# **情報セキュリティ基本方針および情報セキュリティハンドブックの概要【付録2・4】（INFORMATION 6-4追補原稿）**

## 概要

* + 1. 「できるところから始める」の次のステップとしての「組織的な取り組み」は、「5分でできる！情報セキュリティ自社診断」を実施し、「情報セキュリティ基本方針」を定め、公開すること。これにより「SECURITY ACTION」の２段階目の「二つ星」を使用することができます。
    2. 情報セキュリティハンドブックは、「5分でできる！情報セキュリティ自社診断」で確認された事項を、従業員向けに明文化したものである。
    3. 組織としての次のステップとして、本格的に取り組むためには、「情報セキュリティ関連規程」として対策基準を明文化することが求められる。

## 情報セキュリティ基本方針（サンプル）

* + 1. 概要
       - 中小企業向けの情報セキュリティ基本方針のサンプルです。必要な項目を選択し、編集することで自社の情報セキュリティ基本方針を作成することができます。
    2. 内容例
       - 株式会社○○○○（以下、当社）は、お客様からお預かりした/当社の/情報資産を事故・災害・犯罪などの脅威から守り、お客様ならびに社会の信頼に応えるべく、以下の方針に基づき全社で情報セキュリティに取り組みます。
       - 1.経営者の責任
         * 当社は、経営者主導で組織的かつ継続的に情報セキュリティの改善・向上に努めます。
       - 2.社内体制の整備
         * 当社は、情報セキュリティの維持及び改善のために組織を設置し、情報セキュリティ対策を社内の正式な規則として定めます。
       - 3.従業員の取組み
         * 当社の従業員は、情報セキュリティのために必要とされる知識、技術を習得し、情報セキュリティへの取り組みを確かなものにします。
       - 4.法令及び契約上の要求事項の遵守
         * 当社は、情報セキュリティに関わる法令、規制、規範、契約上の義務を遵守するとともに、お客様の期待に応えます。
       - 5.違反及び事故への対応
         * 当社は、情報セキュリティに関わる法令違反、契約違反及び事故が発生した場合には適切に対処し、再発防止に努めます。

## 情報セキュリティハンドブック（ひな形）

* + 1. ハンドブック（ひな形）の使い方
       - このハンドブック（ひな形）は、従業員に配付し、自社のセキュリティルールを実行してもらうためのものです。
       - ５分でできる！情報セキュリティ自社診断の対策例に連動しています。
       - 自社のルールに合わせて編集し、全従業員に配付するなどして一人ひとりが実施すべき対策の周知に取り組んでください。
    2. １-１ 全社基本ルール
       - OSとソフトウェアのアップデート
         * パソコンやスマホなど情報機器のOS やソフトウェアは常に最新の状態にする。【自己診断No.1】
       - ウイルス対策ソフトの導入
         * パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイルを最新の状態にする。【自己診断No.2】
       - パスワードの管理
         * パスワードは破られにくい「長く」「複雑な」パスワードを設定する。【自己診断No.3】
    3. １-２ 全社基本ルール
       - アクセス制御
         * 重要情報に対する適切なアクセス制限を行う。【自己診断No.4】
       - セキュリティに対する注意
         * 新たな脅威や攻撃の手口を知り対策を社内共有する仕組みを作る。【自己診断No.5】
    4. ２-１ 仕事中のルール
       - 電子メールの利用
         * 電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつける。【自己診断No.7】
         * 電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施する。【自己診断No.8】
    5. ２-１ 仕事中のルール
       - 電子メールの利用
         * 電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつける。【自己診断No.6】
    6. ２-３ 仕事中のルール
       - インターネットの利用
         * インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をする。【自己診断No.10】
       - データのバックアップ
         * パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得する。【自己診断No.11】
    7. ２-４ 仕事中のルール
       - クリアデスク・クリアスクリーン
         * 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管する。【自己診断No.12】
         * 離席時にパソコン画面の覗き見や勝手な操作ができないようにする。【自己診断No.14】
       - 重要情報の持ち出し
         * 重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をする。【自己診断No.13】
       - 重要情報の保管
         * 紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机上に放置せず、書庫などに安全に保管する。【自己診断No.12】
       - ２-５ 仕事中のルール
         * 入退室

事務所が無人になる時の施錠忘れ対策を実施する。【自己診断No.17】

* + - * + 電子媒体・書類の廃棄

重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにする。【自己診断No.18】

* + - * ３-１ 全社共通のルール
        + 私有情報機器の利用

個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にする。【自己診断No.21】

* + - * ３-2 全社共通のルール
        + クラウドサービスの利用

クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定する。【自己診断No.23】

* + - * ３-３ 従業員のみなさんへ
        + 従業員の守秘義務

従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせる。

* + - * + 事故が起きてしまったら

セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をする。