



TOPPERSが考える車両制御用 Operating System

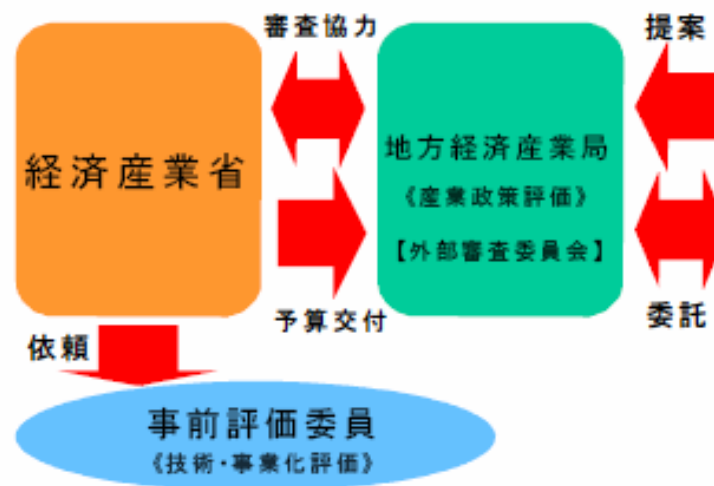
株式会社ヴィッツ

地域新生コンソーシアムとは

経済産業省の研究事業 (2年間)

目的:

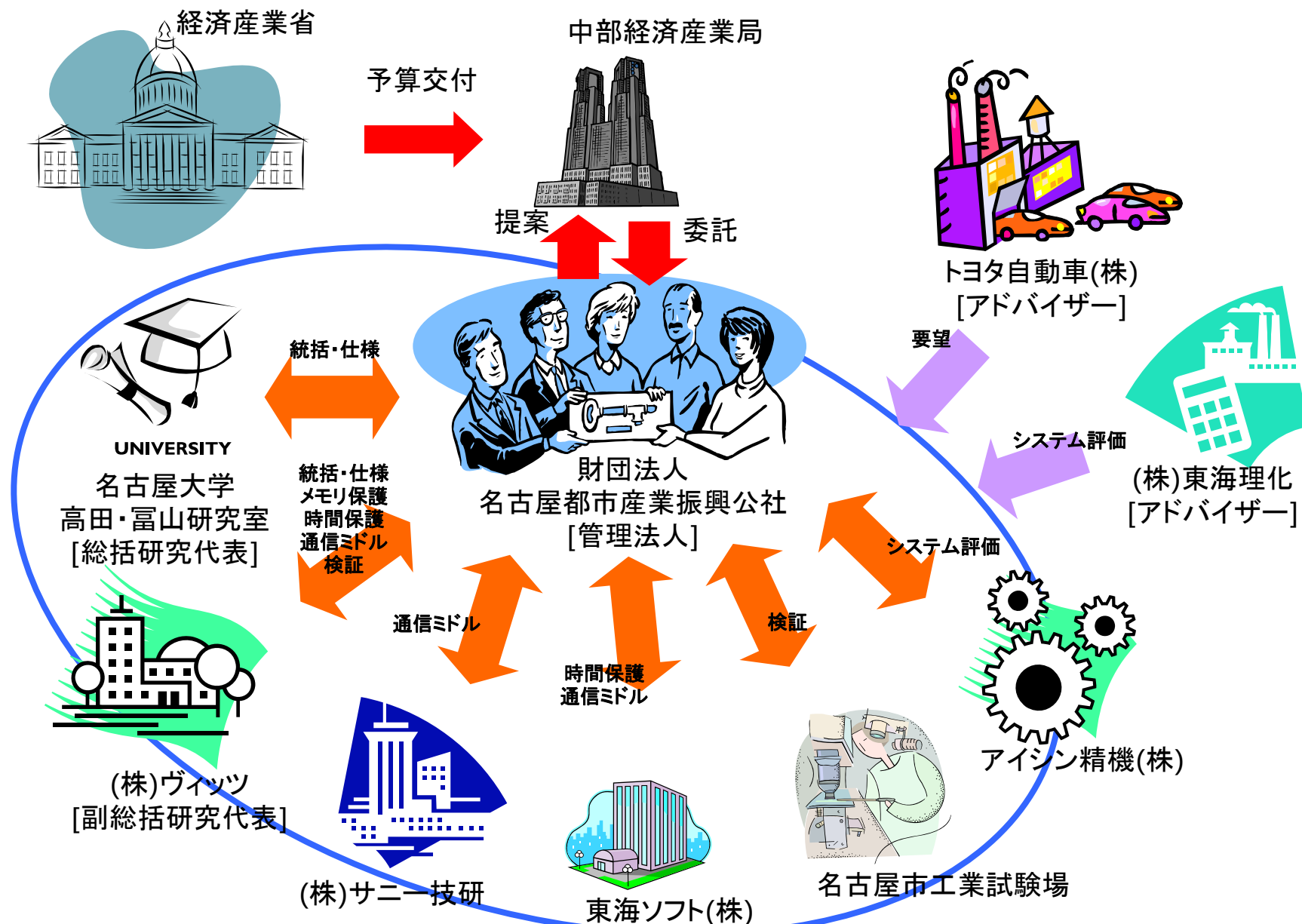
- ・大学等の技術シーズ・知見の活用
- ・地域における産学官の強固な共同研究体制の確立
- ・実用化、新規産業創出可能な事業とし、地域の産業活性、雇用創出を促す



