TPM 1.2 ファームウェア更新手順書
(対象 OS : Windows 7, Windows 8.1, Windows 10)

公開日 2017/11/14
更新日 2018/05/17

1 はじめに

- TPM を使用しない場合は TPM ファームウェアの更新は不要です。
  現在または将来 TPM をご使用の場合は、TPM ファームウェアを更新してください。

  現在の TPM の使用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 は使用されていません。

・互換性のある TPM が見つかりません
・TPM はオフで、所有権は取得されていません。
・TPM はオンで、所有権は取得されていません。

(“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 1.2 の場合の手順です。
仕様バージョンが 2.0 と表示されている場合は、本 TPM 1.2 ファームウェア更新の対象外です。
今後公開予定の TPM2.0 ファームウェア更新をご使用ください。

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。

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
(項目がない場合、ご使用の機種で「デバイスの暗号化」機能はサポートされていません)

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 の状態は以下の手順でご確認いただけます。

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

(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) (C:ドライブに Windows がインストールされている場合)

Manage-bde.exe -status C: と入力し、ENTER を押す

“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)

BitLocker の“保護の中断”は以下の手順で設定できます。

1) 管理者権限でコマンドプロンプトを開く

2) (C:ドライブに Windows がインストールされている場合)

Manage-bde.exe -protectors -disable C: と入力し、ENTER を押す

BitLocker の“BitLocker を無効にする”は以下の手順で設定できます。

1) 管理者権限でコマンドプロンプトを開く

2) (C:ドライブに Windows がインストールされている場合)

Manage-bde.exe -off C: と入力し、ENTER を押す

・(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

3.0 共通

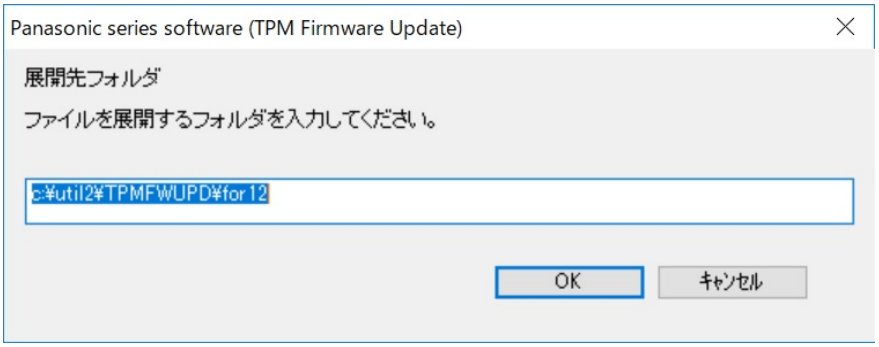
1　TPM 1.2 ファームウェア更新ツールのダウンロードと展開

ダウンロードページに掲載されているプログラム(TPM12FWUpdate432440.exe) をダウンロードした後、対象機種の Windows 上で実行し、作業用フォルダー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) 展開先フォルダーを設定する画面が表示されます。作業用フォルダーは、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 上のフォルダーを指定してください)
展開先フォルダーは標準では「c:¥util2¥TPMFWUPD¥for12」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ーが開きます。(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 1.2 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 4.32、4.40 のいずれでもない場合は、本 TPM 1.2 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 2.0 の場合は、本 TPM 1.2 ファームウェア更新の対象外です。今後公開予定の TPM2.0 ファームウェア更新をご使用ください。

ご使用いただく TPM 1.2 ファームウェア更新ツールは、ファームウェアバージョンによって異なります。

4.32 の場合は、FWUpdate432 フォルダー内の

IFXTPMUpdate_TPM12_v0434.exe

ChgOSMng.bat

OSMngOrg.bat

4.40 の場合は、FWUpdate440 フォルダー内の

IFXTPMUpdate_TPM12_v0443.exe

ChgOSMng.bat

OSMngOrg.bat

です。

それぞれのフォルダー内には IFXTPMUpdate_TPM12_vXXXX.exe の他に、コマンドラインで動作する MS-DOS アプリケーション IFXTPMUpdate_TPM12_vXXXX.com も置かれています。
ソフトを起動する際、誤って com を起動することのないよう、エクスプローラはファイル名拡張子を表示する設定でご使用いただくことをおすすめします。(拡張子を表示する場合は、エクスプローラの“表示“タブ内の”ファイル名拡張子“にチェックをつけてください。)

(本手順書ではファームウェアバージョン 4.40 の場合の画面例を示しています。)

3　以降、ご使用の OS に応じて、手順を進めてください。
TPM 1.2 ファームウェアの更新には現在設定されている TPM 所有者パスワードが必要です。

TPM 所有者パスワードの管理方法はご使用の OS により異なるため、ファームウェア更新手順は、

3.1 Windows 10 バージョン 1607 以降の場合

3.2 Windows 10 バージョン 1511, 1507 の場合

3.3 Windows 8.1 の場合

3.4 Windows 7 (Infineon TPM Professional Package で TPM の初期化を行った場合)

3.5 Windows 7 (Windows の設定画面またはコマンドで TPM の初期化を行った場合)

で相違がありますのでご注意ください。

Windows のバージョン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)　winver と入力し、ENTER キーを押す

3.1 Windows 10 バージョン 1607 以降の場合

1　TPM 所有者情報の管理法を一時的に変更する。

1) 展開先フォルダー内の、[ChgOSMng]（拡張子を表示している場合は [ChgOSMng.bat]）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場合は、[はい]をクリックする。

([管理者として実行]で起動しないと、管理法の設定変更が行えず以降のファームウェア更新手順が正しく実行できません。)

2　TPM 所有者認証情報を Windows に登録する

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)

5) ログイン後、Windows の処理が完了するのを 1 分ほど待ち、tpm.msc を起動する。

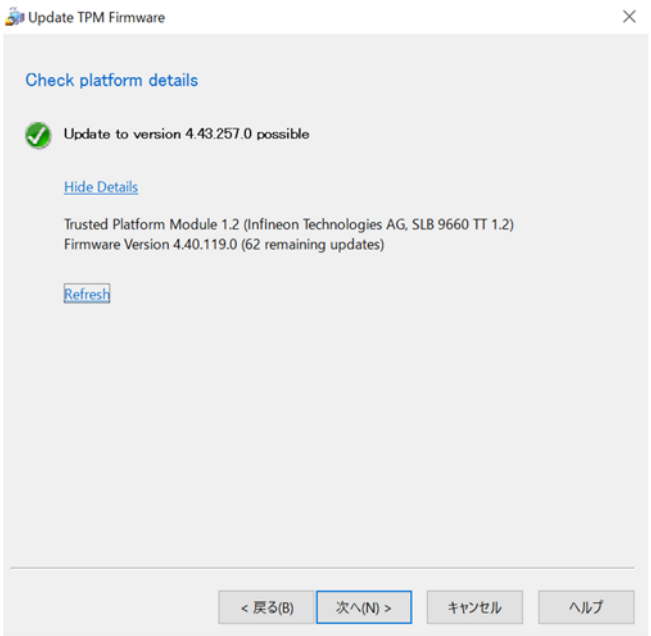
(tpm.msc が起動されていた場合、TPM が正しく認識されなかったり、処理完了前の状態が表示されたりする場合があります。そのような場合は、数分待ってから“最新の情報に更新”をクリックしてみてください。)

