中小企業の情報セキュリティ対策ガイドライン第3版

独立行政法人情報処理推進機構(IPA)
セキュリティセンター

中小企業の情報セキュリティ対策ガイドライン第3版

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

- **中小企業の経営者や実務担当者が、情報セキュリティ対策の必要性を理解し、情報を安全に管理するための具体的な手順等を示したガイドライン**
- **「クラウドサービス安全利用の手引き」を追加**
- **本編2部と付録より構成**
  - 経営者が認識すべき「3原則」、経営者がやらなければならない「重要7項目の取組」を記載
  - 情報セキュリティ対策の具体的な進め方を分かりやすく説明
  - すぐに使える「情報セキュリティ基本方針」や「情報セキュリティ関連規程」等のひな形を付録

第3版の主な変更点について

第1部　経営者編

- ITに詳しくない経営者にも理解しやすくするため、可能な限り専門用語を排する等記述を見直し

第2部　実践編

- 段階を踏んで対策を実践できるよう構成を見直し
- 「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

付録

- 「中小企業のためのクラウドサービス安全利用の手引き」を追加
- 旧版の付録「情報セキュリティポリシーサンプル」は、「情報セキュリティ基本方針（サンプル）」と「情報セキュリティ関連規程（サンプル）」に分割

ガイドラインの対象

ガイドラインP.3

- **対象組織**
  - 全ての業種の中小企業および小規模事業者
    （法人、個人事業主、各種団体も含む）
- **想定読者**
  - 経営者と情報セキュリティ対策を実践する責任者・担当者

経営者

責任者・担当者

ガイドラインの構成

ガイドラインP.3

- **中小企業の情報セキュリティ対策の考え方や実践方法について、本編2部と付録より構成**

構　成		概　要
本編	第１部　経営者編	経営者が知っておくべき事項、および自らの責任で考えなければならない事項について説明しています。
本編	第２部　実践編	情報セキュリティ対策を実践する方向けに、対策の進め方についてステップアップ方式で具体的に説明しています。
付録	付録１　情報セキュリティ５か条	組織の規模を問わず必ず実行していただきたい重要な対策を５か条にまとめ説明しています。
付録	付録２　情報セキュリティ基本方針（サンプル）	組織としての情報セキュリティに対する基本方針書のサンプルです。
付録	付録３　５分でできる！情報セキュリティ自社診断	あまり費用をかけることなく実行することで効果がある25項目のチェックシートです。
付録	付録４　情報セキュリティハンドブック（ひな形）	従業員に対して対策内容を周知するために作成するハンドブックのひな形です。
付録	付録５　情報セキュリティ関連規程（サンプル）	情報セキュリティに関する社内規則を文書化したもののサンプルです。
付録	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	クラウドサービスを安全に利用するための手引きです。15項目のチェックシートが付いています。
付録	付録７　リスク分析シート	情報資産、脅威の状況、対策状況をもとに損害を受ける可能性（リスク）の見当をつけることができます。

第1部　経営者編

ガイドラインP.5-14

1 情報セキュリティ対策を怠ることで企業が被る不利益

(1) 金銭の損失

(2) 顧客の喪失

(3) 業務の停滞

(4) 従業員への影響

2 経営者が負う責任

(1) 経営者などに問われる法的責任

(2) 関係者や社会に対する責任

3 経営者は何をやらなければならないのか

(1) 認識すべき「3原則」

(2) 実行すべき「重要7項目の取組」

(1) 認識すべき「3原則」

ガイドラインP.10-11

● 経営者は、以下の3原則を認識し、対策を進める

原則1 情報セキュリティ対策は経営者のリーダーシップで進める

- 経営者は、IT 活用を推進する中で、情報セキュリティ対策の重要性を認識し、自らリーダーシップを発揮して対策の実施を主導

原則2 委託先の情報セキュリティ対策まで考慮する

- 必要に応じて委託先が実施している情報セキュリティ対策も確認し、不十分な場合は対処を検討

原則3 関係者とは常に情報セキュリティに関するコミュニケーションをとる

- 情報セキュリティに関する取組方針を常日頃より関係者に伝えておくことで、サイバー攻撃によるウイルス感染や情報漏えいなどが発生した際にも、説明責任を果たすことができ、信頼関係を維持することが可能

経営者は何をやらなければならないのか

(2) 実行すべき「重要7項目の取組」

IPA

ガイドラインP.12-13

- 経営者は、以下の7項目を自ら実践するか、実際に情報セキュリティ対策を実践する責任者・担当者に対して指示し、確実に実行することが必要

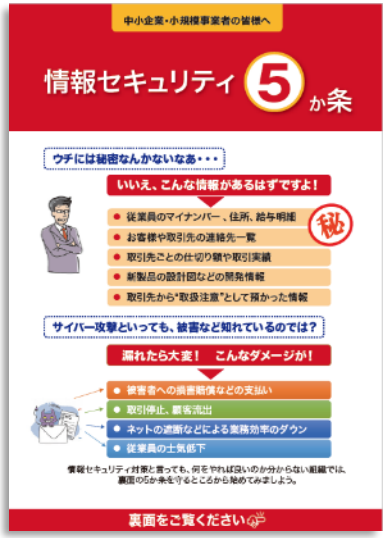
取組1	情報セキュリティに関する組織全体の対応方針を定める
取組2	情報セキュリティ対策のための予算や人材などを確保する
取組3	必要と考えられる対策を検討させて実行を指示する
取組4	情報セキュリティ対策に関する適宜の見直しを指示する
取組5	緊急時の対応や復旧のための体制を整備する
取組6	委託や外部サービス利用の際にはセキュリティに関する責任を明確にする
取組7	情報セキュリティに関する最新動向を収集する

第2部 実践編

ガイドラインP.15-54

●できるところから始めて段階的にステップアップ

Step1
できるところから始める



情報セキュリティ5か条

SECURITY ACTION
★一つ星を宣言

Step2
組織的な取り組みを開始する

5分でできる！
情報セキュリティ自社診断

SECURITY ACTION
★★二つ星を宣言

Step3
本格的に取り組む

情報セキュリティ関連規程

Step4
より強固にするための方策

- 情報収集と共有
- 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
- 情報セキュリティサービスの活用
- 技術的対作例と活用
- 詳細リスク分析の実施方法

