論　説

テレワーク環境における知財実務上の留意点とその対策

平　井　佑　希*

抄　録　コロナ禍でテレワークが急速に普及した。オフィス以外の場所で業務を行うことができるようになったことで，資料やデータなどの情報の取り扱い方が変化したが，情報財を保護する知的財産法は，その影響を最も受ける法分野の１つである。

オフィス以外の場所で情報を活用するために，資料の複製や送信を行う機会も増えるが，その際には著作権法の観点からの注意が必要となる。また，テレワークの際に誤って開発中の製品情報などが漏洩するようなことがあれば，ライバル企業との競争力が低下するのはもちろん，特許や意匠出願に際して新規性が失われるリスクがある。また不正競争防止法に基づく営業秘密の保護の要件としては，その情報が公知ではないことや，有用な情報であることに加えて，その情報が秘密として管理されていることが要求されている。情報の扱い方が変わることによって，この秘密管理性が失われたり，形骸化してしまう可能性がある。

本稿ではテレワーク環境における留意点について，特に知的財産法の観点から，整理して説明する。

目　次

1．はじめに

「働き方改革」が叫ばれて早数年が経つ。2019年４月に働き方改革関連法が施行されたときには，その１年後にコロナ禍によって多くの企業がテレワークを導入することになるなどと，誰が予想できたであろうか。2020年の夏ころには，いったん状況は小康状態を迎え，テレワークの導入割合は減少したと伝えられたが，2020年の大晦日に東京の新規感染者数が1,000人を突破し，2021年１月７日には２回目の緊急事態宣言が発せられる事態となり，首都圏の緊急

* 弁護士・弁理士　Yuki HIRAI

事態宣言の期間延長を経て，３月21日に全国的に緊急事態宣言が解除となった。２回目の緊急事態宣言の中では，大きな柱の１つとして，テレワークを強力に推進し，出勤者の７割減を目指すとされた。

もともとテレワーク導入の効果の１つとして，災害時の事業継続性（Business Continuity）の確保が挙げられていたが，図らずもコロナ禍によってテレワークの普及はこれまでとは全く異なるステージに突入した。最初はやむなくテレワークを始めた人も多いと思うが，今後はそれぞれの企業，それぞれの働き方に合わせて，積極的にテレワークを活用していくことになるであろう。

一方，テレワークを導入すると時間的にも，場所的にも，働き方が変わるので，それに合わせてインフラ，労務，人事など様々な面での変化が求められる。本稿ではそのうち知的財産法の側面に焦点を当てて，テレワークを導入することに関連する知的財産法上の問題について考えてみたい。

2．テレワークの現状

2. 1　テレワークの導入状況に関する調査

(1) 東京都の調査

テレワークの導入状況に関する調査結果は，いくつか公表されている。それぞれ調査時期，規模，地域や対象とした企業などが異なるので，横並びで比較することはできない。

その中で，東京都は2020年３月と４月にテレワークの導入状況に関する緊急調査を行っている[1)]。緊急事態宣言が出されたのが2020年４月７日なので，その前後におけるテレワークの導入状況の変化を見るには良い資料である。

この３月の調査から４月の調査を比較すると，１か月の間に，テレワークを導入していると回答した東京都内の企業の割合は24.0％から62.7％と，約2.6倍に増加している。

なお，その後の東京都の調査では，2020年12月で51.4％，2021年１月の前半で57.1％，同月後半で63.5％と引き続き高い導入率を保っている。導入の規模としても2021年１月後半の調査では，テレワークを実施した社員が平均約５割，テレワークの回数も週３日以上の実施が約６割にのぼっている[2)]。

(2) J. D. パワーの調査

より地域を広げた調査としては，2020年８月下旬から９月下旬にかけて，株式会社ジェイ・ディー・パワージャパンが国内の企業を対象として行ったものがある[3)]。この調査によれば，テレワークの導入率は36％とされている。従業員数が多い企業ほど導入率が高く，従業員数が1,000人以上の企業での導入率は78％に上る。

東京都の調査結果と比べると，導入率が低くなっているが，調査対象が東京と全国で異なるので，地域差の影響が現れたのかもしれない。

(3) 今後の動向予想

では今後，テレワークの導入状況はどのように推移していくのだろうか。東京都の調査では，2020年12月にはテレワークの導入率が一旦51.4％まで減少したが，２回目の緊急事態宣言によって，再び63.5％まで上昇した。

