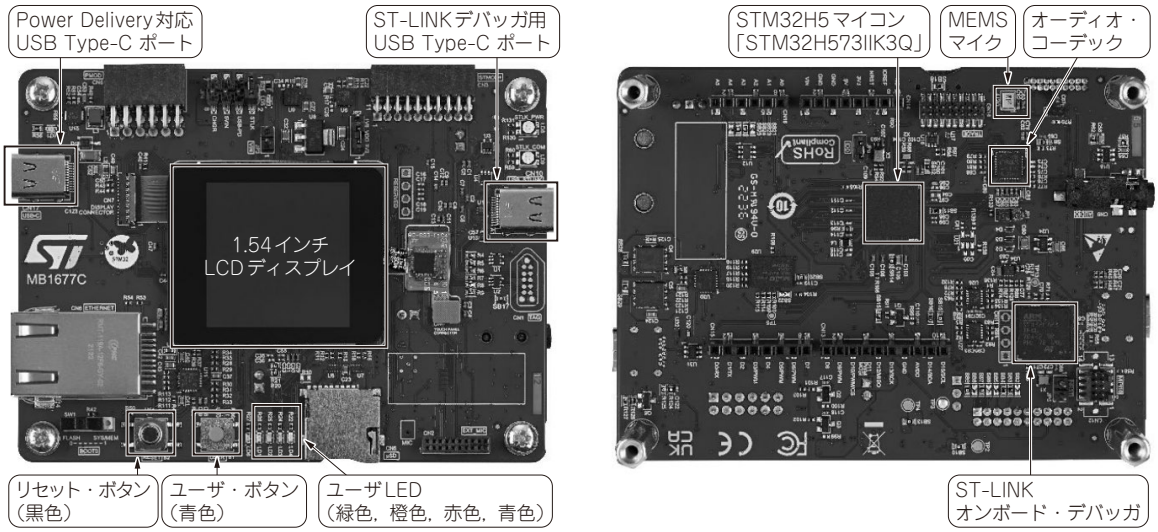
第3章 TrustZoneアプリケーション作成から セキュア・ブート導入まで

初めてのセキュア・アプリケーションの開発

鈴木 伸夫



(a) 表面　(b) 裏面

写真1　STM32H573I-DKディスカバリ・ボード

STマイクロエレクトロニクス(以下，ST)のSTM32H5シリーズは，TrustZoneを始めとするさまざまなセキュリティ機能がある汎用マイコンです．最大250MHz動作のArm Cortex-M33を搭載し，2Mバイトのデュアル・バンク・フラッシュ・メモリと640MバイトのSRAM，SPI/I²C/UARTなど汎用マイコンでは定番のインタフェースに加え，USB Type-C Power Deliveryコントローラ(UCPD)やI3Cといった新しいペリフェラルも採用しています．

セキュリティ機能としては，AESやSHAといったアクセラレータだけでなくSTM32マイコンで初めてセキュア・ブート機能が搭載されました．本章では，STM32H5シリーズの最上位モデルSTM32H573(**写真1**)上で動作するTrustZone対応セキュア・アプリケーションを開発し，セキュア・ブートを導入するまでの手順を解説します．

STM32Cubeで作るTrustZoneセキュア・アプリケーション

● 開発環境…全部入りの「STM32Cube」を使う

STM32H5マイコン向けのTrustZone対応セキュア・アプリケーションを開発するには，動作確認のためのハードウェアはもちろん，統合開発環境や，マイコンへプログラムを書き込むフラッシュ・プログラミング・ツールなどのソフトウェア，マイコンとソフトウェアを接続するデバッガ・ツール，ペリフェラルを制御するためのドライバ群が必要です．しかし，それらは全てSTM32Cubeという開発環境で提供されています．本章で使用する環境は**表1**の通りです．

● TrustZone対応アプリケーションの作成

ボード上の4つのLED(青，赤，橙，緑)と1つのユーザ・ボタンを操作する簡単なアプリケーションを作成します．ただし，LEDの(青)と(赤)はセキュア領域に割り当てます．また，(橙)と(緑)とユーザ・ボ