テレワークセキュリティガイドライン（第4版(案)）の概要

参考資料3
[H30.2.14～3.15パブコメ中]

○ 最近の社会や技術の変化（クラウドサービスやSNSの普及等）、新たなセキュリティ上の脅威（無線LANの脆弱性、ランサムウェアや標的型攻撃の登場等）などを踏まえた改定を実施。[前回改定：平成25年3月29日]

テレワークセキュリティガイドライン（第４版（案））構成

目次

はじめに　※セキュリティ対策の必要性や本ガイドラインの位置付け等を記載

1．テレワークにおける情報セキュリティの考え方
（ア）「ルール」「人」「技術」のバランスがとれた対策の実施
（イ）テレワークの方法に応じた対策の考え方
（ウ）経営者、システム管理者及びテレワーク勤務者それぞれの視点

2．テレワークセキュリティ対策のポイント
（ア）経営者が実施すべき対策
※セキュリティポリシーの策定・見直し、教育・啓発活動の実施を促す等
（イ）システム管理者が実施すべき対策
※アクセス制御等の技術的対策を講じる等
（ウ）テレワーク勤務者が実施すべき対策
※利用者認証情報の適正な管理、電子データ送信の際の暗号化等

3．テレワークセキュリティ対策の解説
（ア）情報セキュリティ保全対策の大枠
（イ）悪意のソフトウェアに対する対策
（ウ）端末の紛失・盗難に対する対策
（エ）重要情報の盗聴に対する対策
（オ）不正侵入・踏み台に対する対策
※「２．テレワークセキュリティ対策のポイント」で明示した内容について、対策分野ごとに詳細に解説

用語集

参考リンク集

【第4版における主な改定のポイント】

○ 会社の端末に加えて**私用端末（BYOD）を利用する場合や、クラウドサービスを利用する場合の留意点**を追加

○ 第３版で33項目（経営者：３、システム管理者：14、テレワーク勤務者：16）だったポイントについて、**無線LANの脆弱性対策（VPNの利用、https接続の利用等）、SNS利用の留意事項等を追加するなどして、計43項目に再編。**

○ **「実施するべき基本的な対策」（基本的対策事項）と、「実施することが望ましい対策」（推奨対策事項）に分けて解説**

○ テレワークに関する**「トラブル事例や対策」及び「コラム」を追加**

○ 本ガイドライン以外に**参考となる情報を「参考リンク集」にまとめ**、概要とURLを**新たに紹介**

テレワークセキュリティガイドライン（第４版）におけるセキュリティ対策のポイント①

経営者が実施すべき対策

※赤字は第4版改定で追加した項目

（情報セキュリティ保全対策の大枠）

1. 経営者は、テレワークの実施を考慮した情報セキュリティポリシーを定め定期的に監査し、その内容に応じて見直しを行う。
2. 社内で扱う情報について、その重要度に応じたレベル分けを行った上で、テレワークでの利用可否と利用可の場合の取扱方法を定める。
3. テレワーク勤務者が情報セキュリティ対策の重要性を理解した上で作業を行えるようにするため、定期的に教育・啓発活動を実施させる。
4. 情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を整えるとともに、事故時の対応についての訓練を実施させる。
5. テレワークにおける情報セキュリティ対策に適切な理解を示した上で、必要な人材・資源に必要な予算を割り当てる。

システム管理者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1. システム全体を管理する重要な立場であることを自覚し、情報セキュリティポリシーに従ってテレワークのセキュリティ維持に関する技術的対策を講じるとともに定期的に実施状況を監査する。
2. 情報のレベル分けに応じて、電子データに対するアクセス制御、暗号化の要否や印刷可否などの設定を行う。
3. 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に、定期的に教育・啓発活動を実施する。
4. 情報セキュリティ事故の発生に備えて、迅速な対応がとれるように連絡体制を確認するとともに、事故時の対応についての訓練を実施する。

（悪意のソフトウェアに対する対策）

5. フィルタリング等を用いて、テレワーク勤務者が危険なサイトにアクセスしないように設定する。
6. テレワーク勤務者がテレワーク端末にアプリケーションをインストールする際は申請させ、情報セキュリティ上の問題がないことを確認した上で認める。
7. 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。
8. 貸与用のテレワーク端末のＯＳ及びソフトウェアについて、アップデートを行い最新の状態に保つ。
9. 私用端末をテレワークに利用させる際は、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させた上で認める。
10. ランサムウェアの感染に備え、重要な電子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。
11. 金融機関や物流業者からの事務連絡を装うなどの不審なメールが迷惑メールとして分類されるよう設定する。

