情報漏えいを防ぐためのモバイルデバイス等

設定マニュアル

～安心・安全のための暗号利用法～

★★★　実践編－Windows10 での設定方法　★★★

目次

〔編集責任〕
独立行政法人 情報処理推進機構

なお、本実践編は、日本マイクロソフト株式会社の協力の下、作成されております。

〔発 行〕
２０１８年 ７月３１日

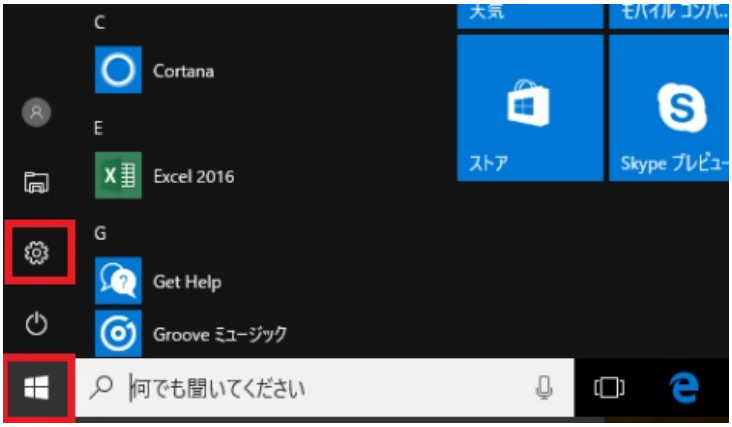
〔問い合わせ先〕
本マニュアルについてのご意見・ご要望がございましたら、下記までご連絡ください。次回改訂の際などに参考にさせていただきます。なお、個別のご質問・ご要望等にはお応えいたしかねる場合もございますので、予めご了承ください。

IPA　セキュリティセンター：　　isec-info@ipa.go.jp

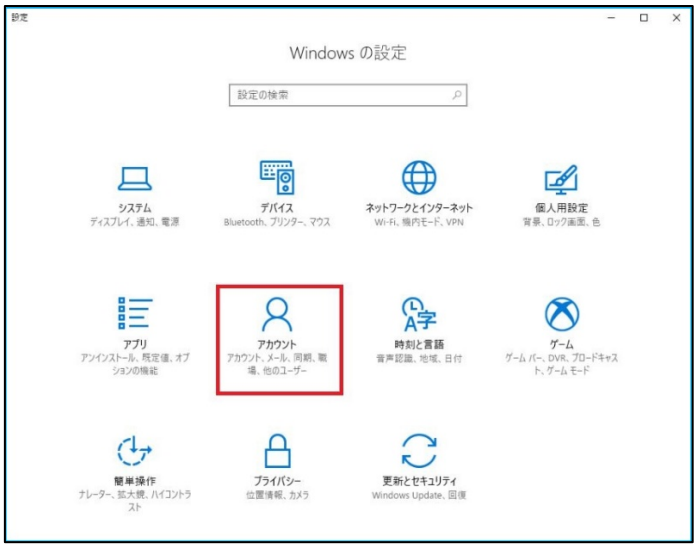
実践編－Windows10 での設定方法

A.1　端末ロックによる利用者認証の有効化（利用者認証の設定方法）

1. ［スタート］ボタンから設定を起動します。



2. ［アカウント］をクリックする。

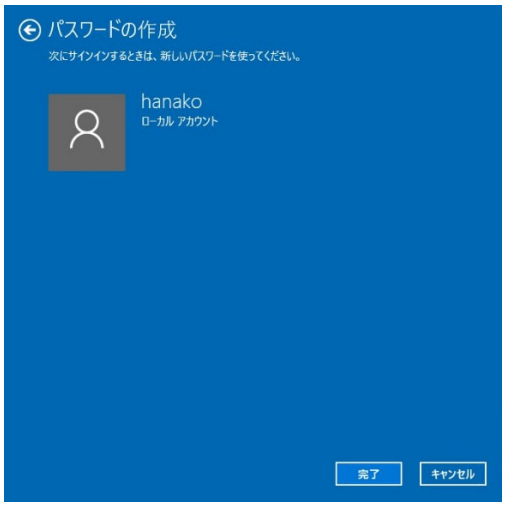


3. ローカルアカウントが表示されていることを確認し､｢サインインオプション｣をクリックします。

4. 「パスワード」欄から「追加」をクリックします。

5. 「パスワードの作成」が表示されます。
「新しいパスワード」「パスワードの確認入力」にパスワードを入力し、「次へ」をクリックします。

6. 「完了」をクリックします。



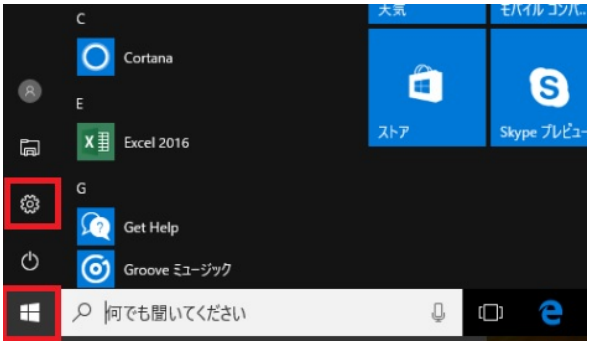
〈追加手順〉

Windows 10 以降では、PIN（暗証番号）を利用してデバイスにサインインすることができます。パスワードを設定した後、PIN を設定しサインインをより安全に、利便性高く利用できます。なお、PIN は設定された特定のデバイスに関連付けられ、ローカルでのみ使用されます。

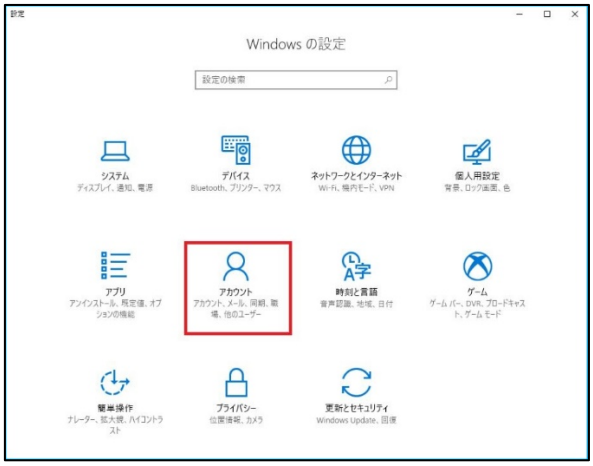
参考情報：PIN がパスワードより安全な理由

https://docs.microsoft.com/ja-jp/windows/access-protection/hello-for-business/hello-why-pin-is-better-than-password

1. ［スタート］ボタンから設定を起動します。



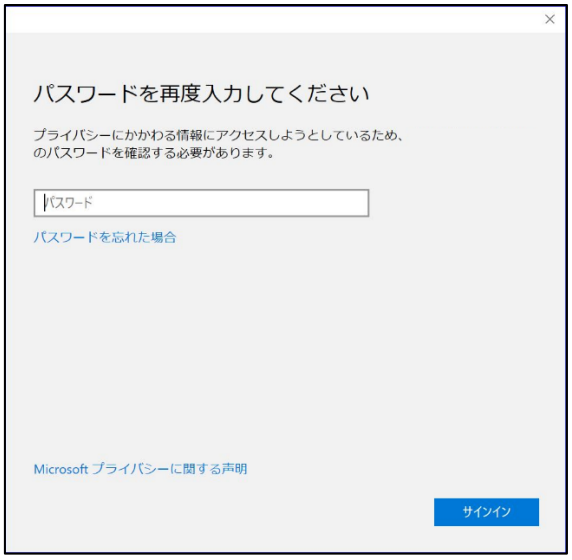
2. ［アカウント］をクリックする。



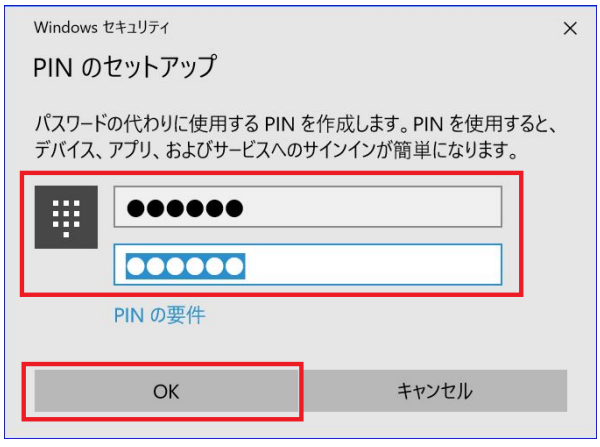
3. ローカルアカウントが表示されていることを確認し、「サインインオプション」をクリックします。

3. 画面右側から「PIN」欄の「追加」をクリックします。

4.「パスワードを再度入力してください」という画面が表示されます。パスワードを入力し、「サインイン」をクリックします。

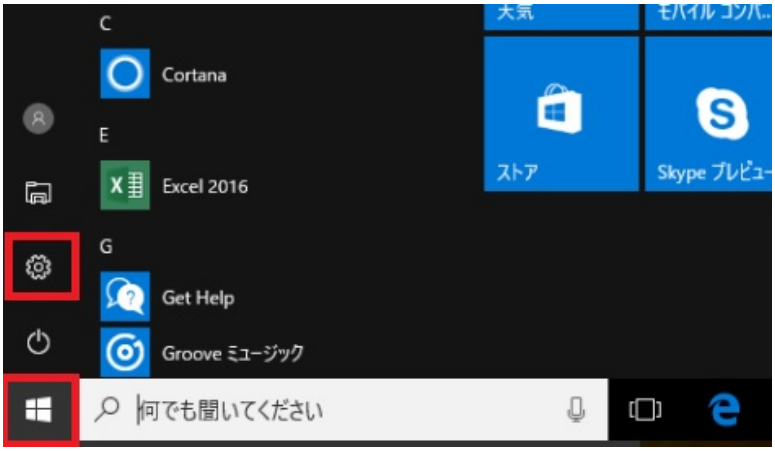


5. 「PIN のセットアップ」が表示されます。
「新しい PIN」ボックスと「PIN の確認」ボックスに、PIN に設定する数字（暗証番号）を入力し、「OK」をクリックします。暗証番号は 4 桁以上の数字で設定してください。

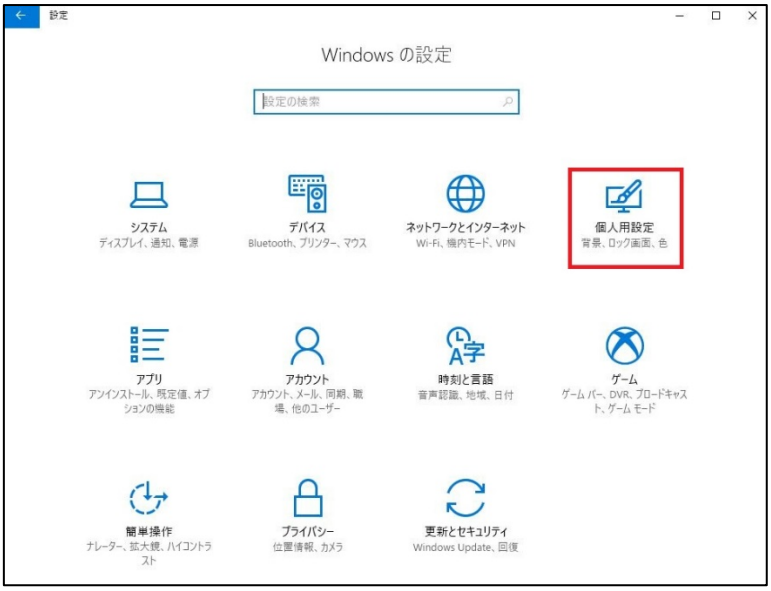


〈スクリーンロックの設定〉

1. ［スタート］ボタンから設定を起動します。



2. 「個人用設定」をクリックします。

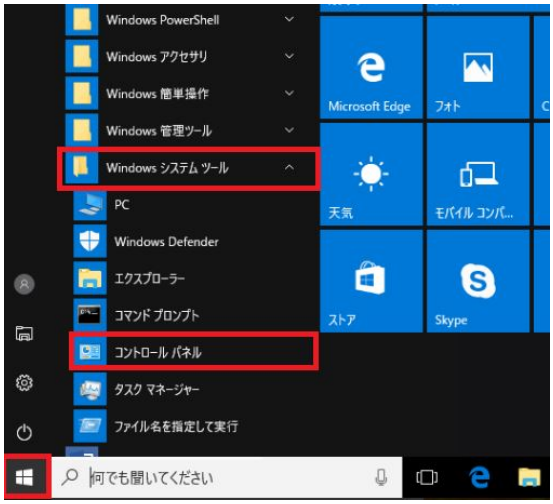


3. 画面左側から「ロック画面」をクリックし、「スクリーンセーバー設定」をクリックします。

4.「スクリーンセーバー」ボックスから任意のスクリーンセーバーの種類をクリックし、「待ち時間」ボックスにスクリーンセーバーが起動するまでの時間を入力します。
ここでは例として、スクリーンセーバーを「リボン」、待ち時間を「5 分」に設定します。
「再開時にログオン画面に戻る」にチェックを入れて、「OK」をクリックします。

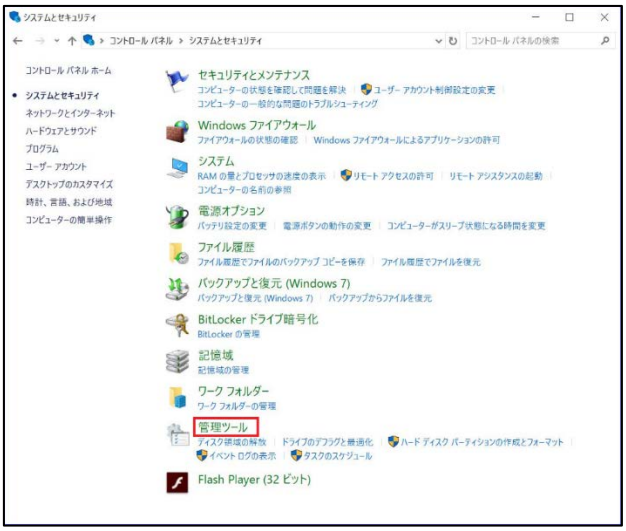
A.2　端末ロックによる利用者認証の安全性強化（利用者認証失敗時の動作設定方法）

1.「スタート」をクリックし、表示されたアプリの一覧の「W」欄から「Windows システムツール」をクリックし、表示された一覧から「コントロールパネル」をクリックします。



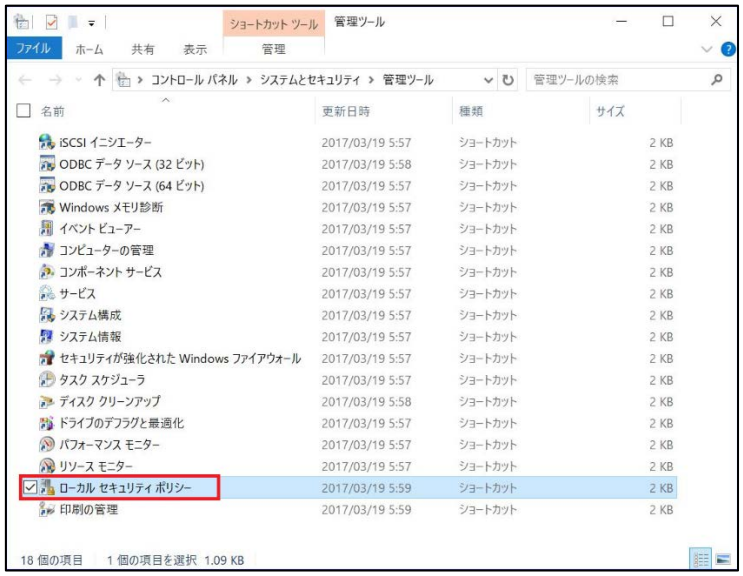
2.〔システムとセキュリティ〕 をクリックします。

3.〔管理ツール〕 をクリックする。

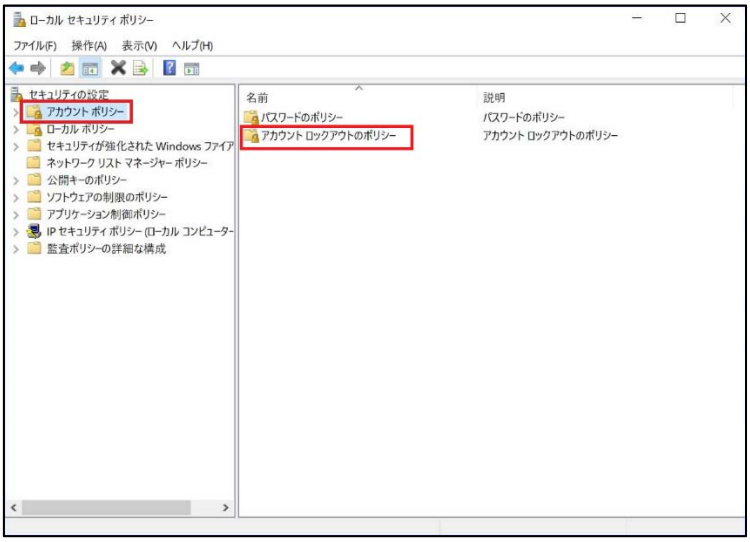


実践編-Windows10 での設定方法－8

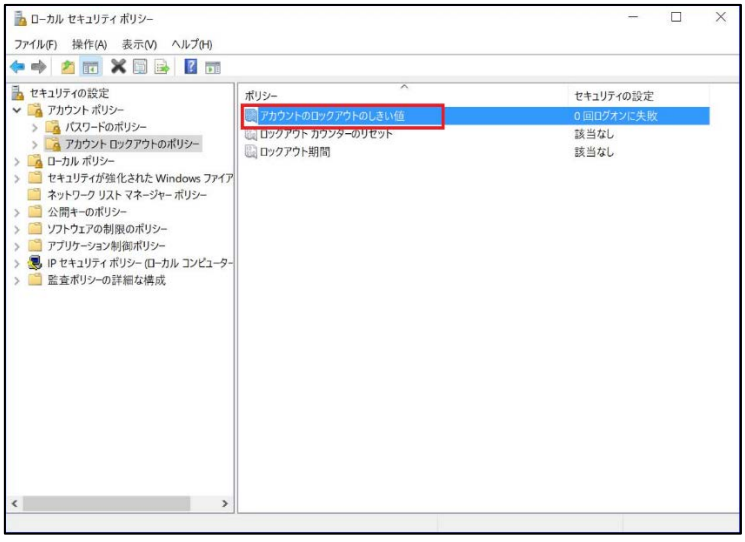
4.〔ローカルセキュリティポリシー〕 をダブルクリックします。



5.〔アカウントポリシー〕 をクリックし、〔アカウントロックアウトのポリシー〕 をダブルクリックします。



6.〔アカウントロックのしきい値〕 をダブルクリックする。



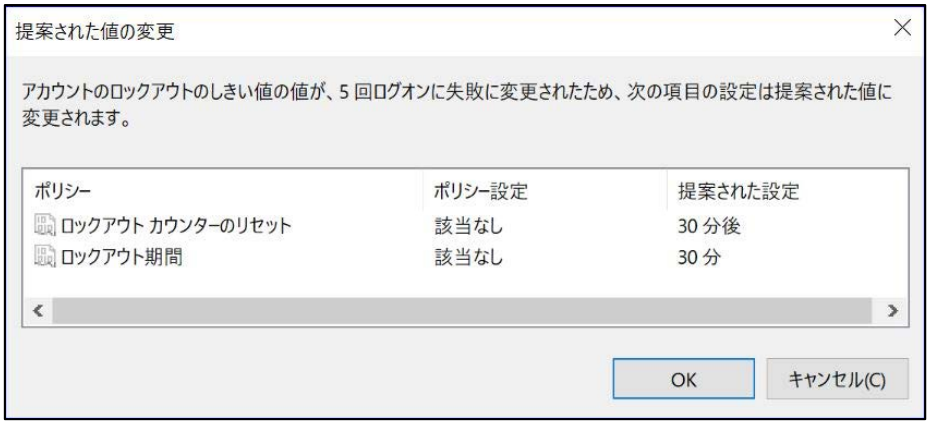
7. テキストボックスに、何回ログオンに失敗したらロックアウトするか、回数を入力し、〔OK〕をクリックします。

※ 回数は持ち歩く情報の情報価値レベルに応じて決定する。例として、オンラインバンキングではおおむね 5 回に設定されている

8.〔ロックアウトカウンターのリセット〕及び〔ロックアウト期間〕の設定が自動的に変更されるので、内容を確認のうえ、〔OK〕 をクリックする。 必要に応じて、それらの設定を変更します。

※ ロックアウトカウンターは利用者認証の連続失敗回数をカウントしたものである。 リセット時間が経過すると連続失敗回数が 0 に戻る

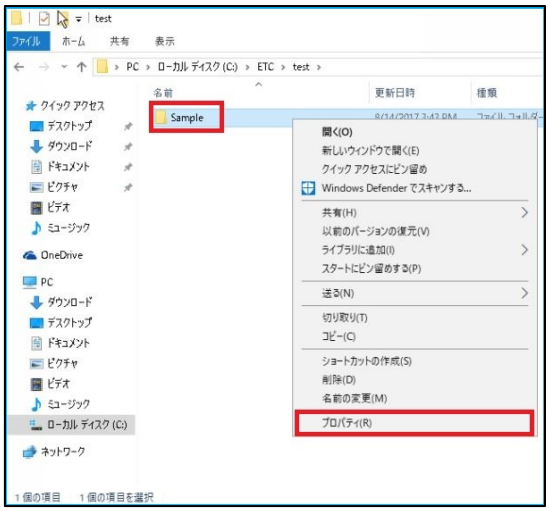
※ ロックアウト時間は、利用者認証の連続失敗によるロックアウトが解除され、利用者認証が再開できるようになるまでの時間を決めるものである



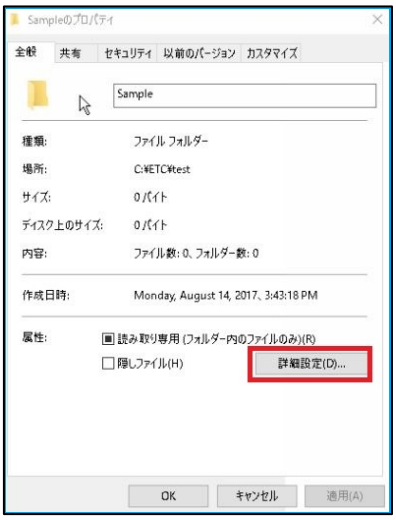
C.1　ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

- **EFS によるフォルダ暗号化**

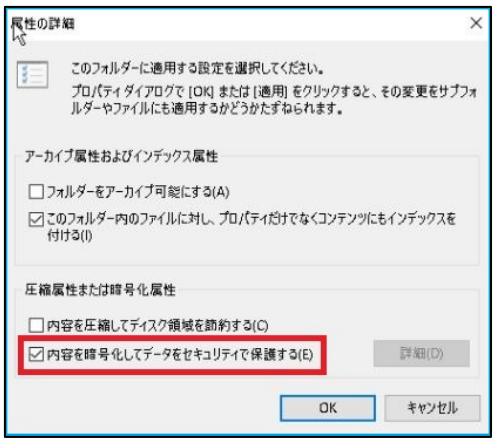
1. 暗号化するフォルダを右クリックし、〔プロパティ〕をクリックする。



2. 〔詳細設定〕をクリックする。

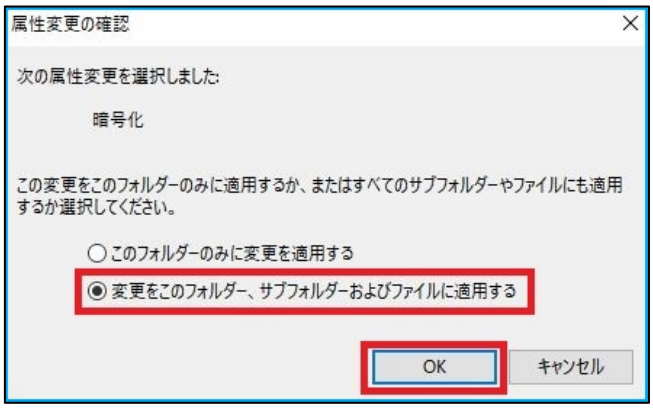


3. 〔内容を暗号化してデータをセキュリティで保護する〕チェックボックスをオンにし、〔OK〕をクリックする。



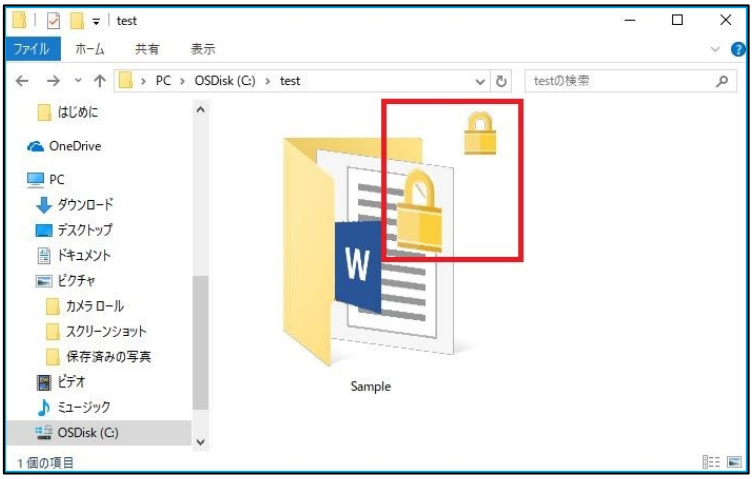
4. 〔適用〕をクリックする

5. 〔変更をこのフォルダー、サブフォルダーおよびファイルに適用する〕ラジオボタンをオンにし、〔OK〕をクリックする



6. 〔OK〕をクリックする

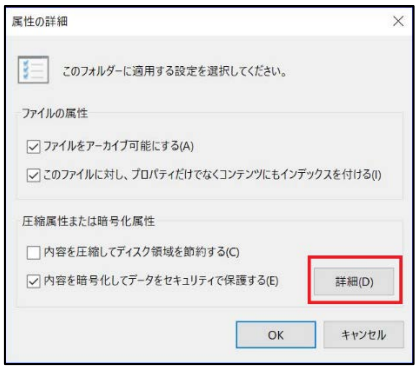
7. 暗号化されたフォルダは緑色で表示され、鍵アイコンが表示されます。



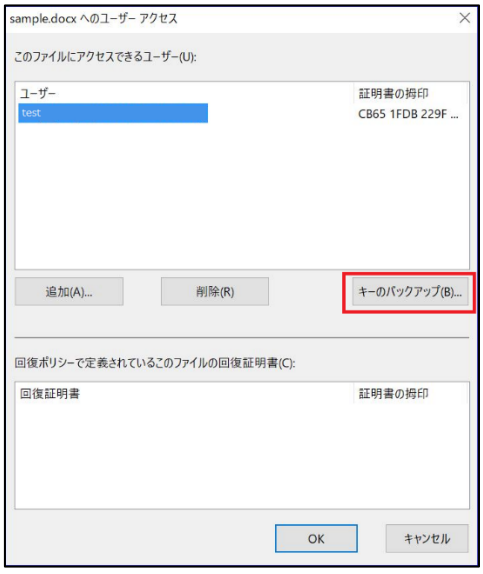
● EFS 証明書のバックアップ

1. 暗号化を行った PC 上で、暗号化したファイルを右クリックし、プロパティを表示します。
2. ［詳細設定］をクリックします。

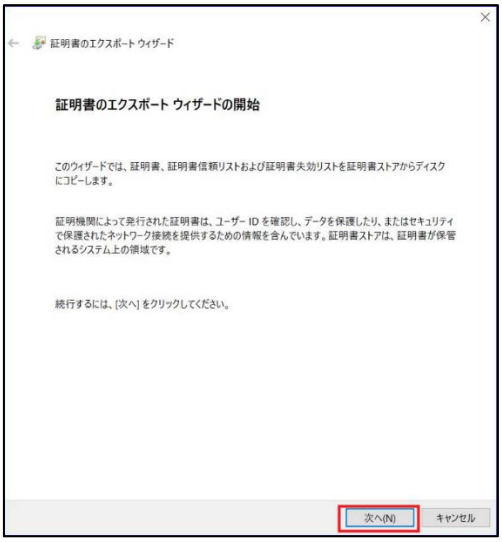
3.［詳細］ボタンをクリックします。



4. ユーザー名を選んで［キーのバックアップ］をクリックします。

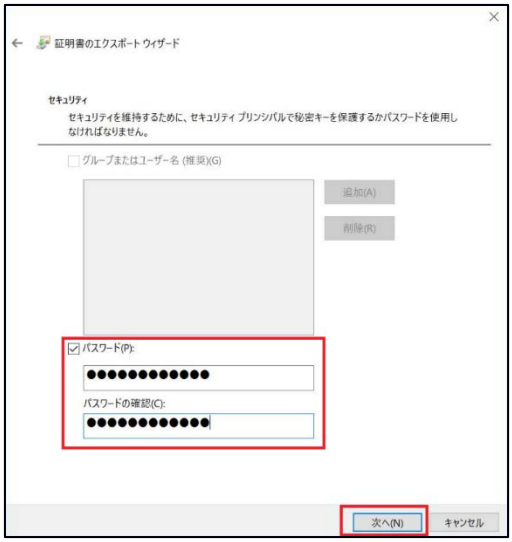


5. ［証明書のエクスポート ウィザード］ が開始されます。［次へ］をクリックします。



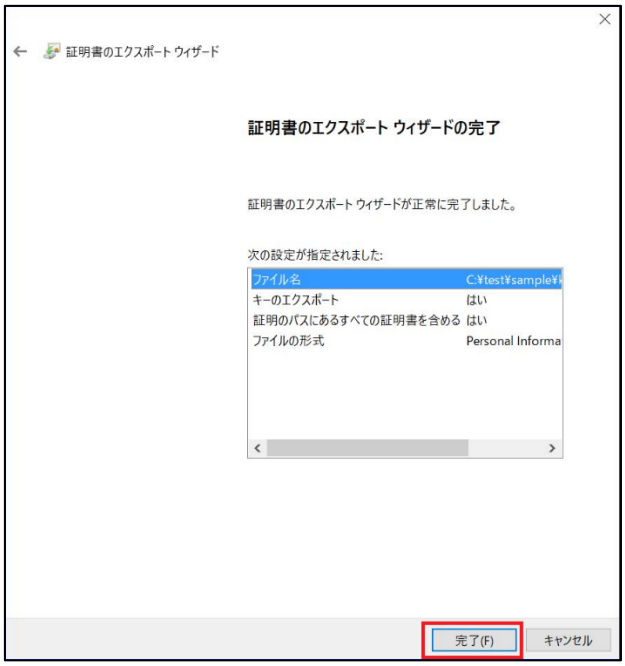
6. ［Personal Information Exchange - PKCS #12 (.PFX)］が選択されていることを確認し、［次へ］をクリックします。

7. パスワードを入力し、［次へ］をクリックします。パスワードは、EFS で暗号化したファイルを復号する際に利用する秘密鍵を安全に利用するために設定するものです。



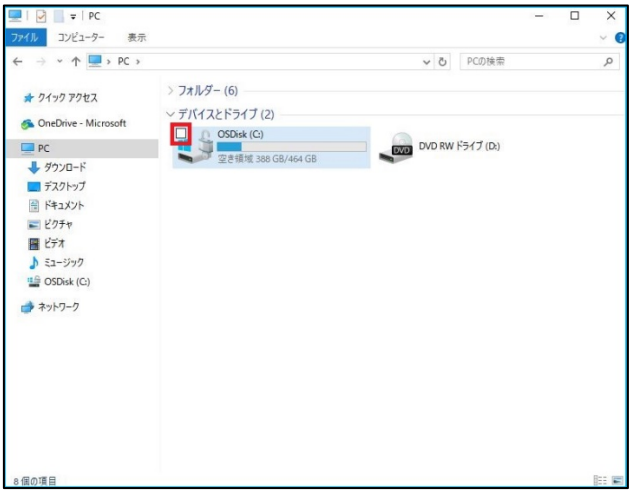
8. 証明書の保存先を指定し［次へ］をクリックします。

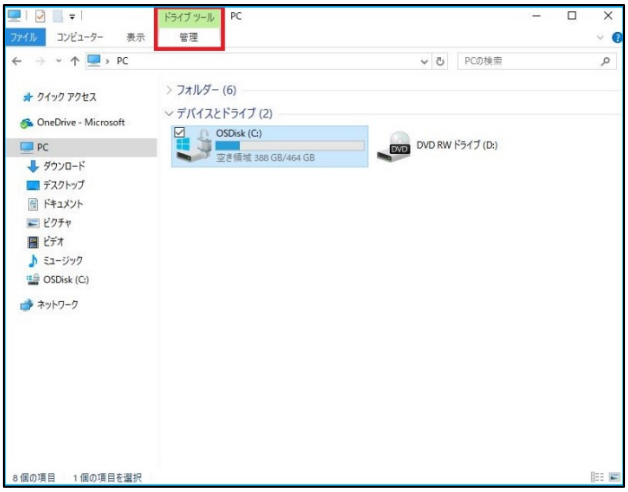
9. ［完了］をクリックします。



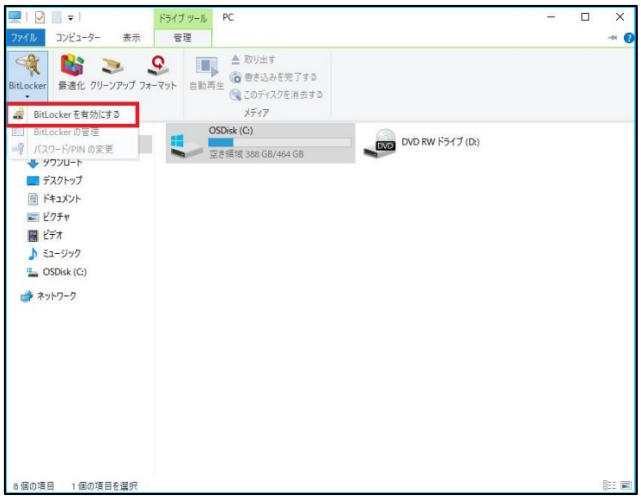
● BitLocker によるドライブ暗号化

1. デスクトップから〔エクスプローラー〕 を起動する。
2.〔コンピューター〕をクリックし、〔ローカルディスク〕の左上にあるチェックボックスをオンにする。

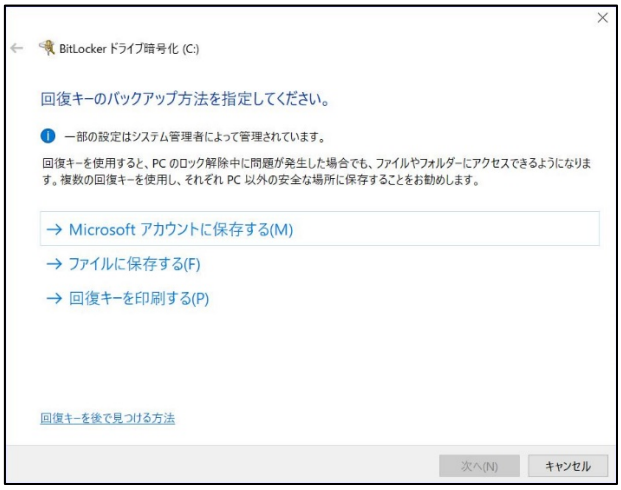




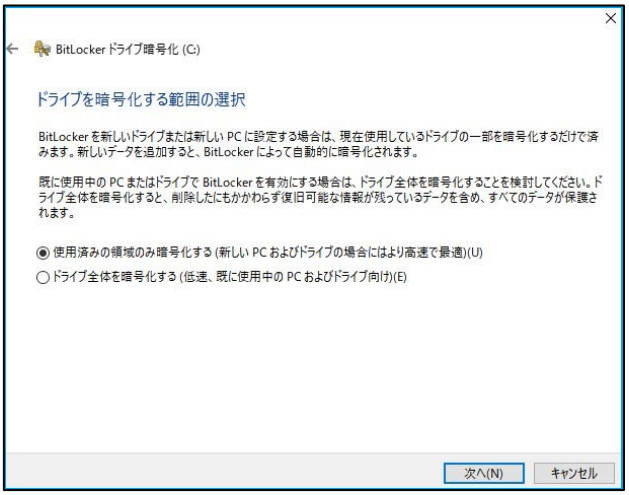
3. 〔ドライブツール〕 の〔管理〕 タブをクリックし、［Bitlocker］のメニューから［Bitlocker を有効にする］をクリックします。



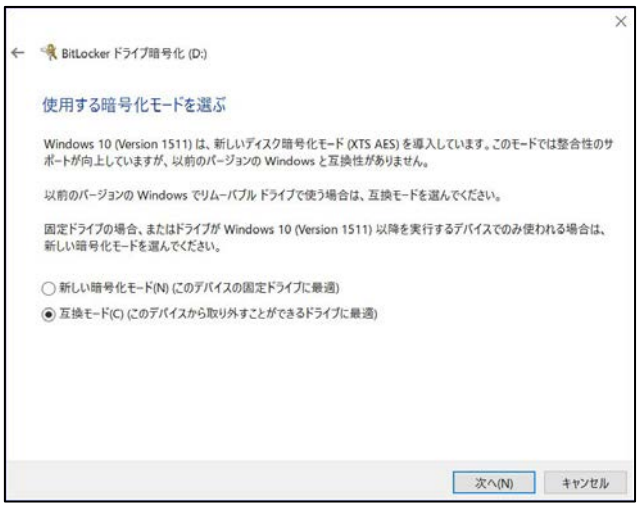
4. 回復カギのバックアップ方法を指定します。Microsoft アカウントに保存しておく場合は［Microsoft アカウントに保存する］をクリックします。USB ドライブなどに保存する場合は［ファイルに保存する]をクリックします。印刷した紙に保存する場合は［回復キーを印刷する］をクリックします。



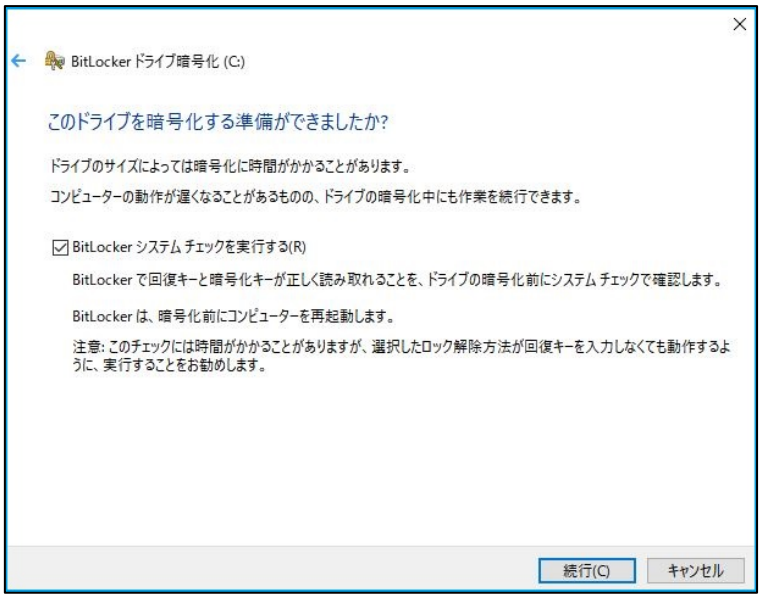
5. ［使用済みの領域を暗号化する］を選択し［次へ］をクリックします。



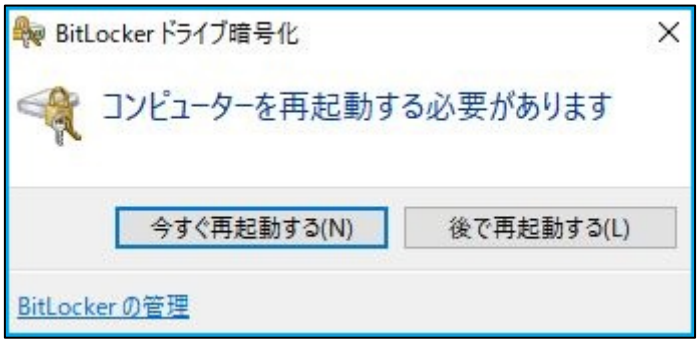
6. ［互換モード］を選択し［次へ］をクリックします。



7. ［続行］をクリックします。

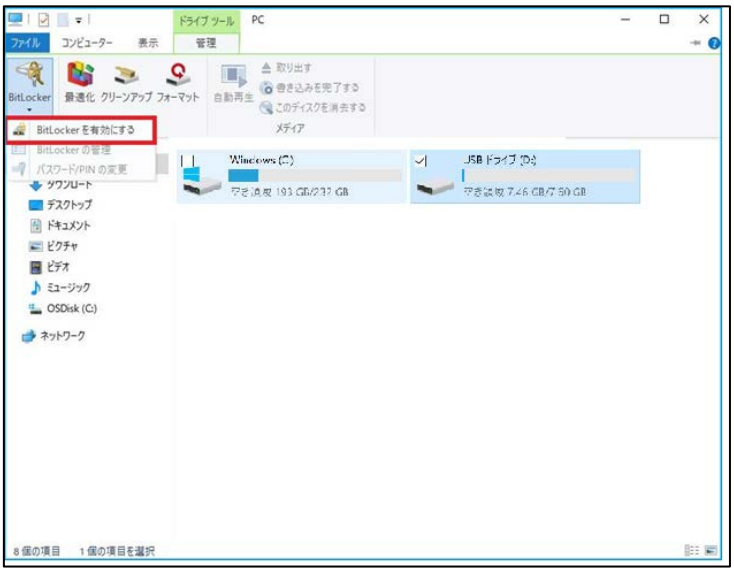


8. Bitlocker ドライブの暗号化が完了すると、再起動を求められます。［今すぐ再起動する］をクリックし、再起動を行います。

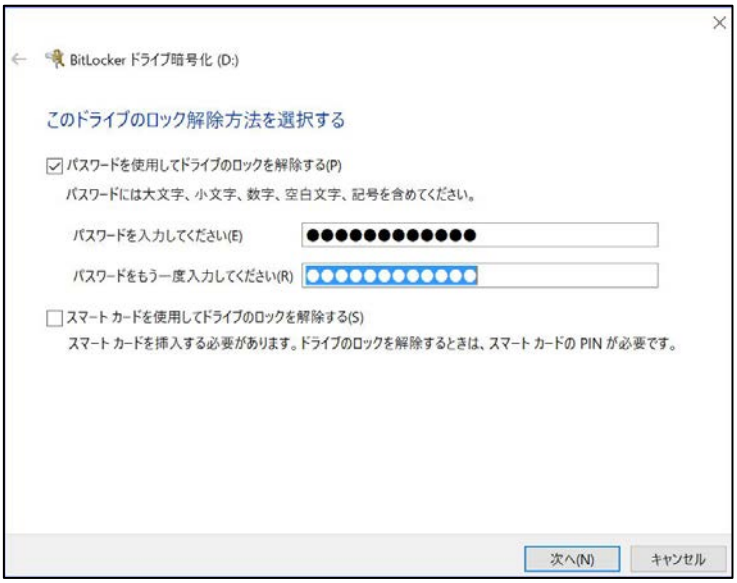


● BitLocker TO GO の設定

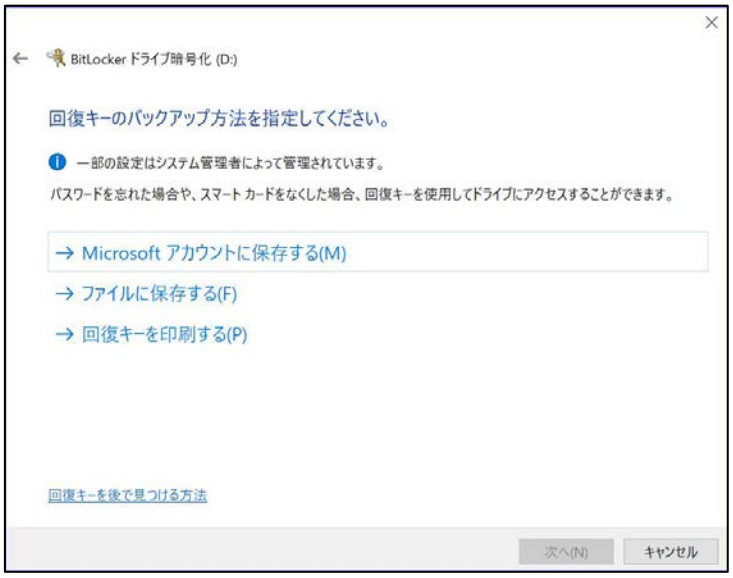
1. デスクトップから〔エクスプローラー〕 を起動する。
2. 〔コンピューター〕 をクリックし、暗号化を行う USG ドライブの左上にあるチェックボックスをオンにします。
3. 〔ドライブツール〕 の〔管理〕 タブをクリックし、［Bitlocker］のメニューから［Bitlocker を有効にする］をクリックします。



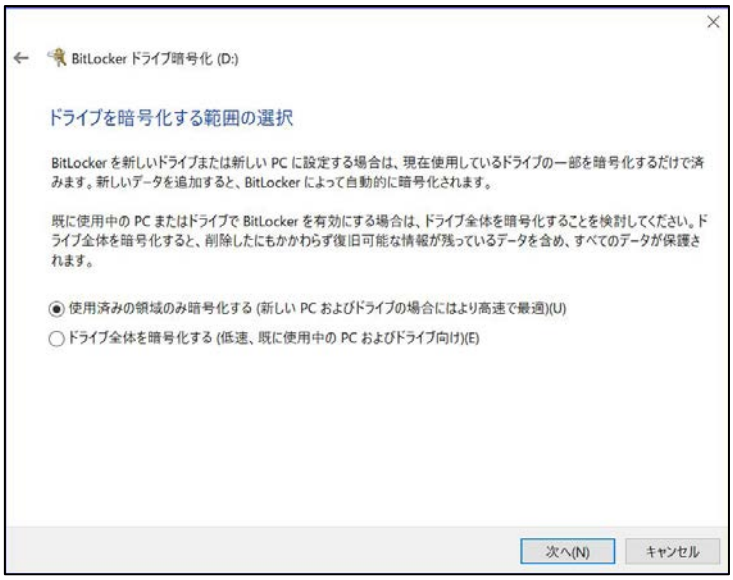
4. ドライブのロックを解除する際に必要となるパスワードを設定します。



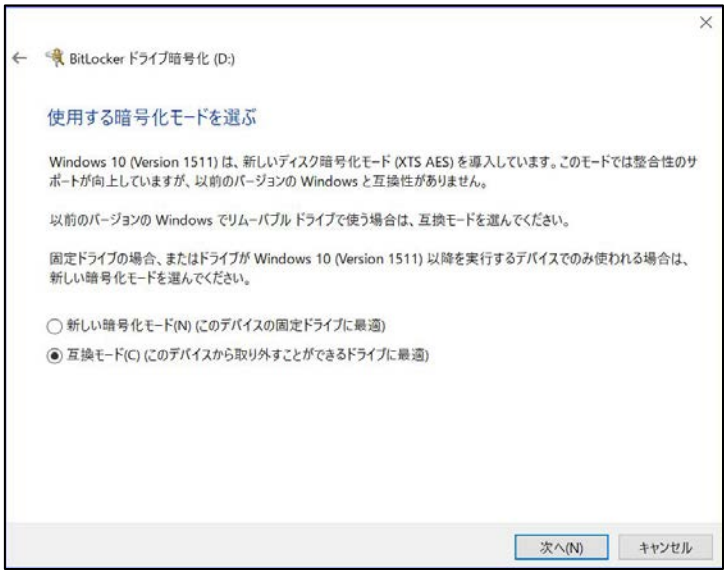
5. 回復カギのバックアップ方法を指定します。Microsoft アカウントに保存しておく場合は［Microsoft アカウントに保存する］をクリックします。USB ドライブなどに保存する場合は［ファイルに保存する]をクリックします。印刷した紙に保存する場合は［回復キーを印刷する］をクリックします。



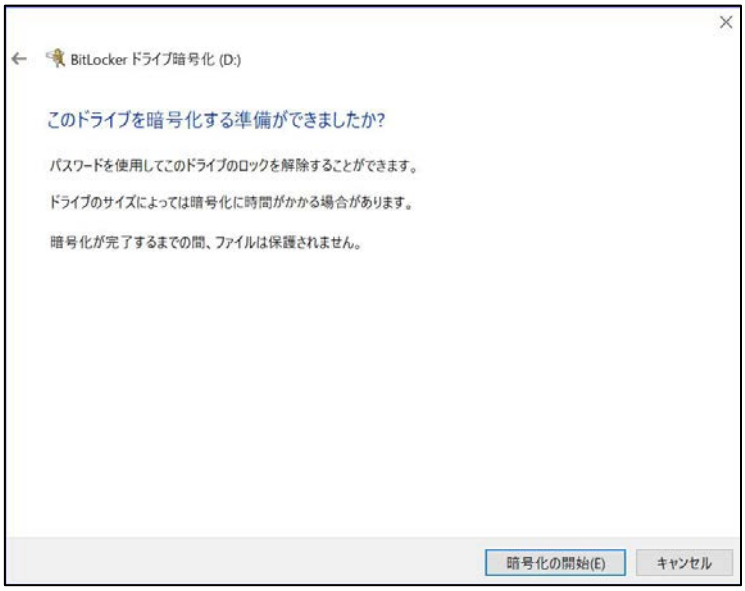
6. ［使用済みの領域を暗号化する］を選択し［次へ］をクリックします。



7. ［互換モード］を選択し［次へ］をクリックします。



8. ［暗号化の開始］をクリックします。

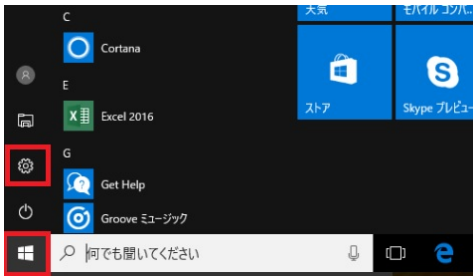


● デバイス暗号化の設定（Win10）

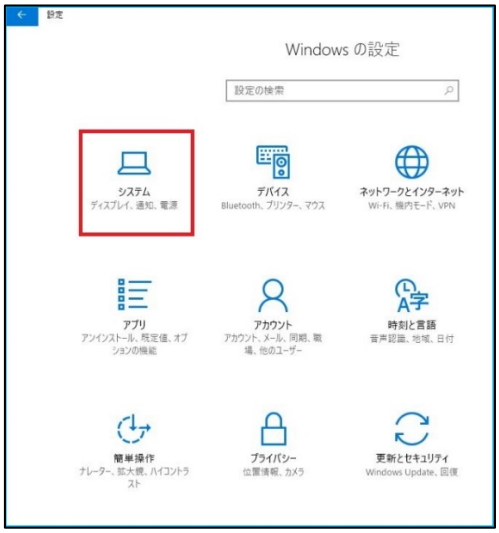
Windows 10 以降、すべてのエディションの Windows 10 で、ドライブの暗号化（システムドライブの暗号化）が利用できます。Bitlocker が利用できないエディションを利用している場合は、ドライブの暗号化を利用してデバイスの暗号化を行ってください。

注意：デバイスの暗号化を利用するためには、マイクロソフト アカウントでサインインする必要があります。

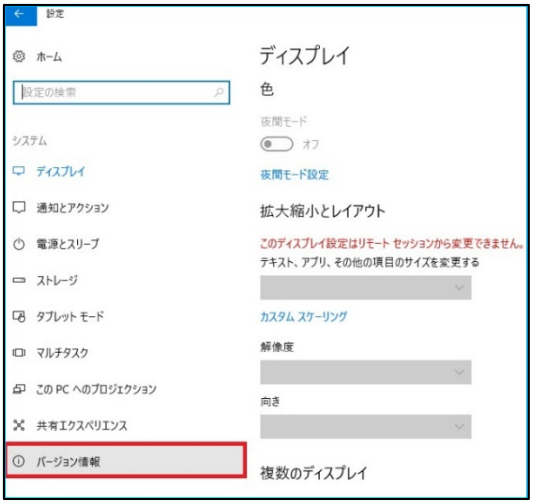
1. ［ スタート ］→［ 設定 ］の順にクリックします。



2. 「 Windows の設定 」 画面が表示されます。［ システム ］をクリックします。

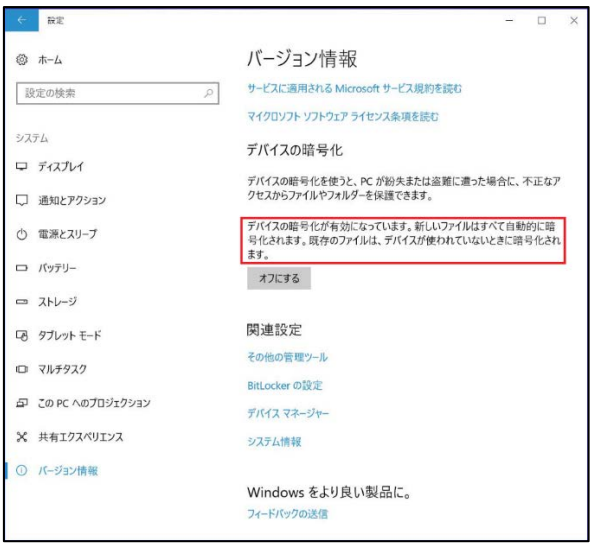


3.「 システム 」 画面が表示されます。［ バージョン情報 ］をクリックします。

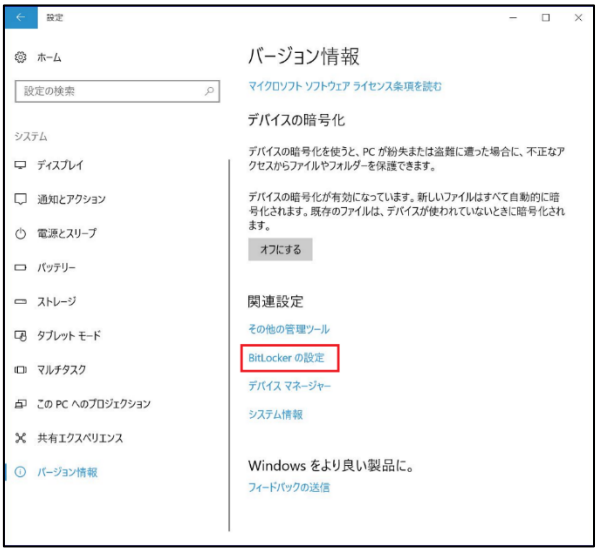


4. デバイス暗号化の［ オンにする ］をクリックします。

5.「 デバイスの暗号化が有効になっています。 」 と表示されることを確認します。

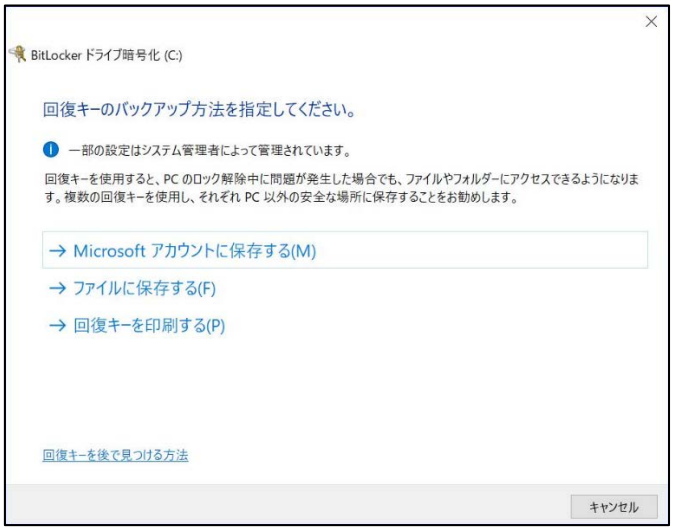


6.「 関連設定 」 の［ BitLocker の設定 ］ をクリックします。



7.[回復キーのバックアップ] をクリックします。

8. 回復カギのバックアップ方法を指定します。Microsoft アカウントに保存しておく場合は［Microsoft アカウントに保存する］をクリックします。USB ドライブなどに保存する場合は［ファイルに保存する］をクリックします。印刷した紙に保存する場合は［回復キーを印刷する］をクリックします。



9.［完了］をクリックします。