より強固にするため方策

できるところから始める

ガイドラインP.17・付録1

Step1 Step2 Step3 Step4

（1）情報セキュリティ5か条

できるところから始める

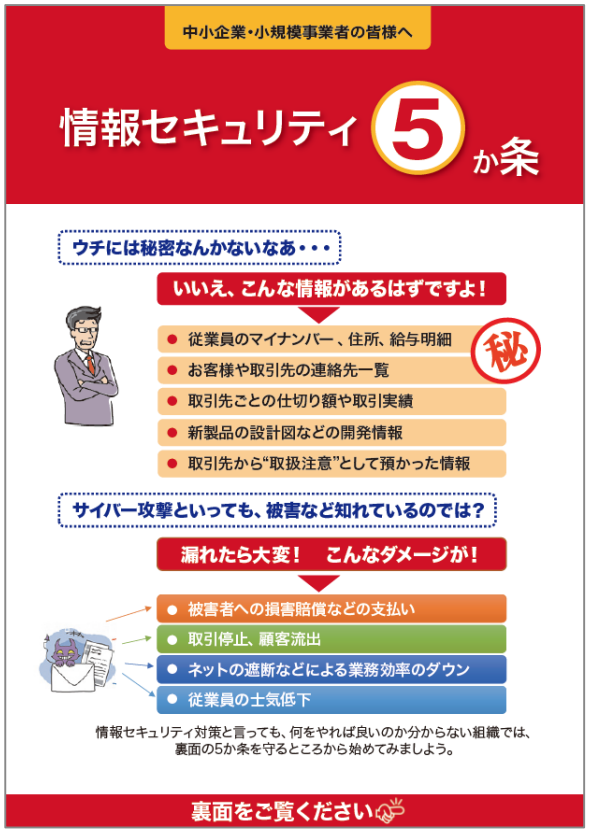
(1) 情報セキュリティ5か条

- **情報セキュリティ対策と言っても、何をやれば良いのか？**

情報セキュリティ5か条

を守るところから始めてみましょう。

1. OSやソフトウェアは常に最新の状態にしよう！
2. ウイルス対策ソフトを導入しよう！
3. パスワードを強化しよう！
4. 共有設定を見直そう！
5. 脅威や攻撃の手口を知ろう！



情報セキュリティ5か条

①OSやソフトウェアは常に最新の状態に

ガイドラインP.17・付録1

- **OSやソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウイルスに感染してしまう危険性があります。**
- **お使いのOSやソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。**

＜対策例＞

- Windows Update(Windows OSの場合)/
  ソフトウェア・アップデート(Mac OSの場合)/
  OSバージョンアップ(Android の場合)
- Adobe Flash Player/Adobe Reader/
  Java実行環境(JRE) など
  利用中のソフトウェアを最新版にする

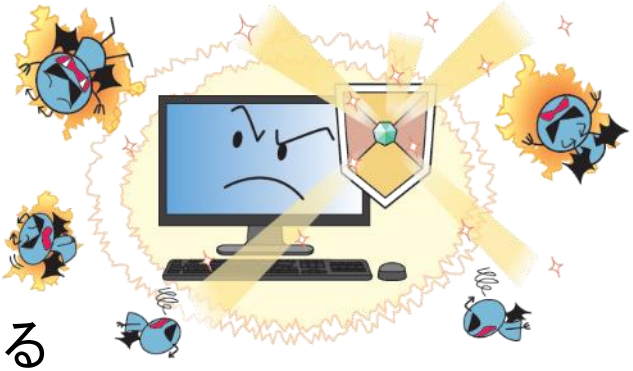
②ウイルス対策ソフトを導入

ガイドラインP.17・付録1

- **ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスが増えています。**
- **ウイルス対策ソフトを導入し、ウイルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。**

＜対策例＞

- ウイルス定義ファイルが自動更新されるように設定する
- 統合型のセキュリティ対策ソフト(ファイアウォールや脆弱性対策など統合的なセキュリティ機能を搭載したソフト)を導入する



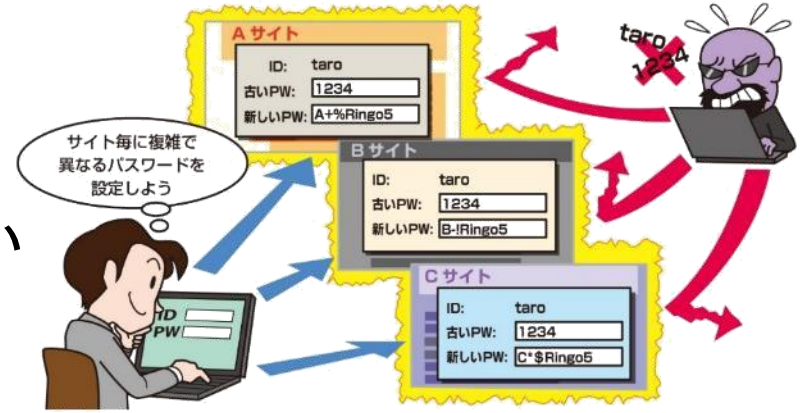
③パスワードを強化

ガイドラインP.17・付録1

- **パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。**
- **パスワードは「長く」、「複雑に」、「使い回さない」ようにして強化しましょう。**

＜対策例＞

- パスワードは英数字記号含めて長い文字数にする
- 名前、電話番号、誕生日、簡単な英単語などはパスワードに使わない
- 同じID・パスワードをいろいろなウェブサービスで使い回さない



情報セキュリティ5か条

④ 共有設定を見直す

ガイドラインP.17・付録1

- **データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。**
- **無関係な人が、ウェブサービスや機器を使うことができるような設定になっていないことを確認しましょう。**

＜対策例＞

- ウェブサービスの共有範囲を限定する
- ネットワーク接続の複合機やカメラ、ハードディスク(NAS)などの共有範囲を限定する
- 従業員の異動や退職時に設定の変更(削除)漏れがないように注意する

