

中小企業の情報セキュリティ対策ガイドライン

# わが社の情報セキュリティポリシー

情報セキュリティポリシーは、ひな型をそのまま使ってもうまく機能しません。企業の業務やIT環境などに応じて作成・カスタマイズする必要があります。

中小企業の情報セキュリティ対策ガイドラインの付録3のツールを利用して、自社にどのような情報があるか、どのような脅威への対策が必要かに答えると、自社にあった情報セキュリティポリシーを簡単に作成することができます。わが社の情報セキュリティポリシーを策定してみましょう！

手順

1

## 情報資産管理台帳を作成する

自社で保有している情報を<ツールA リスク分析シート>の「情報資産管理台帳」シートへ記入例に従い書き出し、それぞれの重要度を判定してください。

- 重要度2 事故が起きると事業に深刻な影響がある
- 重要度1 事故が起きると事業に重大な影響がある
- 重要度0 事故が起きても事業に影響はない

手順

2

## リスク値の算定

<ツールA リスク分析シート>の「脅威の状況」シートで想定される脅威を指定し、「対策状況チェック」シートで自社の対策状況を指定すると情報資産ごとのリスク値が計算されて対策が必要な情報資産が分かります。

- リスク値4～6 大 重点的に対策を実施
- リスク値1～3 中 対策を実施
- リスク値 0 小 現状維持

手順

3

## 情報セキュリティ対策を決定

<ツールA リスク分析シート>の「対策状況チェック」シートで自社の対策状況を以下から選択すると、「診断結果」シートに診断結果と自社で策定すべき情報セキュリティポリシーが表示されます。

- 1: 実施している …対策を実施済みの場合
- 2: 一部実施している …対策を実施しているが、十分でない場合
- 3: 実施していない／わからない …対策を実施していないか、関連情報がない場合
- 4: 自社には該当しない …当該項目に該当する業務を行っていない場合

手順

4

## 情報セキュリティポリシーを策定

手順3で表示された情報セキュリティポリシーを<ツールB 情報セキュリティポリシーサンプル>の中から選択し、自社の状況に合わせて編集すれば、自社専用の情報セキュリティポリシーが完成します。

なお必要に応じて、さらに項目を追加していただいてもかまいません。

※付録3のツール利用には、Microsoft Excel(2007以降)を実行できる環境が必要です。

※情報セキュリティポリシーの策定手順の詳細については、ガイドラインの「第2部 管理実践編 4. 情報セキュリティポリシーの策定」を参照してください。