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）

経済産業省知的財産政策室

令和２年５月７日

はじめに

昨今の情勢に鑑み、多くの企業でテレワークが実施されています。テレワークの実施にあたっては、日頃は企業内部で厳密に保管されている情報を紙媒体で持ち帰って、あるいは、自宅等外部から共有ドライブにアクセスして業務を遂行することも生じます。

一方で、企業の保有する技術情報、営業情報、顧客情報などは、秘密としておくことで自社の競争力を高め、また、他社との差別化を図ることができる情報も多くあり、これらが一度漏えいしてしまうと、情報資産としての価値が失われるだけでなく、企業経営にも甚大な影響を及ぼしかねません。

こうした中で、秘密情報を持ち帰らせることなどによる情報漏えいリスクや法的保護の毀損への懸念から、テレワークへの切り替えを躊躇するケースも想定されますが、適切な管理を行いながらテレワークを推進することは可能と考えられます。

そこで、主に、不正競争防止法上の「営業秘密の保護」の観点から、企業の秘密情報を適切に守りながら、テレワークを実施していく上でのポイントをまとめました。

（本資料は、今後、必要に応じ、改訂を行っていくことを予定しています。）

なお、本資料は、あくまで不正競争防止法上の「営業秘密の保護」の観点から記載しているものです。これからテレワークへの切り替えを検討されている方向けには、テレワーク環境の整備、テレワーク時のセキュリティ確保の方策等について、以下の公表資料が参考になりますので、本資料と併せてご参照ください。

・総務省「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

※１：本資料の以下に記載している内容は、経済産業省が発刊している「営業秘密管理指針」、「秘密情報の保護ハンドブック」等の内容を踏まえ、作成したものです。「営業秘密管理指針」は、不正競争防止法によって差止め等の保護を受けるために必要となる最低限の水準の対策を示しており、一方で、「秘密情報の保護ハンドブック」は、漏えい防止ないし漏えい時に推奨される（高度なものも含めた）包括的対策について掲載しています。

更に詳細な内容を御覧になりたい場合には、下記のページからそれぞれの冊子をダウンロードしてご参照ください。

・営業秘密管理指針
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf
・秘密情報の保護ハンドブック
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

なお、本資料で記載している対策例は、必ずしも営業秘密として法的保護を受けるための“最低限の水準の対策”だけではなく、「秘密情報の保護ハンドブック」に掲載されているような秘密情報の漏えい防止に有効な“推奨的な措置”も多く含みます。したがって、必ずしも本資料に記載の対策について網羅的に実施する必要はありません。実際には、以下の対策例を参考にしながら、各社の事業規模や取り扱う情報の性質などに応

じて取捨選択し、合理的で適切な情報漏えい対策を検討・実施していくことが求められます。

※２：不正競争防止法における「営業秘密」の保護：
不正競争防止法では、
①秘密として管理されていること（秘密管理性）、
②有用な技術上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）
の３つの要件を満たす「営業秘密」（第２条第６項）について、その不正な取得や使用等に対し、営業上の利益を侵害された者からの差止め、損害賠償請求などの民事救済措置のほか、侵害行為を行った者に対する刑事的措置（懲役刑・罰金刑）を規定しています。
不正競争防止法と営業秘密の保護について詳細な内容を御覧になりたい場合には、下記の冊子をダウンロードしてご参照ください。
・不正競争防止法２０１９
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/201909_unfaircompetitiontextrev.pdf

※３：本資料に関するお問い合わせ
経済産業省　経済産業政策局　知的財産政策室
電　話：０３－３５０１－３７５２（直通）
ＦＡＸ：０３－３５０１－３５８０

目　　次

Ｑ１

当社は、今までテレワークに対応した準備をしてきませんでしたが、昨今の情勢に鑑み、従業員のテレワークを認めたいと考えています。テレワークにあたってはこれまで企業の内部で保管していた営業秘密に該当する秘密情報も一部持ち帰って作業を行うなどの取り扱いを検討する必要がありそうです。営業秘密としての保護との関係が気になるところですが、まずは、どのような対応から始めたらよいのでしょうか。

