2020 年 4 月 28 日

サービス＆セキュリティ株式会社 e-Gate センター

テレワーク(在宅勤務)におけるセキュリティリスクと対策について

1. 概要

働き方改革の一環として導入されてきたテレワークですが、新型コロナウイルス感染症（COVID-19）の感染拡大で緊急事態宣言が発令され、政府からテレワークの実施が推奨されたことにより、急ぎ導入している企業が増えてきています。しかし、社内の整備されたセキュリティ環境外で業務を行うことで、情報漏えいやマルウェア感染などのリスクが高くなることが懸念されます。安全に利用するためには、セキュリティリスクに対する理解と対策が必要です。そこで今回は、テレワークを導入するうえで注意すべきセキュリティリスクとその対策について紹介します。

2. テレワーク導入による課題

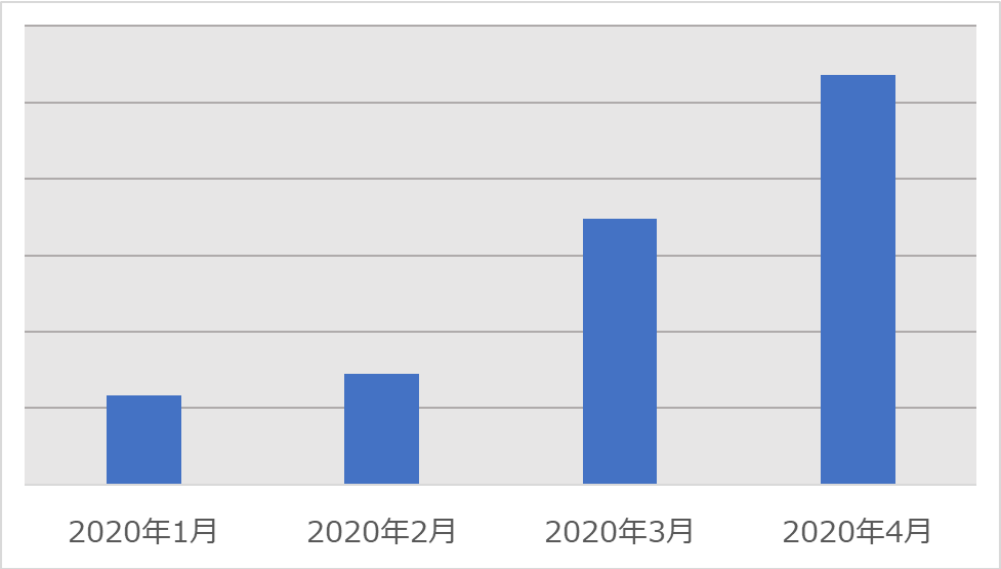
2.1 テレワークとは

テレワークとは、情報通信技術(ICT)を活用した、場所や時間にとらわれない柔軟な働き方のことです。勤務する場所によって在宅勤務(自宅利用型)、モバイルワーク、サテライトオフィス勤務(施設利用型)の 3 つに分けられます。

政府は新型コロナウイルスの拡大防止対策として、テレワークの一種である「在宅勤務」を強く呼びかけています。

2.2 外部サービス利用通信の増加

e-Gate センターにおいてもテレワークによる通信の増加を確認しています。チャットツールや Web 会議システムの利用による通信は次の図のとおり、緊急事態宣言が発令された 4 月は従来の約 5 倍に増加しています。