１回目の緊急事態宣言が解除された後に行われた東京都の調査（６月）によれば，今後テレワークを「継続・拡大したい」が40.6％，「継続したいが拡大は考えていない」が39.8％であり，合わせると約80％の企業が継続の意向を示している。

単に疫病から免れるという消極的な理由ではなく，より積極的にテレワークのメリットを享受するためにテレワークを継続・拡大していく企業も出てくると予想される。従業員としても，多様な働き方を実現するためのツールの１つと

して，テレワークを望む人が増えてくるのではないだろうか。

テレワークの環境を整えておくことは，今後の企業経営や，多様かつ優秀な人材の確保のためには，有用な対策であると考える。

2. 2　テレワーク導入の際の課題

テレワークを導入する上での課題として，まっさきに思い浮かぶのは，「紙文化」や「はんこ文化」の高い壁である。奇しくもコロナ禍に入る直前の2019年12月，国際ロボット展で「押印ロボ」が展示され話題になったが，書類を紙で管理し，押印するという文化の見直しは，コロナ禍を契機として加速した。特許庁は，令和２年12月28日付で，特許庁関係手続における押印の見直しを行い，押印が大幅に省略されることになった[4)]。

前述のJ. D. パワーの調査でもテレワーク実施・推進においての課題として「オフィス内でしか行えない書類業務への対応」（２位：54％）と並んで上位を占めたのが，「セキュリティ」（１位：60％）と「社員のITリテラシー」（３位：54％）である。

我々弁護士のように，単独あるいは比較的少人数のユニットで業務を行う者ですら，紙文化や押印文化の壁を感じるくらいであるから，企業内でテレワークを進めていく際には尚更これらの壁を越えていく必要性は高いだろう。

そしてこの点は実は，本稿で扱う知的財産法上の問題とも，密接に関わる問題である。

3．著作権にまつわる問題

3. 1　スキャンも「複製」

テレワーク導入によって，様々なシーンで書類をコピーしたり，電子化することが増えたのではないだろうか。

社員が一堂に会しているのであれば，書類が１部あれば，みんなで回し読みもできる。しかしテレワークを導入して，各社員がそれぞれ自宅などで業務を行っている場合には，回し読みはできないので，各社員が書類にアクセスしたいと思えば，１部ずつコピーをして持ち帰るか，PDF化して自分のパソコンや外部メモリに保存したり，サーバにアップロードして他の社員とシェアしたりする必要がある。

書類を紙でコピーする行為が，著作権法でいう「複製」に当たるというのは，言葉どおりであるのでわかりやすいが，実はスキャンしてPDFとして保存する行為や，サーバにアップロードする行為も「複製」に当たる。

3. 2　雑誌，新聞などの複製

現在，新聞や専門雑誌などを会社で購入し，部署などで回し読みに供しているというケースは多いのではないだろうか。

著作権は，複製，公衆送信といった支分権に該当する行為を専有する権利であるが，回し読みすることは支分権に該当する行為ではないので，著作権を侵害することはない。また回し読みをしている中で，興味のある記事があった場合に，これを自分の資料としてコピーしたり，PDF化しておくことは，「複製」には当たるが，著作権法30条１項が規定する私的使用目的での複製として適法と考えられている。

これに対し，テレワークで会社に来ない人のために，雑誌や新聞をPDF化してメールで配ったり，共用サーバにアップロードする場合には，PDF化してパソコンやサーバに保存する行為が「複製」に当たるうえ，たとえ少人数であっても会社内で共有するために行われる複製は，私的使用目的での複製には当たらない（「個人的に又は家庭内その他これに準ずる限られた範囲内」における使用ではない。）とする見解が有力である。そうすると，このようにテレワーク中に部署内の情報共有のために雑誌や新聞を複

製するためには，著作権者の許諾を得る必要がある。出版社や新聞社によっては，出版者著作権管理機構（JCOPY）や日本複製権センター（JRRC）などの著作権等管理事業者にこういった複製の許諾業務を委託しており，そこが窓口となって許諾申請を行うことができるケースもある。そういったケースであれば，個々の著作権者に直接連絡を取る必要はないので，許諾の事務処理は比較的簡便に済む。またこういった著作権等管理事業者は，複製の都度申請する「個別許諾」のほかにも，一定の期間内であれば回数を問わずに複製可能な「包括許諾」の枠組みも用意しているので，こういった包括許諾を利用すれば，複製の都度許諾申請を行う手間が省ける。

