トレンドワードから効率化を読む（第19回）

テレワーク時の端末の紛失などのセキュリティ対策

2020.11.06

働き方改革などの影響により、テレワークを導入する企業が増えています。そんな中、テレワークに関わる課題の解決ができず、導入が思うように進まない企業も多いのではないでしょうか。課題の中でも、情報セキュリティに関する課題は最も大きな問題の1つであり、対策が難しいものです。

そこで今回は、テレワークの導入による課題の概要から、情報セキュリティリスクの解説、情報セキュリティ対策とそのポイントについて解説していきます。

テレワークの導入における課題とは

テレワークの導入における課題はさまざまですが、その中でも次の3つが大きな課題として挙げられるでしょう。

・情報セキュリティの確保
・導入コスト
・社内のコミュニケーション問題

テレワークはオフィス外で業務を実施するため、情報漏えいが起きないようにセキュリティ対策を施す必要があります。また、テレワークを実現するにはICT（情報通信技術）環境の整備だけでなく、労務管理や社内ルールの整備も考慮しなければなりません。そのため、機器の単純導入コストだけでなく、導入に関する計画の立案や計画の試行・改善のコストもかかることが課題して挙げられます。

さらに、社内のコミュニケーション問題も大きな課題です。従来の対面によるコミュニケーションはテレワークでは実現できないため、こちらもICTを活用した新たな取り組みが求められます。

テレワークの導入でさまざまなメリットが得られる一方で、ここで挙げたような課題をクリアする必要があります。とりわけ、情報セキュリティの確保は非常に難しい課題で、以降、情報セキュリティの確保について掘り下げていきます。

テレワークの課題である情報セキュリティリスク

テレワークの導入に際して、具体的にどのような情報セキュリティリスクが考えられるのでしょうか。テレワークにおける情報セキュリティリスクには、次のようなものが挙げられます。

・情報漏えい
・不正アクセス
・情報の消失
・パソコンや記録媒体の紛失
・脆弱性が内在するアプリケーションの利用
など

テレワークの際に特に注意すべきセキュリティリスクは、「情報漏えい」や「不正アクセス」です。主にインターネットを介して会社の情報へ接続するため、セキュリティ対策が施されていないとこれらのリスクが発生する恐れがあります。

また、社内システムなどに接続する端末や重要データが保存された記録媒体を紛失した場合にも同様のリスクが懸念されます。紛失しないためのルールの策定を講じるとともに、万が一紛失してしまったとしても、事態が大きくならない対策が必要です。

さらに、社内システムに接続する端末のセキュリティ対策として、利用するアプリケーションの管理も重要です。特に注意すべきは、脆弱性が内在するアプリケーションを利用しないようにすることです。これを怠ると、サイバー攻撃の標的とされる可能性も考えられます。

テレワーク実現には、これらの情報セキュリティリスクに対する対策が必要不可欠なのです。

テレワークにおける情報セキュリティ対策

テレワークにおける情報セキュリティ対策として、特に重要な対策方法を紹介します。これから紹介する対策はいずれかを実施すれば良いわけではありません。すべてを網羅的に実施することが重要です。

＜不正アクセス対策＞
テレワークで利用する端末や、接続先となる端末・社内システムへの不正アクセスを防ぐには、次に挙げるような対策が有

効です。

・多要素認証を利用する
・通信を暗号化する(VPN接続・SSL化)
・ファイアウォールなどのネットワークセキュリティを導入する

テレワークで利用する端末に対するセキュリティとして、多要素認証を用いることは非常に有効です。多要素認証は、ID/パスワードによる認証と併せて、指紋による生体認証などの異なる要素の認証を組み合わせるものです。多要素認証を用いて認証強度を高め、本人以外が端末を扱えないようにして不正アクセスを防ぎます。

また、テレワークでは主にインターネットを介して接続するため、通信を暗号化するVPN接続を用いると、通信内容を傍受されるリスクを低減することが可能です。

併せて、社内システムとの通信経路上にファイアウォールやIPS(侵入防止システム)/IDS(侵入検知システム)を導入し、不正アクセスへの対策を施しましょう。

＜端末・重要データの盗難、紛失対策＞
テレワークを利用するうえで、端末や重要データの盗難・紛失した際のリスクが気になる企業も多いのではないでしょうか。これらの対策方法としては、次のような対策が考えられます。

