2020.04.22

サイバーセキュリティニュース ＜2020 No.001＞

テレワークにおけるセキュリティ上の留意点

【要旨】
■ 新型コロナウイルスの世界的な感染拡大に伴い、非常災害時の事業継続対応として、多くの企業でテレワークの活用が推進されている。安全配慮義務を果たしつつ事業活動を継続するために、テレワークの実施および範囲の拡大は必須となっている。
■ 一方で、テレワークには、導入以前よりもサイバーリスクが顕在化する危険があり、適切なセキュリティ対策をとる必要がある。
■ テレワークセキュリティ対策は、自社のテレワークにおいて何を実現し何を守るべきか明確にした上で、その実現に適した方法を選び、必要なリスク対策を行うことが肝要である。

１．テレワークとは

テレワーク[1)]とは、ＩＣＴ（情報通信技術）を利用し、時間や場所を有効に活用できる柔軟な働き方である。テレワークの主な形態としては、「雇用型（企業に勤務する被雇用者が行うもの）」には在宅勤務、モバイルワーク[2)]、サテライトオフィス勤務[3)]などがあり、「自営型（個人事業者・小規模事業者等が行うもの）」としては、Small Office Home Office（ＳＯＨＯ[4)]）がある。

本来、コスト削減や業務効率の向上、働き方改革推進の施策の一つとして積極的に活用する意義・効果のあるものだが、昨年末から続く新型コロナウイルスの世界的な感染拡大に伴い、非常災害時の事業継続対応として、多くの企業でテレワークの活用が推進されている。すなわち、災害発生時等の緊急事態においても、従業員に対して安全に業務を遂行できる環境を提供する義務（安全配慮義務）を果たしつつ、事業活動を継続するために、テレワーク導入を進める企業が急速に増えている。

一方、テレワークの導入・運用方法によっては、サイバーセキュリティを脅かす新たなリスクを生じさせてしまう。本稿では、テレワーク導入で顕在化するサイバーリスクとその対策のポイントを解説する。

２．テレワークの導入で顕在化するサイバーリスク

オフィスでの勤務であれば、端末やネットワークに一定のセキュリティ対策がされており、安全な環境のもとで業務がおこなわれる。一方、テレワークでは、端末やネットワークにおけるセキュリティ対策が適切でないまま外部のネットワークを経由して社内システムへアクセスし、テレワーク導入以前よりもサイバーリスクが増大する可能性がある。テレワーク導入で顕在化する代表的なサイバーリスクは表１のとおりであり、これらの特性を理解した上で、テレワークを活用する必要がある。

１）総務省「政策＞情報通信（ICT 政策）＞ICT 利活用の促進＞テレワークの推進＞テレワークの意義・効果」
https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/18028_01.html（最終アクセス 2020 年 4 月 14 日）
２）顧客先や移動中に、パソコンや携帯電話を使うなど、施設に依存せず、いつでも、どこでも仕事が可能な状態なもの
３）勤務先以外のオフィススペースでＰＣなどを利用した働き方
４）企業などから委託された仕事を、情報通信を活用して自宅や小規模事務所等で個人事業主として請け負う労働形態のこと（出典：一般財団法人日本ＳＯＨＯ協会ホームページ）

【表1】 テレワークにおける代表的なサイバーリスク

サイバーリスク	概要	想定される脅威シナリオ
マルウェア感染	テレワークで利用する端末や社内システムがマルウェアに感染する	ウイルス対策ソフトの更新ができていない端末がマルウェアに感染、遠隔操作され、機密情報を窃取される
端末の紛失、盗難	テレワークで使用する端末を紛失したり、盗難される	会社支給の持ち出し用端末を紛失し、取り扱っていた機密情報が外部に漏えいする
機密情報の盗聴	ネットワーク上の通信内容が、悪意のある第三者によって盗聴される	悪意のある第三者が用意した公衆無線LANを使用したことでパスワードやメールの内容が読み取られる
不正アクセス	本来アクセス権限をもたない者が社内システムや機密情報にアクセスする	モバイルワーク中に不審者に画面を覗き見、IDとパスワードを盗み見られ、社内システムへ不正にアクセスを許し、保存していた機密情報を窃取されたり改ざんされる
外部サービスの不適切な利用	メッセージングアプリケーションやSNSの設定や操作の誤りにより、組織に何らかの悪影響が生じる	社内の情報共有ツールとしてSNSに取引先の未公開情報を投稿したが、誰でも閲覧できる状態となっており、取引先からの信用が失墜し、今後の取引が停止となる
従業員のヒューマンエラー（過失や軽微な故意）	従業員がテレワークのルールを逸脱した結果、機密情報の漏えいが発生する	利用禁止の共用端末でテレワークを行ったため、端末に保存されていた機密情報が外部に漏えいする