一方，日本経済新聞などは企業内での利用頻度が多そうな新聞であるが，上記のような著作権等管理事業者を許諾窓口としておらず，自社で著作権管理を行っている。このような場合には，直接会社の方に許諾申請をする必要がある。

著作権等管理事業者を通じて許諾を得る場合でも，直接会社から許諾を得る場合でも，対象著作物の範囲や，許諾（利用）の条件などには注意が必要である。

3. 3　イントラネットと外部サーバ

著作権法上「公衆送信」からは同一構内での送信は除かれている。したがって，同一構内で運用されているイントラネットを使って同一構内の社内で資料を共有する行為については，イントラネットへの複製だけが問題となり，公衆送信権の問題は生じなかった。

これに対して，テレワークを導入して，各社員が自宅などの外部からでもアクセスできるようにすると，もはや同一構内での送信に止まらないので，公衆送信権の問題も生じる。

許諾の内容にもよるが，イントラネット上で共有することの許諾（複製の許諾）があったとしても，必ずしも外部からもアクセス可能なサーバ上で共有することの許諾（複製及び公衆送信の許諾）まで含意されているとは限らないので，イントラネットで共有していたものを同一構内以外の外部からアクセス可能にする場合には，注意が必要である。

3. 4　会議やセミナーでの資料共有

テレワークを導入して，オンラインの会議やセミナー（ウェビナー）の機会が格段に増えた。このようなオンラインセミナーやウェビナーで資料を共有する行為については，著作権法上どのように考えたら良いのだろうか。

まず，インターネット上で公開されている論文などの資料のリンクを送って，各自がサイトにアクセスする場合，リンクを貼るというのは支分権に該当する行為ではないので，著作権侵害の問題は生じない。

これに対して，一度自分のパソコンなどに資料を保存して，画面共有機能で参加者に示す場合，保存の段階で複製権，画面共有の段階で公衆送信権の問題が生じ得る。

ここで公衆送信権については，著作権法上「公衆」とは特定多数又は不特定少数と理解されている（著作権法２条５項を参照。）。逆に特定かつ少数は「公衆」には当たらないので，特定少数への送信は公衆送信権侵害にならない（例えば，メール送信などが典型。）。

何人までが少数で，何人からが多数なのかは，一概には言えないが，文化庁の「著作権なるほど質問箱」[5]では「50人を超えれば多数」という一応の基準が示されている。あくまでも一応の基準なので若干余裕を見るとして，数人～十数人程度の部署のメンバーでオンライン会議を行うような場合に，その会議中に資料等が画面共有されるとしても，それは公衆送信には当たらないと考えて良い。

ただし公衆には不特定少数も含まれる。そし

て，この「不特定」というのは，例えば誰でも申込可能なウェビナーであれば，仮に不人気で参加者が結果的に１人であっても，不特定の範囲から募集した結果の「１人」であるので，不特定少数であると解釈されている。したがって，その１人に送信をすることは，１対１の通信であるが，公衆送信に当たる。

3. 5　著作権に関する小括

著作権は支分権に該当する行為に対して及ぶ。みんなで資料を共有するという同じ目的から行われる行為であっても，１部の資料をみんなで回し読みする場合と，コピーして配る場合，PDF化して送信する場合では，それぞれ著作権法上の扱いは異なる。

テレワークによって場所的な離隔が生じることで，同じようなことをしようとしても，「複製」の頻度が上がったり，態様が変わったりする。そのように複製が生じる場合には，改めて著作権法の観点からの注意が必要である。

また場所的な離隔によって「送信」の頻度も上がり，態様も変わってくる。送信を特定多数又は不特定少数に対して行うと，「公衆送信」となり，やはり著作権法の観点からの注意が必要である。

4．特許や意匠などにまつわる問題

4. 1　新 規 性

特許法や意匠法といったいわゆる創作法において，特許や意匠登録を受けるためには，出願前に公然知られたものではないことなどが要求されており，「新規性」（novelty）の要件などと呼ばれている（特許法では29条１項，意匠法では３条１項。以下では特に区別する必要がない限り，特許法の条文を指摘して説明する。）。

新規性について，１号，２号の「公然」とは必ずしも多数の者ということを意味せず，きわめて少数の者が知っている場合でも，これらの者が秘密保持義務を有しない者であれば「公然」に該当し，逆に多数者が知っていても，これらの者が秘密保持義務を有しているのであれば，「公然」には該当しないと説明されている。

