



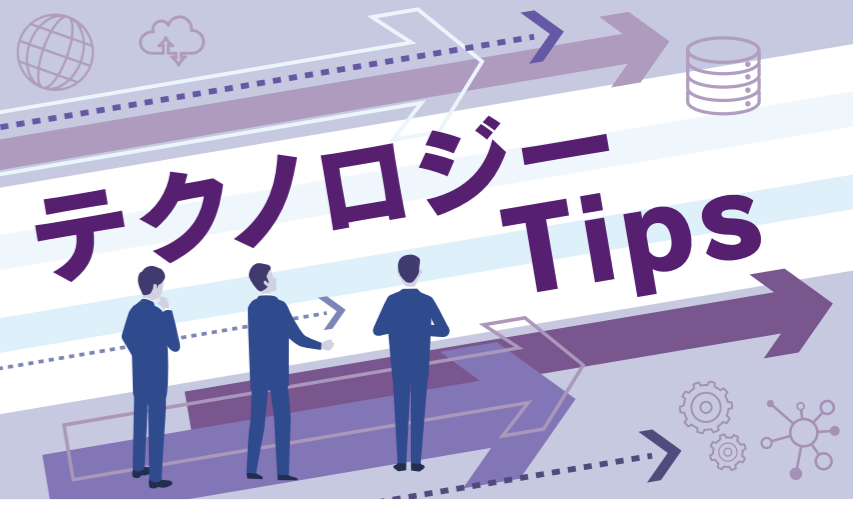
「何から始めればいいのかわからない」企業の経営者様・担当者様へ

情報セキュリティ

はじめの一歩。

お金を
かけない

IPA公式「6か条」+
SECURITY ACTION で、
信用と取引を守る経営の土台づくり



1. なぜ今、セキュリティに本気で取り組むのか重要なのか

IPAが毎年公表している「情報セキュリティ10大脅威 2026」では、組織編の上位に衝撃的な顔ぶれが並びました。

1位:ランサムウェアによる被害

2位:サプライチェーン攻撃

3位:AIを悪用した攻撃(初登場)

特に注目すべきは2位の「サプライチェーン攻撃」。これは、防御が強固な大企業を直接狙うのではなく、取引先の中小企業を踏み台にして侵入する手口です。「ウチみたいな小さな会社、狙われないでしょ」——この油断こそが、最も危険です。もし自社が踏み台になれば、信頼を失うだけでなく、取引先全体を巻き込む「加害者」にもなりかねません。



でも、安心してください。お金をかけなくても、今日から打てる手はたくさんあります。本号では、その具体的なやり方をご紹介します。

●情報セキュリティ10大脅威 2026 [組織]

順位	「組織」向け脅威	初選出年	順位	「組織」向け脅威	初選出年
1位	ランサム攻撃による被害	2016年 (11年連続11回目)	6位	地政学的リスクに起因するサイバー攻撃 (情報戦を含む)	2025年 (2年連続2回目)
2位	サプライチェーンや委託先を狙った攻撃	2019年 (8年連続8回目)	7位	内部不正による情報漏えい等	2016年 (11年連続11回目)
3位	AIの利用をめぐるサイバーリスク	初選出	8位	リモートワーク等の環境や仕組みを狙った攻撃	2021年 (6年連続6回目)
4位	システムの脆弱性を悪用した攻撃	2016年 (6年連続9回目)	9位	DDoS攻撃(分散型サービス妨害攻撃)	2016年 (2年連続7回目)
5位	機密情報を狙った標的型攻撃	2016年 (11年連続11回目)	10位	ビジネスメール詐欺	2018年 (9年連続9回目)

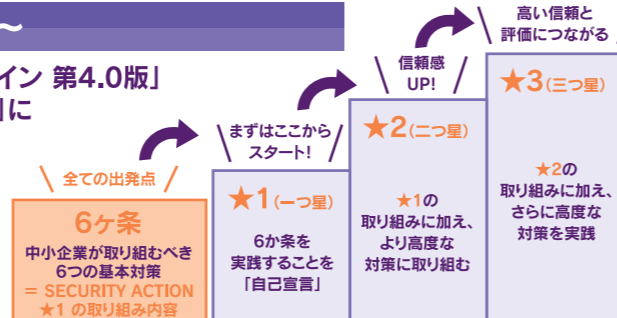
<https://www.ipa.go.jp/security/10threats/10threats2026.html> (IPA「情報セキュリティ10大脅威 2026」公式ページ) 出所:IPA

2. IPA「情報セキュリティ6か条」～まずはここから～

2026年3月27日、IPAは「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」を公開しました。最大の改訂ポイントは、これまでの「5か条」が「6か条」に拡張されたこと。背景には、ランサムウェア被害の深刻化があります。

6か条のポジション — セキュリティの「アルファベット」

この6か条は、後述するSECURITY ACTION ★1(一つ星)の取り組み内容そのものです。つまり「6か条をやる」と宣言するだけで、★1自己宣言の中身が揃います。



