情報の利用・管理 / サイバーセキュリティ　7-2

サイバーリスクに対する対応

弁護士　大井 哲也
弁護士　飯田 真弥

Question

① COVID-19 の影響を受け、当社でもテレワークを推進していますが、情報漏えいが生じた場合にはどのような責任を負うことになりますか。

② COVID-19 の影響を受け、テレワークを行う従業員が増加しました。情報セキュリティの観点から、どのような点を見直すべきでしょうか。

Answer

① テレワーク等により情報漏えいが生じた場合、会社法上の取締役の善管注意義務違反、個人情報保護法上の安全管理措置義務違反、取引先との契約違反等によって、損害賠償その他の請求を受ける可能性があります。

② 各社においては、テレワークによって個人データ等の情報の取扱いが変わったことに起因するリスクの洗い出しとその対策の検討を十分に行う必要があります。

例えば、新たにテレワークを導入した場合、取締役はテレワークの実施を考慮した情報セキュリティ管理体制を構築・運用することが求められます。他方で、個人情報保護法では、安全管理措置義務として個人データを取り扱う情報システムの使用に伴う漏えいの防止や、外部からの不正アクセスの防止等の措置を講じることが求められます。

また、テレワークの実施に伴い Web 会議システム等のサービスを導入した場合には、当該サービスの脆弱性情報等を継続的に収集し、速やかな社内への周知の徹底等の対策を行う必要があります。

1. はじめに

COVID-19 感染拡大の影響に伴う緊急事態宣言が発令された際には、テレワークの導入を急いだ企業も多く存在しました。しかし、テレワーク環境の整備に留まり、テレワークの実施を考慮した情報セキュリティ管理体制を構築できていないことも考えられます。

テレワークの実施には、持ち運びが容易なノートパソコン等の端末を利用することが考えられますが、このような端末を使用する場合、インターネットを経由した攻撃を防御する対策がなされたオフィスとは異なり、コンピュータウイルス等の感染、テレワーク端末や記録媒体の紛失・盗難、通信内容の盗聴等のリスクに晒されやすいと言われています[1]。さらには、COVID-19 感染拡大後、企業に対するランサムウエア等を含むマルウエアによる攻撃の活発化が確認されるなど[2]、サイバー攻撃による情報漏えいやシステム障害が生じるリスクは高まってきていると考えられます。

今後 COVID-19 の再流行、再々流行等も懸念されますが、その際には、テレワーク等による情報漏えいリスクを低減させる必要があります。本稿では、テレワーク等の実施により生じる情報漏えいのリスクについて、情報セキュリティの観点から見直すべき点を検討します。

なお、テレワーク導入に伴う労務上の留意点につきましては、Q3-4「リモートワーク・時差出勤や行動制限等の就業規則への反映」をご参照ください。

2. COVID-19 の影響に伴うテレワーク推進により情報漏えいが生じた場合の法的リスク

上述したように、テレワークの実施にはテレワーク特有のサイバーリスクが伴います。テレワークの実施を考慮した情報セキュリティ管理体制を構築しないまま、テレワークにより情報漏えい事故等が生じた場合、会社法上の取締役の善管注意義務違反、個人情報保護法上の安全管理措置義務違反、取引先との契約違反等による法的責任を負う可能性があります。

（１）取締役の善管注意義務違反

会社法上、取締役には善良な管理者の注意を持って職務を行う義務（以下、「善管注意義務」という。）があります。そして、取締役は、内部統制システム構築義務の一環として情報セキュリティ管理体制を構築・運用することが要求されており[3]、情報セキュリティ体制に不備があったことを原因として会社または第三者に損害を与えた場合、任務懈怠責任を負う可能性があります。

もっとも、当該体制の具体的な内容は一義的に規定されず、会社の事業規模や特性、社会の状況等に応じて、その必要性、効果、費用等の諸事情を勘案の上、各社にて必要かつ適切な内容を決定すべきとされています。したがって、取締役は、テレワーク導入を契機とした情報漏えい事故等を発生させないよう、

---

[1] 総務省「テレワークセキュリティガイドライン 第４版」（平成 30 年４月）（https://www.soumu.go.jp/main_content/000545372.pdf）６頁

[2] 内閣サイバーセキュリティセンター（NISC）「夏季休暇等に伴うセキュリティ上の留意点について（注意喚起）」（2020 年７月 30 日）（https://www.nisc.go.jp/active/infra/pdf/summer20200730.pdf）

