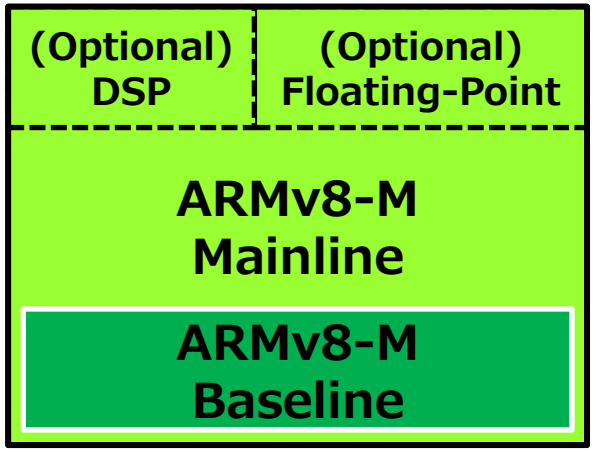
ARMv8-M TrustZone:
組み込みデバイス向けアーキテクチャとセキュリティ機能

FFRI, Inc.
http://www.ffri.jp

ARMv8-M アーキテクチャとは

- 2015年11月にアナウンスされた組み込み機器を対象としたプロセッサ向け (Cortex-M ファミリ) のアーキテクチャ。

- 従来のARMv6-M/ARMv7-Mアーキテクチャの特性を要求する組み込みシステムに対して包括的に対応するために、ARMv8-Mは２つのサブプロファイルを用意している。
  - Baseline
    - 超低消費電力の製品向け
    - ARMv6-M に近い性質
  - Mainline
    - 全機能を備えた、マイコン製品や高性能な組み込みシステム向け
    - ARMv7-M に近い性質



TrustZone

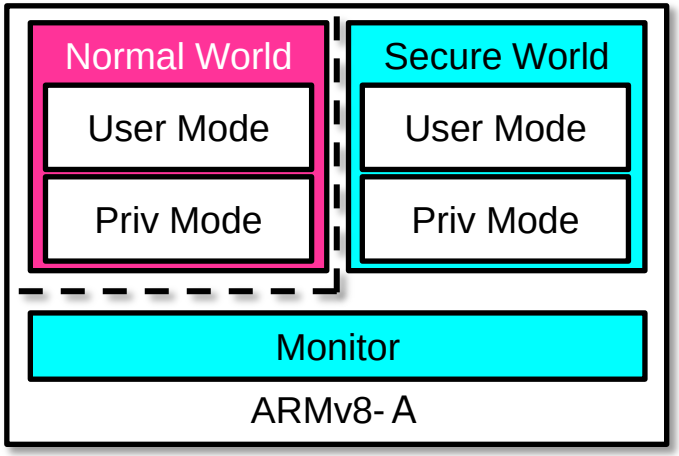
- ARM プロセッサ (Cortex-A ファミリまたは ARMv8-M アーキテクチャを採用した次世代の Cortex-M プロセッサ) が提供するセキュリティ機能。

- セキュリティ状態を追加することで、セキュリティレベルを分離させることが可能。（e.g. Normal World & Secure World）

- ARMv8-M アーキテクチャは、従来の ARMv8-A アーキテクチャ (Cortex-A ファミリ) が提供する TrustZone とはメカニズムが異なり、組み込みシステム向けに最適化されている。

TrustZone (ARMv7, ARMv8-A, etc…)

- モニターモードを追加することで、Normal World と Secure World に分離する。
  - モニターモードには、専用の SMC 命令で遷移
  - OSモニターを用いた仮想化機能の一種とも言える



