
経営者のための「5分でできる！情報セキュリティ 自社診断」ライブ放送！

対策の必要性は感じているが、何から手をつけていいか分からない経営者へ
配布版

2026年10月15日(木) 18:00-19:15

ハクビー株式会社

代表取締役社長 松永赳堯

取締役副社長 田中誠也



目次

- 18:00 オープニング (5分)
- 18:05 「5分でできる！情報セキュリティ自社診断」とは何か (10分)
- 18:15 「セキュリティ対策自己宣言」のご紹介 (10分)
- 18:25 ハクビーが前回の自社診断からどれだけ改善したのか (30分)
- 18:55 Q&A (15分)
- 19:10 クロージング (5分)



1. オープニング

2. 「5分でできる！情報セキュリティ自社診断」とは何か

3. 「セキュリティ対策自己宣言」のご紹介

4. ハクビーが前回の自社診断からどれだけ改善したのか

5. Q&A

6. クロージング

自己紹介



創業者の田中（左）と松永（右）

会社概要

商号 ハクビー株式会社
代表者 代表取締役社長 松永 昶亮
設立 2026年7月
事業内容 Webアプリの受託開発／情報セキュリティ
住所 静岡県浜松市中央区舞阪町舞阪2701-9
浜松市舞阪支所4階
セキュリティ対策自己宣言 二つ星 ★★



自己紹介

代表取締役社長 松永 昶亮（まつなが たけあき）
大手ネットワーク機器メーカーでソフトウェアエンジニアとして、大規模なWebアプリケーション開発を経験後に独立。修士（工学）。犬が好き。

取締役副社長 田中 誠也（たなか せいや）
大手自動車メーカーのIT部門で、会社の業務を支える大規模システムの開発・運用を経験後に独立。修士（工学）。武士の歴史が好き。

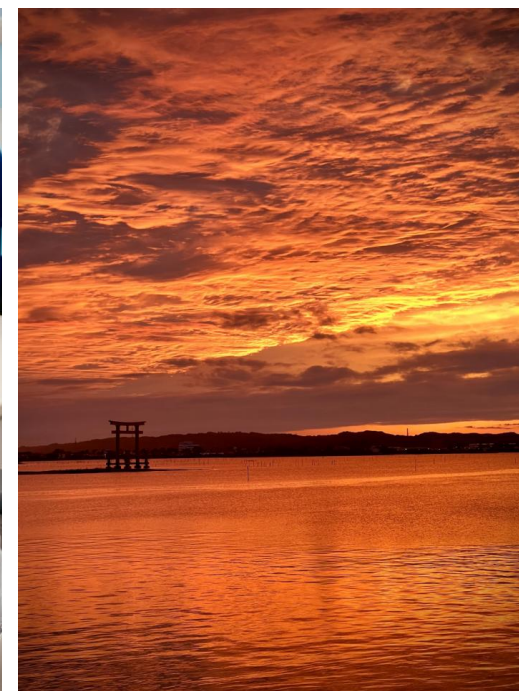
自己紹介



眺めがいいオフィス
(浜松市さまに感謝！)



オフィスのネットワークをつくる松永



弁天島の夕焼け

ハクビー株式会社 | 情報技術で浜松の事業を創り、守る。



背景：国内のセキュリティ事情

脅威

- 10大脅威2026（組織）は1位ランサム攻撃、2位サプライチェーン攻撃
- 守りの薄い取引先・委託先が、発注元へ侵入する踏み台にされる
- 内部不正（7位）やビジネスメール詐欺（10位）など人を突く脅威も上位

制度

- 経産省のSCS評価制度：★3・★4は2026年度末頃に申請受付開始予定
- ガバナンス整備・取引先管理などの組織的対策を要求
- 技術だけでなく組織的・人的対策をサプライチェーン全体で求める流れ