⑤ 脅威や攻撃の手口を知る

ガイドラインP.17・付録1

- **取引先や関係者と偽ってウイルス付のメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げてID・パスワードを盗もうとする巧妙な手口が増えています。**
- **脅威や攻撃の手口を知って対策をとりましょう。**

＜対策例＞

- IPAなどのセキュリティ専門機関のウェブサイトやメールマガジンで最新の脅威や攻撃の手口を知る
- 利用中のインターネットバンキングやクラウドサービスなどが提供する注意喚起を確認する

組織的な取り組みを開始する

ガイドラインP.18-21

Step1 Step2 Step3 Step4

（1）情報セキュリティ基本方針の作成と周知

（2）実施状況の把握

（3）対策の決定と周知

組織的な取り組みを開始する

（1）情報セキュリティ基本方針の作成と周知

ガイドラインP.18・付録2

- 経営者が定めた情報セキュリティに関する基本方針を、従業員や関係者に伝えるために簡潔な文書を作成・周知
- 「情報セキュリティ基本方針（サンプル）」を付録に収録

情報セキュリティ基本方針の記載項目例

- 管理体制の整備
- 法令・ガイドライン等の順守
- セキュリティ対策の実施
- 継続的改善　　など

組織的な取り組みを開始する

(2) 実施状況の把握

ガイドラインP.18-19・付録3

- **自社のセキュリティ対策の実施状況を把握するために「5分でできる！情報セキュリティ自社診断」を活用**
  - 25項目の設問に答えるだけで、自社の情報セキュリティの問題点を簡単に把握できる
  - 解説編の対策例を参考に、社内ルールを作成することができる
  - 付録の情報セキュリティハンドブックを活用すると従業員に対する社内ルールの周知が簡単にできる

5分でできる！情報セキュリティ自社診断

自社診断のための25項目

IPA

ガイドラインP.18-19・付録3

- 25項目の設問に答え、自社の情報セキュリティ対策の実施状況を把握

基本的対策　5項目

脆弱性対策、ウイルス対策、
パスワード強化など

従業員としての対策 13項目

標的型攻撃メール、電子メール、
持ち出し、廃棄、ウェブ利用など

組織としての対策 7項目

守秘義務、インターネット利用、
ルール化　など

	No	診断内容
基本的対策	1	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していますか？
	2	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※1 は最新の状態にしていますか？
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？
	4	重要情報※2 に対する適切なアクセス制限を行っていますか？
	5	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はできていますか？
従業員としての対策	6	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ていますか？
	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していますか？
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？
	9	無線 LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？
	10	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していますか？
	11	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していますか？
	12	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していますか？
	13	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していますか？
	14	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していますか？
	15	関係者以外の事務所への立ち入りを制限していますか？
	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？
	18	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していますか？
組織としての対策	19	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ていますか？
	20	従業員にセキュリティに関する教育や注意喚起を行っていますか？
	21	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していますか？
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？
	23	クラウドサービスやウェブサイトの運用などで利用する外部サービスは、安全・信頼性を把握して選定していますか？
	24	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していますか？
	25	情報セキュリティ対策（上記 1 ～ 24 など）をルール化し、従業員に明示していますか？

基本的対策

ガイドラインP.18-19・付録3

No.	診断内容	実施している	一部実施している	実施していない	わからない
1	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していますか？	4	2	0	-1
2	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※1 は最新の状態にしていますか？	4	2	0	-1
3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1
4	重要情報※2 に対する適切なアクセス制限を行っていますか？	4	2	0	-1
5	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はできていますか？	4	2	0	-1

※1　コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる
※2　営業秘密など事業に必要で組織にとって価値のある情報や顧客や、従業員の個人情報など管理責任を伴う情報のこと

従業員としての対策

ガイドラインP.18-19・付録3

No.	診断内容	実施している	一部実施している	実施していない	わからない
6	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ていますか？	4	2	0	-1
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していますか？	4	2	0	-1
8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1
9	無線LAN を安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1
10	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していますか？	4	2	0	-1
11	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していますか？	4	2	0	-1

5分でできる！情報セキュリティ自社診断

従業員としての対策

IPA

ガイドラインP.18-19・付録3

No.	診断内容	実施している	一部実施している	実施していない	わからない
12	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していますか？	4	2	0	-1
13	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していますか？	4	2	0	-1
14	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していますか？	4	2	0	-1
15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	-1
16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	-1
17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	-1
18	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していますか？	4	2	0	-1

組織としての対策

IPA

ガイドラインP.18-19・付録3

No.	診断内容	実施している	一部実施している	実施していない	わからない
19	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ていますか？	4	2	0	-1
20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	-1
21	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していますか？	4	2	0	-1
22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	-1
23	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していますか？	4	2	0	-1
24	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していますか？	4	2	0	-1
25	情報セキュリティ対策（上記1 ～ 24 など）をルール化し、従業員に明示していますか？	4	2	0	-1

