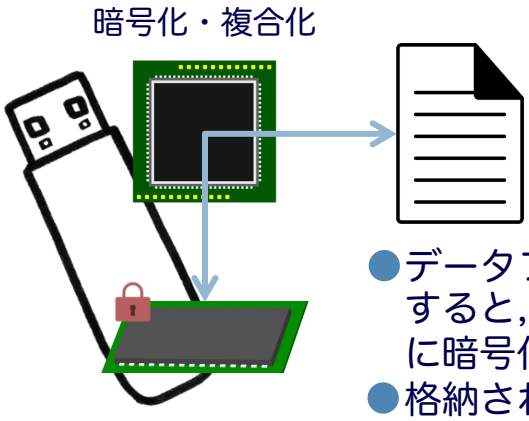
USBフラッシュメモリ利用ガイド

USBフラッシュメモリ（USBメモリ）を安心安全に利用できるように，万が一紛失や盗難にあった際も意図していない他の人（他人）に，中に入っているデータを意味ある情報として見らないようにするガイドです．

AI& ICT
×
教員養成

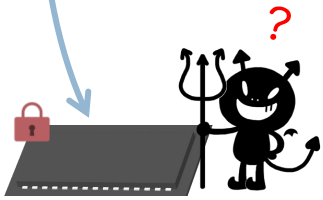
ハードウェア暗号化は必須です

他人に見られては困る情報を入れたいならば，必ずハードウェア暗号化機能があるものを使いましょう．



- データファイルを書き込もうとすると，メモリに記録される前に暗号化が行われます．
- 格納されているデータファイルを読み出そうとすると，その都度複合化（暗号化の解除）が行われます．

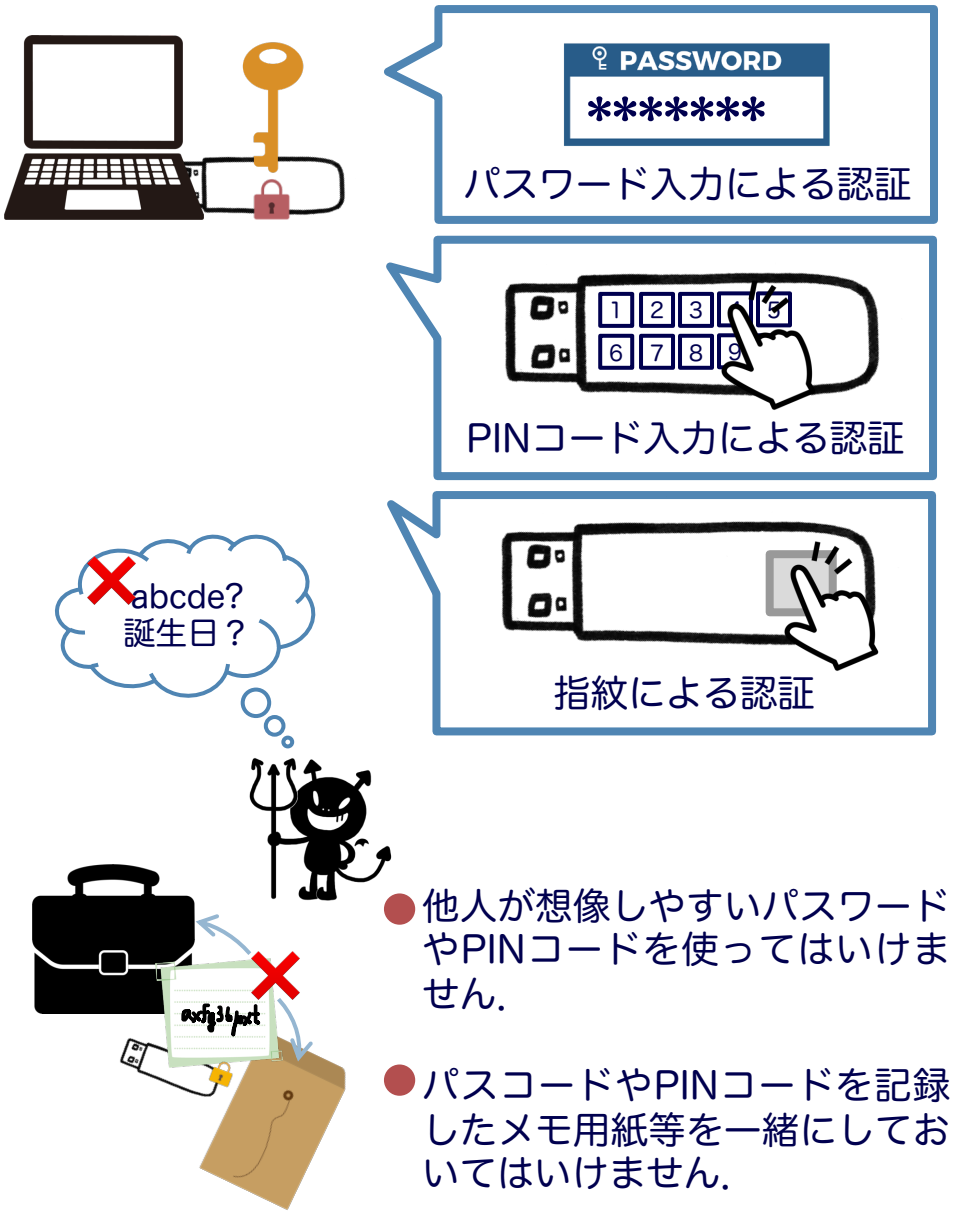
- データファイルを読み書きするためにOSにドライブ（リムーバブルメディア）として認識させるには認証が必要です．



