Windows 安心設定ガイド

パソコンとアカウント、保存したファイルを安全に守ります。

画面を見ながら、一つずつ確認できます。

家庭や仕事でWindows 11を使う方へ。

更新、ウイルス対策、暗号化、バックアップを確認する説明書です。

画面や項目名は、Windowsの版、エディション、機種、更新状況で異なります。
設定をしても、詐欺や情報漏えいを完全に防げるわけではありません。



操作の模式図

覚えておきたいこと

第1版 2026年9月20日。Microsoft公式サポートを参照した独自の説明書です。Microsoftの公式マニュアルではありません。

この本の使い方

準備と更新：3〜10ページ
ウイルス・通信・アプリ：11〜21ページ
端末・データ・プライバシー：22〜38ページ
公式情報の出典：39〜41ページ

画面例は操作場所を示す模式図です。実際の画面では、同じ意味の項目を探してください。

覚えておきたいこと

最初にWindows UpdateとWindows セキュリティを確認し、その後にサインイン、暗号化、バックアップを見直します。

設定を始める前に

☐ 作業中のファイルを保存します。

☐ 管理者の許可が必要な端末か確認します。

□ Microsoftアカウントへサインインできます。

□ BitLocker回復キーの保管先を確認します。

☐ 感染が疑われる場合は38ページを先に確認します。

会社・学校の端末では、組織の管理ポリシーを優先し、情報システム担当者へ連絡してください。

覚えておきたいこと

大きな変更や回復操作の前に、必要なファイルをバックアップします。

共通の入口：設定とWindows セキュリティ

更新の設定と保護機能の入口を分けて覚えます。

- ［スタート］から［設定］を開きます。
- 更新は［Windows Update］を開きます。
- 保護機能は［プライバシーとセキュリティ］を開きます。
- ［Windows セキュリティ］から各保護画面を開きます。

確認：設定とWindows セキュリティの両方を開けました。



操作の模式図

覚えておきたいこと

スタートの検索欄へ項目名を入力して開くこともできます。

今日、確認する10項目

□ Windowsの版とサポート状況

□ Windows Updateと再起動

☐ ウイルス対策とスキャン

☐ ファイアウォール

□ SmartScreenと不要アプリ対策

☐ メモリ整合性とセキュア ブート

□ Windows Helloと2段階認証

□ BitLockerと回復キー

☐ バックアップとアプリ権限

☐ 感染や紛失時の対応

覚えておきたいこと

更新とDefenderを先に確認し、次にデータとアカウントを守ります。

Windowsの版とサポート状況

セキュリティ更新を受け取れるWindowsを使います。

- ［設定］＞［システム］＞［バージョン情報］を開きます。
- Windowsのエディションとバージョンを確認します。
- Windows 11の更新状況を確認します。
- Windows 10では移行、ESU、端末更新を検討します。

Windows 10の通常サポートは2025年10月14日に終了しました。ESU加入端末や組織管理端末は管理者の案内に従います。

確認：利用中のWindowsとサポート状況を確認しました。

覚えておきたいこと

古いWindowsが動作していても、セキュリティ更新がない状態では危険が増えます。

Windows Update

Windowsと組み込みの保護機能を最新にします。

- ［設定］＞［Windows Update］を開きます。
- ［更新プログラムのチェック］を選びます。
- 表示された更新をダウンロードしてインストールします。
- 必要な場合は再起動して完了を確認します。

更新中は電源を切りません。ノートPCは電源へ接続し、安定した通信環境で行います。

確認：Windows Updateに未処理の更新がありません。

覚えておきたいこと

更新履歴では、インストール済みの品質更新と機能更新を確認できます。

オプション更新とドライバー

機器を動かすドライバーも安全な版へ更新します。

- ［Windows Update］＞［詳細オプション］を開きます。
- ［オプションの更新プログラム］を確認します。
- 必要なドライバーだけを選びます。
- インストール後は動作を確認して再起動します。

オプションのドライバーは自動で入らない場合があります。問題がなければ、むやみに古い版へ戻しません。

確認：必要なドライバー更新を確認しました。

覚えておきたいこと

Windows Updateにない場合は、PCや機器メーカーの公式サイトを確認します。

再起動とアクティブ時間

更新を完了しながら、作業中の再起動を避けます。

- ［Windows Update］＞［詳細オプション］を開きます。
- ［アクティブ時間］を開きます。
- 自動調整または普段使う時間を設定します。
- 再起動待ちの更新を放置せず完了させます。