Ａ）

テレワークへの切り替えにあたって、改めて、秘密情報の管理の態様や諸規程の整備状況を確認し、必要に応じて見直しを図ることが有用と考えられます。

具体的には、

① 営業秘密管理規程や情報取扱規定、セキュリティ規定等の社内規程がテレワークに即した内容になっているかの確認・改訂、

②当該諸規程について従業員（派遣労働者も含みます。）への周知徹底（メールによるリマインドやｅ－ラーニングの実施等）、

③情報の性質に応じた当該情報への適切なアクセス権者の設定、

④「㊙」（マル秘）・「社内限り」といった秘密であることの表示の付記、

⑤ＩＤ・パスワードの設定、

といった対応をとることが考えられます。

不正競争防止法が求めている営業秘密該当性の３要件のうち、テレワークへの切り替えにあたっては、特に、秘密管理性要件をどのように確保するかについて、悩まれることもあると思います。この秘密管理性要件の趣旨は、「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化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」ことにあります〔詳細⇒「営業秘密管理指針」４～５頁〕。

そこで、まず、会社として、自社が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ために、どのような措置（秘密管理措置）を実施するかを検討する必要があります。

例えば、営業秘密管理規程や情報取扱規程、セキュリティ規程等を設けている場合、「秘密として管理しようとする情報」が当該規程上の「秘密情報」等に含まれるかを確認することが有用です。また、各種情報取扱規程等との関係では、テレワークの実施にあたり、秘密情報等の社外への持ち出しを認めることが予想されますが、一方で、各種情報取扱規程等において、「秘密情報の社外への持ち出し禁止」などとのみ規定されている場合

には、テレワークの実施によって、当該規程等が形骸化することになり、ひいては、従業員の予見可能性を減退させる可能性も出てきます。

そこで、各種情報取扱規程等の関連規程を改めて見直し、通常勤務における情報の取り扱いに関する規定に加えて、テレワークの実施を念頭に、必要な場合には秘密情報の社外への持ち出しを認めつつ、その場合のルール（秘密管理措置）を定めること（各種情報取扱規程等の見直しも含みます。）が考えられます。

その他、従前から取り組んでいるものもあるかと思いますが、テレワーク開始にあたって、改めて、従業員の予見可能性を確保するために、情報の性質に応じた当該情報への適切なアクセス権者の設定、秘密情報が含まれる媒体への「㊙」（マル秘）・「社内限り」といった秘密であることの表示の付記、ＩＤ・パスワードの設定等の措置（各種情報取扱規程等におけるルールの設定状況及び実施状況）を再確認し、必要に応じ追加的措置をとることも有用です。

なお、テレワーク実施の過程で上長等への申請や許可の取得を求めるべきケースも想定されますが、テレワークの実効性を確保するため、申請・許可を伝統的な「捺印」ではなく、「電子的方法」によることができるよう、また、申請等の履歴データを残すという意味でも、必要に応じて関連規程の確認・見直しをすることも考えられます。

具体的な措置の方法については、Ｑ２以降もご参照ください。

また、テレワーク環境の整備、テレワーク時のセキュリティ確保の方策等については、「はじめに」でも紹介しましたが、以下の公表資料も参考になります。

・総務省「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

Ｑ２
　テレワークの実施にあたって、当社が紙媒体で管理している秘密情報（重要書類）を従業員が自宅等へ持ち帰る必要が生じています。このような場合であっても、営業秘密として保護されるのでしょうか。

Ａ）
　テレワークの実施にあたって、通常、企業内部において紙媒体で保存している秘密情報（重要書類）を、自宅等に持ち帰ったとしても、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。
　以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として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ります。

　秘密管理性要件の趣旨は、Ｑ１に記載のとおり、「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化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」ことにあります。

　したがって、例えば、持出しをする秘密情報が紙媒体の場合、当該書面に「㊙」（マル秘）・「社内限り」等の秘密であることの表示を付すことによって、従業員の予見可能性を確保するといった方法が考えられます。

