中小企業セキュリティ対策スタートガイド - よくある質問 Q&A 集

作成日: 2025-12-30

対象: 「3 日で学ぶ！中小企業セキュリティ対策スタートガイド」受講者向け

📋 目次

---

1. 講座全般について

Q1-1. この講座は本当に 3 日で完了できますか？

A: はい、完了できます。動画講座は合計約 3 時間（Day1: 約 50 分、Day2: 約 55 分、Day3: 約 1 時間 5 分）なので、1 日 1 時間の学習で 3 日間で視聴完了できます。ただし、実際に対策を実施する時間（Windows Update の設定、パスワード管理ツールの導入など）を含めると、**3 日間で合計 6〜10 時間程度**が目安です。

具体的な時間配分の例:

- **Day1（2〜3 時間）**: 動画視聴約 50 分＋診断チェックリスト記入 1〜2 時間
- **Day2（3〜5 時間）**: 動画視聴約 55 分＋実際の対策実施 2〜4 時間
- **Day3（2〜3 時間）**: 動画視聴約 1 時間 5 分＋報告資料作成 30 分〜1 時間

本業と兼任の方でも、**1 週間以内**に目安に完了できる内容です。

Q1-2. 私は IT 初心者で、専門知識が全くありません。それでも大丈夫ですか？

A: はい、大丈夫です。この講座は**「専門知識ゼロ」の方**を想定して設計しています。ただし、基本的な PC 操作（ファイルの保存、設定画面の操作など）ができる方を対象としています。実演デモを見ながら一緒に操作できるので、セキュリティ初心者の方でも安心して学べます。

この講座の特徴:

- ✅ 専門用語を使わず、初心者にも分かる言葉で説明
- ✅ 実演デモ付き（画面操作を見ながら一緒に設定できる）
- ✅ ステップバイステップのチェックリスト
- ✅ 「何から始めればいいか」を具体的に提示

実際、**Udemy 講座（全講座の累計受講者数は 2,000 人以上、本講座のベースとなった「情報セキュリティ 5 か条」講座は平均評価 4.2/5.0）**でも、「専門知識がなくても理解できた」という声を多くいただいています。

Q1-3. Mac や Linux を使っていますが、この講座は対応していますか？

A: この講座の実演デモは **Windows 環境**を前提としており、Mac/Linux ユーザーの方は一部の操作手順が異なります。基本的な考え方は OS 共通ですが、具体的な設定方法はご自身でお調べいただく必要があります。Windows 以外の環境での受講を検討される方は、その点をご了承ください。

Mac/Linux ユーザーの方へのアドバイス:

- ✅ **Day1（診断と 5 つの対策の理解）**: OS 関係なく、そのまま活用できます
- ✅ **Day2（実践的な対策）**:
  - OS 更新: macOS（システム環境設定の「ソフトウェアアップデート」機能） / 各 Linux ディストリビューションのパッケージ管理ツール（apt、yum、dnf など）
  - ウイルス対策: macOS（標準搭載の XProtect（自動マルウェア検出・削除）） / Linux（ClamAV（オープンソース・無料）等）
  - パスワード管理: 1Password、Bitwarden（いずれも Windows、macOS、Linux、iOS、Android に対応したクロスプラットフォーム対応製品）
- ✅ **Day3（報告と継続運用）**: OS 関係なく、そのまま活用できます

Mac/Linux 特有の操作については、質問サポートで可能な限りお答えいたします。

Q1-4. 会社の PC で実施する対策は、上司や経営陣の承認が必要ですか？

A: はい、**会社の PC に変更を加える対策については、事前に上司や経営陣の承認を得ることをおすすめします。**

承認が必要な対策の例:

- パスワード管理ツールの導入
- 自動更新の設定変更
- 共有設定の変更

承認を得る際のポイント（Day3 で詳しく解説）:

- ✅ 「なぜ必要か」をデータで示す（IPA の統計など）
- ✅ 「どんな対策をするか」を具体的に説明
- ✅ 「予算は不要（無料ツール使用）」であることを強調
- ✅ 経営陣向け報告資料テンプレートを活用

承認を得る方法については、Day3 のレクチャー11-3「経営陣向け報告資料の作り方」で詳しく解説しています。

Q1-5. 受講期間中に質問できますか？

A: はい、受講期間中（購入後 30 日間）は質問対応を行っています。

質問サポートの詳細:

- **質問回数: 原則 3 回まで**
- **回答時間**: 2 営業日以内（土日祝除く）
- **質問方法**: メールまたは専用フォーム
- **よくある質問**: まずは「FAQ 集（このドキュメント）」をご確認ください

質問フォーマット:

✓ どの動画の、どの部分について質問か
✓ 自分で調べたこと、試したこと
✓ 具体的に困っていること

さらに、専用コミュニティもあります:

- コミュニティでは、回数制限なく質問・相談が可能
- 講師が直接参加、原則 2 営業日以内に対応

- 講座内の 3 回は「集中的に解決したい重要な質問」に、コミュニティは「日々の小さな疑問や壁打ち」にご活用ください

サポート対応時間の補足:

- 「2 営業日以内」は土日祝日を除くカウント
- 年末年始（12/29-1/3）、お盆期間（8/13-8/15）は除外
- やむを得ず遅延する場合は、事前に案内

