これから10年使える技術！
標準AUTOSAR開発プラットホーム入門

安全に使い回す！車載ソフトウェアの世界

第11回　クルマ用OSの安全メカニズム①…アクセス保護

高田 光隆

表1　AUTOSAR OSには幾つかの保護機能を備えたクラスが用意されている
第9回表3再掲

種　類	説　明
SC1	基本機能セット（OSEK/VDK仕様の上位互換相当）
SC2	SC1 + タイミング保護
SC3	SC1 + メモリ（アクセス）保護
SC4	SC1 + タイミング保護 + メモリ（アクセス）保護

● クルマ用定番AUTOSAR OSの保護機能

今回は，クルマ用標準開発環境AUTOSARの，アプリケーションを「安全」に使うための仕組みや機能について説明します．

AUTOSAR OSには，スケーラビリティ・クラスという機能別のクラスが用意されています（**表1**）．例えば，SC2ではタイミング保護機能が，SC3ではメモリ保護機能が仕様に盛り込まれています（第9回，第10回でも説明）．

アプリケーションの設計ミスやコンフィグレーションの設定間違いなどで，アプリケーションや基本ソフトウェア・モジュール（BSW）が想定外の振る舞いをした場合でも，これらの保護機能があれば，問題の発生を検知して影響範囲を限定的に抑えることができるようになります．

アクセス保護の単位「OSアプリケーション（OSAP）」

● OSが管理するタスクやカウンタなどの機能の単位…OSオブジェクト

AUTOSARのOSモジュールOsは，タスク，割り込みサービス・ルーチン（ISR），カウンタ，アラーム，スケジュール・テーブルといったOSオブジェクトを管理しています．

● OSオブジェクトはアクセス保護単位OSアプリケーション（OSAP）に所属する

Osは，メモリ保護機能が有効になっている場合（SC3，SC4を使用する場合），OSアプリケーション（OSAP）の単位でアクセスの保護を行います（**図1**）．OSオブジェクトは，どこかのOSアプリケーションOSAPに所属することになります．

AUTOSAR OS仕様では2つのOSアプリケーションを定義しています．

● タイプ1：信頼OSアプリケーション（Trusted OS-Application）

信頼OSアプリケーション（信頼OSAP）は，ハードウェアへのアクセスやシステム・サービスの使用に制

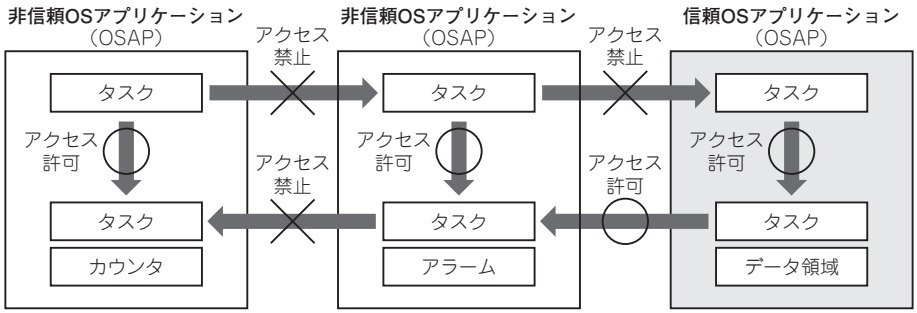

図1　AUTOSAR OSはOSアプリケーション単位でアクセス保護を行える
OSアプリケーションには，信頼/非信頼のタイプがあり，非信頼タイプは他のOSアプリケーションにアクセスできない．タスクやカウンタなどのOSオブジェクトは，必ずどれか1つのOSアプリケーションに所属することになっており，漏れなくアクセス管理できる

第1回　車載ソフトウェアの基本構造（2016年1月号）
第2回　AUTOSAR準拠ソフトウェアの基本開発ステップ（2016年2月号）
第3回　実験のハードウェア＆使用した車載マイコン（2016年3月号）