事務所News ニュース
2021.5
K-021
発行：佐園達哉税理士事務所

経営バイタルの強化書 KEIEI VITAL

テレワークの情報セキュリティ

テレワークの情報セキュリティと情報セキュリティ10大脅威 2021

緊急事態宣言やまん延防止措置が実施され、新型コロナウイルスの感染拡大を防止するためにテレワークが浸透してきましたが、通常とは異なる環境での業務の中で、メールの誤送信を含む情報セキュリティの問題が多発してきています。

総務省では、従来のテレワークセキュリティガイドラインを改定予定としており、IPAが毎年公表する情報セキュリティ10大脅威でも新たにテレワーク等ニューノーマルな働き方を狙った攻撃が3位になる等対策が必要になっています。

テレワークの普及で問題となる情報セキュリティとは?

1 ニューノーマルな働き方でのテレワーク・オンライン会議

新型コロナウイルス感染症（COVID-19）の影響により、ICTを用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進みました。

感染拡大を防止するために、新しい生活様式（ニューノーマル）の働き方が提唱され、テレワークやローテーション勤務、会議はオンライン等対面を回避する働き方が求められており、急速にテレワークやオンライン会議が進展した一方で、普段とは異なる自宅等での環境下での働き方には情報セキュリティ上の問題が潜んでいます。

情報セキュリティの普及啓発活動等を行っているIPA（情報処理推進機構）では、昨年よりテレワークを行う際のセキュリティ上の注意事項を公開し対策啓発映像等も公開していますが、毎年公表している情報セキュリティ10大脅威にも組織の脅威第3位に「テレワーク等のニューノーマルな働き方を狙った攻撃」が新たにランクインしました。

情報セキュリティ10大脅威 2021

昨年順位	個　人	順位	組　織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	**テレワーク等のニューノーマルな働き方を狙った攻撃**	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

https://www.ipa.go.jp/security/vuln/10threats2021.html より

2 テレワーク等のニューノーマルな働き方を狙った攻撃と対応

テレワークのために私物PCや自宅ネットワークを利用したり、VPN等のために初めて使うソフトウェアを導入したり、以前までは緊急用として使っていた仕組みを恒常的に使う必要性がでてくるなど業務環境の急激な変化を狙った攻撃が行われています。業務環境に脆弱性があると、社内システムに不正アクセスされたり、ウェブ会議をのぞき見されたり、テレワーク用PCにウイルスを感染させられたりするおそれがあります。

攻撃の手口としては下記のようなものがあります。

●テレワーク用ソフトウェアの脆弱性の悪用

VPN等のテレワーク用に導入している製品の脆弱性を悪用し、社内システムに不正アクセスしたり、PC内の業務情報等を窃取したりします。また、ウェブ会議サービスの脆弱性を悪用し、ウェブ会議をのぞき見し、情報を盗用したりします。

●急なテレワーク移行による管理体制の不備

テレワークで利用しているPC内のOSやソフトウェアのセキュリティ管理を組織側から行うことは難しく、テレワークへの急な移行によりルール整備やセキュリティ対策のノウハウが不十分なまま利用を開始していることが多く、この管理体制の不備を狙った攻撃が行われます。

●私物PCや自宅ネットワークの利用を狙ったもの

私物PCをテレワークで利用している場合、ウェブサイトやSNSにアクセスしたり、私物のソフトウェアをインストールしたりする私的利用を行うことがあります。その際、PCがウイルスに感染したり、攻撃者にソフトウェアの脆弱性を悪用され、テレワーク用の認証情報等を窃取されたりするおそれがあります。また、組織支給のPCを利用している場合でも、適切なセキュリティ対策が行われていない自宅ネットワークを利用することで組織の適切なセキュリティ対策が適用されず、PCがウイルスに感染する等のおそれがあります。

攻撃事例としては、脆弱性の悪用によりVPNのパスワードが流出した事例（2020年8月、VPN製品の脆弱性が悪用されて窃取された認証情報約900件がインターネット上で公開）やテレワーク中にウイルス感染、社内に拡大した事例（2020年4月、テレワーク中の従業員が社有PCで社内ネットワークを経由せずに外部ネットワークに接続し、SNSを利用した際にウイルスに感染し、社内ネットワークにウイルス感染が拡大）等があります。

対策としては、テレワーカー、セキュリティ担当者、経営層別に下記のような対策をとることが必要となります。

テレワーカー

私物のPCを利用しないことやテレワーク環境の検討等セキュリティ意識を高める教育を受講して情報リテラシーや情報モラルを向上する、セキュリティ事故に遭遇した場合、関係者に遅滞なく連絡し、対応を行うことが必要となります。また、被害の予防として、基本的な情報セキュリティ対策を実施し、決められたテレワークのルールを守ることも必要です。

セキュリティ担当者

テレワーカー向けに基本的な情報セキュリティ対策を実施し、テレワークのルールを作成、教育の機会を設けることが必要となります。また、被害の予防として、セキュリティパッチの適用（VPN装置、ネットワーク機器、PC等）やテレワークで利用するソフトウェアの脆弱性情報の収集と周知、対策状況の管理が必要です。

経営層

基本的な情報セキュリティ対策、テレワークのルールの決定（テレワークのセキュリティポリシーの策定等）を行い、通常と異なる作業環境での業務の実施に支障がないように指示を行うことが必要となります。

また情報セキュリティ対策予算を確保し、継続的な対策を実施することが必要です。情報セキュリティ対策は小さな会社では、予算や人員の制約から行うことが困難であり、盗用されるような情報はないと経営層が考えていることもあり、なかなか進んでいませんが、テレワークの進展でメールの誤配信や重要情報の漏えいのリスクは高まっており、取引先に迷惑をかけてしまう可能性も高まってきています。

IPA（情報処理推進機構）では、「中小企業の情報セキュリティ対策ガイドライン」を策定し、中小企業でも実施可能な基本的な情報セキュリティ対策を公開しており、これを利用して必要な対策を実施することも重要です※1。

また、総務省ではテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として、テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示した「テレワークセキュリティガイドライン」を策定・公表しており、改訂第5版を近々公表することを予定しています※2。

※1「中小企業の情報セキュリティ対策ガイドライン」（URL：https://www.ipa.go.jp/security/keihatsu/sme/guideline）
※2「テレワークにおけるセキュリティ確保」（URL：https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/#guide）