※より継続的なサポートが必要な場合は、実践プログラムまたは顧問契約をご検討ください。

Q1-6. 質問は 3 回までとのことですが、それ以上質問したい場合は？

A: 講座内の質問サポートは 3 回までですが、**専用コミュニティ（Discord）に参加していただければ、継続的に相談可能**です。

講座内サポート（3 回まで）：

- 目的: 集中的に解決したい重要な質問
- 期間: 購入後 30 日間
- 回答: 2 営業日以内

専用コミュニティ（継続的）：

- 目的: 日々の小さな疑問、壁打ち
- 期間: コミュニティ参加中（期間制限なし）
- 回答: 原則 2 営業日以内
- 回数: 制限なし

講師も直接参加しており、他の受講生との交流もできます。

あなたを一人にしません。

Q1-7. コミュニティでは 24 時間いつでも対応してもらえますか？

A: コミュニティでは**原則 2 営業日以内に対応**します。24 時間 365 日の即時対応を保証するものではありませんが、可能な限り継続的にサポートします。

サポート対応時間の詳細:

- 「2 営業日以内」は土日祝日を除くカウント
- 年末年始（12/29-1/3）、お盆期間（8/13-8/15）は除外
- 営業時間外や休日の質問は、翌営業日以降の対応
- やむを得ず遅延する場合は、事前に案内

2. 受講前の不安・疑問

Q2-1. この講座を受けるだけで、会社のセキュリティは完璧になりますか？

A: いいえ、「完璧」にはなりません。この講座は**「最低限の対策」**に特化しています。

この講座で達成できること:

- ✅ 中小企業に必要な「最低限の対策」を実施できる
- ✅ 「何もしていない状態」から「対策できている状態」へ
- ✅ 経営陣に説明できる、取引先に証明できる
- ✅ 情報セキュリティの基本対策が完了し、「何もしていない」という不安から解放されます

この講座では扱わない内容:

- ❌ 高度なセキュリティ技術（ペネトレーションテスト、脆弱性診断など）
- ❌ ISMS（ISO27001）やＰマークの取得方法
- ❌ 業界特有の規制への対応（HIPAA、金融庁ガイドラインなど）

セキュリティに「100%完璧」はありません。リスクを「許容範囲内」に抑えることが目標です。より高度な対策が必要な場合は、より深く学べる商品（実践プログラム）やトータルサポート商品（顧問契約）をご検討ください。

Q2-2. 予算が本当にゼロでも始められますか？

A: はい、始められます。この講座で紹介する対策は**無料ツールまたは OS 標準機能**を活用します。

無料で実施できる対策:

- ✅ Windows Update（標準機能）
- ✅ Windows セキュリティ（標準のウイルス対策）
- ✅ 無料パスワード管理ツール（Bitwarden、ブラウザ標準機能など）

- ✅ 共有設定の見直し（設定変更のみ）
- ✅ IPA の無料診断ツール

ただし、より強固な対策には投資が必要です:

- 有料のウイルス対策ソフト（年間数千円〜）
- クラウドバックアップサービス（月額数百円〜）
- 有料のパスワード管理ツール（年間数千円〜）

この講座では、「まず無料で始めて、効果を実感してから投資する」という段階的なアプローチを推奨しています。

また、この講座で学ぶ基本対策は無料で実施できますが、より本格的な体制構築や継続的なサポートが必要な場合は、有料の実践プログラムや顧問契約もご用意しています。

まずは無料で始めて、必要に応じて次のステップをご検討ください。

Q2-3. 高額なコンサルティングと何が違うのですか？

A: この講座は**「自分で実践する」ことを前提**としています。高額コンサルは「専門家が代わりにやってくれる」サービスです。

	この講座	**高額コンサル**
価格	低価格（買い切り型）	高価格（継続型）
対象	自分で学びたい人	専門家に任せたい人
内容	最低限の対策	包括的な対策
サポート	質問対応	継続的なサポート
スキルアップ	自分で判断できるようになる	依存する

この講座のメリット:

- ✅ 低価格
- ✅ 自分で実践できるようになる（スキルアップ）
- ✅ 長期的に自走できる力が身につく

高額コンサルのメリット:

- ✅ 専門家が代わりにやってくれる
- ✅ 高度な対策が可能
- ✅ 継続的なサポート

「まずは自分で実践してみたい」「予算が限られている」という方には、この講座が最適です。

Q2-4. 社内に反対する人がいます。どう説得すればいいですか？

A: 社内の抵抗は、セキュリティ担当者の共通の悩みです。Day3 のレクチャー11 で「経営陣への報告方法」を詳しく解説していますが、ここでもポイントをお伝えします。

説得のポイント:

1. データで示す

- IPA の統計: 中小企業のサイバー攻撃被害件数、被害額
- 「対策しないとこんなリスクがあります」と具体的に

2. ビジネスへの影響を説明

- システム停止 → 業務継続不可、売上損失
- 情報漏えい → 損害賠償、信用失墜、取引先からの契約解除

3. 予算が不要であることを強調

- 「無料ツールで始められます」
- 「まず試してみて、効果を確認してから投資を検討しましょう」

4. 取引先からの要求に対応

- 「大手企業がサプライチェーン管理を強化しています」
- 「取引先から『セキュリティ対策は？』と聞かれた時に答えられないリスク」

5. 経営陣向け報告資料テンプレートを活用

- Day3 で PowerPoint テンプレートを提供
- そのまま使えるので、説明資料の作成時間を短縮

Q2-5. 私の会社は従業員 10 名以下の小規模企業です。この講座は適用できますか？

A: はい、適用できます。むしろ**小規模企業こそ、この講座が最適**です。

小規模企業の特徴:

- ✅ 専任のセキュリティ担当者がいない
- ✅ 予算が限られている
- ✅ 時間がない（兼任が多い）
- ✅ 何から始めればいいか分からない

この講座が小規模企業に最適な理由:

- ✅ 無料ツールで始められる（予算不要）
- ✅ 月 10 時間以内で対応可能（兼任でも OK）
- ✅ 具体的なステップで迷わない
- ✅ 最低限の対策に絞っている（過剰な対策を避ける）

実際、この講座は「従業員 10〜50 名の中小企業」を想定して設計しています。

---

3. Day1: 診断と 5 つの対策の理解

Q3-1. IPA の「5 分でできる自社診断」を実施したら、ほとんどの項目で「実施していない」でした。どこから手をつければいいですか？

A: 「ほとんど実施していない」状態は、実は**多くの中小企業で共通の状況**です。焦らず、優先順位をつけて進めましょう。

優先順位のつけ方（Day1 レクチャー4-3 で詳しく解説）：

【最優先】基本的対策（5 か条）

1. OS・ソフトウェアの更新
2. ウイルス対策ソフト
3. パスワード強化
4. 共有設定の見直し
5. 脅威・攻撃手口の理解

【次に優先】従業員としての対策

- 重要情報の確認
- パスワードの管理
- メール利用時の注意
- USB 管理、SNS 利用時の注意

【その後】組織としての対策

- 情報セキュリティ基本方針の策定
- 従業員教育
- インシデント対応手順の整備

この講座では、最優先の「基本的対策（5 か条）」に絞って実装します。「すべてやろうとすると失敗する」ので、まずは最低限から始めましょう。

Q3-2. IPA の診断ツールは 25 項目もあって時間がかかります。もっと短時間でできる方法はありますか？

A: IPA の診断ツールは、**初回は時間がかかることがあります**。でも、初回だけしっかりやれば、2 回目以降は短時間で済みます。

時間短縮のコツ:

1. 初回は時間をかける

- 25 項目すべてに回答
- 分からない項目は「分からない」で OK
- まずは現状を正確に把握することが重要

2. 2 回目以降は短時間

- 前回の結果と比較しながら回答
- 変更があった項目のみ詳しく確認

3. 月次チェックリストを活用（Day3 で提供）

- 毎月チェックすべき項目に絞った簡易版
- 5〜10 分で完了

この講座では、初回の診断結果をもとに対策を進めます。時間をかける価値があるので、初回はしっかり診断してください。

Q3-3. 情報セキュリティ 5 か条は、IPA のガイドラインそのままですか？この講座独自の内容はありますか？

A: 5 か条の**基本的な枠組みは IPA のガイドライン**ですが、この講座では**実践的な内容を大幅に追加**しています。

IPA ガイドラインとの違い:

	IPA ガイドライン	この講座
説明	概念的・抽象的	具体的・実践的
実演デモ	なし	あり（画面操作あり）
ツール紹介	一般的な説明のみ	具体的なツール名と使い方
テンプレート	一部あり	6 種類提供

質問サポート	なし	あり

この講座の独自性:

- ✅ **実演デモ付き**: Windows Update の設定、パスワード管理ツールの導入など、画面操作を見ながら一緒に設定できる
- ✅ **具体的なツール名**: Bitwarden（パスワード管理）、Windows セキュリティ（ウイルス対策）など
- ✅ **30 年以上の実務経験**: 外資系食品会社での現場経験、Nimda ワーム感染事件などの実体験を反映

本講座のベースとなった「情報セキュリティ 5 か条」Udemy 講座（200 人以上が受講、平均評価 4.2/5.0）でも「分かりやすい」と好評です。

Q3-4. 経営陣が「セキュリティは後回しでいい」と言います。どう説得すればいいですか？

A: 経営陣の理解を得るのは難しいですが、**「リスクとビジネスへの影響」を具体的に示す**ことが重要です。Day3 で詳しく解説していますが、ここでもポイントをお伝えします。

説得のポイント:

1. サイバー攻撃の実態をデータで示す

- IPA の統計: 中小企業の被害件数（昨年比〇〇%増）
- ランサムウェア攻撃の被害額（平均数千万円）
- 「他人事ではない。次はうちかもしれない」

2. ビジネスへの影響を具体的に

- システム停止 → 業務継続不可、売上損失（1 日で〇〇万円）
- 情報漏えい → 損害賠償（1 人あたり〇〇円×顧客数）、信用失墜
- 取引先からの契約解除 → 売上減少

3. 取引先からの要求

- 大手企業がサプライチェーン管理を強化
- 「セキュリティ対策をしていないと、取引停止になるリスク」
- SECURITY ACTION（一つ星）の取得で証明できる