本日のゴール

問

- 今のくらいできていて、次に何をすべきか分かりますか？

ゴール

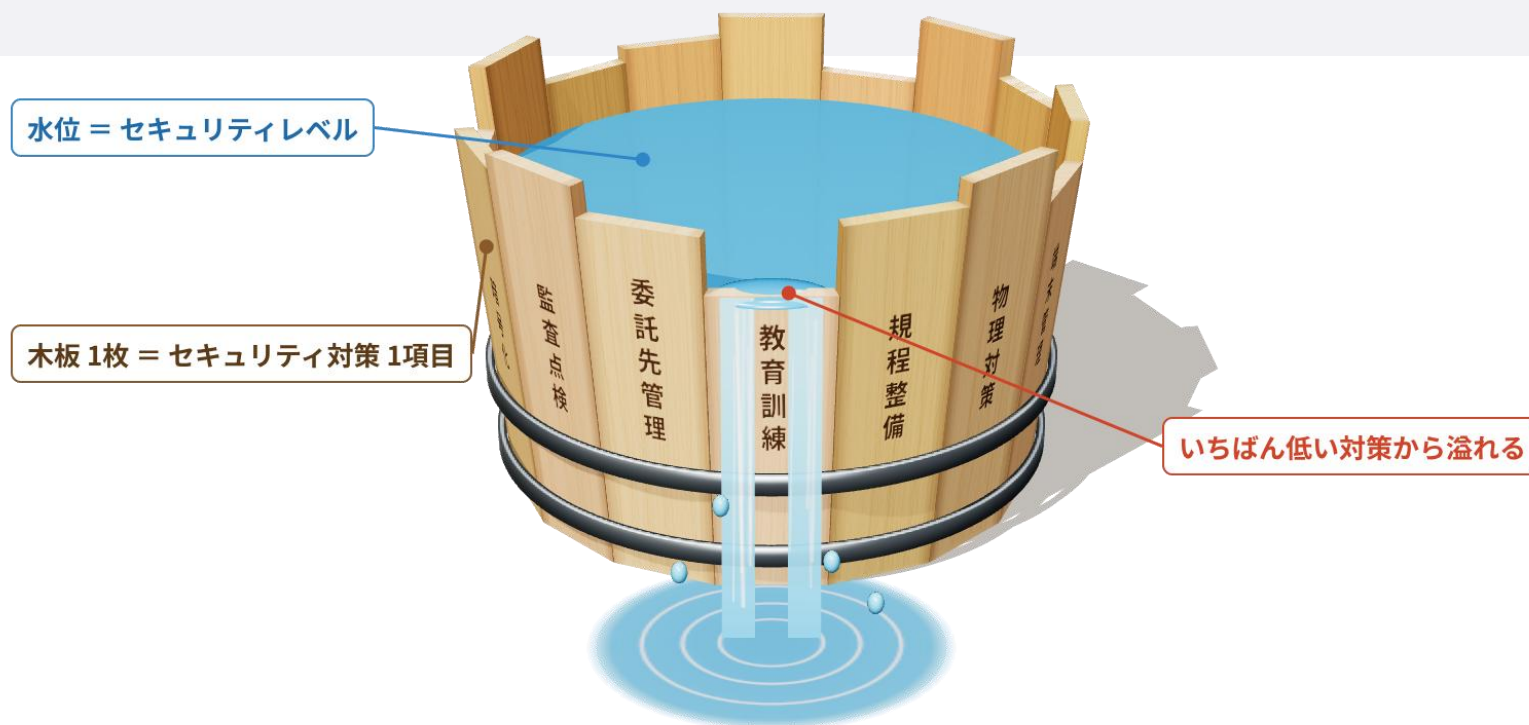
1. 自社診断の使い方が分かる
2. SECURITY ACTIONの位置づけが分かる
3. いまからやることが決まる



1. オープニング
2. 「5分でできる！情報セキュリティ自社診断」とは何か
3. 「セキュリティ対策自己宣言」のご紹介
4. ハクビーが前回の自社診断からどれだけ改善したのか
5. Q&A
6. クロージング