[3] 大会社等においては、取締役（会）が内部統制システムの構築に関する事項を決定すべきことが特に明文で定められており（会社法 348 条３項４号、４項、362 条４項６号、５項等）、これには適正な情報セキュリティ管理体制の構築・運用も要求されていると考えられております。もっとも、大会社等以外においても、適正な情報セキュリティ管理体制の構築・運用に関する事項につき決定しないことが、取締役の善管注意義務・忠実義務違反を構成する可能性がある点に注意が必要です。

善管注意義務を果たす観点からの対応を行うことが必要となります。

（２）個人情報保護法上の安全管理措置義務違反

個人情報保護法上、事業者は、取り扱う個人データの漏えい、滅失または毀損の防止その他の個人データの安全管理のために必要かつ適切な措置（以下、「安全管理措置」という。）を講ずる義務があり、当該措置の内容は、「個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容としなければならない」とされています[4]。テレワークの実施に当たっても、各企業における諸事情を勘案し、リスクに応じた「必要かつ適切な内容」を決定する必要があります。

なお、テレワークにおける個人情報・マイナンバーの詳細な取扱いにつきましては、Q7-1「テレワークでのマイナンバー等の取扱い」も併せてご参照ください。

（３）取引先との契約違反等

取引先等との間で種々の契約を締結する際、提供資料の保管についての善管注意義務や、秘密保持義務、個人情報保護義務などの取引先等の情報について適切な管理を義務づける条項を規定することが多いと考えられます。

契約書にこのような条項が存在する場合、テレワーク導入を契機とした情報漏えい事故等が発生すれば、取引先等との各契約違反（契約解除、損害賠償請求その他の各種請求）となり、債務不履行責任を負う可能性があり、このような事態を生じさせないようにする必要があります[5]。

3. テレワーク等を推進する場合に見直すべきポイント

このように、適切な情報セキュリティ管理体制を構築・運用することが求められる中、総務省では「テレワークセキュリティガイドライン」を策定・公開しており、当該ガイドラインを参考にしつつ、テレワーク等を実施する際の取扱いを定めた情報セキュリティ管理体制を見直していくことが必要といえます。以下では、当該体制を構築・運用していく上で特に留意すべき点について検討します。

（１）基本的な方針

テレワークにおける情報セキュリティ対策を行うには、まずテレワークの情報セキュリティに関する情報を収集し、現状の情報セキュリティ管理体制を把握した上で、どのような脅威や脆弱性、リスクがあるのかを洗い出すことが重要です。そして、洗い出されたリスクに対応した情報セキュリティ対策を講じていくことが必要となります。このとき、情報セキュリティ対策には「最も弱いところが全体のセキュリティレベルになる」という特徴があるため、「ルール」・「人」・「技術」の三位一体のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることがポイントとなります[6]。なお、この「ルール」・「人」・「技術」は、それぞれ「組織的安全管理措置」・「人的安全管理措置」・「技術的安全管理措置」とも

---

[4] 個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン（通則編）」（平成 31 年 1 月）（https://www.ppc.go.jp/files/pdf/190123_guidelines01.pdf）41 頁

[5] なお、契約書にこのような条項が存在しない場合であっても、民法上の不法行為責任が問題となる可能性があります。

[6] 総務省・前掲注１　8 頁

言われております。

ア.「ルール」について

テレワークを行う場合、セキュリティ対策が施されたオフィスとは異なる環境で仕事を行うことになるため、セキュリティ確保のために新たなルールを定める必要があります。

そのためには、上述のとおり、どのような脅威や脆弱性、リスクがあるのかの洗い出しを行った上で、重要度に応じた情報のレベル分けを行い、レベル分けに応じたテレワークでの利用の可否や取扱方法を定めた情報セキュリティポリシーを策定することが重要です。また、情報漏えい事故に備えたインシデント対応マニュアルも策定していくことが望ましいといえます。

総務省では、テレワークセキュリティガイドラインをより具体化した、セキュリティチェックリスト（仮称）等の参考資料を８月末頃に公表予定としているなど[7]、各機関がガイドラインやチェックリスト等を公開しており、セキュリティ管理体制の構築・運用について検討するに当たり参考になります[8]。

他方で、テレワークを既に導入していた場合であっても、テレワークを実施していく中で情報セキュリティ対策に不安が生じたものや、当初テレワークの計画を想定した時からテレワークの利用状況に変更があったものについては、改めてリスク評価を行うことが重要です[9]。

