

小さな会社のセキュリティ対策

〈2026年版〉パスワード・多要素認証・バックアップ・社内規程・BCPの最低限

— IT担当がいなくても、今日から始められる「組織の守り」 —

- ✓ 優先順位つき「最初の3か月」の対策ロードマップ
- ✓ パスワード管理と多要素認証を、社内に定着させる手順
- ✓ ランサムウェアにも備えるバックアップと、1枚の社内ルール
- ✓ 事故が起きたときの初動と、止まらない会社のためのBCP

発行：Harmonic Society株式会社

（千葉市 | ホームページ制作・AI導入支援・IT顧問）

はじめに — 「うちは狙われない」から一歩進むために

「うちのような小さな会社が、わざわざ狙われることはないだろう」。千葉の経営者の方から、よく伺う言葉です。しかし現在のサイバー攻撃の多くは、相手を選ばず、弱いところを機械的に探して入り込む「無差別型」です。規模が小さいことは、安全の理由になりません。

一方で、過度に怖がる必要もありません。被害の入口の多くは、**使い回されたパスワード、更新されていないパソコン、取っていない（または戻せない）バックアップ、そして「誰に報告すればいいか分からない」状態**です。どれも高価な製品ではなく、設定とルールで塞げるものばかりです。

本書は、当社ブログの情報セキュリティ関連記事18本を、専任のIT担当がいない会社の経営者・総務の方が「組織として最低限やること」を順番に実行できるよう、一冊に再構成したものです。サーバー構築やクラウドの細かな設定には踏み込みません。代わりに、社長が決め、社員に頼み、業者に確認すればよいことを具体的に書きました。

読み終えたとき、次の3つを自社の言葉で説明できることがゴールです。

1. 自社で「最初の3か月」に何をするか
2. 事故が起きたら、誰が、誰に、何を連絡するか
3. データが消えても、どこから、どれくらいで戻せるか

巻末には、自己診断チェックリスト20、インシデント初動の連絡表、1枚で作れる社内ルールのひな形を付けています。まずはチェックリストから眺めていただいても構いません。

本書の情報について：本書の内容は2026年9月時点の情報に基づきます。法制度・公的な枠組み・各サービスの機能や料金は変更される場合があります。最終判断の際は、各機関・各社の最新情報をご確認ください。本書は一般的な考え方を示すもので、特定の効果を保証するものではありません。

第1章 まず知っておくこと — 小さな会社のリスクと「最低限」の考え方

1-1. 小さな会社が被害に遭う3つの経路

攻撃者の側から見ると、中小企業には狙いやすい理由があります。

- ・ **対策が手薄になりやすい**：専任担当がおらず、「初期設定のまま」「簡単なパスワード」「更新していない」が残りがちです
- ・ **取引先への踏み台になる**：大手企業と取引のある会社へ侵入し、そこを足がかりに取引先へ攻撃を広げる「サプライチェーン攻撃」があります。自社の被害が、取引先の被害に直結します
- ・ **止まると困る業務がある**：ランサムウェア（データを暗号化して使えなくし、元に戻す代わりに金銭を要求する不正プログラム）は、戻せるバックアップがない会社ほど大きな打撃を受けます

1-2. 被害は「お金」だけではない

情報セキュリティの事故が起きると、影響は4つの方向に広がります。

図表1：情報セキュリティ事故の影響

影響	具体的な内容
業務停止	パソコンやシステムが使えず、受注・請求・連絡が数日～数週間止まる
金銭的損失	復旧・調査の費用、売上の減少、場合によっては損害賠償
信用の低下	顧客・取引先からの信頼を失い、取引の見直しにつながる
法的な責任	個人情報の漏えい時には、報告や本人への通知の義務がある（第5章）

1-3. 目指すのは「100点」ではなく「最低限を全員で」

大企業と同じ体制を作る必要はありません。本書が目指すのは、**高価な製品に頼らず、設定とルールで防げる事故を確実に防ぐこと**、そして**防げなかったときに早く気づき、早く戻せること**です。60点のルールを全員が守るほうが、100点の規程を作ろうとして何も決まらないより、はるかに会社を守ります。

公的な目安としては、IPA（独立行政法人情報処理推進機構）が「中小企業の情報セキュリティ対策ガイドライン」を公開しており、中小企業が自ら対策に取り組むことを宣言する「SECURITY ACTION」という制度も運営しています。本書で基本を押さえたうえで、自社の現状を確かめる材料として活用するとよいでしょう。

