CPSのセキュリティーを確保するセキュアMCUプラットフォーム技術

Secure MCU Platform Techniques to Ensure Security of Cyber-Physical Systems

廣里　暢盛 HIROSATO Nobushige　　橋本　幹生 HASHIMOTO Mikio

CPS（サイバーフィジカルシステム）の構築に向けて急速に普及が進むIoT（Internet of Things）機器用のMCU（Micro Control Unit）には，ネットワーク接続に伴うセキュアな通信機能，及びIoT機器の完全性と可用性を両立させるファームウェア（FW）更新機能の実現が求められている。

東芝デバイス&ストレージ（株）は，Arm社製のArm® Cortex®-Mプロセッサーを搭載したMCU向けに，同社が提供しているArm® Mbed™ OS（基本ソフトウェア（SW））を適用し，安全なネットワーク接続の実現とともにIoT機器のシステム開発・運用に掛かる負担を軽減した。また，FWを記録するフラッシュメモリーを冗長構成にすることで，IoT機器がサイバー攻撃を受けた後でも，FWの安全な更新を可能にするセキュアFWローテーション技術を開発し，完全性と可用性を両立させた。このセキュアFWローテーション技術のハードウェア（HW）をFPGA（Field Programmable Gate Array）を用いて機能試作し，SWと合わせて動作検証を行って，その有効性を確認した。

With the rapid expansion of Internet of Things (IoT) devices as an important component for the construction of cyber-physical systems (CPS) in recent years, demand has been growing for a microcontroller unit (MCU) for IoT devices with both a secure communication function for connecting to the network and a firmware update function to enhance integrity and availability.

Toshiba Electronic Devices & Storage Corporation has been implementing measures to rectify this situation through the development and introduction of the following techniques: (1) introduction of a software platform technique using the Arm® Mbed™ OS, which is an open-source embedded operating system (OS), to its MCUs with an Arm® Cortex®-M processor in order to achieve secure connection to the network and reduction of the burden on developers, and (2) development of a secure firmware rotation technique using redundant flash memories for firmware update that can protect IoT devices against cyberattacks in order to achieve a balance between integrity and availability. We have confirmed the effectiveness of the secure firmware rotation technique through experiments on functional prototype hardware and software using a field-programmable gate array (FPGA).

1. まえがき

CPSは，従来は別々の形で進化してきたIT（情報技術）や，FA（ファクトリーオートメーション），IoTなどを統合する形で，急速に広がりつつある。CPSの中でデジタル世界と現実世界の接点の役割を担うIoT機器には，ネットワーク接続時のセキュアな通信，及び完全性と可用性を両立させるFW更新の実現が求められている。ここで，完全性とはFWが正しい状態で維持されることを，可用性は継続して稼働できる能力を指す。

従来の組み込み機器用MCUでは，モーターや，工作機械，センサーといった機器機能のサポートがFW開発の大半を占めていたが，IoT機器用MCUでは，ネットワーク接続が必須となるため機器事業者のFW開発負担が大きくなる。また，IoT機器のセキュリティーは，誤動作や機密情報漏えいの回避とともに可用性の確保も必要となる。

これらを踏まえて，東芝デバイス&ストレージ（株）は，Cortex®-M搭載MCUにArm社のMbed™ OSを適用して，安全なネットワーク接続を実現するとともに機器事業者の開発負担を軽減した。また，FWの安全な更新と可用性の確保を両立させる特長を持つMCUのHW差異化技術として，セキュアFWローテーション技術を開発した。ここでは，Mbed™ OS及びセキュアFWローテーション技術の概要について述べる。

2. Cortex®-M搭載MCUへのMbed™ OSの適用

組み込み機器用MCUでは，そのシステム開発者の意図に基づいて，複数タスクの並行処理や実時間処理が必要な作業の実装が行われるが，これらをシステム上で保証するために，RTOS（Real Time Operating System）が用いられることが多い。RTOSには，様々なアーキテクチャーに基づいて構成されたものが幾つも存在する。