6) “状態”が[TPM は使用する準備ができています。] となっているのを確認する。

3　IFXTPMUpdate_TPM12_vxxxx.exe を起動する。

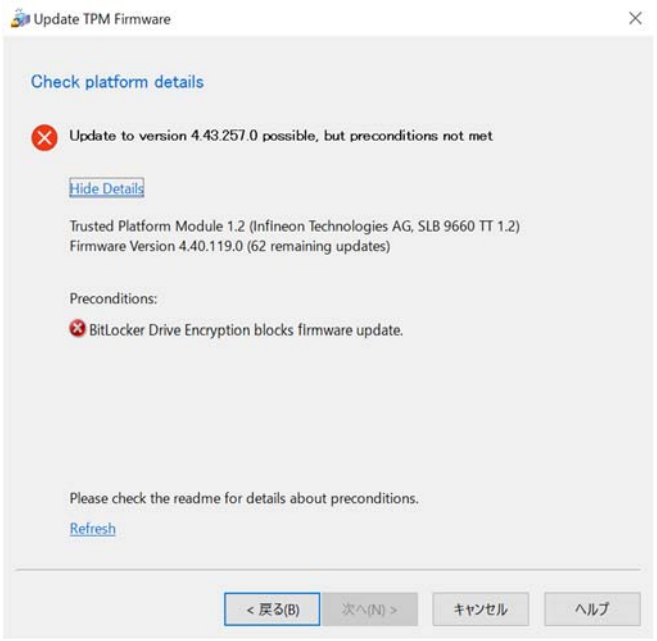
BitLocker が有効になっている場合は、無効 または "保護の中断" に変更してください。
・保護の中断" あるいは 無効 に変更する方法は、「2 .動作条件と注意点」を参照してください。

画面表示に従って “次へ“ または ”キャンセル“ ボタンを押し処理を進めていく。

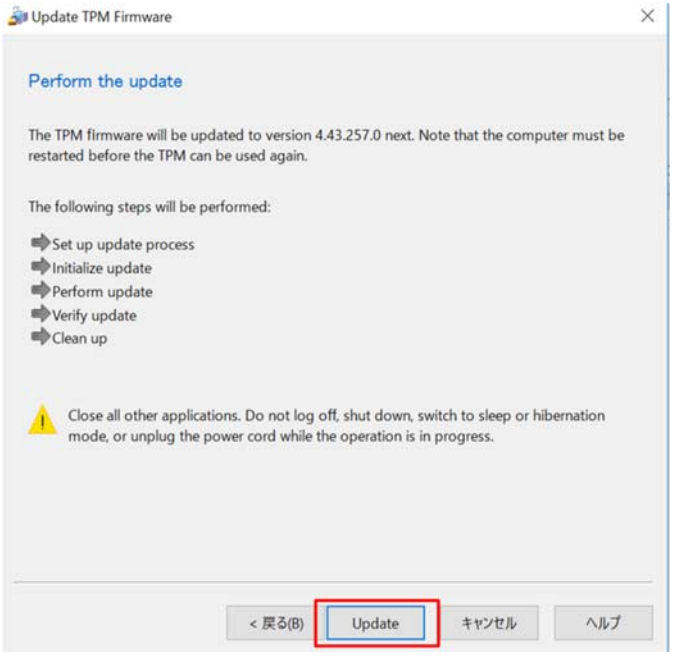


（注意）画面に Update to version 4.xx.xxx possible, but preconditions not met と表示される場合は、ファームウェア更新を行うことはできません。Preconditions: に表示されたメッセージの対訳をご覧ください。

（対訳は本書末尾に記載しています）

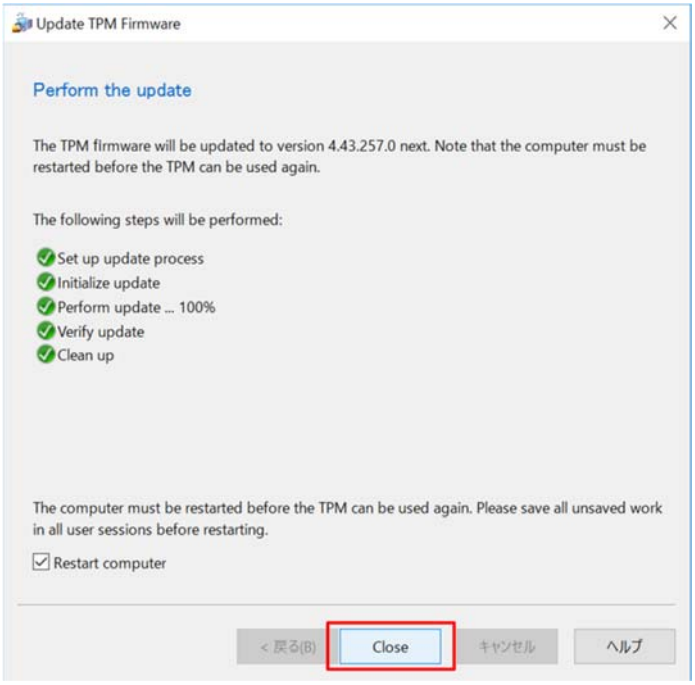


4　更新を実行する



5　処理完了後、PC を再起動する。

（“Restart computer”のチェックを付けたままで“Close”を押すと再起動します）



6　TPM 所有者情報の管理法の設定を元に戻す

1）展開先フォルダー内の、[OSMngOrg]（拡張子を表示している場合は［OSMngOrg.bat]）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場合は、[はい]をクリックする。

7　ファームウェア版数の確認

1）tpm.msc を起動し画面中の“状態”に［TPM は使用する準備ができています。］と表示されており、“製造元のバージョン”が更新されていることを確認する。

・4.32 は 4.34 に、4.40 は 4.43 に更新されます。

8　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）

5）ログイン後、Windows の処理が完了するのを 1 分ほど待ち、tpm.msc を起動する。

（tpm.msc が起動されていた場合、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。）

3.2 Windows 10 バージョン 1511, 1507 の場合

1　TPM の状態を確認する。

1) tpm.msc を起動する

2) TPM 管理画面で“状態”の表示を確認する。

[TPM は使用する準備ができています。]と表示されている場合は、2 の手順に進んでください。

[TPM を制限された機能で使用する準備ができました]と表示されている場合は、Windows が TPM 所有者認証情報を認識できていないためファームウェア更新は実行できませんので、以下の手順により、いったん TPM をクリアしてください。

(TPM クリアの方法)

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)

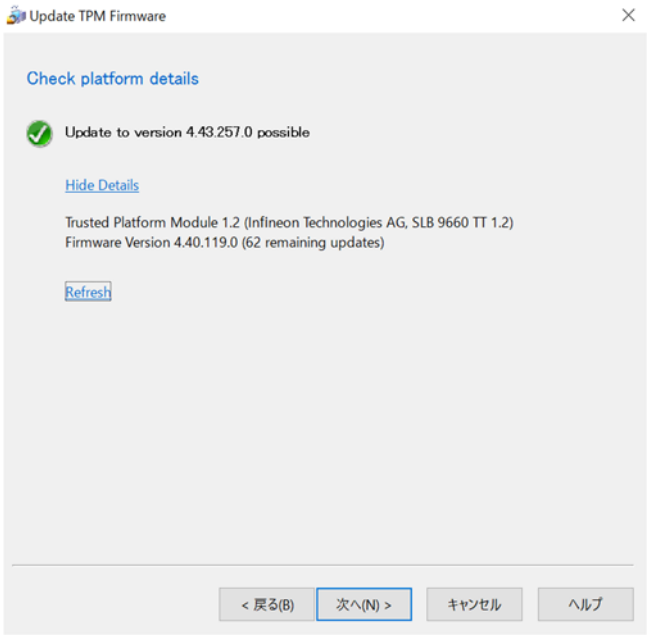
5) ログイン後、Windows の処理が完了するのを 1 分ほど待ち、tpm.msc を起動する。
(tpm.msc が起動されていた場合、TPM が正しく認識されなかったり、処理完了前の状態が表示されたりする場合があります。そのような場合は、数分待ってから“最新の情報に更新”をクリックしてみてください。)