第1章 まず知っておくこと（続き） — 守るものを決め、順番を決める

1-4. 最初の作業は「情報資産の棚卸し」

対策の前に、会社で「どんな情報が、どこにあり、誰が触れるか」を表計算ソフト1枚にまとめます。対象は**顧客情報**（氏名・住所・問い合わせ内容）、**従業員情報**（給与・マイナンバー）、**お金の情報**（会計・ネットバンキング）、**営業秘密**（顧客リスト・価格表・図面）などです。

あわせて、業務で使っているサービス（メール、クラウド会計、ネットバンキング、SNS、ホームページやドメインの管理画面など）のアカウントも書き出します。この作業だけで「誰も使っていないアカウント」「退職者が知っているパスワード」が見つかることがよくあります。

重要度は3段階で十分です。迷ったら「**新聞に載ったら困るか**」で判断します。

図表2：情報の重要度の3段階

レベル	例	扱いの目安
機密	顧客の個人情報、財務、営業秘密	触れる人を限定、持ち出し原則禁止
社外秘	社内マニュアル、取引先リスト	社内に限って共有
公開	会社案内、製品カタログ	制限なし

1-5. 最初の3か月のロードマップ

対策の大半は無料か低コストです。次の順に進めると、効果の大きいものから手が打てます。

図表3：対策の優先順位

時期	やること	本書の章
今日	重要アカウントのパスワード見直しと多要素認証	第2章
1週間以内	OS・ソフトの自動更新、バックアップの開始	第3・4章
1か月以内	パスワード管理ツール導入、端末・Wi-Fiの見直し	第2・3章
3か月以内	社内ルール1枚、復元テスト、初動連絡表とBCP	第4～6章

第2章 パスワードの管理 — 「覚えない」仕組みに切り替える

2-1. いちばん多い入口は「使い回し」

覚えやすさを優先して、複数のサービスで同じパスワードを使っている会社は少なくありません。どこか1つのサービスからパスワードが漏れると、同じ組み合わせで他のサービスにも次々とログインを試されます（「パスワードリスト攻撃」と呼ばれます）。クラウド会計とネットバンキングに同じパスワードを使っていれば、被害はお金に直結します。

「一覧をExcelで全員共有」「モニターに付箋」「会社名＋年号のような推測しやすいもの」「退職者が知ったまま」——こうした状態は、今日から解消の対象です。

2-2. 良いパスワードの条件は「長く、使い回さない」

図表4：これからのパスワードの考え方

項目	推奨
長さ	最低12文字以上。重要なアカウントは16文字以上や、単語を組み合わせた長い文（パスフレーズ）も有効
使い回し	サービスごとに必ず別にする（最重要ルール）
中身	名前・誕生日・社名・辞書の単語そのままは避ける
定期変更	漏えいの疑いがあるときや退職者が出たときに、すぐ変更する。理由のない定期変更は必須ではない
共有	原則として個人ごとのアカウント。やむを得ない共有はツールで権限管理する

「3か月ごとに変更」というルールを見かけることがありますが、近年の国内外の指針では、**定期的な変更を強制するより、長く使い回さないパスワードにし、漏えい時にすぐ変える**ほうが重視されています。頻繁な変更を求めると、かえって「末尾の数字だけ変える」ような弱いパスワードが増えるためです。

とはいえ、長くてバラバラのパスワードを全部覚えるのは不可能です。そこで覚える作業そのものをやめ、**パスワード管理ツール**に任せます（次ページ）。

第2章 パスワードの管理（続き） — パスワード管理ツールを入れる

2-3. パスワード管理ツールとは

パスワード管理ツールは、複雑なパスワードを暗号化して保管し、ログイン時に自動入力してくれるサービスです。利用者は、ツールを開くための「マスターパスワード」を1つ覚えるだけで済みます。**法人向けプラン**なら、管理者が「誰がどのパスワードを使えるか」を一元管理でき、退職者のアクセスもすぐに止められます。費用は1ユーザーあたり月数百円程度からが一般的で、投資対効果の高い対策です（2026年9月時点）。

2-4. 導入の4ステップ

1. **棚卸し**：第1章で作ったアカウント一覧をもとに、管理すべきパスワードを洗い出す
2. **法人プランの契約**：管理者機能のある法人向けプランを選び、まず経営者と総務・経理から使い始める
3. **重要なものから登録**：ネットバンキング、会計、メールなど、漏れたときの被害が大きいものを優先して登録する
4. **使い回しの解消**：ツールの自動生成機能で、使い回していたパスワードを1つずつ固有のものに置き換える