また，３号の「頒布」や「利用可能」は不特定者が閲覧，アクセス可能な状態になれば足りると解されており，文書が現に閲覧されたり，電気通信回線を通じて現にアクセスがなくても頒布や利用可能に当たると解されている[6)]。

4. 2　テレワークによる新規性喪失のリスク

テレワークに伴って，情報を持ち出したり，外部からアクセスしたりする機会は格段に増える。例えば家に持ち帰るためにデータを記録したパソコンや外部メモリを紛失したり，誤って添付ファイルを送信したり，サーバの共有設定を誤り第三者も閲覧可能な状態にしたり，情報を取り扱う場所が変わる（又は増える）ことにより，情報が漏洩するリスクは増加する。

また社員が一堂に会している場合であれば，詳しい人に聞きながらパソコンを操作するなどの対応もできるが，テレワークとなるとなかなかそうもいかない。テレワークの課題としてセキュリティやITリテラシーの問題が挙げられているのも肯ける。

仮にそのようにして漏洩した情報が開発中の製品情報であった場合，そこで開示された内容については新規性を失うリスクがある。

4. 3　新規性喪失の例外

日本の特許法や意匠法では，一定の場合に，公知になってしまったとしても新規性が失われないという，新規性喪失の例外規定が設けられている（特許法30条）。仮に誤って開発中の製品情報が漏洩してしまったような場合には，特許を受ける権利を有する者の意に反して公知になったものとして，特許法30条１項により，１

年間は新規性が失われていないものとみなされることになる。

しかし，この新規性喪失の例外規定は国によって期間や要件が異なるので，日本において新規性が確保できるとしても，他の国でも同様に新規性が確保できるとは限らない。例えば欧州特許条約（EPC）55条では，新規性喪失の例外の期間は６か月とされ，要件も（a）出願人又はその法律上の前権利者に対する明らかな濫用の場合と（b）出願人又はその法律上の前権利者が，国際博覧会に関する条約にいう公式又は公認の国際博覧会に発明を展示したことに限定されている。

また，特許法30条は特許を受ける権利を有する者自身との関係で新規性が失われていないものとみなされるという規定であり，出願日の遡及という効果を有するものではない。したがって，新規性喪失の事情が発生してから，その後特許を受ける権利を有する者が出願するまでの間に，第三者が同様の発明について特許出願を行って特許を取得してしまうリスクはあるうえ，自身の特許出願については拡大先願（特許法29条の２）の問題が生じる。

したがって，この規定があるから安心などと思わず，セキュリティやITリテラシーに起因する新規性喪失のリスクを防止する取り組みが必要である。

4. 4　代表的なリスクと対策

(1) 紛失のリスク

新規性を喪失するリスクとして，まっさきに思い浮かぶのは，製品情報を記録したパソコンや外部メモリなどの紛失である。特に，自宅のみで，完全にテレワークに切り替えてしまうのではなく，何日かは会社，何日かは自宅で業務を行うというような場合には，パソコンなどを持ち運ぶ回数も増えるであろうから，その過程で紛失してしまうリスクも増加する。

その対策としては，まずテレワークに用いる端末のシンクライアント化が挙げられる。ひとことに「テレワーク」と言っても，その実現のための方法は，総務省のガイドライン[7]で６つの方法に分類されている。そのうちの例えば「リモートデスクトップ方式」は，自宅などからテレワーク用の端末を用いて，インターネットなどを通じて，オフィスにある端末にアクセスし，このオフィスの端末を自宅から遠隔操作するというものである。

この場合，テレワーク用の端末はオフィスの端末を操作するための操作窓に過ぎず，データなどはオフィスの端末に保存され，テレワーク用の端末には保存されない。このように，テレワーク用の端末にデータを保存しない方式を「シンクライアント（Thin Client）方式」と呼んでいる。シンクライアント方式を採用していれば，万が一テレワーク用の端末を紛失した場合でも，そこにはデータは保存されていないので，データ漏洩などのリスクを回避することができる。

またシンクライアント方式を採用しない場合であっても，パソコンや外部メモリを開くためのパスワードを設定しておくことが考えられる。現在の多くのパソコンでは起動時に指紋認証や顔認証，あるいはパスワード入力が求められる。しかし外部メモリに関しては未だパスワード入力等が不要なものも使用されているので，外部メモリを使用しない，使用する場合にはパスワード入力等を要求するなどの対応が求められる。

また，一定回数パスワード認証に失敗した場合にデータを消去することができるツールや，遠隔操作によってデータを消去することができるツールも提供されている。こういったツールを合わせて活用することで，さらに紛失の際のリスクを軽減することができる。

