# **情報セキュリティ関連規程に記載すべき項目の概要【付録5】（INFORMATION 6-4追補原稿）**

## 概要

* + 1. 企業を取り巻くリスクは、事業内容や取り扱う情報、職場環境、ITの利用状況などによっても異なることがあり、汎用的な規程をそのまま使っても、自社に適さないことが考えられます。そこでここでは、効率的に自社に適した規程を作成する方法を解説します。
    2. ①対応すべきリスクの特定
       - 経営者が避けたい重大事故から対応すべきリスクを特定
    3. ②対策の決定
       - ・リスクの大きなものを優先して対策を実施
       - ・リスクが小さなものは許容するなど、合理的に対応
    4. ③規程の作成
       - 「情報セキュリティ関連規程（サンプル）」を参考に、自社に適した規定にするために修正を加える

## 情報セキュリティ関連規程の概要

* + 1. 1.組織的対策：
       - 情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
    2. 2.人的対策：
       - 取締役及び従業員の責務や教育、人材育成などのルールを定めます。
    3. 3.情報資産管理：
       - 情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
    4. 4.アクセス制御及び認証：
       - 情報資産に対するアクセス制御方針や認証のルールを定めます。
    5. 5.物理的対策：
       - セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
    6. 6.IT機器利用：
       - IT機器やソフトウェアの利用などのルールを定めます。
    7. 7.IT基盤運用管理：
       - サーバーやネットワーク等のITインフラに関するルールを定めます。
    8. 8.システムの開発及び保守：
       - 独自に開発及び保守を行う情報システムに関するルールを定めます。
    9. 9.委託管理：
       - 業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
    10. 10.情報セキュリティインシデント対応ならびに事業継続管理：
        - 情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
    11. 11.個人番号及び特定個人情報の取り扱い：
        - マイナンバーの取り扱いに関するルールを定めます。

## 1.組織的対策：

* + 1. 情報セキュリティのための管理体制の構築や点検、情報共有などのルールを定めます。
    2. 1.1.情報セキュリティのための組織
       - 情報セキュリティ対策を推進するための組織として、情報セキュリティ委員会を設置する。
       - 情報セキュリティ委員会は、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。
    3. 1.2.情報セキュリティ取組みの監査・点検/点検
    4. 1.3.情報セキュリティに関する情報共有
       - 入手先
         * ・IPA

[情報セキュリティ]

https://www.ipa.go.jp/security/

[ここからセキュリティ]

https://www.ipa.go.jp/security/kokokara/

* + - * + ・JVN（Japan Vulnerability Notes）

https://jvn.jp/index.html

* + - * + ・JPCERT/CC

https://www.jpcert.or.jp/

* + - * + ・個人情報保護委員会

http://www.ppc.go.jp/

## 2.人的対策：

* + 1. 取締役及び従業員の責務や教育、人材育成などのルールを定めます。
    2. 2.1.雇用条件
    3. 2.2.従業員の責務
    4. 2.3.雇用の終了
    5. 2.4.情報セキュリティ教育
    6. 2.5.人材育成

## 3.情報資産管理：

* + 1. 情報資産の管理や持ち出し方法、バックアップ、破棄などのルールを定めます。
    2. 3.1.情報資産の管理
       - 3.1.1.情報資産の特定と機密性の評価
       - 3.1.2.情報資産の分類の表示
       - 3.1.3.情報資産の管理責任者
       - 3.1.4.情報資産の利用者
    3. 3.2.情報資産の社外持ち出し
    4. 3.3.媒体の処分
       - 3.3.1.媒体の廃棄
       - 3.3.2.媒体の再利用
    5. 3.4.バックアップ
       - 3.4.1.バックアップ取得対象
       - 3.4.2.バックアップ媒体の取り扱い
       - 3.4.3.クラウドサービスを利用したバックアップ

## 4.アクセス制御及び認証：

* + 1. 情報資産に対するアクセス制御方針や認証のルールを定めます。
    2. 4.1.アクセス制御方針
    3. 4.2.利用者の認証
    4. 4.3.利用者アカウントの登録
    5. 4.4.利用者アカウントの管理
    6. 4.5.パスワードの設定
    7. 4.6.従業員以外の者に対する利用者アカウントの発行
    8. 4.7.機器の識別による認証
    9. 4.8.端末のタイムアウト機能
    10. 4.9.標準設定等
        - 4.9.1.アクセス制御対象情報システム及びアクセス制御方法
        - 4.9.2.利用者認証方法
        - 4.9.3.利用者アカウント・パスワードの条件
        - 4.9.4.機器の認証方法

## 5.物理的対策：

* + 1. セキュリティ領域の設定や領域内での注意事項などのルールを定めます。
    2. 5.1.セキュリティ領域の設定
    3. 5.2.関連設備の管理
    4. 5.3.セキュリティ領域内注意事項
    5. 5.4.搬入物の受け渡し