（端末の紛失・盗難に対する対策）

12. 台帳等を整備し、貸与するテレワーク端末の所在や利用者等を管理する。

（重要情報の盗聴に対する対策）

13. テレワーク端末において無線LANの脆弱性対策が適切に講じられるようにする。

（不正侵入・踏み台に対する対策）

14. 社外から社内システムへアクセスするための利用者認証について、技術的基準を明確に定め、適正に管理・運用する。
15. レワーク勤務者がインターネット経由で社内システムにアクセスする際のアクセス方法を定める。また、社内システムとインターネットの境界線にはファイアウォールやルータ等を設置し、アクセス状況を監視するとともに、不必要なアクセスを遮断する。
16. 社内システムへのアクセス用のパスワードとして、強度の低いものを用いることができないように設定する。

（外部サービスの利用に対する対策）

17. メッセージングアプリケーションを含むＳＮＳに関する従業員向けの利用ルールやガイドラインを整備し、その中でテレワーク時の利用上の留意事項を明示する。
18. ファイル共有サービス等のパブリッククラウド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方法を禁止する。

テレワークセキュリティガイドライン（第４版）におけるセキュリティ対策のポイント②

テレワーク勤務者が実施すべき対策

（情報セキュリティ保全対策の大枠）

1. 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い、定期的に実施状況を自己点検する。
2. テレワークで扱う情報について、定められた情報のレベル分けとレベルに応じたルールに従って取り扱う。
3. 定期的に実施される情報セキュリティに関する教育・啓発活動に積極的に取り組むことで、情報セキュリティに対する認識を高めることに務める。
4. 情報セキュリティ事故の発生に備えて、直ちに定められた担当者に連絡できるよう連絡体制を確認するとともに、事故時に備えた訓練に参加する。

（悪意のソフトウェアに対する対策）

5. マルウェア感染を防ぐため、ＯＳやブラウザ（拡張機能を含む）のアップデートが未実施の状態で社外のウェブサイトにはアクセスしない。
6. アプリケーションをインストールする際は、システム管理者にその旨を申請し、許可を受けたアプリケーションのみをインストールする。（私用端末利用の場合）テレワークで利用する端末にインストールするアプリケーションは、安全性に十分留意して選択する。
7. 作業開始前に、テレワーク端末にウイルス対策ソフトがインストールされ、最新の定義ファイルが適用されていることを確認する。
8. 作業開始前に、テレワーク端末のＯＳ及びソフトウェアについて、アップデートが適用され最新の状態であることを確認する。
9. テレワークにはルールに定められた情報セキュリティ対策が適用されているものを使用し、スマートフォン、タブレット等に関しては不正な改造（脱獄、root化等）を施さない。
10. テレワーク作業中にマルウェアに感染した場合、その報告漏れや遅れが被害拡大につながる恐れがあることを自覚し、電子メールの添付ファイルの開封やリンク先のクリックに一層の注意を払う。

（端末の紛失・盗難に対する対策）

11. オフィス外に情報資産を持ち出すとき、その原本を安全な場所に保存しておく。
12. 機密性が求められる電子データを極力管理する必要が無いように業務の方法を工夫する。やむを得ない場合は必ず暗号化して保存するとともに、端末や電子データの入った記録媒体（ＵＳＢメモリ等）等の盗難に留意する。

（重要情報の盗難に対する対策）

13. 機密性が求められる電子データを送信する際には必ず暗号化する。
14. 無線LAN利用に伴うリスクを理解し、テレワークで利用する場合は確保すべきセキュリティレベルに応じた対策が可能な範囲で利用する。
15. 第三者と共有する環境で作業を行う場合、端末の画面にプライバシーフィルターを装着したり、作業場所を選ぶ等により、画面の覗き見防止に努める。

（不正侵入・踏み台に対する対策）

16. 社外から社内システムにアクセスするための利用者認証情報（パスワード、ＩＣカード等）を適正に管理する。
17. インターネット経由で社内システムにアクセスする際、システム管理者が指定したアクセス方法のみを用いる。
18. テレワークで使用するパスワードは、使い回しを避け、一定以上の長さで他人に推測されにくいものを用いるように心がける。

（外部サービスの利用に対する対策）

19. 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、社内で定められたＳＮＳ利用ルールやガイドラインに従って利用するようにする。
20. テレワークでファイル共有サービス等のパブリッククラウドサービスを利用する場合、社内ルールで認められた範囲で利用する。