(2) 誤操作のリスク

これは必ずしもテレワークに特有の問題ではないかもしれないが，テレワーク導入を契機として，それまで利用していなかった新たなツールやサービスの利用を開始するケースもある。また，オフィスにいればパソコン操作に長けた同僚に気軽に操作方法などを尋ねることができるかもしれないが，テレワークの場合にはなかなかそうもいかないことが想定される。そのようなことにも起因して，テレワークの最中には誤操作が生じるリスクは増加し得る。

また書類などを電子化して，メール添付などでやりとりをするケースが増えると，誤った相手に，あるいは誤ったファイルを送信してしまうリスクも増加する。例えば守秘義務を負っていない相手に対して，開発中の製品情報が記載されたファイルを誤送信してしまったり，共有設定を誤って第三者も閲覧しうる状態にしてしまったりすれば，新規性喪失のリスクがある。

そういったリスクを軽減するには，社員のITリテラシーを向上させるということが重要であることは言うまでもないが，企業におけるルールとしてそういったリスクが生じにくい状況を作り出すという観点も大事である。

例えばファイルやフォルダへのアクセス権限を管理することで，必要な社員だけがデータにアクセスすることができるようにすることも１つの方法である。またメール添付ではいったん送信されたファイルは戻らないが，サーバにアップロードして相手にダウンロードしてもらう方法であれば，送信後であってもダウンロードが行われるまでの間はファイルを削除することができる。

これに対して，添付ファイルを暗号化し，別メールでパスワードを送るという方式は，広く採用されているが，セキュリティの観点からはあまり効果的ではないとされており，2020年11月17日のデジタル改革担当大臣の定例会見で廃止する方針であることが明らかにされた[8)]。

(3) ウイルス感染などのリスク

この点も必ずしもテレワークに特有の問題ではないかもしれないが，テレワークによって企業の管理が及びにくいネット環境で資料を取り扱う機会が増えると，ウイルスなど悪意のあるプログラムの脅威にさらされるリスクは増加する。

その対策として，まず考えられるのがフィルタリングソフトやウイルス対策ソフトの導入である。ウェブサイトの中には，閲覧者に対して悪意のあるソフトウェアをインストールしようとするような危険なサイトもある。フィルタリングソフトはそのような危険なウェブサイトにアクセスを禁止したり，アクセスしようとした場合に警告を発するものである。またウイルス対策ソフトは，悪意のあるソフトウェアを誤ってダウンロードしてしまった場合でも，その実行などを抑制するものである。こういったソフトウェアを導入することで，社員を危険なウェブサイトから遠ざけ，またウイルスへの感染から守ることができる。ただし，安全性を高めるためには，危険なウェブサイトやウイルスのリストが最新でなければならないので，これらのソフトウェアの定期的なアップデートを怠らないことも重要である。

またテレワークに私物のパソコンを使用させる（BYOD：Bring Your Own Device方式）のではなく，企業において必要なセキュリティ対策を行ったパソコンのみを使用させるということも有益である。あらかじめフィルタリングソフトなどの必要なソフトをインストールしておく一方で，不必要なソフトのインストールを禁止することもできるうえ，データの保存や外部メモリの使用などについて制限を設けることもできる。私物のパソコンは，家族で共用している可能性もあるので，その観点からも指定されたパソコンのみを使用させることは，セキュリ

ティの向上に役立つ。

さらに機密性の高い業務上の情報を取り扱う以上，自宅等における通信環境に関しても，ステルス機能やフィルタリング機能などのセキュリティの充実したルータを導入したり，無線LANを使用する場合には，WPA2，WPA3といったより堅牢なプロトコルを使用するなどの対策を講じることが大事である。

またテレワークに用いる通信にVPN（Virtual Personal Network）を使用することも推奨されている。VPNとは，比喩的に言えば，通信を暗号化することで通信の「トンネル」を構築して，その中で通信を行う手段である。暗号化されたトンネルの中を覗き見されないというメリットがある。

ホテルや店舗などで利用できる公衆無線LANにおいては，データ傍受のリスクやアクセスポイントのなりすましによる情報漏洩のリスクもある。極力そういった通信環境を利用しなくても済むように，企業でモバイルルータを貸与するなどの対応を行うことが望ましいと考える。

(4) その他のリスク

公衆無線LANの問題にも関連するが，店舗などの公の場において，秘密情報を含む内容のやり取りを行うことには，通信セキュリティの問題だけではなく，背後からの盗み見や盗み聞きのリスクもある。