	一般枠	他府省連携枠 ^{※1}	中小企業枠
エネルギー効果	エネルギーの使用の合理化 ^{※2} 又は石油代替エネルギーの開発及び利用に関するものを含む		
応募対象者	研究共同体（管理法人による応募となります）		
募集対象分野	産業技術戦略上の目標達成に資する16の重点分野に該当する研究開発		
研究開発期間	2年以内		
研究開発費 ^{※3}	初年度1億円以内/件 (次年度5千万円以内/件)		初年度3千万円以内/件 (次年度2千万円以内/件)
新規採択予定数	全国6件程度	全国20件程度	全国42件程度
	エネルギー効果に寄与するもの 全国で26件程度		
公募時期	平成17年4月1日（金）～平成17年4月21日（木）		

地域新生コンソーシアム研究事業

コンソーシアム体制図



自動車統合制御用組込みOS開発の概略

<目標>

- ・複数のアプリケーションを同一ECUで安全に動作させることにより、**ECUの搭載個数を半減**させる。
実現方法:メモリ保護(独自MPU開発による実現)、時間保護(多段スケジューラによる実現)を開発する。
2007年で75個以上の搭載予想を2012年には30個まで削減する。

<効果>

・ソフトウェア品質の向上

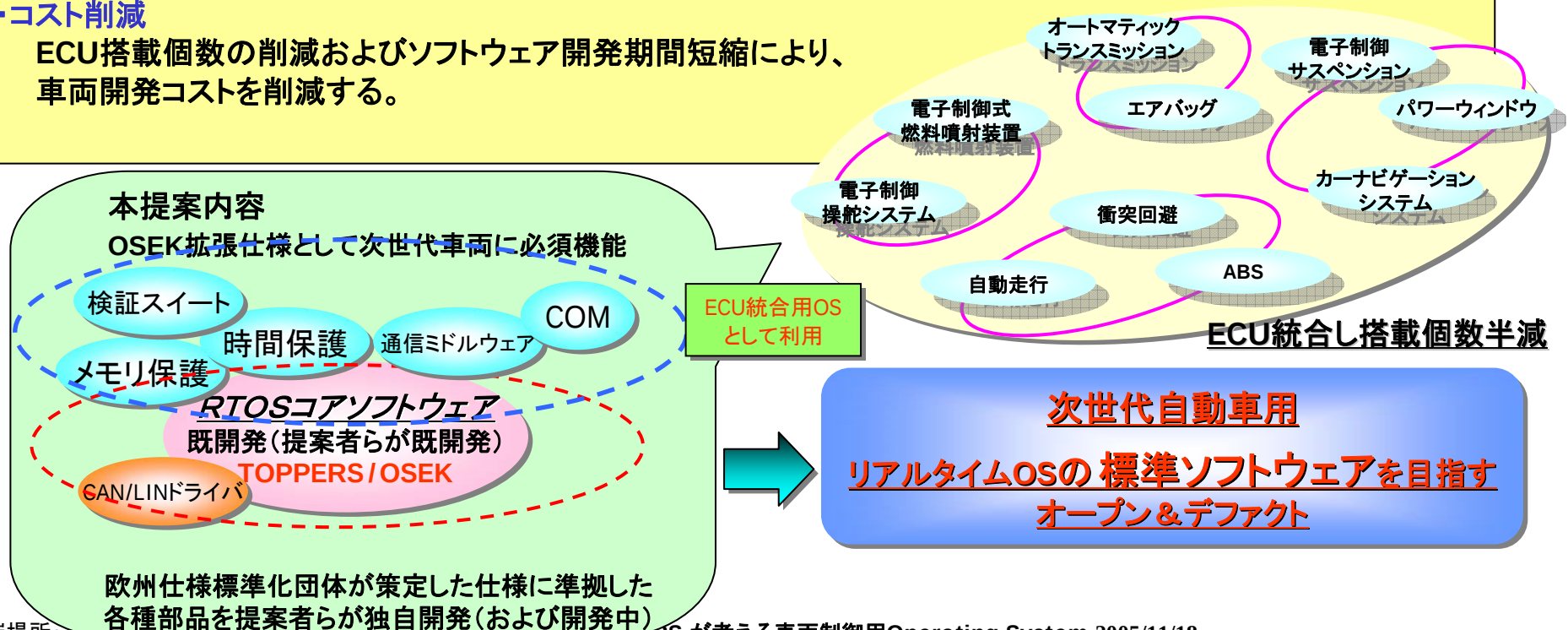
保護機能を有するRTOSを利用し、アプリケーション間の相互干渉を防止し、問題特定を容易にする。

