

在宅勤務に伴う情報保護に関する留意点

弁護士 波田野 晴朗
弁護士 戸田 謙太郎
弁護士 溝端 俊介

Question

テレワークを導入した場合、当社の秘密情報をどのように管理すればよいですか。

Answer

テレワークにより取り扱われる秘密情報を特定し、秘密情報の取扱い状況を管理した上で、秘密情報を外部に流出させず、営業秘密として法的保護が受けられるような情報管理体制を構築する必要があります。具体的には、安全性の高いシステムを導入するとともに、社内規定の整備と周知、持ち出すデータやその保存先へのアクセス制限、アクセスログの記録、ファイルや書類への秘密表示等が考えられます。

次に、秘密情報の持ち出しなどの不祥事が発生したときに早期に不祥事の発生を把握できる体制を整備しておくことも重要です。テレワークでは、対面でのコミュニケーションが減ることから、通常のレポートラインを通じた不祥事の発見が困難になることが危惧されます。そこで、通常のレポートラインを補完する効果を有している内部通報制度の実効性を確保することが重要となります。具体的には、通報受付担当者がテレワークでも内部通報窓口への問い合わせ確認できる体制や、通報の重要度とテレワークの趣旨を考えながら内部調査を進められるような体制を整備することなどが考えられます。

1. 秘密情報の管理

(1) テレワーク導入時の秘密情報管理

顧客名簿や新規事業計画のような営業情報や、製造方法・ノウハウのような技術情報のように競争上高い価値を有する非公知の情報は、第三者に知られないように社内（又は取引当事者間）で秘密にしておくことが、競争力を保つことにつながります。一方で、秘密情報は、事業に活用されることでその価値を発揮することになるため、一切使用せずに厳重に秘密として管理しておけばよいというものでもありません。そこで、意図せざる流出を防止しつつ秘密情報の競争力を活用するために、秘密情報の管理と活用のバランスが重要となります。テレワーク導入時の秘密情報管理についてもこのようなバランスを意識する必要があります。

秘密情報を流出させないためには、まずは秘密情報へのアクセスを極力限定することが最も有効です。情報が記録された媒体、情報へアクセス権限、物理的・技術的なアクセス方法が制限されればされるほど、情報漏洩のリスクは低減します。一方で、情報記録媒体、アクセス権限、アクセス方法を制限すればするほど、情報の活用に関する業務上の効率性や利便性は制限されていきます。テレワークの導入により、オンラインで社内データへのアクセスを可能とすることは、業務の効率性や利便性を増加させることとなります。一方で、情報管理の観点からは、秘密情報への社外からアクセスを拡大することになるため、一般的には情報漏洩のリスクが高まるおそれがあります。

そこで、リモートワークを導入する際には、テレワークにより取り扱うことのできる秘密情報を特定し、その秘密情報の取扱い状況を管理した上で、秘密情報を外部に流出させないような情報管理体制を構築する必要があります。また、万一が一流出した場合に備えて、秘密情報の使用状況（取得、使用、複製等）を事後的に追跡できるようにしておくことも重要です。

まず、従業員等にとって、秘密情報が、社内で秘密情報として取り扱われるべき情報であることを認識できるような管理が重要です。そのためには、秘密情報が、情報の性質、選択された媒体、機密性の高低、情報量等に応じて、秘密情報ではない情報と合理的に区分される必要があります。より具体的には、テレワークを念頭に置いた社内規定を整備・周知し、秘密情報の社外からのアクセスに関するルールを情報の成立に応じて定めておく必要があります。作業環境としても、できるだけ自宅で行うよう指導し、万一自宅外で作業を行う際も、資料やPC等を机の上に放置しないことに関するルールの徹底、PCへののぞき見防止フィルム等の貼付することの徹底等、情報の流出を防ぐルールの徹底を図ることが重要と考えられます。一方で、情報取扱規程が「秘密情報の社外への持ち出し禁止」などと一般的な規定しかされていない場合や、詳細な情報取扱規程が定められていても周知されていない又は規程が形骸化されて規程に従った運用がされていない場合には、従業員等は秘密情報の範囲や取扱いルールを認識することができず、適切な情報管理が行われなくなることになります。このように、テレワーク導入に際しての情報管理ルールを定めた場合には、ルール策定後の周知と運用がより重要となることに留意が必要となります。

また、技術的管理の観点からも、セキュリティの観点から安全性の高いシステムを導入し、情報に対するアクセス・複製を制限し、使用状況をモニターする技術的な措置を講じておく必要があります。たとえば、総務省の「テレワークセキュリティガイドライン」¹では、VPNを利用し迅速なパッチ適用等の

¹ https://www.soumu.go.jp/main_content/000545372.pdf

適切な運用を行う、リモートデスクトップを利用するなどの対応が推奨されています。また、秘密表示等の方法により、アクセス・使用時に秘密情報が客観的に明らかになるような措置を講じるとともに、アクセス対象可能な秘密情報の制限、複製・保存の制限、アクセスログの記録などの技術的管理措置を講じておくことも重要となります。