USBメモリを分解して，メモリ部分を取り出してもまず解読することは不可能です．

ハードウェア暗号化でも認証が重要です

ハードウェア暗号化機能を使う際も，他人が認証を成功させないようにすることが必須です．



- 他人が想像しやすいパスワードやPINコードを使ってはいけません．
- パスコードやPINコードを記録したメモ用紙等を一緒にしておいてはいけません．

おまけ

ハードウェア暗号化機能を有するUSBメモリ

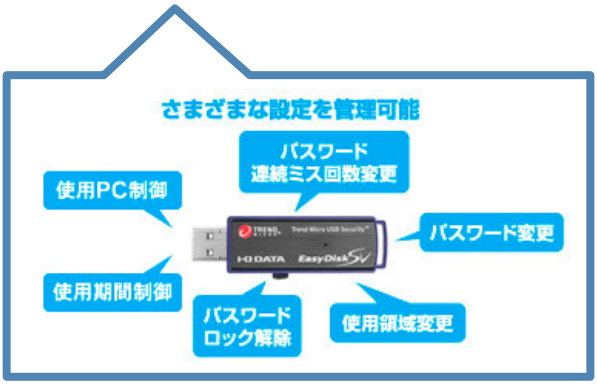
I-O DATA

ED-HB3シリーズ

ハードウェア10キーからのPINコード入力による認証

S4/Rシリーズ

パスワード入力による認証
管理ソフトによる組織での管理が可能



BUFFALO™

RUF3-KVシリーズ

ELECOM
LIFESTYLE INNOVATION

HUD-PUTK3A1シリーズ

おまけ

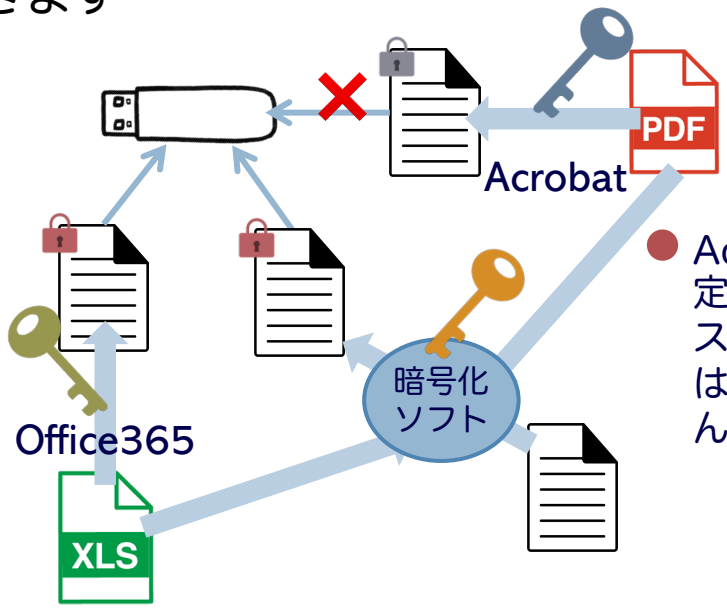
ハードウェア暗号化機能がないUSBメモリは使えない？

他人に見られても問題ない情報しか入れないのであれば，ハードウェア暗号化機能がないものも使って良いでしょう

- 安価なUSBメモリにも付いているソフトウェアの機能による暗号化は簡単に解読できるので，使う意味はありません．

機密ファイルも入れたい！

データファイルを個別に暗号化してから入れることで，他人に見られては困る情報を入れることもできます

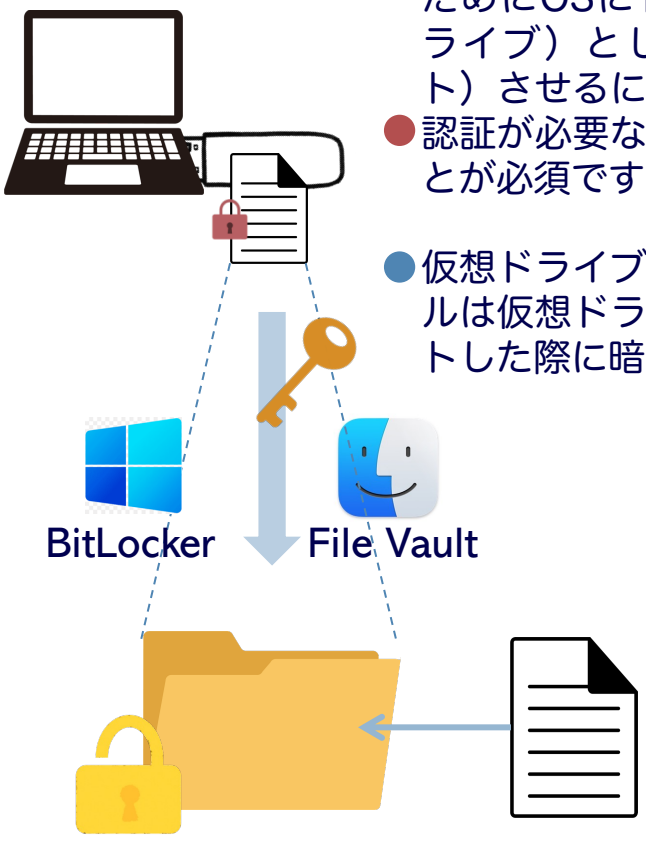


- Acrobat等で設定できるPDFパスワードロックは意味ありません．

おまけ

暗号化仮想ドライブの利用

USBメモリ内に暗号化仮想ドライブを配置することで，ハードウェア暗号化機能のないUSBメモリに他人に見られると困る情報も入れられます

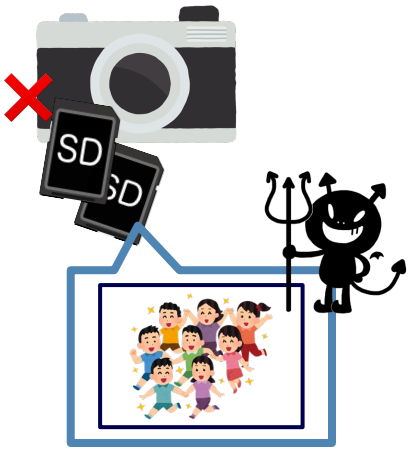


- データファイルを読み書きするためにOSにドライブ（仮想ドライブ）として認識（マウント）させるには認証が必要です.
- 認証が必要なように設定することが必須です
- 仮想ドライブに保存したファイルは仮想ドライブをアンマウントした際に暗号化されます.
- 仮想ドライブがマウントされている状態では暗号化が解除されているので，その状態のPCを他人が触れないように注意が必要です.

