営業秘密官民フォーラムメールマガジン掲載コラム第47回

テレワークにおける情報管理

弁護士知財ネット
弁護士　城石 惣

1　はじめに

現在、新型コロナウイルス感染症（COVID-19）の感染拡大を受け、感染症対策の取組みの大きな柱として、自宅での「テレワーク」を導入する企業・法人が増えています。（※1）
テレワークは、満員電車での通勤や、オフィスという密集空間での業務を避けることができ、感染症対策としては極めて大きな意義を有しています。また、テレワークは、従業員のワークライフバランスの実現や人材の維持・確保、業務プロセスの革新など、経営課題の解決策にもなり得るものであり、今後、利用促進はますます加速していくものと考えられます。

テレワークの導入にあたっては、セキュリティ対策、労務管理を含むルール整備、ICT環境（端末やコミュニケーションツール等）の整備など、様々な課題がありますが、本稿では情報セキュリティの観点から、留意すべき事項等について簡単に整理します。

※1　新型コロナウイルス感染症対策のためのテレワーク導入については、「働き方改革推進支援金」の助成対象となっています。（https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/koyou_roudou/roudoukijun/jikan/syokubaisikitelework.html）

2　テレワークの方式

テレワークとは、ICT（情報通信技術）を活用して行う事業外勤務のことを指します。導入にあたってのICTの構築のあり方は様々ですが、主に、以下の4つの方式があります。（※2）

①リモートデスクトップ方式

オフィスに設置したPCのデスクトップ環境を、別のPC等を用いて遠隔で閲覧・操作する方式です。
保存したファイルはオフィスにある端末上に保存され、（システムや設定によりますが）従業員の手元の端末にデータは残りませんので、情報漏えいが起きにくいというメリットがあります。

②仮想デスクトップ方式

サーバが提供する仮想デスクトップに、手元にあるPCから遠隔でログインして利用する方式です。

サーバにアクセスして利用するという点で、リモートデスクトップ方式（①）と異なります。
作業した内容はサーバに保存され、リモートデスクトップ方式（①）と同様、従業員の手元の端末にデータは残らないことになります。
また、ソフトウェアのアップデート等を管理者が実行することができる、利用者が自由にソフトウェアをインストールするのを防止することができるなどの管理・運営上のメリットがあります。（※3）

③クラウド型アプリ方式
Web 上からクラウド型アプリケーション（Microsoft Office 365、 Dropbox、 サイボウズ Garoon など）にアクセスし、どこからでも同じ環境で作業できるようにする方式です。
従業員の手元の端末からオフィス内のサーバへ直接アクセスすることはできないことになります。
アプリケーションの設定等によっては、クラウド上で作成した資料をローカル環境にダウンロードすることができるものもあります。

④会社 PC の持ち帰り方式
会社で使用している PC を社外に持ち出して業務を行う方式です。
ネットワーク経由でオフィス内のサーバにアクセスする場合は、通常、VPN 経由で接続することで情報漏えい対策を行うことになります。
多くの業務データが格納された PC を社外に持ち出すこととなるため、紛失等による情報漏えいが起きやすく、上記の中で最も慎重な対策が求められる方式であると考えられています。

主な方式は上記のとおりです。テレワークを導入するにあたっては、それぞれの方式の特徴や安全性、導入にかかるコスト等を踏まえ、そのいずれの方式とするかを決定することになります。

※2　総務省「情報システム担当者のためのテレワーク導入手順書」55 頁以下
※3　これに対して、①リモートデスクトップ方式の場合は、必要なソフトウェアのアップデート等を個々の PC ごとに行う必要があります。筆者の経験においても、テレワークを頻繁に実施するわけではない場合、ソフトウェアのアップデートを怠ってしまい、リモートデスクトップを起動できないということはしばしばありました。
※4　なお、昨今話題となった「シンクライアント方式」とは、上記①ないし②の方式を用いた上で、手元の端末上に電子データを保存させないようにする方式のことを指すようです（総務省「テレワークセキュリティガイドライン第 4 版」9 頁）。

3　情報セキュリティ上のリスク
テレワークの導入にあたっては、インターネットを通じて業務データを社外で利用することに

なり、また、場合によっては手元の端末に社内の業務データをダウンロードすることもあるため、以下のような情報セキュリティ上のリスクがあります。

・　機密情報の漏えい
マルウェア感染、端末や記録媒体の紛失、社員によるデータ等の不正な持ち出し等により、機密情報を漏えいするリスクがあります。重要な営業秘密等の漏えいにより、企業の競争力が低下する可能性もあります。

・　個人情報の流出
端末や記録媒体の紛失等により、保有する個人情報を流出するリスクがあります。この場合、損害賠償等にまで発展する可能性もあるほか、企業のブランドイメージを大きく低下させる可能性もあります。