当社は，Arm社のCortex®-Mを搭載したMCUに対して最適化された，Mbed™ OSというRTOSを選択した。Mbed™ OSには，FW開発者のシステム構築をサポートする有用なプラットフォームが用意されている。以下に，Mbed™ OSとそのプラットフォームについて述べる。

Mbed™ OSは，Arm社が提供してきたRTOSのアーキテクチャーと，タスク間通信やリソース共有などの基本機能を踏襲している。FW開発者がMbed™ OSを使用するためには，Cortex®-M搭載MCUのベンダーがMCUとデバッグインターフェースDAPLinkを実装したボード上でMbed™ OSが適切に動作するようにポーティングを行い，Arm社の認定を受ける必要がある。DAPLinkは，認定を得たボードを，Arm社のクラウドサービスに整備されているFW開発プラットフォームに接続する。このように，FW開発を支援するプラットフォームが整備されていることが，Mbed™ OSの特長の一つである。

もう一つの特長は，Mbed™ OSを実装したIoT機器のネットワーク接続をサポートするクラウドサービスArm® Pelion™ IoTプラットフォームが提供されることである。Pelion™ IoTプラットフォームは，IoT機器をネットワークに接続・管理する機能，及びArm社が提供する暗号化通信手段Mbed™ TLS（Transport Layer Security）を用いてセキュア通信を構築する機能を持つ（**図1**）。Mbed™ TLSは，最新の暗号アルゴリズムを備えており，TCP/IP（Transmission Control Protocol/Internet Protocol）準拠の通信機能などを用いて，基本的なネットワークセキュリティー機能を提供する。

これら二つの特長がセキュアなIoT機器用のプラットフォームをつかさどり，ネットワーク接続が必要なIoT機器のFW開発とシステム運用の負担を大幅に軽減する。

当社は，Cortex®-M0，Cortex®-M3，又はCortex®-M4を搭載することで幅広い用途に対応できるTXファミリー及びTXZファミリーを，MCU製品としてラインアップしており，そこにMbed™ OSを適用できる。この中で，セキュアなIoT機器用プラットフォームに適したものとして，Cortex®-M4搭載のTMPM46BF10FGが挙げられる（**図2**）。TMPM46BF10FGにはセキュリティーエンジンが搭載されているため，Mbed™ TLSによる暗号化通信のスループットを向上させることができる。

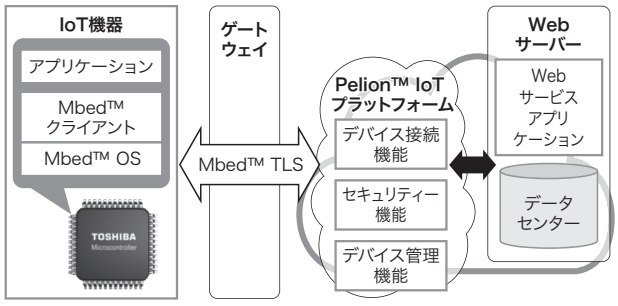


図1. Mbed™ OSを適用したFWプラットフォームの構成

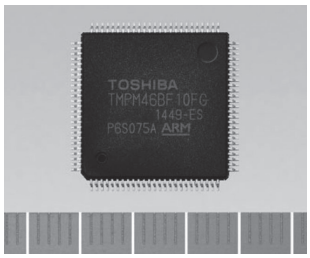
IoT機器用MCUにMbed™ OSを適用することで，Arm社が提供するクラウドサービスと連携した効率的なFW開発やIoT機器管理を実現できる。

