが何よりであるのは間違いありません。
また、仮に情報が漏洩してしまった場合に、当該情報について、不正競争防止法上の営業秘密として法的保護をうけるためには、その情報が秘密として管理されていること（秘密管理性）が必要です。
このような秘密管理措置の重要性については、すでに本コラムでもご紹介されているところであり、経済産業省の「営業秘密管理指針」を参考に、各社ごとの管理体制をとられているところかと思います。

他方、企業が営業秘密の管理措置を適切に講じたとしても、その漏洩を完全に防ぐことができるとは限りません。サイバー攻撃をはじめとする情報漏洩手口の高度化、従業員の故意による漏洩など、様々な要因をすべて排除して営業秘密を守り続けるということができるというのは、もしかすると幸運なことなのかもしれません。

もし、営業秘密が漏洩してしまったら・・・。
会社としては、速やかに漏洩した原因を特定し、漏洩した情報を回復させ、またさらなる情報漏洩を防止する必要があることは言うまでもなく、そのためには、「漏洩を早期に発見する」ことが重要です。
今回のコラムでは、典型的な営業秘密の漏洩事例をご紹介しながら、漏洩発覚の端緒を考えてみたいと思います。

２　漏洩のルート

営業秘密の漏洩を早期に発見するためには、まず、どのようなルートから漏洩が発生するのか、その類型を把握しておくことが重要です。

情報漏洩に関する報道などをみていると、企業のサーバーに外部から不正なアクセスがなされ情報が盗まれたといったような、いわゆるサイバー攻撃の事件を目にすることは多いかもしれません。つい先日も、大手通信会社の海外拠点サーバーが何者かにより不正アクセスを受け、厚生労働省の通信ネットワーク工事等の情報が流出したという報道もありましたし、新型コロナウィルスの研究に関して不正アクセスの危険があるとしてＦＢＩや米国土安全保障省のサイバーセキュリティー機関（ＣＩＳＡ）が注意喚起を促した、といったニュースもありました。
「企業のホームページが改ざんされた」とか「なりすましのＩＤでログインがあった」というレベルの事件まで含めると枚挙にいとまがないところです。

他方、独立行政法人情報処理推進機構（ＩＰＡ）が以前に実施したアンケートによると（※１）、営業秘密漏洩の２大ルートとして、「現職従業員等のミスによる漏洩」「中途退職者（正規社員）を通じた漏洩」が挙げられており、現実的なルートとしては、現職・退職者を含め、従業員が関与したものが多いといえそうです。

経済産業省がまとめている「秘密情報の保護ハンドブック～企業価値向上に向けて～」（以下、「ハンドブック」）（※２）においても、漏洩事案への対応がまとめられておりますが、その中では、漏洩のルートについて、
①従業員等からの漏洩
②退職者等からの漏洩
③取引先からの漏洩
④外部者からの漏洩
の４つに大別されており、非常に参考になります。以下、この４類型について、それぞれの漏洩の兆候について検討したいと思います。

３　類型別の漏洩兆候

①　従業員等からの漏洩について
まず、従業員等からの情報漏洩の兆候としては、以下の例が挙げられています（ハンドブック 122 頁　6-1(1)①）。

- （業務上の必要性の有無に関わらず）秘密情報を保管しているサーバーや記録媒体へのアクセス回数の大幅な増加
- 業務上必要性のないアクセス行為
  ex）担当業務外の情報が保存されたサーバーやフォルダへの不必要なアクセス

ex）不必要な秘密情報の大量ダウンロード
ex）私物の記録媒体等の不必要な持込みや使用

- 業務量に比べて異様に長い残業時間や不必要な休日出勤（残業中・休日中に情報漏洩の準備等を行う従業者が多いことから兆候となり得る）
- 業務量としては余裕がある中での休暇取得の拒否（休暇中のＰＣチェック等による発覚を恐れるため兆候となり得る）
- 経済的、社会的に極めて不審な言動

ex）給与に不満を持っているにも関わらず急激な浪費をし始めた
ex）頻繁に特定の競合他社と接触している

当然のことですが、会社の営業秘密にアクセスすることが業務上不可欠の場合には、従業員が営業秘密にアクセスしたとしても、それ自体何ら不自然ではありません。したがって、「業務上必要がない」にもかかわらず営業秘密にアクセスしていないか、「必要以上に」大量のアクセス、ダウンロードはないか、といった点が判断のポイントになります。

また、営業秘密をできる限りカテゴリー別に管理し、それぞれアクセス権限が異なる仕組みをとることで、当該営業秘密にアクセスする必要があるかどうかの判断をできるようにしておくことも望ましいといえます。
なお、営業秘密の管理措置の具体例については、営業秘密管理指針（平成 31 年 1 月 23 日改訂版）もご参照ください（※３）。

