弁護士が解説　企業経営とサイバーリスク
～在宅勤務・テレワークにおけるリスク～

八雲法律事務所　弁護士／情報セキュリティスペシャリスト　山岡　裕明
2010 年弁護士登録。カルフォルニア大学バークレー客員研究員、内閣サイバーセキュリティセンター法令集サブ WG タスクフォースメンバーも務める。
サイバーセキュリティ法務に特化した業務を展開している。

新型コロナウイルスの感染拡大により、中小企業にも在宅勤務やテレワークといった新しいワークスタイルが急速に定着しつつあります。他方でセキュリティ対策が不十分な場合、思わぬリスクが顕在化します。そこでサイバーセキュリティの専門家である八雲法律事務所山岡裕明弁護士に解説いただきました。

※以下の事例は実際に発生した複数の事故事例をベースにそれらを組み合わせ、創作した想定事例です。

ケーススタディ　サイバーセキュリティ対策不足により、企業に大きな負担が発生した事例

【事例①】

新型コロナウイルスの感染者増加をふまえ、ある会社においては社員を在宅勤務させることとし、社員には各自の私物のパソコンを使用して自宅から会社のシステムにアクセスし作業をさせることとした。

在宅勤務に移行してしばらくした後、在宅勤務をしていたある社員のパソコンがランサムウェアに感染し、その社員のパソコンを経由して会社のシステムもランサムウェアに感染してしまい、社内の重要情報が暗号化されて業務に使用できなくなってしまった。

調査したところ、在宅勤務をしていた社員の私物のパソコンが OS やウイルス対策ソフトのアップデートをしていなかったことからランサムウェアに感染してしまったことが判明した。また、社内のシステム内においても重要情報にアクセス制限をかけるなどの対策をしていなかったことから、社内の重要情報が暗号化されてしまったことが判明した。なお、調査費用として３０００万円の負担が発生した。

【事例②】

会社から支給されたパソコンを用いて在宅勤務をしていたが、自宅には小さい子供がいて仕事にならないため、自宅近くの喫茶店で業務するようになった。

あるとき、パソコンを置いたまま喫茶店のトイレに行ったところ、その間にパソコンを盗まれてしまった。後日、パソコン内に記録されている顧客の氏名や住所、電話番号といった個人情報や、機密情報が記載された契約書、図面等がインターネット上のとある掲示板に掲載されていることが判明し、顧客から１億円の損害賠償が請求された。

盗まれたパソコンは操作画面の自動ロックの設定がされていたが、スリープ状態になる前にパソコンを使用されてしまっていた。また、各パソコンについては、会社からリモート操作して端末内の情報を消去することも可能であったが社員にパソコンを支給する際に利用者の管理を行っておらず、盗まれたパソコンを特定してデータを消去することができなかった。

在宅勤務・テレワークの実情

企業においては、社内で使用するパソコンやネットワーク環境に関してはセキュリティ対策を施していることが多いため、通常の業務形態であれば、サイバーセキュリティ事故に対する耐性が一定程度備わっていることがほとんどです。

（裏面に続く）

しかし、在宅勤務により社員が自宅等で業務を行うようになると、各社員がそれぞれ使用するパソコンやネットワーク環境などのように、外部から攻撃を受ける可能性のある対象が一気に増加します。

また、通常の業務形態とは異なり個人情報等が入ったパソコン等を社外で持ち歩くことからパソコン等の紛失や盗難による情報漏えいの可能性が高まりますし、他の社員やシステム管理者などと物理的に離れて相談しにくい環境になることにより、不審なメールやウェブサイトからのウイルス感染等のサイバーセキュリティ事故が実際に発生するリスクが増加します。さらに、社員の自宅のパソコンをシステム管理者が操作できない等により、サイバーセキュリティ事故が発生した際の被害拡大の可能性が増加するといったことも考えられます。

中小企業が取るべき対策

そのため、企業においては、在宅勤務によるこれらのリスクの増加をふまえ、実施している又は実施しようとしている在宅勤務の方法、企業が保有している情報の価値や漏えいした際の影響、対策にかけられる費用などを総合的に考慮し、選択した在宅勤務の方法に合わせて可能な限りの対策を講じる必要があります。

事例①でいえば、在宅勤務の方法から見直し、OS及びウイルス対策ソフトが最新にアップデートされ、フィルタリングソフトが導入されているパソコンを企業から社員に貸与して使用させるといったことや、在宅勤務において私物のパソコンを使わせるとしてもOS やウイルス対策ソフトは常に最新のものにアップデートするよう注意喚起を行うことなどの対策が考えられます。さらにマルウェアに感染しないよう、業務で使用するパソコンでは、怪しいサイトの閲覧、不要なダウンロード、不自然なメールの添付ファイルの開封をさせないよう徹底することも重要です。また、社内のシステムで保管している情報を機密性の点から段階に分けて閲覧可能な社員を限定する等のアクセス制御を実施し、仮に社内のシステムに侵入されたとしても被害を最小限にするような対策を施しておくことも有効です。

事例②でいえば、貸与するパソコンには全て自動ロックの設定を行った上で、パソコンの紛失、盗難があったとしても操作できない状態にしておくことや、貸与するパソコンの利用者を管理し、リモート操作の設定をすることで、情報漏えいを防止し、又は被害を最小限にする対策を施すといったことが考えられます。

また、事例①、②に共通することですが、如何にサイバーセキュリティ事故の防止に費用をかけたとしても、サイバーセキュリティ事故を完全に防ぐことはできません。そして、一旦サイバーセキュリティ事故が発生した場合には、フォレンジック調査にかかる多額の費用や、取引先からの損害賠償等の思わぬ負担を強いられることになりかねません。そのため、上記のサイバーセキュリティ事故防止の対策に加えて、サイバーセキュリティ事故が起きることを前提にサイバー保険によるリスク移転といった対策をとることも重要です。

POINT

一般に、在宅勤務やテレワークといった業務形態においては、サイバーセキュリティに係るリスクが増大します。

情報の価値や漏洩時の影響、対策にかけられる費用などを総合的に考慮し、在宅勤務の方法に応じて適切な対策を講じる必要があります。

サイバーセキュリティ事故を完全に防ぐことは不可能であり、サイバーセキュリティ事故が起きることを前提に、保険によるリスク移転等の対策をとることが重要です。

三井住友海上火災保険株式会社
MS&AD INSURANCE GROUP

＜お問い合わせ先＞
株式会社ぱれっと
住　所：東京都世田谷区池尻2-32-8 ｺﾝﾄﾞﾐﾆｱﾑ池尻3階
連絡先：03-5787-8640　　担当者：田村