4. 予算が不要であることを強調

- 「まずは無料ツールで始められます」
- 「月 10 時間以内で対応可能です」
- 「高額なコンサルは不要です」

5. 経営陣向け報告資料テンプレートを活用

- Day3 で PowerPoint テンプレートを提供
- 「現状・リスク・対策・必要な支援」を 1 枚にまとめる

---

4. Day2: 実践的な対策の実施

Q4-1. Windows Update を自動更新にすると、業務中に再起動されて困ります。どうすればいいですか？

A: Windows 11 では、**再起動のタイミングをある程度コントロール**できます。

再起動のタイミングを調整する方法:

1. アクティブ時間を設定

- 設定 → Windows Update → アクティブ時間の変更
- 例: 9:00〜18:00 をアクティブ時間に設定
- この時間帯は自動再起動されない

2. 再起動のスケジュールを設定

- 設定 → Windows Update →「再起動のスケジュール」オプション
- Windows Update の適用後に再起動が必要な場合、具体的な日時を指定
- 業務に影響しない時間帯を指定

3. 一時的に更新を延期

- 設定 → Windows Update → 更新の一時停止
- 最大 35 日間、更新を延期できる（緊急時のみ）

ベストプラクティス:

- ✅ 月に 1 回、手動で更新をチェックして適用
- ✅ 重要な作業前は、事前に更新を完了させておく

Q4-2. 無料のウイルス対策ソフトで本当に大丈夫ですか？有料版との違いは何ですか？

A: Windows セキュリティ（標準機能）で、基本的な保護は十分です。ただし、有料版にはより高度な機能があります。

無料 vs 有料の比較:

機能	無料（Windows セキュリティ）	有料（例: Norton、Kaspersky）
ウイルススキャン	⭕ あり	⭕ あり
リアルタイム保護	⭕ あり	⭕ あり
ファイアウォール	⭕ あり（Windows 標準）	⭕ あり（より高度）
ランサムウェア対策	⭕ 基本的な対策	⭕ より高度な対策
フィッシング対策	⭕ あり	⭕ 高度な対策
VPN	❌ なし	⭕ あり（製品により）
パスワード管理	△ ブラウザ標準機能のみ	⭕ 専用ツールあり
サポート	❌ なし	⭕ あり
価格	無料	年間 4,000 円〜7,000 円程度

どちらを選ぶべきか:

無料版（Windows セキュリティ）がおすすめの場合:

- ✅ 予算が限られている
- ✅ ウェブ閲覧・メール利用が中心で、基本的な保護があれば十分
- ✅ まずは無料で始めて、効果を確認してから有料版を検討したい

有料版がおすすめの場合:

- ✅ 機密情報や個人情報を扱うので、より高度な保護が必要
- ✅ 頻繁にオンライン決済・金融取引を行う
- ✅ VPN やパスワード管理など、追加機能が欲しい

この講座では、まず無料の Windows セキュリティで始めることを推奨します。効果を実感してから、有料版への投資を検討してください。

Q4-3. パスワード管理ツール（Bitwarden）を会社の PC に導入するには、上司の承認が必要ですか？

A: はい、**会社の PC に新しいソフトウェアを導入する場合は、事前に上司や情シス担当者の承認を得ることをおすすめします。**

承認を得る際のポイント:

1. なぜ必要かを説明

- 「複雑なパスワードを安全に管理するため」
- 「パスワードの使い回しを防ぐため」
- 「不正ログインのリスクを減らすため」

2. Bitwarden の信頼性を示す

- オープンソース（コードが公開されている）
- 業界標準のセキュリティ（AES-256 ビット暗号化）
- 多くの企業・個人が利用（世界中で数百万ユーザー）

3. 無料であることを強調

- 「追加コストなしで導入できます」

4. ブラウザ標準機能の活用も提案

- もし専用ツールの導入が難しい場合、ブラウザ（Edge、Chrome）の標準パスワード管理機能も活用可能
- 承認が不要な場合が多い

承認が得られない場合の代替案:

- ✅ ブラウザ標準のパスワード管理機能を使う
- ✅ パスワードマネージャーは個人のスマホにのみ導入
- ✅ 会社の PC では、パスワードの複雑化とメモ管理（物理的に安全な場所に保管）

Q4-4. 共有設定を見直したら、業務に必要な共有フォルダまで使えなくなりました。どうすればいいですか？

A: 共有設定の見直しは慎重に進める必要があります。**「誰でもアクセスできる」設定を避けつつ、業務に必要な共有は維持**することが重要です。

共有設定の見直しのポイント:

1. 共有範囲を「関係者のみ」に限定

- ❌「誰でもアクセス可能」（Everyone、Guest）
- ⭕「特定のユーザーのみ」（社内の関係者）

2. アクセス権限を適切に設定

- **読み取り専用**: データを見るだけ（変更・削除は不可）
- **編集可能**: データの変更・追加が可能
- **フルコントロール**: すべての操作が可能（管理者のみ）

3. 業務に必要な共有は維持

- 営業部の共有フォルダ → 営業部のメンバーのみアクセス可能
- 経理部の共有フォルダ → 経理部のメンバーのみアクセス可能

トラブルシューティング:

- もし業務に必要な共有が使えなくなった場合:
  1. 共有フォルダを右クリック → プロパティ → 共有タブ → 詳細な共有
  2. アクセス許可で、必要なユーザー・グループを追加
  3. 適切な権限（読み取り or 変更）を設定