３．テレワーク検討のポイント

（１）テレワークの方針策定

テレワークを行う場合、オフィスとは異なる環境で業務を行うこととなるため、そのセキュリティ確保のために新たなルールを定めることが不可欠である。すなわち、テレワーク実現への第一歩は、情報セキュリティに関係する方針・規程・ルール類を見直し、テレワークの方針を策定、対象とする業務を選定し、対象業務の実施ルールを追加することが必要である。

次いで、社内の機密情報を、その機微性に応じで分類し、テレワークで取り扱える対象を定める。これらが不十分な場合、機密情報の不適切な取扱いが発生し、大きな情報セキュリティ事故につながりかねない。

テレワークにおけるセキュリティ方針、関連する規程類の策定や見直しを行う際には、特定非営利活動法人日本ネットワークセキュリティ協会（以下、ＪＮＳＡ）が提供する情報セキュリティポリシーのサンプル[i)]を参考とされたい。

（２）テレワークの実現方式の選定と留意点

テレワークで扱える業務や情報を定めたら、自社の業務効率化とセキュリティの確保を実現するためのテレワークの方式を定める。本稿では、総務省のテレワークセキュリティガイドライン第 4 版ⅱ）にて定められた以下のパターンごとに選定の留意点を解説する。

【表2】 テレワークの実現方式

テレワークパターン名	概要	テレワーク端末に電子データを保存するか？	オフィスの端末と同じ環境を利用するか？	留意点
リモートデスクトップ方式	オフィスにある端末を遠隔で操作	保存しない	同じ	● オフィスの環境にリモートで接続するための通信機器の追加や、環境の設定変更が必要となり、実現までに期間を要する場合有
仮想デスクトップ方式	テレワーク用の仮想端末を遠隔操作	保存しない	テレワーク専用の環境	● 仮想端末を使用していなければ、仮想端末が必要 ● オフィスの環境にリモートで接続するための通信機器の追加や環境の設定変更が必要となり、実現までに期間を要する場合有
クラウドアプリ方式	クラウド上のアプリケーションを社内外から利用	どちらも可	クラウド型アプリ利用時に関しては同じ	● データを端末に保存できる為、端末に強力なセキュリティ対策の実装することが必要 ● IT ベンダーが提供するアプリで実施できる業務のみ選択可能
セキュアブラウザ方式	特別なブラウザを用いて端末へのデータの保存を制限	保存しない	ブラウザ経由で利用するアプリに関しては同じ	● 特別なブラウザがサポートしたアプリのみ使用可能なため、実施できる業務が限定される場合有 ● 通常のブラウザと比較すると、操作が複雑であり、処理に時間がかかるなどの傾向有
アプリケーションラッピング方式	テレワーク端末内への保存を不可とする機能を提供	保存しない	テレワーク専用の環境	● オフィスの環境にデータ保存する場合は、通信機器の追加導入などの変更が必要となり、実現までに期間を要する場合有 ● クラウドサーバ上にデータ保存する場合、IT ベンダーが提供するアプリで実施できる業務のみ選択可能
会社ＰＣの持ち帰り方式	オフィス端末を持ち帰りテレワーク端末として利用	保存する	同じ	● 端末の盗難や紛失による情報漏えいリスクがあり、端末に強力なセキュリティ対策を実装することが必要