・　システム停止
マルウェア感染等による端末の乗っ取りやデータ破損等により、システムの全部又は一部の停止を余儀なくされ、業務継続に影響を与える可能性があります。

以上のようなリスクについては、大企業特有のものであって、中小企業等が標的とされることはないのではと思われるかもしれません。
しかしながら、情報漏えいの契機としては、端末や記録媒体の紛失、コワーキングスペースや交通機関での作業の覗き見、外部サービス（SNS）への誤投稿など様々なものがあり、大企業特有のものと軽視することはできません(もっとも、リスクやリスクが実現した場合の影響の大きさ、情報セキュリティ対策にかけられるリソース（ヒト・モノ・カネ）は企業規模に応じて様々であり、求められる対策のレベルは当然異なります。）。
また、漏えいや流出等により第三者に対して損害を与えた場合には、会社が損害賠償請求を受けるおそれがありますし（※5）、個人情報について適切な保管体制を構築しなければならないこと（個人情報保護法 20 条等）は、すべての事業者においても求められるところです。
したがって、テレワークの導入にあたっては、以上のような情報セキュリティ上のリスクを踏まえ、適切な情報管理体制を構築する必要があります。

※5　また、取締役がセキュリティ体制を整えていなかったことが原因であるとして、取締役としての任務懈怠責任（会社法 423 条 1 項）を負う可能性もあります。
※6　なお、大企業等にあっては、会社法上や金融商品取引法における内部統制構築義務の一環として、情報セキュリティ対策の構築を講じる義務があると考えられています（総務省「情報システム担当者のためのテレワーク導入手順書」23 頁）。

4　リスクを踏まえた情報管理のあり方

（1）基本的な情報セキュリティ対策

それでは、どのような情報管理を行う必要があるでしょうか。

社内のデータの取り扱いを極めて厳格に（すなわち持ち出しを一切禁止に）すれば、上記リスクを回避することは一応可能のように思われますが、これはテレワークを禁止するに等しいといえます（感染症対策として割り切るのであれば、このようなテレワークと称した有給休暇の導入も一応意味があるのかもしれませんが・・・）。

一方で、上記2の方式のいずれかを導入し、実質的な意味でテレワークを導入するためには、社内データの取り扱いを緩和し、一定程度、社外の取り扱いを許容しなければなりません。この場合、どのような情報を社外で取り扱えるかについて明確なルールを設定した上で、必要な情報セキュリティ対策を講じる必要があります。

この点については、総務省「テレワークセキュリティガイドライン第4版」は、基本的な対策事項として、以下の点を挙げています（同25頁以下）。

○　社内の情報資産を「機密情報」「業務情報」「公開情報」等3つ程度に分類し、公開情報以外の取扱い方法を定める。

・　機密情報には、個人情報（自社従業員に関するものも含む）、顧客から預かった非公開情報、機微情報、営業秘密、自社の経営に関する情報などが該当する。

・　業務情報には、機密情報には該当しないが、公開を前提としない情報（例：社内打合せ資料、勤務管理簿、研修教材等）が該当する。

・　情報資産の持ち出しを伴うテレワークでは、それらの持ち出された情報（電子データ、紙）が外部に漏えいするリスクが高まることから、「業務情報」と「公開情報」のみを持ち出し可能とすることが考えられる。

○　情報資産の利用者が、それぞれのレベル分けを識別できるようにする。

・　電子データ：フォルダによる区別、ファイル名への【機密】の追加など

・　紙媒体：紙面欄外余白部への「機密」表記、ファイルの背表紙への記載など

（2）機密情報（営業秘密など）の取扱い

分類した情報の取扱いをどのようにするかについては、総務省の上記ガイドラインは、「業務情報と公開情報のみを持ち出し可能とすることが考えられる。」としており、この取扱いによれば、機密情報の持ち出しは禁止されることになります。

機密情報が流出した場合のリスクが非常に大きいことから、持ち出しを一切禁止にするというのも一つのやり方ではありますが、業務の内容によっては、テレワークでの勤務の効率性を損な

うこととなりますし（※7）、持ち出しが禁止される範囲が広すぎると、社員による無断の持ち出し（記録媒体の持ち出しや、印刷した紙媒体の資料の持ち出し）も起きかねません。
そこで、機密情報を扱う可能性についても簡単に検討しておきます。

※7　日本組織内弁護士協会「組織内弁護士のリモートワーク／テレワークの実施状況に関するアンケート調査結果」においても、テレワークを難しくする要因として「機密保持」（３１．１％）が挙げられているところです。