この設定が難しい場合は、質問サポートをご利用ください。

Q4-5. フィッシングメールと正規のメールの見分け方が分かりません。具体的なポイントを教えてください。

A: フィッシングメールは巧妙化していますが、**いくつかの特徴**があります。Day2 レクチャー10-2 で詳しく解説していますが、ここでも主なポイントをお伝えします。

フィッシングメールの特徴:

1. 送信者のメールアドレスを確認

- ❌ 送信者名は正規だが、メールアドレスが不審（例: amazon@secure-login.xyz）
- ⭕ 正規のメールアドレス（例: no-reply@amazon.co.jp）

2. 緊急性を煽る文言

- ❌ 「今すぐ対応しないとアカウントが停止されます」
- ❌ 「24 時間以内に確認してください」
- ⭕ 正規の企業は、緊急性を過度に煽らない

3. リンク先の URL を確認（クリックする前に）

- リンクにマウスカーソルを乗せる（クリックしない）
- URL が表示される
- ❌ 不審なドメイン（例: amazon-login.com、secure-amazon.net）
- ⭕ 正規のドメイン（例: amazon.co.jp）

4. 添付ファイルに注意

- ❌ 不審な添付ファイル（.exe、.zip、.js など）
- ⭕ 正規の企業は、重要な情報を添付ファイルで送らない

5. 日本語が不自然

- ❌ 機械翻訳のような不自然な日本語
- ❌ 誤字・脱字が多い

対処方法:

- ✅ 不審なメールのリンクはクリックしない
- ✅ 添付ファイルは開かない
- ✅ 公式サイトに直接アクセスして確認
- ✅ 不明な場合は、送信元企業に電話で確認

無料プレゼントのダウンロード資料「フィッシング詐欺の手口まとめ」も併せてご確認ください。

---

5. Day3: 経営陣への報告と継続運用

Q5-1. 経営陣向け報告資料を作成しましたが、専門用語が多くて経営陣に理解してもらえるか不安です。

A: 経営陣への報告では、**専門用語を避け、ビジネスへの影響を中心に説明**することが重要です。

報告資料作成のポイント:

1. 専門用語を使わない

- ❌「脆弱性」「パッチ適用」「多要素認証」
- ⭕「セキュリティ上の問題点」「システム更新」「二段階認証」

2. ビジネスへの影響を強調

- ❌「ランサムウェアのリスクがあります」
- ⭕「ランサムウェア攻撃を受けると、業務が停止し、1 日で〇〇万円の売上損失が発生します」

3. データで示す

- IPA の統計: 被害件数、被害額
- 「他人事ではない。次はうちかもしれない」

4. 3 つのメッセージに絞る

- ①現状（診断結果）
- ②実施した対策
- ③今後の計画と必要な支援

5. 報告資料テンプレートを活用

- Day3 で PowerPoint テンプレートを提供
- 記入例を参考に、自社の状況に合わせて修正

「経営陣が理解できる言葉で、ビジネスへの影響を中心に説明する」ことを意識してください。

Q5-2. SECURITY ACTION（一つ星）を宣言するメリットは何ですか？

A: SECURITY ACTION は、**自社のセキュリティ対策を対外的に証明できる制度**です。取引先への説明や補助金申請に活用できます。

SECURITY ACTION 一つ星のメリット:

1. 取引先への証明

- ロゴマークを名刺・Web サイト・提案資料に掲載できる
- 「セキュリティ対策をしている企業」として信頼を獲得
- 大手企業のサプライチェーン管理要件に対応

2. 補助金申請での加点

- IT 導入補助金、ものづくり補助金などで加点される場合がある
- 申請時の有利な材料になる

3. 社内の意識向上

- 宣言することで、経営陣・従業員のセキュリティ意識が向上
- 「対外的に宣言した以上、ちゃんとやらなきゃ」という責任感

4. 無料で簡単

- 登録は無料（IPA のサイトで 5 分で完了）
- IPA の「中小企業の情報セキュリティ対策ガイドライン」付録の「情報セキュリティ 5 か条」に取り組むことを宣言するだけ

5. 段階的にレベルアップ

- 一つ星 → 二つ星へとステップアップできる
- 二つ星は、より高度な対策（基本方針の策定など）を宣言

この講座を修了し、Day2 で学んだ対策に取り組む準備ができれば、SECURITY ACTION 一つ星を宣言できます。Day3 レクチャー12-2 で登録方法を解説しています。

※SECURITY ACTION は「情報セキュリティ 5 か条に取り組むことを宣言する制度」であり、すべての対策が完了している必要はありません。取り組む意思表示が重要です。

Q5-3. 月次チェックリストを毎月実施する時間がありません。もっと短時間でできる方法はありますか？

A: 月次チェックリストは、**数時間で完了できる内容**に絞っています。それでも難しい場合は、さらに優先順位をつけて短縮できます。

月次チェックリストの優先順位:

【最優先】毎月必ず実施（1 台あたり 5 分）

1. OS・ソフトウェアの更新確認（3 分）
   - Windows Update が最新か確認
   - 使用中のソフトウェア（Office、Adobe Reader など）が最新か確認
2. ウイルス対策ソフト確認（2 分）
   - Windows セキュリティで確認

【推奨】できれば毎月実施（1 台あたり 3 分+3 分）

3. パスワード見直し（3 分）
   - 長期間変更していないパスワードがないか確認
   - 使い回しパスワードがないか確認
4. 最新脅威の確認（3 分）
   - IPA のサイトで最新のセキュリティニュースをチェック