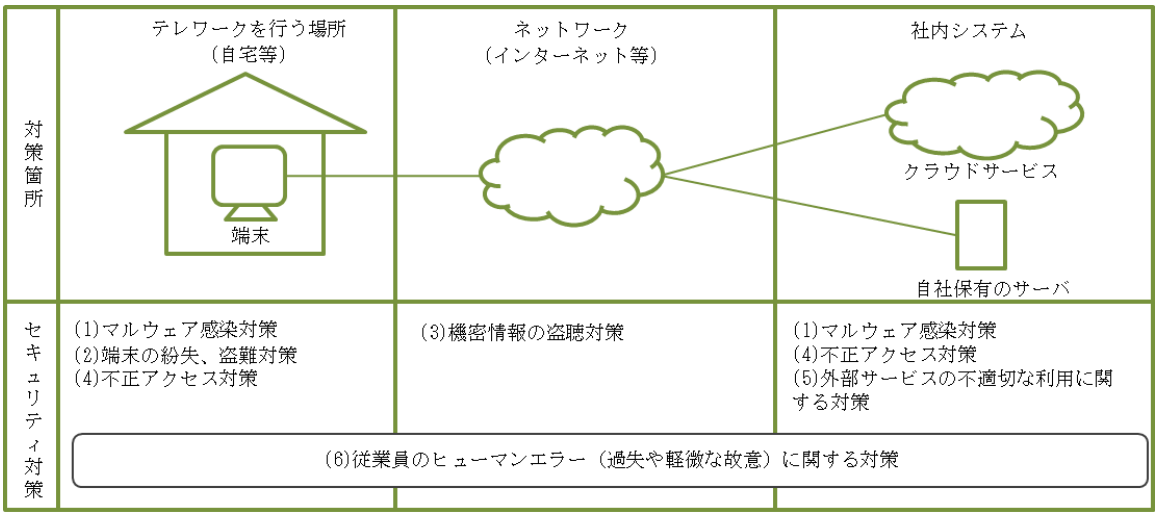
（出典：総務省「テレワークセキュリティガイドライン第 4 版、表 1 テレワークの 6 種類のパターン」をもとにＭＳ＆ＡＤインターリスク総研が作成）

短期間でテレワークを導入する必要がある場合、オフィスの環境設定変更をせずにすぐに導入できるテレワーク方式を選ぶことになる。会社ＰＣの持ち帰り方式は、普段から使用する会社ＰＣをそのまま持ち帰るだけであり、クラウドアプリ方式は、クラウド型アプリをテレワーク端末にインストールすることなどですぐ実現できる。ただし、これらの方式はテレワーク端末に業務に関するデータが保存されるので、端末の盗難や紛失による情報漏えいの発生が懸念される。テレワークにおいては、テレワーク端末に業務に関するデータを保存しないことが望ましいが、上記２方式のいずれかを選択せざるをえない場合は、端末自体に強力なセキュリティ対策を実装することが必要である。

テレワーク端末に業務に関するデータを保存しない方式として、クラウドアプリ方式の安全性を高めてクラウドサーバ上にデータを保存するセキュアブラウザ方式やアプリケーションラッピング方式、リモートで会社ＰＣにアクセスするリモートデスクトップ方式、仮想端末にアクセスする仮想デスクトップ方式がある。これらの方式においては、テレワーク端末の紛失や盗難が発生しても情報漏えいとなるリスクは小さい。ただし、リモートデスクトップ方式は、オフィスの環境にリモートアクセスする為に通信機の追加導入が必要となり、仮想デスクトップ方式とアプリケーションラッピング方式は、テレワーク専用の環境の構築が必要となるため、実現までに期間を要する場合があることに留意が必要である。セキュアブラウザ方式は、テレワーク端末にデータを保存せず、かつオフィス環境にも影響を与えない方式であるが、セキュアブラウザが対応するアプリしか使用できない為、実施できる業務が限定されること、セキュリティ対策が強化されている反面、通常のブラウザと比較すると使用する操作が複雑であったり、実行処理に時間がかかる傾向がある。

４．テレワークセキュリティ対策のポイント

テレワークの実施にあたっては、テレワークで取り扱う情報資産や導入するテレワーク方式に応じて、テレワーク端末、ネットワーク、社内システムそれぞれに個別・具体的な情報セキュリティ対策を策定し、導入することが必要である。以下に対策の例を示すが、詳細は、総務省「テレワークセキュリティガイドライン第４版」を参照されたい。



【図１】セキュリティ対策のポイントと実施箇所

（１）マルウェア感染に関する対策

- テレワーク端末へウイルス対策ソフトを導入し、最新の定義ファイルを適用する。
- テレワーク端末の OS やブラウザなどのソフトウェアのアップデートを行い最新の状態を維持する。

