SQUIRE PATTON BOGGS

テレワークの継続を踏まえたセキュリティ対策及び営業秘密の管理

日本（2020年6月15日）

はじめに

緊急事態宣言が解除され、多くの企業が徐々に通常の勤務形態への復帰を目指しています。一方で、新型コロナウイルス感染症対策を継続しつつ、業務の効率化や従業員のライフスタイルを考慮して、テレワークを取り入れていくことを検討している企業も少なくないところです。

そこで、テレワークを継続するにあたって対策が必要となる情報セキュリティについて、具体的な対策方法及び不正競争防止法上の「営業秘密の保護」の観点から留意しておくべき点をまとめております。東京オフィスでは、これらの留意点に対応したテレワークに関する規則等の導入の支援を行っております。

テレワークセキュリティの概要

総務省が発行したテレワークセキュリティガイドラインによれば、テレワークとは、情報通信技術（ICT）の利用により時間・空間を有効に活用する多様な就労・作業形態をいい、在宅勤務は勿論、モバイル端末による勤務やサテライトオフィスにおける勤務をも含むとされています[1]。

オフィスにおいては、インターネットを経由したウイルス等の感染への対策を行い、各種規程等に基づき、紙文書や各種記録媒体の管理者・管理方法を定めていることが通常です。これと同じように、テレワークにおいてもセキュリティを意識し、十分に体制の整備を行う必要があります。

具体的には、以下のような対策が考えられます。

1. 使用者による対策

- セキュリティポリシーの策定及び定期的な見直し
- 重要度に応じてレベル分けを行った各種情報に関するテレワークにおける取扱方法の明確化
- 社内におけるテレワークセキュリティの教育・啓発

2. システム管理者による対策

- セキュリティポリシーに従ったセキュリティ維持に関する技術的対策の導入及び実施状況の監督
- 各種情報の重要度に応じたアクセス制御、暗号化、印刷可否等の設定
- 貸与端末の使用者等の管理
- 貸与端末のウイルス対策ソフト・アップデート等の管理
- テレワークに供される個人所有端末のウイルス対策・ソフトウェア等の状況確認
- WiFi等の無線LANを通じた情報漏えい対策
- 社内システムへのアクセス権限等の設定及び確認
- ランサムウェアの感染に備えた重要な電子データの社内システムからの切り離し
- その他クラウド、データ共有、SNS等のルールの整備及び明確化

3. テレワーク勤務者による対策

- セキュリティポリシーを含む各種規程及び情報の重要度に応じた取扱いの遵守の徹底
- 端末及び記録媒体の管理の工夫・徹底
- パスワードを含む社内システムへのアクセスに用いる認証情報の適正な管理
- WiFi等の無線LANの利用を含む各種リスクの適正な理解

詳細については、「テレワークセキュリティガイドライン（第4版）におけるセキュリティ対策のポイント」（総務省）[2]をご参照ください。

1 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/main_content/000545372.pdf）4頁
2 https://www.soumu.go.jp/main_content/000532482.pdf

不正競争防止法の営業秘密としての保護

会社としては、テレワークの実施を念頭に情報取扱規程等を見直し、秘密情報の社外への持ち出しのルールを再検討した上で、秘密情報が含まれる紙媒体や記録媒体の持ち出しを許可制とすること、秘密情報が含まれることが明確になるように「㊙」「社内限り」といった表示を行うこと、保存されたデータにIDやパスワードの設定をすること等の措置がとられているか改めて確認を行うべきと考えられます[3]。

不正競争防止法（以下、「法」といいます。）は、事業者間の公正な競争を害する行為を不正競争行為として類型化して禁じており、その中には営業秘密の不正な取得・使用・開示行為等が含まれています。

法第2条第6項は、営業秘密を以下の通り定義づけています。

1. 「秘密として管理されている」（以下、「秘密管理性」といいます。）
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って、」
3. 「公然と知られていないもの」

営業秘密に該当すれば、法に基づく差し止めをはじめとする民事上・刑事上の措置の対象になりうることとなります。

上記三要件のうち、テレワークセキュリティとの関係で最も問題となるのは秘密管理性になります。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が明確化されることによって、当該営業秘密に接した者が事後に不測の嫌疑を受けることを防止し、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[4]。従って、秘密管理性要件が満たされるためには、企業の秘密管理意思が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保されている必要があります[5]。

なお、紙媒体は、その性質上、複製や第三者提供の防止が困難であり、テレワークにおいては一層それらの防止が困難であるため、ペーパーレス化の推進が有用と考えられます[6]。

営業秘密のクロスボーダー侵害事案について

昨今では、営業秘密を海外サーバーや外国支社によって管理しているケースが珍しくありません。そのような状況において営業秘密の侵害がなされ、差止請求及び損害賠償請求訴訟の提起を検討する場合には、準拠法及び国際管轄が問題となり得ますので注意が必要です。

執筆者

モーク・マードック
パートナー、東京
E mork.murdock@squirepb.com

ブレット・ギルバート
シニア・アソシエイト、東京
E brett.gilbert@squirepb.com

安友　雄一郎
アソシエイト、東京
E yuichiro.yasutomo@squirepb.com

大久保　頌子
アソシエイト、東京
E shoko.okubo@squirepb.com

3 経済産業省知的財産政策室「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）」（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf）2頁
4 経済産業省「営業秘密管理指針」（https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf）5頁
5 前掲「営業秘密管理指針」6頁
6 前掲「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）」4頁