・利用端末に暗号化を施す
・利用端末内にデータを残さない
・重要データは暗号化する

利用端末のストレージに対して暗号化を施すことで、もしもの盗難・紛失時に情報を漏えいさせるリスクを軽減できます。端末のストレージは外部接続でもデータを読めますが、暗号化されていると読み取れなくなるからです。

また、そもそも利用端末内にデータを残さないようにするのも有効な対策となります。リモートデスクトップ方式で社内端末へアクセスすることで、オフィス外の端末内にデータを残さず業務が行えます。

最後の「重要データの暗号化」については、テレワーク利用時に限った話ではありませんが、データをやり取りする際に「パスワードを付ける」といった暗号化を施し、データの盗難・紛失時に備えます。

＜外部サービスの利用に対する対策＞
テレワークを利用する中で、オンラインストレージなどの外部サービスを利用する機会もあるでしょう。外部サービスからのマルウエア感染や、外部サービス上の重要データの消失対策も必要です。

これらは、テレワークで利用する端末やシステムに対して、セキュリティ対策ソフトを用いてマルウエア感染を防いだり、重要なデータには定期的なバックアップを行ったりすることで対策が可能です。

また、外部サービス自体にマルウエア対策やバックアップ機能が備わっているかどうかも確認しましょう。

テレワークにおける情報セキュリティ対策のポイント

最後に、総務省の「テレワークセキュリティガイドライン」をもとに、「ルール」「人」「技術」の観点から対策ポイントの概要を解説します。詳細については「テレワークセキュリティガイドライン(総務省)」をご確認ください。

＜「ルール」:セキュリティ確保のための新たなルールを設ける＞
テレワークで業務を実施するにあたり、情報セキュリティの面で安全かどうかを都度判断して対策するのは効率的ではありません。また、専門的な知識を有していなければ判断自体も難しいでしょう。

職場とは異なる環境での業務では、セキュリティ確保のための新たなルールを設けることが重要なポイントとなります。「こうやって業務を行うことで安全を確保できる」という業務の進め方をルールとして定めるのです。

＜「人」:テレワーク勤務者が情報セキュリティに関する必要知識を取得する＞

新たにルールを定めても、テレワークを実施する「人」が守らなければ意味がありません。ルールをテレワーク勤務者に理解させ、情報セキュリティに関する必要知識を身に付けさせる必要があります。

そのため、テレワーク勤務者やその上司・同僚に対して、テレワークの実施における講習・講義を行い、ルールの徹底と情報セキュリティの知識を身に付ける環境を整えます。

＜「技術」:テレワーク先の環境に応じた技術的サポートの実施＞
テレワークにおける情報セキュリティ対策を「ルール」や「人」だけに頼るのは危険です。なぜなら、人間はどんなに気を付けても、多かれ少なかれミスをするものだからです。

ルールを定め、テレワーク勤務者への教育を施したうえで、もしものミスに対応する方法として「技術的対策」を取るべきといえるでしょう。技術的対策はセキュリティリスクに対して「認証」「検知」「制御」「防御」を自動的に実施するものです。

生体認証やファイアウォール、IPS/IDSなどが該当する技術的対策であり、これらの対策を施すこともテレワークにおけるセキュリティ対策ポイントとなります。

テレワーク導入時の情報セキュリティ対策には「セキュリティおまかせプラン」がおすすめ

テレワークの導入時にはさまざまな課題が挙げられますが、情報セキュリティの確保は特に重要です。情報漏えいや不正アクセスといったセキュリティリスクに対して、「不正アクセス対策」や「端末・重要データの盗難、紛失対策」を行いましょう。

これらの情報セキュリティ対策を施す際には、「ルール」「人」「技術」の観点から対策を考えます。情報セキュリティ確保に関する課題をクリアし、安全なテレワーク環境を実現しましょう。

しかし、情報セキュリティ対策は専門的な知識を有していなければ難しいもの。

NTT西日本では、進化し続ける脅威に対して、セキュリティ対策を複合的に組み合わせた「セキュリティおまかせプラン」をご用意しています。このプランでは、ゲートウェイでの防御や、企業向けセキュリティ対策ツール、サポートセンターでの通信監視・ 復旧支援など、手厚いサポートで脅威から企業を守ります。

「セキュリティおまかせプラン」の詳細はこちらをご確認ください。

※本機能はセキュリティに対するすべての脅威への対応を保証するものではありません
※掲載している情報は、記事執筆時点のものです