退職者・転職者による「企業秘密」の漏えい・持込みを防ぐ

雇用の流動化が進むにつれ、退職者・転職者による企業秘密の漏えいリスクが高まっています。自社の企業秘密の漏えいを防ぎ、他社の企業秘密を侵害しないために企業がとるべき対応と留意点を解説します。

アサミ経営法律事務所
弁護士
浅見　隆行

人材の流動化と「企業秘密」を保護する必要性

人材大流動化時代とも言われている現在、働き方に対する価値観の多様性とも相まって、「企業秘密」に接することができる従業員（派遣社員や期間従業員を含みます）の退職、転職は日常茶飯事となっています。

その結果、終身雇用時代に比べると、自社の「企業秘密」に接することができた従業員が、「企業秘密」を持って同業他社に転職する、あるいは独立するリスクが高まっています。また、転職者を中途採用する場合には、転職者が、前職の「企業秘密」を自社に持ち込むリスクも高まっています。

自社の「企業秘密」が持ち出されるリスクに比べると、転職者が前職の「企業秘密」を持ち込むリスクは見過ごされがちです。しかし実際に、転職者が「企業秘密」を持ち込んだことで、転職者と中途採用した企業の両方が刑事罰を受けるケースも発生しています。

回転寿司チェーン店K社の元社長が、同業他社であるH社の取締役から退任する直前に、商品原価や仕入価格などの「営業秘密」をアクセス権限のある当時の部下に命じて入手し、転職後、K社の商品企画部長に「営業秘密」をメールで開示し、商品原価の比較データなどを作成させるなどしたケースです。

元社長は、不正競争防止法違反（営業秘密侵害罪）により懲役3年、執行猶予4年、罰金200万円を命じられ、K社も罰金3000万円を命じられました。

なお、「営業秘密」を持ち出すことに協力させられたH社の部下は罰金50万円、元社長から「営業秘密」を開示するメールを受け取り、商品原価の比較データなどを作成したK社の商品企画部長は懲役2年6か月、執行猶予4年、罰金100万円を命じられています。さらに、H社はK社に対して損害賠償請求を提訴しています。

企業は、いま一度、これらのリスクに巻き込まれないための対策を確認しておくことが急務です。

退職者による「企業秘密」の持出しを防ぐための方策

退職者が「企業秘密」を持ち出すことを防ぐための方策につい

て、①人的管理、②組織的管理、③物理的管理、④技術的管理の4点から説明します。

⑴　人的管理

人的管理とは、退職者に「こういう類の情報は企業秘密に該当する」「企業秘密を持ち出してはいけない」「企業秘密を自社の業務以外の目的で利用してはいけない」などのルールを認識させることです。代表例が、退職者との秘密保持契約の締結と、退職後の「企業秘密」の取扱いに関する説明の実施です。

①　退職者と秘密保持契約を締結する方法

多くの企業が、退職の際に、退職者と「秘密保持契約」を結んでいると思います。しかし、退職の手続きに必要な書類など複数の書類にサインさせるのと同時に行ない、秘密保持契約の締結が、流れ作業のようになっている企業は少なくないようです。

特に退職者には、会社に提出してもらう書類が複数あるので、会社（人事部門）が、退職後の守秘義務について説明することもなく、仮に説明しても一言忠告する程度にとどまっていることが多いのではないでしょうか。

これでは、退職者に秘密保持の重要性を認識させることはできず、「人的管理」をしたことになりません。

理想を言えば、他の書類にサインさせるのとは別の機会を設け、退職者に情報管理に関する説明を時間をかけて行ない、退職後の「企業秘密」の取扱いの重要性を認識させてから、その場で、退職後の秘密保持契約を締結させるのが望ましいやり方です。

退職後の秘密保持契約の締結を拒絶された場合は、「会社から退職後の企業秘密の取扱いについて説明を受けました」などと書いた書類にサインさせるのでもかまいません。

②　秘密保持契約の内容

退職後の秘密保持契約には、「業務上知った情報」「業務上知り得た情報」のような漠然とした文言だけでなく、**「組織図、権限表、従業員の氏名、連絡先などの人事情報」「取引先の社名、担当者名、連絡先、取引内容、取引金額などの取引先情報」**など、会社が持ち出されたくない「企業秘密」の内容をできる限り具体的に例示しておくことも必要です。