【低優先】四半期に 1 回でも OK（1 台あたり 5 分）

5. 共有設定確認（5 分）
   - 共有フォルダのアクセス権限が適切か確認

時間短縮のコツ:

- ✅ 毎月第 1 金曜日など、固定日を決める
- ✅ タイマーをセットして、集中して実施
- ✅ チェックリストをデスクトップに保存して、すぐにアクセス

Q5-4. インシデント（セキュリティ事故）が発生した場合、誰に連絡すればいいですか？

A: インシデント発生時の**連絡先リストを事前に整備**しておくことが重要です。Day3 レクチャー13-2 で詳しく解説していますが、ここでも主なポイントをお伝えします。

インシデント発生時の連絡先リスト:

1. 社内の連絡先

- **上司・経営陣**: ○○さん（内線○○、携帯○○）
- **情シス担当者**: ○○さん（内線○○、携帯○○）
- **全従業員**: 一斉メール、社内チャット

2. 社外の専門機関

- **IPA セキュリティセンター**: 電話窓口（IPA 情報セキュリティ安心相談窓口）
- **警察**: サイバー犯罪相談窓口（#9110 or 最寄りの警察署）
- **JPCERT/CC**: インシデント報告窓口（https://www.jpcert.or.jp/）

3. 取引先・顧客

- 情報漏えいの可能性がある場合、速やかに連絡

4. システムベンダー・サービス提供者

- 使用中のクラウドサービス、ソフトウェアのサポート窓口

インシデント対応の初動 3 ステップ:

1. **被害の拡大を防ぐ**: ネットワークから切断、該当 PC をシャットダウン

2. **証拠を保全する**: ログ、メール、スクリーンショットを保存
3. **専門家に連絡する**: 上記の連絡先リストに基づいて連絡

ダウンロード資料「インシデント対応マニュアル」に、連絡先リストのテンプレートがあります。自社の情報を記入して、すぐにアクセスできる場所に保管してください。

Q5-5. この講座を修了したら、次に何をすればいいですか？

A: この講座修了後、**3 つの選択肢**があります。

選択肢 1: 現状維持（月次チェックリストで継続運用）

- ✅ 月次チェックリストに沿って、毎月数時間のメンテナンス
- ✅ 最新のセキュリティニュースをチェック
- ✅ 年に 1 回、IPA の診断ツールで再診断

おすすめの人:

- 「最低限の対策ができていれば十分」
- 「本業に集中したい」

選択肢 2: より深く学べる商品（実践プログラム）で本格的な体制構築

プラン	期間	内容
ベーシック	3 ヶ月	現状把握＋社内ルール整備＋報告と定着化
スタンダード	6 ヶ月	ベーシック＋リスク管理＋取引先セキュリティ対応など
プレミアム	12 ヶ月	スタンダード＋高度な脅威対策＋事業継続計画など

※長期プランほど学べる内容が充実します。各月ごとに新しいテーマを学び、段階的にセキュリティ体制を構築していきます。

おすすめの人:

- 「もっと本格的な対策をしたい」
- 「SECURITY ACTION 二つ星を取得したい」
- 「継続的なサポートが欲しい」

本講座受講者限定特典:

- ✅ 初月無料

選択肢 3: トータルサポート商品（顧問契約）で専門家のサポートを受ける

プラン	内容
顧問ライト	・月 1 回のオンライン相談（60 分） ・メール・チャット質問対応 ・最新セキュリティ情報の月次配信 ・年 2 回のセキュリティチェック
顧問スタンダード	**顧問ライトの内容に加え：** ・月 1 回の個別コンサル（90 分） ・経営陣向けセキュリティレポート作成・提出（月次） ・内部監査支援（年 2 回） ・従業員向けセキュリティ研修（年 1 回） ・情報セキュリティ規程・マニュアルのレビュー ・ISMS（ISO27001）取得支援 ・インシデント発生時の助言・支援（営業時間内対応） ・年間セキュリティ計画の策定支援

※緊急時の即時対応が必要な場合は、別途セキュリティインシデント対応の専門サービスをご検討ください。

おすすめの人:

- 「専門家に継続的にサポートしてほしい」
- 「ISMS 取得を検討している」
- 「包括的な対策が必要」

次のステップの選び方:

【フローチャート】

最低限の対策で十分？
↓ はい
選択肢 1：現状維持（月次チェックリストで継続運用）

↓ いいえ
もっと本格的な体制を構築したい？
↓ はい
選択肢 2：より深く学べる商品（実践プログラム）

↓ いいえ
専門家のサポートが必要？
↓ はい
選択肢 3：トータルサポート商品（顧問契約）

---

6. 受講後のサポートについて

Q6-1. どんな質問がサポート範囲外ですか？

A: 以下のような質問は、サポート範囲外となります。

サポート範囲外の例:

- ❌ **個別企業のネットワーク構成の診断・設計**
  - 例:「当社のネットワーク図を見て、セキュリティ上の問題点を指摘してほしい」
- ❌ **講座で扱っていない有料ツール・サービスの選定**
  - 例:「有料セキュリティソフト A と B どちらがいいか教えてほしい」
- ❌ **ハードウェア障害のトラブルシューティング**
  - 例:「パソコンが起動しない、修理方法を教えてほしい」
- ❌ **実際のセキュリティインシデント対応の代行**
  - 例:「ウイルスに感染した、駆除作業を代行してほしい」
- ❌ **業界特有の規制への個別対応**
  - 例:「医療業界の HIPAA 対応について、当社の状況を診断してほしい」

サポート範囲内の例:

- ✅ **講座内容の実装方法に関する質問**
  - 例:「Day2 レクチャー6-2 の Windows Update の設定がうまくいかない」
- ✅ **講座で紹介したツールの使い方**
  - 例:「Bitwarden のパスワード保存方法が分からない」
- ✅ **「こんな時どうする？」という一般的な相談**
  - 例:「フィッシングメールを受信した、どう対応すればいいか」
- ✅ **講座内容の理解に関する質問**
  - 例:「情報セキュリティ 5 か条の『共有設定の見直し』の意味が分からない」

より高度なサポートが必要な場合:

- 個別企業の診断・設計が必要な場合 → 実践プログラムまたは顧問契約をご検討ください

- 実際のインシデント対応が必要な場合 → 専門のセキュリティ会社への依頼をおすすめします

Q6-2. 受講期間（30 日間）が終了した後も質問できますか？

A: 受講期間（購入後 30 日間）終了後は、**個別の質問対応は終了**します。ただし、**専用コミュニティは期間終了後も継続して利用可能**です。

受講期間終了後のサポートオプション:

1. 専用コミュニティ（継続利用可能）

- 講座受講後も引き続き参加可能
- 質問・相談を回数制限なく投稿できる
- 講師が直接参加、原則 2 営業日以内に対応
- **一人で悩まない場所として、ずっと利用できます**

2. FAQ 集（このドキュメント）を活用

- よくある質問をまとめているので、まずはこちらをご確認ください
- 無料で永久にアクセス可能

3. より深く学べる商品（実践プログラム）に進む

- より体系的な継続サポート
- グループ Q&A セッション（月 1〜2 回）
- 専用コミュニティでの優先サポート

4. トータルサポート商品（顧問契約）で専門サポート

- 個別の継続サポート
- メール・チャットでの質問対応（無制限）
- 月 1 回の個別コンサル

5. メールマガジンに登録

- 最新のセキュリティニュース、実践的な Tips を配信
- 無料

Q6-3. 講座の内容が更新された場合、追加料金なしで最新版にアクセスできますか？

A: はい、**追加料金なしで最新版にアクセス**できます。

更新内容の例:

- 重要なセキュリティ脅威への対応方法
- 新しいツールの紹介
- FAQ 集の追加・改訂
- 実演デモの改善

更新頻度:

- **随時更新**（重要な変更や新しい脅威に対応するため、必要に応じて更新します）
- すべての更新について、登録メールアドレスに通知

更新対象:

- 動画講座、ダウンロード資料、FAQ 集すべてが対象
- 購入後は永続的に最新版にアクセス可能

※ただし、セキュリティ環境は日々変化するため、すべての脅威への即時対応を保証するものではありません。より包括的な対応が必要な場合は、実践プログラムまたは顧問契約をご検討ください。

---

7. 次のステップについて

Q7-1. より深く学べる商品（実践プログラム）とこの講座の違いは何ですか？

A: この講座は**「最低限の対策」**に特化していますが、実践プログラムは**「本格的な体制構築」**を目指します。

	この講座	実践プログラム
期間	3 日間（動画約 3 時間）	3〜12 ヶ月
内容	最低限の 5 つの対策	本格的な体制構築（段階的）
サポート	質問対応	継続的なサポート
目標	不安から解放される	本格的なセキュリティ体制
成果物	基本的な対策完了	基本方針策定、規程整備、SECURITY ACTION 二つ星など

実践プログラムで学べる内容:

- リスクアセスメントの実施
- 情報セキュリティ基本方針の策定
- 情報セキュリティ関連規程の整備
- SECURITY ACTION 二つ星の取得
- 従業員向け教育の実施
- インシデント対応手順の整備
- 事業継続計画（BCP）の策定

本講座受講者限定特典: 初月無料

Q7-2. ISMS（ISO27001）の取得を検討していますが、この講座は役立ちますか？

A: この講座は **ISMS 取得の「最初の一歩」**として役立ちますが、ISMS 取得には**より高度な対策と文書化**が必要です。

この講座で ISMS 取得に役立つ内容:

- ✅ セキュリティ現状診断（ISMS の「現状分析」に該当）
- ✅ 基本的な対策（ISMS の「管理策」の一部に該当）
- ✅ 経営陣への報告（ISMS の「トップマネジメントの関与」に該当）

ISMS 取得に追加で必要な内容:

- ❌ 詳細なリスクアセスメント
- ❌ 情報セキュリティ基本方針・関連規程の策定
- ❌ 内部監査の実施
- ❌ マネジメントレビュー
- ❌ 認証機関の審査対応

ISMS 取得を目指す場合の推奨ステップ:

1. **この講座で基礎を固める**（3 日間）
2. **実践プログラム（プレミアム 12 ヶ月）で文書化・体制構築**
3. **顧問契約で ISMS 取得支援**
    - 顧問スタンダードに「ISMS 取得支援」が含まれる

