

STMicro TPM ファームウェアアップデート手順書

(Version 1.771.0.0)

本書では、ST マイクロエレクトロニクス社製 TPM(Trusted Platform Module)のファームウェア（以下、ファームウェア）をアップデートする手順について説明します。

【ご注意】

- ・ 対象機種以外では、ファームウェアのアップデートを行えません。ご使用されている機種が対象機種であることを今一度ご確認ください。
- ・ アップデートを実行する際は、必ず「**管理者**」の**権限のユーザーでサインイン**してください。（ユーザーの切り替え機能を使わずにコンピューターの管理者の権限でサインインして操作してください。）
- ・ AC アダプター、および十分に充電されたバッテリーパックを接続してください。充電量が不足している場合、TPM ファームウェアのアップデート処理は実行されません。
- ・ BitLocker を有効にしてご使用中の場合、念のため、有効化時に保存した BitLocker の回復キーをお手元に用意しておき、入力を求められた場合はご使用ください。（**回復キー入力を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。**）

【アップデート方法】

ファームウェアのアップデートは下記の流れで行います。

1. ファームウェアアップデートプログラムの展開
2. ファームウェアアップデートプログラムの実行
3. アップデート後のファームウェアバージョンの確認

1. ファームウェアアップデートプログラムの展開

- (1) ダウンロードしたファームウェアアップデートプログラム (stmicro_tpm_fw_1_771_0_0.exe) 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場合は、[はい]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]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。展開先フォルダは、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。
(標準では C:\util2\stmicro_tpm_fw_1_771_0_0)
- (4) [OK] をクリックします。しばらくして展開が完了すると、展開先フォルダが開きますので、そのままお待ちください。(展開先フォルダが開くまで 1 分以上かかる場合があります。)

2. ファームウェアアップデートプログラムの実行

- (1) 1 の展開先フォルダ内の、[TFInst] (拡張子を表示している場合は [TFInst.bat]) を右クリックし、[管理者として実行] をクリックします。「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] をクリックします。
- (2) 「管理者権限で実行してください。」というメッセージが表示された場合、(1) の手順に従い、管理者権限で実行してください。
- (3) コンピュータに搭載されている TPM のベンダー名とファームウェアバージョンが表示されます。
「TPM ファームウェアを更新する必要はありません。」というメッセージが表示された場合、ファームウェアがすでにアップデート済みか、あるいは今回のファームウェアアップデートプログラムの対象外機種のため、アップデートの必要はありません。
- (4) 「バッテリー残量が不足しているため TPM ファームウェアの更新を中止します。バッテリーを十分に充電してから再度実行してください。」というメッセージが表示された場合、メッセージに従い、バッテリーを十分に充電した後、(1) の手順から実行してください。
- (5) 続いて、BitLocker の状態をチェックします。BitLocker が有効になっている場合、BitLocker の保護の中断を実行した後、「TPM ファームウェアを更新するために、BitLocker の”保護の中断”を設定しました。次回、コンピュータを再起動した際に自動的に再開されます。」というメッセージが表示されます。
- (6) 最後に、「コンピュータの再起動後、TPM ファームウェアの更新を開始します。任意のキーを入力するとコンピュータを再起動します。」というメッセージが表示されます。
ここで、任意のキーを押すと、コンピュータを再起動します。
- (7) コンピュータの再起動後、自動的にファームウェアアップデートが実行されます。
- (8) ファームウェアアップデートが完了した後、Windows が起動します。
- (9) (5) で BitLocker の保護の中断が設定された場合、デスクトップ画面が表示されてから約 1 分で BitLocker が自動的に有効に戻ります。

3. アップデート後のファームウェアバージョンの確認

- (1) 1. の展開先フォルダ内の、[CheckTPMFWVersion]（拡張子を表示している場合は [CheckTPMFWVersion.bat]）を右クリックし、[管理者として実行]をクリックします。
「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]をクリックします。
- (2) 「管理者権限で実行してください。」というメッセージが表示された場合、(1)の手順に従い、管理者権限で実行してください。
- (3) コンピュータに搭載されている TPM のベンダー名とファームウェアバージョンが表示されます。
「TPM ファームウェアを更新する必要はありません。」というメッセージが表示された場合、ファームウェアが正しくアップデートされています。

以上でファームウェアのアップデート作業は完了です。