Windows 11の更新と保護

Windowsの方はこのページ。Macの方は2ページへ。全部を一度に行う必要はありません。

作業前に：仕事のファイルを保存し、電源と通信を確保します。業務ソフトに指定の環境がある場合は、販売元の対応情報も確認します。

1 更新状況を見る

① 「スタート」→「設定」→「Windows Update」を開く。

② 「更新プログラムのチェック」または「確認」に相当するボタンで、更新の有無を見る。表記は環境によって異なる。

③ 利用可能な更新があれば内容を確認し、再起動できる時間に画面の案内に沿って適用する。

「最新の状態」でも、そのOS自体のサポート状況は別に確認が必要です。Windows 10などは、このページの手順だけで対応済みとは判断しません。

2 ウイルス対策が働いているかを見る

① スタートで「Windows セキュリティ」を検索して開く。

② 「ウイルスと脅威の防止」で、警告や対処が必要な表示がないかを見る。

③ 他社の対策ソフトを使っている場合は、そのソフトでも保護状態・更新・契約期限を確認する。

保護機能をオフにして解決しようとせず、不明な警告は公式サポートへ。更新できない場合も「済」にせず、要確認として残します。

確認日：　　結果：□確認済み □要確認

分からなかった表示・問い合わせたいこと：

公式の更新手順（Microsoft）

公式のウイルス対策機能の案内（Microsoft）

Macの更新を確認する

Macの方はこちら。Windowsの方は1ページへ。画面例ではなく、設定を探すための手順です。

1 macOSの更新状況を見る

① 仕事のファイルを保存し、必要なデータのバックアップ状況を確認する。電源と通信も確保する。

② 画面左上のAppleメニュー→「システム設定」→「一般」→「ソフトウェアアップデート」を開く。

③ 利用できる更新と、再起動が必要かを確認する。旧版では「システム環境設定」内にある場合もある。

④ 仕事用ソフトが対応しているか確認したうえで、時間に余裕があるときに画面の案内に沿って更新する。

「最新の状態」は、そのMacに提供される更新の状態を示します。古い機種・古いOSのサポートが続いているか不明な場合は、Appleの公式情報で確認します。

2 ブラウザーと仕事用アプリも確認する

① App Storeから入れたアプリは、App Storeの「アップデート」を確認する。

② それ以外のアプリは、アプリ内の更新機能か、販売元の公式案内を確認する。

「Macだから対策不要」とは判断しません。メールやクラウドのログイン保護、共有範囲の確認も関係します。他社製の対策ソフトを使っている場合は、そのソフトの状態も確認します。

確認日：　　結果：□確認済み □要確認

更新前に対応を確かめたい業務ソフト：

分からなかった表示・問い合わせたいこと：

---

macOSの公式更新手順（Apple）

macOSとアプリの更新について（Apple）

仕事用メールの本人確認

使っているサービスの項目だけ確認します。メールを読むアプリと、契約しているメールサービスは別です。

例：OutlookアプリでGmailを読む場合、Googleアカウント側の設定を確認します。会社・契約先が管理するアカウントは、管理者の方針に従います。

GoogleアカウントでGmailを使う場合

① いつもの公式アプリからアカウント管理を開くか、ブラウザーで myaccount.google.com を自分で開く。

② 「セキュリティとログイン」→「Googleにログインする方法」から、2段階認証の設定状況を見る。

③ 未設定なら、公式案内に沿って、利用できる本人確認方法を設定する。パスキー利用時はログインの流れが異なる。

④ 予備の認証方法やバックアップコードなど、スマホ紛失時の復旧方法を確認する。コードは他人に見せず安全に保管する。

個人用Microsoftアカウントを使う場合

① ブラウザーで account.microsoft.com/security を自分で開く。

② 「サインイン方法の管理」などから、認証方法と2段階認証の設定状況を確認する。

③ 必要な設定は公式案内に沿って行い、予備の認証・復旧方法も確認する。

会社・学校用Microsoft 365は設定が異なります。管理者の案内へ。上記以外の独自ドメインメールなどは、契約先の公式サポートで対応を確認します。

設定前に：パスワードの使い回しも確認。パスキーは自分だけが使う信頼できる端末で設定し、知らない認証要求は承認しません。この用紙にはパスワードや認証コードを書かないでください。

利用サービス：　　□確認済み □管理者・契約先へ相談

Google公式の2段階認証の案内

Google公式のバックアップコードの案内

Microsoft公式の2段階認証の案内

データの保存先と共有を確認する

平常時の基本確認用です。感染や漏えいが疑われる場合は通常の確認を続けず、専門窓口へ相談してください。

1 請求書などの保存先をたどる

① 普段使っている仕事のフォルダーを開き、保存先を確認する。例：パソコン本体／クラウド／外付け機器。

②同じデータの予備が別の保存先にあるか確認する。機器が違うか、過去の版を戻せるかも確認する。

③ 予備の代表的なファイルを開き、中身と保存日を確認する。感染が疑われるPCへ無事な予備は接続しない。

クラウドの同期だけでは削除も反映されることがあります。履歴・復元機能と保存期間は契約先の公式情報で確認します。SSDへのコピー手順は、別の記事で扱います。

対象のデータ：

普段の保存先：　　予備の保存先：

予備の保存日：　　□開けた □予備なし □要確認

---

2 共有相手と、普段の送信方法を見る

① 共有中のファイルを一つ選び、サービスの「共有」「アクセスを管理」などの画面を開く。

② 誰が閲覧・編集できるか確認する。「リンクを知っている全員」など、想定より広い公開がないかを見る。

③ 不要な共有があれば、仕事への影響を確認してから変更する。業務メールでは、宛先と添付を送信前に確かめる。

対象の共有ファイル：　　□確認済み □要確認

このシートは安全性の認定や、すべての対策が済んだことの証明ではありません。該当しない項目は飛ばし、分からない点は管理者・契約先へ確認するためのメモとして使えます。

基本対策の公式資料（IPA 情報セキュリティ6か条）

事業のセキュリティについて相談したいとき（IPA）