Configuration of software platform applying Mbed™ OS

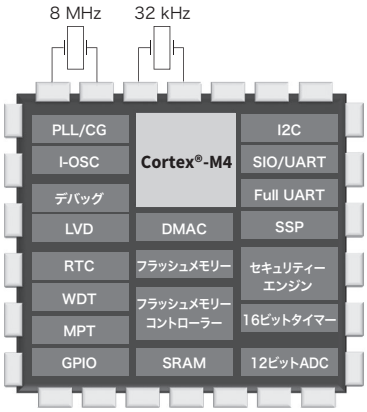
3. セキュアFWローテーション技術の概要

3.1 IoT機器におけるセキュリティーの脅威と制約

2章で述べたとおり，Mbed™ OSを既存MCUに適用すれば，ネットワークセキュリティー機能を備えたIoT機器が



(a) TMPM46BF10FG



(b) ブロック図

PLL/CG：位相同期ループ/クロックジェネレーター
I-OSC：内蔵発振回路
LVD：電圧検出回路
RTC：リアルタイムクロック
WDT：ウオッチドッグタイマー
MPT：多目的タイマー
GPIO：General Purpose Input/Output
DMAC：ダイレクトメモリーアクセスコントローラー
SRAM：Static RAM
I2C：Inter-Integrated Circuit
SIO/UART：Serial Input Output/Universal Asynchronous Receiver Transmitter
SSP：Synchronous Serial Port
ADC：アナログデジタル変換器

図2. Cortex®-M4搭載MCU TMPM46BF10FGのブロック図

TMPM46BF10FGには，演算機能や，各種入出力，フラッシュメモリー，セキュリティーエンジンなど，セキュアなIoT機器を実現するための各種機能が実装されている。

Block diagram of TMPM46BF10FG MCU with Cortex®-M4

容易に開発できるようになる。しかし，IoT機器にはSW脆弱性対策をはじめとしてセキュリティー関連の多くの課題があり，Mbed™ OSを適用するだけでなく，更に適切な対策をすることが必要である。このような追加セキュリティー対策をプラットフォームの要素としてMCUに備えておくことにより，FW開発者の負担を更に軽減できる。

IoT機器は現実世界との接点を持つため，誤動作は人やものに対する損害につながる。不正アクセスによる誤動作を防ぐために，アクセス制御などのセキュリティー機能の導入は不可欠である。同時に，IoT機器には，適切な水準の可用性・信頼性も求められる。しかし，不用意に不正アクセスの排除機能を導入すると，必要とされるユースケースの見落としなどにより，可用性を低下させてしまう場合がある。

IoT機器以外の例では，パソコン（PC）の起動パスワードが連続して誤入力されたときに，PCを起動不能にロックする機能がある。これは，盗難時の不正利用というセキュリティー脅威に対しては，有用な機能である。一方，ユーザー自身によるパスワード忘れなどの理由で連続してパスワードを誤入力した場合には，可用性を低下させてしまうという負の側面もある。そのため，ユーザー認証に失敗した場合のロック解除とパスワード再発行などの仕組みの追加が必要になる。

IoT機器において，FWの完全性と可用性を両立させることが難しい事例の一つとして，ネットワーク経由での更新FWの入手がある。IoT機器の遠隔FW更新は，機器の機能向上やバグ修正に限らず，長期にわたるセキュリティー確保に不可欠なSW脆弱性対策の基本要素である。スマートメーターやPC周辺機器ではFW更新要件が定められており[(1), (2)]，多くの機器がその機能を備えつつある。

FW更新においては，入手した更新FWをデジタル署名検証などの手段で確認することが必須であるとともに，実行時にはフラッシュメモリー上に配置したプログラムが改ざんされていないことを確認することも必要になる。これは，SW脆弱性に対する攻撃を受けて，正規の更新FWの受信後に，不正プログラムによりフラッシュメモリー上のプログラムを改ざんされてしまう脅威を排除するためである。SW脆弱性は不具合の一種であり，セキュリティー上の攻撃に利用できるものの総称である。SW脆弱性には様々なものがあるが，一例として，任意コード実行が挙げられる。これは，通常利用では入力されることのない想定外のパラメーターの通信データを受信したとき，攻撃者が送った通信データの一部がプログラムとして実行されてしまうというものである。このようなSW脆弱性を排除するには，通信経由で送り込まれた不正プログラムが，更新FWを格納するためのフラッシュメモリー領域を不正に書き換えてしまう脅威を想定して，更新FWの実行前に不正プログラムの影響を排除した上で，更新FWの改ざんをチェックする必要がある。

ここで注意すべき点は，任意コード実行のSW脆弱性により一時的に不正プログラムが実行されたとしても，改ざんされたFWの格納先がSRAM（Static RAM）にとどまっている限り，再起動によりその影響は除去される。しかし，不正プログラムがフラッシュメモリー上の更新FWを書き換えた場合，再起動しても影響が残る。したがって，更新FWを実行する前に，最終的な改ざん検証をいつどのように行うかは，この脅威を排除する上で重要なポイントである。