一度に全部を移そうとすると挫折します。1週間に数件ずつでも、重要なものから順に進めれば十分です。

2-5. 定着させる3つのルール

- ・ **新しいサービスを契約したら、必ずツールに登録する**（登録していないアカウントを作らない）
- ・ **共有アカウントは部署やチーム単位で権限を分ける**（全員に全部を見せない）
- ・ **退職・異動の日に、その人が使えたパスワードを変更し、ツールの権限を外す**

2-6. マスターパスワードの扱い

マスターパスワードを忘れると、保管したすべてにアクセスできなくなります。長いパスフレーズにし、多要素認証（次ページ）も必ず設定します。万一に備え、経営者の分は紙に書いて金庫など鍵のかかる場所に保管する方法もあります。管理者を1人だけにせず、**緊急時に回復できる人を2人**決めておくことで安心です。

第2章 パスワードの管理（続き） — 多要素認証で「漏れても入られない」

2-7. 多要素認証とは

多要素認証（MFA）は、ログイン時に**種類の違う2つ以上の確認**を求める仕組みです。確認の種類は「知っているもの（パスワード）」「持っているもの（スマホ・専用キー）」「本人の体（指紋・顔）」の3つ。銀行ATMが「カード（持っているもの）」と「暗証番号（知っているもの）」を組み合わせているのと同じ考え方です。パスワードが漏れても、スマホがなければ入れません。Microsoftは、多要素認証でアカウント乗っ取り攻撃の99.9%を防げるとする調査を公表しています。

サービスによっては「2段階認証」と呼ばれる設定も、本書では同じものとして扱います。

図表5：主な確認方法の比較

方法	安全性	手軽さ	向いている使い方
SMS（ショートメール）のコード	中	高い	他の方法が使えないサービスの最低限
認証アプリ（ワンタイムコード）	高	中	社員全員の標準。無料で使える
パスキー・セキュリティキー	最高	中～高	経営者・管理者・お金に関わるアカウント

SMSは手軽ですが、電話番号を乗っ取る手口（SIMスワップ）があるため、選べるなら認証アプリを使います。パスキーは、パスワードの代わりにスマホやパソコンの指紋・顔認証などでログインする新しい方式で、偽サイトに入力させる詐欺に強いのが特長です。対応するサービスが増えています。

2-8. 設定する順番

1. **メール**（Google Workspace、Microsoft 365など）：乗っ取られると他のサービスのパスワード再設定まで奪われるため最優先
2. **お金**：ネットバンキング、クラウド会計、決済サービス
3. **会社の顔**：ドメイン・サーバー・ホームページの管理画面、SNSアカウント
4. **顧客情報**：顧客管理・予約・EC などのサービス
5. **全社員へ展開**：まず経営者と管理者から始め、慣れたら全員に広げる

2-9. スマホの紛失・機種変更に備える

設定時に表示される**バックアップコード（予備の確認コード）**は印刷して鍵のかかる場所に保管し、スマホ紛失時の再設定手順も決めておきます。定着の近道は、経営者が率先して使うことです。

第3章 日々の守り — パソコン・スマホ・Wi-Fi

3-1. 更新は「自動」にして止めない

OS・ブラウザ・アプリの更新には、見つかった弱点（脆弱性）の修正が含まれています。攻撃の多くは、すでに修正が出ている古い弱点を狙います。

- パソコン・スマホのOS更新を**自動**にし、更新して再起動する曜日を決める
- サポートが終了したOSやソフトは使い続けない**（修正が出なくなるため）
- 使っていないソフト・アプリは削除する（弱点の入口を減らす）

3-2. ウイルス対策ソフト

Windowsには標準でMicrosoft Defenderが搭載されています。製品名より大切なのは、**全台で有効になっていることを誰かが確認していること**です。より手厚い管理が必要なら、法人向け製品を検討します。

3-3. 端末の紛失・盗難

紛失しても情報が読まれないよう、全台に**画面ロック**、保存領域の**暗号化**（WindowsはBitLocker、MacはFileVault）、**「デバイスを探す」機能**を設定し、遠隔でロック・消去する手順を確認しておきます。

3-4. Wi-Fiルーター

図表6：Wi-Fiルーターの点検項目

項目	見直し方
管理画面のパスワード	初期設定のままなら必ず変更する
暗号化方式	WPA3（未対応ならWPA2）を使う
ファームウェア	自動更新を有効にする。サポートの切れた古い機種は買い替える
来客用Wi-Fi	業務用と分けた「ゲスト用」ネットワークを使ってもらう
社外での利用	公衆Wi-Fiでは顧客情報を扱わない。テザリングや会社のVPNを使う