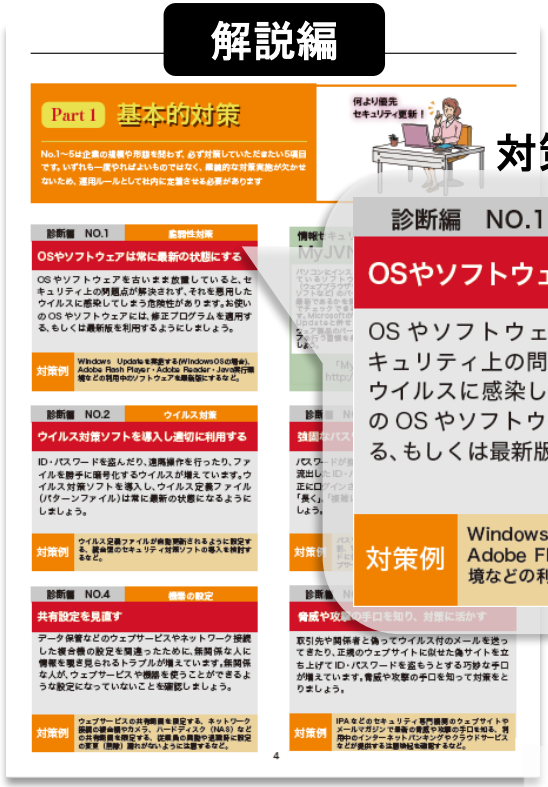
組織的な取り組みを開始する

(3) 対策の決定と周知

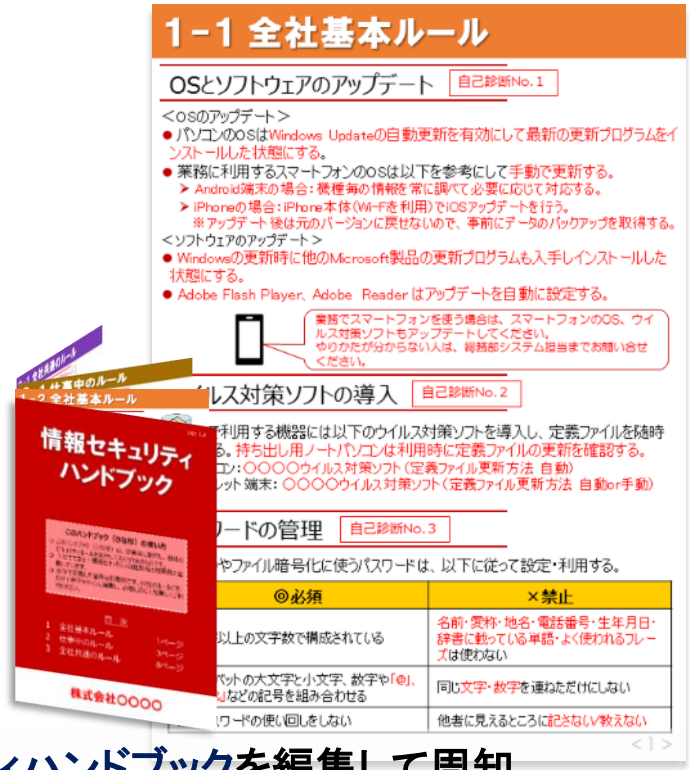
ガイドラインP.20-21・付録4

- 問題があった項目は、**解説編**を参考に対策を決定
- 付録「**情報セキュリティハンドブック（ひな形）**」を編集して社内周知

解説編



対策例を参考にして決定



情報セキュリティハンドブックを編集して周知

本格的に取り組む

（1） 管理体制の構築
（2） IT利活用方針と情報セキュリティの予算化
（3） 情報セキュリティ規程の作成
（4） 委託時の対策
（5） 点検と改善

本格的に取り組む

(1) 管理体制の構築

ガイドラインP.22-23

- 情報セキュリティ対策を推進するための管理体制を決定
- 付録5「情報セキュリティ関連規程」を活用して自社の管理体制を社内に周知

【表5】情報セキュリティ管理のための役割と責任分担(例)

役職名	役割と責任
情報セキュリティ責任者	情報セキュリティに関する責任者です。情報セキュリティ対策などの決定権限を有するとともに、全責任を負います。
情報セキュリティ部門責任者	各部門における情報セキュリティの運用管理責任者です。各部門における情報セキュリティ対策の実施などの責任と権限を有します。
システム管理者	情報セキュリティ対策のためのシステム管理を行います。
教育責任者	情報セキュリティ対策を推進するために従業員への教育を企画・実施します。
点検責任者	情報セキュリティ対策が適切に実施されているか点検します。

【表6】緊急時対応体制の役割と責任(例)

役職名	役割と責任
情報セキュリティ責任者	事故の影響を判断し、対応について意思決定する。
情報セキュリティ部門責任者	対応責任者の判断・意思決定に基づき適切な処置を行う。事故の原因を調べて情報セキュリティ責任者に報告する。
事故・異常を発見した従業員	事故や異常の内容を情報セキュリティ部門責任者に報告する。