・省エネルギーの実現

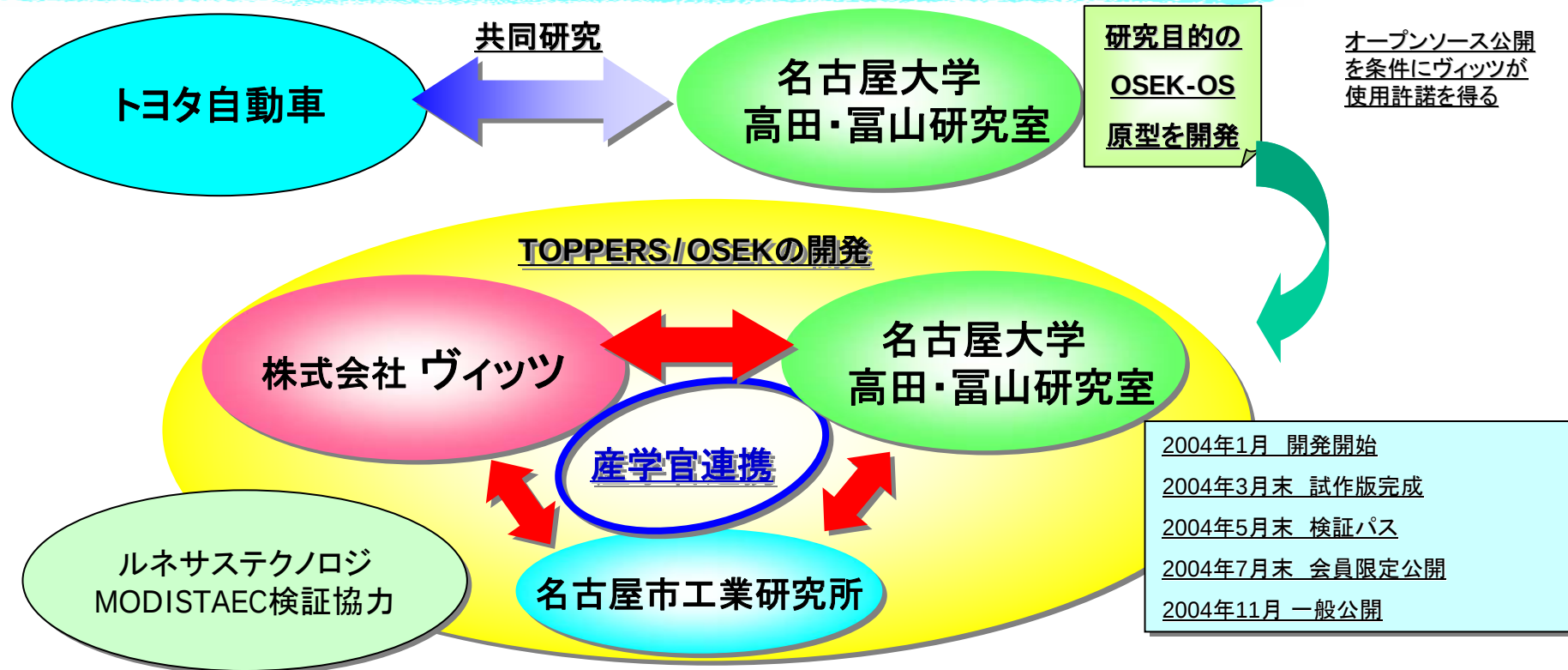
ECU削減により、製造エネルギーの削減やワイヤーハーネスの削減が可能となる。
さらに、ハーネス削減により、車両重量が軽減され、燃費向上が達成できる