働く場所や時間の制約が少ないのがテレワークのメリットであるが，その時の業務内容などに応じてTPOをわきまえることは重要である。現在のスマートフォンには標準で録音，録画，撮影機能が搭載されているので，公の場での会話が録音されたり，製品情報を表示したパソコン画面を背後から撮影されたりする危険性は十分にある。

4. 5 特許や意匠に関する小括

新たな製品の技術やデザインに関する情報の漏洩は，特許出願や意匠出願にあたって新規性喪失のリスクになる。新規性喪失の例外規定は設けられているが，万全ではない。

個々の社員がITリテラシーを高めることも重要であるが，ヒューマンエラーを100％防止することはできない。指定端末の利用など，会社のルール，運用面からも，十分な対策をとることが重要である。

5． 営業秘密にまつわる問題

5. 1 営業秘密としての保護の重要性

日本国内における特許出願件数は，2007年に40万件を下回って以降右肩下がりで推移し，2019年には約30万件となっている[9)]。その一方でPCT出願の件数は増加しており，2019年には５万件を超えた[10)]。

特許制度は「公開代償」と「属地主義」の原則を採用しており，一国にだけ出願しても全世界に向けて公開されてしまうのに対し，その代償として得られる特許権の効力は，出願したその国にしか及ばない。

そのため，何でもとにかく出願してしまうのではなく，発明の内容などに応じて，出願すべきものについては日本に限らず必要な国や地域で出願を行い，営業秘密としての保護を目指すものはノウハウとして管理するというメリハリのある知財戦略は重要であり，前述の出願件数の推移にはそのような知財戦略も影響しているのかもしれない。

5. 2 営業秘密の保護

一般に営業秘密は，秘密保持契約などの契約に基づいて，又は不正競争防止法の規定に基づいて，保護されている。

このうち契約に基づく保護の場合には，どのような情報を，どのような範囲で保護するのかを当事者間の合意によって決定できるので，目的に応じて柔軟な保護を図ることができる。他方，契約の効果は当事者間にしか及ばないので，契約関係にない第三者との間で保護を図ることができない。

これに対し不正競争防止法に基づく保護の場合は，同法２条６項が定める「営業秘密」の要件を満たす必要がある。具体的には，①秘密として管理されていること（秘密管理性），②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ること（有用性）及び③公然と知られていないこと（非公知性）の３要件である。この３要件を満たす営業秘密を，不正競争防止法２条１項４～10号が規定する類型で使用等すると不正競争行為に当たり，差止めや損害賠償請求の対象となる。契約による保護と異なり，不正競争防止法に基づく保護であれば，契約当事者以外にも効力が及ぶ。

5. 3　秘密管理性の要件

(1) 我が国の秘密管理性の要件

上記のとおり，不正競争防止法上の「営業秘密」に該当するためには，秘密管理性を満たす必要がある。非公知でしかも有用な情報であれば，それだけでも法的に保護しても良さそうではあるが，不正競争防止法はさらに秘密管理性を要求している。

非公知性と有用性に加えて秘密管理性を要求している趣旨は，営業秘密として法的に保護される範囲を明確にし，従業員や取引先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る[11)]。これによって当該情報に接する者は，これは秘密情報だから気をつけなければいけない，と理解した上で取り扱うことができるわけである。

例えば，ある情報が社内に留まっている限りにおいては，非公知性は失われていないと言えるが，社内の誰でも自由にアクセスできるような状態になっていれば秘密管理性は失われているということもありえる。このように非公知でも営業秘密に当たらないというケースもありえるので，営業秘密としての保護を受けるためには，非公知性を保つことはもちろんのこと，情報をどのように管理するかという点も非常に重要になってくる。

(2) Trips協定など

秘密管理性の要件については，Trips協定39条（2）（c）においても「当該情報を合法的に管理する者により，当該情報を秘密として保持するための，状況に応じた合理的な措置がとられていること」と規定されている。

アメリカの経済スパイ法（Economic Espionage Act of 1996）の1839条(3)(A）でも情報の保有者が秘密として保持するための合理的な手段を講じていることを要件としている。2016年に成立した営業秘密保護法（Defend Trade Secrets Act of 2016）は，経済スパイ法の1836条を改正し，民事上の営業秘密の保護を追加したものであるので，営業秘密の定義としては，経済スパイ法のものを踏襲している。