なお、導入すべき秘密管理措置の内容・程度は、従業員の多寡、業態、従業員の職務、情報の性質、執務室の状況その他の事情によって異なります。経済産業省では「テレワーク時における秘密情報管理のポイント（Q&A 解説）」²を公表し、具体的なテレワーク業務態様に応じた秘密管理体制のアイデアを提示していますので、テレワーク導入時の秘密管理体制を検討する際には参考となります。

また、次に説明するように、秘密情報は、一定の要件のもとで営業秘密として不正競争防止法において保護を受けることができます。しかしながら、秘密情報の流出によって生じた被害を不正競争防止法に基づく法的措置により完全に回復することは困難です。したがって、テレワーク導入時の秘密情報管理体制を検討する際には、秘密情報の流出を予防し、情報流出が生じた場合に被害を最小限に食い止めるという実務的な観点から、より一層重要となります。

（２）営業秘密としての保護

企業が秘密として管理する情報が流出・不正利用された場合には、その情報が不正競争防止法の定める営業秘密に該当する場合には、一定の保護を受けることができます。

営業秘密は、「秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないもの」と定義され（同法 2 条 6 項）、営業秘密を不正に取得・使用・開示することは、不正競争となります（同法 2 条 1 項 4 号乃至 10 号）。営業秘密の保有者は、これらの不正競争に対して、差止請求（同法 3 条）や、損害賠償請求（同法 4 条）を行うことができます。

ここでいう「秘密として管理されている」（いわゆる秘密管理性）は、従業員がその情報が秘密として管理されていることを客観的に認識し可能な措置が講じられていたと認められる必要があります（知財高判平成 23 年 9 月 27 日、知財高判平成 30 年 3 月 26 日等）。具体的な管理方法としては、経済産業省の公表する「営業秘密管理指針」³や「秘密情報の保護ハンドブック～企業価値向上に向けて～」⁴が参考となります。

テレワークを導入する場合、情報に対する社外からのアクセスが拡大することが想定されるため、この秘密管理性が問題となります。もっとも、テレワークによってアクセス・使用される情報についても、その情報が秘密として管理されていることが客観的に認識可能な措置が講じられていれば、秘密管理性が認められる余地があります。このような秘密管理性の認められる管理方法とは、結局は（１）で述べた情報流出を防止するための管理方法と重複することになりますので、テレワーク導入時において秘密情報が流出しないための適切な組織的・技術的管理措置が講じられていれば、営業秘密としての秘密管理性が認められる余地は十分にあるといえます。

² https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf

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

⁴ <https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf>

2. 情報漏洩に備えた内部通報制度

(1) 内部通報制度の重要性

秘密管理措置を適切に講じていたとしても、悪意を持って秘密情報を持ち出される等、情報漏洩の不祥事が発生することを完全に防止することはできません。そのため、可能な限り早期に不祥事の発生を把握できるようにするための体制を整備しておくことが重要です。

不祥事が発生した際は、上司等への報告や相談という通常のレポートラインを通じて発見されるに至るのが望ましいことは言うまでもありません。しかし、テレワークの普及により対面でのコミュニケーションが減ることから、通常のレポートラインを通じた不祥事の実見が困難になることが危惧されます。

そのため、通常のレポートラインを補完するものとして、内部通報制度の実効性を確保し、法令違反等の早期に発見し、未然に防止することが重要となります。

(2) テレワーク状況下の内部通報制度

テレワークの状況下では、通報受付担当者が自宅から通報内容を確認できないために通報への対応が遅れてしまったり、通報内容の調査のために現地に赴かなくてはならないにもかかわらず必要な人員が確保できなかつたりすることが考えられます。

そこで、通報受付担当者がテレワークであっても内部通報窓口への問い合わせを確認できる体制を整備することが望まれます。具体的には、メールや Web ページへの問い合わせを自宅から確認できるようにすることはもちろん、電話での対応についても、転送する等、できる限りテレワーク導入以前と同様に通報受付担当者が通報内容を確認できる体制を構築することとなります。また、テレワーク導入以前と同様に通報内容を確認する体制を即座に確保する措置がとれない場合には、テレワークの影響により内部通報窓口の運用が変更されている旨を利用者に告知しつつ、できる限り早期にテレワーク導入以前と同様の対応ができるような体制を構築することを模索することが考えられます。

また、テレワークの実施状況によっては、通報内容の調査にあたり、通報者や関係者との面談が困難であったり、関係資料の入手が困難になったりするなど、一定の制約が生じることが考えられます。そのため、テレワーク時における調査には、通常の場合の調査よりも時間を要することとなる可能性もありますが、通報内容によっては会社の経営に重大な影響を及ぼす問題に発展する可能性もあるため、事案の重大性を適切に判断しながら、調査を行っていくことが重要となります。

以上