TPM 2.0 ファームウェア更新手順書
(対象 OS：Windows 10)

公開日 2017/11/28
更新日 2018/05/17

1 はじめに

- 現在の TPM の状態は以下の手順でご確認いただけます。
  1) Windows キー と r キーを同時に押す
  2) tpm.msc と入力し、ENTER キーを押す

(以降、更新手順で「tpm.msc を起動する」と説明されている場合も、上記の操作を行ってください)

(“状態”の内容)

“状態”欄に下記のメッセージが表示されている場合、TPM は搭載されていません。

・互換性のある TPM が見つかりません

(“仕様バージョン”の内容)
本書で説明されているのは、仕様バージョン 2.0 の場合の手順です。
仕様バージョンが 1.2 と表示されている場合は、本 TPM 2.0 ファームウェア更新の対象外です。
TPM1.2 ファームウェア更新をご使用ください。

- 本書では Windows が C:ドライブにインストールされている場合を例に説明しています。他のドライブやフォルダに Windows がインストールされている場合は、適宜読み替えてください。
  Windows がインストールされているドライブ、フォルダは以下の手順でご確認いただけます。

  1) Windows キー と r キーを同時に押す
  2) cmd と入力し、ENTER キーを押す
  3) set と入力し、ENTER キーを押す
  4) Windows がインストールされているドライブ、フォルダの情報が表示される。
     (例) windir=c:¥Windows

2 動作条件と注意点

・万一 TPM ファームウェア更新に失敗した場合、システム起動やデータの使用ができなくなる恐れがあります。あらかじめデータバックアップを行ってください。

・ファームウェア更新は管理者アカウントで実行してください。

・ファームウェア更新は AC 電源およびバッテリーを接続した状態で行ってください。更新中に電源オフされた場合、TPM チップが破損する恐れがあります。

・(Microsoft アカウントをご使用の場合)
”デバイスの暗号化”を、いったんオフに設定変更し、ファームウェア更新後に再度オンに戻してください。
オフの設定は以下の手順で行えます。 (Windows のバージョンによって設定メニューの構成や位置が変更される場合があります)

(Windows 10 バージョン 1703 まで)
1) スタート > 設定 > システム をクリックする
2) 画面左側の[バージョン情報]をクリックする
3) 「デバイスの暗号化」の“オフにする”ボタンをクリックする

(Windows 10 バージョン 1709)
1) スタート > 設定 > 更新とセキュリティ をクリックする
2) 「デバイスの暗号化」の“オフにする”ボタンをクリックする

ファームウェアの更新は、暗号化の解除が完了してから、実施してください。

・(BitLocker をサポートする Windows のエディションの場合)

BitLocker を有効にしてご使用の場合、ファームウェア更新の一連の手順は、いったん BitLokcer を無効化する(“BitLocker を無効にする”)か、または“保護の中断”にして実行してください。BitLocker の無効化には数 10 分から数時間程度の時間がかかります。また TPM ファームウェア更新後に BitLocker の有効化を行う際にも同様の時間がかかります。一方“保護の中断”は処理時間はかかりませんが、PC 再起動時に自動的に解除されるため、TPM ファームウェア更新の一連の手順の中で都度設定が必要です。また BitLocker の回復キー入力が求められた際に回復キーを紛失されているとシステムを起動できなくなります。お使いの環境にあった方法をお選びのうえ、BitLocker を無効にせずにファームウェア更新の一連の手順を実行される場合は、必ず回復キーを把握していることをご確認ください。

BitLocker の状態確認や設定変更の操作については「４ BitLocker 関連手順」をご参照ください。

・(Windows 10 バージョン 1607 以降でサインイン時の PIN を設定している場合)

Windows 10 バージョン 1607 以降でサインイン時の PIN を設定している場合(Windows Hello 使用時を含む)、ファームウェア更新の一連の手順は PIN を削除(Windows 10 バージョン 1703 では″取り出す″)してから実行し、PIN の再設定はファームウェア更新の一連の手順実行後に行ってください。

(PIN の削除をせずにファームウェア更新手順を実行した場合、パスワードがないとサインインできなくなります)。

・(BitLocker およびサインイン時の PIN 以外に TPM を使用するソフトウェアがある場合)