② 退職者等からの漏洩について
退職者等からの情報漏洩の兆候としては、以下の例が挙げられています（ハンドブック 123 頁 6-1(1)②）。

- 退職前の社内トラブルの存在
- 在職時の他社との関係

ex）競合他社から転職の勧誘を受けていた

- 同僚内の会話やＯＢ会等で話題になっている、元従業員の不審な言動

ex）競合他社に転職して、前職と同じ分野の研究開発を実施しているとの取引先からの情報提供

- 退職者の転職先企業が製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準となった

退職者からの漏洩の兆候の場合には、当該従業員が会社を辞めた後に競合他社に転職しているかどうかが重要なポイントです。
もっとも、従業員が自分のノウハウ・スキルを活かそうとするならば、必然的に同分野の会社に転職する可能性は高いと思われますので、退職前後の動き（退職前の会社内でのトラブルの有無、賃金水準が妥当だったかどうか）や多数の社員が競合他社へ転職していないかといった事情もあわせて考慮する必要があります。

なお、ハンドブックには「退職者の転職先企業が製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準となった」というような例が兆候として挙げられていますが、この点を検討するにあたり、営業秘密が他社に持ち込まれたからといってすぐに他社の品質や機能が大幅にあがるとは限らないことに留意する必要があります。

例えば、顧客名簿のようなものならともかく、当該営業秘密が高度の技術情報の場合、その営業秘密によって即座に漏洩先会社の製品が完成するとは限らず、営業秘密を利用した開発実験を行い、評価実験をし、従来の製品に実装する、といった一定の開発工程を経ることも想定されますし、生産のために新規製造ラインの導入が必要な場合もありえます。
そのため、漏洩した営業秘密の内容や自社・他社の製品の種類等を考慮し、一定のタイムラグが生じることを踏まえた分析が必要でしょう。

③　取引先からの漏洩について
取引先からの情報漏洩の兆候としては、以下の例が挙げられています（ハンドブック 123 頁 6-1(1)③）。

- 取引先からの突然の取引の打切り
  ex）自社しか製造できないはずの特別な部品について、発注元からの部品発注が途絶えた
- インターネット上での取引先に関する噂
  ex）インターネット掲示板、ＳＮＳ、ＨＰ等において、自社の非公開情報や自社製品との類似品が取り沙汰されている
- 取引先からの、取引内容との関係では必ずしも必要でないはずの業務資料のリクエストや通常の取引に比べて異様に詳細な情報照会
- 自社の秘密情報と関連する取引先企業の商品の品質の急激な向上
- 自社の秘密情報と関連する分野での取引先の顧客・シェアの急拡大

取引先からの情報漏洩に関していえば、取引開始前（あるいは取引検討の開始前）に秘密保持契約（以下、「ＮＤＡ」）を締結することは広く定着してきているように感じますが、ＮＤＡ締結

後に、どのような情報を相手方に開示するのか（開示している秘密情報の範囲が適切かどうか）の検討については不十分な企業も多いのではないかと思います。

また、ＮＤＡにおいては、秘密保持契約の目的が達成され、あるいは不達成が確定した場合に、営業秘密の返還・廃棄をすることを相手方に義務づける条項を定めておくべきですが、実際に返還・廃棄がされているかどうかについては、必ずしもこれを履行していないケースも見受けられます。

「秘密情報が電磁的データの場合、複製が容易であり、返還・廃棄条項はあまり実効性はない。」という意見もあるかもしれません。しかし、営業秘密の返還・廃棄を求める姿勢を示し、そして現実に返還させ、廃棄証明を提出させることで、自社の営業秘密であることを相手方に対して再認識させる効果もありますし、営業秘密を開示した側にとっても、自社の営業秘密であることを自覚する重要な機会ですので、やはり返還・廃棄は実施させるべきでしょう。
そうした対応をすることで、結果として、その後の取引先の動向を意識し、営業秘密の漏洩・不正使用について認識しやすくなるという効果もあるといえます。

④外部者からの漏洩の疑い
外部者からの情報漏洩の兆候としては、以下の例が挙げられています（手引 124 頁　6-1(1)④）。

- 自社における事件の発生
  ex）社員証・パスワードなどの流出事件の発生

※　流出の態様としては、典型的には盗難行為であるが、巧みな話術による聞出し、盗み聞き・盗み見等を通じた流出があり得ることにも留意
  ex）社員の机上の物など、オフィスにおける盗難事件の発生