・コスト削減

ECU搭載個数の削減およびソフトウェア開発期間短縮により、
車両開発コストを削減する。



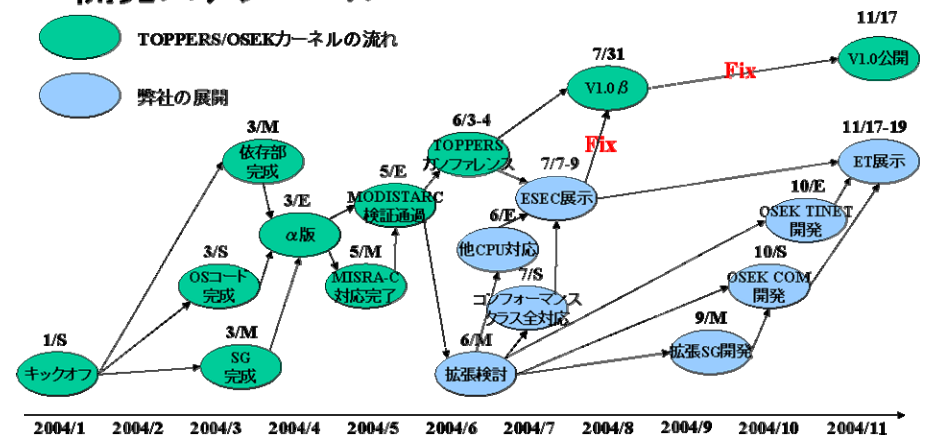
ベースソフト TOPPERS/OSEKカーネルとは



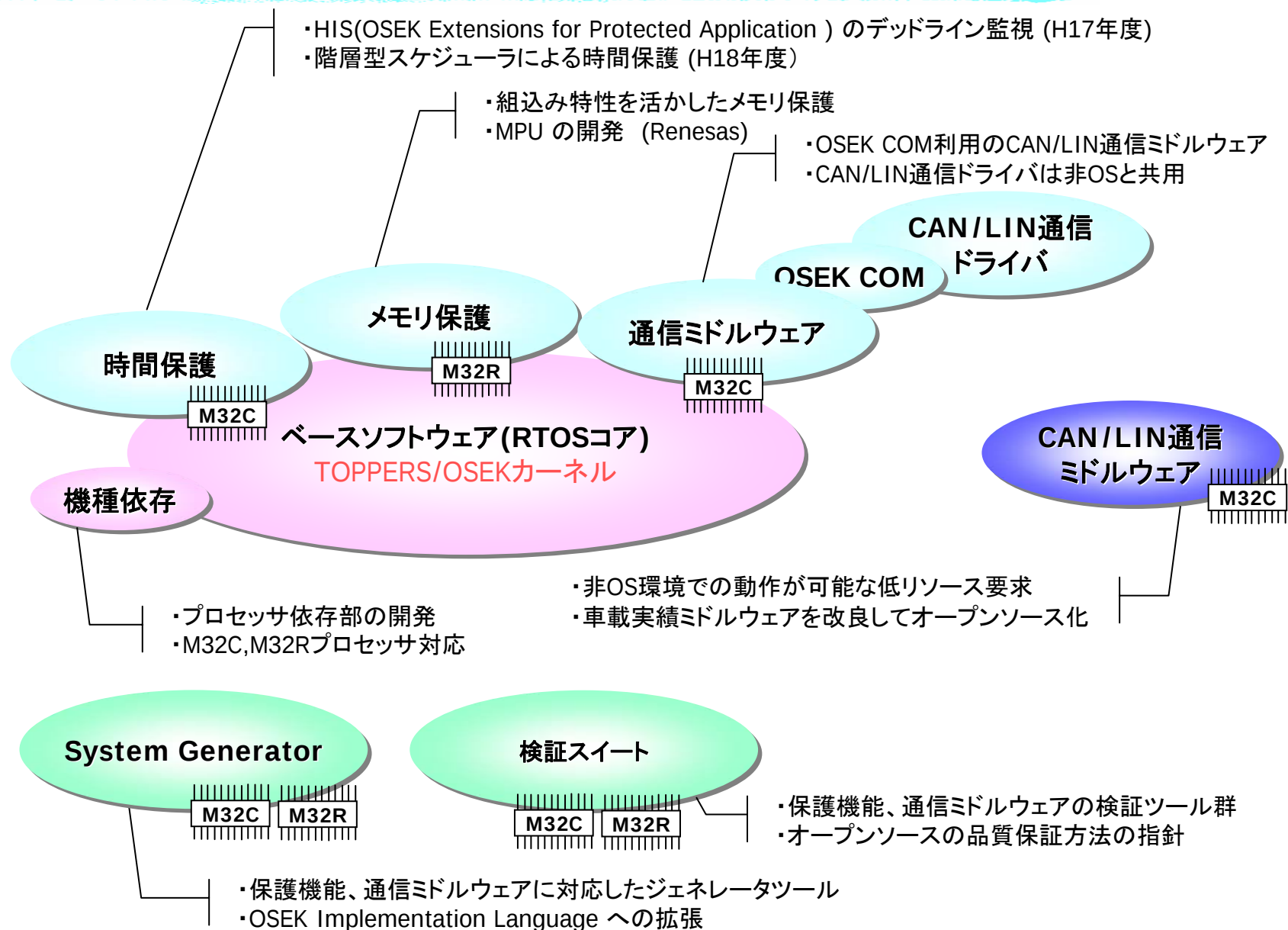
TOPPERS/OSEK仕様

準拠した仕様	OSEK/VDX仕様 Version2.2.1に準拠
コンフォーマンス・クラス	ECC-2 (ただし、一部実装依存あり)
対応プロセッサ	ルネサステクノロジ製 M32C (M32C/83), M16C, H8S
開発ツール	統合開発環境 TM V3.2 Cコンパイラ NM308WA V1.00 シミュレータデバugga PD308S V1.00
使用ROM領域	約6Kバイト
使用RAM領域	59バイト
その他	MISRA-Cに対応 MODISTARCに対応