更新の一時停止は期限を決めて使います。長期間止めたままにしません。

確認：アクティブ時間と再起動待ちを確認しました。

覚えておきたいこと

更新の適用には再起動が必要な場合があります。作業を保存してから実行します。

Windows セキュリティのホーム

パソコン全体の保護状態を一つの画面で把握します。

- ［Windows セキュリティ］を開きます。
- 各項目に緑のチェックがあるか確認します。
- 警告がある項目を開き、推奨操作を確認します。
- 他社製ウイルス対策を使う場合も状態を確認します。

確認：警告の理由と必要な操作を確認しました。



操作の模式図

覚えておきたいこと

Microsoft DefenderアプリとWindows セキュリティは別の製品名です。Windows組み込み保護はWindows セキュリティで確認します。

クイック スキャン

よく狙われる場所を短時間で確認します。

- ［ウイルスと脅威の防止］を開きます。
- 現在の脅威と前回のスキャンを確認します。
- ［クイック スキャン］を実行します。
- 検出結果と必要な操作を確認します。

スキャン中も不審なファイルを開きません。検出通知を無視して許可しません。

確認：クイック スキャンが完了し、結果を確認しました。

覚えておきたいこと

Windows セキュリティは通常、自動でもスキャンします。心配なときは追加で実行します。

フル・カスタム・オフライン スキャン

疑わしい場所やパソコン全体を詳しく確認します。

- ［スキャンのオプション］を開きます。
- 状況に合うスキャン方式を選びます。
- 強い感染が疑われる場合はオフライン スキャンを検討します。
- 開いているファイルを保存して実行します。

Microsoft Defender オフライン スキャンは再起動します。作業中のファイルを先に保存します。

確認：必要なスキャン方法を選べました。

覚えておきたいこと

オフライン スキャンの結果は［保護の履歴］で確認します。

リアルタイム保護と改ざん防止

ファイルを開く時点で脅威を検出できる状態にします。

- ［ウイルスと脅威の防止］＞［設定の管理］を開きます。
- リアルタイム保護をオンにします。
- クラウド提供の保護を確認します。
- 改ざん防止をオンにします。

保護を切るよう指示するソフトや電話サポートを信用しません。除外設定は影響を理解してから使います。

確認：主要な保護設定が有効です。

覚えておきたいこと

他社製ウイルス対策を使う場合は、製品側の保護状態も確認します。

保護の履歴と許可した脅威

検出された脅威への対応が完了しているか確認します。

- ［保護の履歴］を開きます。
- 検出日時、対象、処理結果を確認します。
- 誤って許可した脅威がないか確認します。
- 不要な許可を取り消し、もう一度スキャンします。

名前だけで安全と判断しません。業務ソフトが検出された場合は管理者や開発元へ確認します。

確認：保留中の処理と不要な許可がありません。

覚えておきたいこと

許可した脅威はWindows セキュリティが処理しないため、定期的に見直します。

ランサムウェア防止

重要なフォルダーを不明なアプリの変更から守ります。

- ［ウイルスと脅威の防止］を開きます。
- ［ランサムウェア防止の管理］を開きます。
- ［コントロールされたフォルダー アクセス］を検討します。
- ブロック通知ではアプリの運営元を確認します。

有効にすると正規アプリがブロックされる場合があります。許可する前にアプリの場所と発行元を確認します。

確認：保護対象フォルダーと許可アプリを確認しました。

覚えておきたいこと

バックアップと組み合わせることで、暗号化被害からの復旧に備えます。

Microsoft Defender ファイアウォール

不要なネットワーク通信からパソコンを守ります。

- ［ファイアウォールとネットワーク保護］を開きます。
- 使用中のネットワークを確認します。
- Microsoft Defender ファイアウォールをオンにします。
- 警告がある場合は原因を確認します。

接続できない問題があっても、ファイアウォール全体を切ったままにしません。必要なアプリだけを確認します。

確認：利用中のネットワークでファイアウォールが有効です。



操作の模式図

覚えておきたいこと

会社の端末では、設定を管理者が固定している場合があります。

パブリックとプライベート ネットワーク

周囲の機器から見つけられる範囲を接続場所に合わせます。

- ［設定］＞［ネットワークとインターネット］を開きます。
- 接続中のWi-Fiまたは有線接続を開きます。
- 自宅など信頼できる場所は用途に応じて選びます。
- 店舗やホテルでは［パブリック］を使います。

