

小さな会社のための サイバーの基本7つ(設定手順つき)

長谷部社会保険労務士事務所 2026年10月版

はじめに:高い機械を買う前に

2025年に警察へ届け出があったランサムウェア(身代金ウイルス)の被害は年間226件でした。2025年上半期の内訳では、被害企業の約66%が中小企業で、侵入経路の約84%がVPN機器とリモートデスクトップです。VPN機器を使う組織の半分以上が最新の更新を当てておらず、社外からのアクセスの約4割がIDとパスワードだけで守られていました(警察庁「サイバー空間をめぐる脅威の情勢等について」令和7年、都道府県警の引用資料による)。

今月は大手でも事故が続きました。GMOグループではアンケートサイトから最大約95万件の個人情報が持ち出され、別のサービスでは取引口座の情報が取られて不正取引が起きました。公表された原因は「ソフトウェアの脆弱性」と「セキュリティ上の問題」です。米国のVercel社では、社員が使っていた外部のAIツールが先に破られ、そのツールに渡していたアカウントの権限を通じて社内に入られました。

つまり事故の原因の大半は、高い機械が無かったことではなく、**更新・認証・権限・控え(バックアップ)**という基本の欠落です。基本はほとんどお金がかかりません。この紙の7つを、上から順に確かめてください。

1. 更新を当てる(パソコン・スマホ・ルーター・VPN)

なぜ:侵入の最大の入口は「直っているのに当てていない穴」です。

Windows パソコン

- 設定 → Windows Update → 「更新プログラムのチェック」。再起動まで済ませる。
- 同じ画面の「詳細オプション」で「他の Microsoft 製品の更新プログラムを受け取る」をオン(Officeも更新される)。
- Windows 10 は2025年10月14日でサポートが終わりました。**今も使っているパソコンは原則として更新が来ません(有償の延長サポートを契約している場合を除く)。買い替えか Windows 11 への移行が必要です。
- ウイルス対策:**Windows 標準の「Windows セキュリティ(Defender)」がオンになっているか確認する(設定 → プライバシーとセキュリティ → Windows セキュリティ)。有料のウイルス対策ソフトを入れている場合は、期限切れのまま放置しない。期限が切れると Defender も無効のままになることがあります。

Mac:システム設定 → 一般 → ソフトウェアアップデート → 「自動アップデート」をすべてオン。

スマホ:iPhone は 設定 → 一般 → ソフトウェアアップデート → 自動アップデートをオン。Android は 設定 → システム → システムアップデート。

ルーター・VPN機器・NAS:管理画面にログインし、ファームウェア更新を確認する。**初期パスワードのままなら今すぐ変える。**5年以上前の機器でメーカーの更新が止まっているものは交換する。型番で「サポート終了」を検索すれば分かります。

チェック:☐ パソコン全台が Windows 11 か Mac の最新 ☐ 更新は自動 ☐ ウイルス対策が有効で期限内
☐ ルーター・VPNの管理パスワードは初期値ではない ☐ 機器のファームウェアは今年更新した

2. パスワードを使い回さない + 2段階認証

なぜ:どこか1か所で漏れたパスワードが、他のサービスで試されます。2段階認証(多要素認証)があれば、パスワードが漏れても入られません。

Google(Gmail・Google Workspace)

- 本人:myaccount.google.com → セキュリティ → 「2段階認証プロセス」をオン。できれば「パスキー」も登録。
- 会社の管理者:管理コンソール(admin.google.com)→ セキュリティ → 認証 → 2段階認証プロセス → 「ユーザーが2段階認証を有効にできるようにする」と「適用」をオン。猶予期間を決めて全員に義務づける。

Microsoft 365

- 本人:account.microsoft.com → セキュリティ → 「高度なセキュリティ オプション」→ 2段階認証をオン。
- 会社の管理者:Microsoft Entra 管理センター → Entra ID → 概要 → プロパティ → 「セキュリティの既定値群の管理」→ 有効(全員に多要素認証が求められる)。**注意:**有効にすると古い方式のメール送受信 (Office 2010 など古いOffice、複合機からのメール送信の一部)が止まることがあります。複合機や古いソフトがある会社は、IT業者に確認してから。

