セキュリティ

ICTシステム環境の最適化

働き方改革の盲点!?

テレワークに潜む、情報漏えいのリスクとは

自宅や出張先などオフィス以外の場所で、パソコン等を使って業務を行う「テレワーク」。最近では「働き方改革」の一環として導入する企業も増えているワークスタイルです。しかし、社外での業務は既存のセキュリティ環境の外で行われることから、情報漏えいなどの事故が発生するリスクも高まります。そこで今回は、テレワークに必要なセキュリティ対策について考察します。

「働き方改革」の推進で効果的なテレワーク

昨今、テレワークという言葉が定着してきました。総務省の定義によれば、テレワークとは「情報通信技術(ICT)の利用により時間・空間を有効に活用する多様な就労・作業形態」であり、「企業にとっての競争力強化だけでなく、新しいビジネスの創出や労働形態の改革、事業継続の向上をもたらすとともに、多様化する個々人のライフスタイルに応じた柔軟かつバランスのとれた働き方の実現に寄与する」としています。

テレワークは、少子・高齢化対策、経済再生、雇用創出、地域振興、防災・環境対策などさまざまな面で効果があることが認められており、特に近年は、ワークライフバランスを実現する柔軟な「働き方」として注目されています。

テレワークの方式には、「在宅勤務」「モバイル」「サテライトオフィス」などがあります。在宅勤務は文字通り従業員が自宅で業務を行うこと。モバイルは、ノートPCやタブレット端末などを使用し、外出先で業務を行うこと。サテライトオフィスは、企業の本拠地や常勤している拠点などとは別の場所に設置したワークスペースで仕事をすることです。いずれの場合も、社外のさまざまな場所で業務や会議が可能になるため、通勤や移動にかかるコストや時間を軽減できます。企業側からみれば業務が効率化されますし、従業員側からみれば、より柔軟な働き方が可能になるわけです。

テレワークが情報漏えいのリスクを高める？

多様化する働き方にテレワークは効果的だといわれる一方で、「セキュリティ」対策に頭を抱える企業も多いのではないでしょうか。オフィス内のPCは社内ネットワークに接続され、インターネットとの出入口はファイアウォールやIPS（Intrusion Prevention System ／不正侵入防止システム）などで守られているでしょう。しかし、テレワークでは自社と同様の保護がない環境で、PCやタブレット、スマホなどの端末を使い業務を行うことになります。社外アクセスのセキュリティ対策がされていない場合は、直接インターネットへ接続することが多くなるため、この状況は、逆にインターネット側から端末へアクセスされる可能性もあり得るというリスクが生じます。

特にモバイル通信の場合に注意したいのが、公共の無線LAN（Wi-Fi）の利用です。現在では利便性を高めるために、空港や駅、カフェ、ホテルなどさまざまな場所で無料のWi-Fiサービスが提供されるようになりましたが、こうしたWi-Fiの中には暗号化キーが公開されていたり、そもそも暗号化されていなかったりするケースもあります。暗号化されていない場合、「無線通信の傍受」が容易なため、通信内容だけでなく端末上のさまざまな情報が筒抜けになってしまうリスクがあります。取引先とのメールの内容や、社内サーバーにアクセスするためのIDやパスワードなどが悪意のある第三者に漏れては一大事です。

またサイバー攻撃者はマルウェアの感染経路の1つとして、Wi-Fi環境を悪用するケースがあります。過去には、Wi-Fiルーターへマルウェアを仕込み、無線利用のためにアクセスしてくる端末を感染させた例も報告されています。この場合、もし従業員がマルウェアの感染に気づかず、そのまま企業のネットワークに接続すれば、社内へ広がるおそれもあるでしょう。

サイバー攻撃以外にも、持ち運んでいるノートPCやタブレットなどの端末には、紛失・盗難というリスクが内在するのです。また在宅勤務で個人所有のPCなどを許可なく使っている場合には、個人利用のクラウドサービスやフリーソフトウェアがインストールされていることがあります。それらから、業務上の機密情報をうっかり共有してしまうというリスクも考えられるでしょう。

暗号化やVPNなどテレワークに有効な最新のセキュリティ対策を

こうしたリスクを避けるためにも、企業がテレワークを導入するときには、社外でのセキュリティの確保が重要なポイントとなります。特に重視すべきなのが端末とアカウントの管理、情報漏えい対策です。

まずは、テレワークに「誰」の「端末（パソコンやタブレットなど）」が使われているのかを正確に把握し、個人IDと紐づけられた端末を管理する必要があります。また、端末やグループウェア・クラウドサービスなどのログインには、可能な限り「多要素認証」を導入します。多要素認証とは、IDとパスワードの組み合わせに加え、指紋などの生体認証やワンタイムパスワードなど複数の認証を組み合わせることです。

さらに端末上のデータを暗号化する、もしくはVDI（仮想デスクトップ）化により端末上にデータを保存しない手法もセキュリティの一環となります。これらの手法を採用することで、万が一紛失や盗難に遭っても、情報を盗まれるリスクを低減することができるでしょう。

Wi-Fiに関する情報漏えい対策としては、各種サービスを利用する前に通信に強度の暗号化が施されているかを確認しておきます。また暗号化されていないWi-Fiサービスは原則利用禁止などの規則を設けておきましょう。ただし、現在のところ最強といわれている暗号化形式であるWPA2にも脆弱性が確認されています。次期バージョンとしてWPA3が承認されたところですが、普及するまではもう少し時間がかかりそうです。そこで、Wi-Fiの利用時にはVPN（バーチャル プライベート ネットワーク）を使用するなど、WPAとは別の方法で通信を暗号化するのも1つの手段です。

会社貸与・個人所有（BYOD）の端末に関わらず、テレワーク環境で使用するPCやタブレット、スマートフォンなどの端末にはセキュリティ対策ソフトの導入は必須です。この際、単機能のアンチウイルス製品ではなく、複数の機能を持ったものを選ぶことが大事です。マルウェア対策だけでなく、アンチスパムやフィルタリング、侵入防御、Wi-Fiの安全性の判定など、多機能対策が備わったセキュリティ対策を実装することでさらなるセキュリティレベルの向上が期待できるでしょう。

これらのテレワーク環境整備と同時に、各従業員に割り当てているIDの管理も、外部環境から社内サーバーへのアクセスが増加した際には見直しを図りたいものの1つです。ID管理に関しては、多要素認証の導入を検討してみることをおすすめします。

関連サービス

ID Federation	Office 365・G Suite・Boxなどの1,700以上のSaaSアプリをはじめ、お客さまのオンプレミスアプリやActive Directoryとも連携し、シングルサインオン・アクセスセキュリティ強化を実現する認証サービスです。
Arcstar Universal One クラウドWi-Fi	Arcstar Universal Oneでは、アクセスポイントのレンタルから認証基盤まで、セキュアなWi-Fi環境に必要なすべてをNTTコミュニケーションズが一元的に提供します。さらにアクセスポイント設置やLAN配線工事などを行い、ネットワークと合わせて24時間365日保守対応するプランも提供することで、お客さまの負担を軽減し最適なWi-Fi環境の構築を実現します。
テレワーク・スタートパック	設定不要ですぐにセキュアなテレワークを始められる「テレワーク・スタートパック」。テレワークに必要なノートパソコン、モバイル通信、およびセキュリティサービスをパッケージ化。事前の設定も完了した状態でお届けします。