セキュリティは木桶

- あらゆる項目を満遍なく対策していく必要がある
→ どこか一つだけを伸ばしても効果は薄い



セキュリティ対策は一つを伸ばすのではなく、すべてを万遍なく実施しないと、セキュリティレベル（水位）が低くなる。



まずは現状把握

悩み

- 対策が必要なのは分かるが、何から手をつければいいのか分からない

まずは

- 健康診断と同じで、対策の前に「いま弱い部分」を知ることが第一歩
→ 効果的かつ簡単できる診断チェックリストが欲しい



ツールの概要

- 「5分でできる！情報セキュリティ自社診断」とは、独立行政法人情報処理推進機構（IPA）が中小企業向けに無料で提供しているチェックツール

概要

- IT担当者でなくてもできるほど手軽 → 経営者自身がタイムパフォーマンスよく把握できる
- 25問の「診断編」と、設問ごとの解説・対策を示した「解説編」で構成
- 設問は「基本的な対策」「従業員としての対策」「組織としての対策」の3区分

採点方法

- 「実施している」4点、「一部実施している」2点、「実施していない」0点、「わからない」はマイナス1点で、満点は100点 → わからないことが最大のリスク
- 合計49点以下は、いつ情報漏えいなどの事故が起きてもおかしくない状態



点数が低かったときに、経営者がまず判断すること

- 全部を一度にやらなくてOK → 優先度をつける

まずは

1. 次の点検日を決める
2. 「わからない」をなくす
3. 「実施していない」を「一部実施している」にする

次に

- 情報セキュリティ確保に取り組んでいることを、社外に示す



1. オープニング
2. 「5分でできる！情報セキュリティ自社診断」とは何か
3. 「セキュリティ対策自己宣言」のご紹介
4. ハクビーが前回の自社診断からどれだけ改善したのか
5. Q&A
6. クロージング

セキュリティ対策自己宣言（SECURITY ACTION）とは

- 中小企業が自ら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、段階に応じて「一つ星」「二つ星」のロゴを無料で使える
- IPAが推進している制度で、審査・認証ではない「自己宣言」
→ ハードルが低く、文字通りセキュリティ確保に取り組む意欲さえあれば始められる

★一つ星を宣言する

- 情報セキュリティ6か条に取り組むことを宣言する

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. バックアップを取ろう！
6. 脅威や攻撃の手口を知ろう！



画像出典：IPA「[SECURITY ACTION セキュリティ対策自己宣言](#)」

出典：IPA「[SECURITY ACTION『一つ星』を宣言する](#)」



セキュリティ対策自己宣言（SECURITY ACTION）とは

- 中小企業が自ら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、段階に応じて「一つ星」「二つ星」のロゴを無料で使える
- IPAが推進している制度で、審査・認証ではない「自己宣言」
→ ハードルが低く、文字通りセキュリティ確保に取り組む意欲さえあれば始められる

★★二つ星を宣言する

- 自社診断を実施し、基本方針を公開する
 - 「5分でできる！情報セキュリティ自社診断」を実施する
 - 情報セキュリティ基本方針を策定し、公開する



画像出典：IPA「[SECURITY ACTION セキュリティ対策自己宣言](#)」

出典：IPA「[SECURITY ACTION『二つ星』を宣言する](#)」



セキュリティ対策自己宣言（SECURITY ACTION）とは

- 中小企業が自ら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、段階に応じて「一つ星」「二つ星」のロゴを無料で使える
- IPAが推進している制度で、審査・認証ではない「自己宣言」
→ ハードルが低く、文字通りセキュリティ確保に取り組む意欲さえあれば宣言できる