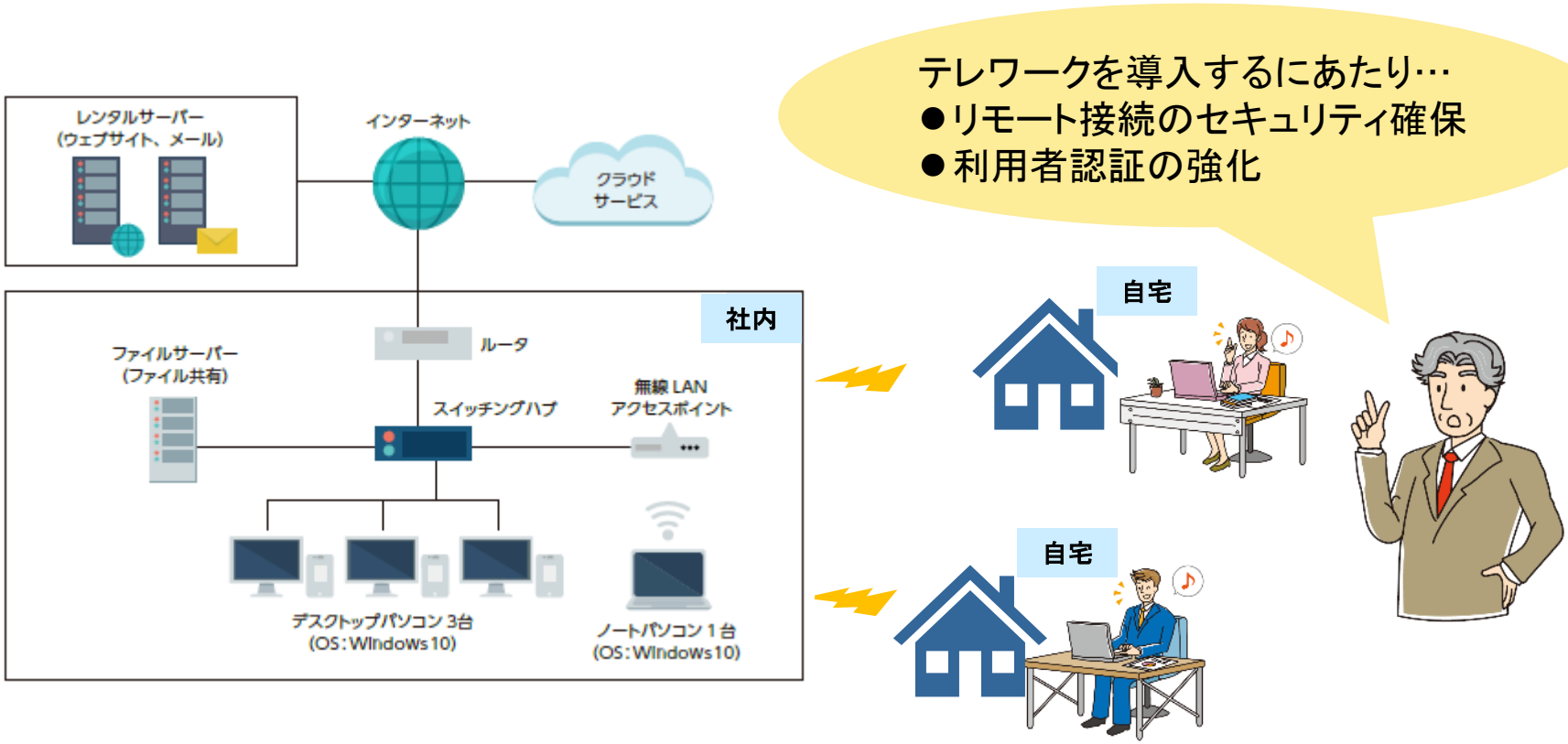
社内規程

本格的に取り組む

(2) IT利活用方針と情報セキュリティの予算化

ガイドラインP.23

- 利用している・検討している情報システムを把握
- 情報セキュリティ対策を検討して予算を確保



本格的に取り組む

(3) 情報セキュリティ規程の作成

ガイドラインP.24-25

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
  - 外部状況：法律や規制、情報セキュリティ事故の傾向、取引先からの情報セキュリティに関する要求事項など
  - 内部状況：経営方針・情報セキュリティ方針、管理体制、情報システムの利用状況など

本格的に取り組む

(3) 情報セキュリティ規程の作成

ガイドラインP.24

② 対策の決定

- リスクが大きなものを優先して対策を実施
  - いつ事故が起きてもおかしくない
  - 事故が起きると大きな被害になるなど
- リスクが小さなものは許容するなど、合理的に対応
  - 事故が起きる可能性が小さい
  - 発生しても被害が軽微であるなど

(3) 情報セキュリティ規程の作成

ガイドラインP.25・付録5

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、自社に適した規程にするために修正を加える
  - サンプル文中の赤字、青字部分を自社向けに修正すれば、自社の規程が完成
  - サンプルに明記されていなくても必要な対策や有効な対策があれば、追記

情報セキュリティ関連規程（サンプル）の概要

ガイドラインP.25・付録5

	名称	概要
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	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	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	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	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	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	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	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	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	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	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。

本格的に取り組む

(4) 委託時の対策

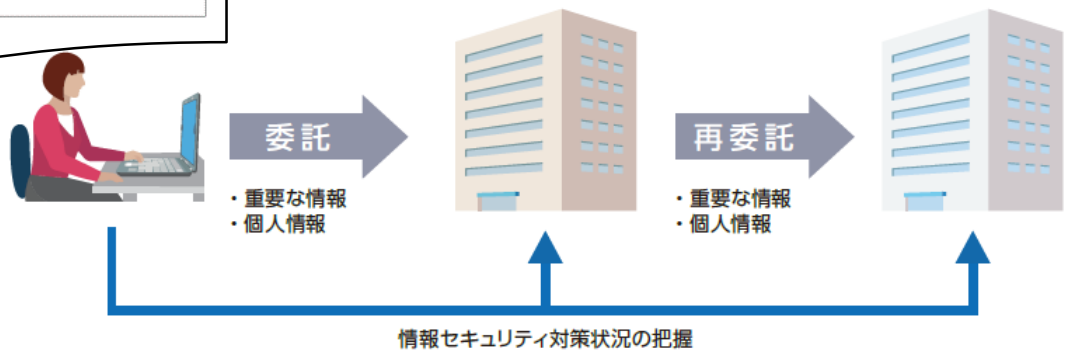
ガイドラインP.26-27

- 契約書や覚書に具体的な対策を明記
- 個別に契約や覚書を交わすことができる場合は、委託先のサービス規約や情報セキュリティ方針を確認
- 個人情報保護法では、個人データの取り扱いを委託する場合は、必要かつ適切な監督の実行

付録5　情報セキュリティ関連規程（サンプル）

9-1 業務委託契約に係る機密保持条項

注：このサンプルは、業務委託契約書における機密保持に関する条項を示すものです。委託元（甲）と委託先（乙）との双方が、相手から機密として提供される情報の守秘義務を負う双務契約の形式としています。

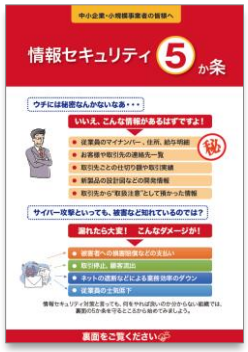


本格的に取り組む

(5) 点検と改善

ガイドラインP.28-29

- **情報セキュリティ対策が本当に実行されているか、見落としている対策はないか、対策がセキュリティ事故防止のために役に立っているか、等を確認**
- **点検の基準例**
  - その1)「情報セキュリティ5か条」
    「5分でできる！情報セキュリティ自社診断」
  - その2)情報セキュリティ対策に関するルール・規程



より強固にするための方策

- **より強固な情報セキュリティ対策に取り組むために、以下の6つの区分について説明**
  - **(1) 情報収集と共有**
    情報セキュリティに関する情報収集の方法と情報共有の枠組み
  - **(2) ウェブサイトの情報セキュリティ**
    ウェブサイトを安全に構築し、運用するためのポイント
  - **(3) クラウドサービスの情報セキュリティ**
    クラウドサービスを安全に利用するためのポイント
  - **(4) セキュリティサービス例と活用**
    情報セキュリティに関する外部サービス
  - **(5) 技術的対策例と活用**
    ITを活用する際の技術的対策
  - **(6) 詳細リスク分析の実施方法**
    「リスク分析シート」(付録7)を活用した詳細リスク分析の実施方法