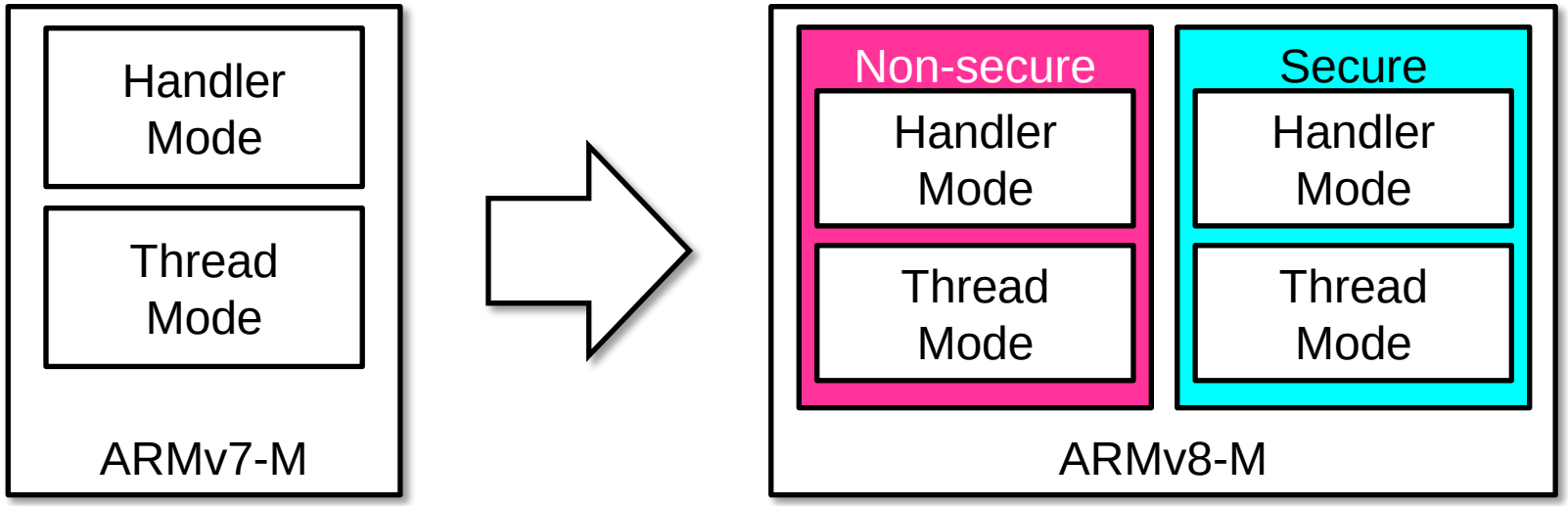
- iPhone に使用されている Secure Enclave 機能も TrustZone を利用していることで知られている。

- 詳細は、Monthly Research 2013年3月「セキュアハードウェアの登場とその分析」を参照。

TrustZone (ARMv8-M)

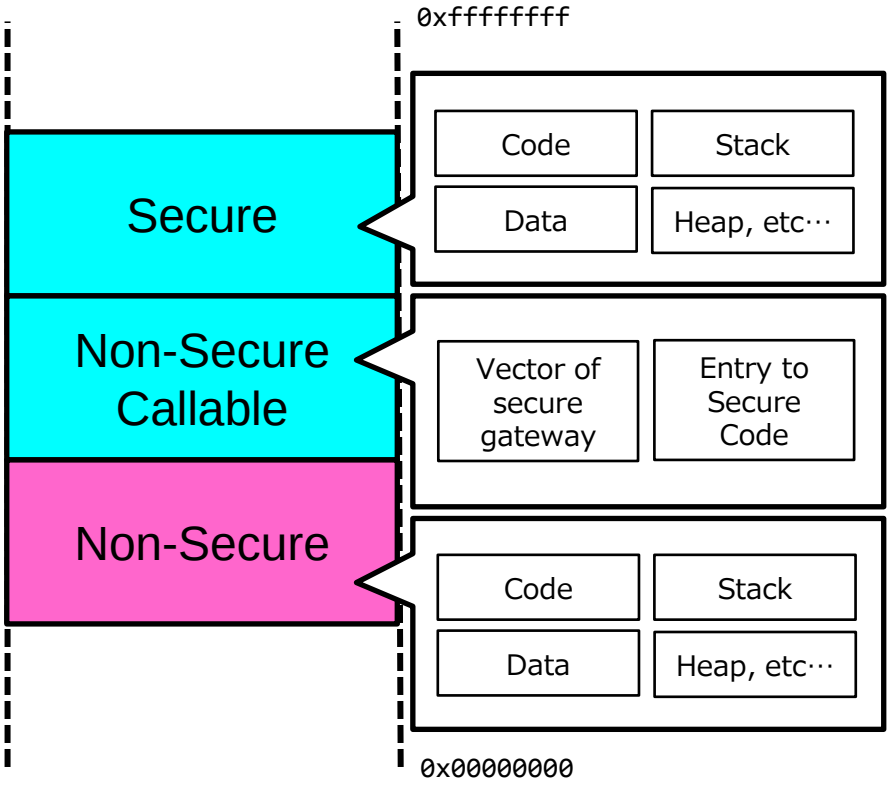
- Secure ステートを追加することで Non-Secure なモードと Secure なモードに分離する (モニターモードは不要)。
  - モード間の遷移には分岐命令を使用する
  - システムはデフォルトで Secure ステートで立ち上がる