6) 状態”が[TPM は使用する準備ができています。] となっているのを確認する。

2　IFXTPMUpdate_TPM12_vxxxx.exe を起動する。

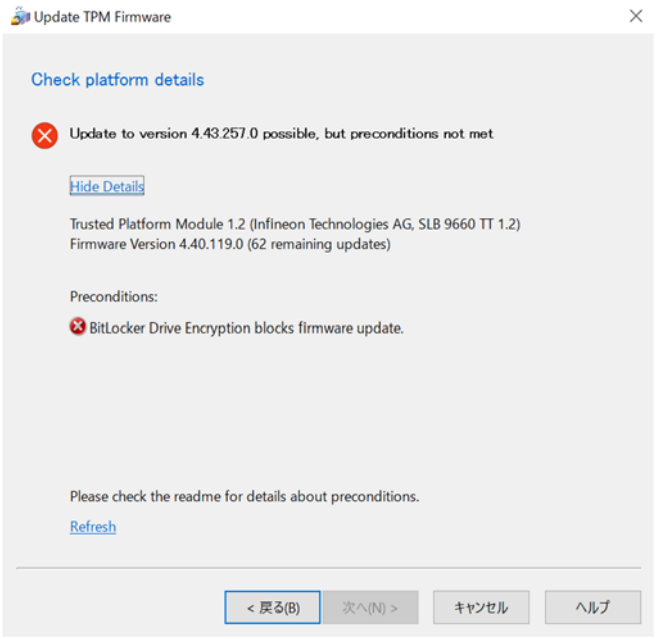
BitLocker が有効になっている場合は、無効 または "保護の中断" に変更してください。
・保護の中断" あるいは 無効 に変更する方法は、「2 .動作条件と注意点」を参照してください。

画面表示に従って “次へ“ または ”キャンセル“ ボタンを押し処理を進めていく。

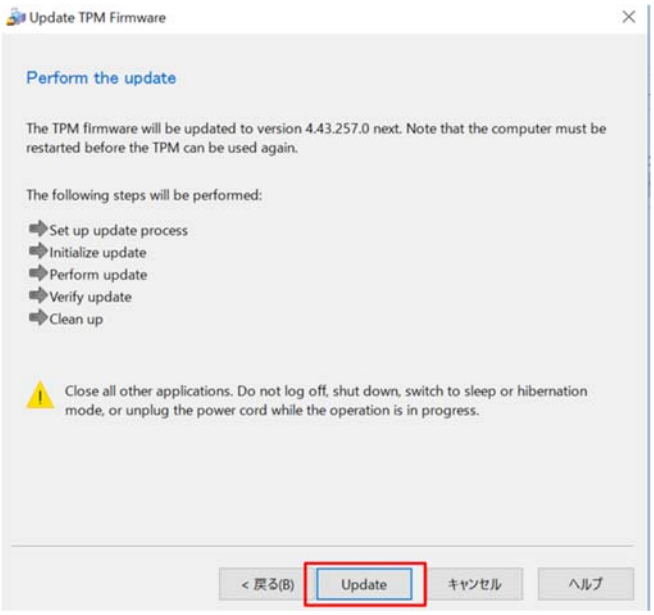


（注意）画面に Update to version 4.xx.xxx possible, but preconditions not met と表示される場合は、ファームウェア更新を行うことはできません。Preconditions: に表示されたメッセージの対訳をご覧ください。

（対訳は本書末尾に記載しています）

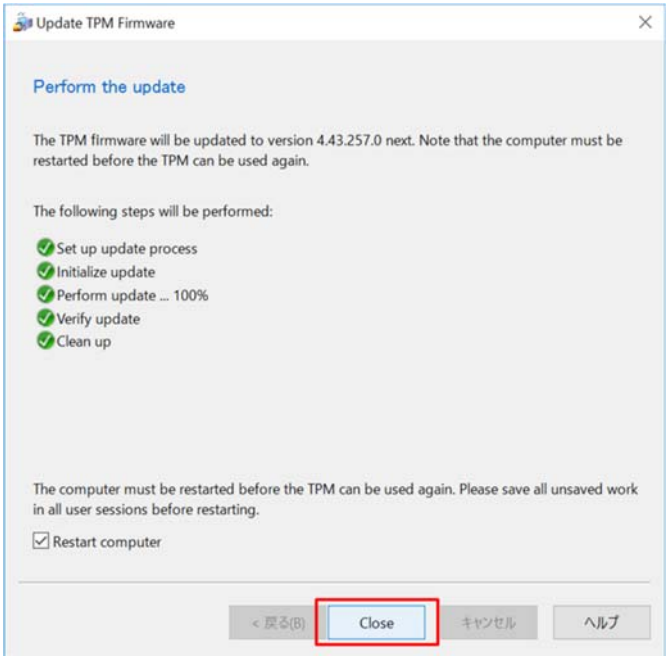


3　　更新を実行する



4　　処理完了後、PC を再起動する。

（“Restart computer”のチェックを外さずに、“Close”を押すと再起動します）



5　　ファームウェア版数の確認

1）tpm.msc を起動し画面中の“状態”に［TPM は使用する準備ができています。］と表示されており、“製造元のバージョン”が更新されていることを確認する。

・4.32 は 4.34 に、4.40 は 4.43 に更新されます。

6　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)

5) ログイン後、Windows の処理が完了するのを 1 分ほど待ち、tpm.msc を起動する。
(tpm.msc が起動されていた場合、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。)

6) “状態”が[TPM は使用する準備ができています。] となっているのを確認する。

3.3 Windows 8.1 の場合

1　Infineon TPM Professional Package がインストールされているかチェックする。

インストールされている場合、ファームウェアの書換え前後でデータの保存と復元が必要です。下記手順で確認してください。

1)　スタート > コントロールパネル > プログラム > プログラムと機能 を開く

2)　表示されるプログラム一覧中に “Infineon TPM Professional Package”があるかを確認する。
ない場合は 2, 3 の手順は不要です。4 以降の手順から実行してください。

2　今回発見された脆弱性に対策するためには、以前作成したキー/証明書の使用を終了し、ファームウェアの更新とキー/証明書の再作成を行う必要があります。

そのため更新手順は

TPM Professional Package で作成した既存のキー/証明書で保護しているデータの保護をすべて解除

ファームウェアの更新

TPM Professional Package を用いた TPM の初期化とキー/証明書の再作成

新たな鍵によるデータ保護の再設定

となります。

作成済のキー/証明書の使用を終了せずファームウェア更新だけを行っても完全な対策とはなりませんので、作成済の鍵/証明書を継続使用する必要がある場合ファームウェア更新は行わないでください。

また、以降の手順で、TPM をクリアする際に BIOS のスーパーバイザーパスワードが必要になります。

3　Infineon TPM Professional Package で保護(暗号化)されていた情報(*)がある場合、保護(暗号化)の解除やリムーバブルディスクなどへのバックアップを行ってください。解除やバックアップは Windows アカウント単位で行ってください。

(*) Personal Secure Drive 内のデータ、%UserProfile%¥Documents に作成される″暗号化されたデータ″という名前のフォルダーや暗号化ファイルシステム(EFS)で暗号化を行ったフォルダー/ファイルなどです。

4　TPM の状態を確認する。

1) tpm.msc を起動する

2) TPM 管理画面で“状態”の表示を確認する。

[TPM は使用する準備ができています。]と表示されている場合は、5 の手順に進んでください。

[TPM を制限された機能で使用する準備ができました]と表示されている場合は、Windows が TPM 所有者認証情報を認識できていないためファームウェア更新は実行できませんので、以下の手順により、いったん TPM をクリアしてください。

(TPM クリアの方法)

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)