（1）情報収集と共有

ガイドラインP.31

① 情報収集の方法

- 定常的に情報収集ができる方法を検討し、体制を整備
  - 情報セキュリティの専門機関、セキュリティベンダーなどのメールマガジンやソーシャルメディアに登録
  - セミナーに参加して積極的な情報収集

② 情報共有の枠組み

- 収集した情報は社内の関係者だけでなく、取引先や同業者に対しても共有することで、対策の向上を図る
- 共有する情報に機密情報が含まれる可能性がある場合は、守秘義務契約を交わす
- 情報共有の枠組みとしては、日本シーサート協議会の他、業界別のISAC＊が組織されている場合がある

＊ ISAC（Information Sharing and Analysis Center）同業界の事業者同士でサイバーセキュリティーに関する情報の共有・分析などを行う組織

より強固にするための方策

(2) ウェブサイトの情報セキュリティ

ガイドラインP.32-33

- **ウェブサイトの運営形態の検討から構築、実際に運営するまでの3つの段階に分けて検討事項を説明**

ウェブサイト運営形態の検討

ウェブサイトでの運営形態によってセキュリティ対策が異なるため、自社の状態に見合った運営形態を検討しましょう。

ウェブサイトの構築

ウェブサイトの技術的な脆弱性を認識したうえで、必要なセキュリティ対策を設計・開発の段階から検討しましょう。

ウェブサイトの運営

運用開始後に発覚した情報セキュリティ上の問題にも適切に対応し、ウェブサイトの安全性を維持向上しましょう。

(3) クラウドサービスの情報セキュリティ

ガイドラインP.34-37

- **クラウドサービスの選定から運用までのセキュリティ対策を3つの段階に分けて検討事項を説明**

クラウドサービスの選定

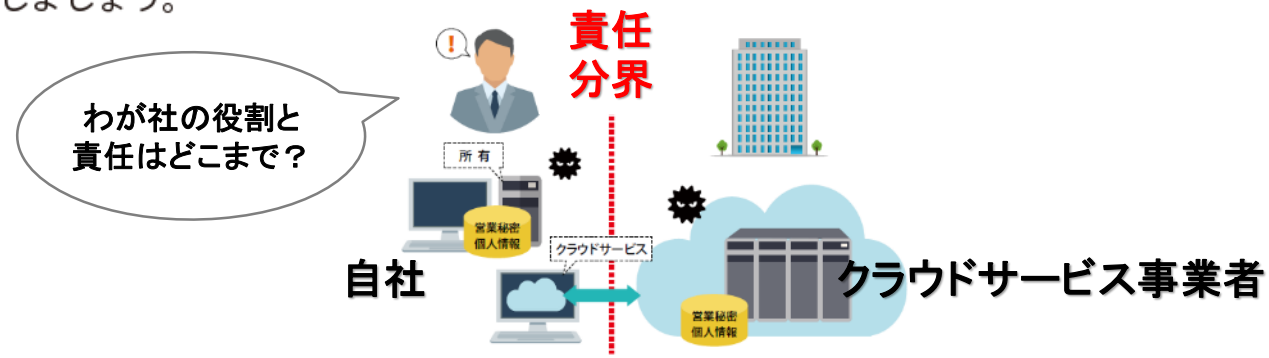
クラウド化する業務によって重視すべきセキュリティ対策は異なるため、業務のセキュリティ要件に見合ったサービスを選定しましょう。

クラウドサービスの運用

クラウドサービスは提供者と利用者が連携して運用するため、その特性を理解して運用しましょう。

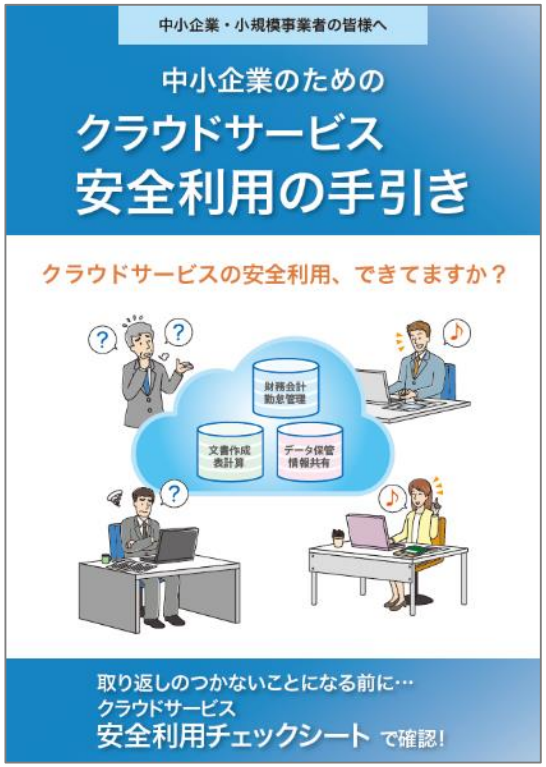
クラウドサービスのセキュリティ対策

サービス利用者が対応すべきセキュリティ対策を理解して実施しましょう。



中小企業のための
クラウドサービス安全利用の手引き

- **クラウドサービスを安全に利用するためには、何をやれば良いのかを説明**
  - クラウドサービス安全利用チェックシートで確認すべきことが分かる
  - 解説編で身近なサービスを例に、何を確認し、どうしたら安全に利用することができるか分かる