申込の流れ

- SECURITY ACTION管理システムを利用
 - デジタル庁が提供する「GビズID」を利用できる。簡単に申請できる

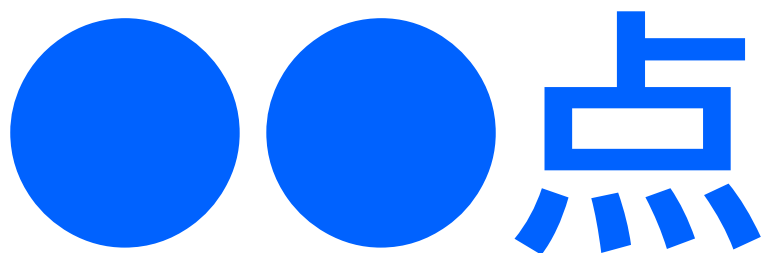


画像出典：IPA「[SECURITY ACTION管理システム](#)」



1. オープニング
2. 「5分でできる！情報セキュリティ自社診断」とは何か
3. 「セキュリティ対策自己宣言」のご紹介
4. **ハクビーが前回の自社診断からどれだけ改善したのか**
前回 2026年7月21日 → 今回 2026年10月15日
5. Q&A
6. クロージング

前回（2026年7月21日）



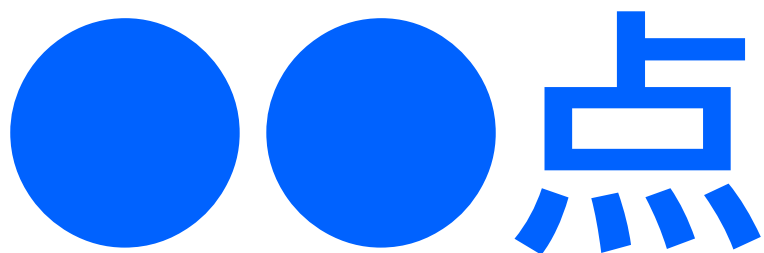
まず目指した●●点に届かず

●点の項目が、●つあった

創業直後の診断：登記は済んでいたが、業務開始前でオフィスもない状態



今回（2026年10月15日）



／ 前回より大幅に向上

+●●点。●点だった●項目のうち、●つが●点に

では、どのように向上させたのか？

※「●」の箇所は、当日のセミナーでのみ公開しています



このあとの見方：1項目ずつ

1

設問と解説

何を問われているか

2

前回の点数

なぜその点数だったか

3

今回の点数

何をして何が残ったか

採点：

4

実施

2

一部実施

0

未実施

／ わからない -1点



Part1 基本的対策 | No.1 脆弱性対策

パソコンやスマートフォンなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？

解説：OSやソフトウェアは常に最新の状態にする

- ・ 古いまま放置すると、問題点を悪用したウイルスに感染する
- ・ 修正プログラムを適用するか、最新版を使う

前回



(非公開)

今回



(非公開)

端末の一覧

端末名	OS	状態
パソコン1	Windows 11	✓最新
パソコン2	Windows 11	▲要更新
スマホ1	iOS	✓最新
スマホ2	iOS	✓最新

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part1 基本的対策 | No.2 ウイルス対策

パソコンやスマートフォン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は最新の状態にしていますか？

解説：ウイルス対策ソフトを導入し適切に利用する

- ID窃取・遠隔操作・ファイル暗号化を行うウイルスが増えている
- 定義ファイル（パターンファイル）は常に最新にする

前回



（非公開）

今回



（非公開）

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part1 基本的対策 | No.3 パスワード管理

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？

解説：強固なパスワードを使用する

- ・ 推測・解析や流出したパスワードの悪用で、不正ログインが増加
- ・ 「長く」「複雑に」「使い回さない」で強化する

前回



(非公開)

今回



(非公開)

🔒 パスワード保管庫

メール q7#Vm2!xLp

会計 Tz9\$kR4@wN

銀行 m!3Hs8&Qe6

タスク管理 Yb5^Lc1%Ud

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part1 基本的対策 | No.4 機器の設定

データの共有設定を必要な人に限定していますか？

解説：共有設定を見直す

- ・ 設定ミスで、無関係な人に情報を見られるトラブルが増えている
- ・ ウェブサービスや複合機を、無関係な人が使えない設定にする

前回



(非公開)

