Windows11 フォルダ暗号化・パスワード設定チェックリスト

※この資料は2025年12月時点の情報を参考に制作しております。
※この資料は参考情報として提供するものです。法令への適合性については、必ずご自身の責任において確認・判断してください。この資料の利用によって生じたいかなる法的問題についても、当方は責任を負いかねます。
※2025年12月24日

Money Forward クラウド

事前確認（方式選定）

チェック	確認事項
☐	保護目的（紛失・盗難対策／共有PCでの覗き見防止／最重要データ管理）を整理した -補足：目的により「暗号化」か「アクセス制御」か「専用ソフト」かを選ぶ
☐	WindowsエディションがPro以上かHomeかを確認した -補足：EFSはPro以上での利用を前提とする（Homeは別の手段を使う）
☐	「フォルダにパスワードを設定したい」の意味を整理した（ログイン連動／別パスワード要求／第三者PCからの解析耐性） -補足：EFSはログインアカウントに紐づくため、“フォルダ単体の独立パスワード”とは性質がるため、「暗号化の証明書とキー」を物理的なUSBメモリ等にバックアップしておく

フォルダ内容を暗号化する（EFS：Pro以上）

チェック	確認事項
☐	保護したいフォルダを右クリックし、「プロパティ」を開いた
☐	「全般」→「詳細設定」を開いた
☐	「内容を暗号化してデータをセキュリティで保護する」にチェックし、OKを押した
☐	プロパティに戻って「適用」を押し、適用範囲で「このフォルダー、サブフォルダーおよびファイル」を選択して確定した -補足：暗号化対象がフォルダ配下全体になっていること
☐	EFSの制約を理解した（同一PCで同一アカウントでログインできれば閲覧され得る／別アカウント・別PCからは原則アクセス不可） -補足：運用上の“想定脅威”に合っていること
☐	OS再インストールやアカウント情報破損等で開けなくなるリスクを認識した

暗号化キー／回復手段のバックアップ（EFS等）

チェック	確認事項
☐	暗号化キー（証明書・回復キー等）が必要になるケース（故障／OS不具合／アカウント破損）を想定した
☐	暗号化キー／回復キー等を外部USBメモリやクラウド等、PC本体とは別の場所にバックアップした
☐	バックアップの保管場所（誰が・どこで・どう管理するか）を記録した

アクセスできるアカウントを制限する（アクセス制御）

チェック	確認事項
☐	保護したいフォルダを右クリックし、「プロパティ」を開いた
☐	「セキュリティ」タブ→「編集」を開いた
☐	制限したい特定のユーザー（アカウント名）を選択し、アクセス許可で「フルコントロール：拒否」を設定して適用した

Homeエディションでの標準機能

チェック	確認事項
☐	端末でDeviceEncryptionが利用可能かを確認した
☐	DeviceEncryptionを使う場合、回復情報の保存先を決めた -補足：回復情報を失うと復旧できないリスクがある

圧縮ソフトでパスワードを設定する

チェック	確認事項
☐	入手元・提供元が明確である圧縮ソフトを準備した
☐	暗号化したいフォルダ／ファイルを圧縮し、暗号化欄にパスワードを設定して圧縮ファイルを作成した
☐	作成した圧縮ファイルを開く際にパスワード入力が求められることを確認した
☐	保護後に、元のフォルダが残っていないか確認し、必要に応じて元データを完全に削除した

フォルダ暗号化ソフトを導入する

チェック	確認事項
☐	「仮想的な暗号化ドライブ」型で運用する方針を理解した（パスワードがないと開けない領域に保存する）
☐	利用するソフトの信頼性を確認した（提供元が明確／実績・利用者が多い等）
☐	初期設定の手間（作成・マウント・運用手順）を作業手順として残した
☐	重要データ（財務データ／顧客情報など）を暗号化領域内に保存する運用になっていることを確認した

運用ルール（パスワード・鍵・復旧）

チェック	確認事項
☐	パスワードを忘れない運用（管理ツール利用／安全な場所への記録）を決めた
☐	暗号化キー・回復キー等が発生する方式では、バックアップが「デジタル」と「アナログ」で完了していることを再確認した
☐	万が一の復旧手順（誰が、どの媒体から、どう復旧するか）を簡潔に文書化した

フォルダ保護とあわせて行うPC全体の対策

チェック	確認事項
☐	Windowsログインパスワードを推測されにくいものに設定し、運用ルール（変更頻度等）を決めた
☐	Windows Hello（指紋／顔）を利用する場合、設定が完了していることを確認した
☐	多要素認証（MFA）を導入する場合、方式選定上の注意（SMSにはSIMスワップなどのリスクがあること）を理解した
☐	3-2-1 ルールでバックアップ（ランサムウェア／故障対策）を実施する運用になっていることを確認した

チェック漏れ防止のための注意事項

チェック	注意事項
☐	アクセス制御は管理者権限で変更され得るため、脅威モデル（誰から守るか）を先に決めるべきである
☐	圧縮のパスワード保護を使う場合、元データが残ると保護が破綻するため削除まで含めて運用する
☐	暗号化キー／回復キーのバックアップを失うと、本人でも復旧不能になり得る
☐	フォルダ保護だけで完結せず、PCのログインパスワード強化と3-2-1 ルールによるバックアップもセットで運用する

※2025年12月時点の情報をもとに作成しています