中小企業等担当者向けテレワークセキュリティの手引きの概要

2022.1.31

総務省では、従来から、テレワークを業務に活用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「テレワークセキュリティィガイドライン」を策定してきました。
本書は、この「テレワークセキュリティガイドライン」を補うものとして、予算やセキュリティ体制等が必ずしも十分ではない中小企業等の担当者を対象としたものです。 具体的には、中小企業等の担当者がテレワークを導入し、利用を進めるに当たり、中小企業等が考慮すべきセキュリティリスクを踏まえ、中小企業等においても実現可能性が高く優先的に実施すべきセキュリティ対策を具体的に示しています。 そのため、本書で示すセキュリティ対策は、必ずしも網羅的ではありませんが、基本的かつ重要な（最低限必要となる）対策です。
まずは、本書で示す対策を実施すること を目標とすることで、効果的にテレワークセキュリティを確保することができます。

1.テレワークとは、情報通信技術（ICT:Information and Communication Technology）を活用し、場所や時間を有効に活用できる柔軟な働き方のことです。 テレワークの形態は、業務を行う場所に応じて、在宅勤務、サテライトオフィス勤務、 モバイル勤務に分類され、本書ではいずれの形態も対象としています。
テレワークの導入や利用に関して最低限必要なセキュリティ対策を実施するためにテレワークセキュリティの手引きとして『テレワークセキュリティガイドライン第５版』と併せての利用が有効です。

2.構成（活用法）
本書は、２部構成で作成されています。
まず、第１部「第１部1. テレワーク方式の確認」で、テレワークでの業 務内容や利用する端末等の状況を基に、該当するテレワーク方式を確認・特定してください。
第２部では、第１部で特定したテレワーク方式に対応するチェックリストを確認し、そのチェックリストをもとにセキュリティ対策を実施いたします。

●テレワーク方式の確認・特定

(1)会社支給端末・ＶＰＮ／リモートデスクトップ方式
(2)会社支給端末・クラウドサービス方式
(3)会社支給端末・スタンドアロン方式
(4)会社支給端末・セキュアブラウザ方式

(5)個人所有端末・ＶＰＮ／リモートデスクトップ方式

(6)個人所有端末・クラウドサービス方式

(7)個人所有端末・スタンドアロン方式

(8)個人所有端末・セキュアブラウザ方式

●テレワーク方式に対応するチェック対策チェックリストの確認（選択）

セキュリティ対策チェックリストを参照しテレワーク方式ごとにチェックリスト一覧表（補足資料）より対策を選択します。

チェックリスト内容

・対策内容

・想定脅威

・優先度

・方式ごとの対策要否

・想定脅威

セキュリティ対策について、優先度の高いものから効率的に着手・実施できる よう、優先度ごとにチェックリストを参照いたします。

●チェックリストの対策を実施するために、具体的な製品の設定例を解説しています。

テレワークツール設定例（設定解説資料）一覧　参照

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

なお、設定解説資料については、特定の製品の利用を促し又は避けるよう勧めるもの

ではありません。

引用元　総務省｜テレワークにおけるセキュリティ確保

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/