誤動作を防止する観点からは，たとえ1ビットでも改ざんされたFWは実行してはならない。その1ビットが重要な条件判断のパラメーターである場合，間接的に重要な判断に影響を与える可能性が否定できないためである。FWに対してデジタル署名技術を正しく適用することで，このような改ざんを検出し排除することができる。

しかし，攻撃者の目的が可用性の低下，すなわち利用できなくすること（プログラム破壊）にある場合は，改ざんを厳密にチェックする方針を採るほど，攻撃者が目的を達成することが容易になる。これが，FWの完全性と可用性の両立が難しいゆえんである。

3.2 FW更新の課題と要件

以下に，FW更新機能に求められる要件を挙げる。

3.1節に記載したように，IoT機器におけるSW脆弱性の対策には，FW更新が必要である。メンテナンス性を考慮すると，現地サービスマンによる対応を必要とせず，遠隔から無人でFW更新できることが，第1の要件である。

小規模なIoT機器では，FWはフラッシュメモリーに格納され，実行される。遠隔からFW更新が可能であるということは，IoT機器のフラッシュメモリーの書き換え手段が提供されていることを意味する。このフラッシュメモリーの書き換え手段が攻撃者に不正に利用される脅威への対策が，第2の要件である。攻撃者が作成した不正プログラムの実行を排除することはもちろんであるが，3.1節で述べたプログラム破壊への対策も必要である。

次に，MCU側の制約から必要になる要件について考える。PCでは，フラッシュメモリーのプログラムをDRAMに展開して実行する方式が一般的である。一方MCUは，フラッシュメモリーに記憶されたFWをSRAMに展開することなく，ワード単位で読み出して実行するXIP（eXecute In-Place）を採用している。これは，SRAMのビット当たりの価格がフラッシュメモリーよりも高いためである。FWは，OSレス，若しくはOSカーネルとアプリケーションが単一イメー

ジとなったファイルシステムレスであることが多い。したがって，FW更新は，システムプログラム一式を書き換える方式となる。これが第3の要件である。

ローエンドMCUを利用することを考慮して，実行中に任意のタイミングで特権状態と非特権状態を切り替える高機能な特権制御は，利用できないことを，第4の要件とする。

そして，更新前のFWに何らかの脆弱性があり，万一，不正プログラムが実行されてしまった場合でも，先の第2の要件を満たした安全なFW更新を保証することで，再度安全な状態を回復できることが，第5の要件である。

上記の環境で，遠隔からFW更新するときは，ネットワーク経由で受信したFWに対する検証が必須である。実行中のフラッシュメモリー上のFWを直接書き換える単純な更新方式を採っていた場合，更新が完全に完了していない状態で再起動が行われると内容に不整合が生じるため，正常な動作ができなくなる。このような不具合に備えて，1セット若しくは複数のバックアップ用のFWを保持しておく方式が広く用いられている。

3.3　開発方式

今回，当社が独自開発したセキュアFWローテーション技術は，フラッシュメモリー上の2面のFW格納領域，FWの検証に特化した“ROMモニター”と呼ぶMCU上のマスクROMに格納された更新支援プログラム，及び簡易的なHWアクセス機構を備えたMCUにより，3.2節で述べた五つの要件を実現した[3]。ROMモニターを改ざん不能なROM領域に格納したことと，ROMモニターが更新FWの検証を完了するまでは，検証済みのFWの格納領域を書き込み禁止状態で保持することが特長である。

図3に，セキュアFWローテーション技術の概要を示す。左側が更新前のMCUの状態，右側が更新後（検証成功後）のMCUの状態を表す。FWを格納するフラッシュメモリーを，領域Aと領域Bの2面に分割している。更新前は領域AのFW1が実行中であり，領域Aは書き込み不可に設定しているためFWの変更はできない。一方，更新に使う領域Bは，FWを自由に書き込みできるように設定している。実行中のFW1は，通信により更新FWとその正当性を担保する署名を取得し，適宜検証を行って，更新FW2として領域Bに書き込む。

