テレワークと営業秘密の保護

弁護士法人中央総合法律事務所
弁護士　中　嶋　章　人

第１　はじめに

先日、社内の技術情報を中国企業に漏洩したとして不正競争防止法違反の罪に問われた大手メーカー元従業員の初公判が行われました。また、今年の１月には、大手電気通信事業者の元従業員がロシアに機密情報を漏洩したとして不正競争防止法違反の容疑で逮捕されています。このように、技術が発展しデータでのやり取りを行うようになった現代においては、データ管理といった視点は重要な課題となっています[1]。

また、昨今の新型コロナウイルスの影響により、社外で仕事を行う「テレワーク」が急速に普及し、従前のような社内での物理的な情報の管理のみでは足らず、社外での作業実施等を念頭に置いた情報管理対策を検討する必要が生じているものと思われます。

今回は、テレワーク実施下において、企業の情報を如何に保護し、企業活動を円滑に進めていくかという観点から、不正競争防止法上の営業秘密保護とテレワークでの秘密管理対策について、確認する機会としたいと思います。

第２　不正競争防止法上の「営業秘密の保護」

１　「営業秘密」といえるための３要件

まず、不正競争防止法において営業秘密として保護されるためには、「営業秘密」と認められる必要があります。

> 〔不正競争防止法２条６項〕
> この法律において「営業秘密」とは、①秘密として管理されている生産方法、販売方法その他の②事業活動に有用な技術上又は営業上の情報であって、③公然と知られていないものをいう。

「営業秘密」といえるためには、

①　秘密として管理されていること（**秘密管理性**）
②　有用な技術又は営業上の情報であること（**有用性**）
③　公然と知られていないこと（**非公知性**）

を満たしている必要があります。

---

[1] 経済産業省知的財産政策室は、令和３年６月２日、「最新の営業秘密侵害事例から見えてくる『営業秘密』保護のポイント～『営業秘密』を保護するために企業はどのような対策が必要か～」を資料としてまとめています。

⑴　秘密として管理されていること（秘密管理性）

秘密管理性が認められるためには、その情報に合法的かつ現実に接触することができる従業員等からみて、その情報が企業にとって秘密としたい情報であることが分かる程度に、アクセス制限や「㊙」（マル秘）・「社内限り」等の表示といった秘密管理措置が施されている必要があります[2]。

この秘密管理性については、経済産業省が「営業秘密管理指針（最終改訂：平成31年1月23日）」[3]（以下「指針」といいます。）において一定の指針を示しており、「秘密管理性要件が求められる趣旨は、企業が秘密として管理しようとする対象（情報の範囲）が従業員等に対して明確にされることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにある」とされています。

また、具体的にどの程度の秘密管理措置が必要となるかについては、一概に定まるものではなく、その内容・程度は、企業の規模、業態、従業員の職務、情報の性質その他の事情の如何によって異なるものであり、当該情報に合法的に、かつ、現実に接することができる従業員等に対して、一般情報（営業秘密でない情報）と対象情報（営業秘密）とを合理的区分し、対象情報が営業秘密として明らかにする措置となっているかといった観点から判断されることになります[4]。

⑵　有用な技術又は営業上の情報であること（有用性）

「有用性」の要件は、公序良俗に反する内容の情報など、秘密として法律上保護する正当な利益が乏しい情報を営業秘密の範囲から除外した上で、広い意味で商業的価値が認められる情報を保護することを趣旨としています[5]。そのため、秘密管理性、非公知性要件を満たす情報は、有用性が認められることが多く、係争となった際にこの点が争いになることはあまりありません。また、現に事業活動に使用・利用されていることを要するものでなく、失敗した実験データ等のいわゆるネガティブ・インフォメーションにも有用性は認められると考えらます。

⑶　公然と知られていないこと（非公知性）

「非公知性」が認められるためには、当該情報が一般的には知られておらず、又は、容易に知ることができないことが必要です[6]。

---

[2] 経済産業省「不正競争防止法テキスト」（2020年11月公開）21頁参照

[3] 指針は、不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準を示すものであるとされています（指針2頁参照）。

[4] 指針6頁以下参照。

[5] 指針16頁。

[6] 指針17頁。

具体的には、当該情報が合理的な努力の範囲内で入手可能な刊行物に記載されていない、公開情報や一般に入手可能な商品等から容易に推測・分析されない等、保有者の管理下以外では一般に入手できない状態をいいます。

2　不正競争防止法違反に関する民事上・刑事上の責任

営業秘密の 3 要件を満たし、「不正競争」（法 2 条 1 項 4 号ないし 10 号）及び「営業秘密侵害罪」（法 21 条 1 項各号及び 3 項）の各要件（規定の行為態様等）を満たす場合には、民事上及び刑事上の措置が定められており、その内容は次のとおりです。

⑴　民事上の措置

・差止請求権（法 3 条）
・損害賠償請求権（法 4 条）
・損害賠償・不正使用の推定等（第 5 条等）
・書類提出命令（法 7 条）
・営業秘密の民事訴訟法上の保護（秘密保持命令（法 10 条）、訴訟記録の閲覧制限（法 12 条）、当事者尋問等の公開停止（法 13 条））
・信用回復措置（法 14 条）