そうすることで、退職者が「企業秘密」を漏らした後に、「これが企業秘密だとは思わなかった」などと言い逃れすることを防ぐことができます。

また、退職時・退職後に禁止される行為については、「不正取得」「不正開示」「使用」といった抽象的な表現にとどめず、

「アクセス権限のない情報にアクセスして閲覧、コピーしてはならない」

「会社の許可なく、独立・転職先で利用してはならない。転職先に開示してはならない」

「メール、ＬＩＮＥでの共有をしてはならない。ＳＮＳに投稿してはならない」

など、具体的に例示しておくことも重要です。

これも、退職者が「企業秘密」を漏らした後に「これまで禁止されるとは思わなかった」などと言い逃れすることを防ぐためです。

⑵　組織的管理

「企業秘密」を守りたいのであれば、企業は、「企業秘密」の取扱いについて、就業規則や情報取扱い規程などの社内ルールを定める、社内組織・体制を整備するなどして、「組織的に企業秘密を守る」必要があります。そうすることで、退職を意図している者が、退職前に「企業秘密」を不正に入手することを予防するのです。

特に重要なのが、「企業秘密」へのアクセス権限についての日頃の運用です。たとえば、

①「企業秘密」にアクセスすることができる者をその「企業秘密」を必要とする業務の担当者とその上司に限定する

②「企業秘密」にアクセスすることができるとしても、「企業秘密」の内容を見ることができる者を限定する

③「企業秘密」の内容を見ることができても、デジタルデータならダウンロードやメールにファイルを添付することができないようにする、紙媒体ならコピーや持帰りを禁止する

など、段階を分けた情報管理が可能だと思います。

また、退職日までに日数があるときでも、

④　退職の意向を示した者には「企業秘密」にはアクセスできないようにする

など、情報管理の方法を変更することも、退職する直前に「企業秘密」を不正に取得することを防止するのに有益です。

(3) 物理的管理

最善の方法は、「企業秘密」そのものを物理的に隔離して、退職の意向を示した者がアクセスできない、別の場所に保管することです。たとえば、共有サーバや共有フォルダに保存されている「企業秘密」（デジタルデータ）を共有されていないサーバやフォルダに移動させることが考えられます。

しかし、退職の意向を示した者による不正取得を防ぐためだけに「企業秘密」を隔離すると、通常業務に支障が出てしまいます。そこで現実的には、「企業秘密」を隔離するのではなく、退職の意向を示した者を「企業秘密」から隔離することが最善策です。

「企業秘密」から隔離する最も簡単な方法は、

① 退職の意向を示した者に有給休暇をとらせ、出社させない

ことです。出社しなければ「企業秘密」にアクセスすることはできません。

ただし、クラウド（SaaS）やテレワークの浸透により、出社しなくとも自宅のパソコンから共有フォルダや共有サーバ内の「企業秘密」にアクセスすることは可能です。そこで、退職の意向を示した者は、

② 退職日まではクラウドやテレワークを利用できないようにする、クラウドやテレワークができるとしても「企業秘密」にアクセスできないようにする

ことも、「企業秘密」からの隔離と言えます。さらに、

③ 退職の意向を示した者は、「企業秘密」を取り扱う会議に参加させない

④ 退職の意向を示した者は、紙媒体などが保存されているキャビネットから席を離す

なども有益な方法です。

(4) 技術的管理

「企業秘密」の多くがデジタルデータ化している今日では、退職の意向を示した者がデジタルデータにアクセスできないように技術を駆使することが不可欠です。たとえば、

① 「企業秘密」を取り扱っている部署に入室できないように入室用セキュリティカードの設定を変更する

② 共有サーバや共有フォルダ内の「企業秘密」を保存している共有フォルダや共有ファイルにアクセスできないように権限を変更する

③ 退職日に先行して、共有サーバやクラウドを利用するためのIDを使えないようにする

などです。

(5) 「企業秘密」と不正競争防止法の「営業秘密」の関係

退職者が「企業秘密」を不正に持ち出して転職先などで使用した場合、持ち出された企業は、退職者や転職先企業に対して損害賠償請求や差止請求をします。訴訟まで至らずとも警告書を送る場合もあるでしょう。

退職者が、退職後の秘密保持契約を結んでいるときは、こうした動きの法的根拠は秘密保持契約違反（守秘義務違反）と、不正競争防止法違反（営業秘密侵害行為）です。退職後の秘密保持契約を結んでいないときは、不正競争防止法違反が法的根拠になります。

ただし、不正競争防止法が損害賠償や差止めを認めているのは「営業秘密」が侵害された場合に限られます。「営業秘密」は、

① 非公知性
② 有用性
③ 秘密管理性

という3つの要件を満たしたものに限定されます。

企業が「企業秘密」として保護したいと考えている情報であっても、3つの要件を満たしていないときには、不正競争防止法では保護されません。そのために、日頃から、(1)～(4)で説明した内容を意識した秘密管理を徹底しておくことが必要です。