第3章 日々の守り（続き） — メールとアカウント

3-5. フィッシング・なりすましメールを見抜く

フィッシングとは、実在の会社や取引先を装ったメール・SMSで偽のサイトに誘導し、ログイン情報やカード情報を盗む手口です。見分けるポイントは次のとおりです。

- ・ **送信元アドレス**が正規のものと微妙に違う（1文字違い、数字の0とアルファベットのOの入れ替えなど）
- ・ 「アカウントが停止されます」「24時間以内に」など、**急がせる文面**
- ・ リンク先のURLが、公式サイトと異なる
- ・ 心当たりのない**添付ファイル**や、不自然な日本語

ただし、最近は見ただ目で判断できない巧妙なものも増えています。そこで、見抜く力よりも**行動のルール**で守ります。

- ・ メール内のリンクからログインしない。**ブックマークや公式アプリから開く**
- ・ 「振込先が変わりました」「至急この口座へ」という連絡は、**メールに書かれていない既知の電話番号で本人に確認**する
- ・ 怪しいと思ったら開かずに報告する。**開いてしまっても、すぐに報告すれば責めない**

最後の項目が特に大切です。「怒られるから黙っておこう」が、被害を最も大きくします。

3-6. アカウントと権限の管理

社員の入れ替わりがある以上、アカウントの管理は仕組みにしておく必要があります。

図表7：入社・異動・退職時のアカウント手続き

タイミング	やること
入社	個人ごとにアカウントを発行。多要素認証を初日に設定。必要なフォルダだけ権限を付与
異動	前の部署の権限を外し、新しい部署の権限を付与
退職	最終日にアカウント停止。共有パスワードを変更。貸与端末を回収し、データを整理
年1～2回	全アカウントと権限の一覧を見直し、不要なものを削除

管理者権限は必要最小限の人数に限定し、日常業務は一般の権限で行います。ファイル共有では「リンクを知っている全員が閲覧可」の設定に注意し、社外と共有するときは相手を指定します。

第3章 日々の守り（続き） — 見落としがちな2つの入口

3-7. 自社のホームページ

ホームページは「会社の顔」であると同時に、インターネットに常に公開されている入口です。古いまま放置されたサイトは機械的に探され、改ざんされて詐欺サイトへの誘導に使われたり、問い合わせフォームの情報を盗まれたりすることがあります。技術的な作業は制作会社や保守会社の担当ですが、経営者として次の点は確認しておきましょう。

- アドレスが「https://」で始まり、ブラウザに鍵マークが表示されているか（警告が出ていないか）
- WordPressなどを使っている場合、**本体・テーマ・プラグインが更新されているか**。誰がいつ更新しているか
- 管理画面のログインに**長いパスワードと多要素認証**が設定されているか。「admin」のような推測しやすいユーザー名を使っていないか
- サイトの**バックアップ**が、サーバーとは別の場所にも保管されているか。戻せることを確認したことがあるか
- ドメインとサーバーの契約者・更新日・管理画面のログイン情報を、**自社で把握しているか**

とくに最後の項目は、制作会社との関係が途切れたときに大きな問題になります。保守契約の内容に「更新・バックアップ・監視」が含まれるかどうか、契約書で確認しておくで安心です。

3-8. 生成AIの業務利用

ChatGPTなどの生成AIは便利な一方、使い方次第で情報漏えいの入口になります。全面禁止にすると、社員が個人のアカウントでこっそり使う「シャドーAI」が生まれ、かえって管理できなくなります。最低限、次の3点を社内ルールに加えましょう。

- **入力してはいけない情報**を決める（顧客の個人情報、取引先の機密、公開前の自社情報など）
- **会社が認めたツールとアカウントだけ**を使う。入力内容を学習に使わせない設定（オプトアウト）や、管理機能のある法人向けプランを基準にする
- AIの出力は、**社外に出す前に必ず人が事実確認**する

活用の進め方は、当社の別冊ホワイトペーパー「生成AI業務活用ガイド」で詳しく扱っています。

第4章 バックアップ — 「取っている」ではなく「戻せる」状態へ

データ消失の原因は、ランサムウェアのほか、誤削除・上書き、機器の故障、火災・水害・盗難、サービスの障害など様々で、どれもある日突然起こります。

4-1. 基本は「3-2-1ルール」

図表8：3-2-1ルール

数字	意味	例
3	データを3つ持つ（元データ+バックアップ2つ）	パソコン本体+外付けドライブ+クラウド
2	2種類以上の異なる保存先に置く	外付けドライブとクラウドストレージ
1	1つは物理的に離れた場所に置く	クラウド、別拠点、代表者の自宅の金庫など

