ETロボコン向け TOPPERS活用セミナー

ソフトウェアプラットフォームとRTOSの基礎

2020年7月18日

高田 広章

NPO法人 TOPPERSプロジェクト 会長
名古屋大学 未来社会創造機構 モビリティ社会研究所 教授
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
Email: hiro@ertl.jp　URL: http://www.ertl.jp/~hiro/

目次

TOPPERSプロジェクトの概要

- TOPPERSプロジェクトとは？，主な開発成果物

ソフトウェアプラットフォーム（SPF）とその必要性

- プラットフォームの構築・活用と標準化

RTOSの基礎

- RTOSとリアルタイムカーネル，RTOS/SPFの主な機能
- マルチタスク機能，タスク間の通信と同期，保護機能
- 静的OS，RTOSを使用するメリット・デメリット

RTOSを用いたシステム設計の指針

- タスクへの分割指針，タスクの優先度の決定

TOPPERS/ASP3カーネル・HRP3カーネルの機能とAPI

付録：TOPPERS/HRP3カーネルの時間パーティショニング機能

TOPPERSプロジェクトの概要

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!

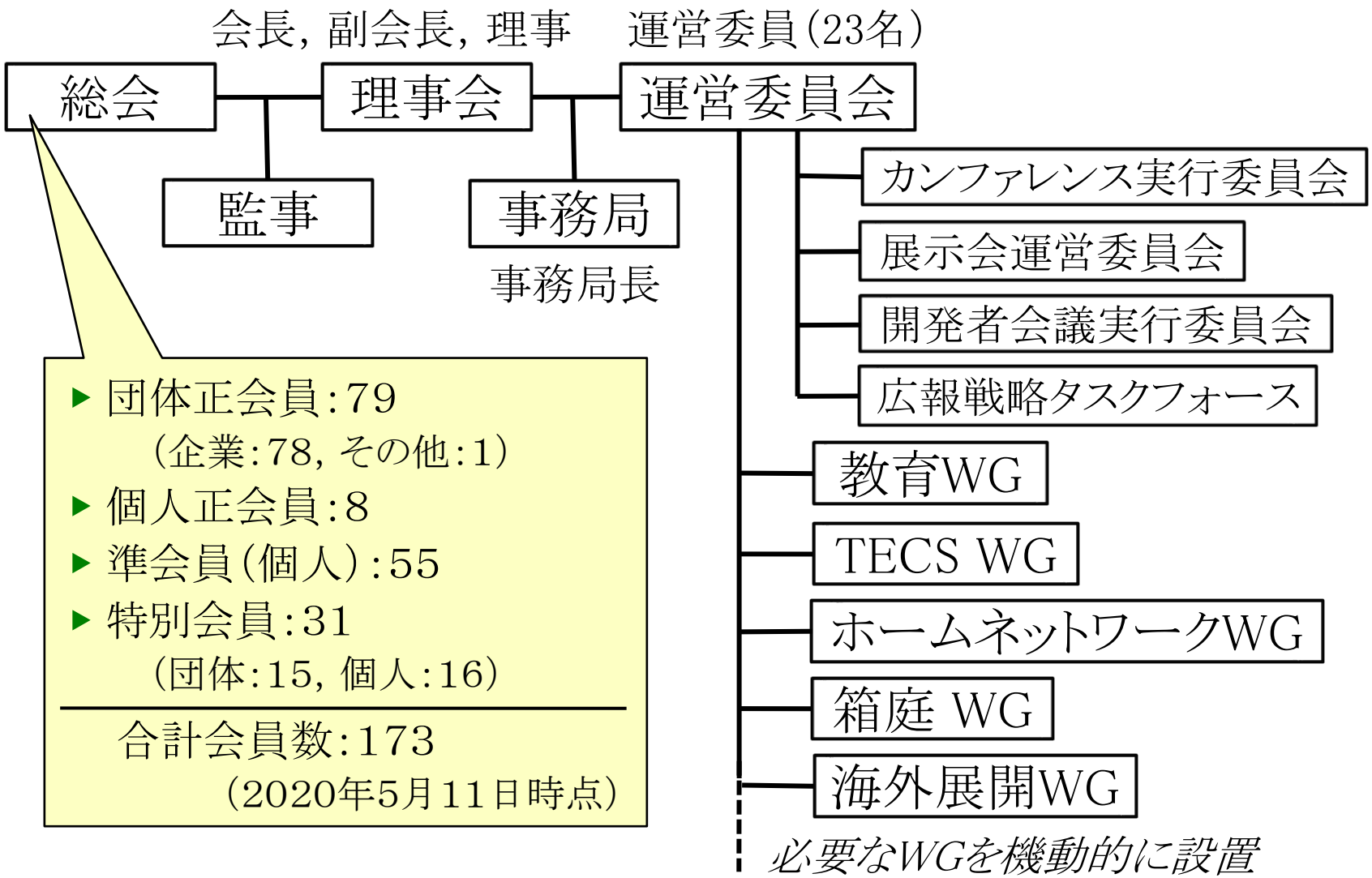
プロジェクトの狙い

- 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
- 組込みシステム開発技術と開発支援ツールの開発
- 組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

NPO法人 TOPPERSプロジェクトの会員と組織

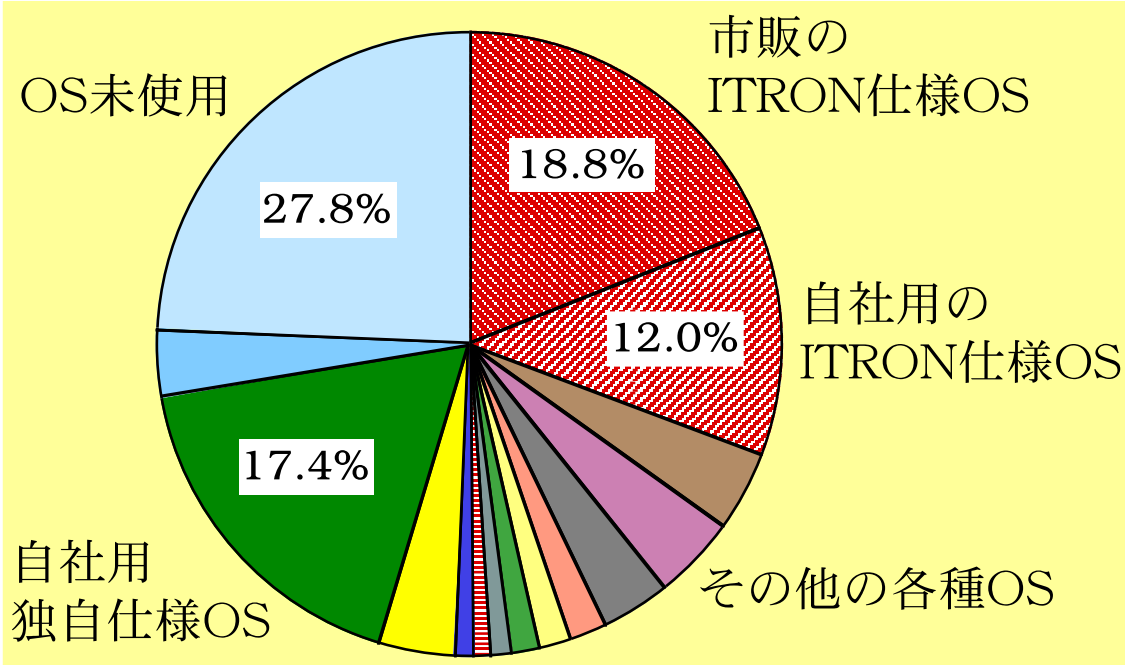


参考) ITRON仕様とは

- トロンプロジェクトにおいて標準化してきた組込みシステム向けのリアルタイムカーネルとそれに関連する仕様
- 誰でも自由に実装できるオープンな仕様

! それに準拠して実装されたOSはオープンとは限らない

- 産学共同の標準化活動の成果
- 多くのプロセッサ上に実装され，国内では業界標準に



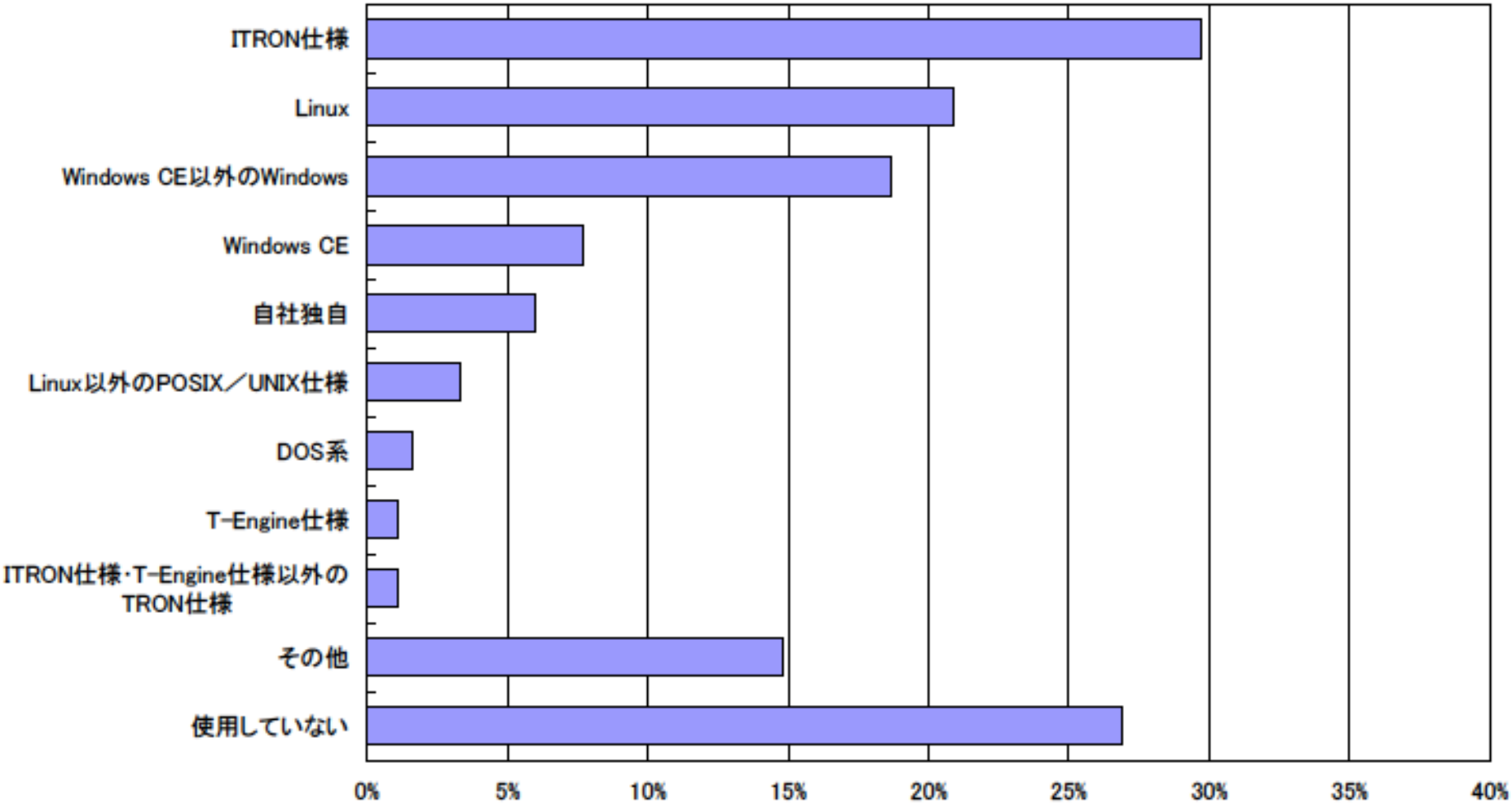
最近開発した組込み機器に使用したOS

（トロン協会による調査，1998年末～1999年頭，日本）

Q2-7 ターゲットOSの種類

複数選択

プロジェクト責任者

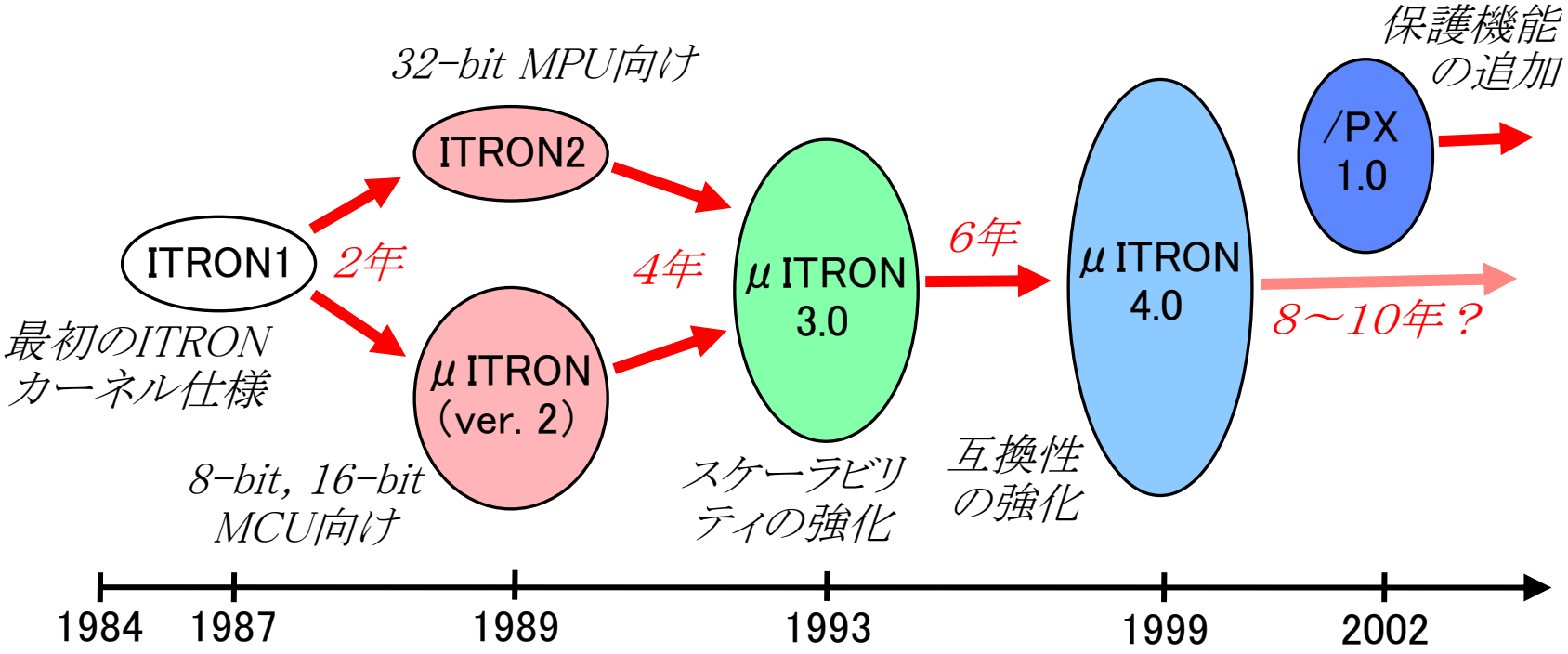


使用プロジェクトの割合

経済産業省 Copyright © 2010 Ministry of Economy, Trade and Industry All Rights Reserved.

ITRONカーネル仕様の歴史

- プロジェクト開始から約20年間に，4世代のITRONカーネル仕様を策定・公開
- μITRON4.0仕様は，この世代のリアルタイムOS技術の範囲では，極めて完成度の高い仕様に



ITRONカーネル仕様の特徴

- OSの小型軽量化が可能
  - ワンチップマイコンにも適用可能
- 仕様の理解が容易
  - ! 技術者教育のための標準化の側面を重視
- 完全にオープンな標準仕様
  - ロイヤリティなしで実装することができる
- 多種多様なプロセッサ用に実装できる/されている
  - 8-bitワンチップマイコンから64-bitマイコンまで
  - 異なるプロセッサへの移行が容易に
- 多くの機器で使用実績がある
  - 組込みシステム分野で最も広く使われているOS仕様
- 多くのメーカ/ベンダがサポート

ITRON仕様カーネルの開発状況

- 多くのITRON仕様準拠のRTOSが開発・販売された
- 自社用に実装した例も多数
- いくつかのオープンソースの実装

ITRON仕様カーネルの主な適用機器例

AV機器，家電，個人用情報機器，娯楽/教育機器

- テレビ，ビデオ，デジタルカメラ，STB，オーディオ，電子レンジ，
- 炊飯器，PDA，電子手帳，カーナビ，ゲーム機，電子楽器

パソコン周辺機器/OA機器

- プリンタ，スキャナ，ディスクドライブ，DVDドライブ，コピー，FAX

通信機器

- 留守番電話機，携帯電話機，放送機器，無線設備，人工衛星

運輸機器，工業制御/FA機器/設備機器，その他

- 自動車，プラント制御，工業用ロボット，自動販売機，医療用機器

TOPPERSの主な開発成果物

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，TOPPERS/HRP3カーネル
- TOPPERS/FMP3カーネル，TOPPERS/HRMP3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（TCP/IPスタック），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）
- TOPPERS BASE PLATFORM（ST，CV，RV）
- SafeG（デュアルOSモニタ），SafeG64
- EV3RT（LEGO Mindstorms EV3向けSPF）
- MDCOM（MultiDomain Communication Module）

教育コンテンツ

- 初級・中級実装セミナー教材
- 基礎1・基礎2・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-IIB（JAXA）

Cell^{3}iMager 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)

TOPPERSライセンス

- TOPPERSプロジェクトで独自に開発したソフトウェアには，独自のライセンス条件を設定する

基本的な考え方

- 組込みシステムの事情を考慮し，GNU GPLやBSDライセンスより自由に使えるライセンス条件とする
- 成果をアピールすることが開発資金獲得に繋がることから，どこでどう使われているかをなるべく知りたい

ライセンスの内容

- 派生物をオープンする義務は課さない．派生物を販売するビジネスも可能
- 機器に組み込んで使用する場合の実質的な義務は，利用したことを報告することのみ … **レポートウェア**

開発成果物の知的財産権に関する規則

基本的な考え方

- ユーザの利益と開発者の参加しやすさを折衷させる
- 著作権（侵害が自覚できる）と産業財産権（特許権など，知らずに侵害する場合がある）を区別して考える

規則の最も重要な部分

- TOPPERSの開発成果物は，TOPPERSの会員（この規則を守ることに合意している）が開発する
- 会員は著作権侵害をしない義務
- 会員は，自らが開発する開発成果物中に，自らが所有する産業財産権が利用されている場合には，開発成果物の利用者に対して，当該産業財産権の実施を無償許諾
- 会員は，開発成果物が何らかの知的財産権を侵害していることを発見した場合に，報告する義務

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仕様ベース）

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

- TOPPERS BASE PLATFORM, ホームネットワーク
- シミュレーション環境（箱庭），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），ドメイン間通信（MDCOM）

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

成果物利用とプロジェクト参加のお誘い

- 開発成果物はウェブサイトから自由にダウンロードできますので，ぜひご利用ください
- プロジェクトの活動に参加したい方/活動を支援して頂ける方は，ぜひプロジェクトにご入会ください
  - 企業会員　入会金:11万円，年会費:11万円
  - 個人準会員　入会金:5.5千円，年会費:5.5千円

TOPPERSプロジェクトは，組込みシステム開発に有用な高品質なオープンソースソフトウェアと教育コンテンツを開発し，組込みシステム開発に新しいスタンダードを提案します

http://www.toppers.jp/

ソフトウェアプラットフォームとその必要性

組込みシステム開発を取り巻く状況

半導体技術，ネットワークの進歩

組込みシステムの大規模化・複雑化

- 機器の複合化・デジタル化・ネットワーク化
- 制御要素に情報処理要素が複合
- コンピュータ制御による高機能化・高付加価値化

ネットワーク接続とクラウド連携の拡大

- 組込みシステムと情報システムを結合した大規模なシステム（統合システム，CPS，IoT）の構築が重要に

組込みシステムの適用分野が拡大

- コンピュータの小型化・低価格化により広がる適用分野

開発期間の短縮やコストダウンに対する要求

- 新興国との競争の中で今まで以上のコストダウン要求

（単一の）プロセッサの高速化の限界

- 消費電力（=発熱量）が最大の制約条件に

組込みシステムの開発効率化と品質確保のために

すぐにできること

- ソフトウェア開発プロセスの地道な改善
- 人材育成 … 時間はかかるが着手はすぐにできる

中期的に取り組むべきこと

- 設計抽象度を上げる＆設計の早い段階での検証
  - モデルベース／モデル駆動開発の流れ
  - シミュレーション（仮想環境）による検証
- 設計資産の再利用を促進する仕組みの構築
  - ソフトウェアの再利用は，差分開発が中心の組込みシステム開発では特に有効
- 応用分野毎のプラットフォームの構築・活用と共通化
  - プラットフォーム＝ハードウェア＋OS＋ミドルウェア
- 非機能要求のモデリングとアシュアランスケース

プラットフォームの構築・活用と標準化

プラットフォームとは？

- プラットフォーム＝ハードウェアPF＋ソフトウェアPF
- ソフトウェアPF（SPF）＝OS＋ミドルウェア＋デバドラ

応用ドメイン毎のプラットフォーム構築と活用

- 適切な範囲（これが難しい）の応用ドメインを設定し，それに向いたプラットフォームを構築
- 構築したプラットフォームを，多くのアプリケーションに活用

プラットフォーム化による再利用性と品質の向上

- アプリケーションの再利用性が向上することに加え，プラットフォーム自身の再利用による開発コスト減も
- システムの品質確保の鍵となる部分であり，高品質なプラットフォームの構築は，システムの品質向上につながる
- 新機能/新技術の導入が容易に

プラットフォームの標準化の意義

- プラットフォームは，業界内での標準化によりその導入意義が増す
- プラットフォームの独占/寡占の回避
  - 特定ベンダのプラットフォーム製品に縛られることを避けることは，コスト最適化の上で重要
  - プラットフォーム（特にSPF）は，独占/寡占が起こりやすい分野
  - プラットフォームの（実質的な）独占/寡占は，独占/寡占したベンダの力を極めて強くする
  - 自動車業界がリソースをかけて標準化を推進する理由
- ソフトウェア構築手順の標準化
  - 自動化（ツール化）が促進される
  - 分散開発が容易に
- 技術者の確保/育成

プラットフォームの共通化・標準化の例

- 社内でのプラットフォーム共通化

  例）パナソニックのUniPhier（ユニフィエ）

  - プロセッサとビデオコーデックなどを含むシステムLSIと，ミドルウェアやOSなどのソフトウェアからなるデジタル家電用の統合プラットフォーム
- 業界内でのプラットフォーム標準化
  - 自動車制御システム向けのプラットフォームやツールの標準化
    - AUTOSAR（http://www.autosar.org/）
    - JASPAR（http://www.jaspar.jp/）
- デファクト標準によるプラットフォーム標準化
  - スマートフォン向けのプラットフォームは2つに収束している（3つめがあるかも？）

AUTOSAR (AUTomotive Open System ARchitecture)

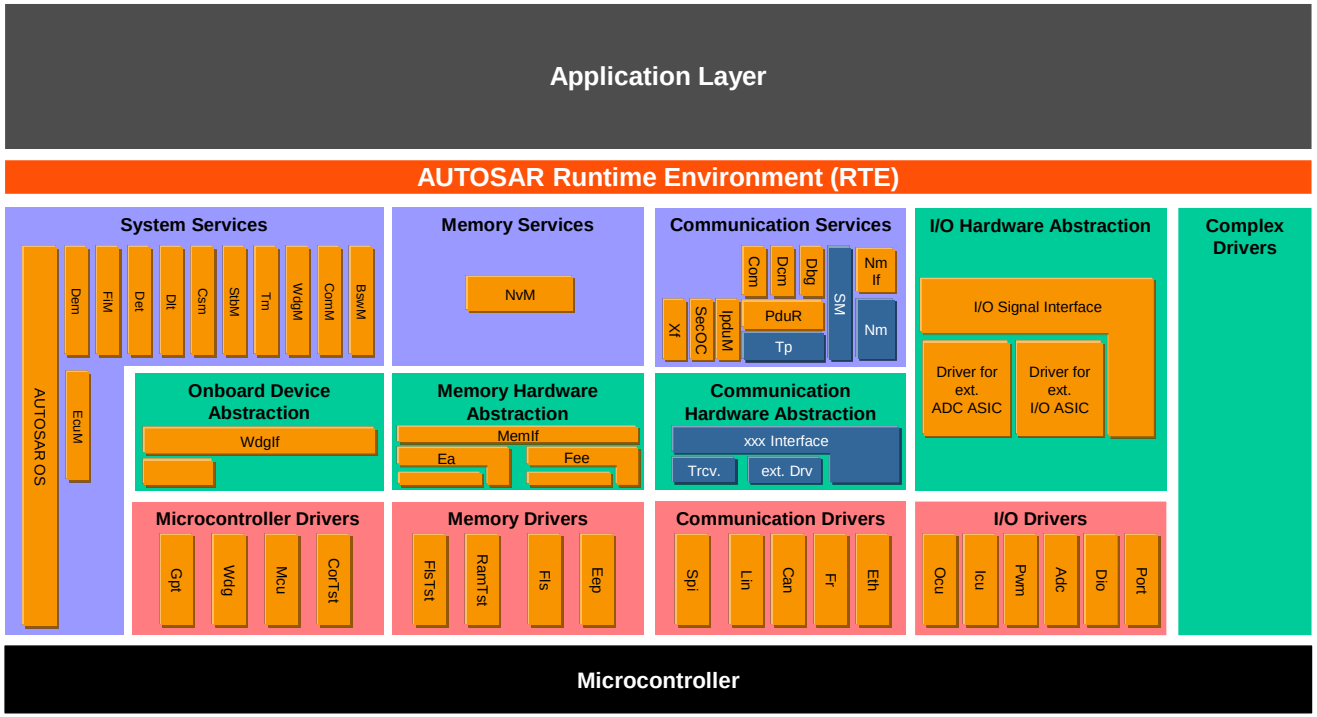
- 自動車，自動車部品，エレクトロニクス，半導体，ソフトウェア企業によるグローバルパートナーシップ（2003年に設立）
  - ソフトウェアの複雑性を軽減するために，ソフトウェア基盤（infrastructure）の業界標準を作成
- コアパートナー（2020年時点）

BMW	Daimler	PSA Peugeot Citroen
Bosch	Ford	トヨタ自動車
Continental	GM	Volkswagen

- 2つのプラットフォーム仕様の標準化を推進
  - 制御システム向けのClassic Platform（CP）仕様は，100を超えるソフトウェア仕様書とほぼ同数の関連ドキュメントなどで構成
  - 自動運転システム向けのAdaptive Platform（AP）仕様は，仕様策定とリファレンス実装が並行して進行中

AUTOSAR Classic Platformの構成

- Runtime Environment (RTE)
  - SW-C間，SW-CとBSW間の通信インタフェースを提供
- Basic Software（BSW）
  - OS+デバイスドライバ+ミドルウェア群



AUTOSAR Layered Software Architecture 4.2.2より

RTOSの基礎

リアルタイムシステムとは?

JISによる「実時間処理」の定義

- 計算機外部の処理に関係を持ちながら，かつ外部の処理によって定められる時間要件にしたがって，計算機の行なうデータ処理

リアルタイムシステム研究者の間で一般的な定義

- 処理結果の正しさが，出力される結果値の正しさに加えて，結果を出す時刻にも依存するようなシステム

! 単に速い応答を求められるシステムをリアルタイムシステムと呼ぶわけではない

多くの組込みシステムはリアルタイムシステム

- 組込みシステムは，機械・機器を制御するシステムであり，制御対象の時間要件にしたがうことが必要
- 一部の処理のみにリアルタイム性が求められる場合も

RTOS (リアルタイムOS) とは?

- 文字通り，リアルタイムシステム構築のためのOS
- 具体的には，次のような特徴を持つOS（これらの特徴をすべて持っているとは限らない）

（1）リアルタイムシステム向けの機能を持つ

- プリエンプティブな優先度ベーススケジューリング
- 優先度継承や優先度上限プロトコルのサポートなど

（2）予測可能性を持つ

- OSの各サービス時間があらかじめわかっている
- ただし，予測可能性にもいろいろなレベルがある

（3）時間制約を管理 ← 一部の研究ベースのRTOS

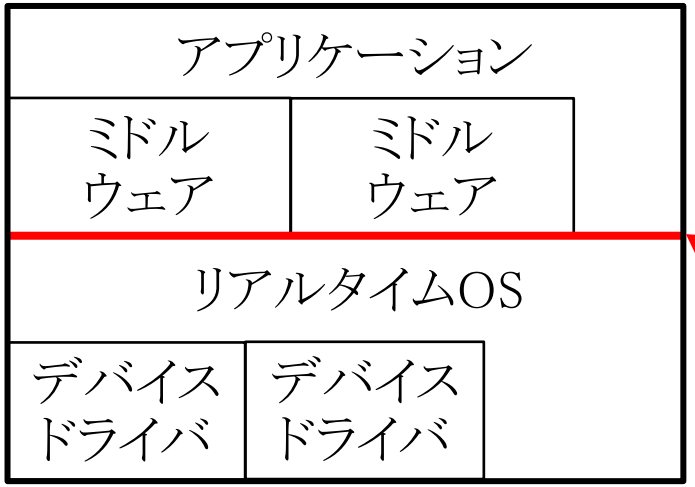
- OSが各処理の時間制約を考慮してスケジューリング

（4）高速に応答（制御対象に対して十分に）

RTOSの構造とリアルタイムカーネル

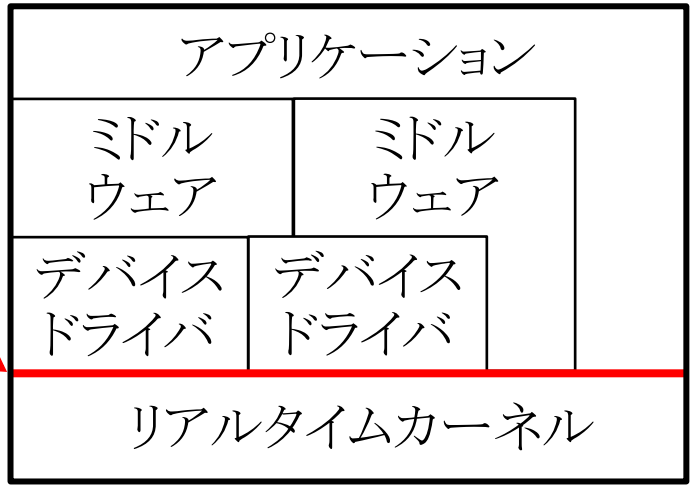
アーキテクチャによるRTOSの分類（中間的なものもある）

- 汎用OS型



- OSの機能は豊富
- サイズは比較的大きい
- 一般に応答時間は遅い
- デバイスドライバは別のAPIで作成

- リアルタイムカーネル型



- カーネルの機能は限定
- カーネルサイズは小さい
- 一般に応答時間は早い
- デバイスドライバとアプリケーションは同じAPI

リアルタイムカーネル

- (元々は)RTOSの中心になるモジュールの意味
  - どのようなコンピュータシステムにも共通する資源(プロセッサ，メモリ，タイマ，…)を扱う
  - 汎用OSのカーネルとは意味(定義)がやや異なる
- 保護機能を持っているとは限らない
- リアルタイムカーネルは，構造上/役割上はOSに他ならないが，汎用OSとは機能的に大きく異なるため，混同を避けたい場合には「リアルタイムカーネル」と呼ぶ
  - リアルタイムカーネル相当の機能しか必要としない場合もある．その場合は，「リアルタイムカーネル＝RTOS」
- リアルタイムモニタ，リアルタイムエグゼクティブと呼ばれることもある

! この講義では，主にリアルタイムカーネル型を想定

確認：オペレーティングシステム（OS）の役割

! どの範囲のソフトウェアをOSと呼ぶかは，明確な定義がない（例：ウィンドウシステムはOSの一部か？）

- ハードウェアの仮想化
  - ハードウェアとしてのコンピュータの機能を拡張し使いやすく柔軟なコンピュータを提供すること
  - そのために，ハードウェアを抽象化・多重化
- ハードウェア資源の管理機能
  - ユーザにハードウェア資源の共同利用を許し，資源が効率よく使用されるように管理すること

例）ファイルシステム

- *ストレージデバイスというハードウェア資源を抽象化・多重化するとともに，複数のアプリケーションからのアクセスを許す*

リアルタイムカーネル型が出てきた理由

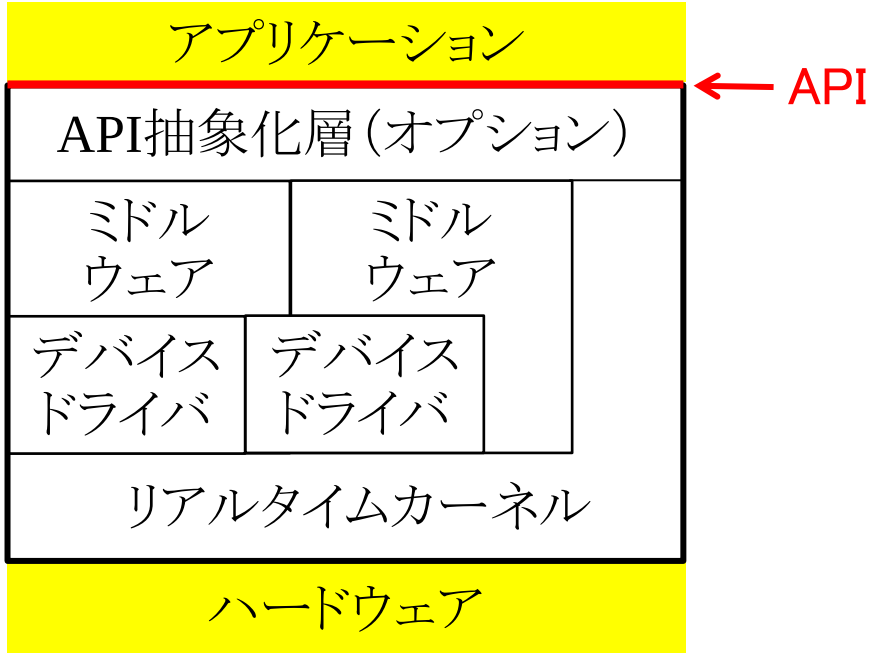
- OSが必ずサポートしなければならないI/O装置はない
  - 多くの組込みシステムが共通に持つI/O装置が無い
    例）ストレージデバイスを持たない組込みシステムも多い
  - 複数のアプリケーションで同一のI/O装置を共有する状況は少ない
- I/O装置の制御は組込みシステムの目的そのもの

保護のための機能は必須ではない

- 組込みソフトウェアは，組込み対象の機器を制御することのみを目的に設計され，機器に固定されている
  → デバッグが終われば，アプリケーションソフトウェアは信頼できるという前提が成り立つ
- 最近では，機能安全への効率的な対応のために，保護機能の必要性が高まっている

リアルタイムカーネルを核にしたプラットフォーム

- リアルタイムカーネルを中心に，あるアプリケーションドメイン向けのデバイスドライバやミドルウェアを載せて，ソフトウェアプラットフォーム（SPF）を構築するケースが多い



- API抽象化層（例えば，POSIXインタフェース層）はあってもなくてもよい

RTOS/SPFの主な機能

リアルタイムカーネルの機能

- マルチタスク機能 → プロセッサの仮想化
- タスク間通信・同期機能
- 時間同期/管理 → タイマの仮想化
- メモリ管理 → メモリの仮想化
- 割込み管理/処理, 例外管理/処理, システム管理　など
- 保護機能 … 保護機能を持ったRTOSも増えつつある

汎用OS型のRTOS/SPFのその他の機能

- 入出力管理／デバイス管理機能
- ファイル管理機能(ファイルシステム)
- 通信・ネットワーク機能(プロトコルスタック)
- ユーザインタフェース機能(GUIなど)
- プログラム管理／ローディング機能　などなど

マルチタスク機能

タスクとは？

! ここでのタスクは，スレッドと同義

- プログラムの並行実行の単位
  - 1つのタスク中のプログラムは逐次的に実行される
  - 異なるタスクのプログラムは並行して実行される
- プロセッサを抽象化・多重化したもの

プロセッサ —（抽象化／多重化）→ タスク

… 仮想化されたプロセッサ

マルチタスク機能

- 複数のタスクを疑似並列に実行するための機能
  - シングルプロセッサシステムでは，実際に同時に実行できるタスクは1つのみ
  - 複数のタスクが同時に実行しているかのように見せる

用語の整理

- *ディスパッチ(タスクディスパッチ，タスク切換え)*
  - プロセッサが実行するタスクを切り換えること
  - ディスパッチを実現するOS内のモジュールがディスパッチャ
- *スケジューリング(タスクスケジューリング)*
  - どの時間にどのタスクを実行するかを決定すること
  - 多くのRTOSにおいては，次に実行するタスクを決定する処理
  - スケジューリングを実現するOS内のモジュールがスケジューラ(UNIX/Linuxのスケジューラは，スケジューリングに加えて，ディスパッチも行う)
- *スケジューリングアルゴリズム*
  - どのようにして次に実行するタスクを決定するか？

プリエンプティブな優先度ベーススケジューリング

- ! ほとんどのRTOSで採用されているスケジューリング方式（RTOSによっては他の方式もサポートしている）
- *優先度ベーススケジューリング*
  - 最も優先度の高いタスクが実行される
  - 優先度の高いタスクが実行できなくなるまで，優先度の低いタスクは実行されない
  - 同一優先度タスク間では FCFS（First Come First Served）
- *プリエンプティブスケジューリング*
  - 優先度の高いタスクが実行可能になると，優先度の低いタスクが実行途中でも，タスク切換えが起こる
  - 実行可能になるきっかけは割込み
- ! 汎用OSのスケジューリングとは大きく異なる

マルチタスクの必要性

タスク分割の基本的な考え方

- 独立した処理の流れを独立したタスクに
  - 複数のサブシステムに対する処理
  - 別々の入出力装置/イベントに対する処理　など

リアルタイムシステムにおけるタスク分割の意義

- *論理的な処理の順序と時間的な処理の順序を分離*
  - プログラムは論理的な処理順序で記述
  - RTOSは時間的な処理順序に従って実行する

↓

- プログラムの保守性・再利用性の向上
- 外部で開発されたソフトウェア部品の導入を容易に

論理的な処理順序と時間的な処理順序の分離

例として次の処理を行う場合を考える

- モータの制御処理を10ミリ秒周期で行う．1回の処理に最大5ミリ秒かかる
- それと並行して，ビデオカメラで撮影した画像を認識する処理を行う．1回の処理に最大100ミリ秒かかる

RTOS無しで実現するには…

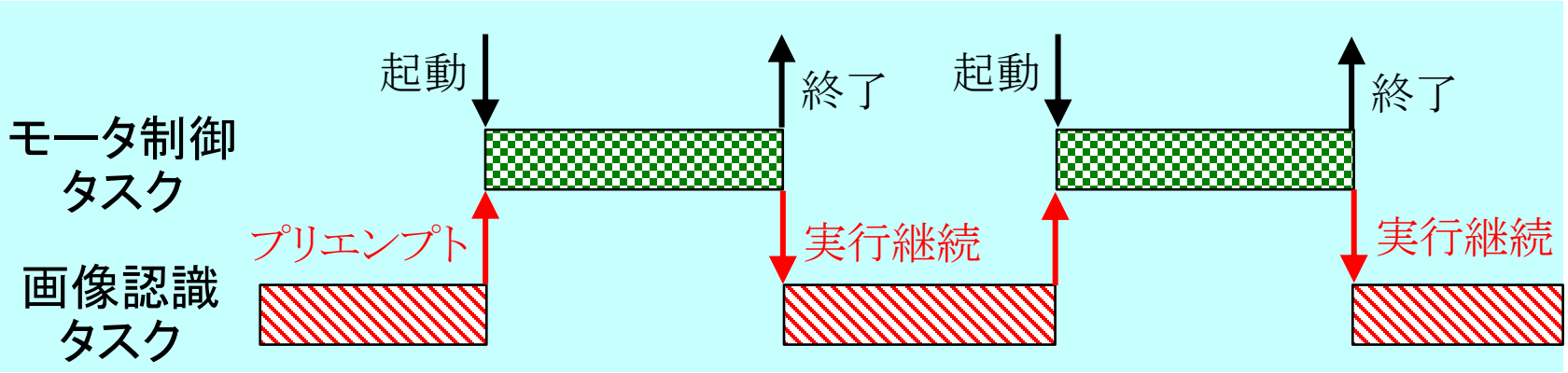
- モータの制御処理を，10ミリ秒周期で回るメインループで実行する
- 画像認識プログラムを，5ミリ秒単位の20個の処理に分割し，メインループの中で1つずつ順に実行する

↓

画像認識プログラムの保守性・再利用性が低下

RTOS（マルチタスク機能）を用いると…

- 2つの処理を別々のタスク（モータ制御タスクと画像認識タスク）で実現
- モータ制御タスクの方に高い優先度を与える
- モータ制御タスクは10ミリ秒周期で起動する



画像認識プログラムを分割する必要はなく，保守性・再利用性が向上

論理的な処理順序と時間的な処理順序の分離が本質

- モータ制御処理と画像認識処理は，論理的には独立の処理
- 時間的には，画像認識処理の途中にモータ制御処理を割り込ませないと間に合わない

↓

- プログラムは論理的な処理順序で（つまり両処理を独立して）記述し，それを時間的な処理順序で実行するのはRTOSに任せる

↓

- *時間制約を持ったプログラムの保守性・再利用性の向上*
- *外部で開発されたソフトウェア部品の導入を容易に*

! ただし，この例の場合には，RTOSを使わずに，メインループと割込み処理で実現する方法もある

タスク状態

基本的なタスク状態

- RTOSでは，タスクが疑似並列実行されている状況をアプリケーション開発者に明示することが必要

実行状態と実行可能状態
(RUNNING)　　(READY)

実行すべき処理が無い状態　休止状態 (DORMANT)

- 低優先度タスクが実行される
- 起動されると，タスクの先頭から実行される

何らかの事象発生を待っている状態　(広義の)待ち状態

! 事象の発生をループで待ってはいけない

- 低優先度タスクが実行される
- 事象が発生した場合に，前の続きから実行される

待ち状態の有用性

- プログラム中のどこを実行しているかで，状態を表現するプログラムで有用
- 特に，呼び出された関数の内部で待ち状態としたい場合

例）サーバからのデータ取出し処理（）

```
{
    サーバにデータAを問い合わせるコマンドを送る;
    サーバからの応答を待ち，変数Aに格納する;
    サーバにデータBを問い合わせるコマンドを送る;
    サーバからの応答を待ち，変数Bに格納する;
}
```

- ローカル変数で状態を保持できるのもメリットの1つ

タスク間の通信と同期

タスク間通信・同期の必要性

- タスクが協調して動作するためには，タスク間でデータをやりとりすること（＝タスク間通信）が必要
- タスク間通信の際には，タスク同士で動作タイミングをあわせること（＝タスク間同期）が必要
- 複数のタスクが同一の資源を取りあう場合にも，タスク間同期が必要（排他制御）

タスク間通信・同期のタイプ

! タスクを仮想化されたプロセッサと捉えるなら，タスク間の通信・同期は，プロセッサ間の通信・同期を仮想化したもの

- 共有メモリによる通信
- メッセージによる通信

共有メモリによる通信

- 複数のタスクからアクセスできるメモリ領域（共有メモリ）上に受け渡しするデータを置く
- 共有データを読み書きする際には，排他制御することが必要．RTOSは排他制御のための機能を持つ
  （共有データが1度に読み/書きできる場合は例外）
  - 割込み/ディスパッチの禁止，タスク優先度の変更
    - ! *マルチプロセッサへの拡張性に注意*
  - セマフォ，ミューテックス
    - ! *デッドロックと優先度逆転に注意*
- 共有データを速やかに処理させたい場合には，事象の発生を知らせる機能を用いる
  - タスクの起動/起床
  - イベントフラグ，条件変数（Condition Variable）

メッセージによる通信

- RTOSが持つメッセージ通信のための機能を用いて，タスク間でメッセージを受け渡しする

メッセージ通信機能のタイプ

- コネクションあり *or* なし，単方向 *or* 双方向，1対1（送受信できるタスクが固定）*or* n対1 *or* n対n
- 通信相手の指定方法
  - 通信オブジェクトを指定 *or* 相手タスクを指定 *or* …
- 同期メッセージ通信 *or* 非同期メッセージ通信
- （非同期通信で）バッファにメッセージが無い時の振舞
  - 待つ（ブロッキング）*or* 待たない（ノンブロッキング）
- （非同期通信で）バッファがフルの時の振舞い
  - 待つ（ブロッキング）*or* 待たない（ノンブロッキング）*or* 上書きする

メッセージ通信機能のタイプ（続き）

- メッセージが固定長 *or* 可変長（任意長）
- （可変長の時に）パケットの単位がある *or* ない
- ポインタを渡す *or* コピーする
  （メッセージが1度に読み/書きできる場合は意味が無い）
- （非同期通信で）メッセージのキューイング順序
  - FIFO順 *or* 優先度順
- 受信/送信待ちタスクのキューイング順序
  - FIFO順 *or* 優先度順
- その他の特殊な機能
  - マルチキャスト/ブロードキャスト
  - 状態メッセージ（OSEK/VDX仕様のunqueued message）

! RTOSの持つメッセージ通信機能（複数の機能を持つ場合も多い）の性質を良く理解することが必要

RTOSの保護機能

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障害を引き起こすのを防ぐための機能

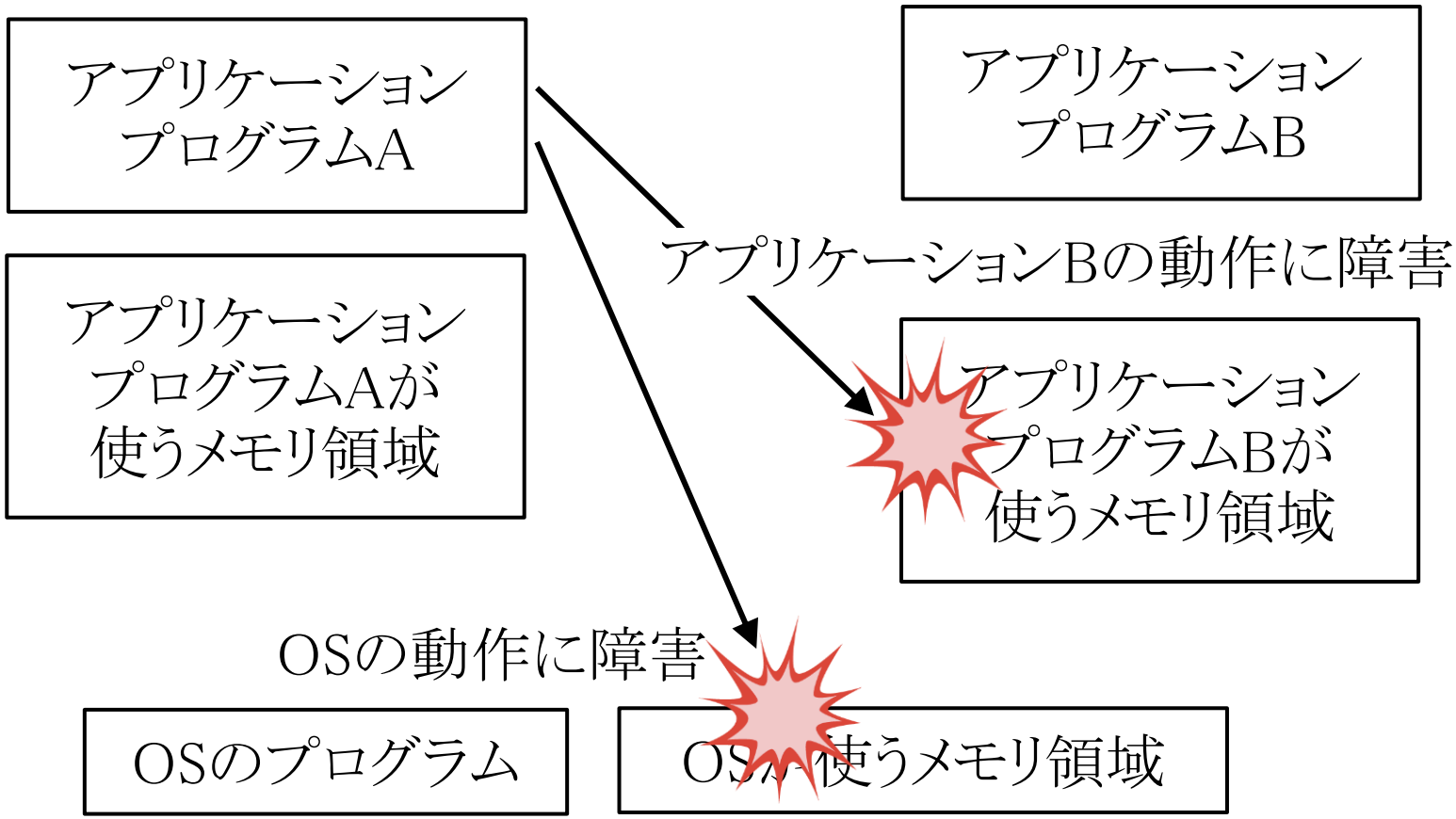
保護機能の有用性

- 潜在しているバグが早期に発見できる
  - ソフトウェアのテスト期間の短縮・テストコストの削減につながる
- 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
- システムの致命的な障害を防ぐ

  例）システム内の重要な機能・データを守る

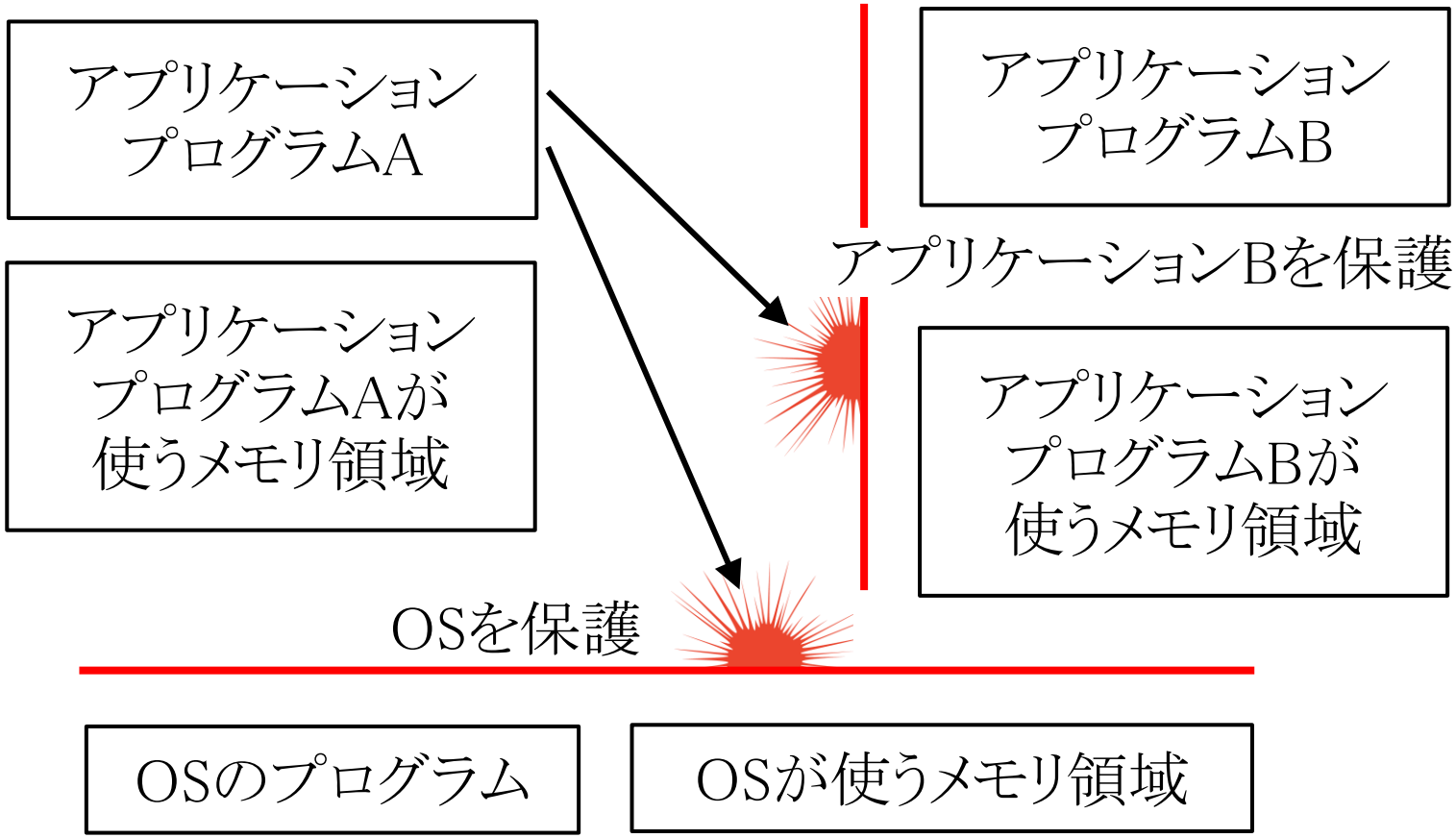
保護機能の有用性 ～ メモリ保護の例で

- メモリ保護機能がない場合，アプリケーションAが誤動作すると…



保護機能の有用性 ～ メモリ保護の例で

- メモリ保護機能があると，前述のような問題を防ぐことができる



RTOSが保護機能を持たなかった理由

- 保護機能を実現するためのオーバヘッドが大きい
  - メモリ保護機能を実現するのに必要なハードウェアを持たないプロセッサも多い
- ソフトウェアが小規模であり，高い信頼性を確保することが比較的容易であった
  - そもそも「あるアプリケーションが誤動作する」ことが許されないと考えられてきた
- 機器の出荷後に外部からプログラムがダウンロードされることはなく，ソフトウェアのデバッグが終わるとシステム内で動作するソフトウェアは信頼できるという前提が成り立った

→ これらの理由は成り立たなくなってきている

保護機能の種類

- 資源のアクセスに関する保護機能
  - メモリ保護：アクセスしてはならないメモリ領域へのアクセスを防止する
  - オブジェクトアクセス保護（またはサービス保護）：アクセスしてはならないカーネルオブジェクトへの（サービスコールによる）アクセスを防止する
- 資源の分配に関する保護機能
  - プロセッサの時間保護：プロセッサの処理時間を使い過ぎるのを防止する
  - メモリの分配保護：メモリを多く確保し過ぎるのを防止する

! *その他の資源に対する時間保護/分配保護も考えられる*

メモリ保護機能

- 保護の単位となるアクセス主体がアクセスできるメモリ領域を限定する

例）タスクは以下のメモリ領域のみにアクセスできる

  - 自タスクのスタック領域
  - 自保護ドメインのプログラム領域とデータ領域
  - 共有のプログラム領域
  - 共有データ領域（すべての保護ドメインから読めて，特定の保護ドメインのみが書き込める領域）
  - 自保護ドメインのアクセスするI/O領域

- サービスコールにポインタを渡し，サービスコール内で行うメモリアクセスも保護の対象とする

! 汎用OSのプロセスのように，保護ドメイン毎に別々のメモリ空間を持つとは限らない（その必要性が低い）

オブジェクトアクセス保護機能（サービス保護機能）

- 保護の単位となるアクセス主体が，サービスコールによってアクセスできるカーネルオブジェクトを限定する

  例）あるセマフォにアクセスできる保護ドメインを限定する

- カーネルオブジェクトに関連しないサービスコールを呼び出せるアクセス主体を限定する

  例）割込みを禁止できる保護ドメインを限定する

プロセッサの時間保護機能

- 保護の単位となるアクセス主体が，与えられた以上のプロセッサ時間を使うことを防止する

特権サービスの呼出し

- 特権モードで実行されるルーチンを登録し，それを呼び出すための機能
  - 特権モードで実行する必要のあるミドルウェアやデバイスドライバの呼出しに用いることを想定

静的OS (Static Operating System)

! 専用システムであるという特性を活かしたOS技術

静的OSとは？

- 使用するOS資源（タスク，セマフォなど）を静的に（設計時に）定義するOS

  例）多くのμITRON仕様OS，多くのTOPPERS OS

  OSEK/VDX仕様OS，AUTOSAR OS仕様（OS資源を動的に生成するAPIが仕様に規定されていない）

静的OSの利点

- メモリ容量（特にRAM容量）を小さくできる
- システム起動時間を短縮できる
- システムの動作中にメモリ不足になることがない
- 静的な情報を使った最適化が可能

コンフィギュレーション記述の方法

(1) コンフィギュレーション記述の言語を定め，そこからツールにより構成・初期化ファイルを生成する方法

- ITRON仕様の静的API
- OSEK/VDX仕様のOIL（OSEK Implementation Language）
- AUTOSAR仕様ではXMLのフォーマットを規定

(2) GUIベースのコンフィギュレーションツールを用意する方法

(3) 構成・初期化ファイルを直接記述する方法（C言語の初期化文の形で記述するのが一般的）

- 静的な情報を使った最適化は難しい

RTOSを使用するメリット

- ソフトウェアの構造化（≒ モジュール化）による生産性，保守性，信頼性の向上
- 時間制約を持った多重処理システムの構築を容易に
  - 論理的な処理順序と時間的な処理順序の分離により，時間制約を持ったソフトウェアの保守性・再利用性が向上

    ➡ ソフトウェア部品を用いたソフトウェア開発（コンポーネントベース開発）の基盤
- プロセッサの違いを隠蔽
  - プロセッサの細部（特に，割込み処理関連）を知らなくても，アプリケーションが構築できる
  - 「リアルタイムカーネルは，プロセッサのデバイスドライバである」
- 保護機能の活用

RTOSを使用するデメリット

RTOSを使用するメリットとの引き換え

- RTOS自身のオーバヘッド
  - オーバヘッドによる実行性能の低下
  - RTOS自身のワークエリアによるメモリの消費

  → リアルタイムカーネルでは，半導体技術やRTOS実装技術の進歩により，問題になる場面は減ってきた
- プリエンプティブスケジューリングのデメリット
  - タスクのスタックエリアによるメモリの消費
  - 非決定性が増すことによるデバッグ・テストの困難化

  → 行儀のよいタスク間同期・通信の設計が必要
- RTOSのブラックボックス化による解析の困難性

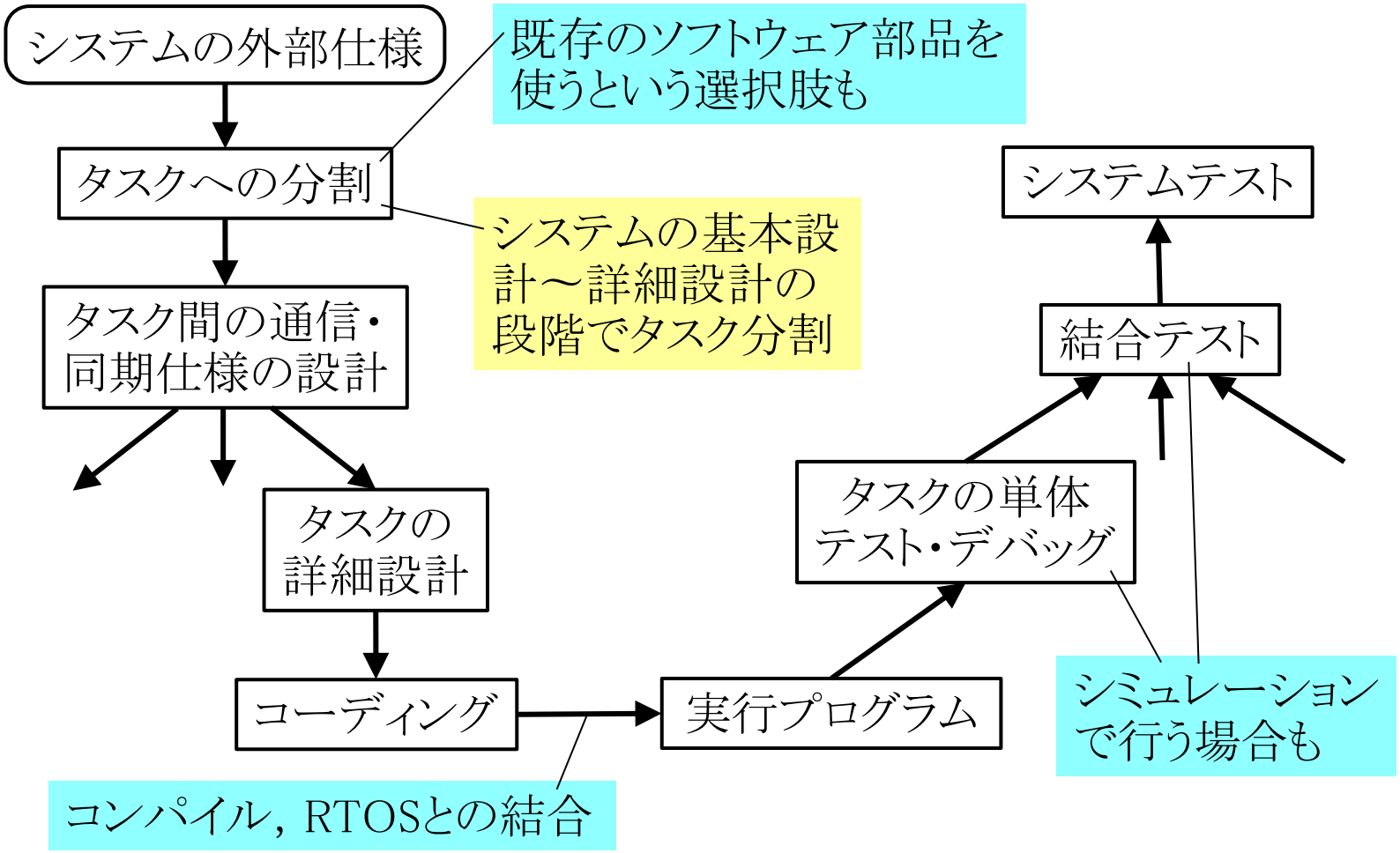
  → RTOSに対応したツールの利用でかなり改善できる

  ! RTOSの原理・内部構造を知るべき

RTOSを用いたシステム設計の指針

リアルタイムOSを用いたソフトウェア開発の流れ

典型的な開発フロー（要求分析工程は除く）



タスクへの分割指針

タスクへの分割

- どのようなアプリケーションにも適用できる一般的な手法は存在しない
- 次のような要因を考慮に入れて決定すべき
  - アプリケーションの機能と性能要件
  - ソフトウェア部品として外部から導入する部分
  - ソフトウェアの開発体制

リアルタイム性向上のための分割指針

- ! 論理的な処理順序と時間的な処理順序の分離により，時間制約を持ったプログラムの保守性が向上
- デッドラインの異なる処理は別タスクに
- （過負荷になる場合）重要度の異なる処理は別タスクに

モジュール化のための分割指針

! ソフトウェアの構造化・開発容易化のための分割

- 異なる機能モジュールや異なるデバイスの操作は別タスクに
- 異なる種類の処理は別タスクに
  - I/Oタスクと内部処理タスクに分割
  - システムの監視・保守・診断の処理を別タスクに
  - 例外時・故障時の処理を別タスクにする方法もある（別タスクにしない方法もある）
- 再利用しやすい単位は単独のタスクに
- まとまった処理単位は同一タスク内に
  - 一つの状態遷移／一つの結果を出す処理／データの流れが綴じた処理は同一タスク内で
  - 状態（モード）毎に別タスクにする方法もある

モジュール化のための分割指針 – 続き

- 同一処理を複数並行して行いたい場合
  - 同一のプログラムを共有して，複数のタスクを動作させる方法
  - データで切り分ける方法もある
- 開発者／グループ毎にタスクを分割する
- 起動イベント／起動タイミングの異なる処理
  - 起動イベント／タイミング毎にタスクを分ける方法
  - 起動周期毎にタスクを分ける方法は一般的
  - 起動イベント／タイミングが異なっていても，まとまった処理単位は同一タスクとする方法も

設計上の留意点

- 分割しすぎはオーバヘッドの増大につながるので注意

タスクの優先度の決定

優先度の決め方

- 時間制約を満たせる範囲では,

  急ぐタスク(デッドラインの短いタスク)を優先

- 一時的な過負荷時に時間制約を満たせない場合には,

  重要なタスク(時間制約を満たせなかった場合の被害が大きいタスク)を優先

時間制約を満たせるかをどう判断するか？

- リアルタイムスケジューリング理論を適用する

一時的な過負荷時にはどうするか？

- 重要性の低いタスクをさぼる／精度を落とす

  QoS (Quality of Service) 制御

- それがダメなら高性能なハードウェアを用いるしかない

タスク間通信・同期の設計

共有メモリ vs. メッセージ通信

- 基本的には，一方で実現できることは，もう片方でも実現できる
  - 一般的には，共有メモリの方がオーバヘッドが小さい
  - システム検証には，通信の粒度が大きく，RTOSレベルで監視できるメッセージ通信の方が扱いやすい

    → 例えば，問題の切り分けが容易
- 状況により，どちらかが有利／便利な状況がある
  - 情報の流れが 1:n の場合（ブロードキャストを含む）や，情報が必要なタイミングが不定の場合には，共有メモリが有利
  - 情報のキューイングが必要な場合には，メッセージ通信機能が便利

設計上の留意事項

- 両方式を混在させて使うと，システム設計が複雑になって，見通しが悪くなる可能性がある
- セマフォ／ミューテックスによる排他制御では，デッドロックと優先度逆転に関して注意が必要
- メッセージ通信によりサーバタスクに処理依頼する場合にも，優先度逆転の問題が起こりうる

デッドロック（deadline）

- 2つのタスクが，互いに相手の処理が進むのを待つ状態．3つ以上のタスク間でも発生
  - 典型的には，2つ以上のセマフォ／ミューテックスを，タスクによって異なる順序でロックする場合に発生
  - ロックする順序を決めれば解決（常にできるとは鍵らない）

テスト (検証) とデバッグ

タスク／割込みハンドラの単体テスト

- 当該タスク／割込みハンドラを含んだ最小構成でリンク
- 他のタスクの振舞いはシミュレーションで
- タスク／割込ハンドラの処理時間，スタック使用量などを評価する

など

複数タスクの結合テスト

- シミュレーションされているタスクを，単体テスト済みのタスクに入れ換えていく
- タスク間のインタフェースの確認
- 資源の競合テスト（排他制御が正しいか？）

など

TOPPERS/ASP3カーネル・HRP3カーネルの機能とAPI

TOPPERSにおけるリアルタイムカーネル開発の流れ

! 高信頼性・安全性・リアルタイム性を追求

第１世代のリアルタイムカーネル

- μITRON4.0仕様準拠＋αのリアルタイムカーネル
  - TOPPERS/JSP, FI4, FDMP, HRP
- OSEK/VDX OS仕様準拠のリアルタイムカーネル
  - TOPPERS/ATK1

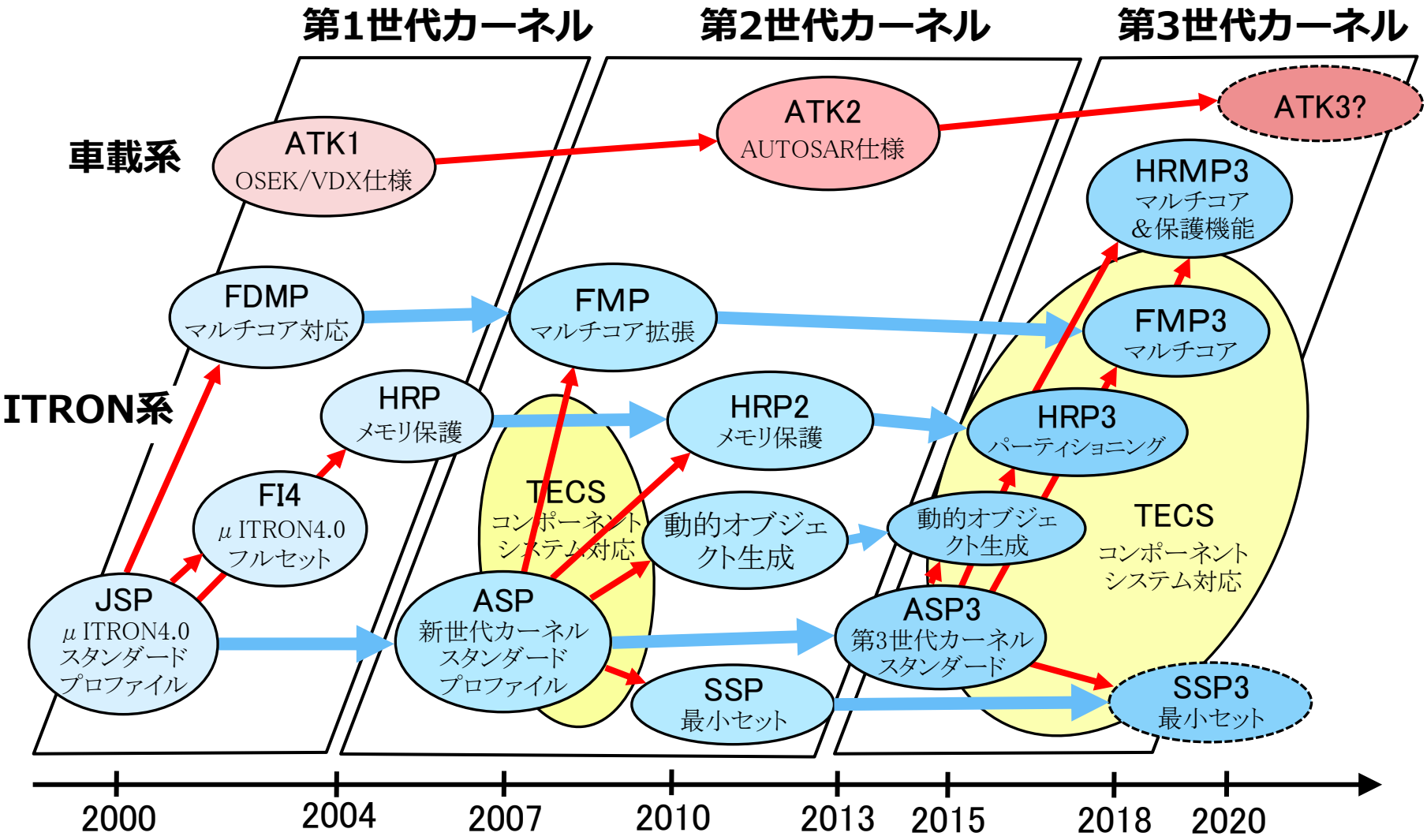
第２世代のリアルタイムカーネル

- TOPPERS新世代カーネル（ITRON仕様からの発展）
  - TOPPERS/ASP, FMP, HRP2, SSP
- AUTOSAR OS仕様ベースのリアルタイムカーネル
  - TOPPERS/ATK2（SC1, SC3, SC1-MC, SC3-MC, …）

第３世代のリアルタイムカーネル

- TOPPERS第3世代カーネル（ITRON系）
  - TOPPERS/ASP3, HRP3, FMP3, HRMP3, …

TOPPERSカーネル開発ロードマップ



第3世代カーネル (ITRON系) の仕様策定方針

基本的な設計方針 … *第2世代を踏襲*

- μITRON4.0仕様をベースに拡張・改良を加える
- ソフトウェアの再利用性を重視する
- 高信頼・安全なシステム構築を支援する
- アプリケーションシステム構築に必要な機能は積極的に取り込む

特に留意した設計方針（これまでも暗黙に存在）

- システム／アプリケーションによって要求が異なる機能は，ミドルウェア等で実現することとし，カーネルにはその実現に必要な最低限の機能を導入する
  - ポリシーとメカニズムの分離の考え方
- 実装方法を合わせて検討し，オーバヘッドの大きい仕様を避ける

第2世代から第3世代への主な仕様変更点

(1)時間パーティショニング機能の導入

- 機能安全におけるソフトウェアパーティショニングの実現を容易にするための機能

(2)ティックレスの高分解能時間管理と外部時刻同期

- カーネルが管理する時間の分解能をミリ秒からマイクロ秒に変更
  - タイムティックを使わない実装に変更
- 外部時刻との同期のための機能を導入

(3)マルチコアにおける動的負荷分散機能への対応

- マルチコアプロセッサにおけるロードバランシングを実現するために以下の機能を導入
  - タスクとスケジューリング状態の参照機能
  - サブ優先度機能

(4)仕様のスリム化・シンプル化(主なもの)

- タスク例外処理機能の廃止とタスク終了要求機能の導入
  - 必要性が低いにもかかわらず，ターゲット依存部(特に保護機能対応の場合)の実装負担が大きいタスク例外処理機能と待ち禁止状態を廃止
- 非タスクコンテキスト専用のサービスコールの廃止
- メールボックス機能の廃止
  - 保護機能対応では不適切な機能(サポートしていない)

(5)ミューテックスの標準機能化

(6)その他の改良(主なもの)

- タイムイベント処理機能の見直し
- 起動要求をキューイングしないタスクの追加
- 保護ドメインに対するアクセス許可ベクタの新設
- 保護ドメイン毎の標準メモリリージョン

第3世代カーネル (ITRON系) の実装

! カーネルのバージョン番号を「3」に統一

TOPPERS/ASP3カーネル 公開済み

- TOPPERS第3世代カーネルの出発点

TOPPERS/HRP3カーネル 公開済み

- ASP3カーネルにパーティショニング機能（メモリ保護，時間パーティショニングなど）を追加したもの

TOPPERS/FMP3カーネル 公開済み

- ASP3カーネルをマルチコアプロセッサ向けに拡張

TOPPERS/HRMP3カーネル 公開済み

- HRP3カーネルをマルチプロセッサ向けに拡張したもの or FMP3カーネルにパーティショニング機能を追加したもの

TOPPERS/SSP3カーネル 早期リリース中

- ASP3カーネルをベースに機能を絞り込む

TOPPERS/ASP3カーネルの概要

ASP3カーネルの位置付け

- TOPPERS第3世代カーネルの出発点
- TOPPERS/ASPカーネルを拡張・改良したもの

ASPカーネルに追加した機能（基本パッケージでサポート）

- タスク終了要求機能
- ティックレスの高分解能時間管理，システム時刻の調整機能，システム時刻の参照／設定機能
- ミューテックス機能 … 基本機能に格上げ
- 周期通知／アラーム通知機能 … 周期ハンドラ／アラームハンドラ機能を拡張

ASPカーネルから削除した機能

- タスク例外処理機能
- メールボックス機能

周辺ツールの活用・変更

- TECSの活用
  - システムサービス(システムログ機能など)とデバイスドライバの構築にTECSを活用
  - カーネルを利用するだけであれば，TECSを勉強する必要はない
- Ruby版コンフィギュレータの適用

拡張パッケージでサポート

- ドリフト調整機能
- メッセージバッファ機能
- オーバランハンドラ機能
- タスク優先度拡張
- 制約タスク
- サブ優先度機能
- 動的生成機能

TOPPERS/HRP3カーネルの概要

HRP3カーネルの位置付け

- 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
  - 自動メモリ配置（HRP2カーネルと同様）と手動メモリ配置（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
- 拡張サービスコール機能
- メッセージバッファ機能（ASP3では拡張パッケージ）

HRP2カーネルに対する追加／削除機能

- ASPカーネルからASP3カーネルで追加／削除した機能
- 〔追加〕時間パーティショニング機能
- 〔追加〕手動メモリ配置
- 〔削除〕待ち禁止状態とそれを操作する機能
- 〔削除〕オーバランハンドラ機能（拡張パッケージに）

周辺ツールの活用・変更

- TECSの活用
  - ASP3カーネルと同一のシステムサービス（システムログ機能など）とデバイスドライバを利用可能
- Ruby版コンフィギュレータの適用

拡張パッケージでサポート

- オーバランハンドラ機能
- 動的生成機能

TOPPERS第3世代カーネル (ITRON系) 統合仕様書

- TOPPERS第3世代カーネルに属する一連のリアルタイムカーネルの仕様を，統合的に記述した仕様書
- 以下のURLからダウンロード可能
  - http://www.toppers.jp/documents.html

TOPPERS第3世代カーネル（ITRON系）統合仕様書の構成

第1章 TOPPERS第3世代カーネル（ITRON系）の概要

第2章 主要な概念と共通定義

- 複数の機能単位にまたがる概念や共通の定義

第3章 システムインタフェースレイヤAPI仕様

- システムコールインタフェースレイヤ（SIL）のAPI仕様

第4章 カーネルAPI仕様

- カーネルのサービスコールと静的APIのAPI仕様

第5章 リファレンス

第2章 主要な概念と共通定義

2.1 仕様の位置付け
2.2 APIの構成要素とコンベンション
2.3 主な概念
2.4 処理単位の種類と実行
2.5 システム状態とコンテキスト
2.6 タスクの状態遷移とスケジューリング規則
2.7 割込み処理モデル
2.8 CPU例外処理モデル
2.9 システムの初期化と終了
2.10 オブジェクトの登録とその解除
2.11 オブジェクトのアクセス保護
2.12 システムコンフィギュレーション手順
2.13 TOPPERSネーミングコンベンション
2.14 TOPPERS共通定義
2.15 カーネル共通定義

第4章 カーネルAPI仕様

4.1 タスク管理機能
4.2 タスク付属同期機能
4.3 タスク終了機能
4.4 同期・通信機能
4.5 メモリプール管理機能
4.6 時間管理機能
4.7 システム状態管理機能
4.8 メモリオブジェクト管理機能
4.9 割込み管理機能
4.10 CPU例外管理機能
4.11 拡張サービスコール管理機能
4.12 保護ドメイン管理機能
4.13 システム構成管理機能

TOPPERS/ASP3カーネルの仕様の読み取り方

ASP3カーネルがサポートする機能セット

- ASP3カーネルは,「保護機能対応カーネル」,「マルチプロセッサ対応カーネル」,「動的生成対応カーネル」のいずれでもない
  - よって,「保護機能対応カーネルでは」,「マルチプロセッサ対応カーネルでは」,「動的生成対応カーネルでは」で始まる記述は適用さない
- ただし, 動的生成機能拡張パッケージを用いると, 動的生成対応カーネルの機能の一部をサポートし,「動的生成対応カーネルでは」で始まる記述の一部は適用される
- 【TOPPERS/ASP3カーネルにおける規定】の項に書かれていることは,（文字通り）適用される
  - 動的生成機能拡張パッケージを用いた場合のことも, この項の中に書かれている

APIのサポート種別の記号（抜粋）

- 〔P〕〔M〕〔D〕は，それぞれ，保護機能対応カーネル，マルチプロセッサ対応カーネル，動的生成対応カーネルのみでサポートされるAPI
- 〔T〕はタスクコンテキスト専用のサービスコール
- 〔TI〕はタスクコンテキストからも非タスクコンテキストからも呼び出すことのできるサービスコール

APIのサポート種別の記号の実際の例

- act_tsk〔TI〕… ASP3カーネルでサポートされる
- mact_tsk〔TIM〕… ASP3カーネルでサポートされない
- ref_tsk〔T〕… ASP3カーネルでサポートされる
- acre_tsk〔TD〕… ASP3カーネルでサポートされない．ただし，動的生成機能拡張パッケージを用いると，サポートされる場合も（個別に記述）

TOPPERS/HRP3カーネルの仕様の読み取り方

HRP3カーネルがサポートする機能セット

- HRP3カーネルは,「保護機能対応カーネル」であり,「マルチプロセッサ対応カーネル」,「動的生成対応カーネル」ではない
  - よって,「保護機能対応カーネルでは」で始まる記述は(基本的には)適用され,「マルチプロセッサ対応カーネルでは」「動的生成対応カーネルでは」で始まる記述は適用さない
- ただし, 動的生成機能拡張パッケージを用いると(EV3RTは用いている), 動的生成対応カーネルの機能の一部をサポートし,「動的生成対応カーネルでは」で始まる記述の一部は適用される
- 【TOPPERS/HRP3カーネルにおける規定】の項に書かれていることは,(文字通り)適用される

APIのサポート種別の記号（抜粋）

- 〔P〕は保護機能対応カーネルのみでサポートされるAPI
- 〔M〕〔D〕は，それぞれ，マルチプロセッサ対応カーネル，動的生成対応カーネルのみでサポートされるAPI
- 〔T〕はタスクコンテキスト専用のサービスコール
- 〔TI〕はタスクコンテキストからも非タスクコンテキストからも呼び出すことのできるサービスコール

APIのサポート種別の記号の実際の例

- act_tsk〔TI〕… HRP3カーネルでサポートされる
- prb_mem〔TP〕… HRP3カーネルでサポートされる
- mact_tsk〔TIM〕… HRP3カーネルでサポートされない
- acre_tsk〔TD〕… HRP3カーネルでサポートされない．ただし，動的生成機能拡張パッケージを用いると，サポートされる場合も（個別に記述）

基本的な用語

オブジェクト(カーネルオブジェクト)

- カーネルが管理対象とするソフトウェア資源
- 種類毎に，番号によって識別する

処理単位

- 対応するプログラムを持つオブジェクト(または，そのオブジェクトに対応付けられたプログラム)
- プログラムは，アプリケーションで用意し，カーネルが実行制御する

タスク

- カーネルが実行制御するプログラムの並行実行の単位
- 処理単位の一種

自タスク

- サービスコールを呼び出したタスク

ディスパッチ（タスクディスパッチ）

- プロセッサが実行するタスクを切り換えること

ディスパッチの保留

- ディスパッチが起こるべき状態となっても，何らかの理由でディスパッチを行わないこと
- その理由が解除された時点で，ディスパッチが起こる

スケジューリング（タスクスケジューリング）

- 次に実行すべきタスクを決定する処理

優先順位

- 処理単位の実行順序を説明するための仕様上の概念
- 処理単位は，優先順位の高い順に実行される

優先度

- 処理単位の優先順位やメッセージの配送順序などを決定するために，アプリケーションが与えるパラメータ

割込み（外部割込み）

- プロセッサが実行中の命令とは独立に発生するイベントによって起動される例外処理

割込みのマスク（禁止）

- 周辺デバイスからの割込み要求をプロセッサに伝える経路を遮断し，割込み要求が受け付けられるのを抑止すること
- マスクが解除された時点で,まだ割込み要求が保持されていれば，その時点で割込み要求を受け付ける

NMI（Non-Maskable Interrupt）

- マスクすることができない割込み

CPU例外

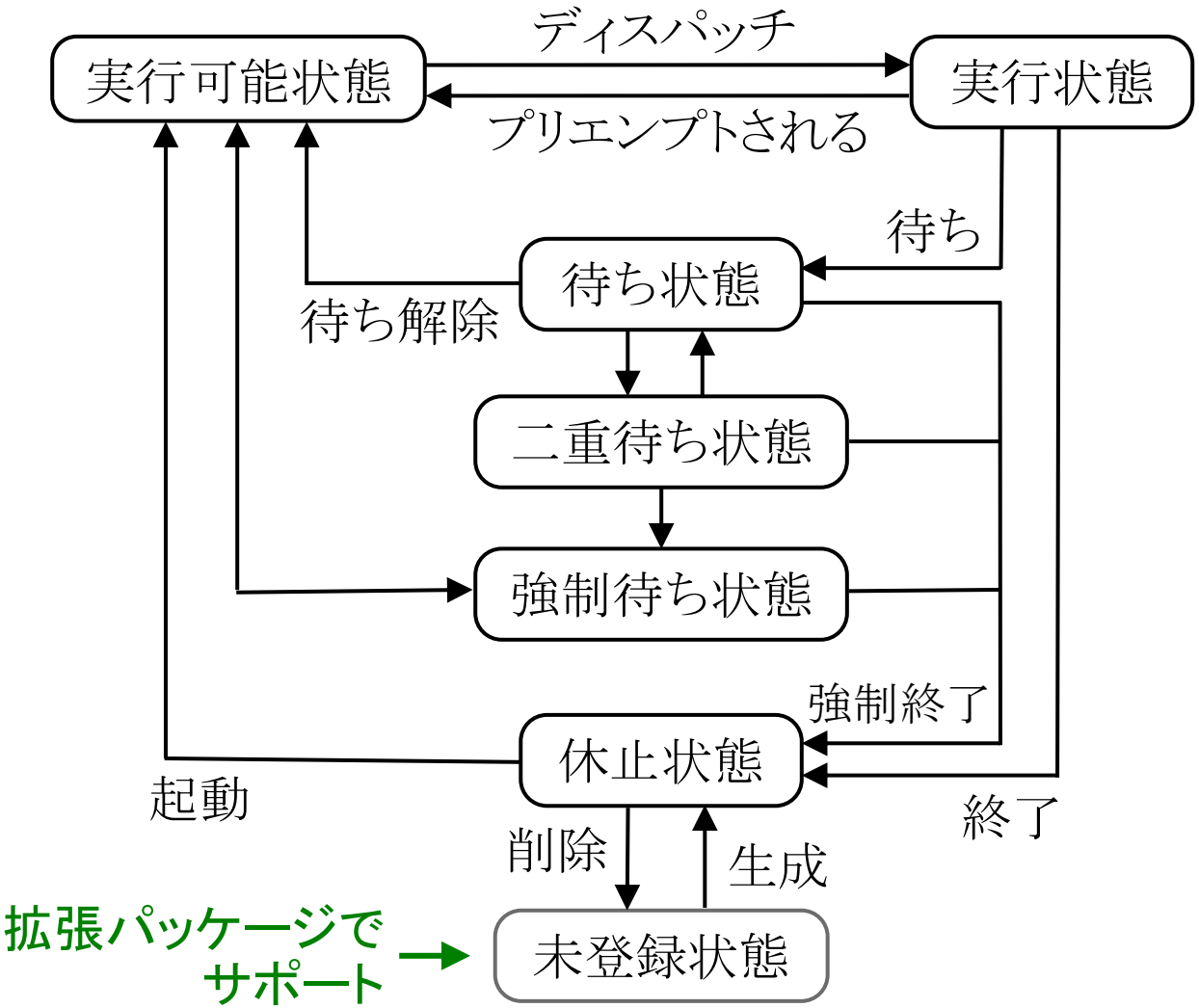
- プロセッサが実行中の命令に依存して起動される例外処理

タスクの状態遷移とスケジューリング規則

タスク状態

- 実行できる状態（runnable）
  - 実行状態（running）
  - 実行可能状態（ready）
- 休止状態（dormant）
- 広義の待ち状態（blocked）
  - （狭義の）待ち状態（waiting）
    … タスクが自ら実行を止めている状態
  - 強制待ち状態（suspended）
    … タスクが他のタスクによって実行を止められた状態
  - 二重待ち状態（waiting-suspended）
- 未登録状態（non-existent）← 拡張パッケージでサポート

タスクの状態遷移(一部省略)



- ディスパッチ
- プリエンプト
- 起動
- 終了
- 強制終了
- 待ち
- 待ち解除
- 強制待ち
- 強制待ちからの再開
- 生成
- 削除

タスクのスケジューリング規則

- タスクに与えられた優先度に基づくプリエンプティブな優先度ベーススケジューリング
- 同優先度のタスクは，先に実行できる状態（実行状態または実行可能状態）になったタスクを先に実行するFCFS（First Come First Served）方式でスケジューリング
  - プリエンプトされても，実行順序は後回しにならない
  - 待ち状態になったタスクの実行順序は最後になる
- 優先度割付けは静的が基本だが，優先度を動的に変更する機能も用意
- 同優先度のタスク内での優先順位を変更する機能を用意
  - これを用いて，同優先度内でのラウンドロビンスケジューリングも実現可能
- ASP3/HRP3カーネルでは，優先度は16段階

処理単位と優先順位

処理単位の種類

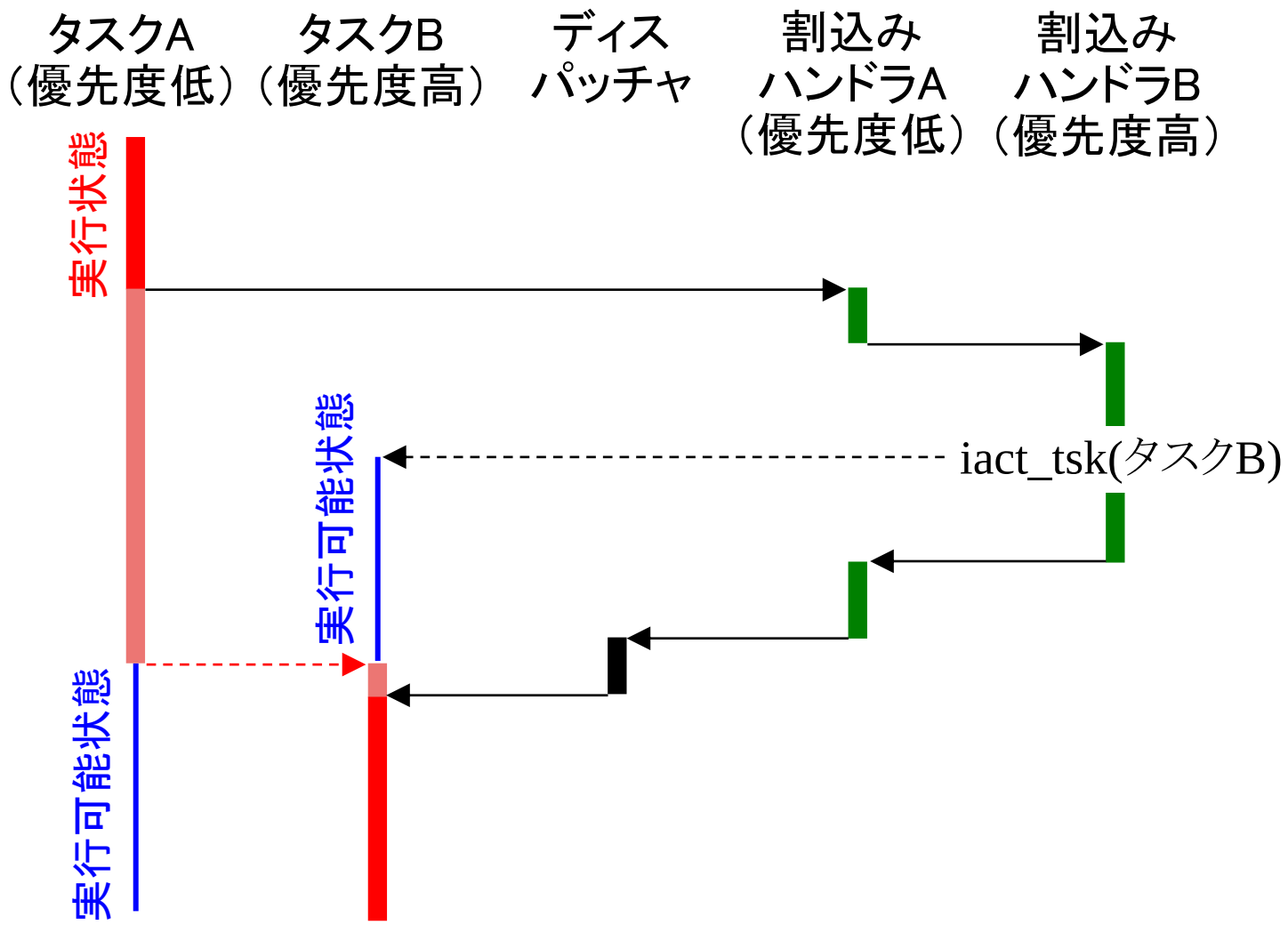
- タスク
- 割込みハンドラ
  - 割込みサービスルーチン（ISR）
  - タイムイベントハンドラ
    - 周期ハンドラ
    - アラームハンドラ
    - オーバランハンドラ ← 拡張パッケージでサポート
- CPU例外ハンドラ
- 拡張サービスコール ← ASP3のサポート外
- 初期化ルーチン
- 終了処理ルーチン

処理単位の優先順位

- 次の順序で優先順位が高い
  - 割込みハンドラ（ISR, タイムイベントハンドラを含む）
  - ディスパッチャ
  - タスク
- 割込みハンドラの優先順位はディスパッチャよりも高いことから，割込みハンドラが動いている間は，タスク切換えは起こらない

  → 遅延ディスパッチの原則
- CPU例外ハンドラの優先順位
  - CPU例外がタスクで発生した場合には，ディスパッチャと同じ優先順位で，ディスパッチャより先に実行
  - その他の処理単位で発生した場合には，その処理単位と同じ優先順位で，その処理単位より先に実行

タスク切換えの遅延（遅延ディスパッチの原則）



システム状態とコンテキスト

タスクコンテキスト

- タスクの一部と見なすことのできるコンテキストの総称
  - タスク
  - タスクコンテキストから呼び出した拡張サービスコール
- 「自タスク」が定義される
  - 自タスクを広義の待ち状態にする可能性のあるサービスコールが呼び出せる

非タスクコンテキスト

- タスクコンテキストに含まれないコンテキストの総称
  - 割込みハンドラ（ISR, タイムイベントハンドラを含む）
  - CPU例外ハンドラ
  - 非タスクコンテキストから呼び出した拡張サービスコール

CPUロック状態

- すべてのカーネル管理の割込みとディスパッチを禁止している状態（カーネル管理外の割込みは禁止しない）
- 呼び出せるサービスコールが限られている

ディスパッチ禁止状態

- ディスパッチを禁止している状態
- 自タスクを広義の待ち状態にする可能性のあるサービスコールは呼び出せない

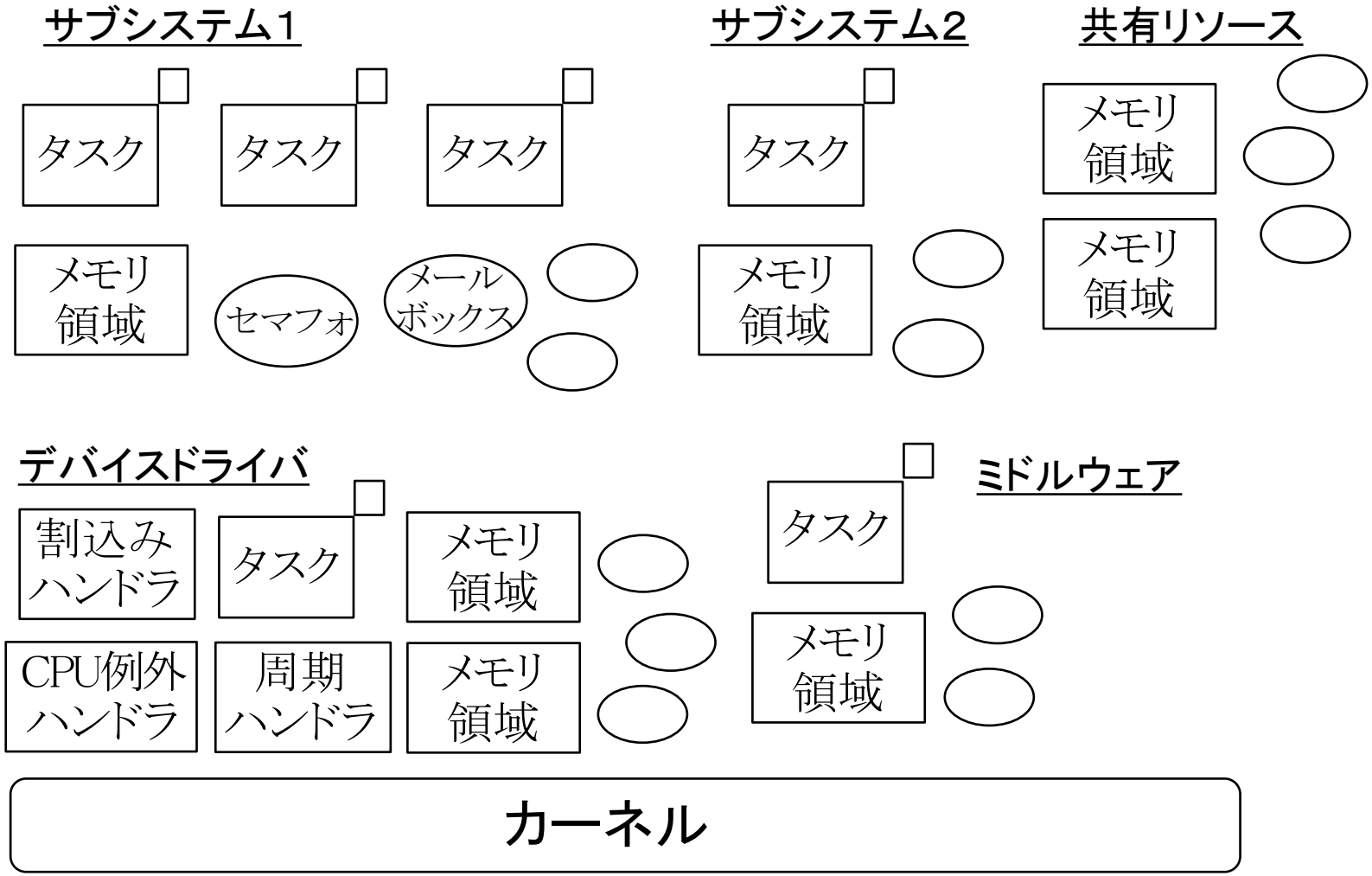
割込み優先度マスク

- 割込み優先度を基準に割込みをマスクするための機構
- 全解除でない時は，ディスパッチは起こらない

ディスパッチ保留状態

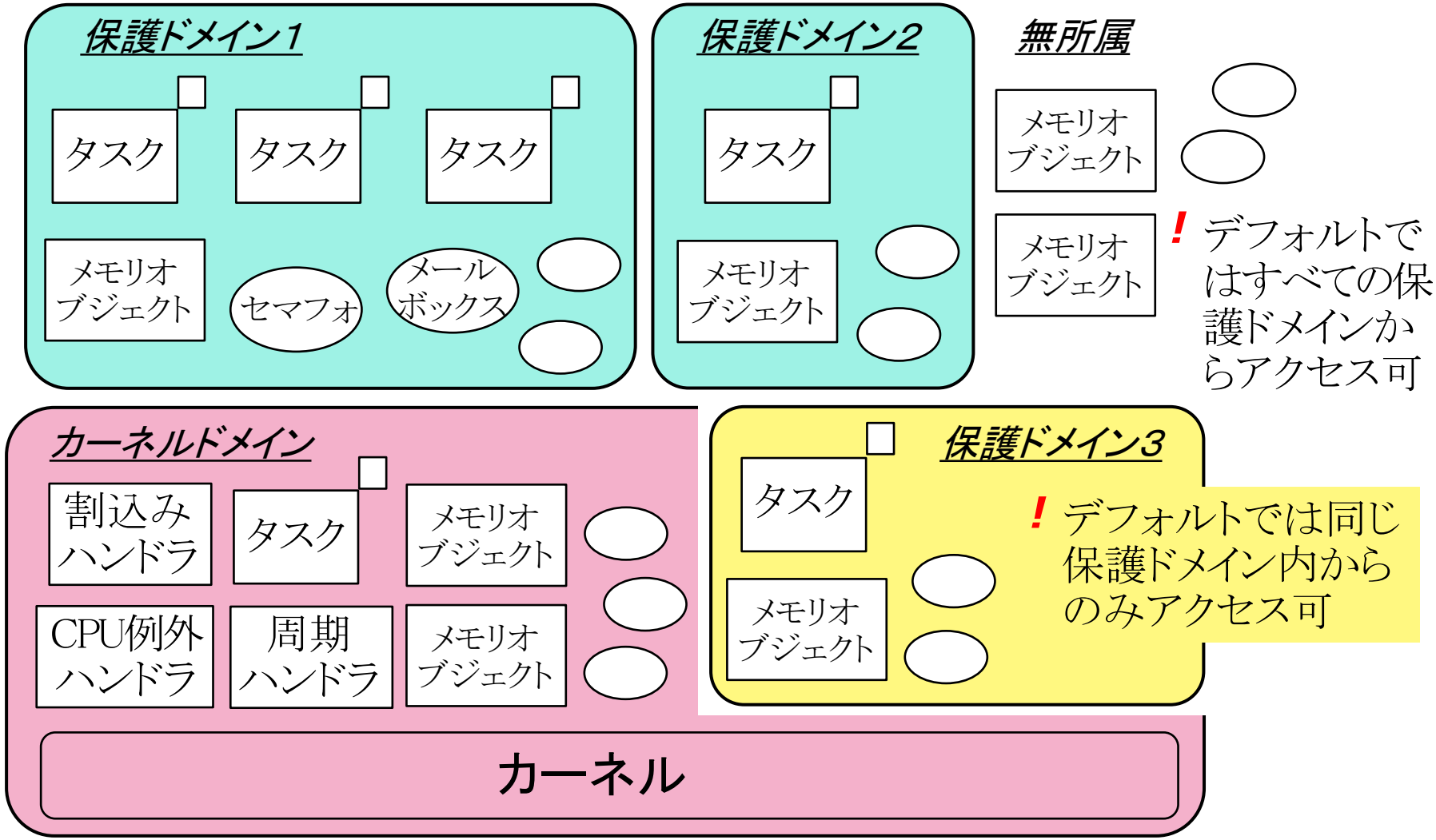
- 何らかの理由でディスパッチが起こらない状態（ディスパッチが起こらない状態の総称）

保護機能の導入イメージ (導入前)



保護機能の導入イメージ (導入後)

! 囲みに穴をあける機能も持つ



保護機能に関する主な概念

アクセス保護

- 処理単位（タスクと考えてよい）が，許可されたカーネルオブジェクトに対して，許可された種別のアクセスを行うことのみを許し，それ以外のアクセスを防ぐ機能
- アクセス制御の用語では，
  - 処理単位 ＝ 主体（subject）
  - カーネルオブジェクト ＝ 対象（object）

メモリオブジェクト（memory object）

- アクセス保護の対象とする連続したメモリ領域で，カーネルオブジェクトの一種
- 互いに重なりあうことはない
- 先頭番地によって識別（先頭番地がオブジェクト番号）
- 先頭番地とサイズにターゲット定義の制約が課せられる

保護ドメイン（protection domain）

- 保護機能を提供するためのカーネルオブジェクトの集合
- 保護ドメインIDによって識別する
- 処理単位は，いずれか1つの保護ドメインに属する
- 他のカーネルオブジェクトは，いずれか1つの保護ドメインに属するか，いずれの保護ドメインにも属さない（無所属のカーネルオブジェクト）

保護ドメインによるアクセス保護

- 処理単位がカーネルオブジェクトにアクセスできるかどうかは，処理単位が属する保護ドメインにより決まるのが原則
- ただし，タスクのユーザスタック領域は，そのタスクのみがアクセスできる
- デフォルトでは，処理単位は，同じ保護ドメインに属するカーネルオブジェクトと，無所属のカーネルオブジェクトのみにアクセスできる

カーネルドメイン（kernel domain）

- システムに1つ存在
- カーネルドメインに属する処理単位は，
  - プロセッサの特権モードで実行される
  - すべてのカーネルオブジェクトに対して，すべての種別のアクセスを行える

ユーザドメイン（user domain）

- ユーザドメインに属する処理単位は，
  - プロセッサの非特権モードで実行される
  - どのカーネルオブジェクトに対してどの種別のアクセスを行えるかを制限できる
- 登録できるユーザドメインの最大数は32

システムタスク（system task）

- カーネルドメインに属するタスク

ユーザタスク（user task）

- ユーザドメインに属するタスク

アクセス許可パターン（access permission pattern）

- アクセスが許可されている保護ドメインの集合を表現するビットパターン（各ビットが1つのユーザドメインに対応）
- ACPTN型（符号無し32ビット整数）で保持
- 以下のマクロと定数を用意
  - TACP(domid) … domid（とカーネルドメイン）のみアクセス可能
  - TACP_KERNEL … カーネルドメインのみアクセス可能
  - TACP_SHARED … すべての保護ドメインからアクセス可能

アクセス許可ベクタ(access permission vector)

- あるカーネルオブジェクトに対する4つの種別のアクセスに関するアクセス許可パターンをひとまとめにしたもの
  - カーネルオブジェクトに対するアクセスは，カーネルオブジェクトの種類毎に，通常操作1，通常操作2，管理操作，参照操作の4つの種別に分類(次のスライド参照)
- 次のように定義されるACVCT型で保持

```
typedef struct acvct {
        ACPTN   acptn1;    /* 通常操作1のアクセス許可パターン
*/
        ACPTN   acptn2;    /* 通常操作2のアクセス許可パターン
*/
        ACPTN   acptn3;    /* 管理操作のアクセス許可パターン
*/
        ACPTN   acptn4;    /* 参照操作のアクセス許可パターン
*/
} ACVCT;
```

カーネルオブジェクトに対するアクセスの種別（抜粋）

	通常操作1	通常操作2	管理操作	参照操作
メモリオブジェクト	書込み	読出し 実行	det_mem sac_mem	ref_mem prb_mem
タスク	act_tsk can_act wup_tsk can_wup …	ter_tsk chg_pri rel_wai sus_tsk ras_tex …	del_tsk sac_tsk def_tex	get_pri ref_tsk ref_tex ref_ovr
セマフォ	sig_sem	wai_sem pol_sel twai_sem	del_sem ini_sem sac_sem	ref_sem
周期ハンドラ	sta_cyc …	stp_cyc	del_cyc sac_cyc	ref_cyc
システム状態	rot_rdq …	loc_cpu …	def_inh …	get_tim …

サービスコール

- 上位階層のソフトウェア（例：アプリケーション）から，下位階層のソフトウェア（例：カーネル，システムサービス）を呼び出すインタフェース

サービスコールの名称

- カーネルのサービスコールは，*xxx_yyy*の形を基本とする

  例）act_tsk

  操作対象を表す．この場合はタスク（task）

  操作方法を表す．この場合は起動（activate）

- *xxx_yyy*から派生したサービスコールは，*zxxx_yyy*の形とする（*z*は，派生したことを表す文字）

  例）slp_tskとtslp_tsk

  タイムアウト付きのサービスであることを表す

サービスコールの例（抜粋）

act_tsk　　タスクの起動〔TI〕

【C言語API】

ER ercd = act_tsk (ID tskid) ;

【パラメータ】

ID　　tskid　対象タスクのID番号

【リターンパラメータ】

ER　　ercd　正常終了（E_OK）またはエラーコード

【エラーコード】

E_CTX　　コンテキストエラー（CPUロック状態からの呼出し）

E_ID　　不正ID番号（tskidが不正）

E_QOVR　　キューイングオーバフロー（……）

【機能】

tskidで指定したタスク（対象タスク）に対して起動要求を行う．
具体的な振舞いは以下の通り．（以下略）

静的API

- オブジェクトの生成情報や初期状態などを定義するために，システムコンフィギュレーションファイル中に記述するためのインタフェース

静的APIの文法とパラメータ

- C言語の関数呼出しと同様の文法で記述．ただし構造体（へのポインタ）は，各フィールドの値を { } で囲んで列挙
- サービスコールと同等の機能を持つ静的APIは，サービスコール名を大文字にした名称とし，パラメータも同一とする
  → サービスコールと静的APIを個別に覚える必要がなくなる
- 静的APIのパラメータは何が記述できるかで4種類に分類
  - 一部のパラメータを除いて，式を記述することができる

静的APIの例

```
CRE_TSK( ID tskid, { ATR tskatr, intptr_t exinf,
        TASK task, PRI itskpri, SIZE stksz, STK_T stk } );
```

対応するサービスコール

```
ER_ID tskid = acre_tsk ( T_CTSK *pk_ctsk ) ;
```

静的APIの記述例

```
CRE_TSK( TASK1, { TA_ACT, 0,
        task_main, 10, STACK_SIZE, NULL } );
```

別のヘッダファイルで
値を定義しておく

コンフィギュレータが
スタック領域を割り付ける

コンフィギュレータがタスクIDを割り付ける

オブジェクトが所属する保護ドメインの指定

- オブジェクトを登録する静的APIを，オブジェクトを属させる保護ドメインの囲みの中に記述
- 無所属のオブジェクトを登録する静的APIは，保護ドメインの囲みの外に記述

例）

TASK_AとSEM_Aは DOM_Aに属する

SEM_Aのアクセス許可ベクタを設定

```
DOMAIN (DOM_A) {
        CRE_TSK(TASK_A, { TA_NULL, 1, taskA_main, … });
        CRE_SEM(SEM_A, { TA_NULL, 1, 1 });
        SAC_SEM(SEM_A, { TA_DOM(DOM_A), TA_SHARED,
                                TA_KERNEL, TA_SHARED });
}
KERNEL_DOMAIN {
        CRE_TSK(TASK_K, { TA_ACT, 0, taskK_main, … });
}
CRE_SEM(SEM_S, { TA_TPRI, 1, 1 });
```

TASK_Kはカーネルドメインに属する

SEM_Sは無所属

システムコンフィギュレーションファイルの記述例

```
DOMAIN (DOM_A) {
        CRE_TSK(TASK_A, { TA_[illegible], 1, taskA_main, … });
        CRE_SEM(SEM_A, { TA_NULL, 1, 1 });
        ATT_MOD("obj_a1.o");
        ATA_MOD("obj_a2.o", { TA_DOM(DOM_A), TA_SHARED,
                                TA_KERNEL, TA_SHARED });
}
KERNEL_DOMAIN {
        CRE_TSK(TASK_K, { TA_ACT, 0, taskK_main, … });
        ATT_ISR({ TA_NULL, 1, INTNO_SIO1, sio_isr, 1 });
        ATT_MOD("obj_k.o");
}
CRE_SEM(SEM_S, { TA_TPRI, 1, 1 });
ATT_MOD("shared_lib.a");
```

obj_a1.oは，DOM_Aの専有領域に配置

obj_a2.oは，DOM_Aの専有ライト共有リード領域に配置

obj_k.oは，カーネルドメインの専有領域に配置

shared_lib.aは，共有領域に配置

コンフィギュレーション手順

コンフィギュレーションの流れ

appl.cfg

システムコンフィギュレーションファイル

```
#include “appl.h”
CRE_TSK(TASK1, { TA_ACT, …
CRE_SEM(SEM1, { TA_TPRI, …
```

コンフィギュレータ

内部的には複雑なステップ

kernel_cfg.c

カーネル構成・初期化ファイル

kernel_cfg.h

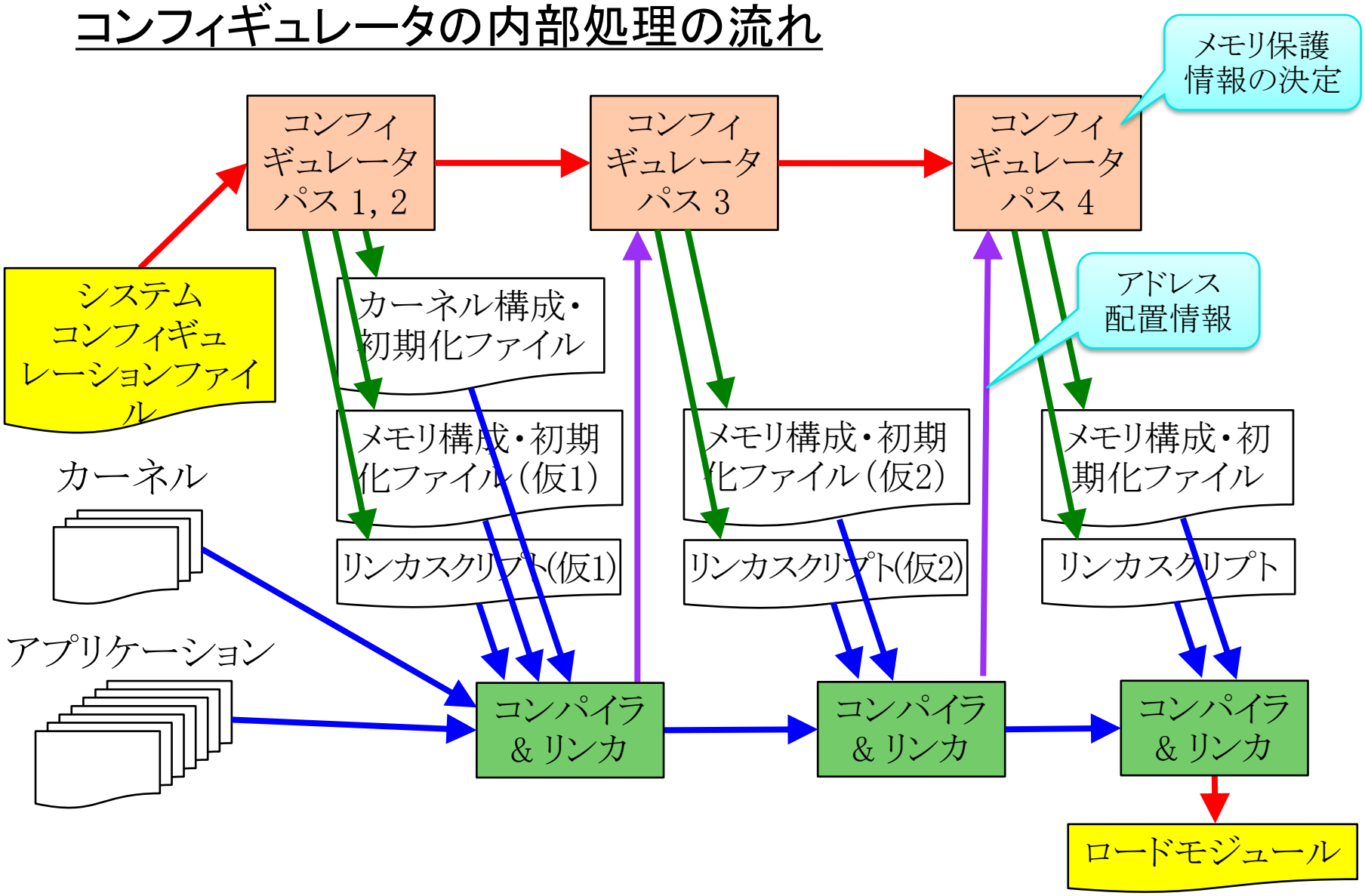
カーネル構成・初期化ヘッダファイル

```
#define   TASK1   2
#define   SEM1    5
```

kernel_mem.c

メモリ構成・初期化ファイル

コンフィギュレータの内部処理の流れ



TOPPER第3世代カーネルの機能リスト

- タスク管理機能
- タスク付属同期機能
- タスク終了機能
- 同期・通信機能
  - セマフォ
  - イベントフラグ
  - データキュー
  - 優先度データキュー
  - ミューテックス
  - メッセージバッファ ← ASP3では拡張パッケージでサポート
  - スピンロック ← ASP3/HRP3のサポート外
- メモリプール管理機能
  - 固定長メモリプール

TOPPERS第3世代カーネルの機能リスト – 続き

- 時間管理機能
  - システム時刻管理
  - 周期通知
  - アラーム通知
  - オーバランハンドラ ← 拡張パッケージでサポート
- システム状態管理機能
- メモリオブジェクト管理機能 ← ASP3のサポート外
- 割込み管理機能
- CPU例外管理機能
- 拡張サービスコール管理機能 ← ASP3のサポート外
- 保護ドメイン管理機能 ← ASP3のサポート外
- システム構成管理機能

タスク管理機能

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- タスクの状態を直接的に操作するための機能

タスク管理機能のAPI

CRE_TSK，acre_tsk*	タスクの生成
AID_TSK*	割付け可能なタスクIDの数の指定
SAC_TSK†，sac_tsk†*	タスクのアクセス許可ベクタの設定
del_tsk*	タスクの削除
act_tsk	タスクの起動
can_act	タスク起動要求のキャンセル
get_tst	タスク状態の参照
chg_pri	タスクの優先度の変更
get_pri	タスクの優先度の参照
get_inf	自タスクの拡張情報の参照
ref_tsk	タスクの状態参照

- タスク起動要求のキューイングとその無効化機能を持つ

タスク付属同期機能

- タスクを直接的に操作して同期を実現するための機能

タスク付属同期機能のAPI

slp_tsk, tslp_tsk	起床待ち
wup_tsk	タスクの起床
can_wup	タスク起床要求のキャンセル
rel_wai	強制的な待ち解除
sus_tsk	強制待ち状態への移行
rsm_tsk	強制待ち状態からの再開
dly_tsk	自タスクの遅延

- タスク起床要求のキューイングとその無効化機能を持つ
- タイムアウト付きの起床待ちと自タスクの遅延は，動作は似ているが，どちらが正常系であるかが違う

タスク終了機能

- タスクを終了させるための3種類の機能
  - 自タスクを終了する機能
  - タスクを安全に終了させるためのタスク終了要求機能
  - タスクを強制終了させる機能

タスク終了機能のAPI

ext_tsk	自タスクの終了
ras_ter	タスクの終了要求
dis_ter	タスク終了の禁止
ena_ter	タスク終了の許可
sns_ter	タスク終了禁止状態の参照
ter_tsk	タスクの強制終了

- 終了要求されたタスクは，広義の待ち状態から解除され，以降も広義の待ち状態になることができない

タスク間同期・通信機能

- ASP3/HRP3カーネルでは，タスク間同期・通信のために以下の機能を用意

(主に)共有メモリによる通信のための機能

- セマフォ(排他制御，事象通知)
- イベントフラグ(事象通知)
- ミューテックス(排他制御)

メッセージ通信のための機能

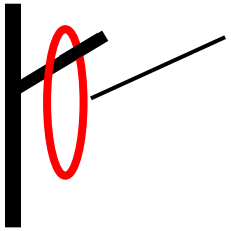
- データキュー(同期・非同期，1ワードのメッセージ)
- 優先度データキュー(同期・非同期，1ワードのメッセージ，優先度順配送)
- メッセージバッファ(同期・非同期，可変長メッセージ)

ASP3では拡張パッケージでサポート

セマフォ機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 使用されていない資源の有無や数量を数値（セマフォの資源数）で管理することにより排他制御を実現
- セマフォは「信号」の意味



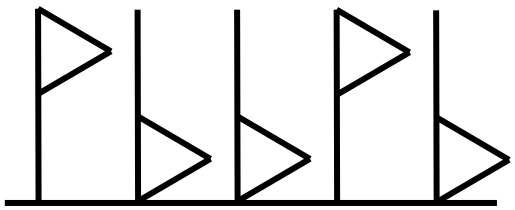
- 列車が単線区間に入る場合には，この輪（これがセマフォ資源と考えるとわかりやすい）を取る
- 一般には輪は複数あっても良い

CRE_SEM，acre_sem*	セマフォの生成
AID_SEM*	割付け可能なセマフォIDの数の指定
SAC_SEM†，sac_sem†*	セマフォのアクセス許可ベクタの設定
del_sem*	セマフォの削除
sig_sem	セマフォ資源の返却
wai_sem，pwai_sem，twai_sem	セマフォ資源の獲得
ini_sem	セマフォの再初期化
ref_sem	セマフォの状態参照

イベントフラグ機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- イベントフラグは，タスク間でイベントの発生を伝えることで同期するための機構．1つのイベントフラグは，複数のフラグで構成



CRE_FLG，acre_flg*	イベントフラグの生成
AID_FLG*	割付け可能なイベントフラグIDの数の指定
SAC_FLG†，sac_flg†*	イベントフラグのアクセス許可ベクタの設定
del_flg*	イベントフラグの削除
set_flg	イベントフラグのセット
cls_flg	イベントフラグのクリア
wai_flg，pol_flg，twai_flg	イベントフラグ待ち
ini_flg	イベントフラグの再初期化
ref_flg	イベントフラグの状態参照

- wai_flgは，指定したフラグのすべてがセットされたか，いずれかがセットされたかの条件で待ち合わせ可能

データキュー機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 1ワードメッセージの非同期メッセージ通信機構
  - リングバッファで実現することを想定
- メッセージは整数としてもポインタとしてもよい
- メッセージが無い/フルの時に待ち合わせる機能
- データキュー領域のサイズを0に設定すると，同期メッセージ通信も実現可能

CRE_DTQ, acre_dtq*	データキューの生成
AID_DTQ*	割付け可能なデータキューIDの数の指定
SAC_DTQ†, sac_dtq†*	データキューのアクセス許可ベクタの設定
del_dtq*	データキューの削除
snd_dtq, psnd_dtq, tsnd_dtq	データキューへの送信
fsnd_dtq	データキューへの強制送信
rcv_dtq, prcv_dtq, trcv_dtq	データキューからの受信
ini_dtq	データキューの再初期化
ref_dtq	データキューの状態参照

優先度データキュー機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 1ワードメッセージの非同期メッセージ通信機構
- データを送信する時に，メッセージの優先度も渡す．メッセージは優先度順にキューイングされる
- データを受信する時に，メッセージの優先度も受け取れる
- メッセージは整数としてもポインタとしてもよい
- メッセージが無い/フルの時に待ち合わせる機能

CRE_PDQ, acre_pdq*	優先度データキューの生成
AID_PDQ*	割付け可能な優先度データキューIDの数の指定
SAC_PDQ†, sac_pdq†*	優先度データキューのアクセス許可ベクタの設定
del_pdq*	優先度データキューの削除
snd_pdq, psnd_pdq, tsnd_pdq	優先度データキューへの送信
rcv_pdq, prcv_pdq, trcv_pdq	優先度データキューからの受信
ini_pdq	優先度データキューの再初期化
ref_pdq	優先度データキューの状態参照

優先度データキュー導入の理由

- μITRON4.0仕様では，メールボックスに送信するメッセージの先頭の領域（数バイト）をカーネルが利用
- アプリケーションが誤ってこの領域を書き換えると，カーネルの中で不具合が発生する
- μITRON4.0仕様 保護機能拡張（PX仕様）では，カーネルの用いる管理領域を分離するようメールボックスの仕様を変更．ただし，元の仕様のメールボックスで発生しない送信時のメッセージフルエラーが発生する

↓

- PX仕様のメールボックス機能の上位互換となる優先度データキュー機能（データを優先度順にキューイングするデータキュー）を新たに追加
- メールボックスは廃止

ミューテックス機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 優先度上限プロトコルをサポートする排他制御機構
  → POSIXリアルタイム拡張のミューテックスに相当
- 上限のない優先度逆転を防止
- 最大資源数が1のセマフォとの他の違い
  - ロックしたタスク以外はロック解除できない
  - タスク終了時に自動的にロック解除される

CRE_MTX, acre_mtx*	ミューテックスの生成
AID_MTX*	割付け可能なミューテックスIDの数の指定
SAC_MTX†, sac_mtx†*	ミューテックスのアクセス許可ベクタの設定
del_mtx*	ミューテックスの削除
loc_mtx, ploc_mtx, tloc_mtx	ミューテックスのロック
unl_mtx	ミューテックスのロック解除
ini_mtx	ミューテックスの再初期化
ref_mtx	ミューテックスの状態参照

メッセージバッファ機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 任意バイト長のメッセージの非同期メッセージ通信機構
- 送信時のメッセージの単位は，受信時に保存される
  - バイトストリームとは異なる
- メッセージが無い/フルの時に待ち合わせる機能
- メッセージバッファ管理領域のサイズを0に設定すると，同期メッセージ通信も実現可能

CRE_MBF，acre_mbf*	メッセージバッファの生成
AID_MTX*	割付け可能なメッセージバッファIDの数の指定
SAC_MTX†，sac_mtx†*	メッセージバッファのアクセス許可ベクタの設定
del_mbf*	メッセージバッファの削除
snd_mbf，psnd_mbf，tsnd_mbf	メッセージバッファへの送信
rcv_mbf，prcv_mbf，trcv_mbf	メッセージバッファからの受信
ini_mbf	メッセージバッファの再初期化
ref_mbf	メッセージバッファの状態参照

メモリ管理機能

サポートする/しないメモリ管理機能

- 多重メモリ空間はサポートしない
  - MMUを使うことによるオーバヘッドが大きく，組込みシステム向けRTOSではメリットが小さい
- HRP3カーネルでは，メモリ保護機能をサポート
- システム共通のメモリ領域をタスクに割り当てる機能（C言語のmalloc/freeと類似の機能）をサポート

メモリプール管理機能

- システム共通のメモリ領域を複数のメモリプールに分割
  - 目的によってメモリプールを分けると，重要な処理にメモリを残しておくといった使い方が可能
- ASP3/HRP3カーネルでは，獲得できるメモリブロックのサイズが固定の固定長メモリプール機能のみをサポート

固定長メモリプール機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 固定長のメモリブロックを獲得/返却するための機能
- メモリブロックのサイズと個数は，メモリプールの生成時に静的に与える
- メモリが足りない時に待ちに入る機能
- メモリフラグメンテーション（断片化）が起こらない
  - 可変長メモリプールは，便利であるが，メモリフラグメンテーションが起こるため，メモリ不足時の対処が難しい

CRE_MPF, acre_mpf*	固定長メモリプールの生成
AID_MPF*	割付け可能な固定長メモリプールIDの数の指定
SAC_MPF†, sac_mpf†*	固定長メモリプールのアクセス許可ベクタの設定
del_mpf*	固定長メモリプールの削除
get_mpf, pget_mpf, tget_mpf	固定長メモリブロックの獲得
rel_mpf	固定長メモリブロックの返却
ini_mpf	固定長メモリプールの再初期化
ref_mpf	固定長メモリプールの状態参照

時間管理機能

システム時刻管理

- システム時刻(カーネルが管理する時刻)を管理する機能
- 性能評価のために高分解能タイマを参照する機能

タイムイベントハンドラ

- 時間の経過をきっかけに呼び出されるハンドラ
- ASP3/HRP3カーネルでは次の3種類のタイムイベントハンドラをサポート
  - 周期ハンドラ(周期的に呼ばれる)
  - アラームハンドラ(指定した時間後に呼ばれる)
  - オーバランハンドラ ← 拡張パッケージでサポート

時間同期のためのその他の機能

- 自タスクの遅延(タスクを指定時間待たせる)
- 待ちに入るシステムコールのタイムアウト機能

システム時刻管理機能のAPI

“*”は拡張パッケージでサポート

- システム時刻の調整（adj_tim）は，システム時刻を即座に進める／戻す
  - 時間区間の一部のみを伸び縮みさせる場合に使用
- ドリフト量の設定（set_dft）は，システム時刻の進み方を早くする／遅くする（ppm単位で設定）
  - 時間区間全体を一様に伸び縮みさせる場合に使用
- 高分解能タイマの参照（fch_hrt）は，システム時刻の調整の影響を受けないため，性能評価に適している

set_tim	システム時刻の設定
get_tim	システム時刻の参照
adj_tim	システム時刻の調整
set_dft*	ドリフト量の設定
fch_hrt	高分解能タイマの参照

周期通知機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 指定した周期で通知処理を行う
- 通知方法は，周期通知の生成時に静的に設定
  - 周期ハンドラの呼び出しによる通知
  - 変数の設定/インクリメントによる通知
  - タスクの起動/起床による通知　*などなど*
- 周期通知の通知周期と初回の通知時刻（相対時間，通知位相と呼ぶ）は，周期通知の生成時に静的に設定

CRE_CYC，acre_cyc*	周期通知の生成
AID_CYC*	割付け可能な周期通知IDの数の指定
SAC_CYC†，sac_cyc†*	周期通知のアクセス許可ベクタの設定
del_cyc*	周期通知の削除
sta_cyc	周期通知の動作開始
stp_cyc	周期通知の動作停止
ref_cyc	周期通知の状態参照

アラーム通知機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 指定した相対時間後に通知処理を行う
- 通知方法は，アラーム通知の生成時に静的に設定
  - アラームハンドラの呼び出しによる通知
  - 変数の設定/インクリメントによる通知
  - タスクの起動/起床による通知　*などなど*
- アラーム通知の通知時刻は，sta_almのパラメータで相対時間により指定

CRE_ALM，cre_alm*	アラーム通知の生成
AID_ALM*	割付け可能なアラーム通知IDの数の指定
SAC_ALM†，sac_alm†*	アラーム通知のアクセス許可ベクタの設定
del_alm*	アラーム通知の削除
sta_alm	アラーム通知の動作開始
stp_alm	アラーム通知の動作停止
ref_alm	アラーム通知の状態参照

オーバランハンドラ機能のAPI

拡張パッケージでサポート

- タスクが使用したプロセッサ時間（経過時間とは異なる）が，指定した時間を超えた場合に起動されるタイムイベントハンドラ
- オーバランハンドラはすべてのタスクに共通で，その先頭番地はオーバランハンドラの定義時に静的に設定
- タスクが使用できるプロセッサ時間は，sta_ovrのパラメータで指定

DEF_OVR	オーバランハンドラの定義
sta_ovr	オーバランハンドラの動作開始
stp_ovr	オーバランハンドラの動作停止
ref_ovr	オーバランハンドラの状態参照

システム状態管理機能

“†”は，ASP3のサポート外

- システム状態を参照/変更するための機能

システム状態管理機能のAPI

SAC_SYS	システム状態のアクセス許可ベクタの設定
rot_rdq，mrot_rdq†	タスクの優先順位の回転
get_tid	実行状態のタスクIDの参照
get_did†	実行状態のタスクが属する保護ドメインIDの参照
get_lod，mget_lod†	実行できるタスクの数の参照
get_nth，mget_nth†	指定した優先順位のタスクIDの参照
loc_cpu	CPUロック状態への遷移
unl_cpu	CPUロック状態の解除
dis_dsp	ディスパッチの禁止
ena_dsp	ディスパッチの許可

- rot_rdqを周期的に呼び出すことで，同一優先度内でのラウンドロビンスケジューリングが行える

システム状態管理機能のAPI – 続き

sns_ctx	コンテキストの参照
sns_loc	CPUロック状態の参照
sns_dsp	ディスパッチ禁止状態の参照
sns_dpn	ディスパッチ保留状態の参照
sns_ker	カーネル非動作状態の参照
ext_ker	カーネルの終了

メモリオブジェクト管理機能

ASP3のサポート外

- メモリオブジェクトの配置を決定し，状態を参照/変更するための機能

メモリオブジェクト管理機能のAPI

“**”は，HRP3のサポート外

ATT_REG	メモリリージョンの登録
DEF_SRG	標準メモリリージョンの定義
ATT_SEC, ATA_SEC	セクションの登録
ATT_MOD, ATA_MOD	オブジェクトモジュールの登録
ATT_MEM, ATA_MEM, att_mem**	メモリオブジェクトの登録
ATT_PMA, ATA_PMA, att_pma**	物理メモリ領域の登録
sac_mem**	メモリオブジェクトのアクセス許可ベクタの設定
det_mem**	メモリオブジェクトの登録解除
prb_mem	メモリ領域に対するアクセス権のチェック
ref_mem	メモリオブジェクトの状態参照

割込み処理モデルと割込み管理機能

割込み処理の流れ（概要）

- 割込みが発生すると，カーネル内の出入口処理を経由して，アプリケーションが登録した割込みサービスルーチン（ISR）または割込みハンドラが呼び出される
- ISR/割込みハンドラはタスクよりも優先して実行
- ISR/割込みハンドラの中でサービスコールを呼び出して，タスクの起動/起床などが可能
- アプリケーションは，プロセッサの割込みアーキテクチャに依存せずに記述できるISRを用意するのが基本
- 割込みハンドラはコンフィギュレータによって生成されるのが基本だが，特殊なケースに対応するために，ユーザ側で用意することもできる

割込み管理機能のAPI

“†”は，ASP3のサポート外
“*”は，拡張パッケージでサポート

- 割込み要求ライン属性の設定（CFG_INT）により，割込み要求ラインの優先度，レベルトリガかエッジトリガか，初期状態で割込みをマスクするか，などを設定できる

CFG_INT	割込み要求ラインの属性の設定
CRE_ISR，acre_isr*	割込みサービスルーチンの生成/追加
AID_ISR*	割付け可能な割込みサービスルーチンIDの数の指定
SAC_ISR†，sac_isr†*	割込みサービスルーチンのアクセス許可ベクタの設定
del_isr*	割込みサービスルーチンの削除
DEF_INH	割込みハンドラの定義

割込み管理機能のAPI – 続き

- 割込みの禁止(dis_int)と許可(ena_int)は，割込み番号を指定して，その割込みのみをマスク/マスク解除
- 割込み優先度マスクの変更(chg_ipm)は，指定した割込み優先度と同じかより低い割込みをマスク
  - TIPM_ENAALL(＝0)に設定すると，割込み優先度マスク全解除(どの割込みもマスクしない)

dis_int	割込みの禁止
ena_int	割込みの許可
clr_int	割込み要求のクリア
ras_int	割込みの要求
prb_int	割込み要求のチェック
chg_ipm	割込み優先度マスクの変更
get_ipm	割込み優先度マスクの参照

CPU例外処理モデルとCPU例外管理機能

CPU例外処理の流れ

- CPU例外が発生すると，カーネル内の出入口処理を経由して，アプリケーションが登録したCPU例外ハンドラが呼び出される
- CPU例外ハンドラはタスクよりも優先して実行
- CPU例外ハンドラの中でサービスコールを呼び出して，タスクの起動/起床などが可能
- CPU例外ハンドラを，プロセッサのアーキテクチャに依存せずに記述することは（現時点では）不可能
- CPU例外ハンドラは，CPU例外ハンドラ番号を指定してカーネルに登録

CPU例外からのリカバリのアプローチ

(a) カーネルに依存せずに，CPU例外の原因を取り除き，実行を継続する

(b) CPU例外を起こしたタスクより優先して実行されるタスクを起動/起床して，その中でリカバリ処理を行う

(c) システム全体に対してリカバリ処理を行う（例えば，システムを再起動する）

CPU例外管理機能のAPI

- CPU例外ハンドラの中で，どのリカバリアプローチが採れるかを判断するためのAPIを用意

DEF_EXC	CPU例外ハンドラの定義
xsns_dpn	CPU例外発生時のディスパッチ保留状態の参照

拡張サービスコール管理機能

ASP3のサポート外

拡張サービスコールとは？

- 非特権モードで実行される処理単位から，特権モードで実行すべきルーチンを呼び出すための機能（特権モードで実行される処理単位からも呼び出すことができる）
  - 拡張サービスコールはカーネルドメインに属する
  - 拡張サービスコールからは，すべてのカーネルオブジェクトに対して，すべての種別のアクセスを行える
- システムサービス（ミドルウェアやデバイスドライバ）の呼び出しに使用することを想定した機能

拡張サービスコール管理機能のAPI

DEF_SVC	拡張サービスコールの定義
cal_svc	拡張サービスコールの呼出し

保護ドメイン管理機能

ASP3のサポート外

- 保護ドメインのアクセス許可ベクタを設定する機能と，時間パーティショニングのための機能が，ここに含まれる
  - HRP3の時間パーティショニング機能については，付録を参照

保護ドメイン管理機能のAPI

ACV_DOM	保護ドメインのアクセス許可ベクタの設定
DEF_SCY	システム周期の設定
CRE_SOM	システム動作モードの生成
chg_som	システム動作モードの変更
get_som	システム動作モードの参照
ATT_TWD	タイムウィンドウの登録

システム構成管理機能

“*”は，拡張パッケージでサポート

システム構成管理機能のAPI

- DEF_ICSとDEF_MPKにより，非タスクコンテキスト用のスタック領域と，カーネルが割り付けるメモリ領域（管理領域等を自動割り付けにした場合に使われる）を設定できる
- 初期化ルーチンは，カーネルの初期化時，カーネルの動作開始前に呼ばれる
- 終了処理ルーチンは，カーネルの動作終了後に呼ばれる

DEF_ICS	非タスクコンテキスト用スタック領域の設定
DEF_MPK*	カーネルメモリプール領域の設定
ATT_INI	初期化ルーチンの追加
ATT_TER	終了処理ルーチンの追加

付録：TOPPERS/HRP3カーネルの時間パーティショニング機能

時間パーティショニング

パーティショニングとは？

- アプリケーション間を分離することによって，アプリケーション間の保護（あるアプリケーションの誤動作が，他のアプリケーションに障害を引き起こすのを防ぐ）を実現すること

プロセッサの時間パーティショニング

- 各アプリケーションを実行する時間を分離することによって，プロセッサの時間保護を実現すること

時間パーティショニングの実現アプローチ

- システム全体を1つの方式によってスケジューリング
- 階層型スケジューリング
  - まずパーティションをスケジューリングし，次にパーティション内でタスクをスケジューリングする
  - ARINC-653のスケジューリング方式（TDMA）が代表的

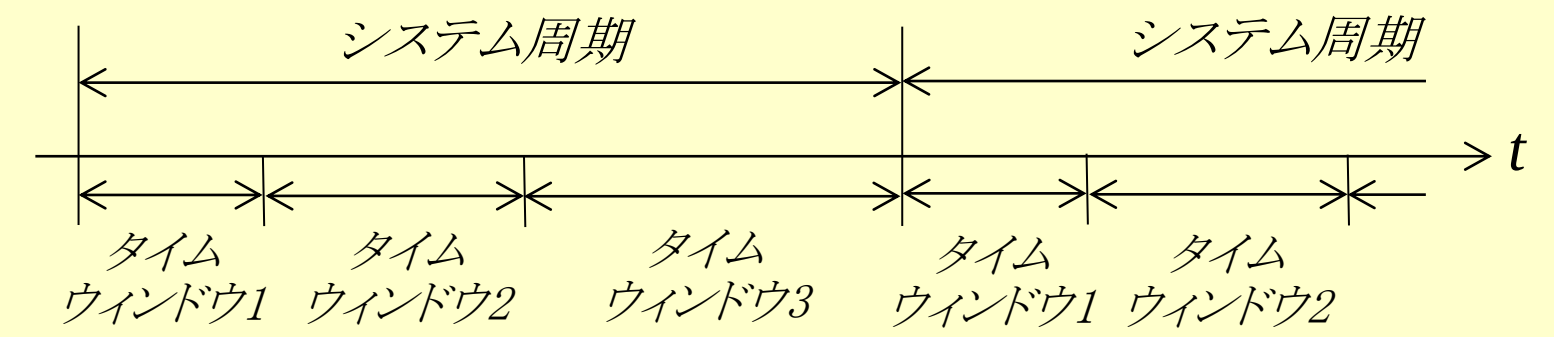
ARINC-653のスケジューリング方式

ARINC-653とは？

- 航空機向けのOSのインタフェース仕様の標準
- アプリケーション統合（IMA）が主なターゲット

スケジューリング方式の概要

- 静的に決定したシステム周期を複数のタイムウィンドウに分割し，パーティションを，それに割り付けられたタイムウィンドウ内で実行する
- パーティションに対する割込みも，パーティションに割り当てられたタイムウィンドウ内でのみ受け付けられる



ARINC-653方式の利点

- タスクが実行されるタイミングが，別のパーティションの影響を受けない
- スケジューリングのオーバヘッド，時間保護のオーバヘッドとも小さい
- 時間保護の原理がシンプルで，パーティション間に影響がないことを主張しやすい

ARINC-653方式の欠点

- 割込みの応答性が低く，高い応答性を求められるシステムを実現しにくい
- システム周期を静的に定めるために，周期の短いパーティションが1つでもあると，周期の長いパーティションも短い周期で切り換える必要がある

ARINC 653方式＋システム割込み拡張

システム割込みとは？

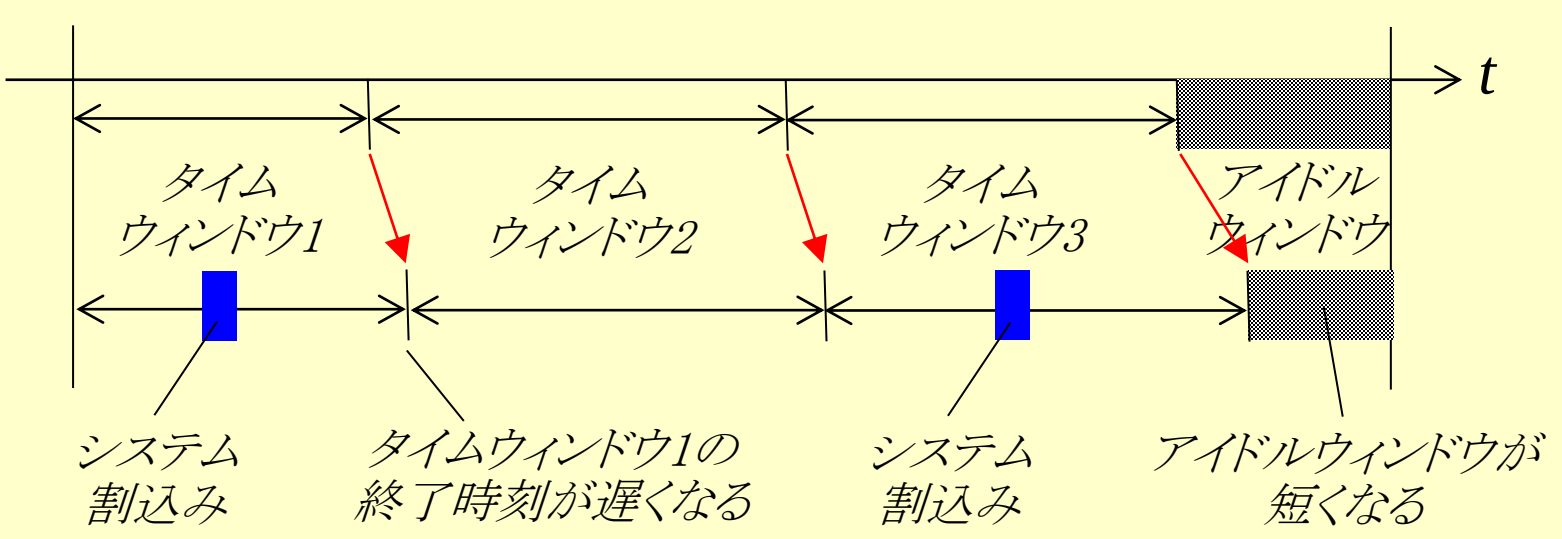
- 特定のパーティションに属さず，タイムウィンドウによらずに受け付けられる割込み
- システム割込みハンドラは，システム内の最も高い安全度水準で開発しなければならない

システム割込みとタイムウィンドウ

- あるタイムウィンドウの途中でシステム割込みが処理された場合，そのタイムウィンドウの終了時刻は，システム割込みの処理時間分，遅くなる
  - タイムウィンドウの正味の長さは変わらない
- タイムウィンドウの終了時刻が遅くなった分，後続のタイムウィンドウの開始時刻および終了時刻も遅くなる

アイドルウィンドウ

- システム周期の最後に，システム周期内で要求されるシステム割込みの最大合計処理時間以上のアイドルウィンドウ(どのパーティションにも割り当てられていないタイムウィンドウ)を置く
- あるシステム周期内で処理されるシステム割込みが，次のシステム周期の開始時刻に影響を及ぼすことはない



HRP3の時間パーティショニング仕様のコンセプト

基本的なアプローチ

- 「ARINC 653方式＋システム割込み拡張」方式を基本とする
- 保護ドメイン（ユーザドメイン）にタイムウィンドウを割り当てる
- タイムウィンドウを割り当てられていない保護ドメイン（ユーザドメイン）は，アイドル時間（タイムウィンドウ内の空き時間，アイドルウィンドウ）に実行する

「基本」からの修正

- カーネルドメインに属する処理単位は，すべて（タスクも）「システム割込み」であるものと扱う
  - カーネルドメインには，タイムウィンドウを割り当てない
- 割込み処理は，カーネルドメインに属する（ユーザドメインに属する割込み処理はサポートしない）

時間パーティショニングに関する主な概念

システム周期（system cycle）

- 保護ドメインを繰り返し実行する基本的な周期

タイムウィンドウ（time window）

- システム周期内の連続した時間区間

アイドルウィンドウ（idle window）

- システム周期内で，タイムウィンドウに含まれない時間区間

タイムウィンドウの割当て

- タイムウィンドウは，1つのユーザドメインに割り当てる
  - 1つのユーザドメインに，任意の数のタイムウィンドウを割り当てることができる

アイドルドメイン（idle domain）

- どのシステム動作モード（後述）においてもタイムウィンドウを割り当てられていないユーザドメインを1つにまとめたもの
  - 該当するユーザドメインが1つ以上ある場合，スケジューリング上は，それらのユーザドメインをまとめて1つのユーザドメインであるかのように扱う
  - あるオブジェクトが「アイドルドメインに属する」といった場合には，タイムウィンドウを割り当てられていないユーザドメインのいずれかに属することを意味する
- アイドルドメインに属する処理単位は，アイドル時間（タイムウィンドウ内の空き時間，アイドルウィンドウ）に実行する

システム動作モード（system operating mode）

- 保護ドメインをどのように繰り返し実行するかを決定するモード
  - タイムウィンドウは，システム動作モード毎に登録する
- ID番号（システム動作モードID）によって識別
- システム周期毎にシステム動作モードを変更できる
  - 各システム動作モードに対して，次のシステム周期のシステム動作モード（遷移先システム動作モードと呼ぶ）を設定できる
- システム周期停止モード（TSOM_STP）では，保護ドメインを繰り返し実行するのを停止
  - システム周期の切換えも，タイムウィンドウの実行も行わない
  - カーネルドメインのみを実行する

時間パーティショニング時のスケジューリング規則

タイムウィンドウのスケジューリング

- プロセッサは，システム周期毎に，現在のシステム動作モードに対して登録されたタイムウィンドウを順に実行する
- システム周期が終わると，システム動作モードを，次のシステム周期での遷移先システム動作モードに切り換える

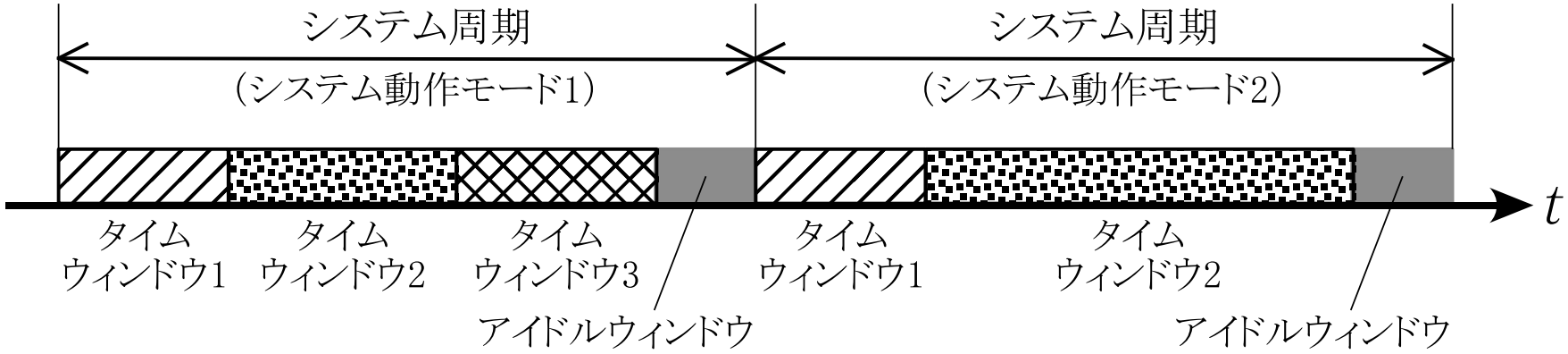


図2-4. システム周期毎のタイムウィンドウの実行

タイムウィンドウ内で実行するドメイン

- そのタイムウィンドウを割り当てられたユーザドメインに属するタスクを，優先度順に実行
- カーネルドメインに属する処理単位（タスク，割込みハンドラ等）は，すべてのタイムウィンドウで実行される
- 実行できる処理単位がない場合には，アイドルドメインに属するタスクを実行

正確に言うと…

- あるタイムウィンドウの実行中は，カーネルドメインに属する実行できる処理単位と，そのタイムウィンドウを割り当てられたユーザドメインに属する実行できるタスクの中から，優先順位の高いものから順に実行される
- これらの保護ドメインに属する実行できる処理単位がない場合には，アイドルドメインに属する実行できるタスクの中から，優先順位の高いものから順に実行される

タイムウィンドウの切換え

- カーネルドメインに属する処理単位が使用したプロセッサ時間の分，タイムウィンドウの切換えを遅延させる
  - 割込みハンドラとCPU例外ハンドラは，カーネルドメインにしか属することができない．つまり，すべての割込みは，システム割込みの扱いになる
  - カーネルドメインに属するタスクの処理時間も，タイムウィンドウに含まない扱いになる

正確に言うと…

- 実行中のタイムウィンドウが使用したプロセッサ時間（いずれの処理単位も実行していなかった時間も含む）から，カーネルドメインに属する処理単位が使用した合計のプロセッサ時間を減じたものが，タイムウィンドウの長さに達すると，次のタイムウィンドウに切り換えられる

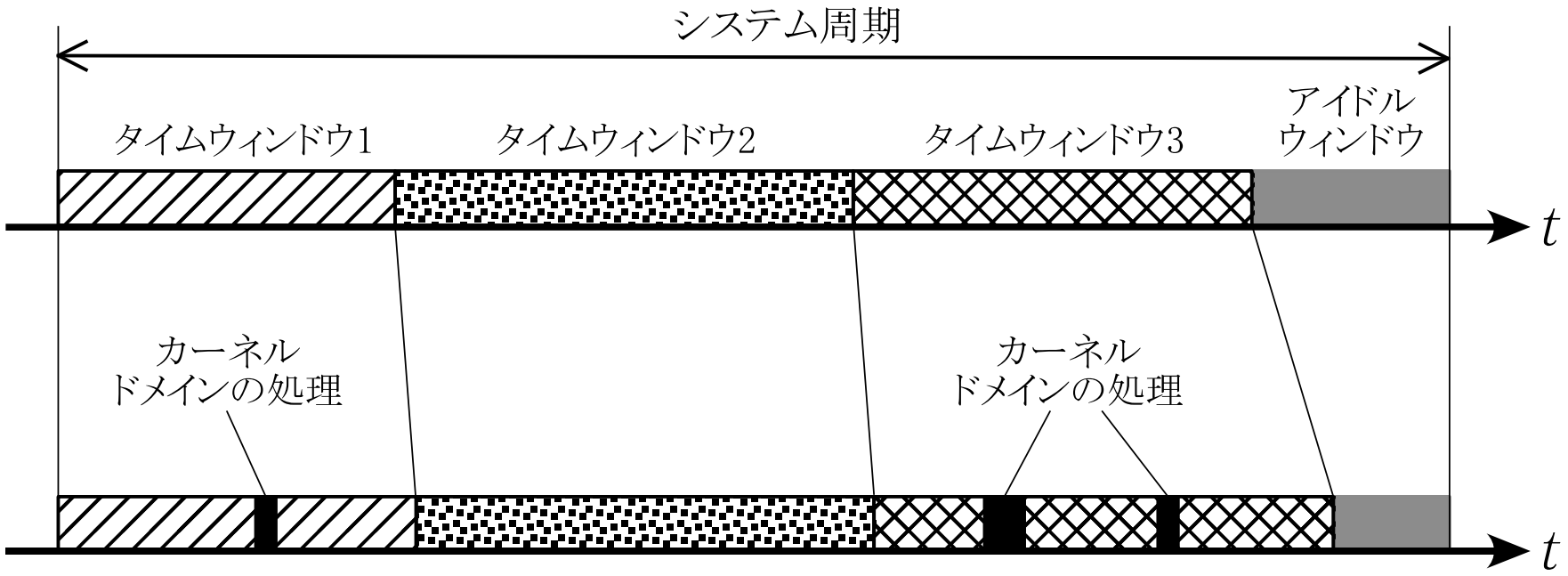


図2-5. タイムウィンドウの切換えタイミング

アイドルウィンドウの扱い

- すべてのタイムウィンドウの実行が終わると，アイドルウィンドウに切り換える
- アイドルウィンドウでは，アイドルドメインに属するタスク（とカーネルドメインに属する処理単位）を優先度順に実行

正確に言うと…

- 〔タイムウィンドウの切換え時に〕次のタイムウィンドウが設定されていない場合（言い換えると，実行中のタイムウィンドウが，現在のシステム動作モードに対して設定された最後のタイムウィンドウである場合）には，アイドルウィンドウに切り換えられる
- アイドルウィンドウの実行中は，カーネルドメインに属する実行できる処理単位と，アイドルドメインに属する実行できるタスクの中から，優先順位の高いものから順に実行される

システム周期オーバラン例外

- システム周期の終了時刻に，タイムウィンドウが実行中であった場合（アイドルウィンドウでなかった場合）に発生する（エミュレートされた，カーネル管理外の）CPU例外
  - システム周期内で，カーネルとカーネルドメインに属する処理単位が使用するプロセッサ時間等を考慮し，十分な長さのアイドルウィンドウを確保するのは，ユーザの責任

システム周期停止モード

- システム周期停止モードでは，システム周期の切換えも，タイムウィンドウの実行も行われず，カーネルドメインに属する処理単位のみが実行される
- 機器が待機している時に使うことを想定

注意事項

- ディスパッチ保留状態（非タスクコンテキストの実行中，CPUロック状態，割込み優先度マスクが全解除でない状態，ディスパッチ禁止状態）では，システム周期の切換えとタイムウィンドウの切換えは保留される
- システム動作モードAにおいてはタイムウィンドウが割り当てられており，システム動作モードBにおいては割り当てられていないユーザドメインは，アイドルドメインにはまとめられない．そのため，システム動作モードBでは，そのユーザドメインは全く実行されない
- カーネルドメインに属するタスクは，ユーザドメインに属する同じ優先度のタスクよりも，高い優先順位を持つ
  - 実装の都合上（ドメイン毎にレディキューを持つ），このような仕様としている

時間パーティショニングに関するAPI

システム周期の設定（DEF_SCY）

DEF_SCY({ RELTIM scyctim })

- システム周期を scyctim に設定
- システム周期を設定しない場合，時間のパーティショニングを行わない

システム動作モードの生成（CRE_SOM）

CRE_SOM(ID somid, { ATR somatr, ID nxtsom })

- IDが somid，システム動作モード属性が somatr（初期モードかどうかを指定），遷移先システム動作モードが nxtsom であるシステム動作モードを生成
- nxtsom の指定を省略した場合，遷移先システム動作モードは，生成したシステム動作モード自身に設定される

タイムウィンドウの登録（ATT_TWD）

ATT_TWD({ ID domid, ID somid, int_t twdord,
PRCTIM twdlen })

- 下のパラメータで指定したタイムウィンドウの登録情報に従って，タイムウィンドウを登録
  - domid：割り当てるユーザドメインのID
  - somid：登録対象のシステム動作モード（名称でしか指定できない）
  - twdord：システム周期内での順序（タイムウィンドウは，twdordの小さい順に並べられる）
  - twdlen：タイムウィンドウの長さ（単位はμ秒）
- PRCTIM型は，プロセッサ時間を表すデータ型．従来仕様のオーバランハンドラのためのOVRTIM型は廃止し，PRCTIM型に統合

システム動作モードの変更（chg_som）

ER ercd = chg_som(ID somid)

- 次のシステム周期での遷移先システム動作モードを，somidで指定したシステム動作モードに設定
  - 再度chg_somを呼び出さない限りは，現在のシステム周期の終了後に，somidで指定したシステム動作モードに切り換わる
- ただし，現在のシステム動作モードがシステム周期停止モード（TSOM_STP）の場合には，somidで指定したシステム動作モードに即座に切り換わる
- somidにTSOM_STPを指定した場合，現在のシステム周期の終了後（現在のシステム動作モードがシステム周期停止モードの場合は，即座）に，システム周期停止モードに切り換わる

ユーザドメインに属するタイムイベント処理

タイムイベント処理機能の見直し

- ユーザドメインにおいても，安全に使用できる周期処理／アラーム処理のための機能として，周期通知／アラーム通知機能（タイムイベント通知と総称）を設けた
  - 従来の周期ハンドラ／アラームハンドラは，カーネルドメイン（特権モード）で実行されるため，ユーザドメインで自由に使うことができない

ユーザドメインに属するタイムイベント通知の処理タイミング

- ユーザドメインに属するタイムイベント通知は，そのユーザドメインに割り当てられたタイムウィンドウへの切換え直後に処理される
- アイドルドメインに属するタイムイベント通知は，アイドルウィンドウへの切換え直後に処理される