・ 開発スケジュール

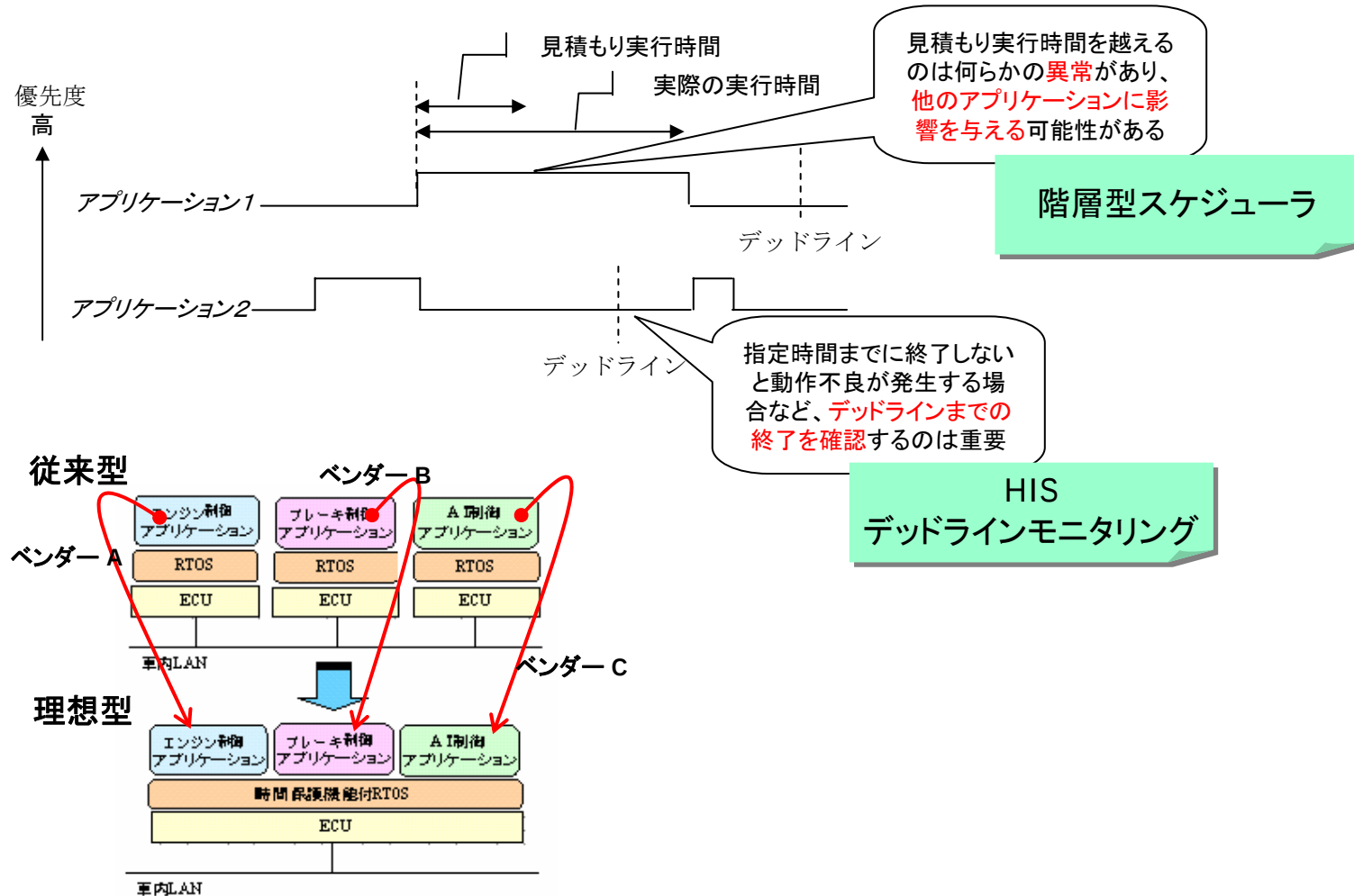


自動車統合制御用組込みOS開発内容



時間保護

単一プロセッサ上に複数のアプリを混在させると、アプリの実行が他のアプリに影響を与える場合がある。
複合システムではこのアプリケーションに対して静的に決定された時間設計を厳守する必要がある。



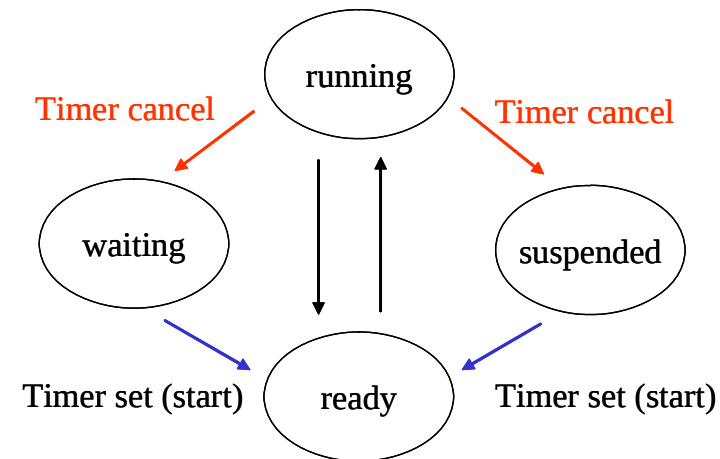
<時間保護 第一段階>

・HISの時間保護 (Deadline monitoring)

タスクの動作開始と終了を捕まえて、デッドライン超過を監視する

監視対象はタスク単位

監視時間はタスク毎にOILで指定



タイマキャンセル前にタイマ設定時間経過 (エクスパイア)すると

当該タスクと同じアプリに属する全てのタスクが終了させられる

タスク(複数形なのでアプリに属するタスク群) によって獲得されていた全てのOSEKリソースが開放される

OILで指定された、エラー発生時のエラーハンドラが起動される

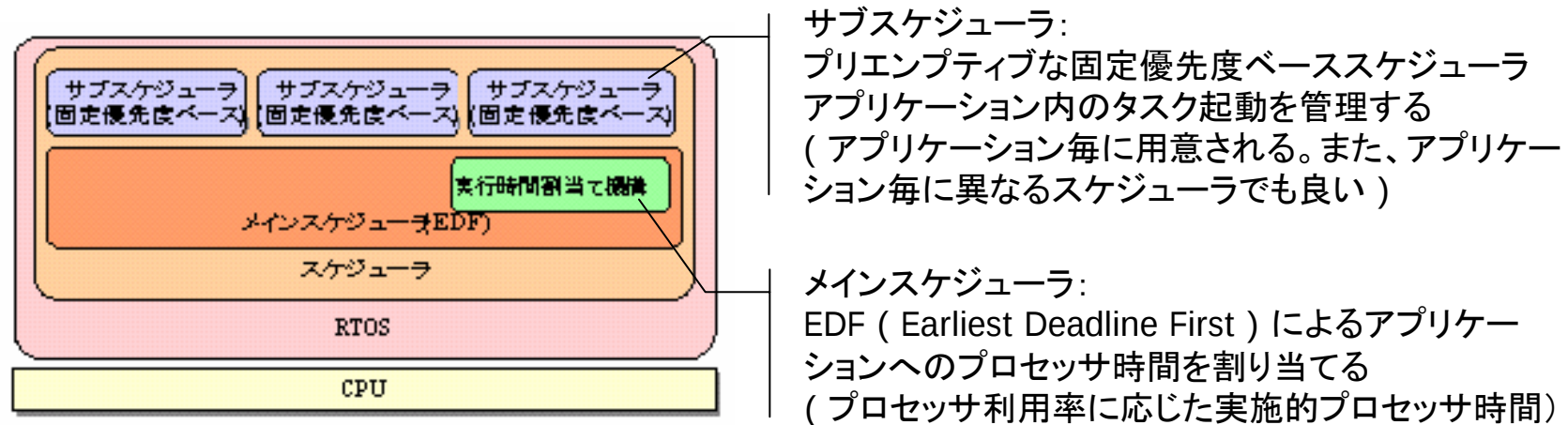
(アプリの再初期化(再起動)に利用可能)

検討！ waiting からのタイマスタートはタイマ値初期化で良いか？

この方式は、デッドラインまでに処理の完了を確認するには良い方法。しかし、保護という意味はほとんどない。

<時間保護 第2段階>

- ・多段ディスパッチャー方式 (高田研究室で現在研究中)

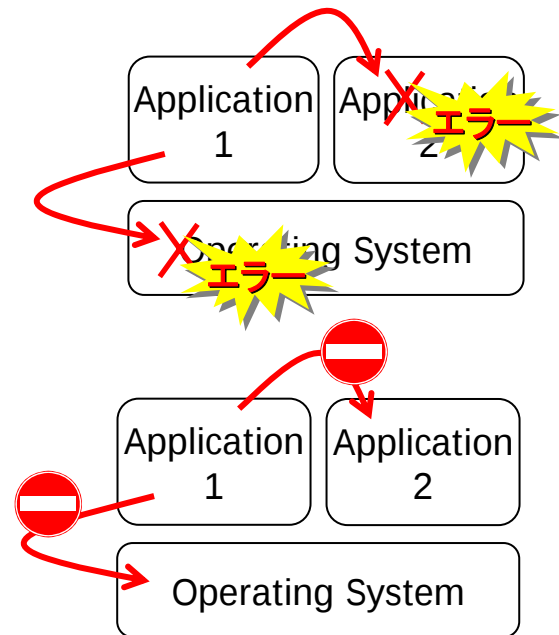


- ・RTOSに組み込むことにより、時間保護機能をOSレベルでサポート
- ・システム開発者が独自に実装しなくて良いため、開発者の負担を軽減
- ・複数ベンダーが低速プロセッサ上で開発・検証したアプリケーションを高速プロセッサ上で複合システムを構築することが可能となる

メモリ保護 1

<メモリ保護機能>

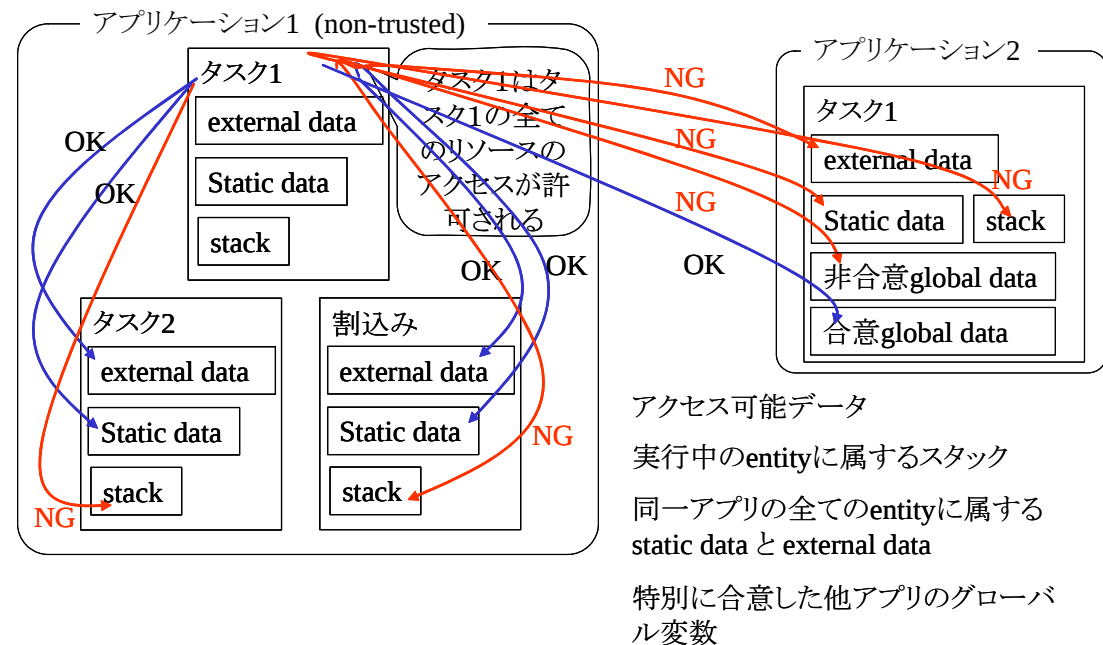
- ・プロセッサ内のMMUを改良し、MPU (Memory Protection Unit) を開発し利用する
- ・車載ソフトウェアの特徴である静的マッピングを利用し、アドレス変換を用いない



メモリ保護

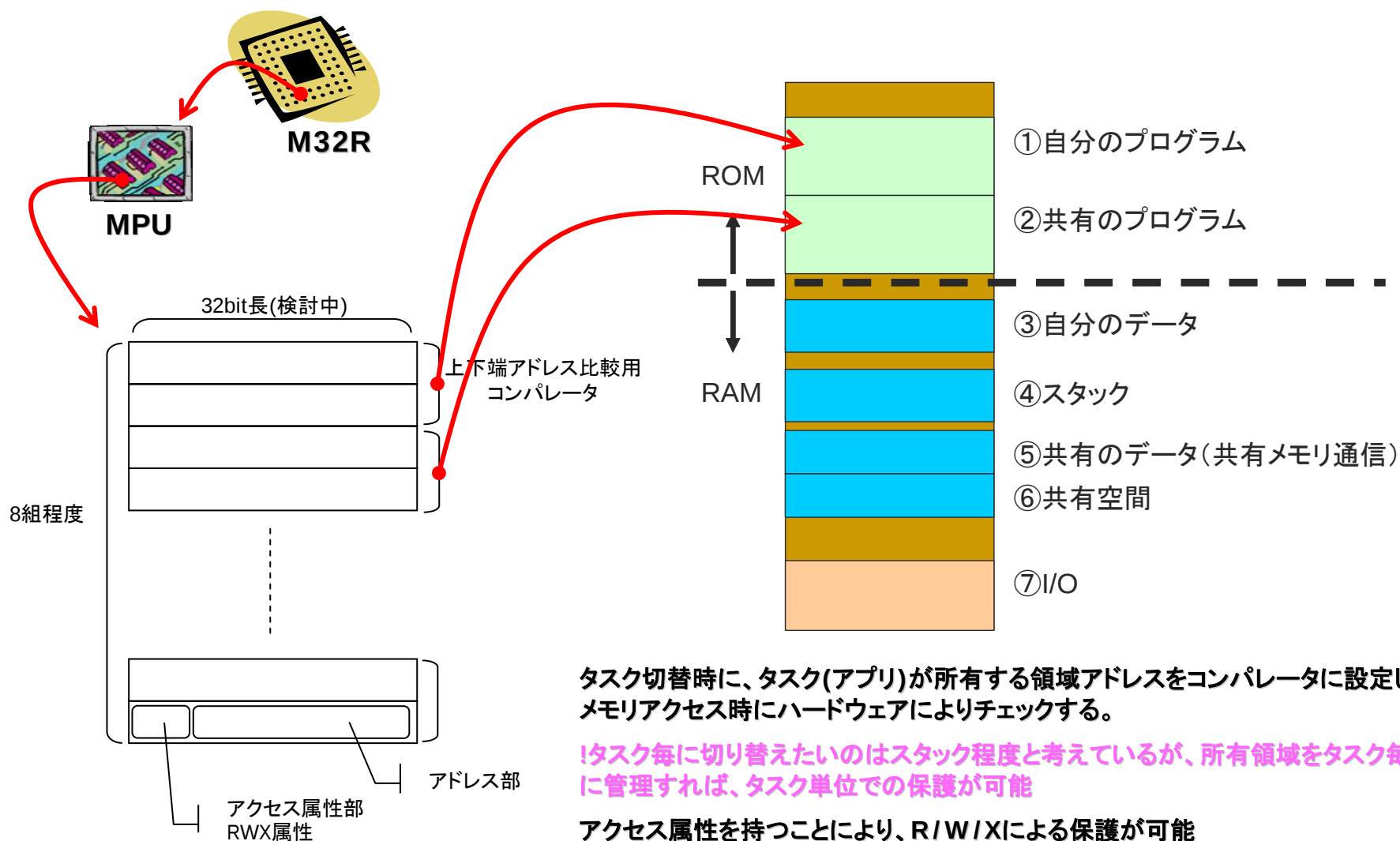
HISの保護を拡張し、Writeに加え、
Read, Execution にも対応

HISと異なり、同一アプリケーション内でも保護可能
(保護粒度をタスク単位管理した場合)



HISのメモリ保護 (HISの保護は書込みのみ)