今回



(非公開)

保管場所を2つに分ける



機密情報

閲覧：管理者のみ



業務用の共有

閲覧：社員全員

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：[IPA「5分でできる！情報セキュリティ自社診断」](#)（[中小企業の情報セキュリティ対策ガイドライン第4版 付録3](#)）の診断内容・解説を引用



Part1 基本的対策 | No.5 バックアップ

故障や誤操作、ウイルス感染などによる重要情報の消失に備えて、定期的にバックアップを取得していますか？

解説：定期的にバックアップを取る

- ・ 故障・誤操作・ウイルス感染で、データが消えたり暗号化されたりする
- ・ 事業を続けられるよう、バックアップを取得しておく

前回



(非公開)

今回



(非公開)

事業継続計画書（抜粋）

■ランサムウェア感染・アカウントの不正利用

原因への対策を行ったうえで、バックアップから復元する。

■クラウドサービスの障害

端末に同期済みのファイルで作業を継続する。

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part1 基本的対策 | No.6 情報収集

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？

解説：脅威や攻撃の手口を知り、対策に活かす

- ・ 取引先を装うメールや偽サイトで、ID・パスワードを盗む手口が増えている
- ・ 最新の手口を知り、対策を取る

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：[IPA「5分でできる！情報セキュリティ自社診断」](#)（[中小企業の情報セキュリティ対策ガイドライン第4版 付録3](#)）の診断内容・解説を引用



Part2 従業員としての対策 | No.7 電子メール

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？

解説：身に覚えのない電子メールは疑ってみる

- ・ 添付ファイルやURLリンクからのウイルス感染が続いている
- ・ 身に覚えのないメールの添付やリンクは開かない

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：[IPA「5分でできる！情報セキュリティ自社診断」](#)（[中小企業の情報セキュリティ対策ガイドライン第4版 付録3](#)）の診断内容・解説を引用



Part2 従業員としての対策 | No.8 電子メール

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？

解説：宛先の送信ミスを防ぐ

- ・ 送り先の間違いやアドレスの誤開示で、情報漏えいが起きている
- ・ 送信前に宛先と、複数宛先の指定方法（BCCなど）を確認する

前回



(非公開)

今回



(非公開)

メール送信の流れ

 送信をクリック

 送信を保留

10～30秒

 宛先を再確認

誤りは取消

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part2 従業員としての対策 | No.9 電子メール

重要情報の受け渡しは、暗号化など安全な手段で行っていますか？

解説：重要情報を送信する時は保護する

- ・ 本文に書かず、パスワードで保護したファイルを添付する
- ・ パスワードはメール以外の手段で伝える

前回



(非公開)

今回



(非公開)

ファイル転送サービスで送る



※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」(中小企業の情報セキュリティ対策ガイドライン第4版 付録3)の診断内容・解説を引用



Part2 従業員としての対策 | No.10 無線LAN

無線LANを安全に使うため、適切な暗号化方式を設定していますか？

解説：無線LANの盗聴や無断使用を防ぐ

- ・ 設定が不十分だと、通信を盗み見られたり、不正接続で悪用されたりする
- ・ 盗聴や無断使用を防ぐセキュリティ設定をする

前回



(非公開)

今回



(非公開)

用語 WPA2・WPA3は無線LANの暗号化方式。
WPA3のほうがパスワード攻撃により強い

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：[IPA「5分でできる！情報セキュリティ自社診断」](#)（[中小企業の情報セキュリティ対策ガイドライン第4版 付録3](#)）の診断内容・解説を引用



Part2 従業員としての対策 | No.11 インターネット

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？

解説：インターネットを介したトラブルを防ぐ

- ・ 危険なサイトの閲覧や、SNSへの不適切な投稿で会社が被害を受ける
- ・ 業務での利用を制限する仕組みとルールで被害を防ぐ

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「[5分でできる！情報セキュリティ自社診断](#)」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part2 従業員としての対策 | No.12 情報管理