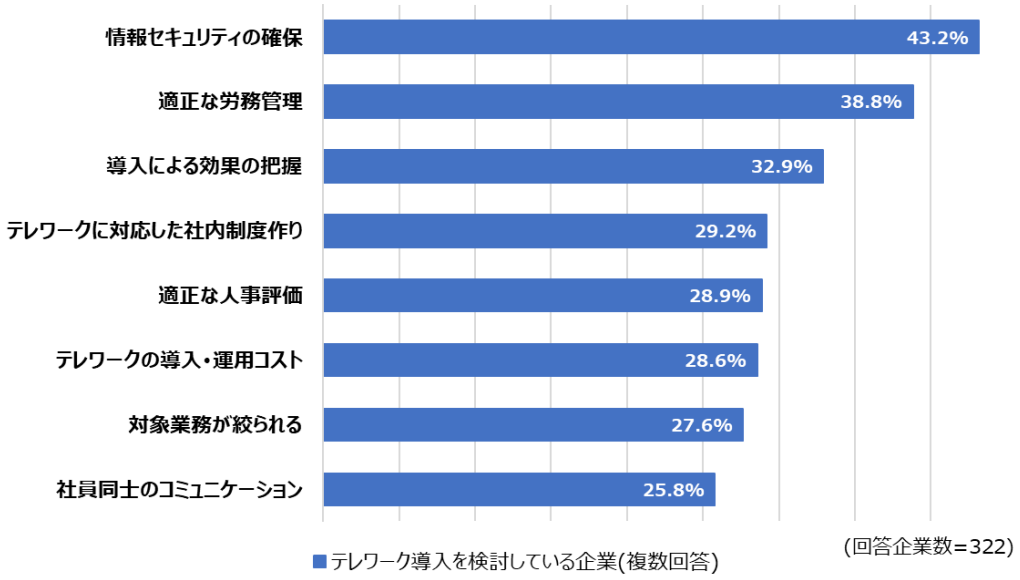


【図 1】外部サービス利用による通信の推移

2.3 テレワーク導入状況と導入による課題

しかし、検討しているという企業は多々あるものの導入が進んでいないのが現状です。パーソル総合研究所が 2020 年 3 月 9 日～15 日に実施した「新型コロナによるテレワークへの影響についての全国 2 万人規模の緊急調査」では、実施率は約 13%でした。感染拡大が進んでいる現在では導入は増加していることが予想されますが、依然として低い数値が推測されます。テレワーク導入の課題として、多くの企業が挙げているのが情報セキュリティの確保です。

総務省が実施した「ICT 利活用と社会的課題解決に関する調査研究」では、テレワーク導入を検討している企業の導入にあたっての課題は次の図のとおり、情報セキュリティの確保が一番の課題となっていることがわかります。



【図 2】テレワークの導入にあたっての課題、導入するとした場合の課題

（出典：総務省「ICT 利活用と社会的課題解決に関する調査研究（平成 29 年）」を加工して作成）

3. テレワーク(在宅勤務)時におけるセキュリティリスク

テレワークをされる利用者の観点でのセキュリティリスクを整理してみました。利用者がどのような情報を社外の環境で扱うのかをよく把握し、扱う場所におけるリスクを洗いだすことが肝要です。

なお、新型コロナウイルスに関するフィッシングメールが急増しており、在宅勤務では社員間でのコミュニケーションが取りづらく普段より騙されやすい環境にあるため、注意が必要です。「新型コロナウイルスに便乗したフィッシング」の詳細につきましては以下 URL をご参照ください。

『新型コロナウイルスに便乗したフィッシング』

https://www.ssk-kan.co.jp/topics/?p=10717

(1) PC や記録媒体の紛失

テレワークを実施する際、業務用 PC や USB メモリ、HDD といった機器・記録媒体の社外持ち出しが必要となる可能性があります。しかし、持ち出し時に物理的な紛失や盗難による情報漏えいのリスクが存在します。

(2) 家庭内ネットワーク利用

ホームルータのセキュリティ上の不備があると、悪意を持った第三者により、不正侵入、ネットワークに接続する端末や機器が不正なサイトへの誘導(フィッシング)やマルウェア感染などの被害に遭うリスクが高まります。また、社内ネットワークに侵入するための踏み台として、家庭内ネットワークが悪用される可能性があります。

(3) 個人端末利用(BYOD=Bring Your Own Device)

十分なセキュリティ対策が施されていない個人端末を使用することでセキュリティリスクが高まります。また、個人端末が既にマルウェアに感染していることも想定されます。その他にも端末の紛失や、家族・知人の端末利用時に情報漏えいする可能性があります。

(4) マルウェア感染

業務に無関係な Web サイトの閲覧や不必要なソフトウェアのインストールによるマルウェア感染。先述したとおり、悪意を持った第三者による不正サイトへの誘導(フィッシング)など様々な感染経路が想定されます。

マルウェアに感染してしまうと、業務停止や情報漏えいなど様々な被害が発生する可能性があります。また、テレワーク環境でマルウェアに感染した端末をそのまま社内で使用することで、社内ネットワークに拡散する恐れがあります。

(5) 内部不正

機密情報の持ち出しなど、内部不正のリスクは高まっています。IPA（情報処理推進機構）の「情報セキュリティ 10 大脅威 2020」では、「内部不正による情報漏えい」は 2 位となっており、昨年の 5 位よりランクアップしています。また、テレワークでは周りに監視する人がいないため、不正のリスクが高くなります。

(6) 脆弱性が内在するアプリケーションの利用

テレワークの実施においてチャットツールや Web 会議システムなど、情報連携を行う上で必要不可欠ですが、セキュリティ対策が万全ではない可能性があります。

2020 年 4 月 3 日に IPA（情報処理推進機構）よりビデオ会議システム「Zoom の脆弱性対策について」の注意喚起が発表されています。詳細は後述の **5.参考情報**をご参照ください。

セキュリティ対策が万全であったとしても、ユーザ側の過失によって情報漏えいなどのトラブルが発生する可能性があります。

セキュリティリスク	(1)PCや記録媒体の紛失	(4)マルウェア感染		(5)内部不正	(6)脆弱性が内在するアプリケーションの利用
		(2)家庭内ネットワーク利用	(3)個人端末利用		
脆弱性	■ 電車の網棚にPC入りバッグを失念する ■ 盗難被害に遭う ■ 暗号化未実施 ■ バックアップ未実施	■ 無線LAN設定不備 ■ アップデート未実施 ■ 推測されやすいパスワードの使用 ■ 不正アクセス ■ 偽メールに添付されたファイル開封やリンクのクリック	■ ログイン方法を書いたメモを放置 ■ アップデート未実施 ■ ウイルス対策ソフト未導入・更新不備	■ 重要情報への無断アクセス ■ 重要情報の持ち出し	■ 重要情報の盗聴 ■ 脆弱性の悪用 ■ アップデート未実施

