



TOPPERSプロジェクトの最新状況と 本日の発表内容について



2017年11月15日

高田 広章

NPO法人 TOPPERSプロジェクト 会長
名古屋大学 大学院情報学研究科 教授
附属組込みシステム研究センター長
APTJ株式会社 代表取締役会長・CTO

Email: hiro@ertl.jp URL: <http://www.ertl.jp/~hiro/>

TOPPERSプロジェクトの概要と 最新状況

TOPPERSプロジェクトとは?



- ▶ ITRON仕様の技術開発成果を出発点として、組み込みシステム構築の基盤となる各種の高品質なオープンソースソフトウェアを開発するとともに、その利用技術を提供

組み込みシステム分野において、Linuxのように広く使われるオープンソースOSの構築を目指す!

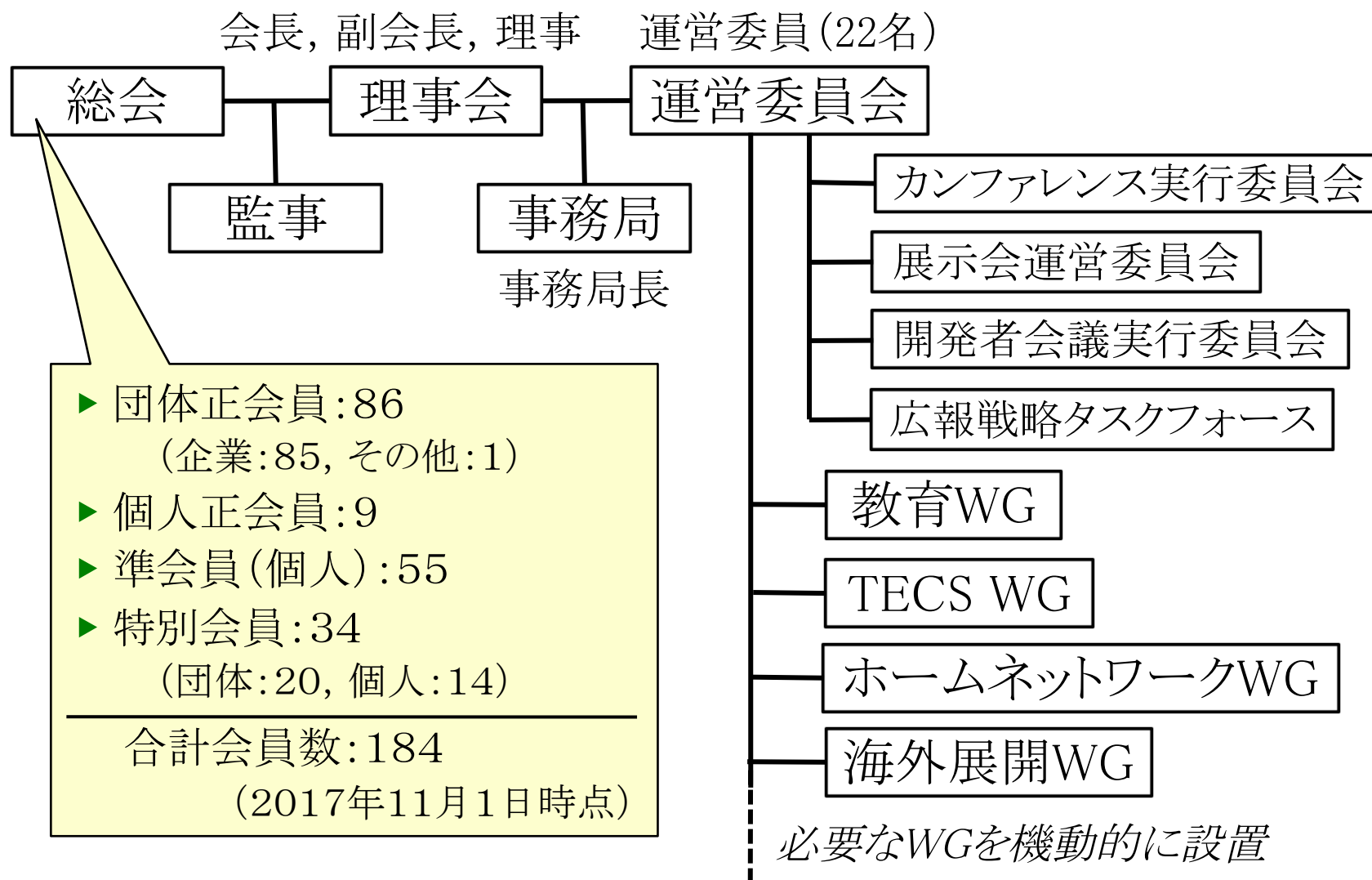
プロジェクトの狙い

- ▶ 決定版のITRON仕様OSの開発 ← 完了
- ▶ 次世代のリアルタイムOS技術の開発
- ▶ 組み込みシステム開発技術と開発支援ツールの開発
- ▶ 組み込みシステム技術者の育成への貢献

