事例で学ぶセキュリティインシデント（第5回）

うっかりパソコンを置き忘れ。ハイブリッドワークの落とし穴

2023.10.17

情報システム担当者が机の上の書類を片付け、退社しようとしている時に携帯電話が鳴った。「すみせん、パソコンを入れたカバンを電車の網棚に置き忘れてしまいました。どうしましょう」。あわてて電話をかけてきたのはE社の営業部員だ。情報システム担当者は、パソコンを電車に置き忘れたことを鉄道会社と警察に届け出た後、会社に戻って事情を説明するように伝え、電話を切った。そして「ハイブリッドワークで心配していたことが起こってしまった……」とつぶやいた。

会社と自宅の間でパソコンを持ち歩いて紛失

E社は大阪に本社のある中堅の出版社だ。西日本の観光スポットやグルメなどの最新情報を取材・紹介するガイドブックの発行で読者の人気を集めてきた。新型コロナが猛威を振るっていた時にはほとんどの従業員がテレワークを余儀なくされたが、今は在宅勤務と出社勤務を組み合わせたハイブリッドワークを導入するなど柔軟な働き方を可能にしている。

ハイブリッドワークを認めたことで情報セキュリティの新たなリスクが顕在化している。E社ではテレワーク時に会社で各人が使用していたパソコンを自宅に持ち帰らせ、オンライン会議ツールを使った社内ミーティングや取引先との打ち合わせや、メールの送受信、編集業務に利用してきた。テレワーク時には会社のパソコンを一旦、自宅に持ち帰れば、再び出社勤務に戻るまで自宅に置いたままだ。だが、ハイブリッドワークでは自宅と会社の勤務場所に応じて頻繁に端末を持ち運ぶ必要がある。その結果、パソコンの紛失・盗難による情報漏えいのリスクが高くなることを情報システム担当者は懸念していた。

営業部員にパソコンの入ったカバンを電車に置き忘れた経緯を尋ねたところ、取引先訪問後、電車に乗り込み、新刊書籍の手荷物があったことからパソコンを入れたカバンを網棚に置いた。パソコンには取引先との受発注データなどが保存されていたが、顧客の個人情報など機微なデータは含まれていないという。幸い、パソコンが入ったカバンは置き忘れたその日に鉄道会社の駅係員によって無事に回収され、翌日、営業部員が受け取りに行き、大事には至らなかった。だが、このセキュリティインシデントはハイブリッドワーク、テレワークの情報セキュリティの課題を改めて浮き彫りにした。

多要素認証などでパソコンの不正利用を抑止

E社では、コロナ以前は情報漏えい防止の観点から社内パソコンの社外持ち出しを禁止していた。だが、多くの企業と同様にコロナの感染拡大でテレワークになり、「緊急避難」的に社内パソコンの社外利用を認めてきた。営業部員のようにパソコンを置き忘れ、紛失するリスクの他にも、営業車の中に置いたパソコンが盗まれたり、ネットカフェなどでパソコン操作中に盗み見されたりする恐れもある。

悪意のある第三者が紛失・盗難のパソコンを不正に入手し、パソコンに保存された機密情報を盗み取る手口もある。万一、機密情報や個人情報が漏えいした場合、企業の信用失墜のみならず、取引停止などの可能性もある。パソコンだけでなく、USBデバイスにデータを保存して会社から自宅に持ち帰る際、盗難・紛失による情報漏えいのリスクもある。そこで、情報漏えい防止策として、データの暗号化や、第三者に不正アクセスされないように推測されにくいID、パスワードの設定、複数の認証を組み合わせる多要素認証といった対策も効果的だ。

また、パソコンの情報漏えい対策として、パソコン内にデータを残さない仮想デスクトップなどを導入する方法もある。既存パソコンからの切り替えにコストはかかるが、セキュリティ対策の他、一括したアプリケーションの導入・更新が可能になり、パソコンの運用管理の効率化も期待できる。

インシデント対応の手順を再確認

テレワーク、ハイブリッドワークに欠かせないのがパソコンのエンドポイントセキュリティ対策だ。会社では、社内ネットワークとインターネットとの境界にUTM（統合脅威管理）を置いてウイルスの侵入や不正アクセスを防ぐことが一般的だ。だが、テレワークではパソコンレベルでウイルス対策や不正アクセス対策を行う必要がある。

コロナ禍のテレワーク導入時に会社支給のパソコンが間に合わず、私有パソコンの業務利用を認めたケースもある。かつての「パソコンの社外持ち出し禁止」のように、エンドポイントセキュリティ対策がなされていない場合、「私有パソコンの社内持ち込み禁止」といった措置を講ずる。新型コロナウイルスの感染症法上の位置付けが5類感染症になり、私有パソコンの業務利用などの「例外措置」をそろそろ見直す必要もありそうだ。

E社の情報システム担当者は、今回のインシデントの経緯を全社員に説明し、再発防止を徹底するよう伝えた。パソコンには個人情報や取引先の重要情報が保管されておらず、情報漏えいもなかったことから、経営層とも相談の上、社外に公表しなかった。そして、パソコンや外部記憶デバイスの盗難・紛失などの問題発生時には、直ちに上司や情報システム担当者へ連絡する。情報漏えいが疑われる場合、情報の種類や件数、データ暗号化の有無などの状況を確認するといったセキュリティインシデント対応の手順を再確認した。

すべての従業員に対して、ID、パスワードを定期的に更新することや、パソコンの基本ソフトやアプリケーションの更新を適切に行うこと、メールの添付ファイルの開封やURLのクリックを安易に行わないことなど、基本的なセキュリティ対策を守るように周知。そして、パソコンレベルでウイルス対策やUSBデバイスの制御が可能なエンドポイントセキュリティの導入や、社内の情報共有のみならず、取引先と受発注データなどを安心してやり取りできるクラウドストレージサービスの導入を検討することとした。セキュリティ対策を強化し、パソコンの利用や情報の取り扱いのルールを規定しても、従業員が守らなければリスクとなる。E社ではハイブリッドワーク、リモートワークといった柔軟な働き方を続けるためにも、従業員がルールを順守するよう教育・啓もう活動にも力を入れていく考えだ。