⑵　刑事上の措置

・営業秘密侵害罪（21 条 1 項各号、3 項）
　10 年以下の懲役若しくは 2000 万円（海外使用等は 3000 万円）以下の罰金
・法人両罰規定（22 条 1 項 1 号、2 号）
　5 億円（海外使用等は 10 億円）以下の罰金
・不当収益の没収、追徴（21 条 10 項、12 項）

第３　テレワーク時における情報管理

1　テレワークに関し企業で検討しておくべき事項

秘密情報を持ち帰ることなどによる情報漏洩のリスクや法的保護の毀損への懸念を解消し、適切な情報管理を行いながらテレワークを推進するべく、経済産業省知的財産政策室は、不正競争防止法上の「営業秘密の保護」の観点から、テレワーク実施のポイントをまとめています（「テレワーク時における秘密情報管理のポイント（Q&A）」令和 2 年 5 月 7 日）。

また、総務省は、企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、テレワーク導入に当たってのセキュリティ対策の考え方や対策例を示した「テレワークセキュリティガイドライン（第 5 版）」（令和 3 年 5 月）を公表しています。さらに、中小企業等におけるシステム管理担当者を対象として、テレワークを実施する際に最低限のセキュリティを確保するための手引

きとして「中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（第2版）」（令和3年5月）も公表しています。テレワーク環境の整備・セキュリティ確保にあたっては、こちらをご参照いただければと思います。

以下では、テレワーク実施にあたり、各場面にわけてその検討事項・ポイントを中心に、営業秘密として保護を受けるための対策をご紹介したいと思います[7]。

2　状況と対策の例

⑴　テレワーク導入時

ア　検討事項

テレワークを実施するにあたり、秘密情報の管理の態様や諸規定の整備状況を改めて確認し、テレワークにも対応した内容になっているかを確認し、必要に応じて見直しを図っておく必要があります。

Ex)・営業秘密管理規定や情報取扱規定、セキュリティ規定等の社内規程の確認及び修正

・各種規定を修正する場合にはその内容、従前の規定等で問題ない場合には、改めて当該各種規程について従業員への周知の徹底（メールでの共有やe-ラーニングの実施等）

・情報の性質に応じ、改めて各種情報への適切なアクセス権者の設定の見直しや、「㊙」（マル秘）・「社内限り」といった秘密であることの表示の付記の徹底、ID・パスワードの設定を徹底するなど、テレワークの実施にあたり、再度営業秘密の保護を意識する機会を設ける

イ　解説

テレワーク実施にあたっては、営業秘密の3要件のうち、「秘密管理性」をどのように確保するかが問題となりますが、前述のような秘密管理性の趣旨に照らせば、企業として保有している情報のうち秘密として管理しようとする情報の範囲を明確にするとともに、当該情報に対する従業員の予見可能性を確保することが重要と考えられます。

テレワークにあたっては、情報の社外持出しが予定されますが、各種取り扱い規程等において「秘密情報の社外持出し禁止」などとのみ規定されている場合には、テレワーク実施により当該規定が形骸化してしまう可能性があります。そのため、このような規定は、テレワークの性質に照らして、必要な場合には秘密情報の社外への持出しを認めつつ、持出しの場合のルールを厳格化する規定（持出し可能な情報と持出し不可の情報を分類する、持出し可能な情報であっても一定の手続（上長の決済を経る

---

[7] 前記の「テレワーク時における秘密情報管理のポイント（Q&A）」（令和2年5月7日）の内容を中心にご紹介したいと思います。

等）を要する等）を定めること等が考えられます。

また、実質的に営業秘密を保護するためには、従業員に営業秘密が法律上保護されていること、そして、自社企業における秘密情報は何かということをしっかりと意識してもらう必要があると考えられ、テレワークの実施にあたってこれらの再確認を行うことも有益と考えられます。

⑵　貸与端末機器のローカルフォルダへのデータ保存を許す場合

ア　検討事項

営業秘密としての保護を受けるための対策として、持出し可能とするデータそのものや保存先のローカルフォルダについて ID やパスワードによるアクセス制限をすることを徹底すること、これにつき各種規程により定めておくこと等が挙げられます。

また、企業活動の柔軟性との兼ね合いもあり、法的保護を受けるための必須の要件ではありませんが、秘密情報の保護に役立つ手法としては次のものが挙げられます。

・ローカルフォルダに保存を認めるデータを厳選する
・保存にあたって上長等の事前許可を必要とする
・保存をしたもの・ファイル・期間を一覧で管理する
・業務上の必要がなくなった場合の廃棄を義務づける　等

イ　解説

貸与端末機器のローカルフォルダに保存することを認める場合であっても、直ちに営業秘密としての法的保護を失うわけではありませんが、秘密管理性の趣旨から、具体的に対策を講じる必要があると考えられます。貸与端末機器へのローカルフォルダへの保存は、社内限りの情報を外部媒体へ保存するという点で、従業員の認識として、秘密管理性が緩和されているといった印象を与える可能性もあるため、そのような印象を与えないよう、予め上記のような一定の対策を施しておくことが有益と考えられます。

