

# STM32でRoot of Trustを実現 セキュリティ・ソフトウェア・パッケージ

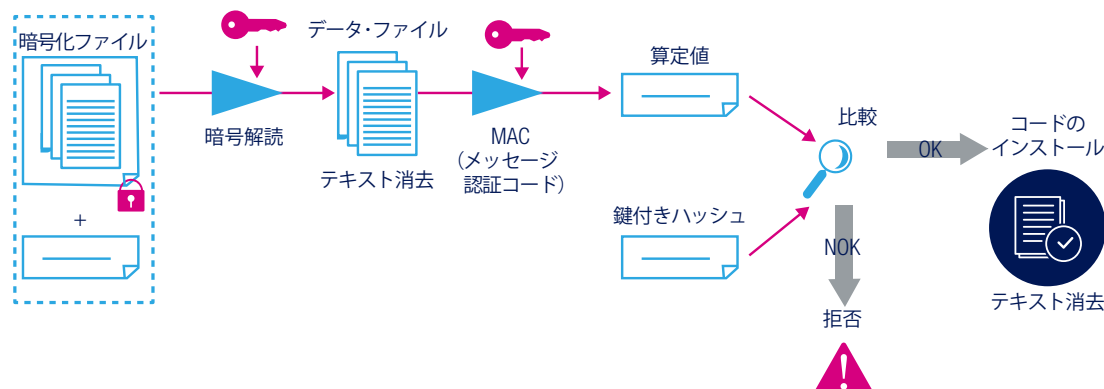


## 組み込みアプリケーションのセキュア・ファームウェア・インストールおよびアップグレードを可能にするソリューション

X-CUBE-SBSFUセキュア・ブート & セキュア・ファームウェア・アップデート・ソリューションは、STM32マイクロコントローラの組み込みプログラムをフィールドで新しいファームウェア・バージョンにアップデートし、新しい機能の追加やファームウェアの潜在的な問題の修正を可能にします。アップデートのプロセスはセキュアな方法で実行され、不正なアップデートやデバイス内の機密データへの不正なアクセスを防ぎます。

### 特徴

- セキュア・ブート・モジュール
  - Root of Trustサービスによる実行
  - 実行前のアプリケーション認証と完全性チェック
- セキュア・ファームウェア・アップデート・モジュール
  - インストールする新しいFW/バージョンの検出
  - FW/バージョンの管理(不正なアップデートや不正なインストールのチェック)
- セキュア・エンジン・モジュール
  - ユーザ・アプリケーション・ソフトウェアの実行から隔離されたコード
  - 暗号アルゴリズムの実行専用
  - セキュア鍵ストレージの管理



## STM32Cube用セキュア・ブート & セキュア・ファームウェア・アップデート拡張パッケージ

セキュア・ブートによるRoot of Trustサービスは、STM32のセキュリティ・メカニズムをチェックおよびアクティベートし、実行前に毎回ユーザ・アプリケーション・コードの真正性と完全性をチェックして、無効または悪意のあるコードが実行される可能性がないことを保証します。

セキュア・ファームウェア・アップデート・アプリケーションは、暗号化されたファームウェア・イメージを受け取り、その真正性をチェックし、復号した後に、コードの完全性をチェックしてからインストールします。

X-CUBE-SBSFUはSTM32Cubeソフトウェア技術を基盤としているため、異なるSTM32マイコン間の移植が容易です。

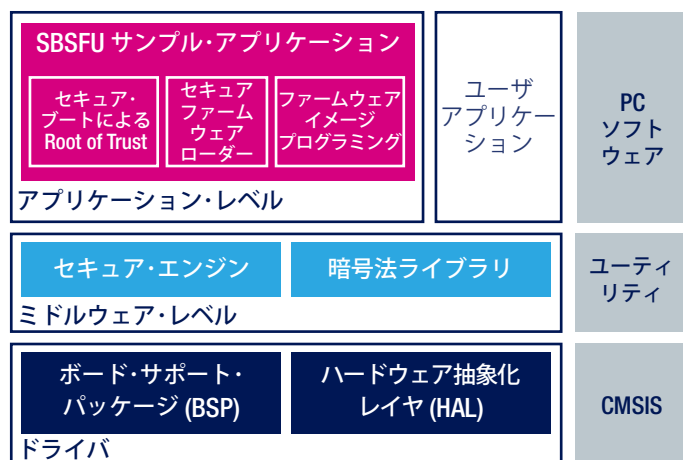
このソフトウェア拡張パッケージは、STM32セキュリティ保護を実行するためのリファレンス・コードとして提供されます。

X-CUBE-SBSFU拡張パッケージには、STM32L4シリーズで動作するサンプルが付属します。

詳細はこちら



### アーキテクチャ概要



### セキュリティ・レイヤ



- アプリケーション特徴 / サービス通信 (TLS)
- セキュリティ・サービス  
セキュア・ブート、セキュア・ファームウェア更新
- 暗号機能  
秘密性、安全性、可用性
- マイコンの安全機能  
ファイアウォール、PCROP、RDP、WRP、MPU

### STM32対応表

X-CUBE-SBSFU STM32Cube用 拡張ソフトウェア	STM32F4	STM32F7	STM32H7	STM32L0	STM32L4/L4+
	高性能マイコン			超低消費電力マイコン	
セキュア・ブート	○	○	○	○	○
セキュアFW更新	○	○	○	○	○
セキュア・エンジン				○	○
リリース予定	2018第4四半期	2018第4四半期	2018第4四半期	2018第4四半期	提供中

### ST コミュニティ



STM32ユーザ向けコミュニティで、質問したり、議論したり、色んなアイデアをシェアして、皆で一緒に取組みましょう。 [community.st.com/stm32](http://community.st.com/stm32)