イ.「人」について

情報セキュリティポリシー等のルールを策定しても、実際にテレワーク勤務者やシステム管理者がそれを守らなければ効果を発揮できません。特にテレワーク勤務者はオフィスから目の届きにくいところで作業をすることになるため、当該ルールが守られているかどうかを企業が確認を行うことが困難です。

このような場合にルールを定着させるには、従業員への教育を通じてルールの趣旨を自ら理解してもらい、ルールを遵守することが自分にとってメリットになることを自覚してもらうことが重要です。

具体的には、社内において作成・改訂した情報セキュリティポリシーやインシデント対応マニュアル等を周知徹底し、テレワーク特有のリスクについても、わかりやすくまとめた説明文・Q&A 集を作成するなどして社内教育を実施していくことが望ましいと考えられます。

ウ.「技術」について

技術的対策は「ルール」や「人」では対応できない部分を補完するものであり、情報セキュリティを確保するためには重要です。テレワーク先の環境の多様性を考慮して、それぞれの環境での情報セキュリティ維持のために適切な対策を講じておく必要があります。

例えば、テレワークの実施に伴う VPN やリモートデスクトップの利用だけでなく、一般的なサイバー攻撃対策としてファイルへのアクセス制限、Web ブラウザのフィルタリング、アプリケーションの利用制限、マルウエア検知ソフトの導入といった手段も講じていくことが考えられます。

---

[7] 総務省「テレワークにおけるセキュリティ確保」（https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/）

[8] テレワークにおけるセキュリティ対策については、独立行政法人情報処理推進機構（IPA）が「テレワークを行う際のセキュリティ上の注意事項」（2020 年 7 月 15 日）（https://www.ipa.go.jp/security/announce/telework.html）として各機関の情報を集約しており、参考になります。

[9] NISC「テレワーク等への継続的な取組に際しての留意事項（注意喚起）」（2020 年 6 月 11 日）（https://www.nisc.go.jp/active/general/pdf/telework20200611.pdf）1 頁

また、VPN やリモートデスクトップ、Web 会議サービス等のテレワーク関連サービスにおいては、随時、新たな脆弱性や、サイバー攻撃手法が発見されており[10]、このようなサービスを導入している場合には、当該サービスの脆弱性情報やその対策等の情報収集を継続的に実施し、社内への周知徹底を行う必要がある点、留意が必要です。

（２）基本的な情報セキュリティ対策の構築のポイント

以上の基本的な方針をふまえて、情報セキュリティ対策を行っていくことが望ましいと考えられますが、以下では「テレワークセキュリティガイドライン」を参考に、ポイントとなる対策を紹介します。

実施主体	対策内容
経営者	① テレワーク等の実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。 ② 社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用の可否と取扱方法を定める。 ③ 従業員に対しては、定期的に教育を行う運用を定める。 ④ 情報セキュリティ事故に備えて、インシデント対応マニュアルを策定する。
システム管理者	① 情報セキュリティポリシーに従って、テレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。 ② 不正侵入や悪意のあるソフトウエア、端末の紛失・盗難に対する対策、端末・ソフトウエアの脆弱性対策等が適切に実施・運用されているか確認する。
テレワーク実施者	① 情報セキュリティポリシー等に従って業務を行う。 ② OS や各種ソフトウエアを最新の状態に保つ。 ③ 情報セキュリティ事故が生じた、または、生じるおそれがあると認められる場合、直ちに規定された担当者に連絡する。

なお、総務省をはじめとした関係省庁では、テレワーク導入支援施策として、情報セキュリティ対策についての相談事業や情報提供を行う取り組みがなされておりますので、これらの施策を活用することもご検討ください[11]。

4. 結語

COVID-19 の感染拡大に伴いテレワークを導入・活用している場合には、今後の再流行にも備え、情報セキュリティのリスクを洗い出し、上述したようなテレワークの活用に対応したサイバーリスクへの対策を行っておくことが望ましいと考えられます。

以上

[10] IPA「Zoom の脆弱性対策について」（2020 年 4 月 3 日）（https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html）

[11] テレワーク関連支援情報につき、総務省「新型コロナウイルス感染症対策としてのテレワークの積極的な活用について」（令和 2 年 8 月 21 日）（https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/02ryutsu02_04000341.html）