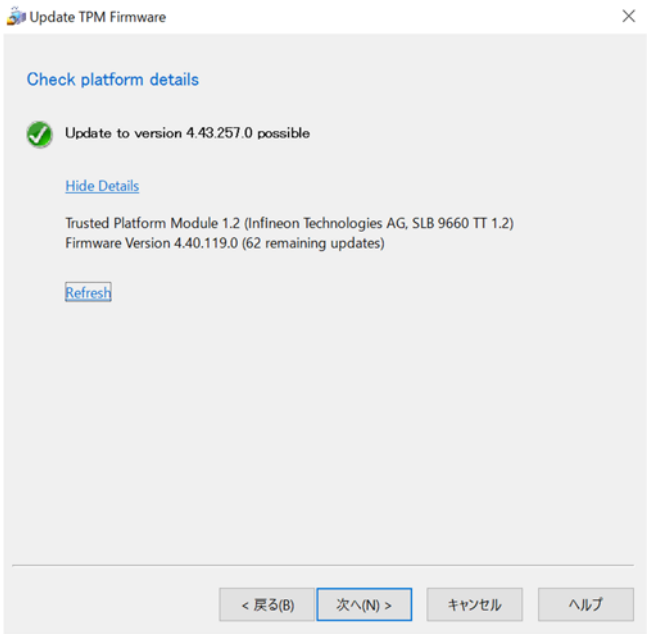
5) ログイン後、Windows の処理が完了するのを 1 分ほど待ち、tpm.msc を起動する。
(tpm.msc が起動されていた場合、TPM が正しく認識されなかったり、処理完了前の状態が表示されたりする場合があります。そのような場合は、数分待ってから“最新の情報に更新”をクリックしてみてください。)

6) 状態”が[TPM は使用する準備ができています。] となっているのを確認する。

5 IFXTPMUpdate_TPM12_vxxxx.exe を起動する。

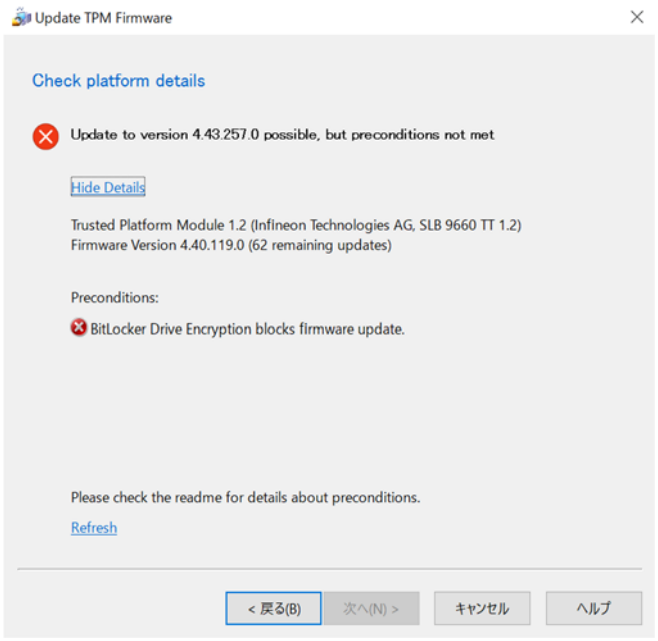
BitLocker が有効になっている場合は、無効 または "保護の中断" に変更してください。
・保護の中断" あるいは 無効 に変更する方法は、「2 .動作条件と注意点」を参照してください。

画面表示に従って “次へ“ または ”キャンセル“ ボタンを押し処理を進めていく。

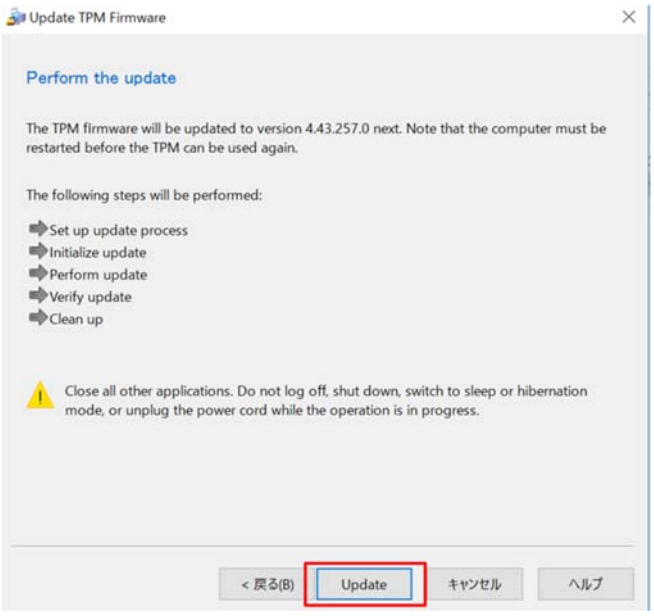


（注意）画面に Update to version 4.xx.xxx possible, but preconditions not met と表示される場合は、ファームウェア更新を行うことはできません。Preconditions: に表示されたメッセージの対訳をご覧ください。

（対訳は本書末尾に記載しています）

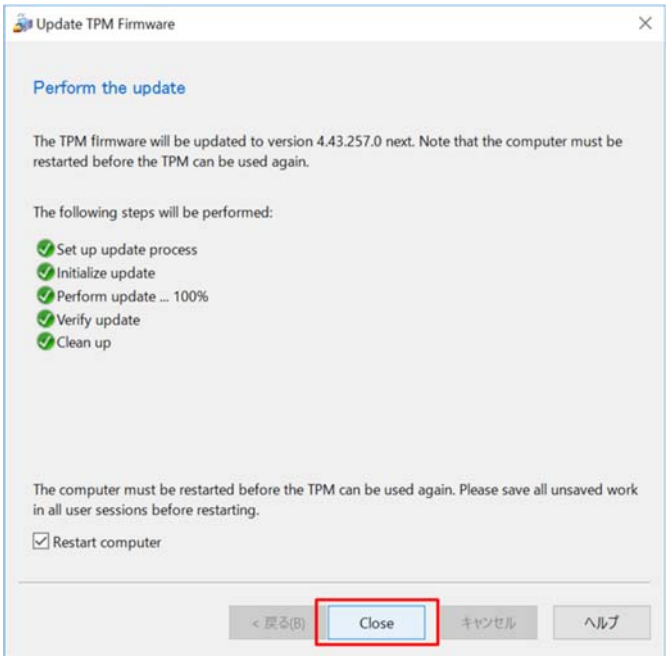


6　　更新を実行する



7　処理完了後、PC を再起動する。

（“Restart computer”のチェックを外さずに、“Close”を押すと再起動します）



8　ファームウェア版数の確認

2）tpm.msc を起動し画面中の“状態”に［TPM は使用する準備ができています。］と表示されており、“製造元のバージョン”が更新されていることを確認する。

・4.32 は 4.34 に、4.40 は 4.43 に更新されます。

9　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。

2）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）

5）ログイン後、Windows の処理が完了するのを 1 分ほど待ち、tpm.msc を起動する。

（tpm.msc が起動されていた場合、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。）

6）“状態”が［TPM は使用する準備ができています。］となっているのを確認する。

10　(Infineon TPM Professional Package がインストールされていた場合)

Infineon Security Platform 初期化ウィザード を実行する

1) タスクトレイに“Security Platform の復元”の案内が表示されても、無視して復元操作は行わない(復元操作を行った場合、キー/証明書は再作成されません)

2) タスクトレイの Security Platform アイコン 

を右クリックし、(盾のアイコン表示が付いている)“Security Platform を管理する”をクリックする

3) 「全般」以外のタブを選択すると自動的に初期化ウィザードが表示されるので、画面指示に従い初期化(Security Platform 所有者の作成、機能選択など)を行う。
(設定は「詳細設定初期化(詳しい知識のあるユーザー向け)」で行ない、また復元ではなく“Security Platform の初期化”を行ってください。ファームウェア更新前に作成されたファイルへの上書き確認が表示された場合は、「既存のファイルを置き換える」を選択してください。その他、詳細は Infineon TPM Professional Package のマニュアルをご参照ください。)

4) 引き続き、タスクトレイから現在のユーザーに対する初期化を促すポップアップが表示されるので、クリックし“Security Platform クイック初期化ウィザード”を起動する。

5) 「詳細設定初期化(詳しい知識のあるユーザー向け)」を選択し、画面指示に従い初期化(基本ユーザーパスワード関連の設定、Security Platform の機能の選択など)を行う。

6) 保護(暗号化)を解除してリムーバブルディスクなどにバックアップを取ったデータを使用して、Infineon TPM Professional Package による保護(暗号化)を再設定してください。

