第1章 論理的に分離し隔離する

Armv8-M向けTrustZoneのコンセプトとアーキテクチャ

金丸 敦礼

TrustZoneは，幅広い組み込みアプリケーションにおけるセキュリティ上の脅威に対応するためのシステム基盤を提供することを目的としたセキュリティ拡張です．本章では，Armv8-M向けのTrustZone for Cortex-Mのコンセプトとアーキテクチャの概要について解説します．

1．TrustZoneのコンセプト

TrustZoneのコンセプトは，ソフトウェアやメモリなどのリソースを安全な場所に論理的に隔離することにより，高いセキュリティのシステム基盤を提供することです．TrustZoneは，もともとCortex-A向けに用意されており，Armv8-Mでその適用範囲をCortex-Mにも広げました．TrustZoneの他にもさまざまなアプローチでリソースを安全な場所に隔離する手段があり，それらを組み合わせることでより安全なソフトウェア実行環境を実現できます．

● 組み込みアプリケーションにおけるセキュリティ上の脅威

現在，組み込みアプリケーションにおけるセキュリティ上の脅威として，一般的に次の3種類のサイバー攻撃が挙げられます（**図1**）．

▶通信経路への攻撃

組み込みデバイスへの通信経路を狙った攻撃です．攻撃手法の例としては，中間者攻撃（Man In The Middle Attack）や通信経路の改ざん，傍受などが挙げられます．これらの攻撃を防ぐためには，通信経路の暗号化などを行い，通信経路のセキュリティを強化することが重要です．

▶ソフトウェアへの攻撃

組み込みデバイスで実行されているソフトウェアを狙った攻撃です．攻撃手法の例としては，バッファ・オーバフローやマルウェアなどが挙げられます．これらの攻撃は，組み込みソフトウェアの脆弱性を悪用して実行されるため，脆弱性を特定し，対策を講じることが重要です．

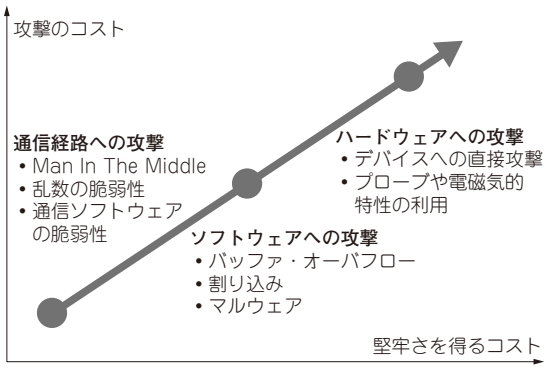

図1　組み込みアプリケーションにおけるセキュリティ上の脅威

▶ハードウェアへの攻撃

組み込みデバイスのハードウェアそのものを狙った物理的な攻撃です．攻撃手法の例としては，JTAGなどのI/Oを介したデバイスへの物理的なアクセス，デバイスの電磁気的な特性を利用したサイド・チャネル攻撃などが挙げられます．これらの攻撃に対しては，物理的な攻撃への耐性の向上や攻撃を受けたときに自壊する仕組みを用いることで防ぐことが可能です．

いずれのサイバー攻撃においても，攻撃する側，防御する側，双方に相応のコスト・労力がかかります．また，通信経路への攻撃よりもソフトウェアへの攻撃の方が，さらにはハードウェアへの攻撃の方が，より多くのコスト・労力を必要とします．

● 守りたいものだけを隔離して守る

サイバー攻撃に対する一般的なセキュリティ対策のコンセプトは，ソフトウェアやメモリなどのリソースを安全な場所に隔離して守ることです．サイバー攻撃から守りたいものがデバイス上に分散して存在すると，その管理や防御に大変な労力がかかります．あらゆるソフトウェアのバグがセキュリティ上の欠陥につながる可能性があるため，検証しなければならない範囲が非常に広くなり，脆弱性が生じるリスクが上がります．守りたいものだけを安全な場所に隔離して管