パブリック ネットワークでは、共有や検出を必要な範囲へ絞ります。

確認：現在の接続場所に合うネットワーク種類です。

覚えておきたいこと

プライベートでは同じネットワークの機器から見つけられる場合があります。

ファイアウォールの許可アプリ

通信を許可するアプリを必要なものへ絞ります。

- ［ファイアウォールによるアプリの許可］を開きます。
- 覚えのないアプリや不要な許可を確認します。
- 必要な場合だけ対象ネットワークを選びます。
- 使わなくなった許可を外します。

ポートを開く操作は、アプリを許可するより危険が大きくなります。理由が分からない設定を追加しません。

確認：必要で信頼できるアプリだけが許可されています。

覚えておきたいこと

知らないアプリへファイアウォールの許可を与えません。

アプリとブラウザーの制御

危険なアプリ、ファイル、サイト、ダウンロードを見分けます。

- ［アプリとブラウザーの制御］を開きます。
- 評判ベースの保護を確認します。
- Smart App Controlの状態を確認します。
- 警告を無視して不明なファイルを実行しません。

確認：利用できる保護機能の状態を確認しました。

覚えておきたいこと

利用できる項目はWindowsの版とインストール状態で異なります。

評判ベースの保護とSmartScreen

既知の危険なサイトや不審なダウンロードを止めます。

- ［評判ベースの保護の設定］を開きます。
- アプリとファイルの確認をオンにします。
- Microsoft EdgeのSmartScreenを確認します。
- 不要な可能性のあるアプリのブロックを確認します。

警告が出たファイルを、発行元や入手先を確認せず実行しません。

確認：SmartScreenと不要アプリの保護を確認しました。

覚えておきたいこと

正規アプリでも誤検出の可能性があります。公式配布元と署名を確認します。

Smart App Control

信頼できないアプリの実行を防ぎます。

- ［アプリとブラウザーの制御］を開きます。
- ［Smart App Controlの設定］を確認します。
- ［オン］または［評価］なら状態を維持します。
- ［オフ］の場合は再設定の条件を確認します。

Smart App ControlはWindows 11の新規インストールなど条件があります。一度オフにすると、再インストールやリセットが必要な場合があります。

確認：表示された状態と制限を確認しました。

覚えておきたいこと

この機能が表示されなくても、DefenderやSmartScreenの確認を続けます。

デバイス セキュリティ

ハードウェアを使った保護機能の状態を確認します。

- ［Windows セキュリティ］を開きます。
- ［デバイス セキュリティ］を開きます。
- コア分離、セキュリティ プロセッサ、セキュア ブートを確認します。
- 警告があれば機種のサポート情報を確認します。

確認：利用できるハードウェア保護を確認しました。

覚えておきたいこと

表示項目はCPU、TPM、UEFI、Windowsの版により異なります。

コア分離とメモリ整合性

重要なWindowsプロセスを不正なドライバーから守ります。

- ［デバイス セキュリティ］を開きます。
- ［コア分離の詳細］を開きます。
- ［メモリ整合性］の状態を確認します。
- 互換性のないドライバーは更新を探します。

動かない機器があっても、原因を確認せず保護を切りません。メーカーの更新ドライバーを先に探します。

確認：メモリ整合性とドライバーの状態を確認しました。

覚えておきたいこと

有効化や変更後に再起動が必要な場合があります。

TPMとセキュア ブート

起動前の改ざんと暗号化キーをハードウェアで守ります。

- ［デバイス セキュリティ］を開きます。
- ［セキュリティ プロセッサ］でTPMを確認します。
- セキュア ブートの状態を確認します。
- 無効の場合はPCメーカーの手順を確認します。

UEFIやBIOSの変更を誤ると起動できない場合があります。BitLocker回復キーを確認し、メーカー手順に従います。

確認：TPMとセキュア ブートの状態を確認しました。

覚えておきたいこと

Windows 11ではTPM 2.0とセキュア ブート対応がシステム要件に含まれます。

サインイン オプション

自分に合う安全なサインイン方法を選びます。

- ［設定］＞［アカウント］を開きます。
- ［サインイン オプション］を開きます。
- 顔、指紋、PINなど利用できる方法を確認します。
- 離席後に再サインインを求める設定を確認します。

確認：利用中のサインイン方法と予備手段を確認しました。



操作の模式図

覚えておきたいこと

使える方法はカメラ、指紋センサー、組織ポリシーにより異なります。

Windows HelloとPIN

端末に結び付いた方法でWindowsへサインインします。

- ［サインイン オプション］を開きます。
- ［PIN（Windows Hello）］を設定します。
- 対応機器では顔認証や指紋認証も設定します。
- 他人にPINを見せず、推測しにくい値にします。