転職者による「企業秘密」の持込みを防ぐための方策

(1) 転職者による前職の「企業秘密」の持込みの法的リスク

転職者が、前職の「企業秘密」を「お土産」として持ち込むことは従来からよく見られてきた光景です。しかし、不正競争防止法が2003年に改正され、前職の「営業秘密」の不正取得、不正開示は刑事罰の対象となりました。2015年にはさらに改正され重罰化し、また持ち込まれた企業も刑事罰の対象となっています。

現在は、前職から「企業秘密」を「お土産」として持ち込むことは犯罪行為になり得ると認識を改めさせる必要があります。

(2) 中途採用の面接時・入社時点での警告

中途採用する企業の情報管理に対する問題意識が高くとも、転職

者の問題意識が低いと、転職者は従来の感覚のまま前職の「企業秘密」を「お土産」として持ち込んでくる可能性があります。なかには、転職者がいち早く成果を出したいからという自分の利益のために前職の「企業秘密」を持ち込み、中途採用された企業で使用、開示することもあります。

こうした持込みリスクを防ぐには、中途採用の面接時・入社時点で、「前職の『企業秘密』や『営業秘密』は絶対に持ち込まないでください」と警告をすることが必要です。

しかし、採用面接に際して、「これまでの知識と経験をわが社で活かしてください。期待しています」などと安易に言っていたりすると、転職者に「警告は建前」と受け取られる可能性があります。建前ではなく「本気」であることを伝えるには、そもそも中途採用の面接時に誤解されるような表現をしないように慎重である必要があります。

また、退職の意向を示した者と退職後の秘密保持契約を締結する際のポイントと同様に、

① 転職者を中途採用し秘密保持契約を締結する際に、入社に関する書類の締結とは別に、情報管理についての説明の機会を設け、説明の後に秘密保持契約を締結する

② 秘密保持契約書に「前職の人事情報、財務情報、技術情報など『企業秘密』や『営業秘密』に類する情報は持ち込まないこと」「わが社ではこれらの情報を使用、開示しないこと」と具体的に記載しておく

ことが必要です（**上例**）。

③ 前職の「企業秘密」の持込み、不正使用、不正開示などが発覚した場合には、懲戒解雇の対象になる

ことなども注意しておくと、さらに警告となるでしょう。

＊　＊　＊

退職者が「企業秘密」を持ち出し、転職先で使用していることが明らかになった場合は、持ち出された企業は、退職者と転職先に対して秘密保持契約違反（守秘義務違反）、不正競争防止法違反（営業秘密侵害行為）を理由に損害賠償と差止めを警告する、不正競争防止法違反（営業秘密侵害罪）を理由に刑事告訴をすべきです。

他方、転職者によって前職の「企業秘密」が持ち込まれていることが明らかになった場合には、ただちにその使用を止めます。場合によっては、当該企業に謝罪し、事実を説明に行くことも必要だと思います。

■中途採用者と締結する「秘密保持契約書」の例

秘密保持に関する誓約書

この度、私は貴社に採用されるにあたり、下記事項を遵守することを誓約いたします。

記

第１条（在職時の秘密保持）

就業規則および情報管理規程を遵守し、次に示される貴社の秘密情報について、貴社の許可なく閲覧・コピーをしない、メールやLINEで第三者と共有しない、SNS等に投稿しないなど、目的外で利用しない、かつ不正取得、不正開示、不正使用しないことを約束いたします。

①人事情報　②財務情報　③技術情報

④その他業務中に知った、または知ることができた情報

第２条（退職後の秘密保持）

前条各号の秘密情報については、貴社を退職した後においても、独立・転職先で利用・開示しないことを約束いたします。退職時に、貴社との間で秘密保持契約を締結することに同意いたします。

第３条（損害賠償）

前２条に違反して、第１条各号の秘密情報を開示または使用した場合、法的な責任を負担するものであることを確認し、これにより貴社が被った一切の被害を賠償することを約束いたします。

第４条（第三者の秘密情報）

1　第三者の人事情報、財務情報、技術情報など第１条各号の秘密情報その他「企業秘密」や「営業秘密」に類する情報を含んだ媒体（文書、図画、写真、USBメモリ、DVD、ハードディスクドライブその他情報を記載または記録するものをいう）を一切保有しておらず、また今後も保有しないことを約束いたします。

2　貴社の業務に従事するにあたり、第三者が保有するあらゆる秘密情報を当該第三者の事前の書面による承諾なくして貴社に開示し、または使用もしくは出願（以下「使用等」という）をさせない、貴社が使用等するように仕向けない、または貴社が使用等しているとみなされるような行為を貴社にとらせないことを約束いたします。

（以下略）

あさみ　たかゆき　２０００年、弁護士登録。企業危機管理・リスクマネジメントを中心に、会社法・株主総会・情報セキュリティ（企業秘密・個人情報）・危機管理広報など企業法務全般に取り組んでいる。