3.4 Windows 7 (Infineon TPM Professional Package を使用して TPM の初期化を行っていた場合)

1　Infineon TPM Professional Package がインストールされているかチェックする

3)　スタート ＞ コントロールパネル ＞ プログラム ＞ プログラムと機能 を開く

4)　表示されるプログラム一覧中に “Infineon TPM Professional Package”があるかを確認する。
ない場合は、TPM の初期化は他の方法で行われたと考えられますので「3.5 Windows 7 (Windows の設定画面またはコマンドで TPM の初期化を行った場合)」の手順を実施してください。

2　Infineon TPM Professional Package で TPM の初期化が行われたかをチェックする

1)　スタート ＞ すべてのプログラム ＞ Infineon Security Platform ソリューション ＞ Security Platform の管理 をクリックする。

“Security Platform の状態” の “所有者” が “初期化完了” の場合は 3 の手順に進んでください。

”初期化完了(モード１)” あるいは“初期化完了(モード２)”の場合は、Windows あるいは他のソフトウェアを使用して TPM の初期化が行われています。
Infineon TPM Professional Package で保護(暗号化)されていた情報(*)は、保護(暗号化)の解除やリムーバブルディスクなどへのバックアップを行ってから「3.5 Windows 7 (Windows の設定画面またはコマンドで TPM の初期化を行った場合)」の手順を実施してください。解除やバックアップは Windows アカウント単位で行ってください。

(*) Personal Secure Drive 内のデータ、%UserProfile%¥Documents に作成される″暗号化されたデータ″という名前のフォルダーや暗号化ファイルシステム(EFS)で暗号化を行ったフォルダー/ファイルなどです。

3　今回発見された脆弱性に対策するためには、以前作成したキー/証明書の使用を終了し、ファームウェアの更新とキー/証明書の再作成を行う必要があります。

そのため更新手順は

TPM Professional Package で作成した既存のキー/証明書で保護しているデータの保護をすべて解除
ファームウェアの更新
TPM Professional Package を用いた TPM の初期化とキー/証明書の再作成
新たな鍵によるデータ保護の再設定

となります。

作成済のキー/証明書の使用を終了せずファームウェア更新だけを行っても完全な対策とはなりませんので、作成済の鍵/証明書を継続使用する必要がある場合ファームウェア更新は行わないでください。

また、以降の手順で、TPM をクリアする際に BIOS のスーパーバイザーパスワードが必要になります。

4　Infineon TPM Professional Package で保護(暗号化)されていた情報(*)がある場合、保護(暗号化)の解除やリムーバブルディスクなどへのバックアップを行ってください。解除やバックアップは Windows アカウント単位で行ってください。

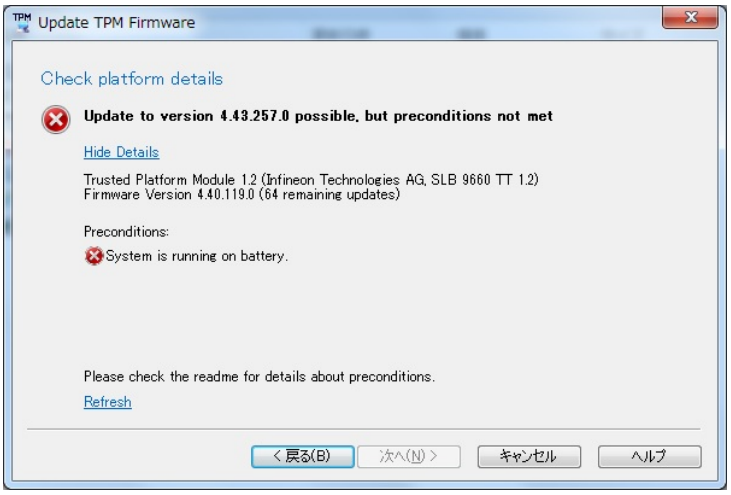
(*) Personal Secure Drive 内のデータ、%UserProfile%¥Documents に作成される"暗号化されたデータ"という名前のフォルダーや暗号化ファイルシステム(EFS)で暗号化を行ったフォルダー/ファイルなどです。

5　IFXTPMUpdate_TPM12_vxxxx.exe を起動する。

BitLocker が有効になっている場合は、無効 または "保護の中断" に変更してください。
・保護の中断" あるいは 無効 に変更する方法は、「2 .動作条件と注意点」を参照してください。

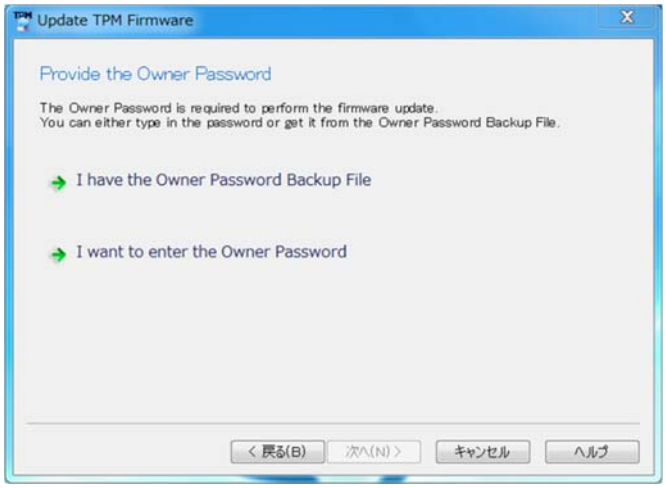
画面表示に従って “次へ“ または ”キャンセル“ ボタンを押し処理を進めていく。

（注意）画面に Update to version 4.xx.xxx possible, but preconditions not met と表示される場合は、ファームウェア更新を行うことはできません。Preconditions: に表示されたメッセージの対訳をご覧ください。(対訳は本書末尾に記載しています)

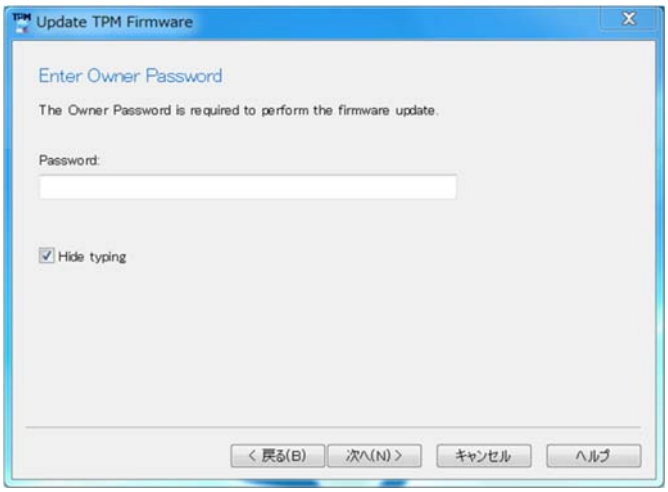


6　　TPM 所有者パスワードを確認する

“I want to enter the Owner Password”を選択して次に進んでください。



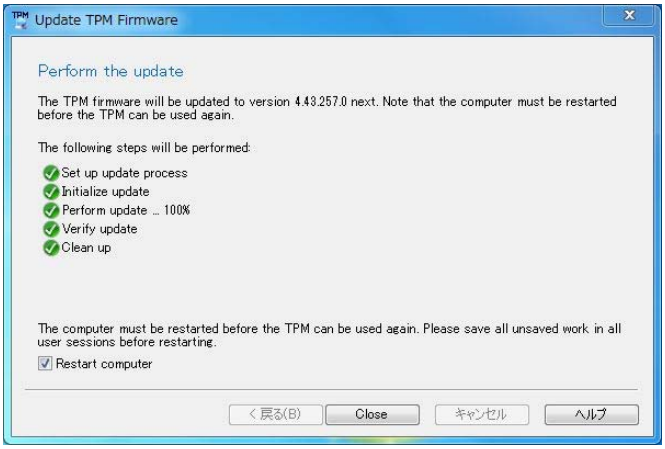
7　　TPM 所有者パスワードを入力する



8　更新を実行する

9　処理完了後 PC を再起動し､Panasonic ロゴ画面が表示されるとすぐに F2 キーを(キーボードのない機種の場合、画面左上隅を)複数回押下し BIOS メニューに入る。

