テレワークセキュリティガイドラインの改定

- 総務省では従来から「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示してきた。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、**2020年９月**には、**実践的かつ具体的で分かりやすい内容のチェックリスト**を作成・公表。
- 今般、テレワークを取り巻く環境やセキュリティ動向の変化を踏まえ、「**テレワークセキュリティガイドライン**」の**全面的な改定**を行い、改定版（第５版）の案に**ついて意見公募を実施するもの**。

テレワークセキュリティガイドライン

（2018年４月　第４版）

2004年12月初版
2006年４月第２版
2013年３月第３版

【想定読者像】

- ✓ システム管理者のほか経営層や利用者を幅広く対象
- ✓ 専任の担当や部門が存在
- ✓ 基本的なIT用語は仕組みとして理解しているレベル
- ✓ 基本的なシステム設定作業は、補助解説なく実施可能

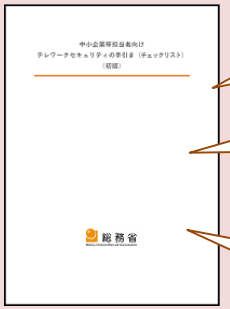
追加

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(チェックリスト)

（2020年９月　初版）

【想定読者像】

- ✓ システム管理担当者向け
- ✓ 専任の担当・部門は存在しない
- ✓ 基本的なIT用語は聞いたことがあるレベル
- ✓ 基本的なシステム設定作業は検索しながら実施可能



テレワーク方式を特定し、その方式に**対応するチェックリストを確認**

チェックリストは**最低限のセキュリティを確実に確保**してもらうためのものに限定

テレワーク用ソフトについて、**設定解説資料を作成**し具体的設定を解説

全面改定

【テレワーク環境・セキュリティ動向の変化】

- ✓ テレワークは「一部の従業員」が利用するものから、Web会議を含め、一般的な業務・勤務形態に
- ✓ クラウドサービスの普及やスマートフォン等の活用が進むなど、システム構成や利用形態が多様化
- ✓ 標的型攻撃等の高度な攻撃が増え、従来型のセキュリティ対策では十分対応できない状況も発生

【ガイドライン改定の主要なポイント】

- ✓ テレワーク方式を再整理した上で、テレワークによって実現する業務の内容や、セキュリティ統制の容易性等から、適した方式を選定するフローチャートを掲載。
- ✓ 経営者・システム管理者・勤務者の立場それぞれにおける役割を明確化。
- ✓ 執るべきセキュリティ対策の分類や内容を全面的に見直し
- ✓ テレワークセキュリティに関連するトラブルについて、具体的事例を含め全面見直し
  （事例紹介のほか、セキュリティ上留意すべき点や、採るべき対策についても明示）

テレワークセキュリティガイドラインの改定（案）概要

第４版（2018年４月）

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対策の考え方

✓ 「ルール」「人」「技術」のバランスのとれた対策の必要性を説明。
✓ テレワークの方式を6種類に整理し、その概要と対策の考え方を簡単に説明。
✓ 私用端末利用（BYOD）やクラウドサービス利用の留意点を追加。
✓ 「経営者」「システム管理者」「テレワーク勤務者」のそれぞれの立場について簡単な説明。

2. テレワークセキュリティ対策のポイント

✓ 「経営者」「システム管理者」「テレワーク勤務者」の類型ごとに実施すべき対策を記載。
✓ 第3版で33項目だったものを、計43項目に再編。（無線LANの脆弱性対策（VPNの利用、https接続等）やSNS利用の留意事項等を追加）
✓ 対策事項は、6個の脅威カテゴリに分類。

3. テレワークセキュリティ対策の解説

✓ 「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。
✓ 「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。
✓ 「トラブル事例や対策」や「コラム」を追加。

※上記のほか、「用語集」「参考リンク集」がある。

分割

- テレワーク**環境の変化**（感染症対応）等を追加
- **想定読者（チェックリストとの差異）**の項目を追加
- 経営者・管理者・勤務者の**役割を具体的に列挙**（適切な役割分担の重要性についても強調）
- テレワークやセキュリティの環境変化を踏まえ、
  - **クラウドサービス**の利用上の**考慮事項を追記**
  - サイバー攻撃の高度化を踏まえ、**ゼロトラストセキュリティ**に関する項目を追加
- **方式選定にもガイドラインは活用**されているため、
  - テレワーク方式の解説を章として独立・増強
  - **選定フローチャート**や**特性比較表**を新規作成
- テレワークの利用の広がりに合わせて、
  - **テレワーク方式を７種類に再編**（変更・細分化）
  - **派生的な構成**についても明記
- テレワーク利用の広まりや、サイバー攻撃の深刻化に対応するため、**対策事項を全面見直し**(倍増)
  例）オンライン会議システムのセキュリティ対策や、VPN機器のファームウェアアップデート等を新たに追加
- 対策事項を、13個の対策カテゴリに分類
- 各対策事項の詳細な解説についても、近年の動向を踏まえて全面的に見直し
- トラブル事例の対策に当たっては、複数対策が紐付く場合もあるため、章として独立
- 近年の実事例等を踏まえ、事例を全面更新

第５版（意見募集中）

第１章 はじめに

✓ 背景、目的、テレワークの形態、想定読者等を説明。

第２章 テレワークにおいて検討すべきこと

✓ 「ルール」「人」「技術」のバランスのとれた対策の必要性を説明。
✓ 「経営者」「システム・セキュリティ管理者」「テレワーク勤務者」の適切な役割分担の重要性と、各立場の役割を具体的に説明。
✓ テレワークを取り巻く環境変化を踏まえ、クラウドサービスの有効性やセキュリティ上の留意事項に関して説明。
✓ サイバー攻撃が高度化している状況を踏まえ、セキュリティ手法として注目されるゼロトラストセキュリティに関する考え方を説明。

第３章 テレワーク方式の解説

✓ テレワーク方式を7種類に再整理し、各方式について、基本的構成に加えて派生的な構成まで詳細に解説。
✓ 各テレワーク方式に特有のセキュリティ上の留意点について説明（各方式共通の対策は第4・5章）。
✓ 実現しようとする業務内容等を踏まえ、適した方式を選定するフローチャートや、各方式の特性比較表を掲載。

第４章 テレワークセキュリティ対策一覧

✓ 「経営者」・「システム・セキュリティ管理者」・「テレワーク勤務者」の役割ごとに、実施すべきセキュリティ対策を記載。（セキュリティ対策は「基本対策」と「発展対策」に区分。）
✓ テレワークが一般的な業務形態となってきたことに対応し、対策項目は98項目に倍増
✓ 対策分類は、13個のカテゴリに細分化し、見通しを整理。

第５章 テレワークセキュリティ対策の解説

✓ 第4章で明示した内容について、対策分類ごとに詳細に解説。

第６章 テレワークにおけるトラブル事例と対策

✓ トラブル事例を具体的に紹介した上で、セキュリティ上留意すべき点や、本ガイドライン内のどの対策が有効であるかを説明。