―コロナ下、そして
収束後を見据え

テレワーク導入前のセキュリティ対策

インフォシア代表
情報処理安全確保支援士
社会保険労務士
髙　橋　真　悟

3

テレワーク導入の課題のひとつに情報セキュリティの確保が難しいといった意見もあり、過去にはテレワークで使用する機器の脆弱性を突く攻撃により、情報漏えいなどの被害が発生しています。

テレワークに特化した情報セキュリティ対策もありますが、今回はテレワーク導入前にやっておきたい情報セキュリティ対策について取り上げていきます。テレワークの有無にかかわらず基本的な情報セキュリティ対策なのでテレワークを導入している、導入を検討している企業だけでなく全ての企業に共通する内容となります。

■ソフトウェアを最新の状態にしておくこと

前提として「バグのないソフトウェアはない」という認識を持つことです。バグとは一般的にソフトウェア上の欠陥、不具合のことです。また、セキュリティに関するバグのことをセキュリティホールと呼ぶこともあります。バグのあるソフトウェアは不良品で、そんなものは使えないと考える人もいるかもしれません。バグのないとされるソフトウェアは現時点でバグが発見できていないだけで、未来永劫バグが存在しないとはいえません。そのため「バグのないソフトウェアはない」と考えられています。もちろんソフトウェアの製造元もバグ（特に影響の大きいもの）をそのままにしておいてよいとは思ってはいません。バグによる悪影響を発生させないための回避方法の案内や発見されたバグを修正するためのソフトウェアを配布するなど対応を行っています。マイクロソフトは毎月第2または第3水曜日にWindowsの修正プログラム（アップデート）の配信を行っています。通常は使用しているパソコンへ自動的に修正プログラムが適用されることになりますが、修正プログラムの適用時にパソコンへ負荷がかかり処理が遅くなることを嫌がるなどの理由で、修正プログラムを自動的に適用しないよう設定をしているパソコンは要注意です。

システム管理者などが新しい修正プログラムの影響を確認したうえで、社内のパソコンに修正プログラムを適用する流れになっている場合は、自動的に適用されない状態でも構いませんが、長期間に渡り修正プログラムを適用しないということは、悪意を持った第三者に攻撃してくださいと言っているようなものですので、早急に対応が必要です。

また、Windowsの修正プログラムはパソコンのシャットダウン時や再起動時に適用されますので、常時電源を入れたままになっているパソコンもご注意ください。

さらに、修正プログラムの適用を自動的に行ってくれるものばかりではありません。パソコンに存在するソフトウェアを確認し、最新状態になっている（修正プログラムが適用されている）ことを定期的に確認することも重要です。

ちなみに冒頭で取り上げたテレワークで使用する機器の脆弱性を突いた攻撃も機器のソフトウェアを最新にしておけば、防げるものもありました。

■普段の業務は管理者権限を使用しないこと

WindowsなどOSの多くは利用者の権限を設定することができます。利用者の権限によりシステムの設定、ソフトウェアの追加などできることが変わってきます。また、管理者権限はOSのあらゆることができる権限となっており、Windowsでは管理者のことをアドミニストレータとも呼びます。

全てのことが行える管理者権限を利用すること

が便利なように思えますが、情報セキュリティ上は好ましくありません。なぜなら、利用者が自分勝手にソフトウェアを追加できてしまうからです。インターネット上には数多くのソフトウェアが存在します。その中には業務で役に立つものもあるかもしれませんが、怪しいソフトウェアが存在することも忘れてはいけません。一見すると役に立ちそうなソフトウェアも利用者の見えないところで悪さを働く機能がついているものもあります。

インターネット上に数多く存在するソフトウェアのひとつひとつを安全であるかを確認することは現実的ではないので、業務で使用するパソコンには必要なソフトウェアだけをいれておき、利用者が自由にソフトウェアを追加することを制限することは情報セキュリティ上も重要です。また、システムの設定等も簡単に変更できてしまうことは、情報セキュリティ上の問題を発生させる可能性がありますので、変更できないようにすることも大切です。

そのため、普段の業務はできることが制限された標準ユーザを使用するようにしましょう。

一般的なソフトウェアは標準ユーザでも使用することができますので業務への影響は少ないかと思います。

■定期的に教育を行うこと

情報セキュリティ対策のために機器の設定を見直すことや新しい機器の導入など様々な取組をされている企業も多いと思いますが、絶対に大丈夫といったものはありません。なぜなら、その機器を使うのが人間だからです。機器は正しく使ってこそ機能を発揮します。

また、従業員の中でも情報セキュリティに関する知識やスキルに温度差があるのが現状です。企業の情報セキュリティ対策を進めるためには、「やってはいけないこと」、「やるべきこと」、「トラブル発生時に取る行動」など、全従業員が一定程度の知識やスキルを身につけることが不可欠です。情報セキュリティに関する意識の向上、定着のためにもトレンドを踏まえ定期的に教育を行うことは非常に重要です。

今回取り上げた3つのポイントは情報セキュリティ対策を進めている企業にとっては当たり前のことかもしれません。しかし、この機会に改めてできているのだろうか確認をしてみてはいかがでしょうか。

また、情報セキュリティ対策がこれからだという企業においては、手軽に始められる対策として取り組んでみてはいかがでしょうか。（完）

▽　▽

次回の「テレワークセミナー」（無料）は、10月26日に開催します。

新たな履歴書の様式例の作成

～「様式例」を参考にして、公正な採用選考を～

厚生労働省　職業安定局

厚生労働省では、これまで公正な採用選考を確保する観点から、一般財団法人日本規格協会（以下「日本規格協会」という）が、ＪＩＳ規格の解説の様式例において示していた履歴書の様式例の使用を推奨していました。

令和2年7月に日本規格協会が、ＪＩＳ規格の解説の様式例から履歴書の様式例を削除したため、厚生労働省において公正な採用選考を確保する観点から新たな履歴書様式例の検討を行い、事業主の皆様に広く参考にしていただくための様式例（厚生労働省履歴書様式例）を作成し、労働政策審議会職業安定分科会に報告いたしました。

厚生労働省においては、今後、公正な採用選考への理解を深めるさまざまな取り組みを実施するにあたり、本様式例を活用してまいります。

事業主の皆様におかれましても、採用選考時に使用する履歴書の様式については、本様式例を参考にしつつ、公正な採用選考をお願いします。履歴書の様式に本様式例と異なる記載欄を設ける場合は、公正な採用選考の観点に特に御留意をお願いします。

なお、厚生労働省履歴書様式例と、日本規格協会が示していた履歴書様式例（ＪＩＳ規格様式例）の異なる点については以下のとおりです。

【厚生労働省履歴書様式例とＪＩＳ規格様式例の相違点】

1、性別欄は「男・女」の選択ではなく任意記載欄としました。なお、未記載とすることも可能としています。

2、「通勤時間」「扶養家族数（配偶者を除く）」「配偶者」「配偶者の扶養義務」の各項目は設けないことにしました。

※履歴書の様式例は、厚生労働省のホームページで「履歴書」と検索してください。