離れた場所のコピーが大切なのは、火災や水害で事務所ごと被害に遭っても、データだけは生き残るようにするためです。

4-2. よくある「つもり」のバックアップ

「バックアップはある」という会社でも、次の状態はよく見られます。

- ・ **事務所内の外付けドライブだけ**：火災・盗難で元データと一緒に失われる
- ・ **つながっぱなしの外付けドライブやNAS**：ランサムウェアに感染すると、バックアップまで暗号化されることがある
- ・ **クラウドに「同期」しているだけ**：誤って削除したファイルや暗号化されたファイルも、そのまま反映される
- ・ **自動バックアップが止まっている**：容量不足などで失敗し続けていることに誰も気づいていない
- ・ **一度も戻したことがない**：いざ復元しようとしたら壊れていた、手順が分からなかった

4-3. ランサムウェアに備える「もう1つ」

最近では3-2-1に「1つはネットワークから切り離す（または書き換えできない状態にする）」「復元できることを確認してエラーをゼロにする」を加えた「3-2-1-1-0」という考え方も提唱されています。小さな会社でも、バックアップを取ったら外付けドライブを外して保管する、過去の版に戻せる（世代管理のある）バックアップサービスを使うことで、この考え方を実践できます。

第4章 バックアップ（続き） — 小さく始めて、確かめ続ける

4-4. 段階的な始め方

いきなり完璧な体制は必要ありません。次の順で広げていきます。

図表9：バックアップの3段階

段階	やること
第1段階 (今週)	重要データを決まったフォルダにまとめる。外付けドライブを用意して週1回コピーし、終わったら外して保管。最重要ファイルはクラウドにも置く
第2段階（1か月）	OS標準の機能（Windowsのファイル履歴、MacのTime Machine）やバックアップサービスで自動化。外付けドライブを2台にして交互に使い、1台は社外で保管
第3段階（3か月）	社内のデータを1か所（NASやクラウドストレージ）に集約し、世代管理のあるクラウドバックアップを追加。手順書を作り、定期確認を仕組みにする

持ち出す外付けドライブや、社外に保管するバックアップは、**暗号化**しておきます（紛失時の情報漏えいを防ぐため）。

4-5. クラウドサービスのデータも自社で持つ

クラウド会計・顧客管理・電子契約・メールなども、障害や乗っ取り、誤操作に備えて、**定期的にデータを書き出して（エクスポートして）別の場所にも保存**しておくで安心です。

4-6. 何をどれくらいの頻度で

頻度は「**どこまで失っても再入力できるか**」で決めます。毎晩1回なら、最悪その日1日分の入力やり直しです。目安は、会計・受発注・顧客情報など日々更新されるデータは**毎日**、提案書や業務資料は**毎週**、更新の少ない過去資料は**毎月**です。

4-7. 定期確認で「戻せる」ことを確かめる

- **毎週**：バックアップが最新の日付で取れているかを見る
- **毎月**：ファイルを1つ実際に戻してみる（数分で終わる小さなテストで十分）
- **年に1回**：重要データを丸ごと戻す訓練と、対象・方法の見直し

確認と復元の手順は**2人以上**が分かる状態にしておきます。担当者が1人だけだと、止まっていることにすら気づけません。

第5章 社内ルール — 1枚から始める情報セキュリティ規程

5-1. 規程は「会社として決めたこと」の記録

ここまでの対策は、社員一人ひとりが同じ行動をとって初めて効果を発揮します。そのための文書が**情報セキュリティポリシー（規程）**です。専門家がない会社こそ、「迷ったらこうする」が書かれた文書が役に立ちます。取引先から対策状況の説明や規程の提出を求められる場面も増えています。

一般的には、次の3階層で整理します。

図表10：情報セキュリティ規程の3階層

階層	内容	小さな会社の始め方
基本方針	経営者が示す、情報を守る姿勢と責任	数行～A4半分。社長の言葉で書く
対策基準	全員が守る具体的なルール	A4で1枚（巻末付録3のひな形）
実施手順	現場の作業手順書	入退社・バックアップ・事故報告から順に

5-2. ルールに入れる5つの観点

対策基準は、次の5つの観点で漏れがないかを確認めると整理しやすくなります。

- ・ **組織**：責任者は誰か、教育をいつ行うか
- ・ **人**：入社時の誓約、退職時の手続き、私物端末の扱い
- ・ **物理**：書類の保管、施錠、機器の持ち出し
- ・ **技術**：パスワード、多要素認証、更新、ウイルス対策、バックアップ
- ・ **外部**：委託先・クラウドサービス・生成AIの利用基準