ア　技術的な観点
上記２のいずれの方式においても、特定のフォルダにアクセス制限を設定し、機密情報の閲覧・編集について、利用者や利用できる端末を限定できることは可能です。
しかしながら、アクセス制限がかかっているとはいえ、機密情報を従業員の手元の端末等にダウンロードする形で持ち出せることとなるため、漏えい・流出のリスクはあります。
そこで、上記２のうち、①リモートデスクトップ方式または②仮想デスクトップ方式を採用し、手元の端末にデータが残らないシステムとすることで、漏えい・流出のリスクを避けることができます。
この点、機密情報の取扱いについての記事ではありませんが、株式会社 NTT ドコモにおいては、仮想デスクトップ方式（NTT グループが開発した s-Work Square というシステム）を採用し、従業員の手元の端末にはデータを保存できない仕組みにして社内サーバでの管理を徹底した上で、社内で印刷した紙媒体資料の持ち帰りや USB メモリ等にデータを入れて持ち帰ることも禁止する、という取扱いにしているとのことで（※8）、一つ参考になります。
このほか、手元の端末へのデータ保存を許容しつつ、従業員によるアクセスやダウンロードのログを保存するという方法も考えられます。

※8　「在宅勤務・短時間勤務を活用する企業内弁護士の働き方　株式会社 NTT ドコモを例に」（NIBEN Frontier2020 年 5 月号 28 頁）
※9　なお、ペーパーレス化が進んでいない企業・法人においては、紙媒体資料の持ち出しを一切禁止するのは現実的でない場合もあるかもしれません。機密情報以外であれば、管理表を作成して持ち出し・返却を管理する等により、持ち出しを認めるという方法もあり得ます。

イ　営業秘密保護法制（不正競争防止法）からの観点　―秘密管理性―
技術的に端末にデータを保存できない仕組みにすることが可能としても、悪意を持った社員や第三者において機密情報等を持ち出されるリスクを完全になくすことはできません。このようなリスクは、技術のみをもって防止することは極めて困難であり、最終的には、営業秘密であれば不正競争防止法（個人情報であれば個人情報保護法）による保護や抑止効果等を期待するほかなく、万が一の場合でも法的保護を受けられるよう必要な体制を整えておくことは重要なこと

です。

営業秘密として不正競争防止法上保護されるためには、秘密管理性、有用性、非公知性の３つの要件を満たす必要があります（不正競争防止法２条６項）。そこで、テレワークの導入により、自宅などで営業秘密を扱えるとした場合に、これらの要件（特に秘密管理性）をみたすかどうかが問題となります。

この点については、経済産業省「営業秘密管理指針」や、当コラム執筆中にリリースされた、同「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）」が非常に参考になりますので、ポイントだけ指摘します。

○　秘密管理性の要件が満たされるためには、（a）自社が保有している情報のうち秘密として管理する情報の範囲を明確にするとともに、（b）当該情報に対する従業員の予見可能性を確保するために秘密管理措置を実施することが重要 ○　テレワークの実施にあたって、 ・　企業内部において紙媒体で保存している秘密情報を自宅に持ち帰る ・　企業の営業秘密を従業員が使用する勤務先貸与端末機器のローカルフォルダに保存する ・　従業員が、社外から会社サーバへアクセスする ・　外部クラウドを利用して営業秘密を管理する ・　従業員の個人所有のPC等を利用する（いわゆるBYOD） といった取り扱いを行なっても、直ちに営業秘密としての法的保護を失うわけではなく、ファイルに「㊙□」など秘密であることの表示を付す、アクセス制限をかけるなどの措置を講じることにより、不正競争防止法による法的保護を受けられる可能性がある。 （以上につき経済産業省「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）」1ないし8、12頁）。

ウ　営業秘密保護法制（不正競争防止法）からの観点　―不正行為や図利加害目的の立証―
仮に従業員による営業秘密の不正使用等があった場合、当該従業員の民事・刑事上の責任を追及するためには、当該従業員による持ち出し行為を立証することが必要になります。
テレワークを導入した場合には、データの複製等を自宅で行うことができることになり得るため、その複製行為等の立証に困難を伴う可能性があることは一応注意が必要です。（※10）

また、上記従業員の民事・刑事上の責任を追求するためには、「不正の利益を得る目的」または「営業秘密の保有者に損害を加える目的」（２つをまとめて「図利加害目的に」と呼ばれています。）の立証を要することもあります（不正競争防止法２条１項７号、21条１項など）。

例えば、ライバル企業に営業秘密を譲渡する目的で、従業員が営業秘密を無断で持ち出したとすれば、これは刑事罰の対象となり得ますが（不正競争防止法 21 条 1 項 3 号）、図利加害目的について、「社内規定に反していたが、テレワークで勤務するために必要だったので不正の利益を得る目的ではない」などと反論された場合に、どのように考えるべきでしょうか。