　この他、必ずしも営業秘密として保護されるために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、以下のような秘密情報（重要書類）を社外に持ち出すに当たってのルールを整備することも考えられます。
・持ち出しを認める書類を厳選する
・持ち出しにあたって上長等の事前許可を必要とする
・持ち出しをした者・書類・期間を一覧で管理する
・持ち出しをした際の管理方法を徹底させる（書類を机上に放置しない等）
・業務上の必要がなくなった場合には返却を義務付ける、あるいはシュレッダーで裁断するなどの秘密保持に資する安全な方法による廃棄を義務付ける　等

　また、テレワーク中に従業員による書類のコピーやファイルの印刷を認める場合もあるかもしれません。その場合には、上記と同様に、以下のようなファイルをコピー等するにあたってのルールを整備することも考えられます。
・コピー等をした際に当該書面に「㊙」（マル秘）・「社内限り」等の秘密であることの表示が付されるように設定をしておく
・コピー等を認めるファイルを厳選する
・コピー等にあたって上長等の事前許可を必要とする
・コピー等をした者・書類を一覧で管理する

・コピー等をした際の管理方法を徹底させる（書類を机上に放置しない等）
・業務上の必要がなくなった場合には返却を義務付ける、あるいはシュレッダーで裁断するなどの秘密保持に資する安全な方法による廃棄を義務付ける　等

これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

なお、紙媒体は、技術的に複製を制限することや、第三者への提供等を制限することが困難ですので、中長期的には、可能な範囲でペーパーレス化を進めることも、有用です。

Ｑ３
　テレワークの実施にあたって、当社が電子データで管理している営業秘密を、各従業員の社用ＰＣなど当社が貸与した端末機器（勤務先貸与端末機器）のローカルフォルダに保存する必要が生じています。このような場合であっても、営業秘密として保護されるのでしょうか。

Ａ）
　テレワークの実施にあたって、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ことを認めたとしても、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。
　以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として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ります。

　秘密管理性要件の趣旨は、Ｑ１に記載のとおり、「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化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」ことにあります。

　したがって、例えば、持出しをするデータや保存先のローカルフォルダについて、ＩＤ・パスワードによるアクセス制限を実施する、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すことによって、従業員の予見可能性を確保するといった方法が考えられます。

　この他、必ずしも営業秘密として保護されるために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、以下のようなローカルフォルダへの保存にあたってのルールを整備することも考えられます。
・ローカルフォルダへの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
・できる限り私物端末機器ではなく勤務先貸与端末機器を使用させる
・勤務先貸与端末機器には勤務先が承認していないソフトをインストールしない（勤務先貸与端末機器に技術的な設定変更制限が可能であれば設定する）
・私用・家族との共用を許可しない
・保存をする勤務先貸与端末機器には勤務先所定のウイルス対策ソフトのインストールを徹底する等十分なセキュリティ対策を行う
・保存をした者・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付ける　等

また、質問への直接の回答ではありませんが、電子データの管理という点では、勤務先の同僚等とメールでやりとりをする場合、営業秘密である添付ファイルへのパスワード設定を徹底させることも考えられます。

これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

Ｑ４
　テレワークの実施にあたって、従業員が、社外から当社サーバー上において電子データで管理している営業秘密にアクセスすることができる環境を整えました。このような場合であっても、営業秘密として保護されるのでしょうか。

A）
　テレワークの実施にあたって、社外から会社サーバーへのアクセスを認めたとしても、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。
　以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として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ります。

　秘密管理性要件の趣旨は、Ｑ１に記載のとおり、「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化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」ことにあります。

　したがって、例えば、アクセス権者を制限する、会社サーバーへアクセスする際にＩＤ・パスワードの入力を要求する、会社サーバー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追加の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すことによって、従業員の予見可能性を確保するといった方法が考えられます。

　これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

Ｑ５
　当社では、外部クラウドを利用して、営業秘密を管理しています。このような場合であっても、営業秘密として保護されるのでしょうか。

Ａ）
　外部クラウドを利用したとしても、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。営業秘密管理指針にも、「外部の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わけではない」旨記載されています〔詳細⇒「営業秘密管理指針」１１頁〕。
　以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として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ります。

　秘密管理性要件の趣旨は、Ｑ１に記載のとおり、「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化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」ことにあります。

　したがって、例えば、企業内の部署・職位等に応じてアクセス権者を制限する、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すことによって、従業員の予見可能性を確保するといった方法が考えられます。

　これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

　なお、外部クラウド上で営業秘密を管理するにあたっては、そもそも選定するクラウドの安全性等に十分注意することや、契約後ファイルをクラウド上にアップロードする際に公開範囲の設定に十分注意することも必要になります。例えば、外部クラウド上の不特定多数の者が閲覧可能なフォルダ等に営業秘密をアップロードしてしまった場合、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生じるものと考えられます。また、不要となったファイルのクラウド上からの消去の徹底にも注意を要します。消去できているか不安が残るときは、暗号化して読めなくする方法も考えられます。

※「非公知性」が認められるためには、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〔詳細⇒「営業秘密管理指針」１７頁〕。

Ｑ６
　当社の従業員の中には、自宅外でテレワークを実施している者もいます。このような場合であっても、営業秘密として保護されるでしょうか。

Ａ）
　自宅外でテレワークを実施したとしても、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。その営業秘密の性質等に応じ、これまで紹介したＱ１～Ｑ５に記載しているポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として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ります。

　なお、特に、自宅外の不特定多数の者が出入り可能な場所でテレワークを実施する場合には、紙の資料・ＰＣ画面ののぞき見や盗撮、これらの盗難等のリスクがあります。
　そこで、そのような場所でテレワークを実施する場合には、以下のような措置を実施することも考えられます。
・紙の資料・ＰＣ等を机上等に放置しないことに関するルールの徹底
・ＰＣにのぞき見防止フィルム等を貼付することの徹底
・いわゆるオンライン会議は、Ｑ９に記載のとおり他人がいる場所では控える　等

　また、自宅外でのテレワークの実施にあたり、従業員が公衆無線ＬＡＮを使用する場合、他者に通信内容を傍受される等のリスクの増加が想定されますので、公衆無線ＬＡＮは使用せず、会社が支給するポケットＷｉｆｉや従業員のポケットＷｉｆｉ・テザリングを使用することを徹底することも考えられます。

　これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

Ｑ７
　万が一、情報漏えいや、不正な持出し等があった場合に備えて、事前に行うことができる対策はあるでしょうか。

Ａ）
　企業が情報管理を適切に行っていたとしても、悪意を持って秘密情報を持ち出されてしまうケースがないとは言い切れません。

　そこで、万が一の事態に備えて、以下のような手立てを講じておくことも考えられます。

（未然の防止策）

①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がアクセスできないようにすること。

②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漏えいに対する危機意識を高めること。

③情報漏えい行為を実施しにくい状況を作り出すための工夫として例えば以下のような対策を行うこと。

- メールの転送制限
- メールへのファイル添付の制限
- メールを送信する際に上長の承認を必要とする設定
- メールを送信する際に上長が常にＣＣ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ツールの利用
- 社用ＰＣにＵＳＢやスマートフォンを接続できないようにする設定
- コピー防止用紙やコピーガード付きの記録媒体等の利用
- プリントアウトの制限　等

　また、以下のような対策を講じることによって、万が一、情報漏えいが起きた場合でも、開示先等による営業秘密へのアクセスを制限したり、営業秘密の流出元・流出先を把握することが可能になると考えられます。

（事後的な対応を可能とするための対策）

- データの暗号化による閲覧制限
- ＰＣのシンクライアント化
- 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の保存
- 一定回数、パスワード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