PINはMicrosoftアカウントのパスワードとは別です。忘れた場合の回復方法も確認します。

確認：Windows Helloのサインイン方法を確認しました。

覚えておきたいこと

共有PCでは利用者ごとに別のWindowsアカウントを作ります。

Microsoftアカウントの2段階認証

パスワードが知られても追加確認でアカウントを守ります。

- account.microsoft.com/security を開きます。
- サインイン方法の管理を開きます。
- 2段階認証を有効にします。
- 認証アプリと予備の連絡方法を確認します。

確認コードや承認通知を他人へ渡しません。予備の連絡方法が古いままになっていないか確認します。

確認：2段階認証と予備の方法を確認しました。

覚えておきたいこと

会社や学校のアカウントでは、組織が指定するMFA設定を使います。

画面ロックと動的ロック

離席中に他人がパソコンを操作するのを防ぎます。

- 離席時はWindowsキーとLキーでロックします。
- ［サインイン オプション］を開きます。
- 必要ならスマートフォンをBluetoothで接続します。
- ［動的ロック］を有効にして動作を確認します。

動的ロックは補助機能です。離席時は自分で画面をロックします。

確認：画面ロックと再サインインを確認しました。

覚えておきたいこと

Microsoftによると、動的ロックは端末がBluetooth範囲外になると約1分以内にロックします。

デバイスの検索

紛失したパソコンの位置確認と遠隔ロックに備えます。

- MicrosoftアカウントでWindowsへサインインします。
- ［設定］＞［プライバシーとセキュリティ］を開きます。
- ［デバイスの検索］をオンにします。
- account.microsoft.com/devices で対象端末を確認します。

事前にデバイスの検索と位置情報を有効にする必要があります。会社の端末では管理者へ連絡します。

確認：Microsoftアカウントに対象端末が表示されます。

覚えておきたいこと

盗難では自分で回収せず、警察や保険会社へ端末情報を伝えます。

デバイス暗号化とBitLocker

紛失や盗難時に、ディスクを外して読まれるのを防ぎます。

- ［設定］＞［プライバシーとセキュリティ］を開きます。
- ［デバイスの暗号化］を確認します。
- Proでは［BitLockerドライブ暗号化］も確認します。
- 暗号化の状態と対象ドライブを確認します。

エディションや機種により表示が異なります。設定変更前に回復キーを保管します。

確認：システムドライブの暗号化状態を確認しました。



操作の模式図

覚えておきたいこと

デバイス暗号化は自動で有効になる場合があります。

BitLocker回復キー

暗号化されたドライブを回復できるようにします。

- 回復キーIDと保管先を確認します。
- Microsoftアカウントの回復キーページを確認します。
- 会社・学校の端末は管理者へ確認します。
- PC本体とは別の安全な場所にも保管します。

Microsoftサポートは失われた回復キーを再作成できません。キーがなければデータへアクセスできない場合があります。

確認：対象端末の回復キーを取り出せます。

覚えておきたいこと

回復画面ではキーIDを確認し、対応する48桁の回復キーを使います。

Windows バックアップとOneDrive

故障、紛失、初期化の前にファイルと設定を保存します。

- ［設定］＞［アカウント］＞［Windows バックアップ］を開きます。
- アプリ、設定、資格情報のバックアップを確認します。
- OneDriveでデスクトップやドキュメントを保護します。
- 復元できることと保存容量を確認します。

同期は削除も反映する場合があります。重要データは別媒体や別サービスにも複製します。

確認：重要なファイルと設定のバックアップ先を確認しました。

覚えておきたいこと

Windows バックアップとOneDriveで保存される内容は同じではありません。

回復オプションと復元ポイント

更新やソフトの問題から戻せる準備をします。

- ［設定］＞［システム］＞［回復］を開きます。
- 利用できる回復方法を確認します。
- システムの保護と復元ポイントを確認します。
- 回復前にバックアップとBitLocker回復キーを確認します。

回復方法により、アプリや設定、ファイルが消える場合があります。実行前に影響を確認します。

確認：使える回復方法と必要なキーを確認しました。

覚えておきたいこと

感染が疑われる場合は、信頼できる回復メディアからの再インストールも検討します。

アプリの権限

アプリが使える機器と個人情報を必要な範囲へ絞ります。

- ［設定］＞［プライバシーとセキュリティ］を開きます。
- ［アプリのアクセス許可］を確認します。
- 位置情報、カメラ、マイクなどを順に開きます。
- 不要なアプリの権限をオフにします。