書き込みが完了すると，実行中のFW1は更新指示を示すフラグをフラッシュメモリーに書き込んでリセットを発行し，再起動する。再起動後は，ROMモニターが動作する。このときROMモニターは，全てのフラッシュメモリー領域に自由にアクセス可能な権限を持つ。ROMモニターは，更新指示があることを確認すると，更新用領域Bの内容に対する署名検証を行う。署名検証に成功した場合は，フラッシュメモリーに対するアクセス制御設定を変更し，領域Bを書き込み不可，領域Aを書き込み可に設定して，更新された領域BのFW2の実行を開始する。これが図3の右側の状態である。次の更新では，領域A，Bの役割が入れ替わり，左側の状態に戻って，FWローテーションが行われる。

一連の動作において，検証と実行FWの選択はリセット後に動作するROMモニター機能の制御下にあり，たとえFWがSW脆弱性に対する攻撃により一時的に誤動作したとしても，再起動すれば不正プログラムが動作する可能性は排除できる。ROMモニターとFWローテーションは時間的に分離されており，特権機能を持たないローエンドMCUにも適用可能である。

更に，セキュアFWローテーション技術の特長により，SW脆弱性への対応を含む更新FWを配布する前に攻撃が顕在化する，いわゆる“ゼロデイ攻撃”を受けた場合にも，安全にFW更新できる。この技術では，独立したROMモニターがFW検証を担うため，仮に旧FWが攻撃を受けたとして

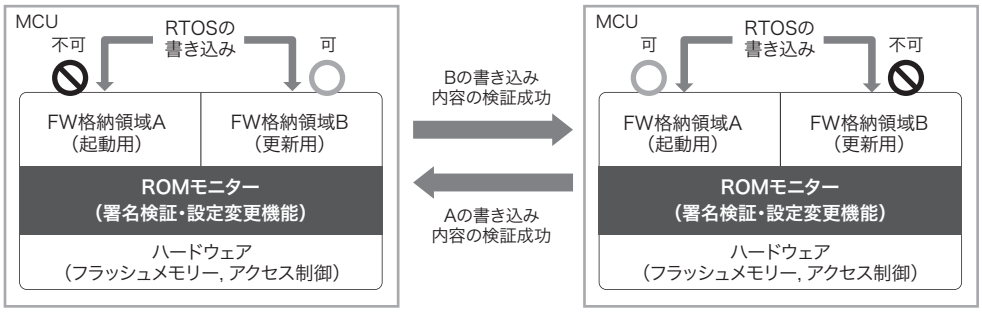


図3. セキュアFWローテーション技術の概要

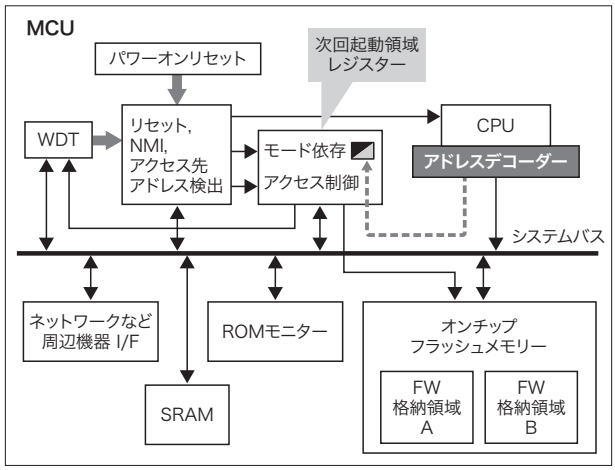
フラッシュメモリー内に2面のFW格納領域を用意し，一方を書き込み不可の起動用に，他方を書き込み可の更新用に設定する。更新用領域に書き込んだFWを正当と判断した場合だけ，起動用領域及び書き込み不可の設定を切り替える。