⑶　外部クラウドを利用し、社外からのアクセスを許す場合

ア　検討事項

秘密管理性を確保するため、次のような方法が考えられます。

・企業内の部署・職位等に応じてアクセス権者を制限する（階層制限に基づくアクセス制御）
・クラウド上のデータや当該データを格納するフォルダにアクセスする際に ID・パスワードの入力を要求する
・当該データのファイル名や当該データ上に「㊙」（マル秘）・「社内限り」等の秘密であることの表示を付ける　等

また、非公知性要件との関係では、次のような対策を行っておくことが考えられま

す。

・外部クラウドを選択するにあたっては、クラウドの安全性等に配慮し、現にクラウドにデータをアップロードするにあたっては、その公開範囲の設定に十分注意する

・クラウド上で保管する必要がなくなったとなったファイルはクラウド上から消去することを徹底する

・クラウド上での消去が確実ではない場合には、暗号化やファイルのセキュリティ強化により可読困難にしておく　等

イ　解説

社内で営業秘密として扱っている情報を、外部クラウドに供した場合であっても、直ちに営業秘密として法的保護が失われるものではありません。なお、指針においても、「外部クラウドを利用して営業秘密を保管・管理する場合も、秘密として管理されていれば、秘密管理性が失われるものでない」とされています。

クラウドを利用する上での特有の問題として、外部クラウド上において、当該情報（データ）が不特定多数の者により閲覧可能な状況となってしまった場合（公開のフォルダ等にアップロードしてしまった場合、クラウド提供者側の不備等）営業秘密の3要件の1つである「非公知性要件」を満たさなくなる可能性があります。そのため、仮にそのような状況が生じた場合であっても非公知性を確保するための手段を講じておくことは有益と考えられます。

⑷　自宅外でのテレワークを行う場合

ア　検討事項

不特定多数の人が出入りする場所でテレワークを実施する場合には、効果的に営業秘密を保護するため、次のような対策の検討が有益と考えられます。

・紙の資料やPC等を机の上等に放置しないことに関する規定を制定もしくは徹底

・PCの画面にのぞき見防止フィルム等を貼付する等のルール化

・オンライン会議を実施する場合等には不特定多数の人の出入りがない場所を選択することや、イヤホンを着用する等のルール化

また、セキュリティの面からは、自宅外で用いる通信環境には配慮する必要があり、公衆無線LAN等を利用しない・接続しないこととする規定の制定もしくは徹底をしておくことが有益と考えられます。

イ　解説

自宅外でのテレワークそれ自体は、秘密管理性の有無を直接左右するものではなく、前述の秘密管理措置が講じられている限りは、この要件を充足すると考えられます。もっとも、不特定多数人が周りにいることで、秘密情報（データ）ののぞき見や盗撮、盗難等他の者に知られる恐れがあり、非公知性要件を欠く恐れがあるほか、不正競争

防止法上の保護を受けられる場合であっても、実際上の問題として秘密情報が流出する危険がありますので十分注意が必要といえます。

また、セキュリティの面からは、外部による侵害を防ぐため、公衆無線 LAN 等の不特定多数が共有する通信を用いることは避けるべきです。

⑸　参考：万一の情報漏洩への備え

ア　検討事項

〔未然の防止策〕

・営業秘密へのアクセス権者の設定範囲を改めて確認し、当該営業秘密にアクセスする必要のない従業員等がアクセスできないような措置を講じておく

・社内教育の実施や社内規程の周知等を通じて、秘密情報管理の重要性に関する従業員の理解を深め、情報漏洩に対する危機意識を高めておく

・情報漏洩行為を実施しにくい状況を作り出すため、次のような工夫をしておく

メールの転送制限や、メールへのファイル添付制限

メールを送信する際に上長が常に CC 等に追加される設定

遠隔操作により PC 内のデータを消去できる措置を講じておく

社用 PC に USB メモリ等の外部記憶媒体を接続できない設定を講じておく　等

〔事後的な対応を可能とするための対策〕

・データの暗号化・セキュリティによる閲覧制限を施しておく

・PC のシンクライアント化をしておく

・従業員による営業秘密へのアクセスやダウンロードのログを保存しておく

・一定回数パスワードの認証に失敗すると秘密情報を消去できるツールの利用　等

イ　解説

情報漏洩や不正な情報の持出しなどは、悪意を持ってなされることもあり、企業が営業秘密として法的に保護されるための対策を進めていても、現実的な漏洩等は、必ず阻止できるというものではありません。

そのため、上記に挙げたものは、営業秘密として法律上保護されるために必須の対策ではありませんが、漏洩してしまった場合の損害は金銭では回復できない場合も多いため、可能な限り漏洩を防止し、仮に漏洩が生じた場合でも被害を最小限にとどめる対策は有益なものといえます。これらのほかにも、漏洩防止や漏洩時に推奨される包括的な対策等（高度なものを含む）については、経済産業省が「秘密情報の保護ハンドブック～企業価値の向上に向けて～」（平成 28 年 2 月）の中でも詳しく書かれておりますので、是非ご参照いただければと思います。

以上