選択するときの確認ポイント

IPA

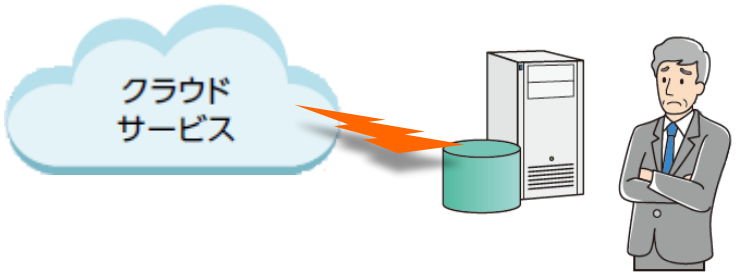
ガイドラインP.36・付録6

1	どの業務で利用するか明確にする	どの業務をクラウドサービスで行い、どの情報を扱うかを検討し、業務の切り分けや運用ルールを明確にしましたか？
2	クラウドサービスの種類を選ぶ	業務に適したクラウドサービスを選定し、どのようなメリットがあるか確認しましたか？
3	取扱う情報の重要度を確認する	クラウドサービスで取扱う情報が漏えい、改ざん、消失したり、サービスが停止した場合の影響を確認しましたか？
4	セキュリティのルールと矛盾しないようにする	自社のルールとクラウドサービス活用との間に矛盾や不一致が生じませんか？
5	クラウド事業者の信頼性を確認する	クラウドサービスを提供する事業者は信頼できる事業者ですか？
6	クラウドサービスの安全・信頼性を確認する	サービスの稼働率、障害発生頻度、障害時の回復目標時間などのサービス品質保証は示されていますか？

運用するときの確認ポイント

ガイドラインP.36・付録6

7	管理担当者を決める	クラウドサービスの特性を理解した管理担当者を社内に確保していますか？
8	利用者の範囲を決める	クラウドサービスを適切な利用者のみが利用可能となるように管理できていますか？
9	利用者の認証を厳格に行う	パスワードなどの認証機能について適切に設定・管理は実施できていますか？（共有しない、複雑にするなど）
10	バックアップに責任を持つ	サービス停止やデータの消失・改ざんなどに備えて、重要情報を手元に確保して必要なときに使えるようにしていますか？



セキュリティ管理の確認ポイント

IPA

ガイドラインP.36・付録6

11	付帯するセキュリティ対策を確認する	サービスに付帯するセキュリティ対策が具体的に公開されていますか？
12	利用者サポートの体制を確認する	サービスの使い方がわからないときの支援（ヘルプデスクやFAQ）は提供されていますか？
13	利用終了時のデータを確保する	サービスの利用が終了したときの、データの取扱い条件について確認しましたか？
14	適用法令や契約条件を確認する	個人情報保護などを想定し、一般的契約条件の各項目について確認しましたか？
15	データ保存先の地理的所在地を確認する	データがどの国や地域に設置されたサーバーに保存されているか確認しましたか？

(4) 情報セキュリティサービスの活用

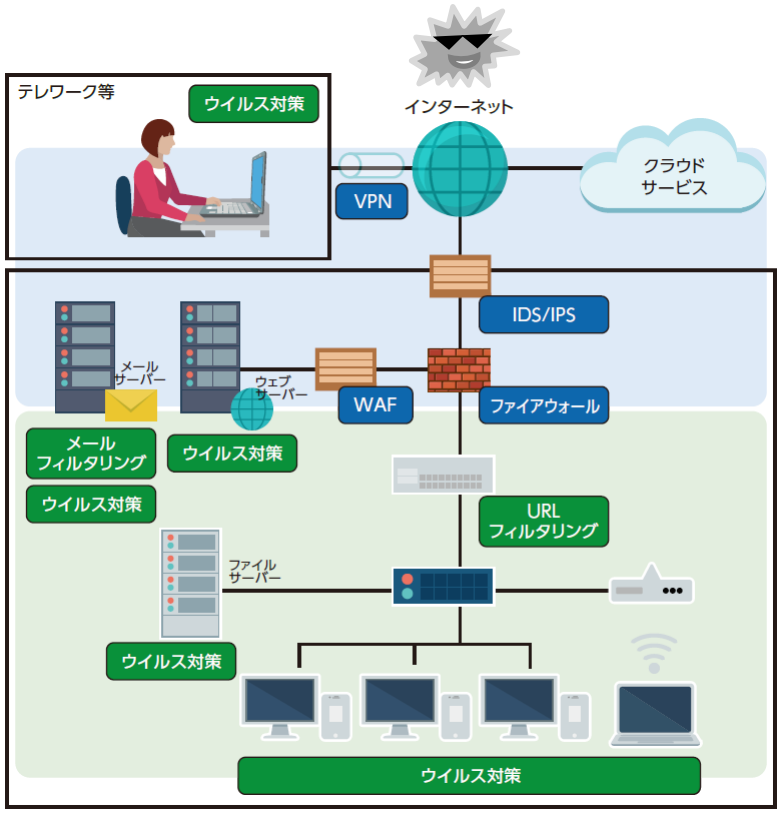
ガイドラインP.38

- **外部の情報セキュリティサービスを利用することで、より強固で有効な対策を実施することが可能**
- **情報セキュリティ人材が社内に不足している場合や、情報セキュリティの向上に有用**
  - ① 情報セキュリティコンサルテーション
  - ② 情報セキュリティ教育サービス
  - ③ 情報セキュリティ監査サービス
  - ④ 脆弱性診断サービス
  - ⑤ デジタルフォレンジックサービス
  - ⑥ セキュリティ監視・運用サービス

(5) 技術的対策例と活用

ガイドラインP.40-43

- **コンピュータやインターネットを利用するときに施す技術的対策(製品やソフトウェア)を紹介**
  - ① ネットワーク脅威対策
  - ② コンテンツセキュリティ対策
  - ③ アクセス管理
  - ④ システムセキュリティ管理
  - ⑤ 暗号化
  - ⑥ データの破棄



（6） 詳細リスク分析の実施方法

ガイドラインP.44-54

- 付録6「リスク分析シート」を使い、以下の手順で行う

手順1　情報資産の洗い出し

どのような情報資産があるか洗い出して重要度を判断する

↓

手順2　リスク値の算定

リスクの大きさを算定し対策が必要な情報資産を把握する

↓

手順3　情報セキュリティ対策の決定

リスクの大きな情報資産に対して必要とされる対策を決める

（6）詳細リスク分析の実施方法

手順１：情報資産の洗い出し

ガイドラインP.47・付録7

- **業種、事業内容、IT環境によって保有する情報資産は異なるため、台帳記入例を参考に、自社の情報資産を一通り洗い出し、以下の要領で作業を進める**
  - 情報資産の洗い出し
  - 情報資産ごとの機密性・完全性・可用性の評価
  - 機密性・完全性・可用性の評価値から重要度を算定