5-3. 形骸化させない3つのコツ

1. **現場で守れる内容にする**：理想的すぎるルールは守られません。現場の意見を聞き、業務の流れに合わせます
2. **短く、具体的に書く**：「適切に管理すること」ではなく「退職日にアカウントを停止する」のように、行動が分かる言葉で書きます
3. **完璧を目指さない**：まず1枚で運用を始め、年に1回見直して育てます

策定は総務・事務の担当者を中心に、各部署の代表の意見を集め、最後に経営者が承認する流れが現実的です。

第5章 社内ルール（続き） — 周知・教育と、個人情報の義務

5-4. 周知と教育は「短く、繰り返す」

ルールは作っただけでは守られません。次のように、短い時間で繰り返し伝えます。

- **入社時**：ルール1枚を説明し、署名をもらう
- **年1～2回**：30分程度の全員向け研修（パスワード、フィッシング、報告の方法）
- **随時**：朝礼や月例会議で、実際にあった不審メールやヒヤリとした事例を共有する

特に大切なのは、**報告しやすい雰囲気**です。「怪しいメールを開いてしまった」「USBメモリをなくした」と正直に言った人を責めると、次からは隠されます。早い報告を評価する姿勢を、経営者が言葉と態度で示してください。

5-5. 記録を残す

教育の実施日、アカウントの発行・削除、事故やヒヤリハットの内容と対応は、簡単でよいので記録します。記録は、次の見直しの材料になるだけでなく、万一のときに「会社として対策していた」ことの説明にもなります。

5-6. 個人情報を扱う会社の義務

個人情報保護法は、取り扱う件数にかかわらず、**個人情報を事業に使うすべての事業者**が対象です。顧客名簿や問い合わせ情報を持っていれば、小さな会社も例外ではありません。

図表11：押さえておきたい主な義務（2026年9月時点）

義務	内容
利用目的の特定と通知・公表	何に使うかを具体的に決め、プライバシーポリシー等で示す
安全管理措置	組織・人・物理・技術の面から漏えい等を防ぐ（本書の対策そのもの）
委託先の監督	業務委託先やクラウドサービスでの扱いも確認する
漏えい等の報告・通知	一定の場合、個人情報保護委員会への報告と本人への通知が必要

報告が必要になるのは、要配慮個人情報（病歴など）の漏えい、財産的な被害のおそれがある漏えい、不正な目的によるおそれがある漏えい、1,000人を超える漏えいなどです。報告は、事態を知ってから概ね3～5日以内の「速報」と、原則30日以内（不正な目的によるおそれがある場合は60日以内）の「確報」の2段階とされています。該当するか迷うときは、個人情報保護委員会の案内を確認し、早めに専門家へ相談してください。

第6章 事故が起きたら — 初動対応と連絡の流れ

6-1. 最初の1時間で被害の大きさが変わる

事故（インシデント）は完全には防げません。差がつくのは、**気づいてからの最初の行動**です。

6-2. 典型的な場面と最初の行動

図表12：場面別の最初の行動

場面	最初にやること
不審なメールのリンク・添付を開いた	端末をネットワークから外し（LANケーブルを抜く・Wi-Fiを切る）、責任者に報告
身代金の要求が出た・ファイルが開けない	端末を外し、バックアップ等への接続も止める。電源操作や復旧は専門家の指示を待つ
身に覚えのないログインがあった	別の安全な端末からパスワードを変更し、他の端末を強制ログアウト
パソコン・スマホを紛失した	遠隔ロック・データ消去を実行し、関係するアカウントのパスワードを変更
不正送金・振込詐欺の疑い	すぐに取引銀行へ連絡して止められるか相談し、警察にも相談する
個人情報が漏れた可能性	範囲を把握して経営者へ即時報告。報告義務の該当性を確認（第5章）

自己流で復旧作業をすると、原因調査に必要な記録が消えることがあります。**切り離す、報告する、記録する**（時刻つきのメモ）を先に行い、その先は専門家と相談しながら進めます。

6-3. 報告と判断の流れ

1. **発見者**：すぐに責任者（不在時は代理）へ報告する。自分で判断して抱え込まない
2. **責任者**：事実を確認し、被害の範囲を把握する。必要に応じて保守会社・IT顧問に連絡する
3. **経営者**：対応方針を決める。取引先・顧客への連絡、公的機関への相談・報告の可否を判断する
4. **全員**：落ち着いたら原因と再発防止策を話し合い、ルールと手順を更新する