(“Restart computer”のチェックを外さずに、“Close”を押すと再起動します。)



10　TPM をクリアする

1)　BIOS メニュー上部に表示されている“セキュリティ”をクリックする。
2)　スーパーバイザーパスワードを設定していない場合は、次の操作で必要なので設定する。
3)　“内蔵セキュリティ(TPM)“を選択し、ENTER キー押す
4)　“待機中の TPM 操作”から、所有者情報の初期化 を選び、ESC キーを押す
5)　2)でスーパーバイザーパスワードを設定した場合、解除する
6)　BIOS メニュー上部に表示されている“終了”をクリックする。
7)　“設定を保存して再起動”を選択し、ENTER キーを押す
8)　Windows が起動するのでログオンする

11　ファームウェア版数の確認

1)　スタート> すべてのプログラム > Infineon Security Platform ソリューション> Security Platform の管理 を起動する

2)　“全般”タブの“詳細”ボタンをクリックする

3)　“FW バージョン”を確認する

更新前のバージョンが 4.32 の場合は 4.34 に、4.40 の場合は 4.43 に更新されます。

12　Infineon Security Platform 初期化ウィザード を実行する

7)　タスクトレイに“Security Platform の復元”の案内が表示されても、無視して復元操作は行わない(復元操作を行った場合、キー/証明書は再作成されません)

8)　タスクトレイの Security Platform アイコン 

を右クリックし、(盾のアイコン表示が付いている)“Security Platform を管理する”をクリックする

9)　「全般」以外のタブを選択すると自動的に初期化ウィザードが表示されるので、画面指示に従い初期化(Security Platform 所有者の作成、機能選択など)を行う。
(設定は「詳細設定初期化(詳しい知識のあるユーザー向け)」で行ない、また復元ではなく“Security Platform の初期化”を行ってください。ファームウェア更新前に作成されたファイルへの上書き確認が表示された場合は、「既存のファイルを置き換える」を選択してください。その他、詳細は Infineon TPM Professional Package のマニュアルをご参照ください。)

10)　引き続き、タスクトレイから現在のユーザーに対する初期化を促すポップアップが表示されるので、クリックし“Security Platform クイック初期化ウィザード”を起動する。

11)　「詳細設定初期化(詳しい知識のあるユーザー向け)」を選択し、画面指示に従い初期化(基本ユーザーパスワード関連の設定、Security Platform の機能の選択など)を行う。

12)　保護(暗号化)を解除してリムーバブルディスクなどにバックアップを取ったデータを使用して、Infineon TPM Professional Package による保護(暗号化)を再設定してください。

3.5 Windows 7 (Windows の設定画面またはコマンドで TPM の初期化を行った場合)

1　以降の処理で、Windows の機能(tpm.msc で起動する TPM 管理画面など)あるいは市販の TPM アプリケーションを用いて TPM を初期化した際に指定した TPM 所有者パスワードが必要になりますのでご用意ください。

また現在は TPM 未使用だが将来使用する予定がありファームウェア更新を実施する場合は、以下の手順により、いったん TPM を初期化してください。

1) tpm.msc を起動する。
2) 右側の操作ウィンドウの”TPM を初期化”をクリックする。
(TPM が BIOS メニュー内で“無効”に設定されていた場合、再起動が促され次回ログイン後に 3)の状態になります)
3) 自動起動される TPM 初期化画面に従い、初期化を行う。その際に設定した TPM 所有者パスワードを以降のファームウェア更新時に使用する

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

BitLocker を有効化した際に Windows が TPM 所有者パスワードを自動設定していた場合は、TPM 所有者パスワードが不明な状態です。そのような場合、以下の手順で、一度 TPM クリアを実行しご自身で TPM 所有者パスワードを設定することによりファームウェア更新が行えます。

1)　BitLocker の状態を、無効 または 保護の中断 に変更する。
(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)
5) ログイン後自動起動される TPM 初期化画面に従い、初期化を行う。その際に設定した TPM 所有者パスワードを以降のファームウェア更新時に使用する。

3　(市販の TPM アプリケーションをご使用の場合)

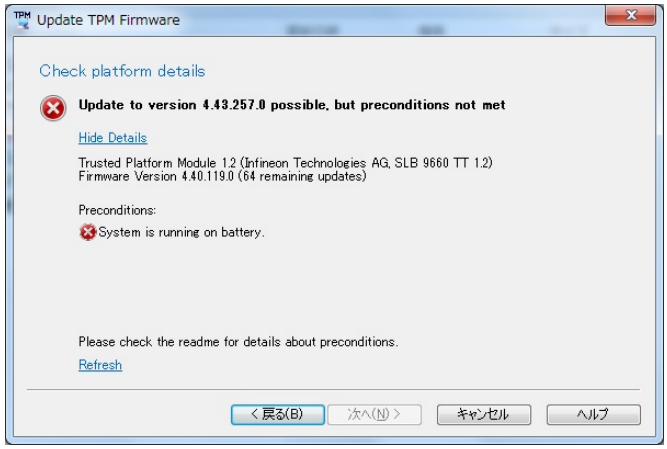
ファームウェア更新前の保存およびファームウェア更新後のリストアが必要になる場合がありますので、TPM アプリケーションの提供元にご確認のうえ必要な処理を行ってください。
これらを行わずにファームウェア更新を行った場合、TPM アプリケーションが管理していたデータにアクセスできなくなる恐れがありますのでご注意ください。

4　IFXTPMUpdate_TPM12_vxxxx.exe を起動する。

BitLocker が有効になっている場合は、無効 または "保護の中断" に変更してください。
・保護の中断" あるいは 無効 に変更する方法は、「2 .動作条件と注意点」を参照してください。

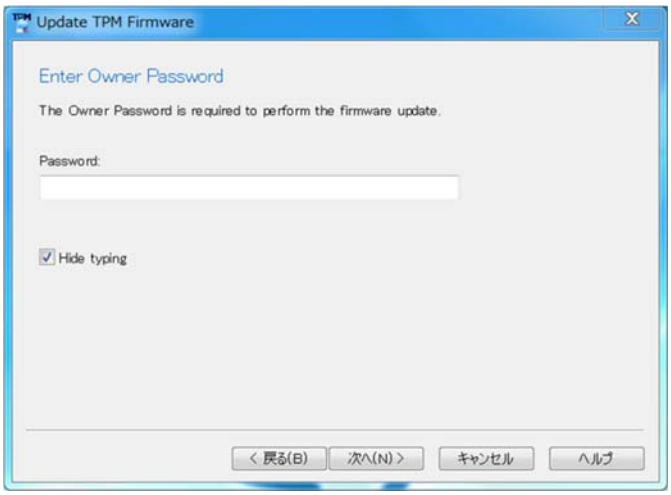
画面表示に従って “次へ“ または ” キャンセル “ ボタンを押し処理を進めていく。

（注意）画面に Update to version 4.xx.xxx possible, but preconditions not met と表示される場合は、ファームウェア更新を行うことはできません。Preconditions: に表示されたメッセージの対訳をご覧ください。（対訳は本書末尾に記載しています）

