

- 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立場

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) マル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) 不正アクセスに対する対策
 - (カ) 外部サービスの利用に対する対策
- ※「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
- **クラウドサービス等の利用にあたっての対策**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**