●情報セキュリティ6か条 (IPA公式・第4.0版)

- OSやソフトウェアは常に最新の状態にしよう
脆弱性を放置しない
- ウイルス対策ソフトを導入しよう
入口を守る
- パスワードを強化しよう
鍵を強くする
- 共有設定を見直そう
「うっかり公開」を防ぐ
- 脅威や攻撃の手口を知ろう
知ることが最大の防御
- バックアップを取ろう (第4.0版で新規追加)
やられても復旧できる



⑥バックアップ追加
(ランサムウェア対策が背景)

「5分でできる!」
情報セキュリティ自社診断が拡充

後述するSCS評価制度の
考え方を取り込み

<https://www.ipa.go.jp/security/guide/sme/about.html> (IPA「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」)
<https://www.ipa.go.jp/security/keihatsu/sme/guideline/6point.html> (6か条 解説ページ) 出所:IPA

3. 6か条、今日からこう実践する ～タダでできることばかり～

では、6か条を「具体的にどう実践するか」。現場目線で、お金をかけずに今日からできるやり方をご紹介します。

- OSやソフトウェアを最新に**
 - Windows Updateを「自動更新ON」に。月1回の再起動を業務ルールに
 - Windows 10は2025年10月にサポート終了済み → Windows 11への移行は「必須」です。
 - スマホもアプリの自動更新を有効に
- ウイルス対策ソフト**
 - Windows標準の「Microsoft Defender」も、有効化していれば一定水準を確保できます。
 - 重要:定義ファイルが最新かを月1回確認
 - 検知ログ・警告履歴も時々チェック(「気づかない感染」を防ぐ)
- パスワード強化**

まさか、4桁パスワードを使っていませんか?
8桁でも、現代のコンピュータで数時間～数日で破られます。

推奨 12桁以上、
英大文字+小文字+数字+記号の組み合わせ
例)Abc123!@#dEf98#

*パスワードマネージャーなどの活用も有効

パスワード管理アプリは、強固なパスワードの自動生成と入力で安全・時短を叶える必須ツール。
GoogleやMicrosoft製なら無料でも手軽に始められます。漏洩リスクを抑え「覚える負担」をゼロにするため、今すぐ活用しましょう!そして、もっと重要なのが…2要素認証(2FA / MFA) を必ず有効に。

用語	意味
2FA	Two-Factor Authentication(2要素認証)
MFA	Multi-Factor Authentication(多要素認証)

無料で今すぐ使える代表ソリューション

無料 Microsoft Authenticator 無料 Google Authenticator 無料 Authy

Microsoft 365、Google Workspace、銀行、SNS、ほぼ全サービスで対応しています。

仕組み 「知っているもの(パスワード)」+
「持っているもの(スマホ等)」で本人確認をします。
- 共有設定を見直す**
 - 具体的には、次のような点を確認してみてください。
 - Google Drive/OneDrive/Dropboxで「リンクを知っている全員」公開になっていないか
 - 退職者のアクセス権限は削除しているか
 - 「全社員に編集権」になっている重要ファイルはないか ●Wi-Fiの暗号化・ゲスト分離設定

4. 人と組織で守る ～技術だけでは守れない～

技術対策と同じくらい大事なのが、**人と組織**。残りの6か条と、組織のマネジメントの話です。

⑤脅威や攻撃の手口を知る = 社員教育

- フィッシングメール、ビジネスメール詐欺(BEC)、ランサムウェア…手口は日々進化しています
- 月1回・15分の社内勉強会でも効果は大きいです
- IPAの「情報セキュリティ10大脅威」を題材にすればOK
- IPAサイトに無料のひな形・教材が豊富にあります。



⑥バックアップ = 最後の砦

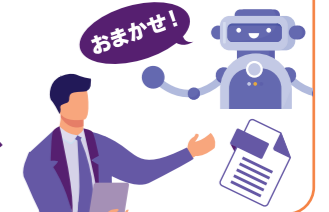
- ランサムウェアに感染してもバックアップがあれば復旧可能
- クラウドストレージの自動バックアップを活用しましょう

●3-2-1ルール



個人情報保護方針・セキュリティポリシーの整備

- ★2取得には「情報セキュリティ基本方針」の公開が必須
- IPAがサンプル(雛形)を無料で提供
- ここにAIを上手に使うのもおすすめ: 自社業務に合わせたカスタマイズの壁打ち、社員向けハンドブックの草案作成、教育資料のたたき台 など



AI活用時の注意 機密情報・個人情報はそのままAIに入力しない。学習に使われない設定(ビジネス契約・データ保護モード)を必ず確認しましょう。

<https://www.ipa.go.jp/security/keihatsu/sme/about.html>
(IPA「中小企業のセキュリティ対策」教材ページ)

5. 「やっています」に見える化 ～SECURITY ACTION ★1・★2～

SECURITY ACTIONとは

IPAが運営する自己宣言制度。認証ではなく、宣言。費用は無料です。

2026年4月1日システム刷新/

★1(一つ星)



セキュリティ対策自己宣言

「情報セキュリティ6か条」に取り組むことを宣言

★2(二つ星)



セキュリティ対策自己宣言

「5分でできる! 自社診断」で現状把握+「情報セキュリティ基本方針」を策定・公開を宣言

G BizID連携でログインがシンプルに



オンラインで申込み・即日でロゴ取得可能



補助金申請にも活用しやすくなりました



取得のメリット

無料
公式ロゴを名刺・HP・提案書に掲載できる

取引先・顧客に対する信用シグナル
企業価値の向上



補助金
デジタル化・AI導入補助金など、各種補助金の加点要件になりやすい



★3への階段がスムーズになる



<https://www.ipa.go.jp/security/security-action/> (IPA「SECURITY ACTION」公式ページ)
●<https://www.ipa.go.jp/security/security-action/onestar/> (★一つ星) ●<https://www.ipa.go.jp/security/security-action/twostar/> (★二つ星)
●<https://www.ipa.go.jp/security/security-action/it-hojo.html> (補助金との関係) 出所: IPA

6. その先へ ～SCS評価制度(★3～★5)と明日からの動き方～

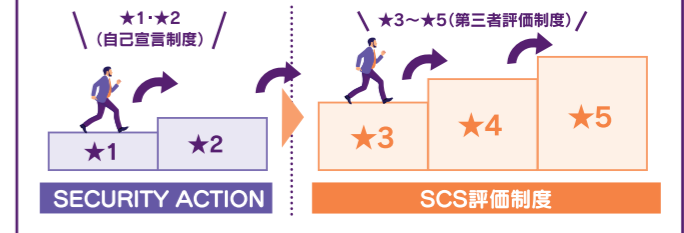
SCS評価制度とは

正式名称: サプライチェーン強化に向けたセキュリティ対策評価制度(経済産業省・内閣官房)

- 2026年度末スタート予定 ●★3～★5は第三者評価(自己宣言ではない)
- 取引先選定・大手企業との取引で判断材料になる可能性大

今、★1・★2を取る意味

★1・★2の取り組みは★3への土台そのもの。「今やっておく会社は、★3が始まったときに有利」それが、いま★1・★2を獲得する最大の意味です。



<https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html> (経済産業省「SCS評価制度」制度構築方針 確定版・2026年3月27日)
●<https://www.meti.go.jp/press/2025/12/20251226001/20251226001-b.pdf> (SCS評価制度 概要1枚ペーパー: ★3～★5一覧表) ●出所: 経済産業省

明日から動くー3ステップ実践プラン

STEP 1

今日～1週間
6か条+2FA を実装
0円

STEP 2

1ヶ月以内
SECURITY ACTION ★1を宣言
0円

STEP 3

3ヶ月以内
★2へ。自社診断+基本方針を公開
0円

次の一歩

半年～
社内勉強会の定着、★3取得を視野に準備
投資検討

<https://www.ipa.go.jp/security/security-action/entry/> (IPA SECURITY ACTION 申込ページ・申込フロー図あり) ●<https://gbiz-id.go.jp/> (G BizID)

まとめ セキュリティは「未来の選択肢」を守る投資

リスクを避けるための「守り」ではなく、機会を掴むための「準備」。

信用が積み上がる
取引機会が増える

社員が安心して働ける
採用・定着にプラス

業務が止まらない
経営の安定

大手取引先の要請に応える
ビジネス拡大

セキュリティはお金じゃない。「今日、はじめの一歩を踏み出すかどうか」の話です。

セキュリティで
会社の信用と未来を守る
3本の柱

今日から実践

IPA公式「6か条」で、お金をかけずにセキュリティの土台を作る。

信用の見える化

SECURITY ACTION ★1・★2で、取り組みを社外へシグナルする。

来年への準備

SCS評価制度(★3～★5)に備えて、今から階段を1段ずつ。

ぜひ、ご相談ください!
御社のAI×DX伴走パートナー
であり続けます。



- IPA SECURITY ACTION: <https://www.ipa.go.jp/security/security-action/>
- IPA 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: <https://www.ipa.go.jp/security/guide/sme/about.html>
- IPA 情報セキュリティ10大脅威 2026: <https://www.ipa.go.jp/security/10threats/10threats2026.html>
- 経済産業省 SCS評価制度: <https://www.meti.go.jp/press/2025/03/20260327001/20260327001.html>
- G BizID: <https://gbiz-id.go.jp/>

参考文献・注記: 本資料は2026年5月時点の公開情報を基に作成されています。制度の詳細や最新情報については、IPA・経済産業省の公式サイトをご確認ください。