

中小企業の情報セキュリティ対策ガイドライン第3版 改訂のポイント

■ 改訂ポイント

(1) 全体構成

① 項目名称・構成の変更

- 項目名称を“付録の説明”から“何を行う”、“何ができる”を示す記述に変更
- 記述の順序の入れ替えとともに、具体的な対策に関する事項を 第2部 実践編の4. および5.に記載（詳細は下記（3）を参照

第2.1版	第3版
第1部 経営者編 1. 情報セキュリティ対策を怠ること 2. 経営者が負う責任 3. 経営者は何をすればよいか 第2部 実践編 1. 情報セキュリティ管理実践の進め方 2. 情報セキュリティ5か条 3. 5分でできる！情報セキュリティ 自社診断 4. 情報セキュリティポリシーの策定 5. 情報セキュリティ対策のさらなる改善に向けて	第1部 経営者編 1. 情報セキュリティ対策を怠ること 2. 経営者が負う責任 3. <u>経営者は何をやらなければならないのか</u> 第2部 実践編 1. 実践編の進め方 2. <u>できるところから始める</u> 3. <u>組織的な取り組みを開始する</u> 4. <u>本格的に取り組む</u> 5. <u>より強固にするための方策</u>

(2) 第1部 経営者編

- ① ITにあまり詳しくない経営者の方々にも理解していただけるよう、専門用語などをなるべく排して説明するように見直し
- ② 「SECURITY ACTION 自己宣言制度『一つ星』」との関連を解説したコラムを追加

(3) 第2部 実践編

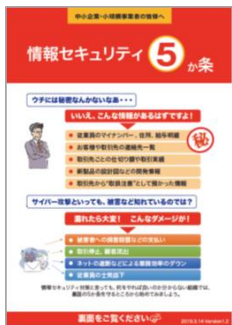
- ① 組織的な実施体制の構築と具体的な対策実践を段階的に進めてられるよう構成を見直し
- ② 「3.組織的な取り組みを開始する」に記載の「5分でできる自社診断」について、各診断項目の記述を簡素化
- ③ 「4.本格的に取り組む」において、「管理体制の構築」として、責任分担、連絡体制や緊急時対応体制の整備、予算化について解説。また情報セキュリティ規程の作成については、第2.1版において示した詳細なリスク分析を前提とせず、経営者が懸念する重大事故を踏まえたリスクの洗い出しを経た対策の決定と、「情報セキュリティ関連規程（サンプル）」（付録5）を活用した規程作成を提示
- ④ 「5.より強固にするための方策」において、技術的対策例、セキュリティサービス例などの具体的な対策手法を記載。「ウェブサイトの情報セキュリティ」、「クラウドサービスの情報セキュリティ」に関する解説を追加し、クラウドサービスについては安全利用のためのチェック項目を提示
- ⑤ 「SECURITY ACTION 自己宣言制度『二つ星』」との関連を解説したコラムを追加

(4) 付録

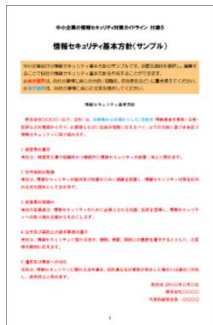
- ① 「5分のできる自社診断」のチェック項目の配点を一部変更。第2.1版で0点としていた「わからない」をマイナス1点に変更
→ 状況を把握できていない、あるいは内容を理解できていない状態は、情報セキュリティの確保において最も避けるべき状態であることからマイナス点とした
- ② 第2.1版の付録「情報セキュリティポリシーサンプル」を「情報セキュリティ基本方針(サンプル)」(付録2)と「情報セキュリティ関連規程(サンプル)」(付録5)に分割
- ③ 「中小企業のためのクラウドサービス安全利用の手引き」(付録6)を新規追加
→ 2011年4月に公開した同手引きの内容の見直しと再編集を行い、本ガイドラインに付録として統合

■ 参考：付録一覧

- 付録1： 情報セキュリティ5か条 (Adobe PDF形式)
- 付録2： 情報セキュリティ基本方針(サンプル) (Microsoft Word形式)
- 付録3： 5分のできる！情報セキュリティ自社診断 (Adobe PDF形式)
- 付録4： 情報セキュリティハンドブック(ひな形) (Microsoft PowerPoint形式)
- 付録5： 情報セキュリティ関連規程(サンプル) (Microsoft Word形式)
- 付録6： 中小企業のためのクラウドサービス安全利用の手引き (Adobe PDF形式)
- 付録7： リスク分析シート (Microsoft Excel形式)



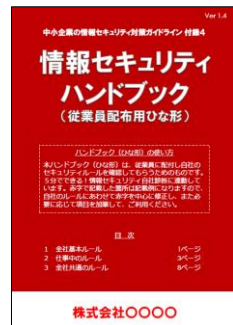
情報セキュリティ5か条



情報セキュリティ基本方針(サンプル)



5分のできる！情報セキュリティ自社診断



情報セキュリティハンドブック(ひな形)



情報セキュリティ関連規程(サンプル)



中小企業のためのクラウドサービス安全利用の手引き

リスク分析シート