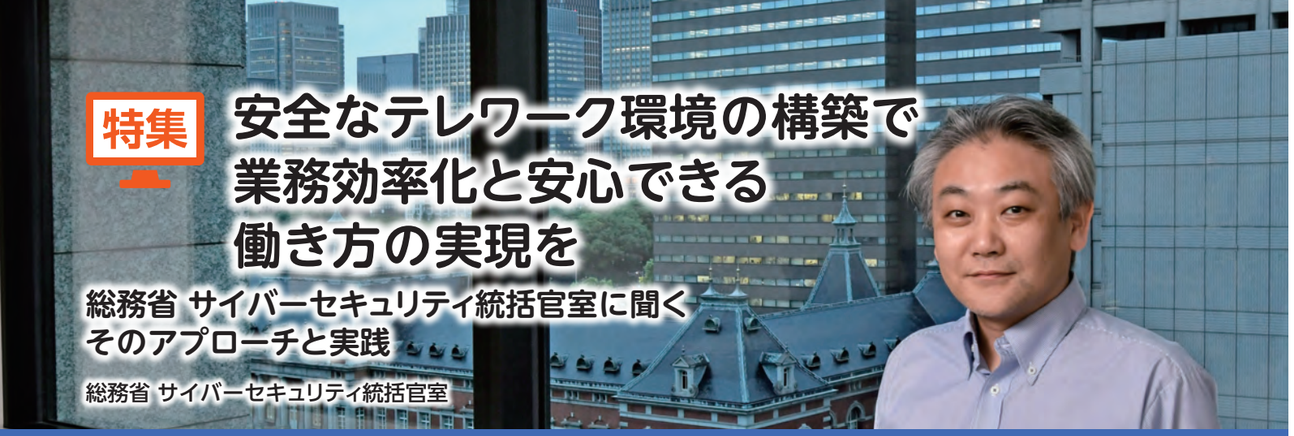


特集

安全なテレワーク環境の構築で業務効率化と安心できる働き方の実現を

総務省 サイバーセキュリティ統括官室に聞く そのアプローチと実践

総務省 サイバーセキュリティ統括官室

コロナ禍でも安全に働くため、テレワークの活用が広がっています。今回は「どうやってセキュリティを守りつつテレワークを導入するか」について、総務省サイバーセキュリティ統括官室の高村 信参事官にお話をうかがいました。

総務省
サイバーセキュリティ統括官室
参事官
高村 信氏

―サイバーセキュリティ統括官室とはどのようなお仕事をされている部署でしょうか。

「総務省の中で、情報通信分野のセキュリティ向上を担当しています。一般の方々に向けてインターネット利用上の注意喚起、通信事業者とのセキュリティ情報の共有やサイバーセキュリティ人材の育成、さらにはテレワークに関するガイドライン作成など、業務は広範です」

―企業内でのITセキュリティと、テレワークでのセキュリティにはどのような違いがありますか。

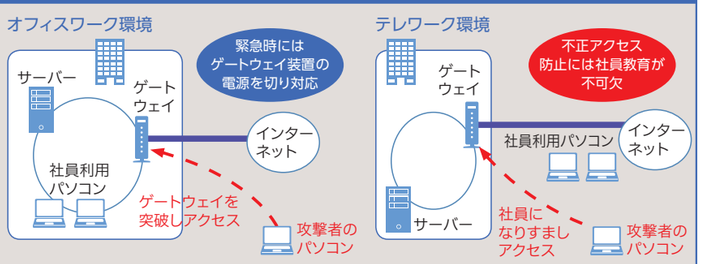
「企業内のセキュリティは、基本的に“モノの管理”です。オフィスにあるパソコンにセキュリティソフトがきちんとインストールされているか、OSやアプリケーションソフトのアップデートが行われているかなど、管理しているIT機器の設定をきちんとすることでセキュリティが確保できます（図1参照）。万一セキュリティ上の危機が発生した場合でも、社内のネットワークがインターネットにつながるゲートウェイの電源を切ってしまえば、被害の拡大を最小限に抑えることができます。しかしテレワークでは、社員がスマートフォンやパソコンなどの端末を社外に持ち出して仕事をするため、そうした管理の目が行き届きません。またデータやシステムのクラウド化を進めている場合を除き、社員が社外から社内システムにアクセスすることを前提とするため、インターネットに向けての何らかの入口が開いている状態となります。そのため、そうした端末を扱う社員の教育が非常に重要になるのです」