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？

解説：重要情報の放置を禁止する

- ・ 机上に放置した情報は、持ち去られたり盗み見られたりする
- ・ 保管場所を決め、使うときだけ取り出し、終わったら戻す

前回



(非公開)

今回



(非公開)

机に出っぱなしにしない

 使うときだけ出す

利用時

 伏せる・しまう

離席時

 書庫に入れて施錠

退社時

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part2 従業員としての対策 | No.13 情報管理

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？

解説：重要情報は安全な方法で持ち出す

- ・ 社外への持ち出しでは、盗難や紛失が起こりうる
- ・ パスワード設定や暗号化で、紛失しても読み取られないようにする

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」(中小企業の情報セキュリティ対策ガイドライン第4版 付録3)の診断内容・解説を引用



Part2 従業員としての対策 | No.14 情報管理

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？

解説：重要情報は復元できないように消去する

- そのまま捨てた書類や、削除しただけのデータから情報が漏れる
- シュレッダーや消去ソフトなど、媒体ごとに適切に処分する

前回



(非公開)

今回



(非公開)

重要情報の廃棄方法



書類・フィルム

細断



USB・HDD・CD

破壊・完全消去



単純なデータ削除

不可

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part2 従業員としての対策 | No.15 事務所の安全管理

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？

解説：機器を勝手に操作させない

- ・ 離席中やパスワードなしのパソコンは、不正に使われるおそれがある
- ・ 画面ロックなどで不正使用から守る

前回



(非公開)

今回



(非公開)

画面を見せない・開けさせない



自動ロック

5分以内



離席時にロック

Win+L



外出先の
スマホ・PC

のぞき見防止
フィルム

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」(中小企業の情報セキュリティ対策ガイドライン第4版 付録3)の診断内容・解説を引用



Part2 従業員としての対策 | No.16 事務所の安全管理

関係者以外の事務所への立ち入りを制限していますか？

解説：見知らぬ人には声をかける

- ・ 立ち入りを制限しないと、侵入されて情報を盗まれる
- ・ 重要な保管場所への無断立ち入りを防ぎ、施錠と退出を記録する

前回



(非公開)

今回



(非公開)

セキュリティ領域



入退室記録

日時	氏名	目的
—	—	—
—	—	—
—	—	—
—	—	—
—	—	—
—	—	—
—	—	—

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」(中小企業の情報セキュリティ対策ガイドライン第4版 付録3)の診断内容・解説を引用



Part2 従業員としての対策 | No.17 事務所の安全管理

退社時にノートPC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？

解説：機器・備品の盗難防止対策を行う

- ・ 持ち運びやすい機器や備品は、盗難・紛失の危険も高い
- ・ 使わないときは施錠できる引き出しなどに保管する

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：[IPA「5分でできる！情報セキュリティ自社診断」](#)（[中小企業の情報セキュリティ対策ガイドライン第4版 付録3](#)）の診断内容・解説を引用



Part3 組織としての対策 | No.18 ネットワーク管理

内部ネットワークを守るため、不正アクセス対策機能を設定していますか？

解説：外部から内部ネットワークへの不要な通信を遮断する

- ・ 内部ネットワークに侵入されると、悪用されるおそれがある
- ・ 外部からに加え、内部発の不要な通信も遮断する

前回

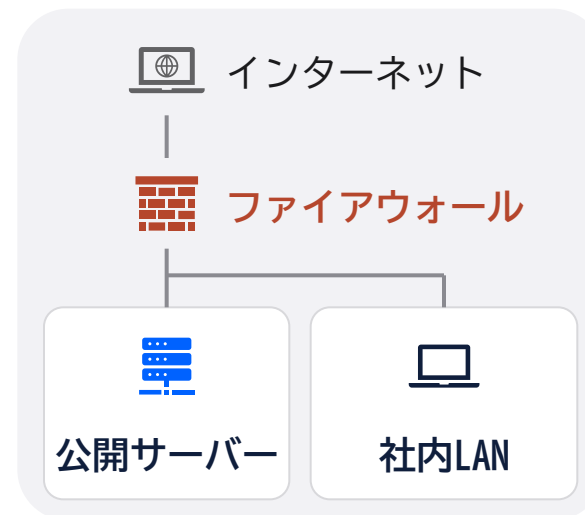


(非公開)