Q7-3. 他の Udemy 講座との違いは何ですか？どの講座から始めればいいですか？

A: 講師（佐藤豊史）は **Udemy 講師として全 20 講座以上を提供**しており、全講座の累計受講者数は 2,000 人以上です。この講座は、それらの実証済みコンテンツをベースに、さらに実践的に進化させたものです。

Udemy 講座全講座との関係:

この講座（スタートガイド）の位置づけ:

- ✅ **Udemy 講座のベストセレクション＋実演デモ＋テンプレート**
- ✅ 特に本講座のベースとなった「情報セキュリティ 5 か条」講座（200 人以上が受講、平均評価 4.2/5.0）のエッセンスを凝縮

- ✅ より実践的（実演デモ、質問サポート、テンプレート 6 種類）

どの講座から始めるべきか:

初心者の方:

- ✅ **この講座（スタートガイド）**から始めるのが最適
- 理由: Udemy 講座「情報セキュリティ 5 か条」などのエッセンスを 3 日間で学べる、実演デモ付き、質問サポート付き

特定のトピックを深く学びたい方:

- Udemy 講座の個別トピック（ウェブサイト、EC、テレワーク、クラウドなど）
- 例:「ウェブサイトセキュリティ」、「EC サイトセキュリティ」

資格取得を目指す方:

- 「情報セキュリティマネジメント試験受験編」ブログ
- 「IT パスポート試験受験編」ブログ及び Udemy 講座

この講座修了後、さらに深く学びたい方:

- 実践プログラムで体系的に学ぶ
- または、Udemy 講座の個別トピックで特定分野を深掘り

Q7-4. 生成 AI 関連のセキュリティ対策も学びたいのですが、この講座で扱っていますか？

A: この講座では、**生成 AI のセキュリティ対策は扱っていません**。ただし、講師（佐藤豊史）は Udemy 講座で生成 AI 関連の講座を提供しています。

生成 AI 関連の Udemy 講座:

1. 生成 AI 利用ガイドライン策定

- 自社向け生成 AI ガイドラインの策定方法
- ChatGPT、Copilot などの安全な利用方法

2. 生成 AI 活用時のリスクと予防策

- 生成 AI 活用時のリスク（情報漏えい、著作権侵害など）
- 予防策の具体的な方法

3. AI と情報セキュリティの基礎

- AI とセキュリティの基礎知識、リスク管理

おすすめの学習順序:

1. **この講座（スタートガイド）で基礎を固める**
2. **Udemy「生成 AI 利用ガイドライン策定」で生成 AI 対応**

または

- **実践プログラム（プレミアム 12 ヶ月）**: 最新技術対応（生成 AI 含む）のコンテンツが含まれる

Q7-5. 私の会社は医療業界（または金融業界）です。業界特有の規制にも対応していますか？

A: この講座は**業界横断的な「基本的対策」**を扱っており、**業界特有の規制（HIPAA、金融庁ガイドラインなど）には対応していません。**

この講座で学べる内容（業界共通）:

- ✅ OS・ソフトウェアの更新
- ✅ ウイルス対策
- ✅ パスワード管理
- ✅ 共有設定の見直し
- ✅ 脅威・攻撃手口の理解

この講座では扱わない内容（業界特有）:

- ❌ 医療業界: HIPAA、個人情報保護法（医療分野の特則）、医療情報システムの安全管理ガイドライン

- ❌ 金融業界: 金融庁ガイドライン、FISC 安全対策基準
- ❌ 製造業: サプライチェーンセキュリティ、制御システムのセキュリティ

業界特有の規制への対応が必要な場合:

選択肢 1: 顧問契約

- 顧問スタンダードで、業界特有の規制への対応をサポート
- 専門家が個別にアドバイス

選択肢 2: 業界特有の専門コンサルタントに依頼

- この講座で基礎を固めた後、業界特有の専門家に相談

まずは、この講座で基本的対策を完了させてから、業界特有の対応を進めることをおすすめします。

📞 その他の質問

この FAQ で解決しない質問がある場合

1. まずは FAQ を再確認

- このドキュメントの目次から、関連する項目を探してください

2. 質問サポートを利用（受講期間中）

- メールまたは専用フォームで質問
- 回答時間: 2 営業日以内（土日祝除く）

3. 実践プログラム・顧問契約を検討

- より継続的なサポートが必要な場合

4. お問い合わせ

- Email: toyoshi.satoh@toyoshisatoh.jp
- 件名に「スタートガイド FAQ」と記載してください

📝 最後に

この講座を受講いただき、ありがとうございます。

あなたはもう「何をすればいいか分からない」状態ではありません。

3 日間で学んだ知識と対策を、ぜひ実践してください。そうすれば、『何もしていない』という不安から解放され、対策が取れている状態になります。

もし、さらに深く学びたい、継続的なサポートが欲しいと思ったら、次のステップ（実践プログラム・顧問契約）でお待ちしています。

あなたは一人ではありません。一緒に進めましょう。

講師: 佐藤豊史（さとうとよし）

情報処理安全確保支援士（国家資格）

サトウトヨシ・コンサルティング

この FAQ 集は随時更新されます。最新版はダウンロードページでご確認ください。

価格情報については、公式サイト（https://toyoshisatoh.com）またはお問い合わせください。

最終更新日: 2026-1-04