テレワークでのセキュリティ管理には「社員の教育」が重要

―端末を外に持ち出すことで、どのようなリスクが生まれるのでしょうか。

「最大のリスクは、端末を落とすこと、紛失することです。この場合、二つの被害が生まれます。まず、その端末に入っていたデータを業務で活用できなくなることです。もう一つは、端末に入っていたデータが抜き取られ、漏えいしてしまうことです。こちらのほうがより大きな被害につながる可能性があります。端末を持ち歩く時には、紛失や置き忘れに注意することを社員に徹底するとともに、パソコンにはパスワードを設定、スマートフォンにもパスワード、もしくは画面を指でなぞってロックを解除する『パターンロック』により、第三者が入手しても中のデータにアクセスできないようにしておくことが重要です。ただ、パターンロックでも、長く使っていると指の軌跡に沿って画面保護フィルムに跡が残ることがあり、“一直線”のようなパターンの登録は見破られてしまう可能性があります。できるだけ複雑なパターンで登録することが、セキュリティ向上につながります」

図1：一般企業内のITセキュリティとテレワークセキュリティの違い



オフィス内のITセキュリティは、たとえ外部から攻撃を受けたとしても、インターネットにつながるゲートウェイを遮断すれば、被害を最小限にとどめることができる。テレワーク環境では「社員が外部からアクセスすること」が前提なので、社員になりすましてログインする攻撃者への対策が求められる。
そのため、より高度なセキュリティ機器を配置し物理的に遮断するほか、リモートツール利用時のIDやパスワードの管理について、社員の意識を高めることが重要になる。

Point

- テレワークセキュリティには社員のマインド啓発が不可欠
- スマートフォンやパソコンを紛失すると大きな被害の発生に
- 「チェックリスト」の活用でセキュリティの重要ポイントの確認を

短時間でセキュリティの必要項目が分かる「チェックリスト」を用意

図2：「テレワークセキュリティの手引き（チェックリスト）」の積極活用を

テレワークセキュリティの手引き（チェックリスト）

予算や社内の対策が必ずしも十分でない中小企業等が、テレワーク導入や利用を進める上でのセキュリティ対策を簡潔に示した冊子。フローチャートでテレワークの方式を確認した後、それぞれの方式で求められるセキュリティ対策を優先度順に記している。PDFのダウンロードはhttps://www.soumu.go.jp/main_sosiki/cybersecurity/telework/（下のQRコードからでもOK）にて。またZoomなど主要なウェブ会議アプリケーションの設定方法を図解で解説する資料も用意されている。

Point

それぞれのテレワーク方式について「優先度：◎の項目」「優先度：○の項目」を例示し、とるべき対策を分かりやすく解説している。

Point

「端末は会社支給か個人所有か」「会社のネットワークにアクセスするかどうか」など、二者択一の質問に答えるだけで自社のテレワーク方式が選択できる。

下のQRコードからもアクセスできます

―こちらのチェックリストは、どのような内容になっているのでしょう。

「IT関連の単語は知っている、もしくはネット検索で中身を調べることができるといった方々を想定し、適切にセキュリティの設定ができるよう配慮した内容となっています。フローチャートを使って自社のテレワーク環境を8つの方式から選び、それぞれの方式に用意された『セキュリティ対策チェックリスト』に従い、設定などを確認していただくことで、通常想定される外部からの侵入、情報の漏えいを防ぐことができます。それぞれの対策は優先度◎が1ページ、○が2ページ程度ですので、読み解き、理解するために多くの時間がかかることもありません」

―今後のご活動について、展望を教えてください。

「こうしたテレワーク導入に向けてのセキュリティ対策を広く中小企業さまに周知していくことが課題と考えています。また現在、テレワークセキュリティの無料相談窓口を開設していますが、こちらのご利用も広く呼びかけたいと思っています。さらに今回のコロナ禍で各企業がどのようにテレワークに取り組んだのか、アンケートを行っているところです。その内容を反映し、年度内にはガイドラインの第5版を、そしてチェックリストもより内容を分かりやすくした第2版を年内に発行する予定です」

分からないことは「無料相談窓口」へ

総務省は、テレワークにおけるセキュリティ無料相談窓口を開設中（詳細は裏表紙）。これから導入する企業などだけでなく、すでに導入済みでも、具体的なセキュリティ対策方法や適切性のコンサルティングなどを幅広く相談可能です。セキュリティ専門企業である株式会社ラックが相談に対応します（https://www.lac.co.jp/telework/security.html）。

ユーザ協会　D10003　検索