TPM のファームウェア更新前後で必要な処理がある可能性がありますので、そのソフトウェアのサポート窓口に対応方法をご確認ください。

3 更新手順

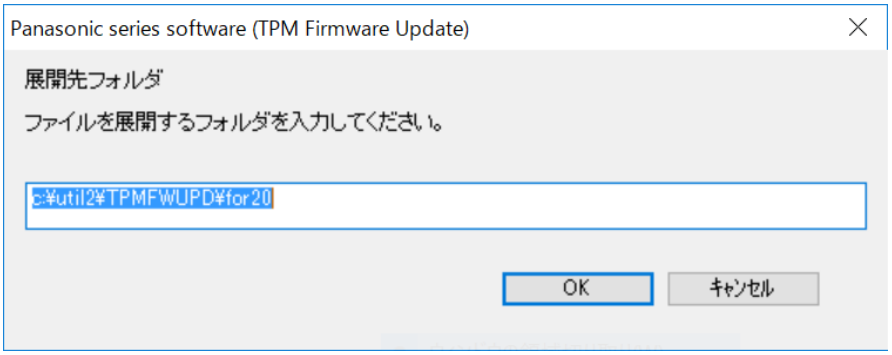
1　TPM 2.0 ファームウェア更新ツールのダウンロードと展開

ダウンロードページに掲載されているプログラム(TPM20FWUpdate551561.exe) をダウンロードした後、対象機種の Windows 上で実行し、作業用フォルダにファイルを展開します。

1) ダウンロードしたプログラムをダブルクリックして実行します。
「ユーザーアカウント制御」の画面が表示されたら、[はい(Y)]をクリックします。

2) 使用許諾契約の画面が表示されますので、内容をよくお読みいただき、[はい(Y)]をクリックしてください。

3) 展開先フォルダを設定する画面が表示されます。作業用フォルダは、プログラムが自動的に作成しますので、特に変更する必要はありません。(変更する場合は、必ず、本体内蔵のハードディスク/SSD 上のフォルダを指定してください)
展開先フォルダは標準では「c:¥util2¥TPMFWUPD¥for20」が設定されています。
[OK]をクリックしてください。



しばらくすると展開が完了し、展開されたフォルダが開きます。(展開が完了するには約 20 秒かかります)

2　ファームウェアバージョン等を確認する

以下の方法で確認できます。(“製造元のバージョン”がファームウェアバージョンです)

1) tpm.msc を起動し、画面内容を確認する。
- “製造元名”が 、IFX 以外の場合は、本 TPM 2.0 ファームウェア更新の対象外ですので、以降の処理は不要です。
- ”製造元のバージョン”が 5.51、5.61 のいずれでもない場合は、本 TPM 2.0 ファームウェア更新の対象外ですので、以降の処理は不要です。
- ”仕様バージョン”が 1.2 の場合は、本 TPM 2.0 ファームウェア更新の対象外です。TPM1.2 ファームウェア更新をご使用ください。

更新用のファームウェアデータはファームウェアバージョンによって異なりますので、バージョンに応じてTPM 2.0 ファームウェア更新ツールの展開先フォルダにある以下のバッチファイルをご使用ください。

5.51 の場合： UPD551.bat

5.61 の場合： UPD561.bat

後の手順でファームウェア更新を実行する際、このファイル名を入力する必要がありますので、念のためメモをとっておいてください。

(本手順書ではファームウェアバージョン 5.61 の場合の画面例を示しています。)

3 (BitLocker が有効化されている場合) BitLocker を"無効"または"保護の中断"に変更する

「5 TPM をクリアする」を実行すると、次回の Windows 起動時に回復キーの入力が求められる場合があります。

回復キーを紛失されている場合はシステムが起動できなくなりますので、ここでファームウェアの更新手順を中止し、以降の手順は実行しないでください。

回復キーが保管されていて、必要に応じて回復キーを手入力できる場合は、下記を参照して BitLocker を"保護の中断" あるいは無効に変更してください。

「4 BitLocker 関連手順」

(無効に変更した場合は、BitLocker の無効化処理が完了してから以降の手順を実行してください。
無効化処理の完了には、数 10 分から数時間程度の時間がかかります)