【図 3】テレワーク(在宅勤務)における脅威と脆弱性

4. 対策

企業・団体向けのテレワークにおける基本対策を以下に挙げました。多岐にわたる観点で対策が必要です。これらはシステム管理者ならびにシステム利用者の双方が良く理解をして運用する必要があります。

テレワークは企業が定めるポリシーに従って行動するのが原則です。システム利用者の理解として重要な点として、社内の整備されたセキュリティ環境外で業務を行う場合は、普段以上に注意を払って行動しましょう。

【システム管理者向け対策】

① 情報セキュリティ保全対策

・テレワーク勤務者の情報セキュリティに関する認識を確実なものにするため、定期的に教育、啓発活動を実施する

・情報セキュリティ事故の発生に備え、迅速な対応がとれるように連絡体制を整備する

② 端末の紛失・盗難に対する対策

・貸与するテレワーク端末や記録媒体の所在や利用者等を管理する

・貸与用のテレワーク端末に多要素認証の設定、HDD の暗号化を行う

③ マルウェア対策

・貸与用のテレワーク端末にウイルス対策ソフトをインストールし、最新の定義ファイルが適用されているようにする

・貸与用のテレワーク端末の OS およびソフトウェアのバージョンは常に最新に保つ

・個人端末利用(BYOD)を許可する際は、その端末に必要な情報セキュリティ対策が施されていることを確認する

・不必要なソフトウェアの使用、業務外の Web サイト閲覧ができないよう設定する

④ 不正アクセス対策

・リモート環境からの情報資産へのアクセス制限設定を行う
・なりすましや不正アクセスを防ぐため、多要素認証を導入する
・社内システムとインターネットの境界にセキュリティ対策機器を設置し、ログを監視する
・社内システムにアクセスする際のアクセス方法を定め、アクセス状況を監視し不必要なアクセスは遮断する
・社内システムへのアクセス用のパスワードは、強度の低いものは使用できないよう設定する

⑤ 外部サービス利用に対する対策

・外部サービスの利用ルールを整備し、情報漏えいにつながる恐れのある利用を禁止する

【テレワーク利用者向け対策】

① 情報セキュリティ保全対策

・テレワーク作業中は、利用する情報資産の管理責任を自らが負うことを自覚し、情報セキュリティポリシーが定める技術的・物理的及び人的対策基準に沿った業務を行う
・情報セキュリティ事故の発生に備え、迅速な対応がとれるように連絡体制を確認する

② マルウェア対策

・個人端末利用時は OS およびソフトウェアのバージョンは常に最新に保つ
・ソフトウェアの利用ルールに従い、許可されていないソフトウェアを利用しない
・新しいソフトウェアのインストールが必要な場合は管理者へ確認する
・不審なメールに添付されたファイルやリンクを不用意に開かない

③ 不正アクセス対策

・社内システムにアクセスする際は、システム管理者が指定したアクセス方法のみを用いる
・社内システムへのアクセス用のパスワードは強固なものにし、使い回しを避ける
・家庭内ネットワーク利用時は、ホームルータなどのパスワード設定が初期のまま使用しない

④ 外部サービス利用に対する対策

・ビデオ会議用の招待メールや URL などは公開しない
・外部サービスの利用ルールに従い、不必要なサービスを無許可で利用しない

⑤ 重要情報の盗難対策

・機密性が求められるデータをやり取りする際は、必ず暗号化する
・第三者と共有する環境で作業を行う場合、覗き見防止フィルターや作業場所を考慮し、覗き見防止に努める

5. 参考情報

・総務省

「テレワークセキュリティガイドライン（第 4 版）」（案）に対する意見募集の結果及び当該ガイドラインの公表
https://www.soumu.go.jp/menu_news/s-news/01ryutsu02_02000200.html

テレワーク推進による労働参加の広がり（3）テレワーク普及の可能性と課題
https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc142130.html

・IPA 独立行政法人 情報処理推進機構

Zoom の脆弱性対策について
https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html

情報セキュリティ 10 大脅威 2020
https://www.ipa.go.jp/security/vuln/10threats2020.html

・パーソル総合研究所

新型コロナによるテレワークへの影響について、全国 2 万人規模の緊急調査結果
https://rc.persol-group.co.jp/news/202003230001.html

6. e-Gate のサービスについて

企業・団体のセキュリティ対策を強固にするためには不正な通信を検知するためのセキュリティ対策機器の導入と、そのログの監視が重要です。”e-Gate”の MSS や脆弱性診断サービスの導入を是非ご検討ください。

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate“のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

※本資料には弊社が管理しない第三者サイトへのリンクが含まれています。各サイトの掲げる使用条件に従ってご利用ください。
リンク先のコンテンツは予告なく、変更、削除される場合があります。

«お問合せ先»

サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp