

USBメモリを安全に持ち歩く **Bit Locker**

USBメモリが盗まれたり、
不正に使用されてもパ
スワードを入力しないと、
読み取りができないよう
にするための設定



BitLockerとは

- Windowsにはじめから標準で付属しているディスク暗号化機能で、USBメモリやSDカードを暗号化し、パソコンに接続後、パスワードを入力しないとアクセスすることが出来ません。
- USBメモリのような持ち運びすることが多い記憶メディアに設定しておくことで、万が一どこかに置き忘れたり、不正に持ちだされてもパスワードを入力しないと保存したファイルを読み書きできません。
- ロックを解除するには、BitLockerの回復キーが必要です。

データの追加

- BitLockerで暗号化されているドライブに新しいファイルやフォルダーを追加すると、ファイルは自動的に暗号化されます。
- 但し、別のドライブやパソコンにファイルをコピーした場合、ファイルは自動的に暗号化解除されます。

BitLockerを起動する①

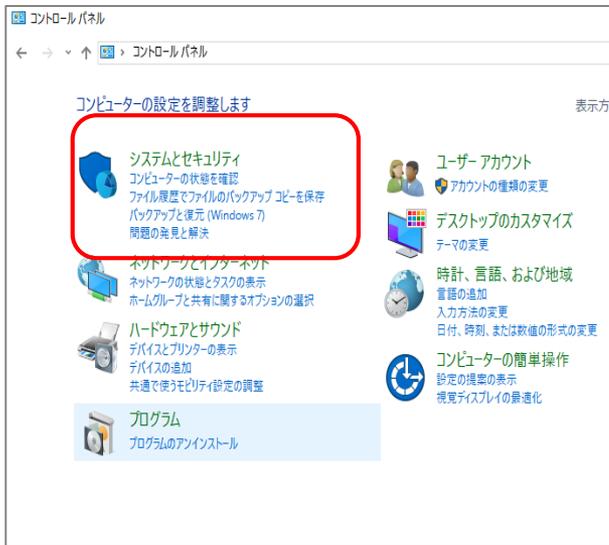
スタート (右クリック)



コントロールパネル



システムとセキュリティ



システムとセキュリティ

→ ↓ ↑ コントロール パネル > システムとセキュリティ

コントロール パネル ホーム

システムとセキュリティ

ネットワークとインターネット

ハードウェアとサウンド

プログラム

ユーザー アカウント

デスクトップのカスタマイズ

時計、言語、および地域

コンピューターの簡単操作



セキュリティとメンテナンス

コンピューターの状態を確認して問題を解決 | ユーザー アカウント制御設定の変更 | コンピューターの一般的な問題のトラブルシューティング



Windows ファイアウォール

ファイアウォールの状態の確認 | Windows ファイアウォールによるアプリケーションの許可



システム

RAM の量とプロセッサの速度の表示 | リモート アクセスの許可 | リモート アシスタンスの起動 | コンピューターの名前の参照



電源オプション

バッテリー設定の変更 | 電源ボタンの動作の変更 | コンピューターがスリープ状態になる時間を変更



ファイル履歴

ファイル履歴でファイルのバックアップ コピーを保存 | ファイル履歴でファイルを復元



バックアップと復元 (Windows 7)

バックアップと復元 (Windows 7) | バックアップからファイルを復元



BitLocker ドライブ暗号化

BitLocker の管理



記憶域

記憶域の管理



ワーク フォルダー

ワーク フォルダーの管理



管理ツール

ディスク領域の解放 | ドライブのデフラグと最適化 | ハード ディスク パーティションの作成とフォーマット | イベント ログの表示 | タスクのスケジュール



Flash Player

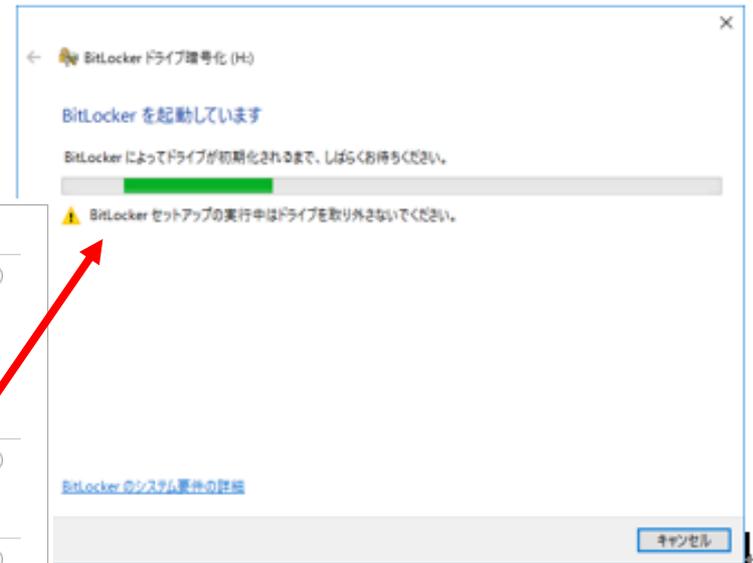
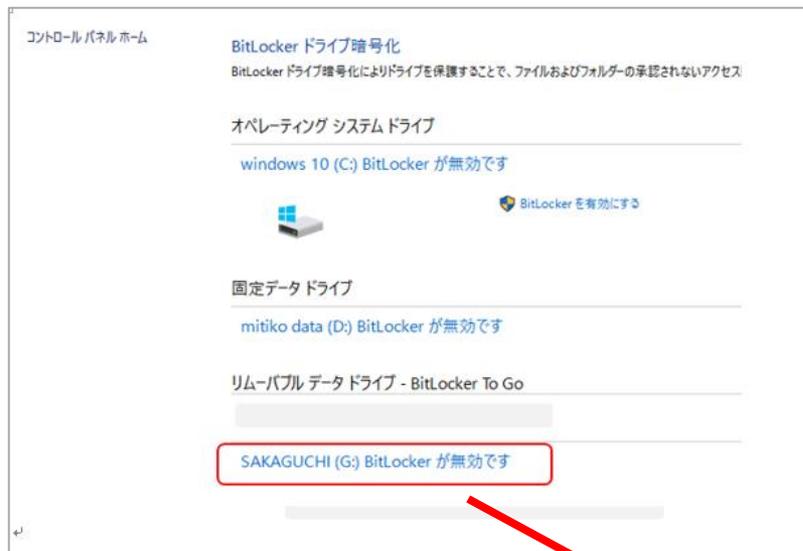
BitLockerを起動する ②

Windows検索ボックス
を利用する

Windows検索ボックス
に「BitLocker」と入
力して、[BitLockerの
管理]をクリックします



USBメモリをポートに差し込んでおきます。



BitLockerが起動
され、ドライブ
暗号化の準備を
開始します。

パスワードは大小文字、数字、記号で 8桁以上 (7桁以下はエラーメッセージが出る)

エラーメッセージ

BitLocker ドライブ暗号化 (H:)

このドライブのロック解除方法を選択する

入力したパスワードは、長さの最小要件を満たしていません。

パスワードを使用してドライブのロックを解除する(P)
パスワードには大文字、小文字、数字、空白文字、記号を含めてください。

パスワードを入力してください(E)

パスワードをもう一度入力してください(R)

スマートカードを使用してドライブのロックを解除する(S)
スマートカードを挿入する必要があります。ドライブのロックを解除するときは、スマートカードの PIN が必要です。

次へ(N) キャンセル

BitLocker ドライブ暗号化 (H:)

このドライブのロック解除方法を選択する

パスワードを使用してドライブのロックを解除する(P)
パスワードには大文字、小文字、数字、空白文字、記号を含めてください。

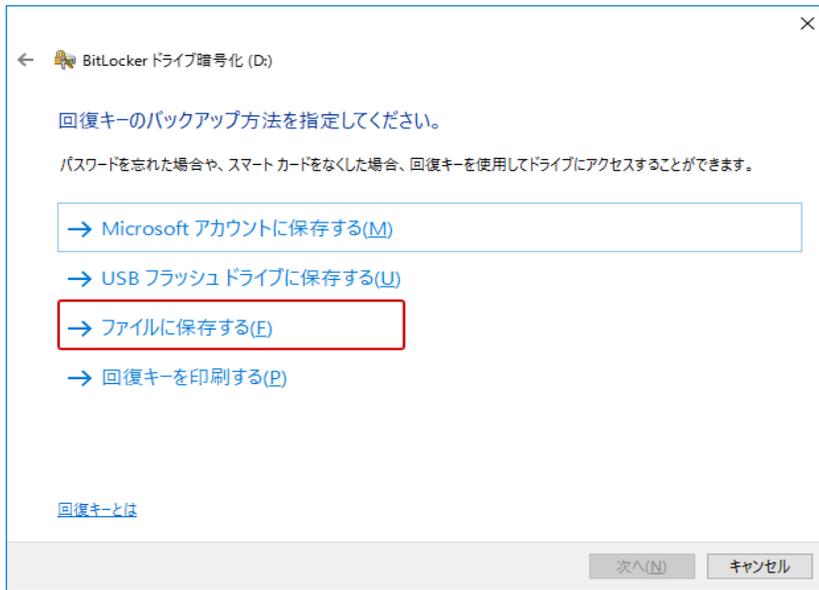
パスワードを入力してください(E)

パスワードをもう一度入力してください(R)

スマートカードを使用してドライブのロックを解除する(S)
スマートカードを挿入する必要があります。ドライブのロックを解除するときは、スマートカードの PIN が必要です。

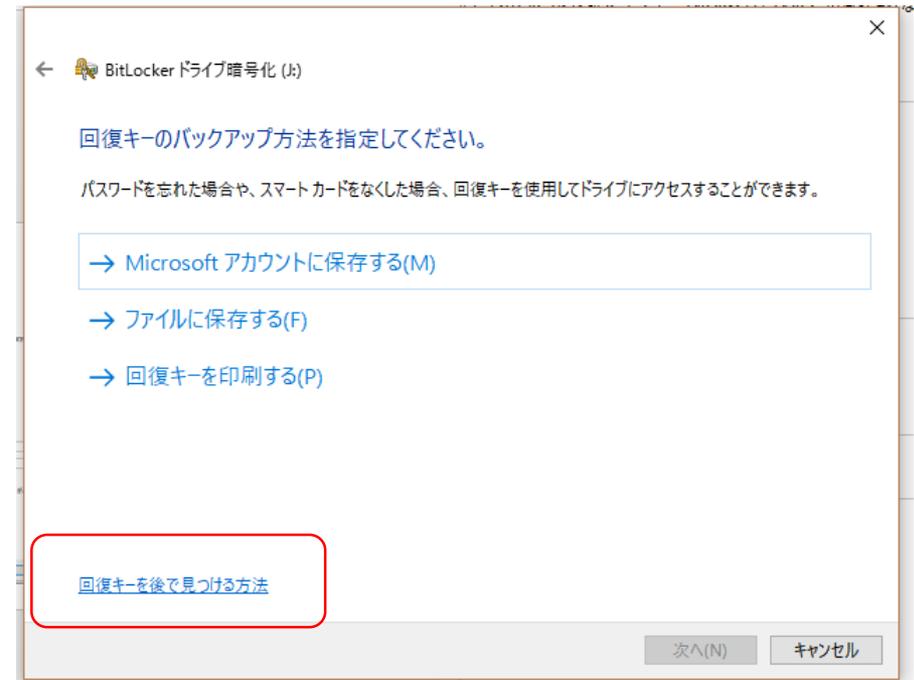
サンプル用PW: **passo12345**

次へ(N) キャンセル

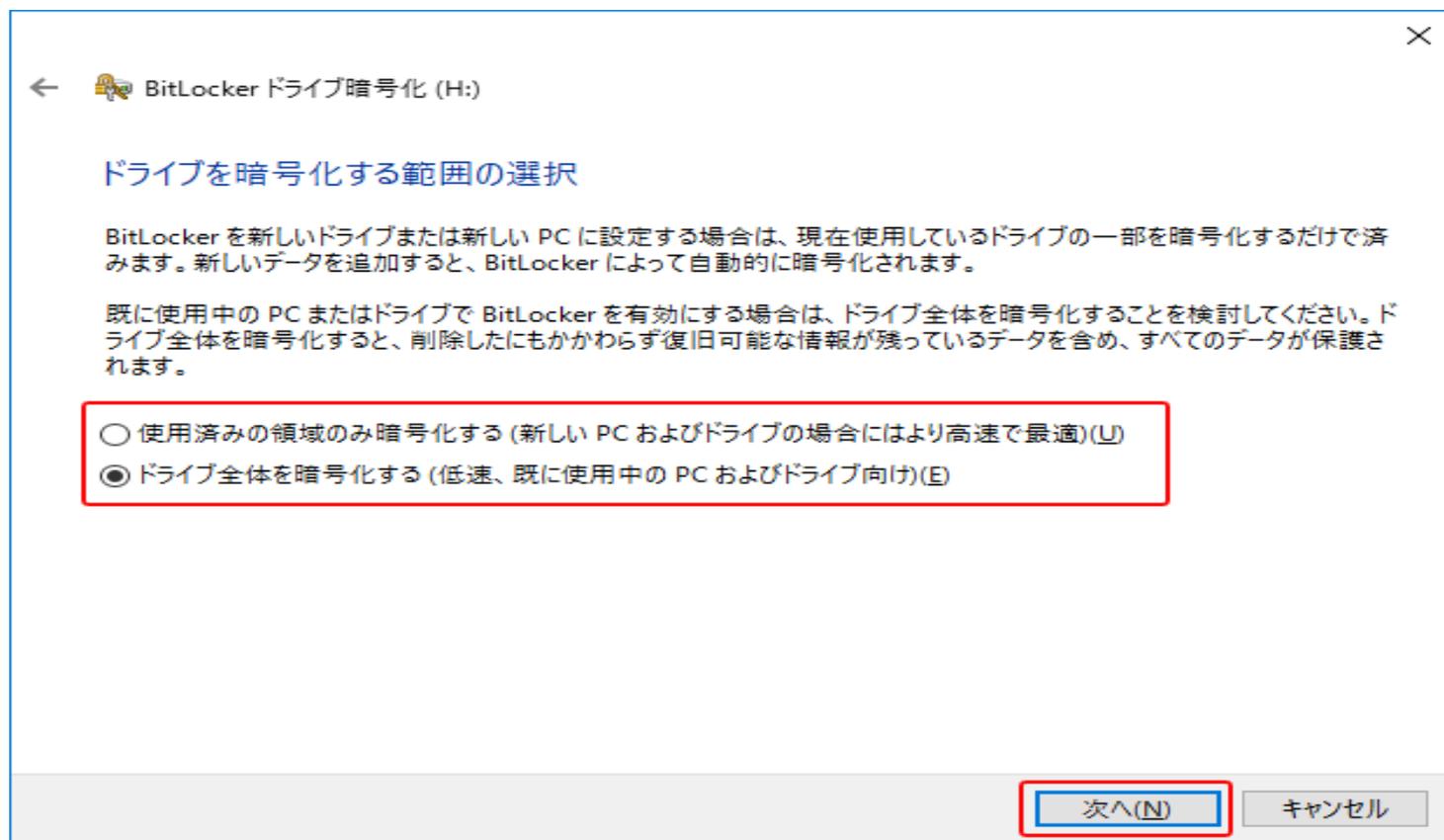


① 回復キーを保存する任意のフォルダーを指定

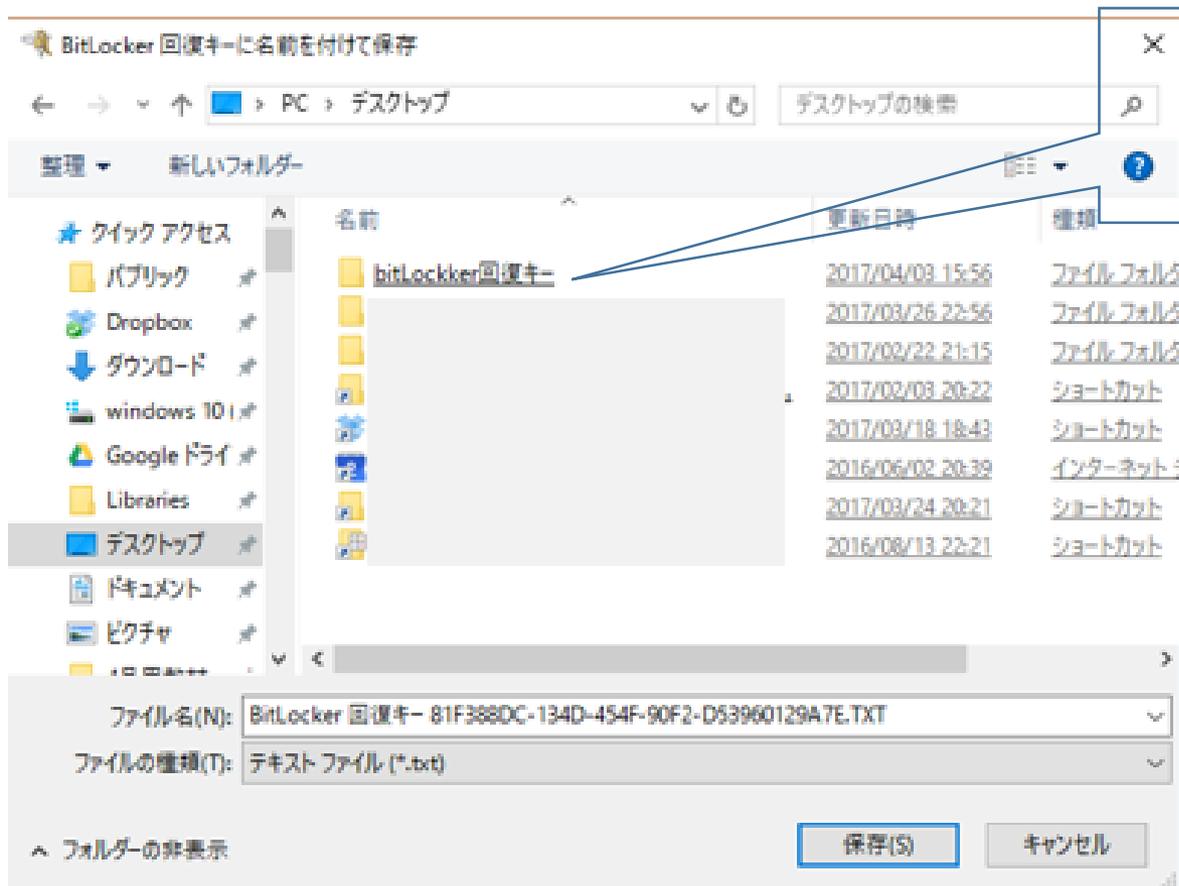
例) テキストファイル(.txt)として保存



ドライブを暗号化する範囲を選択します。「使用済みの領域のみ暗号化する」か「ドライブ全体を暗号化する」か、どちらかを選び「次へ」をクリックします。

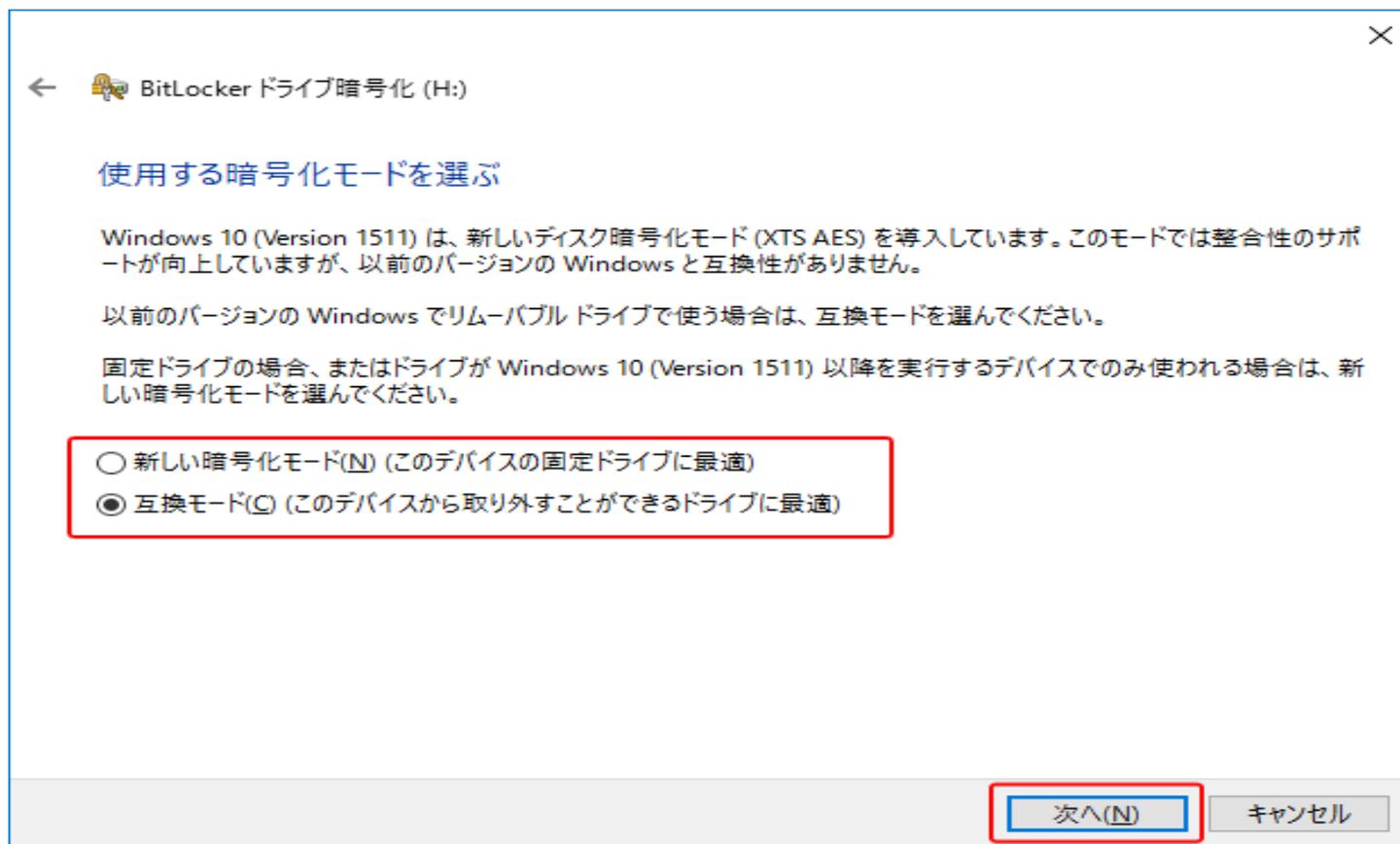


『デスクトップのファイルに保存』を選択(スライドNO.9)



『BitLocker回復キー』
フォルダに保存

次に、使用する暗号化モードを選択し「次へ」をクリックします。



これで暗号化する準備が整いましたので、
「暗号化の開始」ボタンをクリックします。



USBメモリードライブの暗号化が始まります。

BitLocker ドライブ暗号化



暗号化しています...

ドライブ G 99.1% 完了



一時停止(P)



ドライブを取り外す前に、暗号化を一時停止してください。ドライブ内のファイルが破損する可能性があります。

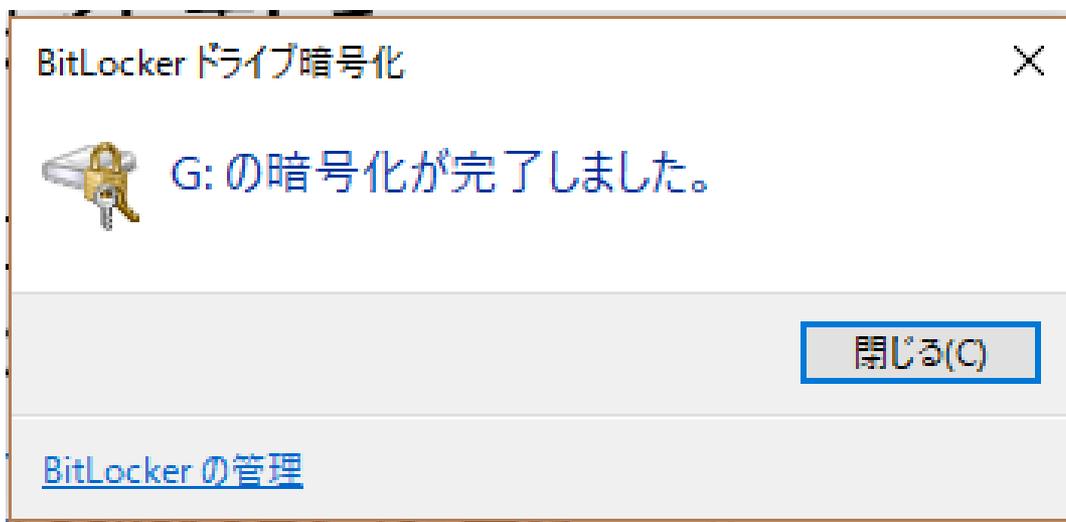
[BitLocker の管理](#)

途中でドライブを取り外す場合は「一時停止」ボタンをクリック

暗号化が完了しました。

完了まで約16分ほど掛かりました。(旧VISTA機USBポート2.0)

通常のCやD内臓ドライブの場合、ハードディスクの状況によって違いますが軽く1時間はかかります。



時間に余裕のある時にこの作業をするのがいいでしょう

↑  > コントロール パネル > システムとセキュリティ > BitLocker ドライブ暗号化

パネル ホーム

BitLocker ドライブ暗号化

BitLocker ドライブ暗号化によりドライブを保護することで、ファイルおよびフォルダーの承認されない。

オペレーティング システム ドライブ

windows 10 (C:) BitLocker が無効です



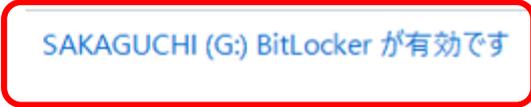
 BitLocker を有効にする

固定データ ドライブ

mitiko data (D:) BitLocker が無効です

リムーバブル データ ドライブ - BitLocker To Go

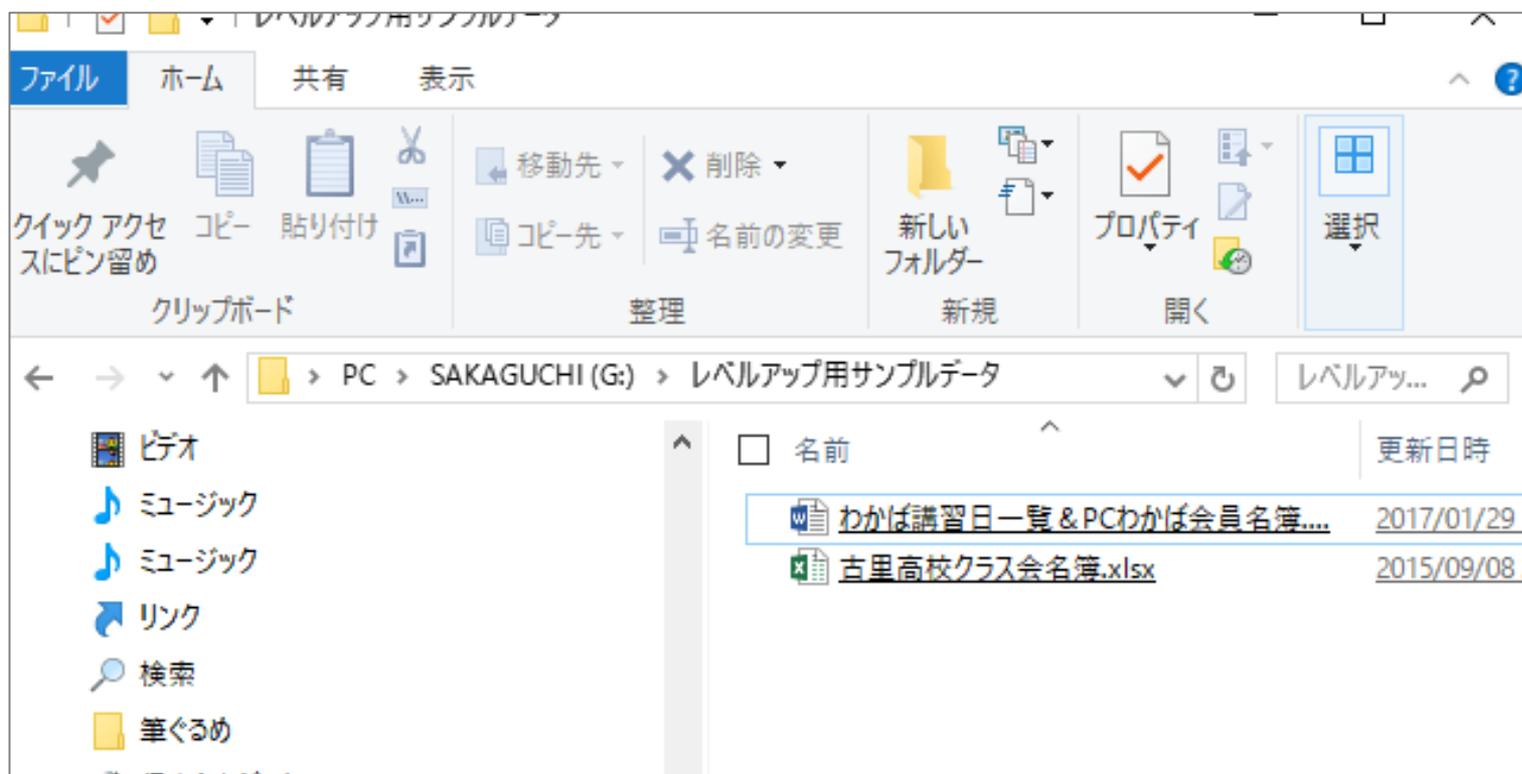
 (F:) BitLocker が無効です

 SAKAGUCHI (G:) BitLocker が有効です

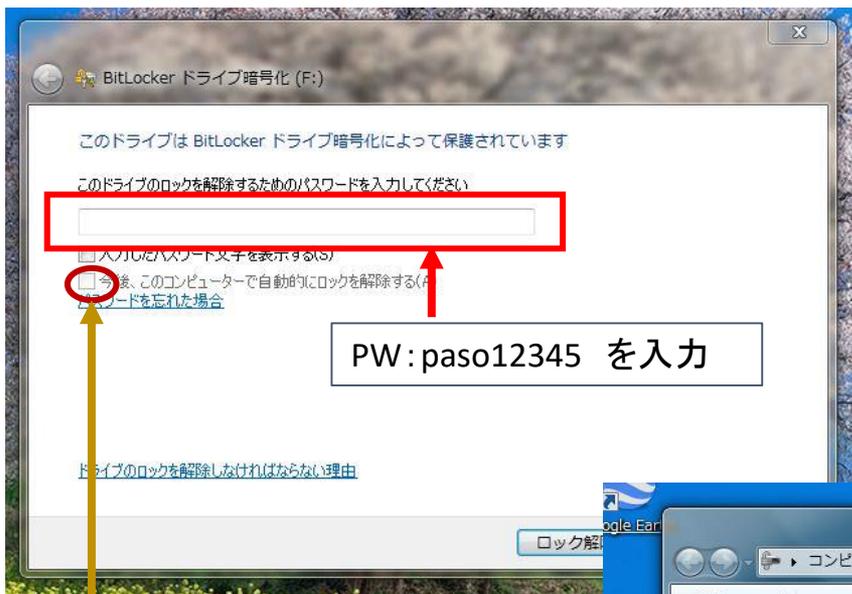
Bitlockerの設定をしていないUSB メモリ

Bitlockerの設定をしているUSB メモリ

Bit locker設定したパソコンでUSBメモリを開いた場合

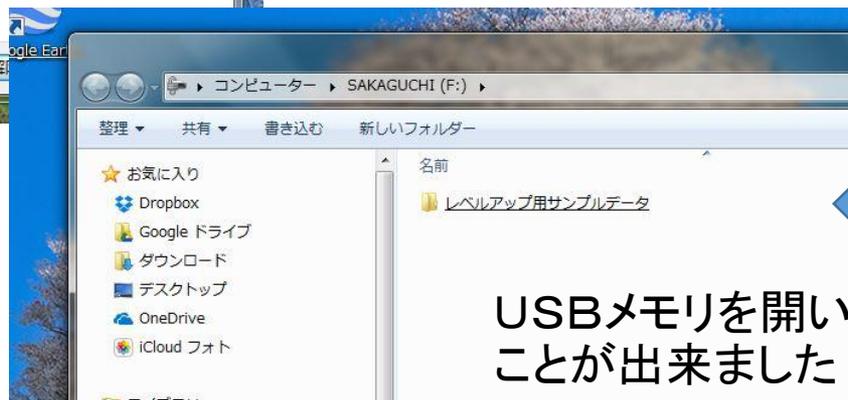


別のパソコンでUSBメモリを開いた場合



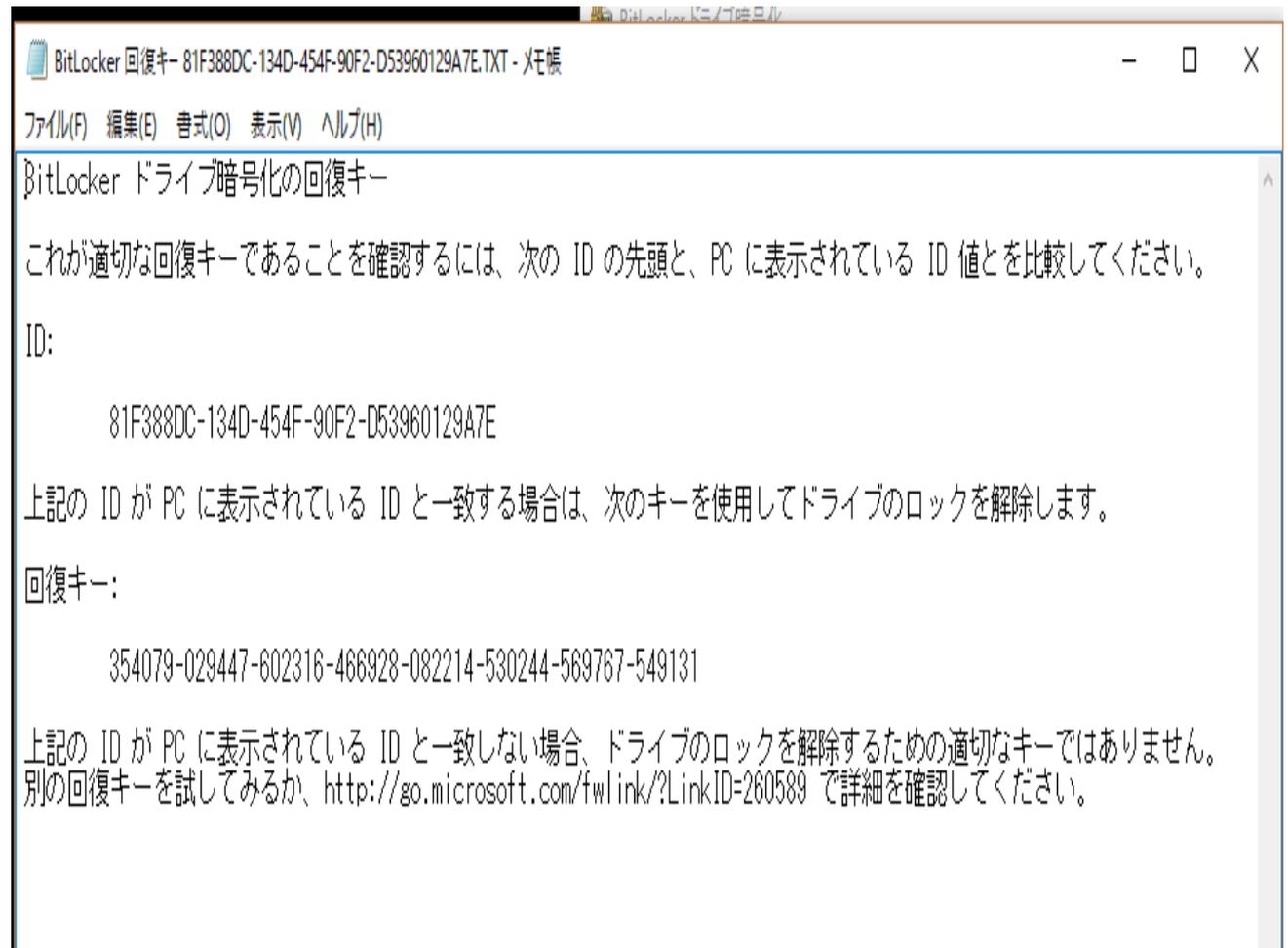
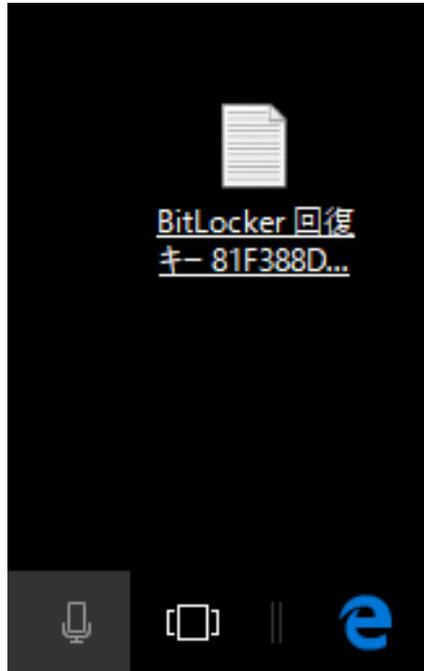
PW: paso12345 を入力

今後も使用するPCの場合は『今後もこのPCで使用する』に☑を付けると以降のPW入力を不要にする事ができる

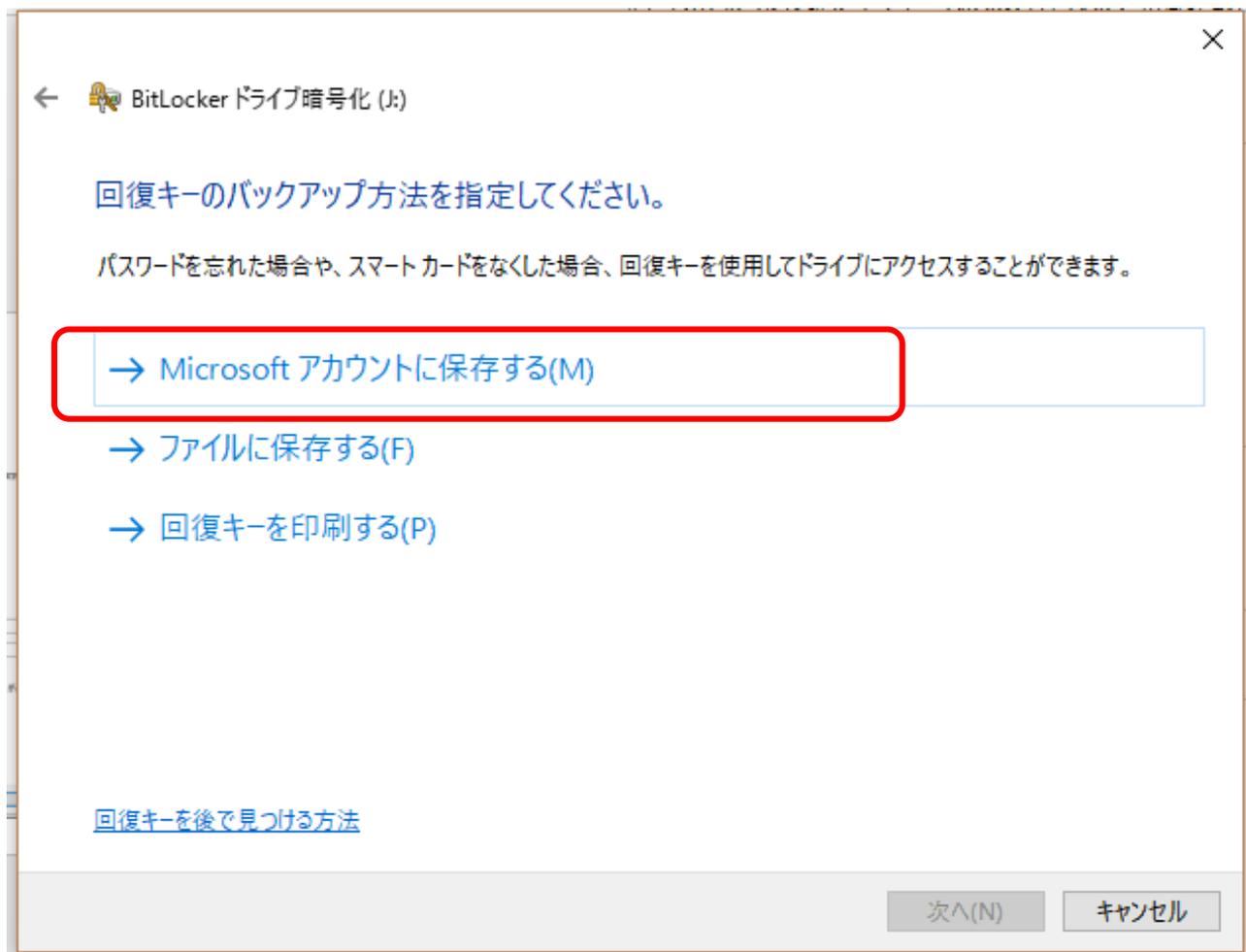


USBメモリを開いてデータを見ることが出来ました

デスクトップにテキストで保存した暗号化の回復キー



Microsoftアカウントに保存した暗号化の回復キー



- Microsoft アカウントに保存した場合。[BitLocker 回復キー] に移動します。



サインイン

Microsoft アカウントを使用してください。
Microsoft アカウントとは?

次へ

アカウントをお持ちでない場合、作成できます。

[利用規約](#) [プライバシーと Cookie](#)
Microsoft

ところで、

Windows標準に付属のBitLockerと
なっていますが
homeエディションにはこの機能が
ないことがわかりました。

Windows10 のhomeとPROの違い

HomeとProの違いは、

Homeが一般ユーザー向け

Proは一般ユーザー及びスモールビジネス向けと定義づけられています。

Windows 10 Homeから Windows 10 Proに乗り換える。

スタート → 設定 → 更新とセキュリティ →
ライセンス認証 → ストアの移動 →

『クレジットカード』か『PayPal』で支払方法を選択

→ アップグレード作業開始

アップグレード
13,824円

おしまい

坂口