- サーバ側のマルウェア感染によるデータの破壊に備えて、社内データのバックアップを社内システムから切り離した状態で保存する。

（２）端末の紛失、盗難に関する対策

- 端末管理（または持ち出し）台帳を整備し、貸与するテレワーク端末の所在や利用者などを把握できるようにする。
- 端末紛失・盗難時の連絡ルールを定め、利用者へ周知徹底を行う。また、連絡を受けた後の端末の処置を定める。

（３）機密情報の盗聴に関する対策

- テレワークを実施する際には原則として公衆無線 LAN を使用しない。
- 公衆無線 LAN を使用する場合は取り扱う情報や業務の制限を設ける。

（４）不正アクセスに関する対策

- 認証においては、第三者から容易に推測されない十分な長さのパスワードを用いたり、パスワード以外の認証要素（所有者、生体）を利用して、強固な認証方式を採用する。
- インターネットと社内システムの境界にファイヤーウォールやセキュリティ機器を設置し、アクセス状況を監視する。

（５）外部サービスの利用に関する対策

- メッセージングアプリケーションを含む SNS をテレワークで利用する場合は、公開範囲の限定や業務上の守秘義務が課せられている情報の取り扱い禁止などの制限を設ける。

（６）従業員のヒューマンエラー（過失や軽微な故意）に関する対策

- テレワークに関する方針・規程・ルール類を整備した上で従業員に周知する。
- 情報セキュリティに関する社内教育を実施し、テレワークにより生じるリスクと対策の啓発を行う。
- テレワークの実施状況をモニタリングし、ルールの逸脱がないか確認する。

テレワークは、これまで十分に活用されてこなかった新しい働き方であり、導入にあたっては、テレワーク環境におけるセキュリティ対策に適切な投資を行うことが必要である。これには通信機器・設備やセキュリティ製品の購入だけでなく、その運用・管理を行う人的資源の確保も含まれる。

また、テレワークセキュリティ対策は、単に多額の投資を行えばよいものではない。自社のテレワークにおいて何を実現し何を守るべきか明確にした上で、その実現に適した方法を選び、その方法に求められるリスク対策を行うことが肝要である。

世界は未曽有の危機的な状況下にあるが、「ルール」・「ヒト」・「技術」が三位一体となり、バランスの取れたセキュリティ対策を備えたテレワークの活用を通じて、多くの企業がこの難局をしなやかに力強く乗り切る力（レジリエンス）をつけていくことを切に願う。

ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部 サイバーリスク室
上席コンサルタント　青山　昇司
上席コンサルタント　角田　悠樹

ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランス グループのリスク関連サービス事業会社として、リスクマネジメントに関するコンサルティングおよび広範な分野での調査研究を行っています。
サイバーリスク・情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研株式会社
新領域開発部　サイバーリスク室
千代田区神田淡路町2-105 TEL:03-5296-8961／FAX:03-5296-8941
https://www.irric.co.jp/

＜参考文献＞

i）JNSA「情報セキュリティポリシーサンプル改版（1.0 版）」
https://www.jnsa.org/result/2016/policy/
中小企業向けの情報セキュリティポリシーのサンプルを提供。テレワーク導入にあたっては以下の文書類を参考にされたい。
01_情報セキュリティ基本方針.pdf
01_情報セキュリティ方針.pdf
02_人的管理規程.pdf
07_リスク管理規程.pdf
08_セキュリテイインシデント報告・対応規程.pdf
14_スマートデバイス利用規程.pdf
15_SNS利用規程.pdf

ii）総務省「テレワークセキュリティガイドライン(第四版)」
https://www.soumu.go.jp/main_content/000545372.pdf
テレワークの実現方式の分類、事例を踏まえたセキュリティ対策のポイントを解説。

iii）日本テレワーク協会「中堅・中小企業におすすめのテレワーク製品一覧」
https://japan-telework.or.jp/wordpress/wp-content/uploads/2019/05/Tool-product-list-Ver2.0.pdf
コストを抑えたテレワークの製品を一覧化。コミュニケーションツールや、テレワークの実現の参考にされたい。

iv）米国国立技術標準研究所「NIST　SP800-46　Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security」
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf
米国国立技術標準研究所(NIST)が発行するテレワークのセキュリティ上の留意点をまとめたレポート。米国の政府機関がセキュリティ対策を実施する際に利用することを前提とした文書であるが、政府機関、民間企業を問わずセキュリティ担当者にとって有益な内容である。