「不正の利益を得る目的」とは、公序良俗又は信義則に反する形で不当な利益を図る目的のことで、例えば、残業目的で、権限を有する上司の許可を得ずに、営業秘密が記載された文書や USB を自宅に持ち帰る行為はこれに当たらないと考えられています（経済産業省編「逐条解説不正競争防止法　令和元年 7 月 1 日施行版」250 頁）。
したがって、社内規定に抵触していたことのみをもって「不正の利益を得る目的」を認めることはできません。（※11）

結論としては、様々な周辺事情（間接事実）を積み重ねて「不正の利益を得る目的」を立証することになることとなり、例えば、ライバル企業への営業秘密の譲渡を立証できれば同目的を立証する上で積極的（決定的）な事情となるでしょうし、一方で、従業員においてテレワークで当該営業秘密を取り扱う業務上の必要があったことや、営業秘密を持ち出す必要があったこと（テレワークのシステムの使い勝手があまりに悪いことなど（※12））は、消極的な事情と評価され得るでしょう。
いずれにしても、テレワークの導入により図利加害目的の立証が困難になるという事態は、

この点について参考となる最近の判例（最判平成３０年１２月３日刑集７２巻６号６１８頁）を紹介しておきます。事案の概要は次のとおりです。

被告人は、自動車会社（A 社）の商品企画本部第一商品企画部所属の従業員として勤務し、同社が秘密として管理している同社の自動車の商品企画に関する情報等について、同社のサーバに保存されたそれらの情報にアクセスするための識別符号であるＩＤ及びパスワードを付与されていたところ、同業他社への転職直前に、以下のとおり２度にわたり、A 社のサーバーコンピュータに保存されていた営業秘密に係るデータファイル合計１２件の複製を作成した。
・　被告人の自宅において、A 社から貸与された PC を利用して A 社サーバにアクセスし、A 社の商品企画に関する情報等を自己所有のハードディスクに転送・複製した。
・　A 社テクニカルセンターにおいて、A 社から貸与された PC を利用して A 社サーバにアクセスし、A 社の商品企画に関する情報等を自己所有のハードディスクに転送・複製した。
被告人は、不正競争防止法２１条１項３号違反で起訴されたのに対して、業務関係データの整理を目的としたものであるなどと主張し、「不正の利益を得る目的」の有無等が争われた。

判決は、結論として、有罪（懲役１年、執行猶予３年）としています。その理由は概ね以下のとおりです。

- １件目の複製作成につき、被告人が複製した各データファイルを用いて勤務先会社の業務を遂行した事実はない上、同社の業務遂行のためにあえて同社から貸与されていたノートパソコンから私物のハードディスク等に各データファイルを複製する必要性も合理性も見いだせないので、A 社の業務遂行以外の目的によるものである。
- ２件目の複製作成につき、最終出社日の翌日に行ったもので同社の業務を遂行する必要がなかったことは明らかであるので、A 社の業務遂行以外の目的によるものである。
- その他の正当な目的の存在をうかがわせる事情もないなどの本件事実関係によれば、当該複製が被告人自身又は転職先その他の勤務先以外の第三者のために退職後に利用することを目的としたものであったことは合理的に推認できるから、被告人には法２１条１項３号にいう「不正の利益を得る目的」があったといえる。

※10　テレワークを導入しているか否かにかかわらず、複製等は会社にばれないように行うはずで、立証が容易でないことはあまり変わらないようにも思われます。もっとも、従業員によるアクセスやダウンロードのログを保存するということは一応有効と考えられます。

※11　社内規定への違反については、別途懲戒処分等の対象となり得ますので、明確な規定の整備はこのような事態の発生を防ぐ上では有用と考えられます。

※12　筆者の経験において、10 分程度 PC の作業をしないでいると接続が切れ、再度 ID と PASS の入力をしなければならないということがありました。なりすまし防止の観点からは有効な対策なのかもしれませんが、業務の効率性をあまりに損なうシステム設定は、社員による無断の持ち出しを促進しかねないように思います。

エ　まとめ

以上のとおり、テレワークにおいて、営業秘密等の機密情報を扱うことは技術的に可能であり、また営業秘密保護法制（不正競争防止法）との関係でもこれにより法的保護を受けられなくなるものでないと考えられます。

もっとも、不正競争防止法上保護されるためには、秘密であることの表示、アクセス制限などの措置を講じる必要がありますので、経済産業省「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）」を参考に、社内の体制についてきちんと検証する必要があるでしょう。

なお、テレワークを導入するにあたっては、得てしてデータの取扱いを厳格にする方向になりがちですが、ユーザー（従業員）にとって使いやすいものとなることも重要であること（使いにくいシステムだと、無断での持ち出しが起きやすくなってしまいます。）は改めて強調しておきたいと思います。

（参考文献）

蔦大輔「テレワーク・BYODに潜むサイバーリスクへの対応」（NBL1169号44頁）
森亮二「BYOD（個人所有端末の業務利用）の法的留意点」（NBL1019号24頁）
経済産業省「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）」

以上