相談先としては、IPAの「情報セキュリティ安心相談窓口」、各都道府県警察のサイバー犯罪相談窓口、個人情報の漏えい時は個人情報保護委員会などがあります。連絡先は巻末付録2の表に書き込み、**紙でも保管**しておきましょう。

第6章 事故が起きたら（続き） — 止まらない会社のためのBCP

6-4. BCPとは

BCP（事業継続計画）は、災害・感染症・システム障害・サイバー攻撃などが起きたときに、**大事な業務を止めない、止まってもすぐ再開する**ための計画です。人命を守る防災計画に、「どの業務から、いつまでに戻すか」という経営の視点を加えたものです。

6-5. 小さな会社のBCP 4ステップ

1. **中核業務を決める**：売上や顧客への影響が大きく、最優先で続ける業務を1～2個に絞る
2. **戻す目標を決める**：その業務を「何時間・何日以内に」再開するか。データを「どこまで失っても再入力できるか」も決める（第4章）
3. **止まる原因を洗い出す**：その業務に欠かせない「人・物・お金・情報」を書き出し、それぞれが使えなくなったときの代わりを考える
4. **手順を1枚にまとめる**：初動のチェックリスト、連絡先、業務の優先順位を書く

図表13：「人・物・お金・情報」の点検例

観点	問い	代わりの手段の例
人	誰がいないと止まるか	手順書化、代行者の指名、社長不在時の決裁者
物	どの設備・端末が欠かせないか	予備のパソコン、自宅で使える端末、代替の作業場所
お金	売上が止まって何か月耐えられるか	手元資金の確認、保険（サイバー保険を含む）の見直し
情報	どのデータ・システムが欠かせないか	離れた場所のバックアップ、連絡手段の予備、紙の連絡先

6-6. ITの備えと、年1回の見直し

ITの面では、**連絡手段の予備**（普段のチャットやメールが使えないときの代わり）、**紙の連絡先リスト**、**在宅でも仕事ができる準備**の3つを整えておきます。そのうえで年に1回（9月1日の防災の日など時期を決めて）見直し、安否確認・バックアップの復元・在宅勤務への切り替えといった小さな訓練を行います。訓練で見つかった問題が、そのまま改善項目になります。

巻末付録1 セキュリティ自己診断チェックリスト20

【体制とアカウント】

- ☐ 1. 重要な情報と、使っているサービス・アカウントを一覧にしている
- ☐ 2. 情報セキュリティの責任者と、その代理を決めている
- ☐ 3. ドメイン・サーバー・ホームページの契約と管理画面を把握している
- ☐ 4. サービスごとに別のパスワードを使い、使い回しが無い
- ☐ 5. パスワードを付箋や共有の表計算ファイルで管理していない
- ☐ 6. パスワード管理ツール（法人プラン）を導入している
- ☐ 7. メール・ネットバンキング・会計に多要素認証を設定している
- ☐ 8. 経営者・管理者のアカウントはパスキー等の強い方法で守っている

【日々の守り】

- ☐ 9. 全端末で自動更新が有効で、サポート切れのOSがない
- ☐ 10. 全端末でウイルス対策が有効なことを確認している
- ☐ 11. ノートパソコン・スマホに画面ロックと暗号化を設定している
- ☐ 12. Wi-Fiルーターの管理パスワードを初期設定から変更している
- ☐ 13. 振込先の変更依頼は、既知の電話番号で確認するルールがある
- ☐ 14. 退職日にアカウントを停止し、共有パスワードを変更している

【バックアップ・ルール・非常時】

- ☐ 15. 重要データを3-2-1ルールで保管し、1つは社外にある
- ☐ 16. つなぎっぱなしでない、または過去の版に戻せるバックアップがある
- ☐ 17. この3か月以内に、実際にファイルを復元してみた
- ☐ 18. 生成AIの扱いを含む社内ルール1枚を、全員に説明している
- ☐ 19. 事故時の報告先と連絡表があり、紙でも保管している
- ☐ 20. 中核業務と再開目標を決めたBCPがあり、年1回見直している

判定の目安：10個以下なら、まず4・7・9・15・19の5項目から。16個以上なら、訓練と年1回の見直しを定着させる段階です。

巻末付録2 インシデント発生時の初動連絡表

コピーして記入し、事務所の見える場所と各自の手元（紙）に保管します。公的機関の連絡先は各機関の公式サイトで確認し、**年に1回、BCPの見直しと同時に更新します。**