EUの営業秘密指令（Directive 2016/943）の２条（1）（c）でも，情報の保有者が，当該情報を秘密として保持するための，状況に応じた合理的な措置を講じていることを営業秘密の要件としている。

このように若干の規定ぶりは異なるが，秘密管理性のような要件を求めるというのは，一般的なものと言えそうである。

5. 4　秘密管理措置

秘密情報として管理していると言えるためには，秘密管理の対象となる情報を区分して，営業秘密であることを示すという秘密管理措置が

取られている必要がある。

情報の区分については，必ずしも紙の資料１枚ずつや電子ファイル１つずつについて秘密情報か否かを区分する必要はなく，例えば紙の資料を収納するファイルごと，そのファイルを格納しているロッカーごと，電子ファイルを格納するフォルダごとなど，一定のまとまりごとに区分することで足りるとされている（そのため，合理的区分などと呼ばれている。）。

またそのようにして合理的に区分された情報について，「秘密」，「㊙」，「Confidential」など，秘密である旨表示をしたり，IDやパスワードなどでアクセスできる者を限定したり，秘密保持契約を締結するなどして，それらが秘密として守るべき情報であることを示すことが必要である。ただし，従業員等が秘密情報であることを理解できることが大事であるので，単に「秘密」などと表示されているか否かといったように形式的に判断されるものではなく，社内の認知度合いやルールの運用状況なども踏まえて，予測可能性が確保されているか否かを判断することになる。

5. 5　秘密管理措置の形骸化

秘密管理措置が取られているか否かの判断は，実質的に行われる。形式的には秘密管理措置が存在しても，実際の運用等に照らして形骸化していると評価されてしまうと，秘密管理性は否定されてしまう。

裁判例では，ある資料の原本について仮に一定の管理がされていたとしても，社員がそこに記載された情報をノートに転記することが日常的に認められていたことなどを捉えて，秘密管理措置は実効性を失い，形骸化していたと認定されたものがある（知財高判平28・12・21（平28(ネ)10079））。

また何にでも「秘密」と書いていればいいというものでもなく，むしろそのような運用は，真に秘密として取り扱うべき情報の範囲を不明確にし，従業員等の予測可能性も低下させる。

このように，秘密管理措置が取られているか否かという点については，単に形式的にそのような措置が存在するというだけでは意味がない。社内での運用としても適切に合理的な区分と表示が行われ，社内での告知や教育などによって，その情報を秘密情報として扱わなければならないことが理解されていることが重要になってくる。

5. 6　テレワークに伴う代表的なリスクと対策

営業秘密との関連において，テレワークの導入に伴い生じうるリスクとしては，公知性の喪失と秘密管理性の喪失である。このうちの公知性の喪失については，上記4. 4において特許や意匠に関して述べたところが基本的には妥当するので，説明を省略し，以下では，テレワークの導入が秘密管理性に与える影響について説明する。

なお，4. 4で説明したようなケースで，幸いにして新規性が失われなかったような場合でも，管理が甘い状況が常態化すれば，秘密管理性を失わせるリスクにもなるので，下記（1）で説明するようなマニュアルや運用の見直しを行うことが大事である。

（1）秘密管理措置の見直し

まず，テレワークの導入により，情報の所在や移動の態様が変化する。そのため従来テレワークを前提とせずに規定されていた情報管理のマニュアルや運用が，テレワークを導入したことによって適合しなくなる可能性がある。

例えば，「社外持出禁止」という表示が付された資料があったとする。従来はオフィスで業務を行うことが中心であったため，そのとおりの運用がされていたとしても，テレワークの導

入に伴って社外への持ち出しが日常的に行われるようになってしまえば，そのような秘密管理措置は形骸化していると評価されるリスクが生じる。

また資料の原本や原データには秘密管理措置が施されているとしても，テレワークに当たって，コピーや転記が日常的に行われ，そのコピー等の取り扱いについて特段の指示等もされていなければ，やはり秘密管理措置が形骸化していると評価されるリスクが生じる。

テレワークの導入に当たっては，テレワークも含めた業務実態に合った情報管理の方法が必要になってくるので，この機会に情報管理のマニュアルや運用を見直すことも大事である。