- 以後、ARMv8-M の TrustZone について言及する。



ARMv8-M TrustZone - メモリ空間の分離

- マイコンやSoCの開発者による定義のほか、プロセッサの SAU や IDAU インタフェースを利用することでソフトウェアからも定義可能。
- メモリ空間は大きく右記の３つに分類することができる。
- プロセッサの状態 (Secure or Non-Secure) は右記メモリ空間の定義に依存するため、以降の説明は「状態」ではなく「領域」に統一する。



SAU: Software Attribution Unit
IDAU: Implementation Defined Attribution Unit

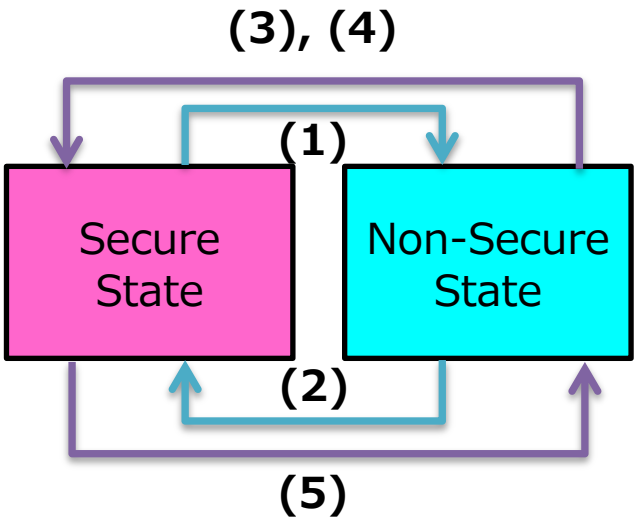
ARMv8-M TrustZone – セキュアゲートウェイ

- Non-Secure 領域から Secure 領域の処理を呼び出す場合は かならずセキュアゲートウェイ (SG命令) を中継する。
  - Non-Secure 側から呼び出される関数の最初の命令は、必ず SG 命令でなければならない
  - SG 命令は、NSC 領域に存在しなければならない

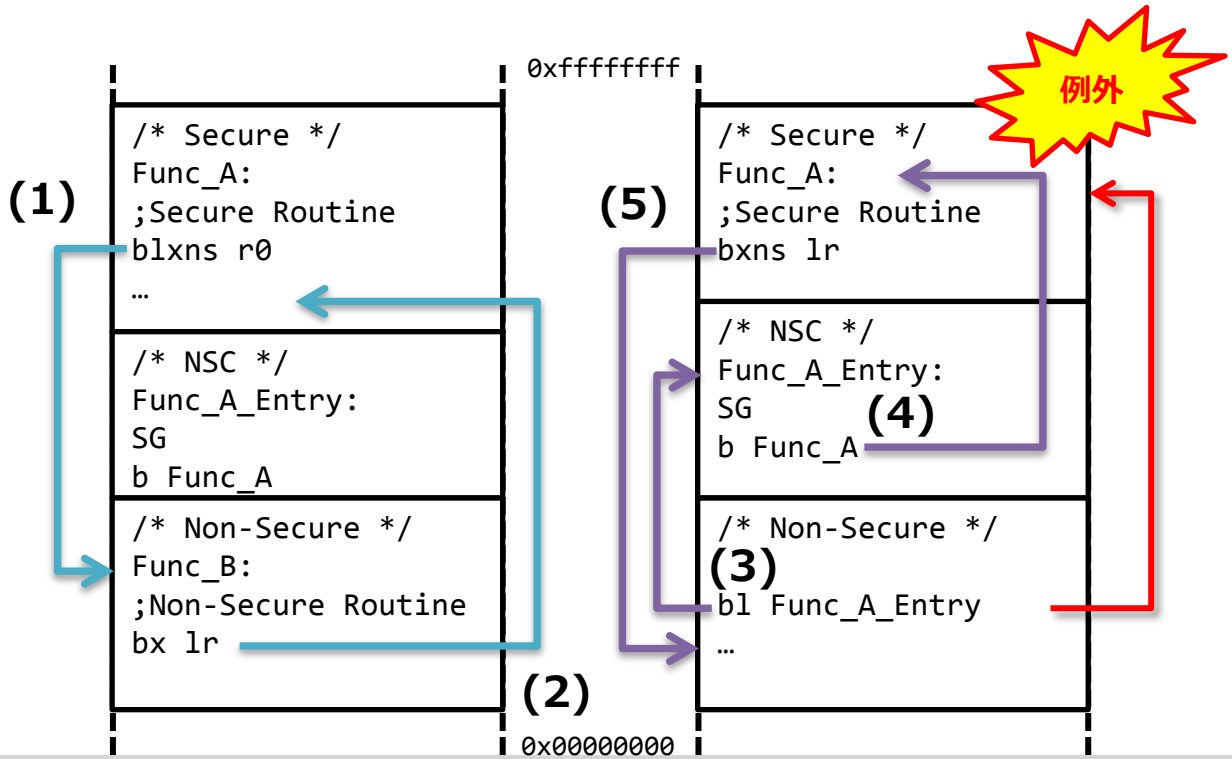
- Secure 領域から Non-Secure 領域の処理を呼び出した場合、Secure 領域のスタックに状態をプッシュして Non-Secure 領域への遷移が行われる。
  - Non-Secure 状態への遷移時にリンクレジスタ (LR) に予約値 FNC_RETURN がセットされる
  - Secure 状態への復帰時はこの FNC_RETURN (LR) へ分岐する

ARMv8-M TrustZone – セキュアゲートウェイ

- Non-Secure 領域のプログラムから直接 Secure 領域のアドレスにアクセスした場合は、以下の例外が発生する。
  - Mainline では SecureFault(7)、Baseline では HardFault(3) が Secure ステートで発生する。



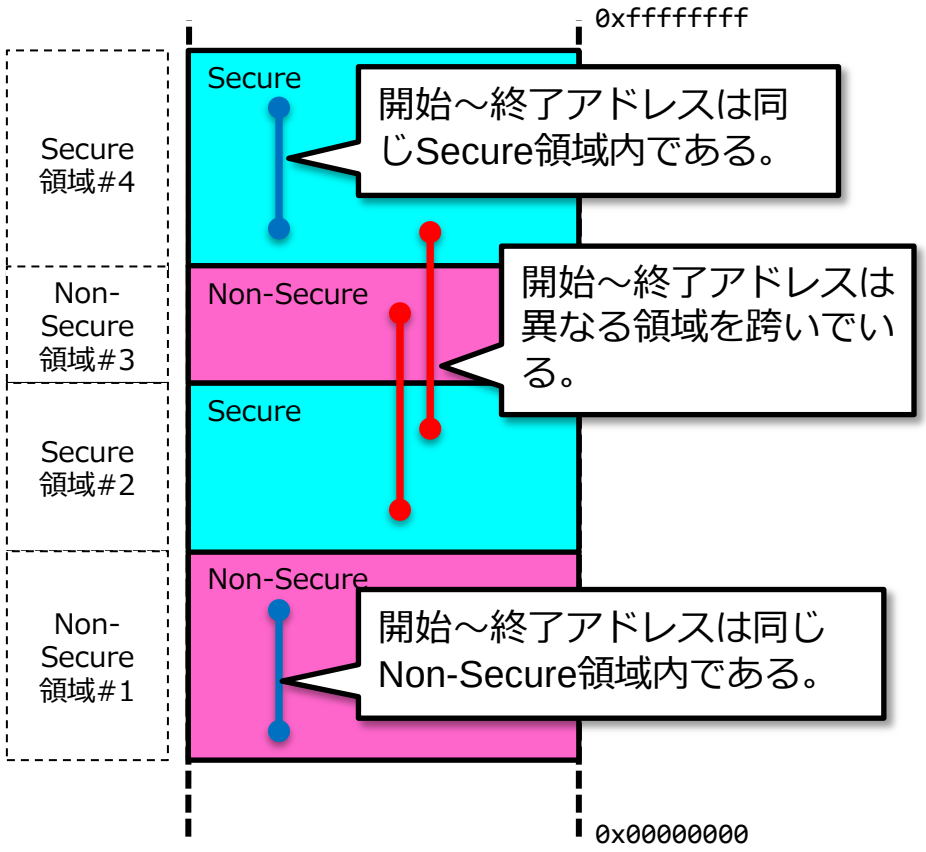
プロセッサの状態遷移



ARMv8-M TrustZone – テストターゲット

- 前述のSAUとIDAUで定義されたメモリ領域には領域番号が付与されている。
  - この領域番号によって対象が連続したセキュリティ属性を持っているかどうかを知ることが可能

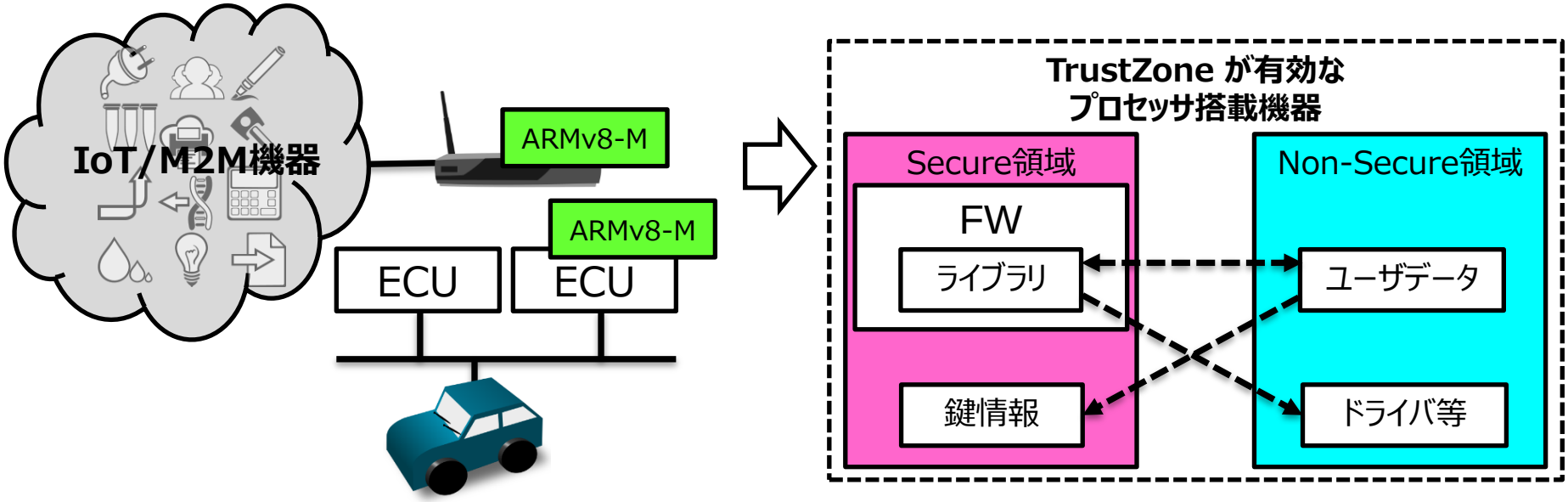
- 新たに追加されたテストターゲット命令は、アドレス値からセキュリティ属性と所属する領域番号を返却する。
  - この命令でメモリ範囲の開始と終了アドレスが同一の領域番号に所属しているか知ることができる。これによって該当範囲が非セキュアであるかどうかを判断可能。



ARMv8-M の TrustZone 活用イメージ

- 組み込み機器向けのアーキテクチャでも TrustZone をサポートしたことで、 様々なIoT機器や車載機器に対してもこの技術によるデータの保護が現実的になる。

- 例えば、M2M向けのゲートウェイ機器などに見られる Java やC言語などで任意のアプリケーションをユーザが実装できる形態の製品では、ファームウェアをセキュア領域に格納することでリバースエンジニアリング対策となることが期待できる。



まとめ

- 今回は、ARMv8-M に関して現時点で ARM社 によって公開されている情報の中から、TrustZone を紹介した。
  - 一部資料は Beta 扱いのため今後仕様が変わる可能性がある

- 現時点で、ARMv8-M アーキテクチャを採用したプロセッサ及び評価用のボードは確認できていないため、詳細な動作検証等は行えていない。
  - コンパイラについても、 GCC や Clang は現在対応中。

- 自動車向けについては、HSM規格（Hardware Security Module）が標準規格として存在しているため、 半導体メーカーは自動車向けとしてはこの規格に準拠したマイコン製品を主に出荷している
  - ARMv8-M の登場により今後、 TrustZone を活用した製品がアナウンスされる可能性はある

参考資料

- Whitepaper – ARMv8-M Architecture Technical Overview
  - https://community.arm.com/docs/DOC-10896
- ARM® コンパイラ ソフトウェア開発ガイド バージョン6.3
  - http://infocenter.arm.com/help/index.jsp?topic=/com.arm.doc.dui0773dj/pge1446115999905_00009.html
- (動画) ARMv8-M architecture: what's new for developers
  - https://youtu.be/V5zr5mPjAvU
- FFRI Monthly Research – セキュアハードウェアの登場とその分析
  - http://www.ffri.jp/assets/files/monthly_research/MR201303_TrustZone.pdf