銀行・会計・給与・請求のクラウド:それぞれの設定画面で2段階認証をオン。**インターネットバンキングは最優先。**

パスワード管理の道具:使い回しをやめるには、人の記憶では無理です。パスワード管理アプリ(例: Bitwarden、1Password)を入れ、サービスごとに長い別々のパスワードを作らせる。1人あたり月数百円が無料です。ブラウザの保存機能でも「使い回し」よりはましです。

チェック:☐ メール・銀行・会計・給与・請求の全部に2段階認証 ☐ 退職者のアカウントは退職日に停止 ☐ パスワードは紙やExcelではなく管理アプリ

3. 控え(バックアップ)を「切り離して」取る

なぜ:ランサムウェアで会社が止まるか止まらないかは、ここだけで決まります。つながったままの控えは、一緒に暗号化されます。

やり方(3つの置き場、2種類の媒体、1つは切り離す)

- 日々:クラウド(Google ドライブ・OneDrive・NASのスナップショット)。ファイルの「以前のバージョン」から戻せるかを一度試す。
- 週1回:外付けハードディスクに複製し、終わったら抜いて金庫へ。2台を交互に使う。
- 年1回:実際に1つのファイルを復元してみる。復元できない控えは控えではありません。

チェック:☐ 切り離れた控えがある ☐ 復元を試したことがある ☐ 給与・会計・顧客台帳の控えの場所を2人以上が知っている

4. 権限を棚卸しする(誰に・何を・どこまで渡しているか)

なぜ: Vercel社の事故は「社員が外部ツールに渡していた権限」から始まりました。便利なツールほど広い権限を求めます。

Google の場合

- 本人: myaccount.google.com → セキュリティ → 「サードパーティ製のアプリとサービス」。覚えのないアプリ、使っていないアプリは「アクセス権を削除」。
- 会社の管理者: 管理コンソール → セキュリティ → アクセスとデータ管理 → 「API の制御」。社員が会社のメールに何のアプリをつないでいるかが一覧で見えます。信頼するアプリだけを「信頼済み」にし、Gmail などを「制限付き」にすると、登録のないアプリはつなげなくなります。**注意:** 制限付きにする前に、今使っている正規のメールソフト(Outlook・Thunderbird・スマホのメールアプリなど)を先に信頼済みに登録してください。先に制限すると、それらも止まります。

Microsoft の場合: Entra 管理センター → エンタープライズ アプリケーション → 同意とアクセス許可。「ユーザーの同意」を管理者承認制にする。

共通

- 管理者アカウントは普段使いと分ける。
- 共有リンクの「リンクを知っている全員」を見直す(Google ドライブ・OneDrive・Dropbox)。
- 退職者・取引終了先のアカウントとアクセス権を消す。

チェック: ☐ 外部アプリの一覧を見た ☐ 「全部許可」のアプリがない ☐ 管理者と普段使いが別 ☐ 退職者のアクセス権がゼロ

5. メールの箱に鍵を置かない

なぜ: メールにはパスワード、再設定のリンク、確認コード、顧客の個人情報が全部入っています。メールを丸ごと読める者は、会社のすべての鍵を持っています。

- パスワードやログイン情報がメールで届いたら、パスワード管理アプリ(または会社の台帳)に移して、メールは削除する。
- マイナンバー・口座・健康情報は、メール本文に書かない、添付しない。送る必要があるときは、パスワード付きファイルより、共有フォルダに置いて権限で渡す方が安全です。
- 送金・振込先の変更は、メールだけで動かず、**元から知っている電話番号で本人に確認する**(偽の請求書・なりすましメール対策)。

チェック: ☐ メールにパスワードが残っていない ☐ 振込先変更は電話で確認する決まりがある

6. AIツールの設定を確かめる

なぜ: 無料のAIは、入力した内容を学習に使う設定になっていることがあります。社員が善意で顧客名簿を貼れば、それは外に出たのと同じです。

3つの決まり

1. **貼らないもの:** 個人の氏名+住所、マイナンバー、口座、健康情報、顧客名簿、取引先との契約内容。貼るなら「Aさん」「某社」に置き換える。

2. 学習に使われない設定にする

- ChatGPT:左下のプロフィール → 設定 → 「データコントロール」→ 「モデル改善に協力する」をオフ。同じ画面の「広告をパーソナライズ」も、会社で使うならオフ。
- Claude:左下の名前 → 設定 → 「プライバシー」→ 環境設定の「Help improve our AI models」をオフ(日本語画面でもこの項目は英語表記)。
- Gemini:左下の「アクティビティ」→ 「アクティビティの保存」をオフ。オフにできない表示のときは、自動削除の期間を一番短くする。
- (画面名は2026年10月29日に実際の画面で確認。お使いのプランや時期で変わることがあります)
- 会社で本格的に使うなら、法人契約(入力を学習に使わない契約)にする。