〔その他詳細⇒「秘密情報の保護ハンドブック」２５～５４頁等〕

これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

Ｑ８
　当社では、従業員が自宅に持ち帰ることが可能な勤務先貸与端末機器がありません。そのため、従業員には、テレワークの実施にあたり、各従業員が個人で所有しているＰＣなど私物端末機器を利用させようと考えています。このような場合でも、営業秘密として保護されるでしょうか。

Ａ）
　私物端末機器の利用を許可したとしても、直ちに、営業秘密としての法的保護の可能性がなくなるわけではありません。
　以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として不正競争防止法による法的保護を受けられる可能性が出てくると考えます。

　秘密管理性要件の趣旨は、Ｑ１に記載のとおり「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化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」ことにあります。

　したがって、例えば、私物端末機器での利用を認める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すことによって、従業員の予見可能性を確保するといった方法が考えられます。

　また、そもそも、従業員の私物端末機器上での営業秘密の利用・管理についても、会社による営業秘密管理の一環であることを明確にするため、「私物端末機器使用マニュアル」等の私物端末機器を使用するにあたっての手続や基準、注意点等をまとめたマニュアル・基準を作成し、従業員に徹底させることも必要になると考えられます。

　これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程、私物端末機器使用マニュアル等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

Ｑ９
　テレワークの実施にあたり、オンライン会議を利用することが増えました。営業秘密管理の点で注意すべき事項等はあるでしょうか。

Ａ）
　オンライン会議を利用することによって、例えば、オンライン会議中に画面共有した資料の営業秘密該当性が直ちに否定されることはないと考えられます。

　もっとも、特に、不特定多数の者が出入り可能な場所でテレワークを実施している場合には、オンライン会議において画面共有した資料ののぞき見・盗撮等のリスクがありますので、Ｑ６記載の措置を取ることが考えられます。
　また、会議の音声を他者が盗み聞きする等の可能性もありますので、不特定多数の者が出入り可能な場所でオンライン会議を実施しない、イヤホンマイクを利用するといった措置を取ることも考えられます。

　これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

　なお、オンライン会議サービスやソフトの中には必ずしもセキュリティが十分とはいえないものがあることも否定できませんので、その選定に際して十分な検討が望まれます。例えば、オンライン会議への第三者の入り込みや会議内容の傍受等の問題も指摘されていますので、当該オンライン会議システムのセキュリティ等については、十分確認のうえ、利用すべきものと考えられます。

　また、オンライン会議サービスやソフトについて、不慣れな従業員が設定ミス等でセキュリティを低下させることを予防するため、勤務先としては、従業員との間で事前にテスト会議をリモート開催する、従業員向けサポート窓口として専用ダイヤル等を設ける、といった方法を講じることも有益です。

Ｑ１０
テレワークの実施にあたり、従業員間や外部の取引先等との間でもチャットツールによって、連絡を取ることが増えました。営業秘密管理の点で注意すべき事項等はあるでしょうか。

A）
チャットツールを利用したとしても、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。
以下のポイントを押さえた管理を意識することで、万が一の場合でも、営業秘密として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ります。

秘密管理性要件の趣旨は、Ｑ１に記載のとおり「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化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」ことにあります。

したがって、チャットツール上で営業秘密の内容に触れざるを得ない場合には、例えば、チャットツール上で送信する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す、営業秘密に関連する内容を取り扱うスレッドを限定するとともに、当該スレッドに参加できる者を制限する、当該スレッドのスレッド名に「㊙」（マル秘）・「社内限り」等の秘密であることの表示を付すことによって、従業員の予見可能性を確保するといった方法が考えられます。

これらの措置の中には従前から取り組んでいるものもあるかと思いますが、改めて、営業秘密管理規程や情報管理規程、セキュリティ規程等の関連規定の内容を再確認（場合により見直し）するとともに、その実施状況の確認をすることが有用です。

なお、チャットツールサービスの中には必ずしもセキュリティが十分とはいえないものがあることも否定できませんので、その選定やチャットツール上での営業秘密の取扱いを認めるか等については、十分な検討が望まれます。