図表14：社内の連絡順

順番	役割	氏名	電話番号
1	情報セキュリティ責任者		
2	責任者の代理		
3	経営者（最終判断）		

図表15：社外の連絡先

連絡先	連絡する場面	担当者・電話番号
IT顧問・保守会社	感染・不正アクセスの疑い、復旧の相談	
ホームページ制作・サーバー会社	サイトの改ざん、表示の異常	
メール・クラウドサービスのサポート	アカウント乗っ取り、サービス障害	
取引銀行	不正送金・振込詐欺の疑い	
警察（サイバー犯罪相談窓口）	犯罪被害の相談	
IPA 情報セキュリティ安心相談窓口	技術的な相談	
個人情報保護委員会	個人情報の漏えい等の報告	
保険会社	保険の適用確認（サイバー保険等）	
主要取引先	取引先に影響が及ぶおそれ	

最初の行動の3原則：切り離す（疑わしい端末をネットワークから外す）／**報告する**（自分で判断せず責任者へ。報告した人を責めない）／**記録する**（いつ・誰が・何をしたかを時刻つきでメモ）

巻末付録3 情報セキュリティ基本ルール（1枚版ひな形）

自社に合わせて書き換え、社長名で全員に配布してください（【 】は記入欄）。

基本方針

当社は、お客様・取引先・社員の情報を守ることを経営の責任と考え、全員でこのルールを守り、年1回見直します。責任者：【氏名】／代理：【氏名】

全員が守ること

1. アカウントとパスワード

- パスワードはサービスごとに別の12文字以上とし、会社指定のツールで管理する。人に教えない
- 会社が指定するサービスでは、多要素認証を必ず設定する

2. パソコン・スマホ

- 更新の通知はその日のうちに適用する。離席時は画面をロックする
- 業務データは会社が認めた端末だけで扱う。紛失したらすぐ責任者へ

3. メールと連絡

- メール内のリンクからログインしない。怪しいメールは開かず責任者へ
- 振込先の変更などお金に関わる依頼は、既知の電話番号で相手に確認する

4. 情報の扱い

- 個人情報・機密情報を持ち出さない。社外との共有は相手を指定する
- 生成AIには、顧客情報・取引先の機密・公開前の社内情報を入力しない。会社が認めたツールだけを扱う

5. 報告

- 「おかしい」と思ったら、すぐに責任者へ報告する。早い報告を責めることはない

会社が行うこと

- 入退社時のアカウント手続き、年1回の権限見直しと研修
- 重要データのバックアップと、毎月の復元確認（担当：【氏名】）

制定日：【 年 月 日】 代表取締役：【氏名】

おわりに — 発行元・ご相談窓口

情報セキュリティは、特別な知識を持つ人だけの仕事ではありません。**長いパスワードを使い回さない、多要素認証を入れる、更新を止めない、戻せるバックアップを持つ、そして何かあったらすぐ報告する。**本書でお伝えしたことの多くは、この数行に集約されます。まずは巻末のチェックリストで現状を確認、今日できる1つから始めてみてください。1つ進めるごとに、会社は確実に守りやすくなります。

Harmonic Society株式会社

千葉市を拠点に、中小企業のホームページ制作・AI導入支援・IT顧問を提供しています。専任のIT担当者がいない会社から、「何から手を付ければいいのか分からない」「今の設定で大丈夫か見てほしい」というご相談を日常的にいただいています。専門用語を使わず、会社の規模と業務に合った「ちょうどいい」対策を一緒に考えます。オンライン対応・全国OK。

サービスのご案内

サービス	内容・価格
IT顧問ライトプラン	セキュリティ・AI・ITの継続相談を月1.5万円から
ホームページ制作・保守	常時SSL・更新・バックアップを含む保守にも対応

まずは30分の無料相談から

「チェックリストで引っかかった項目をどう直せばいいか」「社内ルールを自社向けに整えたい」——本書を読んで浮かんだ疑問を、そのままお持ちください。売り込みはしません。

- Web : <https://harmonic-society.co.jp/contact/>
- お役立ち資料一覧 : <https://harmonic-society.co.jp/whitepaper/>

本書の内容は2026年9月時点の情報に基づきます。法制度・公的な枠組み・各サービスの機能や料金は変更される場合があります。本書は一般的な考え方を示すものであり、特定の効果を保証するものではありません。個別の事案への対応は、専門家や関係機関にご相談ください。記載の会社名・製品名は各社の商標または登録商標です。無断転載を禁じます。