今回



(非公開)



※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」(中小企業の情報セキュリティ対策ガイドライン第4版 付録3)の診断内容・解説を引用



Part3 組織としての対策 | No.19 ウェブサイト管理

ウェブサイトで公開すべきでない情報を公開していませんか？

解説：ウェブサイトを安全に運用する

- ・ 公開前に、重要情報が含まれていないか確認する
- ・ 非公開情報や古い情報が残っていないか確認し、不要なものは削除する

前回



(非公開)

今回



(非公開)

置き場所を分けて守る

クラウド



問い合わせの個人情報

アクセス制限

自社（オンプレミス）



公開サーバー



開発環境

分離して保護

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part3 組織としての対策 | No. 20 従業員教育

従業員に情報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？

解説：従業員に情報セキュリティ教育を行う

- ・ 日常業務では、情報管理の意識が薄れがちになる
- ・ 繰り返し意識付けを行う

前回



(非公開)

今回



(非公開)

年間の教育計画

10 11 12 1 2 3 4 5 6

規程の読み合わせ	☒							☒		
勉強会			☒							☒
脅威情報の共有										
事故対応訓練						☒				
標的型メール訓練										☒

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part3 組織としての対策 | No. 21 私物機器の利用

私物の情報機器を業務で使う場合のセキュリティ対策を明確にしていますか？

解説：個人所有端末の業務での利用可否を決める

- ・ 私物の端末は管理が行き届かず、セキュリティを確保しにくい
- ・ 業務利用の可否とルールを定める

前回



(非公開)

今回



(非公開)

私物スマホの利用条件



許可制

台帳に記録



ウイルス対策

保護を有効化



アプリを限定

Teams・Outlook



保存しない

社外秘禁止

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part3 組織としての対策 | No. 22 取引先管理

重要情報を授受する取引先との契約書に、秘密保持条項を規定していますか？

解説：取引先に秘密保持を要請する

- ・ 「当然秘密にしてくれるだろう」という一方的な期待は禁物
- ・ 機密情報を渡すときは、機密として扱うことを明確にする

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：[IPA「5分でできる！情報セキュリティ自社診断」](#)（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part3 組織としての対策 | No. 23 外部サービスの利用

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？

解説：信頼できる外部サービスを使う

- ・ コスト優先で選ぶと、障害時に補償を受けられないことがある
- ・ 性能・信頼性・補償内容を吟味して選ぶ

前回



(非公開)

今回



(非公開)

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」(中小企業の情報セキュリティ対策ガイドライン第4版 付録3)の診断内容・解説を引用



Part3 組織としての対策 | No. 24 事故への備え

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？

解説：事故発生に備えて事前に準備する

- ・ 事故が起きてからでは冷静に対応できず、事態が深刻化しやすい
- ・ 「自社で起きたら」を想定し、誰がいつ何をするかを決めておく

前回



(非公開)

今回



(非公開)