4 TPM の自動プロビジョニング機能を、いったん無効化する。

1) スタート > Windows PowerShell > Windows PowerShell ISE を右クリック > その他 > 管理者として実行

「ユーザーアカウント制御」の画面が表示されたら、[はい(Y)]をクリックする。

2) 表示 > コマンドアドオンを表示 にチェックを付け、コマンド画面を表示させる。
3) 右ウィンドウのコマンド画面を選択し、”モジュール：”から TrustedPlatformModule を選ぶ
4) 右下部のウィンドウから Disable-TPMAutoProvisioning を選ぶ
5) ウィンドウ下部の 挿入 ボタンを押す (左のウィンドウに Disable…が挿入される)
6) 左ウィンドウを選択し、ENTER キーを押す
7) 右上隅の[x]アイコン押し、PowerShell を閉じる

5 TPM をクリアする

1) BitLocker を使用している場合、無効 または 保護の中断 となっていることを確認する。
(BitLocker が有効になっている場合は、「4 BitLocker 関連手順」を参照し“保護の中断”に変更してください)

2) tpm.msc を起動する

3) 右のウィンドウの“TPM クリア”をクリックし、再起動を選択する。

4) 起動時に TPM クリアの確認が求められた場合は、F12 キーを押す。(ソフトウェアキーボードの場合、SYM キーを押した後 F12 を押す)

6 TPM の無効化

1) コマンドプロンプトを起動し、TPM 2.0 ファームウェア更新ツールを展開したフォルダに移動する。

cd /D c:¥util2¥TPMFWUPD¥for20 (ENTER) (デフォルト時)

(ハードディスク/SSD を 2 個搭載しているモデルでは、コマンドプロンプトで C:と D:が入れ替わって見える場合があります。その場合 C:を D:と読み替えてください。)

2) TPM を無効化するバッチファイルを実行する

DiscTPM.bat (ENTER)

7 トラブルシューティング内のコマンドプロンプトを起動する。

1) スタート > 設定 > 更新とセキュリティ > 回復 > PC の起動をカスタマイズする > 今すぐ再起動する

2) トラブルシューティング > 詳細オプション > コマンドプロンプト

トラブルシューティング内のコマンドプロンプトが起動する

8 ファームウェアの更新と TPM の有効化

1) アカウントを選択し、パスワードを入力する。 -> コマンドプロンプトが起動される

2) TPM 2.0 ファームウェア更新ツールを展開したフォルダに移動する。

cd /D c:¥util2¥TPMFWUPD¥for20 (ENTER) (デフォルト時)

(ハードディスク/SSD を 2 個搭載しているモデルでは、コマンドプロンプトで C:と D:が入れ替わって見える場合があります。その場合 C:を D:と読み替えてください。)

3) ファームウェア更新と TPM の有効化を行うバッチファイルを実行する

UPD561.bat (ENTER) (ファームウェアバージョン 5.61 の場合)

または

UPD551.bat (ENTER) (ファームウェアバージョン 5.51 の場合)

4) 何かキーを押した後、”続行”をクリックする

5) Windows が起動する

9 TPM の自動プロビジョニング機能を有効化する

1) スタート > Windows PowerShell > Windows PowerShell ISE を右クリック > その他 > 管理者として実行

「ユーザーアカウント制御」の画面が表示されたら、[はい(Y)]をクリックする。

2) 表示 > コマンドアドオンを表示 にチェックを付け、コマンド画面を表示させる。

3) 右ウィンドウのコマンド画面を選択し、”モジュール:”から TrustedPlatformModule を選ぶ

4) 右下部のウィンドウから Enable-TPMAutoProvisioning を選ぶ

5) ウィンドウ下部の 挿入 ボタンを押す（左のウィンドウに Enable…が挿入される）

6) 左ウィンドウを選択し、ENTER キーを押す

7) スタート ＞（左下隅の）電源アイコン を右クリック

8) 再起動 をクリックする

10 ファームウェアバージョンの確認

1) TPM の自動プロビジョニング完了まで、１分程度待つ

2) tpm.msc を起動する

3) 表示される “製造元のバージョン”が 5.62.xxx に更新されていることを確認する。

11 更新されたファームウェアで鍵ペアを再作成するために、TPM を初期化する。

1) BitLocker を使用している場合、無効 または 保護の中断 となっていることを確認する。
（BitLocker が有効になっている場合は、「2.動作条件と注意点」を参照し“保護の中断”に変更する）