(2) 表示の喪失への対応

合理的区分の箇所で説明したが，秘密管理措置としては，紙の資料１枚ずつや電子ファイル１つずつについて「秘密」などと表示する必要はない。

例えばファイルに「秘密」と表示して秘密管理を行っていたような場合に，テレワークに際してそのうちの必要な箇所だけコピーを取って自宅に持ち帰るなどした場合，コピーからは秘密である旨が読み取れなくなってしまう。コピーを取った本人は，「秘密」と表示されたファイルからコピーを取っているので，秘密情報であることを認識はできているが，その先でコピーを受け取った側の者は，秘密情報であることが認識できない状態になってしまう。このように，秘密管理措置の具体的な態様によっては，情報の移動に伴って秘密である旨の表示が喪失してしまうリスクがある。

このようなリスクを回避するためには，情報のコピーや移動に関するルールを整備するとともに，コピーなどに秘密である旨を表示するなどの運用を心がけることが大事である。

5. 7　営業秘密に関する小括

営業秘密として保護されるためには，単に結果として非公知であるだけでは足りず，秘密として管理されていることが必要である。

秘密として管理されているか否かは，秘密情報とそれ以外の情報との合理的な区分と，区分された情報が秘密情報であることがわかるということが大事であるが，その判断は実質的なものであって，秘密管理措置を形骸化させてはならない。

テレワークによって情報の所在や移動の態様は変化するので，マニュアルや運用を含めて，情報管理のあり方を見直すことが重要である。

6．テレワークにまつわる情報漏洩等の実例

最後になるが，テレワークに際して実際に情報が漏洩してしまった例を紹介する。2020年もいくつかの情報漏洩事案があったが，個人情報保護委員会がテレワークに際して情報が漏洩した事例を２つ公表している[12)]。

１つ目の事例は，テレワーク中の社員がSNSで知り合った第三者からウイルスが添付された電子メールを受領したことがきっかけでPCがウイルスに感染し，出勤時にそのPCを社内ネットワークに接続したことで，社内システムの情報が外部に漏えいしたという事例である。これは社員のITリテラシーを向上させるとともに，上記4. 4 (3)で説明したような対策をしっかりと講じることで防げた事案であるように思う。

２つ目の事例は，脆弱性があるVPN機器への不正アクセスにより社員の認証情報等が外部に漏えいしたという事例である。これはテレワークへの対応として急遽遊休のVPN機器を使用してしまったことにより生じてしまった事案のようである。これも上記4. 4 (3) で説明したような対策によって防げた事案であるよう

に思われるが，加えてパソコンや通信機器のシステムアップデートをきちんと行っておくことも重要であることを示している。

7．おわりに

以上のとおり，テレワークに関しては，知的財産法の側面だけから見ても，著作権を侵害しないように気をつけたり，発明や意匠の新規性が失われないように気をつけたり，営業秘密の秘密管理性が失われないように気をつけたり，様々な影響がある。

しかし，テレワークの導入によって，生産性の向上や優秀な人材の確保，コストの低減など積極的なメリットを得ることも期待できる。また今回のような事態が生じた場合の事業継続性を確保する上でもテレワークは有用である。

必要な対策はしっかりと講じた上で，会社の実態に合ったテレワークを導入していくことが重要である。

注　記

1）東京都報道発表資料（2020年５月11日）
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2020/05/12/10.html

2）東京都報道発表資料（2021年２月５日）
https://www.metro.tokyo.lg.jp/tosei/hodohappyo/press/2021/02/05/27.html
（参照日：2021年３月27日）

3）https://prtimes.jp/main/html/rd/p/000000081.000042677.html

4）https://www.jpo.go.jp/system/process/shutugan/madoguchi/info/oin-minaoshi.html

5）https://pf.bunka.go.jp/chosaku/chosakuken/naruhodo/index.asp

6）特許庁編「工業所有権法（産業財産権法）逐条解説」［第21版］（発明推進協会）86-87頁

7）テレワークセキュリティガイドライン［第４版］
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000200.html

8）ITmedia NEWS「霞ヶ関でパスワード付きzipファイルを廃止へ」
https://www.itmedia.co.jp/news/articles/2011/17/news150.html（参照日：2021年４月23日）

9）特許行政年次報告書2020年版＜統計・資料編＞
https://www.jpo.go.jp/resources/report/nenji/2020/index.html#toukei_shiryou

10）PCT年次報告2020
https://www.wipo.int/edocs/pubdocs/en/wipo_pub_901_2020.pdf

11）営業秘密管理指針
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

12）テレワークに伴う個人情報漏えい事案に関する注意事項
https://www.ppc.go.jp/news/careful_information/telework/

（URL参照日は２）及び８）を除き全て2021年１月８日）

（原稿受領日　2021年１月８日）