プロジェクトの推進主体

- ▶ 産学官の団体と個人が参加する産学官民連携プロジェクト
- ▶ 2003年9月にNPO法人として組織化

TOPPERSプロジェクトの組織と会員



主な開発成果物

一般公開しているもの

第1世代カーネル

- ▶ TOPPERS/JSPカーネル, TOPPERS/FI4カーネル
- ▶ TOPPERS/ATK1 (Automotiveカーネル バージョン1)
- ▶ TOPPERS/FDMPカーネル, TOPPERS/HRPカーネル

新世代(第2世代)カーネル

- ▶ TOPPERS/ASPカーネル, TOPPERS/SSPカーネル
- ▶ TOPPERS/FMPカーネル, TOPPERS/HRP2カーネル

第3世代カーネル(ITRON系)

- ▶ TOPPERS/ASP3カーネル

AUTOSAR関連

- ▶ TOPPERS/ATK2 (Automotiveカーネル バージョン2)
- ▶ TOPPERS/A-COMSTACK, TOPPERS/A-WDGSTACK
- ▶ TOPPERS/A-RTEGEN

ミドルウェア

- ▶ TINET, FatFs for TOPPERS
- ▶ TOPPERS/ECNL (ECHONET Lite通信ミドルウェア)
- ▶ RLL (Remote Link Loader), DLM (Dynamic Loading Manager)

ツール, その他

- ▶ TECS (TOPPERS組込みコンポーネントシステム)
- ▶ SafeG (高信頼組込みシステム向けデュアルOSモニタ)
- ▶ MDCOM (MultiDomain Communication Module)
- ▶ EV3RT (LEGO Mindstorms EV3向けSPF)
- ▶ TLV (TraceLog Visualizer), TOPPERS Builder

教育コンテンツ

- ▶ 初級・中級実装セミナー教材
- ▶ 基礎1・(新)基礎2・(新)基礎3実装セミナー教材
- ▶ 基礎ハードウェア設計セミナー教材
- ▶ ETロボコン向けTOPPERS活用セミナー教材

開発成果物の主な利用事例



エスクード (スズキ)



スカイラインハイブリッド (日産)



IPSiO GX e3300 (リコー)



H-IIIB (JAXA)



Cell³iMager duos
(SCREEN
ホールディングス)



OSP-P300
(オークマ)



SoftBank
945SH
(シャープ)



UA-101 (Roland)



PM-A970(エプソン)

次の10年を見据えた活動指針 (2011年度に策定)

Smart Futureのための組込みシステム技術

- ▶ 組込みシステム技術を、持続可能なスマート社会の実現 (Smart Future) のための重要な要素技術の1つと位置づけ、その研究開発と普及に取り組む
- ▶ それに向けての研究開発課題
 - ▶ Safety & Security
 - ▶ Ecology (高エネルギー効率)
 - ▶ Connectivity

コンソーシアムによるオープンソースソフトウェア開発

- ▶ 同じ技術に関心を持つプロジェクトメンバによりコンソーシアムを結成し、複数組織の協力によりソフトウェアを開発
- ▶ 開発したソフトウェアは、TOPPERSプロジェクトからオープンソースソフトウェアとして公開

重点的に取り組んでいるテーマ

※ SPF:ソフトウェア
プラットフォーム

次世代のリアルタイムカーネル技術

- ▶ TOPPERS第3世代カーネル(ITRON系)
- ▶ 車載システム向けRTOS(AUTOSAR OS仕様からの発展)

ソフトウェア部品化技術

- ▶ TECS(TOPPERS組込みコンポーネントシステム)

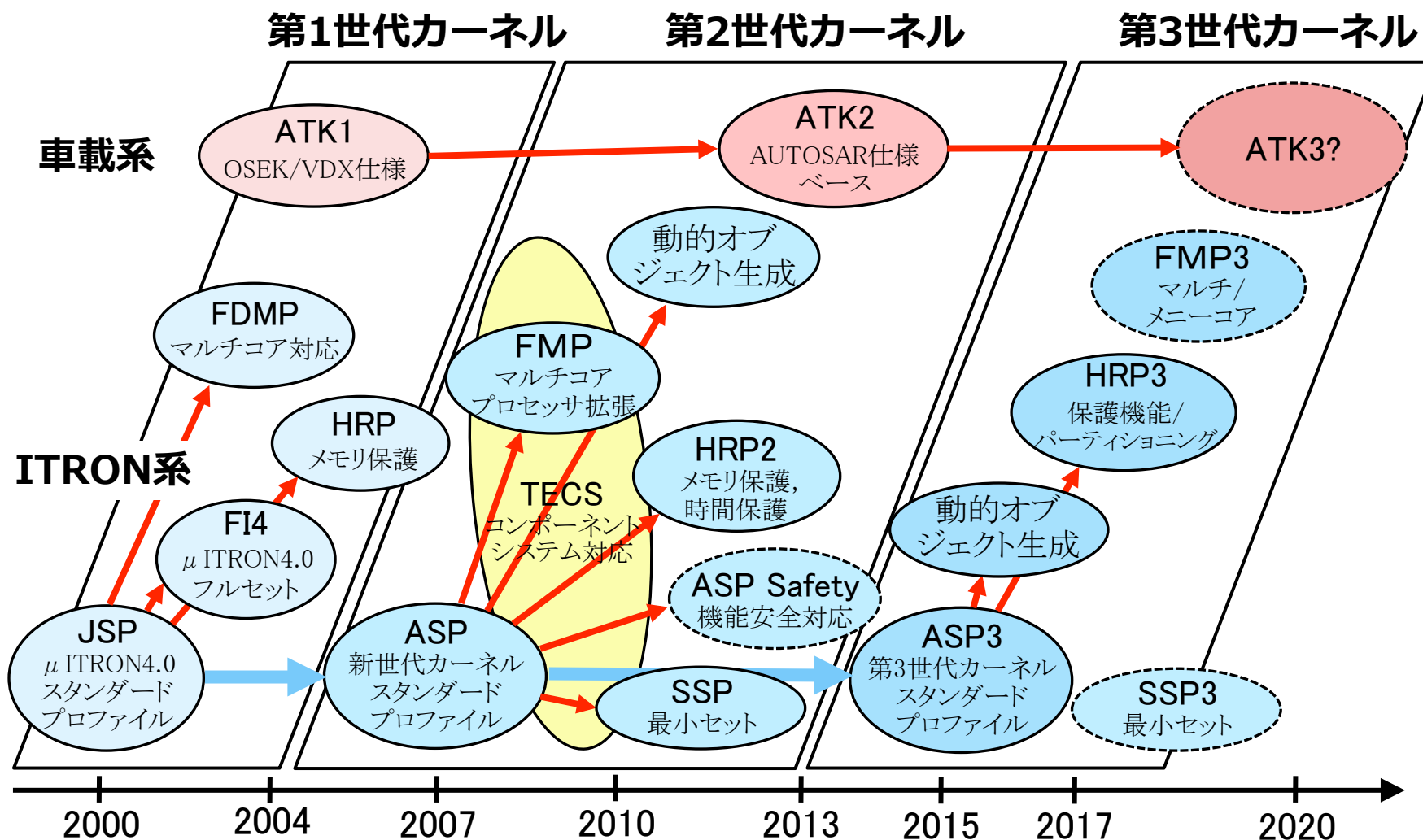
組込みシステム向けSPFと開発支援ツール

- ▶ 車載制御システム向けSPF(AUTOSAR仕様ベース)
- ▶ 仮想化技術(SafeG, A-SafeG), ホームネットワーク
- ▶ 宇宙機向けSPF(SpaceWire OS)
- ▶ 開発支援ツール(シミュレータ, 可視化ツール)

技術者育成のための教材開発

- ▶ プラットフォーム技術者の育成
- ▶ ETロボコン向けSPFと教材の提供

TOPPERSカーネル開発ロードマップ



第3世代カーネルの必要性

求められている/求められつつある技術・機能

- ▶ 機能安全からの要求に応えられるパーティショニング
- ▶ ティックレスの高分解能時間管理と外部時刻同期
- ▶ マルチコアにおける動的ロードバランシング
- ▶ メニーコアプロセッサへの対応 … 今後の課題

一方、廃止すべきと考えられる機能もある

- ▶ タスク例外処理機能, メールボックス

TOPPERS第3世代カーネルへ

- ▶ 第2世代のカーネルの次の世代と位置付けた方が, 大胆な仕様変更が可能
- ▶ 第3世代においても, 2系列(ITRON系, 車載系)のリアルタイムカーネル開発は, 引き続き維持していく

TOPPERS/ASP3カーネル

位置づけ

- ▶ TOPPERS第3世代カーネル(ITRON系)の出発点
- ▶ TOPPERS/ASPカーネルの改良版

新しく実装した機能・特徴(主なもの)

- ▶ タスク終了要求機能 … タスク例外処理機能に代えて導入
- ▶ 高分解能(マイクロ秒単位)の時間管理
- ▶ ティックレスタイマ … 省電力化に貢献
- ▶ 外部時刻同期のための機能
- ▶ システムサービスをTECSを用いて構築
- ▶ Ruby版コンフィギュレータを採用

リリース状況と今後の計画

- ▶ 2016年2月に一般公開, 最新版はRelease 3.2.0
- ▶ 今後, 各種のプロセッサへポーティング

TOPPERS/HRP3カーネルの リリースについて

～機能安全要求に対応できるパーティショニン グ機能を備えたITRON系RTOSを開発～

TOPPERS/HRP3カーネル

位置づけ

- ▶ ASP3カーネルに保護機能／パーティショニング機能を追加したもの(ASP3カーネルの上位互換)
- ▶ TOPPERS/HRPカーネル, HRP2カーネルの改良・拡張版

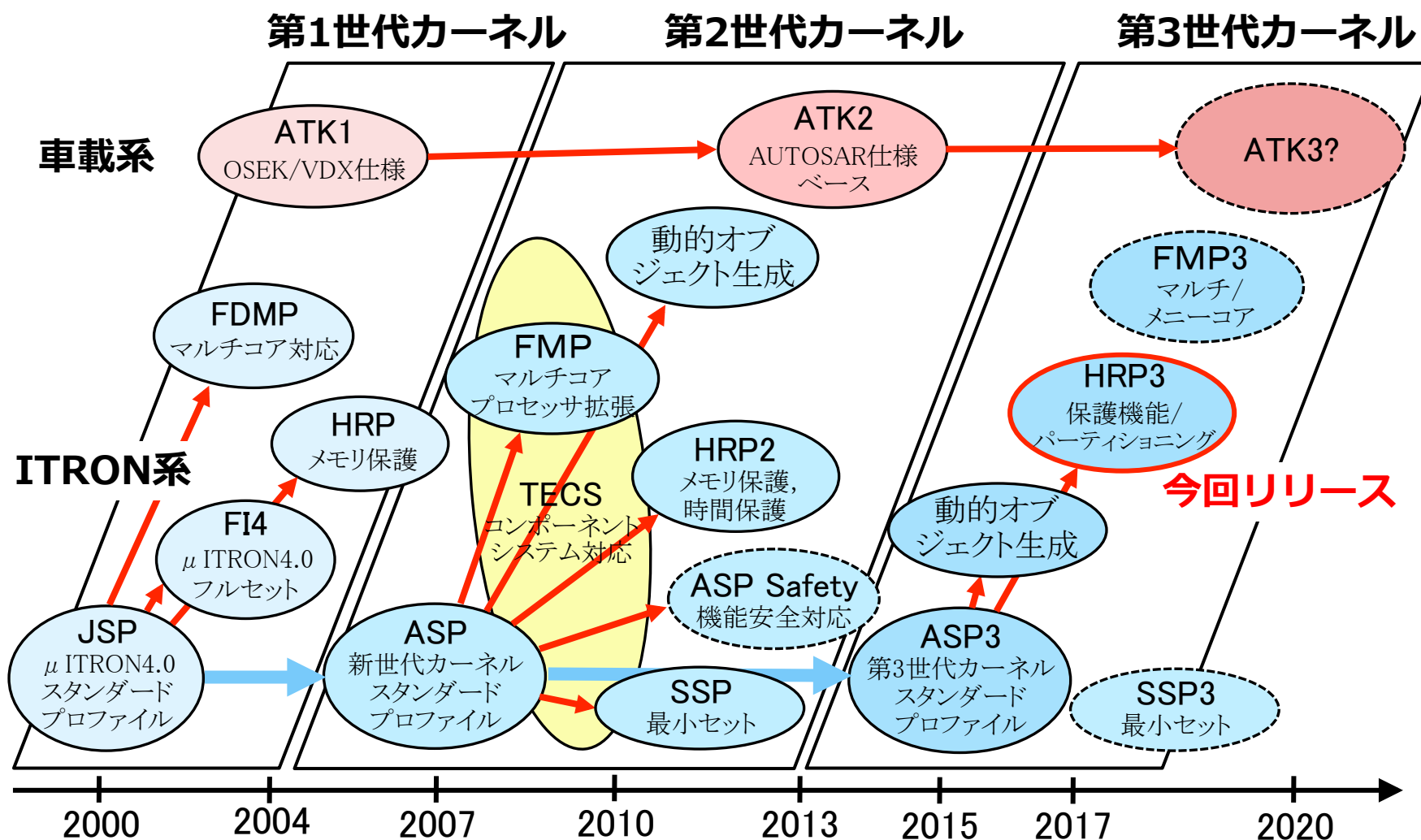
ASP3カーネルに対する追加機能

- ▶ メモリ保護機能
 - ▶ メモリ配置の自動決定(HRP2カーネルと同様)と手動決定(HRPカーネルと同様)の両方をサポート
- ▶ オブジェクトアクセス保護機能
- ▶ 時間パーティショニング機能
- ▶ 拡張サービスクール機能

リリース計画

- ▶ 2018年1月に一般公開予定

TOPPERSカーネル開発ロードマップ



保護機能／パーティショニング機能とは？

OSの保護機能とは？

- ▶ OS上で動作するあるアプリケーションが誤動作した場合に、その誤動作がOS自身や他のアプリケーションに悪影響を及ぼすこと(悪影響の波及)を防ぐための機能

保護機能の有用性

- ▶ アプリケーション毎に必要な信頼性レベル(例:機能安全規格における安全度水準(SIL))まで検証すればよい
- ▶ セキュリティの確保・向上
 - ▶ サイバー攻撃の直接的な対象となるネットワークアプリケーションから他のアプリケーションを保護
- ▶ 潜在しているバグが早期に発見できる
 - ▶ テスト期間の短縮・テストコストの削減につながる
- ▶ システムの致命的な障害を防ぐ

悪影響の波及の2つのパターン

(1) アプリケーション間の通信を通じて

- ▶ 誤動作したアプリケーションが間違ったデータを渡すことにより、悪影響が他のアプリケーションに波及する

(2) 共有資源を通じて

- ▶ 誤動作したアプリケーションが、他のアプリケーションと共有する資源に誤ったアクセスを行い、その結果、悪影響が他のアプリケーションに波及する

OSのパーティショニング機能とは？

- ▶ アプリケーションが使用する資源を**分離**することにより、あるアプリケーションが誤動作した場合でも、他のアプリケーションに悪影響を及ぼすことを防止するための機能
 - ▶ 共有資源を通じた悪影響の波及を防ぐための対策
 - ▶ アプリケーション間の通信を通じた悪影響は別途対策が必要(アプリケーション間を分離すると通信できない)

共有資源の共有方法

- ▶ 共有資源は、時間分割、空間分割、またはその組み合わせによって、複数のアプリケーションで共有される

共有資源の種類による整理

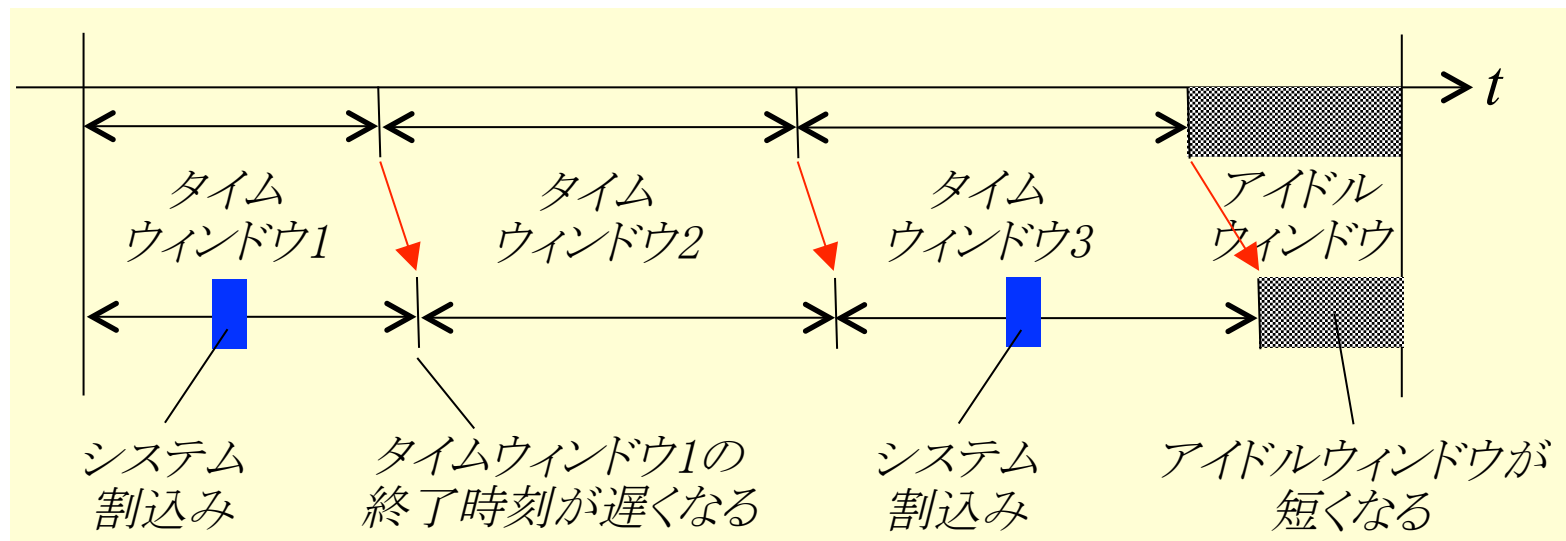
- ▶ プロセッサ
 - ▶ プロセッサおよびその一部とみなされる資源
 - ▶ (シングルスプロセッサでは) 時間分割により共有
- ▶ メインメモリ
 - ▶ (動的メモリ管理を用いない限りは) 空間分割により共有
- ▶ 周辺デバイス
 - ▶ 複数のアプリケーションから使われる周辺デバイス(以下, 共有デバイスと呼ぶ)
 - ▶ 共有方法は, 周辺デバイス毎に異なる
- ▶ カーネルやミドルウェアなどが管理するオブジェクト

HRP3カーネルの保護機能／パーティショニング機能

- ▶ HRP3カーネルがサポートする機能とパーティショニング
 - ▶ 時間パーティショニング機能 → プロセッサの時間パーティショニング機能(そのもの)
 - ▶ メモリ保護機能 → メインメモリの空間パーティショニングを実現可能
 - ▶ オブジェクトアクセス保護機能 → カーネルオブジェクトの空間パーティショニングを実現可能
- ▶ 共有デバイスは、ミドルウェア(またはデバイスドライバ)で管理されるのが一般的であり、それに対する保護機能／パーティショニング機能はミドルウェアでサポートすべき
 - ▶ HRP3カーネルは、それを可能にするための機能をサポートする

TOPPERS時間パーティショニングスキーム

- ▶ 各パーティションは、システム周期内で各パーティションを実行するタイムウィンドウを決める方式(航空機向け規格であるARINC 653で採用)をベースとして、システム割込み(タイムウィンドウによらずに受け付けられる割込み)を許すように拡張した方式でスケジュール
- ▶ パーティション内で複数のタスクを実行する場合には、従来のOSと同じ方式でスケジュール(階層型スケジュール)



HRP3カーネルへのTECSの導入

TECS (TOPPERS組込みコンポーネントシステム)とは？

- ▶ 各種のソフトウェアモジュールを部品化し、必要な部品を組み合わせることによって大規模な組込みソフトウェアを効率的に構築するための技術

HRP3の保護機能を使えるように拡張

- ▶ TECSジェネレータのプラグインで対応

HRP3のシステムサービスをTECSを用いて構築

- ▶ 拡張サービスコール(ユーザタスクから特権モードで動作するシステムサービス呼び出す場合に用いる)のグルーロジックを、TECSジェネレータにより生成
 - ▶ 記述が大幅に楽になる
 - ▶ ASP3カーネル向けとHRP3カーネル向けで、システムサービス本体の記述が同じにできる
- ! AUTOSARのRTEジェネレータと類似の技術

今後のカーネル開発計画

各種のターゲットへのポーティング

- ▶ TOPPERS/ASP3およびHRP3を各種のターゲットプロセッサへポーティング
 - ▶ HRP3は、現時点ではARMプロセッサのみをサポート

第3世代カーネルの充実

- ▶ TOPPERS/FMP3カーネル
 - ▶ マルチ/メニーコアプロセッサ向け拡張
 - ▶ HRP3カーネルとの統合も検討
- ▶ TOPPERS/SSP3カーネル
 - ▶ 最小セットカーネル