- 自社会議室における偵察機器（盗聴器など）の発見
- 競合他社等での秘密情報漏洩、不法侵入等の事案発生（類似の技術を持つ自社の情報についても狙われやすいと考えられるため兆候となり得る）
- ウィルス対策ソフト、セキュリティ対策機器による警報
- 自社の秘密情報それ自体ではないが、それと不可分一体のはずの情報が漏洩していること
- 電話、メール等を受信した関係者からの通報
  ex）自社の顧客名簿に記載された者が、競合他社から営業の電話を受けたが、その競合他社に連絡先を教えた覚えがないため、不審に思ってその旨連絡をしてきた
  ex）他所における侵害を調査していたセキュリティ調査機関が、侵害されたサーバーにおいて自社の情報を発見したと連絡してきた

外部者からの漏洩については、不法侵入による盗難や盗み見・盗み聞きなどもありえないわけではありませんが、情報の電子化やサイバー攻撃の高度化といった点を鑑みると、その多くはネットワークを通じての漏洩ではないかと思われます。

クライアントに話を伺うと、一定規模以上の会社ですと、外部からの不正アクセスがあった場合には必ずアラートがなり、また、アクセスログも全て記録されるといったセキュリティシステムを導入しているところが多いようです。
外部からの不正アクセスに対応するためには、一定のコストをかけてシステムを構築することは不可欠ではありますが、とはいえ、敵もさる者、どんなに高度のセキュリティ対策を講じたとしてもまた新しい手法のサイバー攻撃が登場する、という鼬ごっこ状態となります。
サーバー等の情報機器をインターネットと完全に遮断して管理する（スタンドアローン型）といった物理的な対策もありえますが、すべての営業秘密につきそのような方策をとることは現実的には難しいでしょう。やはりそれなりのコストを投じてセキュリティ対策を講じなければ、営業秘密漏洩は防げませんし、そもそも気づくことすらできないということにもなりかねません。

なお、「サイバーセキュリティ経営ガイドライン Ver2.0」（経済産業省・独立行政法人情報処理推進機構）（※４）においては、
- 重要業務を行う端末、ネットワーク、システム又はサービス（クラウドサービスを含む）には、多層防御を実施する
- アクセスログや通信ログから当該イベントが発生していないか、検知した場合には速やかに関係者にアラートを上げるなど適切な対処を行えるような体制を整える
- 従業員に対する教育を行い、適切な対応が行えるよう日頃から備える

といった具体的なセキュリティ対策が紹介されておりますので、こちらもご参照いただければと思います。

４　情報漏洩の疑いがあった場合の対応

以上のような兆候から情報漏洩を感じとった場合、次のステップとして、その疑いがどこまで確信に近いものなのかの調査を実施し、最終的には法的手続まで意識した証拠集めをすることになるでしょう。
調査方法は、記録の収集、関係者ヒアリングの実施、さらにヒアリングから得られた供述の裏付証拠の収集等、多岐にわたります。並行して、営業秘密漏洩の影響範囲を検討し、適切な手法の選択（民事裁判、刑事裁判の可能性の分析や、また漏洩先への警告書の送付等）はもちろん、再発防止策の検討も行う必要があります。できる限り早期に専門家への相談や警察への告訴・被害届提出などを実施し、協力を得ながら最善策を選択することになります。

情報漏洩発覚後の初動対応については本稿では割愛いたしますが、弁護士知財ネットをはじめとする各専門団体にて、情報漏洩対策や漏洩時の対応について相談窓口を設けておりますのでご相談いただければと思います。

５　結び

冒頭に紹介しましたＩＰＡのアンケート結果によると、営業秘密漏洩を経験した企業における、その漏洩を認識した主なきっかけは以下のとおりです。

①第三者から指摘を受けた(41.3%)
②役員・従業員等からの報告があった(38.5%)
③自発的な活動により流出したことが発覚した(17.3%)
④製品の類似品が市場に出回った(12.5%)
⑤インターネット等に掲載されているのを偶然発見した(11.5%)
⑥他社が使用しているのを偶然発見した(5.8%)
⑦競業他社の研究開発のスピードが速まった(1.0%)

これらを見てみると、「第三者から指摘を受けた」とか「偶然発見した」という偶発的な検知経路が少なくないことがわかります。会社の「自発的な活動により流出したことが発覚した」というのはわずか17.3%にとどまります（アンケート時点での数字であるため、必ずしも現時点での実態を示すものではありません）。

このような結果を見ると、「今、まさに現在進行形で、自社の営業秘密が漏洩している可能性はないか?」という疑いの目をもって、自社の管理体制を見直していただきたいと思う次第です。

※１　https://www.ipa.go.jp/files/000057774.pdf

※２　https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706blueppt.pdf

※３　https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

※４　https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf