HP Elite x2 1012 G1
Windows 10 Pro
BitLocker ドライブ暗号化
導入手順書
(TPM 利用 PIN 認証設定例)

V 1.0
2016 年 6 月
株式会社 日本 HP

本書の取り扱いについて

本書は、株式会社 日本HPが販売する製品を検討されているお客様が実際のご利用方法に合わせた設定を行う際に役立つ手順の一例を示すものです。いかなる場合においても本書の通りになる事を保証するものではありません。

本書の内容は、将来予告なしに変更されることがあります。HP製品およびサービスに対する保証については、該当製品およびサービス保証規定書に記載されています。本書のいかなる内容も、新たな保証を追加するものではありません。本書の内容につきましては万全を期しておりますが、本書中の技術的あるいは校正上の誤り、省略に対して責任を負いかねますのでご了承ください。

はじめに

本手順書では HP Elite x2 1012 G1 の Windows 10 pro 環境における BitLocker 暗号化の導入におきまして、PIN 認証を行う設定例の手順を説明します。

BitLocker 暗号化設定手順

※設定作業にてキーボードによる入力が必要です。あらかじめ、専用トラベルキーボードあるいは USB キーボードの接続を行ってください。

1. BIOS に入り、以下の項目の設定を確認します。

   - Security > TPM Embedded Security の設定画面にて、「TPM State」にチェックが入っているか確認します。入っていない場合は、チェックを入れます。
   - Advanced > Boot Options の設定画面にて、「Fast Boot」のチェックが入っていないことを確認します。入っている場合は、チェックを外します。

   設定変更した場合は、Main > Save Changes and Exit にて設定保存して BIOS を終了し、PC を再起動します。

2. 管理者ユーザーでサインオンします。

3. ファイル名を指定して実行(Windows キー+R キー)にて、tpm.msc と入力して実行します。TPM の管理の画面が現れます。

4. TPM の管理の画面にて「TPM をクリア」を実行します。

「TPM セキュリティハードウェアをクリアします」の画面が表示されますので、「再起動」ボタンをクリックして再起動します。

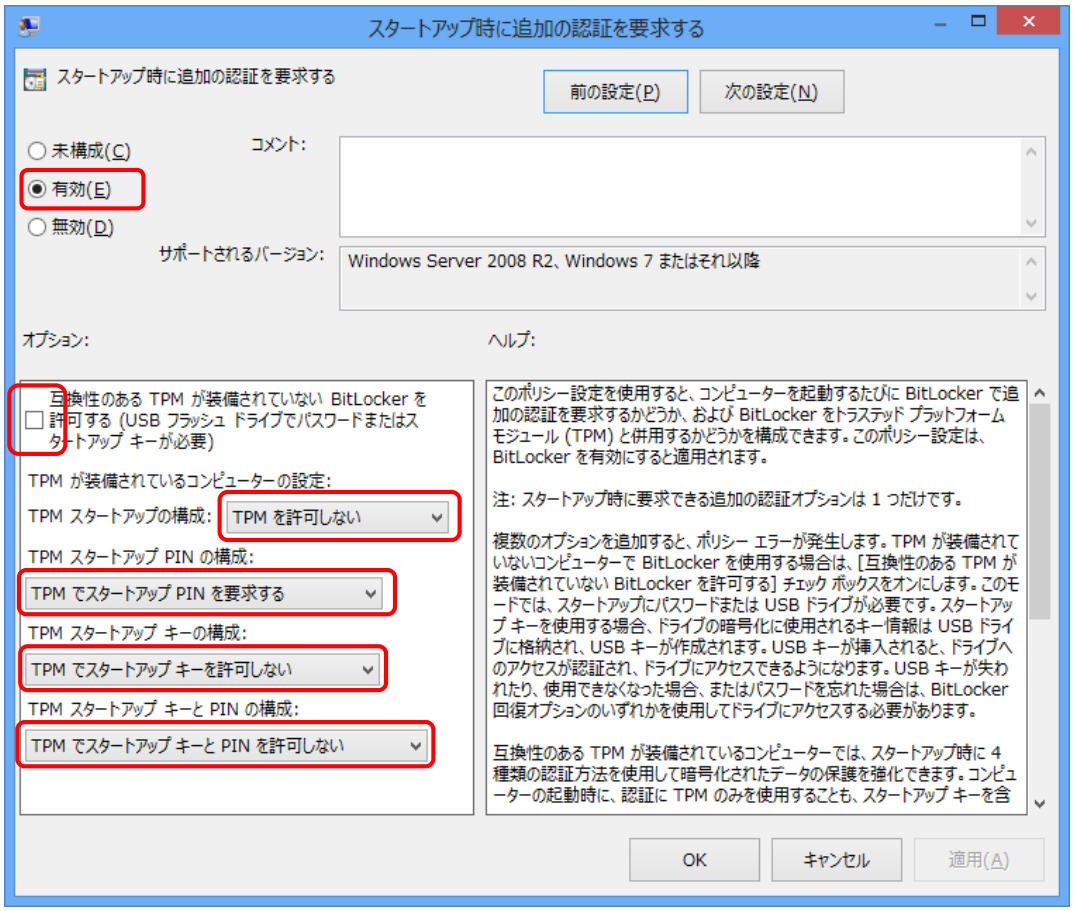
5. OS 起動の前に、画面に「A configuration change was requested to clear this computer's TPM(Trusted Platform Module ...」と表示されますので、接続したキーボードにて F1 キーを押して承諾します。その後、OS が起動します。

6. あらためて管理者ユーザーでサインオンして、tpm.msc を実行します。TPM の管理の画面にて「TPM を準備する」を実行します。

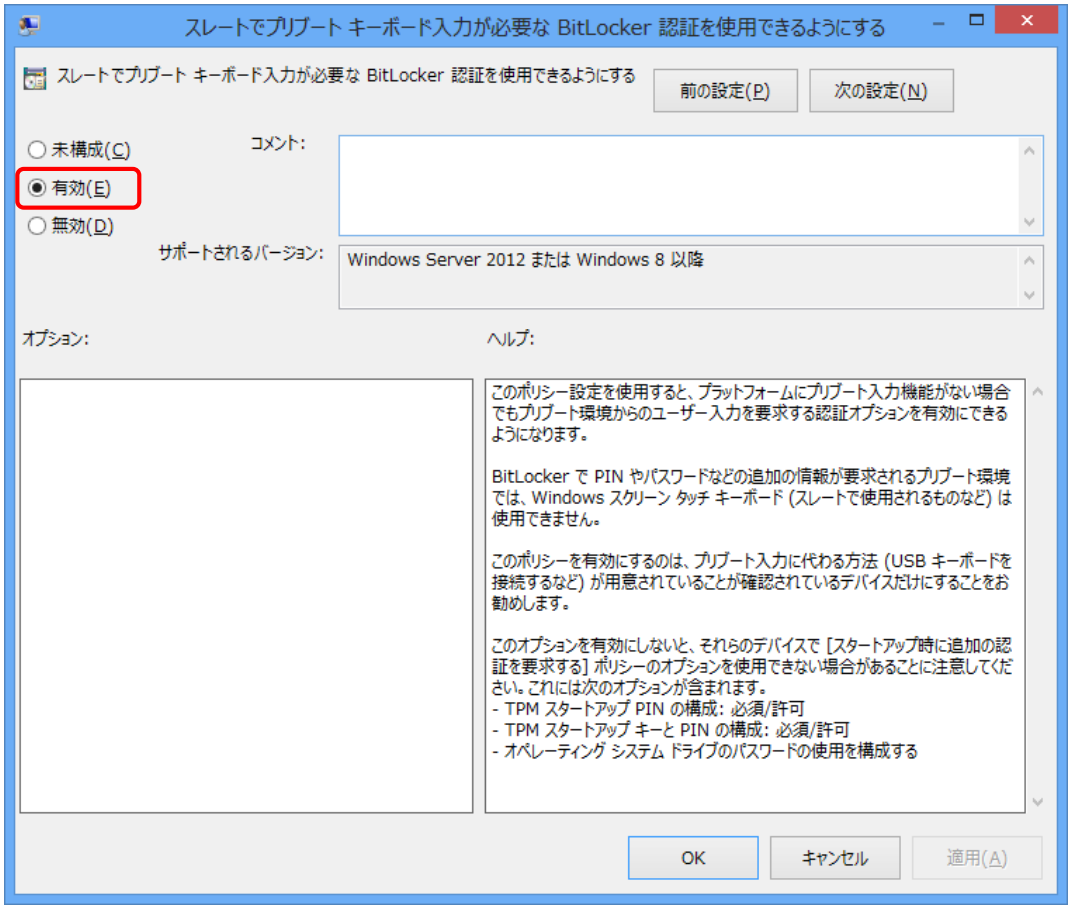
7. 「TPM の準備ができました」という画面が表示されます。「TPM 所有者パスワードを保存する」をクリックし、外部ストレージデバイスなどに TPM 所有者パスワードファイル(ホスト名.tpm)を保存して、この画面を閉じます。

8. ファイル名を指定して実行にて gpedit.msc (ローカルグループポリシーエディター)を実行します。

9. ローカルグループポリシーエディターにて、コンピューターの構成→管理用テンプレート→Windows コンポーネント→BitLocker ドライブ暗号化→オペレーティングシステムのドライブ　とクリックします。次に「スタートアップ時に追加の認証を要求する」をクリックして画面を開きます。未構成から有効に変更し、さらに以下の赤枠部分について変更を行います。すべて変更したら、「適用」ボタンを押し、「OK」ボタンで画面を閉じます。



10. 同じく「オペレーティングシステムのドライブ」の場所にて、「スレートでプリブートキーボード入力が必要な BitLocker 認証を使用できるようにする」をクリックして設定画面を開き、未構成から有効に変更します。変更したら、「適用」ボタンを押し、「OK」ボタンで画面を閉じます。

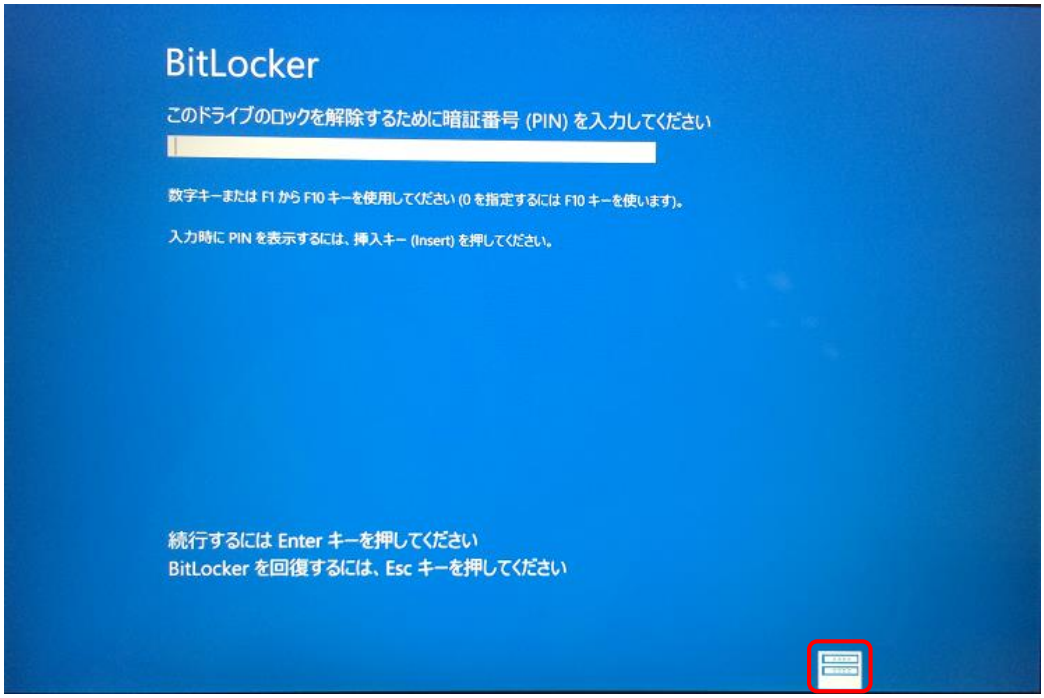


11. ローカルグループポリシーエディターを閉じ、ファイル名を指定して実行にて gpupdate /force を実行し、変更したポリシーに更新します。

12. コントロールパネルを表示し、システムとセキュリティ→BitLocker ドライブ暗号化とクリックして、「BitLocker を有効にする」をクリックしてウィザードに従って進めます。設定ウィザードでは、認証に入力する PIN の設定、回復キーの保存などを行います。

13. ウィザードが終了したら、PC を再起動します。OS 起動の前に、PIN 入力を求める画面が表示されます。

14. 暗号化が完了した後、パワーキーボードなどが接続されておらず本体のみの構成の場合は、スクリーンキーボードを表示して PIN の入力が可能です。電源オン後の認証画面にて、画面の右下部の赤枠のアイコンをタップします。



15. キーボード言語の選択画面が現れます。[INTL]をタップします。

16. スクリーンキーボードが現れます。スクリーンキーボードからの PIN 入力により、OS 起動できることを確認します。

PIN 認証入力に関する補足

- 誤った PIN 入力の回数が 32 回を超えてしまうと、「TPM ロックアウト」という状態なります。TPM ロックアウト状態になると、それ以降は、正しい PIN 入力も受け付けなくなります。Windows を起動するには、回復キーの入力が必要になります。
- TPM ロックアウト状態が完全にクリアされるには、おおよそ 18 日以上の日数が必要になります。
- TPM ロックアウト状態にて、回復キーの入力にて Windows を起動し、管理者ユーザーにて tpm.msc(TPM の管理)を実行して「TPM ロックアウトのリセット」を実行すれば、ロックアウト状態は解除されます。
- この一連の動作については、内部的に固定された仕様動作となります。変更する設定はご提示されません。

以上