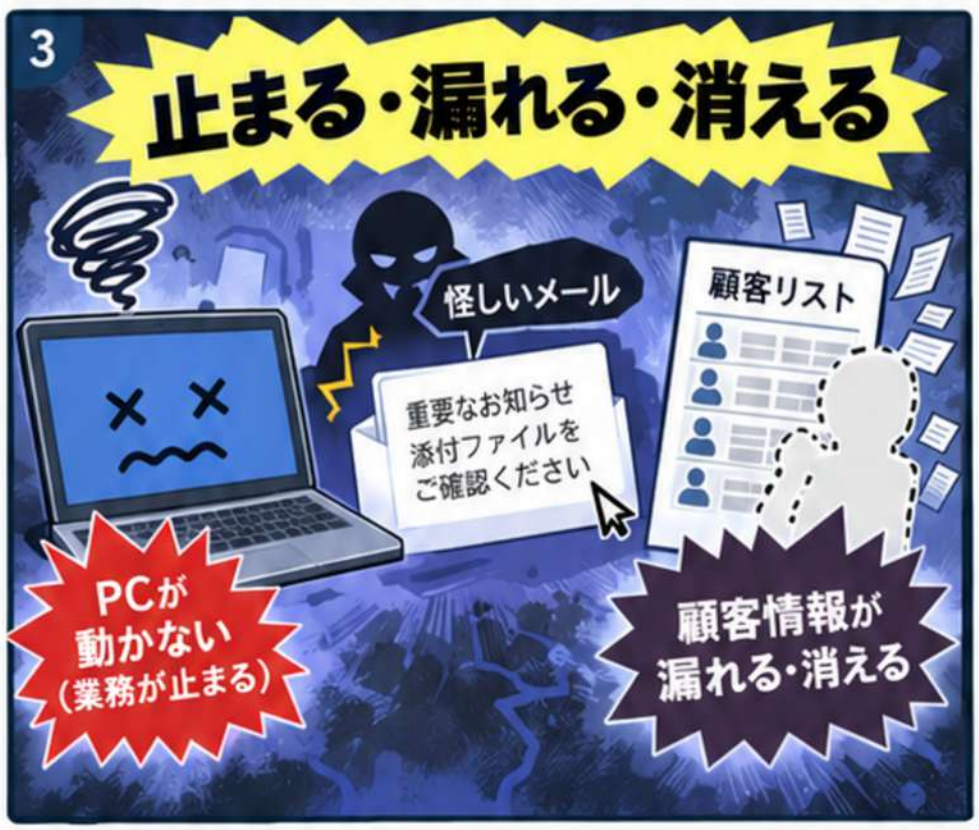
# マンガでわかる！
# 中小企業の情報セキュリティ対策

『中小企業の情報セキュリティ対策ガイドライン 第4.0版』をやさしく解説


















経営者編のポイント

# 経営者が押さえる3つの原則

1




2

## 原則1 経営者が主導する




- 方針や目標の決定
- 必要な予算・体制の確保
- 定期的な見直し・確認

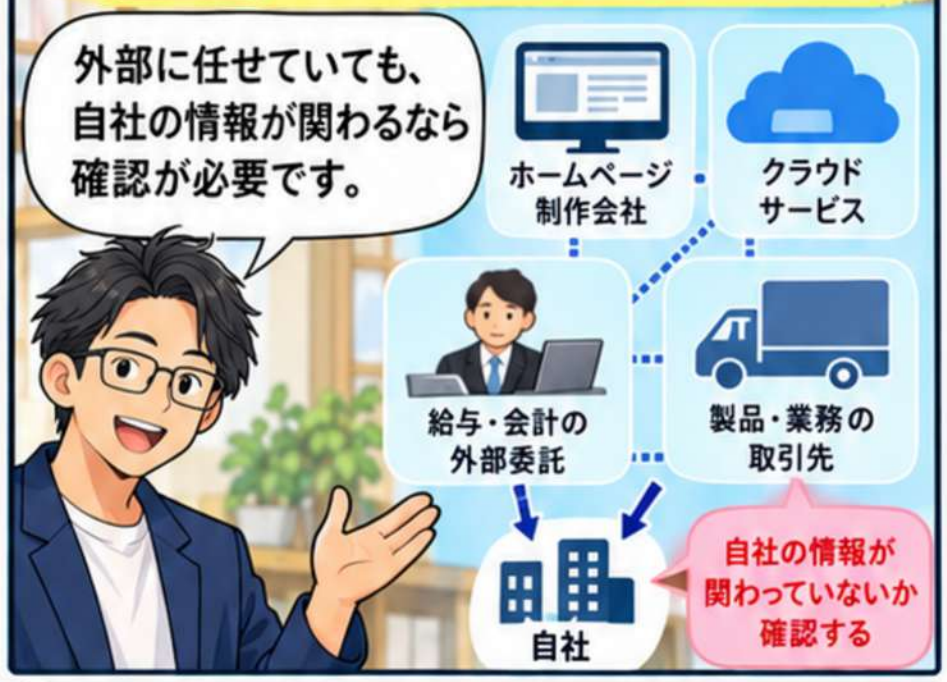
3

## 「何を守るか」「どこまでやるか」を決める




4

## 原則2 委託先・外部サービスも考える




5

## 原則3 関係者と普段から共有する




6




## 3つの原則 まとめ

1. 主導する — 経営者が方向を決める
2. 外部も確認 — 委託先・外部サービスも考える
3. 共有する — 関係者と普段から共有する

# 経営者が実行すべき重要7項目（前半）

1～4をやさしく整理




1

原則が分かったら、
次は**具体的な行動**です。

**経営者が実行すべき重要7項目**

1. 方針を決める
2. 予算と担当者を確保する
3. 必要な対策を考えて実行する
4. 定期的に見直す
5. 社内に周知・教育する
6. インシデント時の対応を整える
7. 社外とも連携する

2

## 1 方針を決める

「どんな情報を守るのか」
「何を大事にするのか」を
会社として決めましょう。

**基本方針**

- 守る情報
- 大切にすること
- 全社での取り組み方

3

## 2 予算と担当者を確保する

対策には人と時間とお金が
必要です。担当者を決め、
必要なら外部の力も
借ります。

- 予算（お金）
- 担当者（人）
- 時間
- 外部の力（専門家など）

4

## 3 必要な対策を考えて実行する

現場の実情を見て、必要な
対策を選び、実行を指示します。
ルール化すると続けやすく
なります。

**対策の例**

- ☑ パスワード管理