Outline of secure firmware rotation technique

も，ROMモニターには影響が及ばない。更新FWの脆弱性が修正されていれば，ROMモニターによる検証後に起動する更新FWから，旧FWの脆弱性は排除される。更新FWの検証成功まで，旧FWは書き込み不可状態で保持されるため，旧FWに脆弱性があったとしても破壊を免れる。更新FWの取得とROMモニターによる検証に成功するまで，何度でも再起動と更新FW取得の試行を繰り返すことができる。広範囲に多数の機器が設置されるセンサーノードやスマートメーターでは，1台ごとの更新時間は延びるものの，サービスマン派遣によるFW更新に比べて効率化できる。

3.4 機能試作

Arm社製のCortex®-R4プロセッサーとオンチップフラッシュメモリーを備えたワンチップMCUの設計をベースに，セキュアFWローテーション技術のHW及びSWの機能試作を実施した(**図4**)。HWについては，Cortex®-R4を含む全ての要素を論理合成してFPGAで実現した。SWについては，ROMモニター相当の機能とFW（RTOS及びアプリケーション）を実装した。ROMモニターによる更新FWの完全性検証には，RSA-2048及びSHA-256ハッシュ関数によるデジタル署名を使用している。このとき，デジタル署名及びデータを含むROMモニターのフットプリントは約18 Ki（キビ：2^{10}）バイトであった。長期使用される機器では，より長い鍵長のRSA-3072とSHA-384の導入が始まっているが，その場合でもROMモニターのサイズは数Kiバイトの増加にとどまると推定している。



NMI：Non-Maskable Interrupt（ソフトウェアからマスク不可能な割り込み）
I/F：インターフェース

図4. セキュアFWローテーション機能を実装した試作品のブロック図
Cortex®-R4プロセッサーやオンチップフラッシュメモリーを備えたMCUをFPGAで試作し，セキュアFWローテーション機能を確認した。
Block diagram of prototype MCU incorporating secure firmware rotation technique

この機能試作の結果，開発したセキュアFWローテーション機能が正しく動作することを確認した。

4. あとがき

CPSの中でデジタル世界と現実世界の接点の役割を担うIoT機器用MCUへの，当社の取り組みについて述べた。

提供中のMCUにMbed™ OSを適用することより，IoT機器を安全かつ容易にネットワーク接続・管理することができる。MCUのHW差異化技術であるセキュアFWローテーション技術は，FWの安全な更新と可用性の確保を両立させる特長を持ち，現在，製品化に向けた取り組みを進めている。

また，ここで述べたIoT機器のセキュリティーに加えて，デジタル認証局に代表されるトラストサービスもセキュアなIoT機器の実現を支える重要な仕組みである。当社は，デジタル認証局で実績のあるサイバートラスト（株）と業務提携し，新規開発するMCUをキーコンポーネントとする総合的なトラストサービスの運用基盤の確立に向けた具体的な検討も開始した[4]。

当社は，今後も市場の要求に適合したMCU関連技術を開発し，完全性と可用性を兼ね備えたMCU製品を提供して，CPSのセキュリティー確保に貢献していく。

文 献

(1) JESC Z0003：2016．スマートメーターシステムセキュリティガイドライン．
(2) NIST Special Publication 800-193：2018. Platform Firmware Resiliency Guidelines.
(3) 橋本幹生，ほか．IoT機器に向けた不揮発性メモリセキュリティ技術の提案 ～メモリ内蔵MCUおよび汎用プロセッサ向けの保護機構～．信学技報．2016，**116**，240，p.37–42.
(4) 東芝デバイス＆ストレージ．“東芝デバイス＆ストレージとサイバートラストがIoT機器向けトラストサービスで提携”．ニュースリリース，<https://toshiba.semicon-storage.com/jp/company/news/news-topics/2019/07/micro-20190709-1.html>，（参照 2019-07-10）．

廣里 暢盛 HIROSATO Nobushige
東芝デバイスソリューション（株）
システムソリューション統括部 システムソリューション技術第一部
IEEE 会員
Toshiba Electronic Device Solutions Corp.

橋本 幹生 HASHIMOTO Mikio
東芝デバイス&ストレージ（株）デバイス&ストレージ研究開発センター ソフトウェアソリューション技術開発部
IEEE・電子情報通信学会・情報処理学会会員
Toshiba Electronic Devices & Storage Corp.