デスクトップ アプリは、個別のスイッチで制御できない場合があります。アプリ側の設定も確認します。

確認：不要なアプリ権限を見直しました。

覚えておきたいこと

必要な機能が動かない場合は、使用時だけ権限を戻して確認します。

カメラ・マイク・位置情報

映像、音声、現在地を使えるアプリを把握します。

- ［プライバシーとセキュリティ］を開きます。
- カメラとマイクを使えるアプリを確認します。
- 位置情報とデバイスの検索の関係を確認します。
- タスクバーのマイク表示やカメラ ランプを確認します。

Windows Helloはアプリのカメラ権限をオフにしても顔認証でカメラを使う場合があります。

確認：必要なアプリだけに権限があります。

覚えておきたいこと

位置情報をオフにすると、デバイスの検索など一部機能が使えなくなります。

標準ユーザーと管理者

ソフトのインストールや重要設定を変更できる人を絞ります。

- ［設定］＞［アカウント］＞［他のユーザー］を開きます。
- 管理者になっている利用者を確認します。
- 日常利用は標準ユーザーを検討します。
- 使わないアカウントを削除または無効にします。

アカウント削除では、その利用者のローカルデータが消える場合があります。先に必要なファイルを確認します。

確認：必要な利用者だけが管理者です。

覚えておきたいこと

Microsoftは管理者を少数にし、日常作業では標準ユーザーを使う方法を案内しています。

リモート接続と共有機能

外部や周囲の機器から接続できる入口を減らします。

- ［設定］＞［システム］＞［リモート デスクトップ］を確認します。
- 使わない場合はオフにします。
- ［近距離共有］は［自分のデバイスのみ］を検討します。
- ネットワーク共有と共有フォルダーも確認します。

リモート デスクトップの受信機能はWindows Proが対象です。遠隔サポートは自分から依頼した信頼できる相手だけに許可します。

確認：必要な共有とリモート機能だけが有効です。

覚えておきたいこと

公衆Wi-Fiでは近距離共有とネットワーク共有をオフにします。

感染が疑われるときの対応

被害の拡大を止め、信頼できる状態へ戻します。

- Wi-Fiや有線LANを切り、通信を止めます。
- 警告画面、日時、ファイル名を記録します。
- Windows セキュリティで更新後にフルまたはオフライン スキャンします。
- 直らない場合は専門担当へ相談し、回復や再インストールを検討します。

画面に表示された電話番号へ連絡しません。別の安全な端末から重要アカウントのパスワード変更と2段階認証を行います。

確認：通信、記録、スキャン、相談先を確認しました。



操作の模式図

覚えておきたいこと

会社・学校の端末では、電源を切る前に情報システム担当者の指示を受けます。

公式情報の出典（1）

出典 S01　Windows 10のサポート終了

出典 S02　Windows Updateをインストール

出典 S03　ドライバーの更新

出典 S04　Windows Updateのアクティブ時間

出典 S05　ウイルスと脅威の防止

出典 S06　ファイアウォールとネットワーク保護

出典 S07　ファイアウォールでアプリを許可する危険

出典 S08　アプリとブラウザーの制御

各項目名をクリックすると公式ページが開きます。

覚えておきたいこと

確認日：2026年9月20日。Microsoft公式サポートを参照しています。Windowsの版、エディション、機種、組織管理により画面や条件は異なります。

公式情報の出典（2）

出典 S09　Windows セキュリティのデバイス セキュリティ

出典 S10　Windowsのサインイン オプション

出典 S11　Microsoftアカウントの2段階認証

出典 S12　紛失したWindows端末を探してロック

出典 S13　BitLockerの概要

出典 S14　BitLocker回復キーを探す

出典 S15　Windows バックアップの設定

出典 S16　OneDriveで重要フォルダーをバックアップ

各項目名をクリックすると公式ページが開きます。

覚えておきたいこと

確認日：2026年9月20日。Microsoft公式サポートを参照しています。Windowsの版、エディション、機種、組織管理により画面や条件は異なります。

公式情報の出典（3）

出典 S17　Windowsの回復オプション

出典 S18　Windowsのアプリ権限

出典 S19　カメラ、マイク、プライバシー

出典 S20　位置情報サービスとプライバシー

出典 S21　Windowsのユーザー アカウント管理

出典 S22　リモート デスクトップの使い方

出典 S23　近距離共有の設定

出典 S24　不要なソフトウェアからPCを保護

各項目名をクリックすると公式ページが開きます。

覚えておきたいこと

確認日：2026年9月20日。Microsoft公式サポートを参照しています。Windowsの版、エディション、機種、組織管理により画面や条件は異なります。