- ☑ メールの注意
- ☑ 機器の管理
- ☑ データのバックアップ

…など

→ ルール化 → 社内ルール

5

## 4 定期的に見直す

やりっぱなしはNG。
月次や定期的に、
できているか確認し、
改善しましょう。

確認（チェック） → 改善

**チェック項目の例**

- ☑ ルールが守られているか
- ☐ 問題はないか
- ☐ 新たなリスクはないか
- ☐ 対策は効果があるか

…など

6

方針→人と予算
→実行→見直し、
ですね！

はい。
次は残りの
3項目です。

# 経営者が実行すべき 重要7項目（後半）

## 5〜7と、もしもの備え

1

前回は1〜4まで教えてもらいましたが、今回は5〜7ですね。どんな内容ですか？

はい。今回は5〜7と、もしもの備えについて説明します。

田中

**経営者が実行すべき 重要7項目**

1 2 3 4 前回（基本対策）

5 6 7 今回（5〜7と、もしもの備え）

2

## 5 緊急時の対応と復旧を準備する

パソコンが動かない…！

!!

トラブルが起きたときの連絡先、役割、復旧手順を決めておきましょう。訓練も効果的です。

- 緊急連絡先リスト
- 役割分担
- 復旧手順（バックアップから復元）
- 訓練の実施

3

## 6 最新情報を集める

攻撃の手口は変わります。公的機関や業界の情報を定期的に確認しましょう。

新しい攻撃の手口の情報

注意喚起（アラート）

セキュリティニュース

業界の動向・対策事例

4

## 7 委託先・外部サービスとの責任を明確にする

クラウドや委託先を使うときは、誰が何を守るのかを契約やルールで確認します。

クラウドサービス ⟷ 委託先（外部サービス）

田中

**契約書・ルール**

- ☑ どこまでが自社の責任か
- ☑ どこまでが相手の責任か
- ☑ セキュリティ対策の内容
- ☑ トラブル時の対応　など

5

## 実際の現場では…

「外に任せているから大丈夫」ではないんですね。

はい。任せても確認は必要です。

×

任せきりはNG!

