滋賀県警からのサイバーセキュリティに関するお知らせ

テレワークのセキュリティ対策の確認をお願いします

新型コロナウイルスの感染拡大を受け、テレワークを活用し自宅での勤務を行う企業が増えてきています。

しかし、テレワークを活用するにあたり、セキュリティ対策を確実に行わないと、情報漏えい等の問題が発生する可能性があります。

テレワークとは、ICT(情報通信技術)を活用し、離れた場所で仕事を行う業務形態です。

Web 会議システムやリモートデスクトップ、クラウド等を利用することもテレワークの１つです。

テレワークのセキュリティリスク

私物のパソコンやタブレットを使用するリスク

テレワークでは、個人所有のパソコンやタブレット等の端末を使用する場合があります。

個人所有の端末は、ウイルス対策ソフトが更新されていない場合や、そもそもインストールされていない場合があるので、社内システムへのウイルス感染の可能性が高くなります。

Web 会議システムのリスク

急激に使用者が増加していることにより、システム自体が攻撃の的になる可能性があります。

脆弱性を突いた不正アクセスや会議を盗み見られることによる情報流出の可能性があります。

無線 LAN のセキュリティリスク

暗号化等のセキュリティ対策を行っていない無線 LAN は通信内容を盗み見される可能性があります。

また、正規の Wi-Fi スポットを騙る「偽 Wi-Fi スポット」も存在します。

意図しない情報を公開してしまうリスク

テレワークを利用するには、外部から社内システムへ接続する必要があります。

社内データへのアクセス権限設定を適切に行っていないと、本来公開していないデータ等が誰でも見ることができる状態になる場合があります。

テレワークに関連する標的型攻撃のリスク

「会議はすでに始まっています」、「あなたの参加を待機しています」など、参加を促すような文言で偽のサイトに誘導する等の攻撃を受ける可能性があります。

テレワークにおけるセキュリティ対策

上記のようなセキュリティリスクへの対応としては、「**テレワークの使用ルールを決める**」ことが重要です。最低限以下のようなルールを事前に取り決めておくことが望ましいです。

○テレワークに使用する端末のウイルス対策ソフト、OS、ソフトウェアを常に最新にする。

○不特定多数が集まる場所やセキュリティ対策されていない公衆無線 LAN 等は使用しない。

○個人情報などの重要な情報は暗号化する。　など

これらのルールは一例ですが、新たなシステムを導入すると予想外のセキュリティ事故が発生する可能性が高まります。この機会に、テレワークだけでなく社内のシステム等のセキュリティ対策が万全であるかを確認しましょう。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）