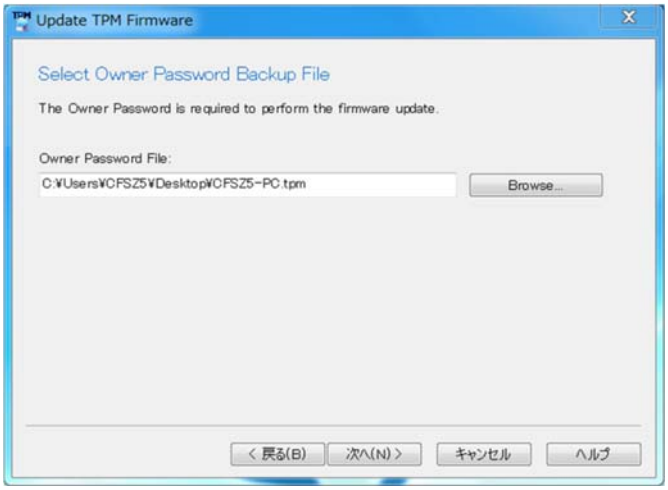


5　TPM 所有者パスワードを確認します。

6　　TPM 所有者パスワードを入力するか、作成時に保存したファイルを指定してください。



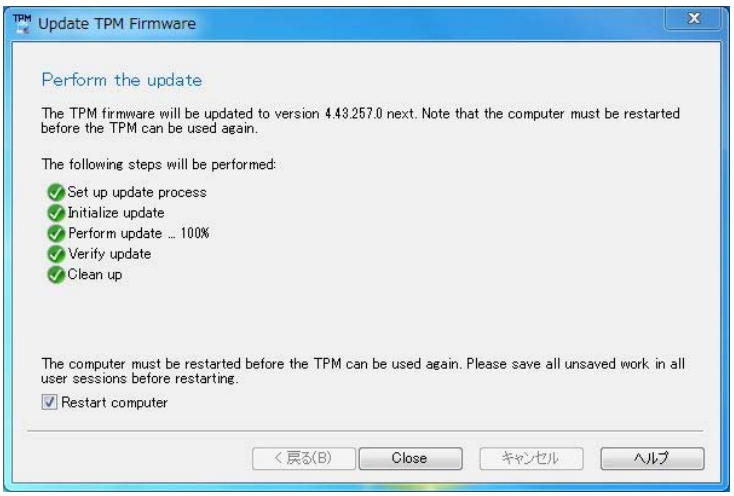
または



7　　更新を実行する

8　処理完了後、PC を再起動する。

(“Restart computer”のチェックを外さずに、“Close”を押すと再起動します)



9　ファームウェア版数の確認

1) tpm.msc を起動し、“製造元のバージョン”が更新されていることを確認する。

・4.32 は 4.34 に、4.40 は 4.43 に更新されます。

10　(現在は TPM を使用しない場合)

TPM を停止する。

1) tpm.msc を起動する

2) 右のウィンドウの“TPM をオフにする”をクリックし、画面指示に従い処理を進める。(TPM 所有者パスワードの入力が求められます)

将来 TPM をご使用になる際には、BIOS メニューのセキュリティ > 内蔵セキュリティ(TPM)で、[待機中の TPM 操作]の［所有者情報の初期化］を実行し、TPM の初期化を行ってください。

(TPM を使用する場合)

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 を再初期化する。

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、さらに”TPM の初期化”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)

5) ログイン後自動起動される TPM 初期化画面に従い、初期化を行う。

11　市販の TPM アプリケーションをご使用の場合で、ファームウェア更新後のリストアが必要な場合は必要な処理を実施してください。

4 TPM 1.2 ファームウェア更新ツールのメッセージ訳

英文	訳
A system restart is required	システムの再起動が必要です
A wrong command line was specified. Make sure to specify correct parameters as described in the readme.	誤りのあるコマンド引数が指定されています
A wrong Owner Password was specified. Make sure to specify the correct Owner Password.	TPM 所有者パスワードが正しくありません
Accept the terms of this license agreement	このライセンスに同意する
Administrative rights required.	管理者権限が必要です
An unexpected close attempt was detected. To avoid an invalid firmware state, do not close this message as long as the firmware update is in progress.	予期しない終了操作が検知されました。ファームウェア更新中はこのメッセージを終了させないでください。
Another instance of TPM Firmware Update is already running. Do not start TPM Firmware Update while the same program is already running.	二重起動はできません。
BitLocker Drive Encryption blocks firmware update.	ファームウェア更新は BitLocker によってブロックされています。
BitLocker Drive Encryption blocks TPM Firmware Update. Use the "BitLocker Drive Encryption" control panel applet provided by the operating system to turn off or suspend BitLocker. For details, please refer to Microsoft resources on BitLocker.	ファームウェア更新は BitLocker によってブロックされています。ブロックを解除するには、BitLocker の管理画面で"BitLocker を無効にする"、または"保護の中断"に変更します。詳細はマイクロソフトの BitLocker に関する資料を参照してください。
BitLocker is active	BitLocker が有効状態です。
Close	閉じる
Close all other applications. Do not log off, shut down, switch to sleep or hibernation mode, or unplug the power cord while the operation is in progress.	他のすべてのアプリケーションを終了させてください。また更新中は AC 電源プラグとケーブルを抜かず、ログオフ、スリープや休止状態への移行も行わないでください。
Critical	致命的
Deferred physical presence is not set	遅延フィジカルプレゼンスが設定されていません。
Dictionary attack defense measures are currently in effect.	現在、辞書攻撃に対する保護がかかっています。
Due to multiple failed attempts to provide a valid owner password, the TPM is locked to prevent dictionary attack. The TPM will be automatically unlocked after a certain amount of time. The exact time depends on how many failed attempts have been registered. Depending on your TPM configuration, the TPM may not only be locked but also temporarily disabled. In that case a restart is required in addition to elapsed lockout time	複数回、誤った TPM 所有者パスワードが入力されたため、TPM は辞書攻撃に対する保護状態に入りました。保護は時間経過によって自動的に解除されますが、解除までの時間は構成により異なります。

Enter Owner Password	TPM 所有者パスワードの入力してください。
Error	エラー
Firmware update is not applicable to this TPM model	本ソフトは、この TPM チップをサポートしていません。
Firmware update requires a restart. Please restart the system and re-run the program afterwards.	ファームウェア更新を実効するには再起動が必要です。システムを再起動した後、本ソフトを再度実行してください。
Hide typing	文字を隠す
I have the Owner Password Backup File	TPM 所有者パスワードバックアップファイルを持っている
I want to enter the Owner Password	TPM 所有者パスワードを入力する
Invalid Owner Password Backup File	TPM 所有者パスワードバックアップファイルではありません。
Multiple TPM Firmware Update preconditions are not met.	ファームウェア更新を実行するための前提条件が満たされていません。
No administrative rights	管理者権限がありません。
No information on Trusted Platform Module and firmware available.	TPM チップとファームウェアバージョンの情報が取得できません。
No matching firmware available.	対応したファームウェアバージョンではありません。
No TPM connection	TPM チップにアクセスできません。
No TPM device	TPM チップが見つかりません。
No Trusted Platform Module was found. Check whether your system has a TPM as specified in the readme. Make sure that the system BIOS settings do not hide the TPM.	TPM チップが見つかりません。BIOS で TPM が無効に設定されていないか確認してください。
not initialized	初期化されていません。
Open Owner Password Backup File	TPM 所有者パスワードバックアップファイルを開く。
Owner Password	TPM 所有者パスワード
Owner Password Backup File (*.tpm)	TPM 所有者パスワードバックアプファイル (*.tpm)
Owner Password File:	TPM 所有者パスワードファイル
Owner secret not stored by the operating system	TPM 所有者認証情報がオペレーティングシステムに保存されていません。
Password	パスワード
Perform the update	更新を実行
Platform Details:	プラットフォームの詳細
Platform is not initialized	プラットフォームは初期化されていません。
Please enter the Owner Password.	TPM 所有者パスワードを入力してください。
Power cord not plugged	AC 電源が接続されていません。
Power plan settings cannot be changed	電源プラン設定を変更できません。
Precondition state:	前提条件の状態