## 6.IT機器利用：

* + 1. IT機器やソフトウェアの利用などのルールを定めます。
    2. 6.1.ソフトウェアの利用
       - 6.1.1.標準ソフトウェア
       - 6.1.2.ソフトウェアの利用制限
       - 6.1.3.ソフトウェアのアップデート
       - 6.1.4.ウイルス対策ソフトウェアの利用
       - 6.1.4.1.ウイルス検知
       - 6.1.4.2.ウイルス対策ソフト定義ファイルの更新
       - 6.1.4.3.社外機器のLAN接続
       - 6.1.5.ウイルス対策の啓発
    3. 6.2.IT機器の利用
    4. 6.3.クリアデスク・クリアスクリーン
    5. 6.3.1.クリアデスク
    6. 6.3.2.クリアスクリーン
    7. 6.4.インターネットの利用
       - 6.4.1.ウェブ閲覧
       - 6.4.2.オンラインサービス
       - 6.4.3.SNSの個人利用
       - 6.4.4.電子メールの利用
       - 6.4.5.ウイルス感染の防止
    8. 6.5.私有IT機器・電子媒体の利用
       - 6.5.1.利用開始時
       - 6.5.2.利用期間中
         * 6.5.2.1.社内での利用
       - 6.5.3.利用終了時
    9. 6.6.標準等
       - 6.6.1.標準ソフトウェア
       - 6.6.2.ソフトウェアのアップデート方法
       - 6.6.3.ウイルス対策ソフトウェアの定義ファイルの更新方法

## 7.IT基盤運用管理：

* + 1. サーバーやネットワーク等のITインフラに関するルールを定めます。
    2. 7.1.管理体制
    3. 7.2.IT基盤の情報セキュリティ対策
       - 7.2.1.サーバー機器の情報セキュリティ要件
       - 7.2.2.サーバー機器に導入するソフトウェア
       - 7,2.3.ネットワーク機器の情報セキュリティ要件
    4. 7.3.IT基盤の運用
    5. 7.4.クラウドサービスの導入
    6. 7.5.脅威や攻撃に関する情報の収集
    7. 7.6.廃棄・返却・譲渡
    8. 7.7.IT基盤標準
       - 7.7.1.サーバー機器情報セキュリティ要件
       - 7.7.2.IT基盤標準ソフトウェア
       - 7.7.3.標準ネットワーク機器
       - 7.7.4.ネットワーク機器情報セキュリティ要件
       - 7.7.5.クラウドサービス情報セキュリティ対策評価基準

## 8.システムの開発及び保守：

* + 1. 独自に開発及び保守を行う情報システムに関するルールを定めます。
    2. 8.1.新規システム開発・改修
    3. 8.2.脆弱性への対処
    4. 8.3.情報システムの開発環境
    5. 8.4.情報システムの保守
    6. 8.5.情報システムの変更

## 9.委託管理：

* + 1. 業務委託にあたっての選定や契約、評価のルールを定めます。業務委託契約書の機密保持に関する条項例と委託先チェックリストのサンプルが付属します。
    2. 9.1.委託先評価基準
    3. 9.2.委託先の選定
    4. 9.3.委託契約の締結
    5. 9.4.委託先の評価
    6. 9.5.再委託

## 10.情報セキュリティインシデント対応ならびに事業継続管理：

* + 1. 情報セキュリティに関する事故対応や事業継続管理などのルールを定めます。
    2. 10.1.対応体制
    3. 10.2.情報セキュリティインシデントの影響範囲と対応者
    4. 10.3.インシデントの連絡及び報告
    5. 10.4.対応手順
       - 10.4.1.漏えい・流出発生時の対応
       - 10.4.2.改ざん・消失・破壊・サービス停止発生時の対応
       - 10.4.3.ウイルス感染時の初期対応
       - 10.4.4.欠番
       - 10.4.5.届出及び相談
    6. 10.5.情報セキュリティインシデントによる事業中断と事業継続管理
       - 10.5.1.想定される情報セキュリティインシデント
       - 10.5.2.復旧責任者及び関連連絡先
       - 10.5.3.事業継続計画

## 11.個人番号及び特定個人情報の取り扱い：

* + 1. マイナンバーの取り扱いに関するルールを定めます。
    2. 11.1.関係法令・ガイドライン等の遵守
    3. 11.2.利用目的
    4. 11.3.安全管理措置に関する事項
    5. 11.4.委託の取り扱い
    6. 11.5.継続的改善
    7. 11.6.特定個人情報等の開示
    8. 【参考】「個人番号及び特定個人情報取扱規程」サンプル

## 情報セキュリティハンドブック

* + 1. このハンドブック（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。
       - 赤字で記載した箇所は記載例です。自社のルールにあわせて赤字を中心に編集し、必要に応じて加筆してご利用ください
    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
         * 自己診断No.１
       - ウイルス対策ソフトの導入
         * 自己診断No.2
       - パスワードの管理
         * 自己診断No.3
    3. １-２ 全社基本ルール
       - アクセス制御
         * 自己診断No.4
       - セキュリティに対する注意
         * 自己診断No.5
    4. ２-１ 仕事中のルール
       - 電子メールの利用
         * 自己診断No.7,8
    5. ２-１ 仕事中のルール
       - 電子メールの利用
         * 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
         * 自己診断No.10
       - データのバックアップ
         * 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
         * 自己診断No.12,14
       - 重要情報の持ち出し
         * 自己診断No.13
       - 重要情報の保管
         * 自己診断No.12
       - ２-５ 仕事中のルール
         * 入退室

自己診断No.17

* + - * + 電子媒体・書類の廃棄

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

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

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

自己診断No.23

* + - * + 事故が起きてしまったら

自己診断No.24