2) tpm.msc を起動する

3) 右のウィンドウの“TPM クリア”をクリックし、再起動を選択する。

4) 起動時に TPM クリアの確認が求められた場合は、F12 キーを押す。（ソフトウェアキーボードの場合、SYM キーを押した後 F12 を押す

12 TPM の状態を確認する。

ログイン後、Windows の処理が完了するのを１分ほど待ち、状態を確認する。
（処理が完了していない場合、TPM が正しく認識されなかったり、処理完了前の状態が表示されたりする場合があります。そのような場合は、数分待ってから“最新の情報に更新”をクリックしてみてください。）

1) Tpm.msc を起動し、状態が“TPM は使用する準備が出来ています”となっていることを確認する。

2) BitLocker を使用していた場合は、有効状態に戻っていることを確認する。（確認方法は、４ BitLocker 関連手順 を参照してください）

４ BitLocker 関連手順

BitLocker の状態確認や設定変更には、コマンドプロンプトでコマンド実行する方法と「BitLocker ドライブ暗号化」ウィンドウの画面操作を行う方法があります。

４．１ コマンドプロンプトでコマンド実行する方法

以下の手順で、現在の状態が確認できます。

1) 管理者権限でコマンドプロンプトを開く

1-1) Windows キー と r キーを同時に押す

1-2) Explorer.exe c:¥windows¥system32 と入力し、ENTER キーを押す

1-3) 右側のウィンドウから[cmd]（拡張子を表示している場合は [cmd.exe]）を
右クリックし、[管理者として実行]をクリックする。
「ユーザーアカウント制御」の画面が表示されたら、[はい(Y)]をクリックする。

(以降、更新手順で「管理者権限でコマンドプロンプトを開く」と説明されている場合も、上記の操作を行ってください)

2) Manage-bde.exe -status C: と入力し、ENTER を押す
(C:ドライブに Windows がインストールされている場合)

“保護状態：保護はオンです”と表示された場合、BitLocker は有効状態です。
“保護状態：保護はオフです（残り１回の再起動)”と表示された場合、BitLocker は”保護の中断”状態です。
(“BitLocker のバージョン： None”と表示される場合、ご使用の Windows で BitLocker はサポートされていません)

保護の中断は、以下の手順で設定することができます。

1) 管理者権限でコマンドプロンプトを開く
2) Manage-bde.exe -protectors -disable C: と入力し、ENTER を押す
(C:ドライブに Windows がインストールされている場合)

また、BitLocker の無効化は以下の手順で設定することができます。

1) 管理者権限でコマンドプロンプトを開く
2) Manage-bde.exe -off C: と入力し、ENTER を押す
(C:ドライブに Windows がインストールされている場合)

４．２ 「BitLocker ドライブ暗号化」ウィンドゥの画面操作を行う方法

以下の手順で、現在の状態が確認できます。

1) Windows キー と e キーを同時に押し、エクスプローラを開く
2) 左側のウィンドウで“PC”をクリックする
3) 右側のウィンドウで Windows がインストールされたドライブ(デフォルトは C:)を右クリックする
4) “BitLocker の管理(B)”をクリックする

「BitLocker ドライブ暗号化」ウィンドウが表示され、“オペレーティングシステム ドライブ“の下に現在の BitLocker の状態が表示されています。
4) の手順で“BitLocker の管理(B)”の項目が表示されない場合、ご使用の Windows で BitLocker はサポートされていません。

BitLocker の”保護の中断”は、「BitLocker ドライブ暗号化」ウィンドウの“オペレーティングシステム ドライブ“で、以下の手順を行うことで設定できます。

1) “保護の中断”をクリックする。
   (「ユーザーアカウント制御」の画面が表示されたら、[はい(Y)]をクリックする)
2) 確認ウィンドウが表示されるので“はい”をクリックする

また BitLocker の無効化は、この画面で以下の手順を行うことで設定できます。

1) “BitLocker を無効にする”をクリックする。
   (「ユーザーアカウント制御」の画面が表示されたら、[はい(Y)]をクリックする)
2) 確認ウィンドウが表示されるので“はい”をクリックする
   (無効化が完了するまで、数 10 分から数時間程度の時間がかかります)

以上