事故への備え

🔍 リスク洗い出し 影響度で分類

👥 連絡先を整理 関係者を特定

📋 対応フロー作成 作業を明確化

🛡️ サイバー保険 損害に備える

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



Part3 組織としての対策 | No. 25 ルールの周知

情報セキュリティ対策（1～24など）をルール化し、従業員に明示していますか？

解説：情報セキュリティ対策をルール化する

- ・ 明文化されていないと、従業員は都度経営者の指示を仰ぐことになる
- ・ ルールを明文化し、いつでも見られるようにする

前回



（非公開）

今回



（非公開）

ルールの周知の流れ



規程を作成

✓完了



全条項を読み合わせ

✓完了

Tips 要約版があると伝えやすい

※「●」の箇所は、当日のセミナーでのみ公開しています

出典：IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）の診断内容・解説を引用



2名の会社が、何から手をつけたか

限られた人員と予算の中で、私たちが取った順番と考え方です

1 まず体制を決める

誰に責任があるのかを明確にした。技術的な対策よりも先に取り組んだ

2 次にルールを決める

IPAのひな形を参考にしつつ、自社の実態に合うよう一つずつ書き換えた

3 守れるルールにする

事故が起きたときの被害と、運用の手間・コストを天秤にかけて決めた

4 負担は最小限に

パスワード管理は信頼できるツールで、少人数なら無料で提供されるものを、ファイル転送は信頼できるツールのなかで安価なものを選んだ



結果：●●点 → ●●点（+●●点）

今回の合計

●● / 100点

評価区分：非公開

目標●●点の達成：●●
「わからない」の回答はなし

Part1
基本的対策
(24点満点)

Part2
従業員としての対策
(44点満点)

Part3
組織としての対策
(32点満点)

Part別の点数は
当日のみ公開

次は、4点にした項目を「継続運用する」こと

※「●」の箇所は、当日のセミナーでのみ公開しています



1. オープニング
2. 「5分でできる！情報セキュリティ自社診断」とは何か
3. 「セキュリティ対策自己宣言」のご紹介
4. ハクビーが前回の自社診断からどれだけ改善したのか
5. Q&A
6. クロージング

1. オープニング
2. 「5分でできる！情報セキュリティ自社診断」とは何か
3. 「セキュリティ対策自己宣言」のご紹介
4. ハクビーが前回の自社診断からどれだけ改善したのか
5. Q&A
6. クロージング

今日から始める3つ

1

自社診断をする

25問・約5分。「わからない」を残さず、いまの点数を知る

2

一つ星を宣言する

6か条に取り組むと決め、GビズIDで無料で申し込む

3

点検日を決める

3か月後など日付を先に決め、点数の変化を追う



法律と同じく、セキュリティも解釈や判断に迷う場面が多くあります。
特に「リスクを受容するか」の決断は、経営者にとって大きな負担です。

判断に迷われたときは、
ハクビーを思い出していただけましたら幸いです。

セキュリティ事業の詳細

[情報セキュリティ | ハクビー株式会社](https://www.hakubee.jp/services/security)
<https://www.hakubee.jp/services/security>

お問い合わせ（代表窓口）

contact@hakubee.jp



出典一覧

1. IPA「情報セキュリティ10大脅威 2026」

掲載スライド：6 | <https://www.ipa.go.jp/security/10threats/10threats2026.html>

2. 経済産業省「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（SCS評価制度）」

掲載スライド：6 | <https://www.meti.go.jp/policy/netsecurity/scs.html>

3. IPA「5分でできる！情報セキュリティ自社診断」（中小企業の情報セキュリティ対策ガイドライン第4版 付録3）

掲載スライド：11、21～45 | https://www.ipa.go.jp/security/guide/sme/ug65p90000019cbk-att/sme_guideline_v4.0_app_3.pdf

4. IPA「SECURITY ACTION セキュリティ対策自己宣言」

掲載スライド：14、15 | <https://www.ipa.go.jp/security/security-action/>

5. IPA「SECURITY ACTION『一つ星』を宣言する」

掲載スライド：14 | <https://www.ipa.go.jp/security/security-action/onestar/>

6. IPA「SECURITY ACTION『二つ星』を宣言する」

掲載スライド：15 | <https://www.ipa.go.jp/security/security-action/twostar/>

7. IPA「SECURITY ACTION管理システム」

掲載スライド：16 | <https://sme-security.ipa.go.jp/>





Hakubee