Preconditions not met	前提条件が満たされていません。
Preconditions:	前提条件
Restart computer	コンピュータを再起動する
Restart now	すぐに再起動する
Restart system?	再起動しますか？
Set up update process	更新プロセスの準備中です。
Show Details	詳細を表示する
Shut Down, Hibernate and Sleep cannot be blocked. or blocking of Shut Down, Hibernate and Sleep cannot be reverted. A possible reason is that this is not allowed by policy settings. To get permission, contact your group policy administrator.	シャットダウン、休止状態、スリープをブロックできません。ポリシー設定で変更が禁止されている可能性があります。
System is running on battery.	システムはバッテリー動作中です。
The computer must be restarted before the TPM can be used again. Please save all unsaved work in all user sessions before restarting.	TPM を再度使用するには再起動が必要です。再起動前には未保存の作業とデータは保存してください。
The content of the specified Owner Password Backup File does not match the current Owner Password. The specified file could be found and identified as a valid Owner Password Backup File. But the file content does not match the current Owner Password. Make sure to specify the correct Owner Password Backup File.	TPM 所有者パスワードバックアップファイルの内容は、現在の TPM 所有者パスワードと一致しません。
The firmware update is not applicable to this TPM model. Please select a firmware update package for this TPM model instead.	本ソフトは、この TPM チップをサポートしていません。
The maximum allowed number of firmware updates has been reached.	ファームウェア更新回数の上限に達しました。
The Owner Password is required to perform the firmware update.	ファームウェア更新を行うためには、TPM 所有者パスワードが必要です。
The Owner Password is required to perform this update.	更新を実行するには、TPM 所有者パスワードが必要です
The owner secret cannot be retrieved from the operating system. Run the program with the /pwd or /pwdfile switch.	TPM 所有者認証情報がオペレーティングシステムから取得できません。/pwd または /pwdfile 引数で指定してください。

The password is incorrect. Note that letters in passwords must be typed using the correct case.	パスワードが一致しません。 大文字と小文字は区別されますのでご注意ください。
The selected command could not be started because the TPM is currently deactivated or disabled. Make sure that the TPM is activated and enabled before you start any firmware update actions, or contact your system administrator.	現在 TPM が非アクティブ、または無効状態なのでコマンドは実行できません。
The selected file is not the correct Owner Password Backup File. Please select the correct file.	指定された TPM 所有者パスワードバックアップファイルは、正しい形式ではありません。
The specified file path is either invalid, or the file cannot be created due to missing permissions, or the file already exists.	ファイルが見つからないか、アクセスが禁止されています。
The specified Owner Password Backup File does not exist, cannot be opened, or is not a valid Owner Password Backup File. Make sure to specify the correct file path of an existing Owner Password Backup File.	指定された TPM 所有者パスワードバックアップファイルが見つからないか、正しい形式ではありません。
The system is running on battery. Plug the power cord. Do not unplug it before TPM Firmware Update completes.	システムバッテリー動作中です。 AC 電源を接続し、ファームウェア更新が完了するまで抜かないでください。
The TPM already runs the firmware included with this program or a newer one.	TPM はすでに新しいファームウェアで動作しています。
The TPM does not have an owner. Take ownership of the TPM before updating the TPM firmware.	TPM に所有者パスワードが設定されていません。
The TPM is not enabled. The TPM must be explicitly enabled and the TPM Owner must be explicitly set, before the TPM firmware can be updated. The necessary steps are described in the preconditions section of the readme.	TPM は有効状態ではありません。 ファームウェア更新は、TPM が有効状態にあり TPM 所有者パスワードが設定済の場合に実行できます。
The TPM Owner is not set. The TPM must be explicitly enabled and the TPM Owner must be explicitly set, before the TPM firmware can be updated. The necessary steps are described in the preconditions section of the readme.	TPM 所有者パスワードが設定されていません。 ファームウェア更新は、TPM が有効状態にあり TPM 所有者パスワードが設定済の場合に実行できます。

The TPM returned an authentication error. Make sure to enter the correct Owner Password.	認証エラーが返されました。 正しい TPM 所有者パスワードを指定したかご確認ください。
The TPM vendor is not supported. Manufacturer Name: %s, Manufacturer Version: %s, Specification Version: %s	サポートされていない TPM 製造社です。
This power plan is used temporarily during TPM Firmware Update and can be deleted afterwards if not done automatically.	この電源プランはファームウェア更新中に一時的に使用されます。自動的に削除されない場合は明示的に削除することもできます。
This program updates Infineon TPM1.2.	本ソフトは Infineon TPM 1.2 用です。
This wizard helps you update the firmware of your computer's Trusted Platform Module.	このウィザードに従って、ファームウェア更新が実行できます。
To continue, accept the license agreement and click "Next".	続行するには、ライセンスに同意し"Next" をクリックしてください
TPM Firmware Update has been explicitly prohibited by policy settings for your system. To get permission, contact your group policy administrator.	ファームウェア更新は、システムのポリシー設定により禁じられています。 グループポリシーの管理者にご確認ください。
TPM Firmware Update not allowed by policy settings	ファームウェア更新はポリシー設定で許可されていません。
TPM Firmware Update Power Plan	ファームウェア更新の電源プラン
TPM Firmware Update Wizard failed	ファームウェア更新ウィザードが失敗しました。
TPM is deactivated or disabled	TPM は非アクティブ、または無効状態です。
TPM is not enabled.	TPM は有効状態ではありません。
TPM needs an owner.	TPM 所有者パスワードが設定されていません
TPM not enabled	TPM は有効状態ではありません。
TPM Owner is not set.	TPM 所有者パスワードが設定されていません
Trusted Platform Module vendor is not supported. Check whether your system has a Trusted Platform Module as specified in the readme.	この TPM ベンダーはサポートしていません。 Readme に記載の TPM が搭載されているかご確認ください。
Update	更新
Update is for different SLB model	異なる TPM チップ用のファームウェア更新プログラムです。
Update not allowed by policy settings.	ポリシー設定によりファームウェアの更新が許可されていません。
Update the firmware of the Infineon TPM1.2 to the latest version supported by this tool. Administrative rights are required to perform the update. On Windows 8 and higher the tool retrieves the owner password from the operating system automatically if one is available.	このツールで Infineon TPM1.2 のファームウェアを最新バージョンに更新してください。 更新の実行には管理者権限が必要です。 Windows 8 及びそれ以後の OS では TPM 所有者パスワードをシステムから自動的に取得します（システムが管理している場合）。

Options /pwd and /pwdfile can be used to overwrite this behavior. On Windows 7 one of these options is mandatory.	/pwd オプションや/pwdfile オプションを使って TPM 所有者パスワードを指定することもできます。 Windows 7 ではこのオプションで TPM 所有者パスワードを指定してください。
Update to version %s possible	バージョン XXX への更新が可能です。
Update to version %s possible, but preconditions not met	バージョン XXX への更新が可能ですが、更新に必要な条件が整っていません。
Update TPM Firmware	TPM のファームウェアを更新します。
Updates the firmware of the Infineon TPM1.2 on the local computer to the latest TPM1.2 firmware version supported by this tool.	このツールで Infineon TPM1.2 のファームウェアを最新バージョンに更新してください。
Usage:	使用方法：
Use TPM owner password <pwd> to authorize the firmware update of the TPM.	TPM 所有者パスワード<pwd>を使用して、TPM のファームウェアの更新を認証します。
Use TPM owner password from the (.tpm) file pointed to by <file>.	<file>で指定したファイル(.tpm)に保存された TPM 所有者パスワードを使います。
User abort	処理が中断されました。
User has canceled TPM Firmware Update.	TPM のファームウェアを更新がキャンセルされました。
Verify update	更新を確認します。
Warning	警告
Welcome	ようこそ
Will automatically restart Windows once the update has finished successfully.	更新が完了すると自動的に Windows が再起動されます。
Write a log file to the location specified by <file>.	<file>で指定した場所にログが書き込まれます。
Wrong command line	コマンド引数に誤りがあります。
Wrong Owner Password	TPM 所有者パスワードに誤りがあります。
Wrong Owner Password Backup File	TPM 所有者パスワードのバックアップファイルが正しくありません。
Wrong TPM vendor	サポートしていない TPM ベンダーです。
You do not have permission to perform this operation. Make sure that you have administrative rights.	実行する権限がありません。管理者権限が有ることを確認してください。

以上