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			評価値				保存期限	登録日
						個人情報	要配慮個人情報	マイナンバー	機密性	完全性	可用性	重要度		
人事	社員名簿	社員基本情報	人事部	人事部	事務所PC	有			2	0	0	2		2016/7/1
人事	健康診断の結果	雇入時・定期健康診断	人事部	人事部	書類		有		2	2	1	2	5年	2016/7/1
経理	給与システムデータ	税務署提出用源泉徴収票	給与計算担当	人事部	事務所PC			有	2	2	1	2	7年	2016/7/1
経理	当社宛請求書	当社宛請求書の原本（過去3年分）	総務部	総務部	書類				1	1	1	1		2016/7/1
共通	電子メールデータ	重要度は混在のため最高値で評価	担当者	総務部	事務所PC	有			2	2	2	2		2016/7/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	社内サーバー	有			2	2	2	2		2016/7/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	可搬電子媒体	有			2	1	1	2		2016/7/1
営業	顧客リスト	得意先（直近5年間に実績があるもの）	営業部	営業部	モバイル機器	有			2	1	1	2		2016/7/1

情報資産管理台帳 記入例

手順2：リスク値の算定

IPA

ガイドラインP.49-50

- **手順1で洗い出した情報資産について、対策の優先度を決めるため、リスク値（リスクの大きさ）を算定**
  - 本ガイドラインでは「重要度」と「被害発生可能性」の2つの数値の掛け算で行う

リスク値 ＝ 重要度 × 被害発生可能性

重要度 ＝ 手順1にて算定
被害発生可能性 ＝ 脅威・脆弱性から算定

リスク値	4～6 大	深刻な事故が起きる可能性大
	1～3 中	重大な事故が起きる可能性有
	0 小	事故が起きる可能性小、起きても被害は受容範囲

例）
- ECサイトの顧客DB
- Webサーバ内に保存
- SQLインジェクション攻撃未対策

脅　威=3
脆弱性=3

重要度　＝2
被害発生可能性 ＝3

重要度 2×被害発生可能性 3=リスク値 6　深刻な事故が起きる可能性 大

手順３：情報セキュリティ対策を決定

ガイドラインP.52

- **手順2で算定したリスク値の大きいものから対策を検討し、自社に適した対策を決定する**
- **対策は以下のように区分して検討する**

① リスクを低減する

- 自社で実行できる情報セキュリティ対策を導入ないし強化することで、脆弱性を改善し、事故が起きる可能性を下げる

② リスクを保有する

- 事故が発生しても許容できる、あるいは対策にかかる費用が損害額を上回る場合などは対策を講じず、現状を維持する

③ リスクを回避する

- 仕事のやりかたを変える、情報システムの利用方法を変えるなどして、想定されるリスクそのものをなくす

④ リスクを移転する

- 自社よりも有効な対策を行っている、あるいは補償能力がある他社のサービスを利用することで自社の負担を下げる

参考情報

SECURITY ACTION 制度概要

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

IPA

- **中小企業自らが情報セキュリティ対策に取組むことを自己宣言する制度※**
  - 「中小企業の情報セキュリティ対策ガイドライン」の実践をベースに２段階の取組み目標を用意

１段階目（一つ星）

「情報セキュリティ5か条」に取組むことを宣言

２段階目（二つ星）

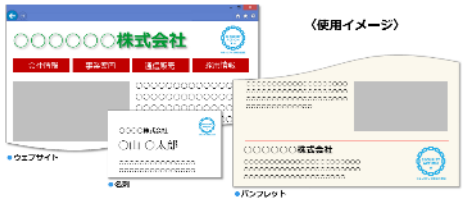
「5分でできる！情報セキュリティ自社診断」で自社の状況を把握したうえで、情報セキュリティ基本方針を定め、外部に公開したことを宣言

※SECURITY ACTION制度は、中小企業等自らが情報セキュリティ対策に取り組むことを自己宣言する制度です。
各企業等の情報セキュリティ対策状況等をIPAが認定する、あるいは認証等を付与する制度ではありません

SECURITY ACTION 制度のメリット

●情報セキュリティ対策への取組みの見える化

☞ ロゴマークをウェブサイトに掲出したり、名刺やパンフレットに印刷することで自らの取組み姿勢をアピール



●顧客や取引先との信頼関係の構築

☞ 既存顧客との関係性強化や、新規顧客の信頼獲得のきっかけに

●公的補助・民間の支援を受けやすく

☞ SECURITY ACTIONを要件とする補助金の申請、普及賛同企業から提供される様々な支援策が利用可能

（参考）普及賛同企業等

- **SECURITY ACTIONの趣旨に賛同し、当制度の普及促進のための積極的な取組みを実施する企業及び団体等です。**
- **中小企業が自己宣言するための支援策等を提供します。**
  - セキュリティに関する情報提供
  - セキュリティ体制の構築を支援
  - セキュリティ関連サービス提供時に優遇

ロゴマーク申込手順

IPA

STEP 1

使用規約を確認

SECURITY　ACTION自己宣言者サイトで使用規約をご確認ください。

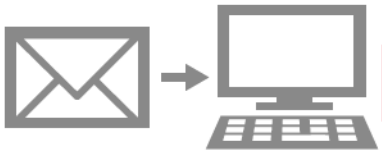
STEP 2

申込みフォームに入力

必要事項を入力してください。

STEP 3

申込み手続きを完了させる



申込み受付メールに記載されたURLをクリックして、申込み手続きを完了してください。

STEP 4

ダウンロード

申込み手続きを完了後、1～2週間程度でロゴマークをダウンロードできます。

SECURITY ACTION自己宣言者サイト

https://security-shien.ipa.go.jp/security/entry/

ご清聴ありがとうございました

独立行政法人 情報処理推進機構
セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目28番8号
文京グリーンコート センターオフィス
TEL 03（5978）7508　FAX 03（5978）7546
電子メール　isec-pr-nw@ipa.go.jp
URL　https://www.ipa.go.jp/security/