クラウドサービス ⟷ 委託先

自社でも契約内容の確認や運用状況のチェックを行いましょう。

6

## もしもの前に備えることが、被害を小さくします。

よし！早めに準備しよう！

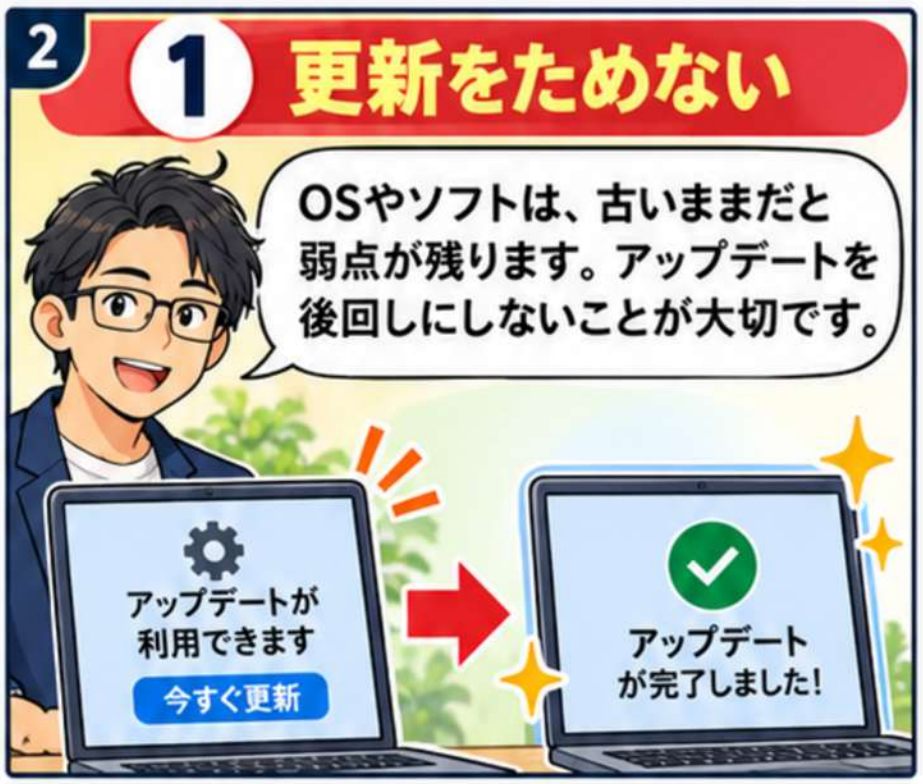
次は、今日からできる実践編です。

田中

# まずはここから！情報セキュリティ6か条（前半）

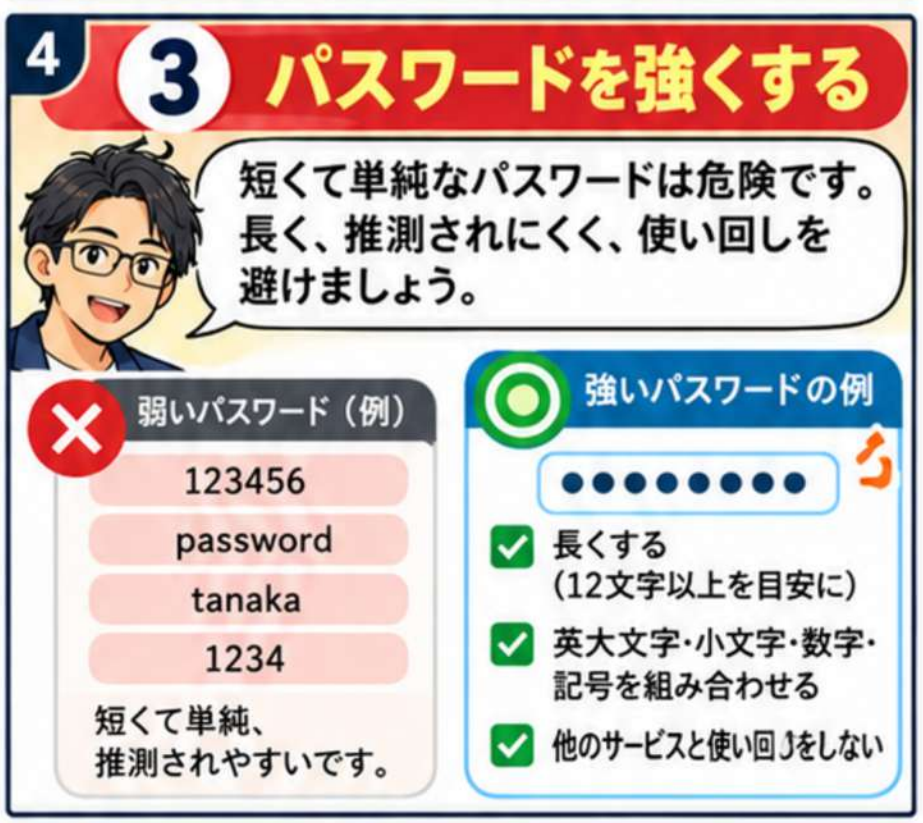
1〜3を今日から実践















# マンガでわかる！
# 情報セキュリティ6か条（後半）と、今日からの一歩

4〜6＋まとめ

## 1 4 共有設定を見直す

「社内だけのつもりが外から見えていた」を防ぐため、共有範囲を確認しましょう。







必要な人にだけ共有することが大切です！

## 2 5 バックアップを取る

消えた後では遅いこともあります。大事なデータは定期的にバックアップし、復元できるかも確認します。




そして、いざという時に復元できるかも確認しましょう。

## 3 6 脅威や攻撃の手口を知る



不審メール、偽サイト、詐欺電話など、よくある手口を知るだけでも被害は減らせます。

### 不審メール（フィッシング）




本物そっくりのメールでID・パスワードを盗み取る手口です。

### 偽サイト




本物と似た偽のWebサイトで情報を入力させる手口です。

### 詐欺電話（なりすまし）




取引先や公的機関を装って金銭や情報をだまし取る手口です。

## 4 全部を一気に完璧にしなくても大丈夫




## 5 今日からの一歩

1. **大事な情報を洗い出す**
   どんな情報を扱っているか、リストにしてみましょう。
2. **6か条を確認する**
   1〜6の内容を振り返り、自社でできているかチェックしましょう。
3. **自社診断をしてみる**
   ガイドラインの「5分でできる自社診断」で現状を把握しましょう。
4. **困ったら専門家に相談する**
   ITベンダーや支援機関など、信頼できる専門家に相談しましょう。

## 6 一歩が、会社の未来を守ります




参考：ガイドラインでは「5分でできる自社診断」などの付録も活用できます。