3. 出てきたものは確認して使う:数字・法令・日付は元を見る。AIは自信たっぷりに間違えます。

つなぐ権限:AIにメールやカレンダーをつなぐときは、「読み取りだけ」にできるか、どのアカウント(会社か個人か)か、を決めてから。4の棚卸しの対象です。

チェック:☐ 社員が使うAIを把握している ☐ 学習に使わない設定 ☐ 貼ってはいけないものを紙で配った

7. 事故が起きたときの手順を1枚、今作っておく

最初の10分

1. ネットワークから切り離す(LANケーブルを抜く、Wi-Fiを切る)。電源は原則として切らない(調査に必要な痕跡が消えるため)。ただし、警察や依頼した専門業者から指示があればそれに従う。
2. 周りのパソコンも同じようにする。
3. 責任者に連絡する。身代金の要求があっても応じない。

連絡先(書いておく)

- 警察相談専用電話: #9110(都道府県警。サイバー犯罪相談窓口につないでもらう)
- IPA 企業・組織向けサイバーセキュリティ相談窓口:メールのみ cs-support@ipa.go.jp(電話窓口はありません。ipa.go.jp からの返信を受け取れる設定に)
- 急ぎで人と話したいときは、上の警察相談専用電話か、契約しているIT業者・お助け隊へ
- 契約しているIT業者・お助け隊・保険会社
- 当事務所(個人情報・マイナンバーが関わる場合の届出の相談)

届出の期限:個人情報の漏えい等のうち、次のいずれかに当たるとき(おそれを含む)は、個人情報保護委員会への報告と本人への通知が法律で義務づけられています。①要配慮個人情報(病歴・健康診断結果など)が含まれる ②不正利用で財産的被害が生じるおそれがある(クレジットカード番号・口座など) ③不正アクセスなど不正の目的によるもの ④1,000人を超える。期限は、速報がおおむね3～5日以内、確報が30日以内(③の不正目的によるものは60日以内)です。マイナンバーが含まれる場合は、件数にかかわらず委員会への報告対象になることがあります。当てはまるか迷うときは当事務所にご連絡ください。

チェック:☐ この手順を印刷して電話の横に貼った ☐ 連絡先が埋まっている

お金をかける価値があるもの・ないもの

価値がある	目安
パスワード管理アプリ、2段階認証	1人 月0～数百円
切り離れた控え(外付けHDD 2台)	数万円、一度きり
Windows 10 の買い替え	1台 10～20万円
サイバーセキュリティお助け隊(経産省・IPAの枠組み。見守り・駆けつけ・保険の束。デジタル化・AI導入補助金の対象)	月額制。価格は提供事業者ごと
事故後の費用を払うサイバー保険	年数万円～

先に基本を済ませてから考えるもの

高額なUTM機器のリース、常時監視(SOC)サービス。見る人がいないと警報が鳴るだけです
診断だけのサービス。直す人がいなければ紙が増えるだけです
「AIセキュリティ」と名のつく新製品。中身を聞いてから

今日やる3つ(30分)

1. メール・銀行・会計の2段階認証をオンにする。
2. Google の「サードパーティ製のアプリ」を開き、覚えのないものを消す。
3. 7の手順を印刷して電話の横に貼る。

ご不明な点は当事務所まで。設定の代行や、社内の点検(権限の棚卸し・個人情報とマイナンバーの管理)も承ります。

長谷部社会保険労務士事務所 札幌市西区西野8条1丁目7-5 TEL (011)215-8972 E-mail: hasebe.sr.office@gmail.com <https://www.hasebe-sr-office.com/>

この資料は、公的機関の公表情報に基づく一般的な情報提供です。個別の機器やシステムの設定については、保守を委託しているIT事業者にもご確認ください。この資料の実施により事故が起きないことを保証するものではありません。

出典:警察庁「サイバー空間をめぐる脅威の情勢等について」(令和7年)の都道府県警による引用資料、IPA「情報セキュリティ10大脅威 2026」、GMO各社・Vercel社の公式発表、個人情報保護委員会「漏えい等の対応」。設定の画面名は2026年10月時点。各社の画面は変わることがあります。