おまけ

シビアな動画像を撮影するときはスマホが適しています

他人に見られると困るシビアな動画像を撮影する場合，保存された動画像を見るためには認証が必要となるようにできるタブレット機器やスマートフォンが適しています

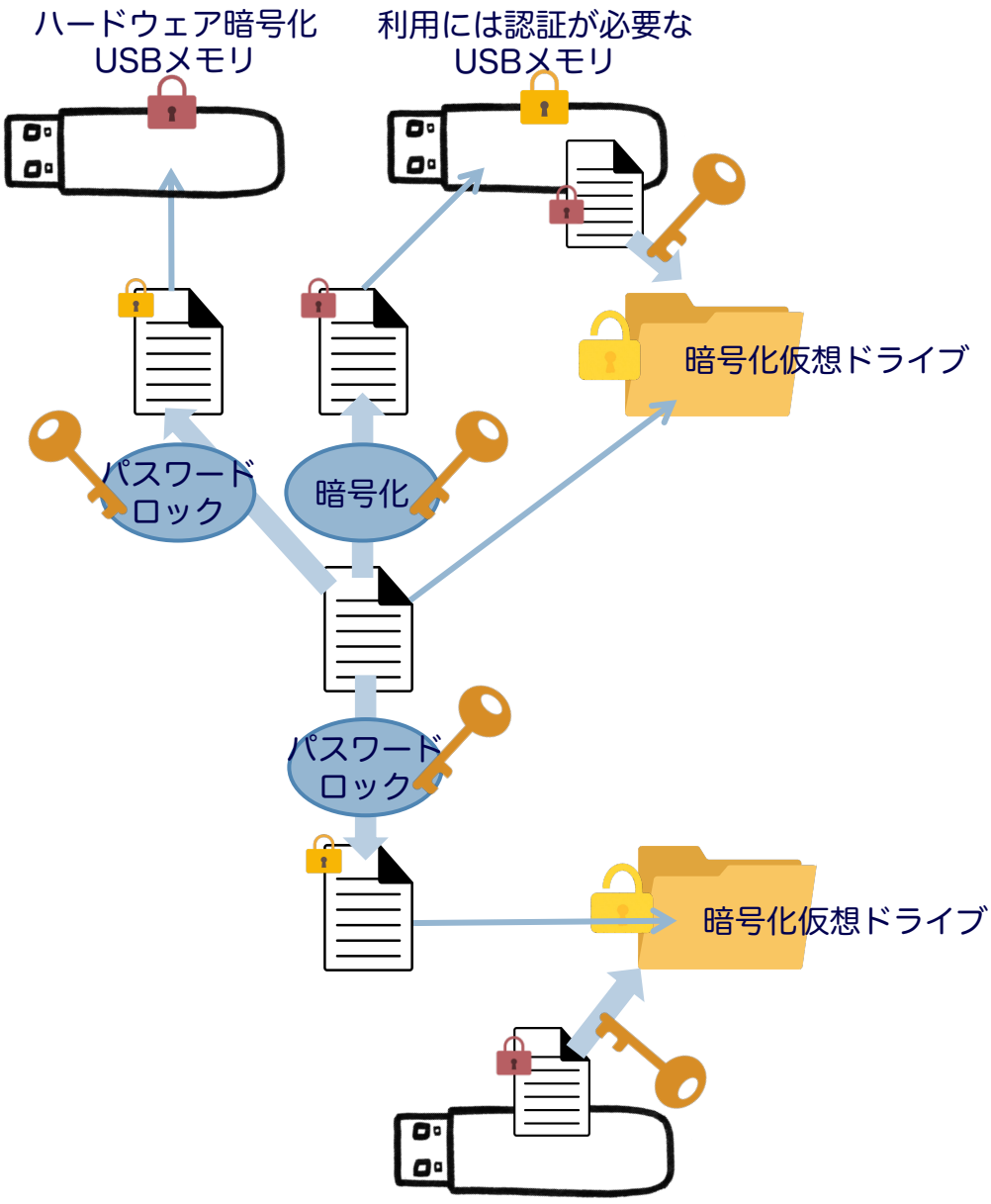


- ほとんどのデジタルカメラは，デジタルカメラ（又はSDカード等の記録メディア）を手にした人が保存されている動画像を容易に見ることができてしまいます．それらハードウェアの十分な管理ができない場合は，シビアな動画像の撮影はしない方が良いでしょう．
- タブレット機器やスマホを使う場合も，機器へのログイン認証の設定と管理をしっかりとすることが重要です．
- 当然ですが，撮影した動画像データファイルがクラウドストレージ等に同期して保存される場合，同期先のセキュリティの設定と管理をしっかりとしてください．

おまけ

東京学芸大学のUSBメモリ利用ルール

２回の認証が必要な場合のUSBメモリの使い方



※最低限のルートを表しています