メモリ保護 2



タスク切替時に、タスク(アプリ)が所有する領域アドレスをコンパレータに設定し、メモリアクセス時にハードウェアによりチェックする。

!タスク毎に切り替えたいのはスタック程度と考えているが、所有領域をタスク毎に管理すれば、タスク単位での保護が可能

アクセス属性を持つことにより、R/W/Xによる保護が可能

領域データは静的に決まるため、タスク切替時に書込みのみで良い

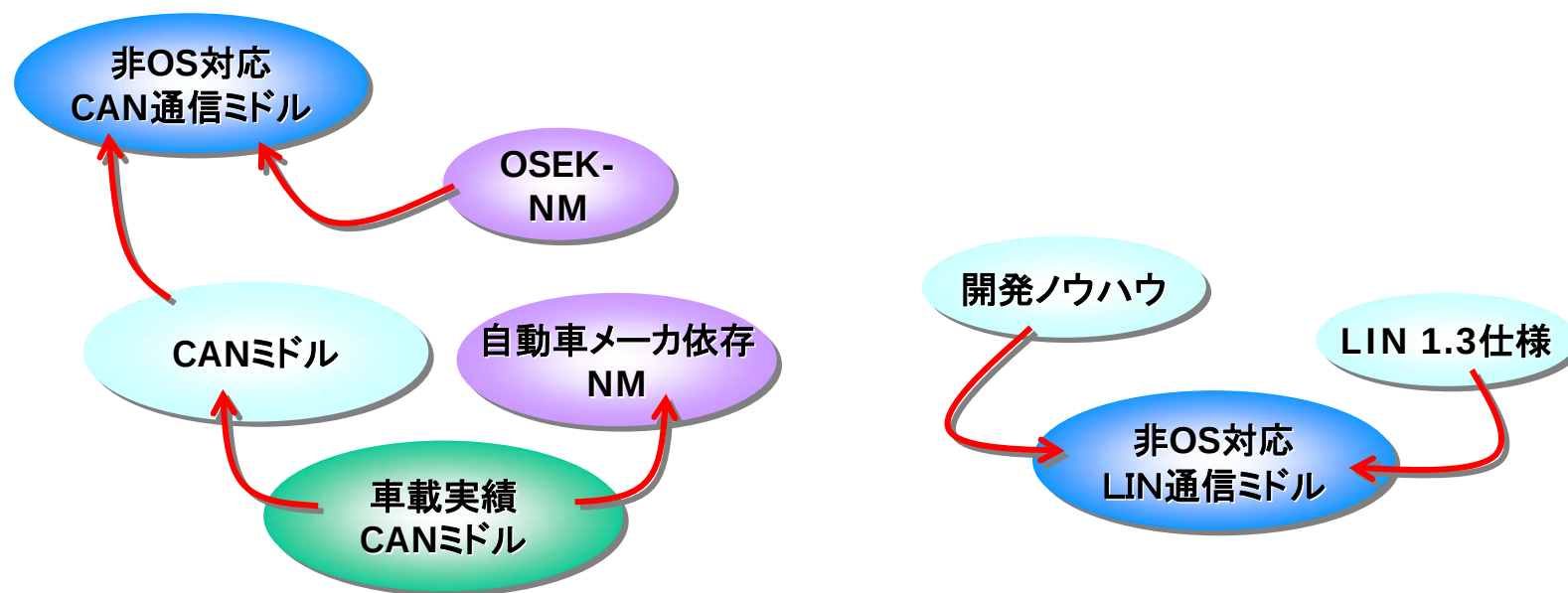
領域データは静的に決まるため、アドレス変換は不要

<CAN通信ミドルウェア>

- ・自動車搭載実績のあるCAN通信ミドルウェアをベースとしたオープンソースCAN通信ミドルウェア
- ・搭載実績ノウハウを継承した Communication Layer
- ・自動車メーカーに依存しない、OSEK 仕様に準拠した Network Management (direct/indirect)

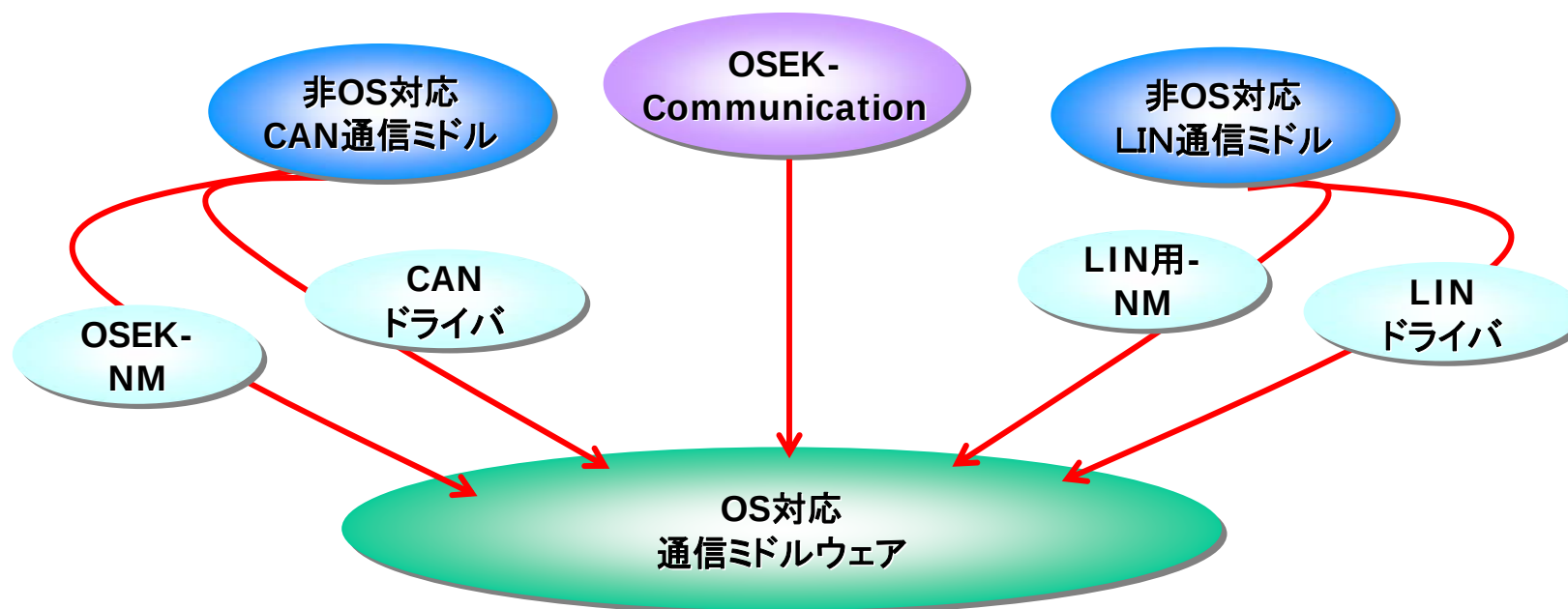
<LIN通信ミドルウェア>

- ・自動車搭載LIN通信ミドルウェア開発のノウハウを利用したオープンソースLIN通信ミドルウェア
- ・マスターノード/スレーブノードを独立させ、省リソースを実現する設計



<OS対応通信ミドルウェア>

- ・OSEK Communication 仕様を利用したECU内/外 通信ミドルウェア
通信相手 (タスク、CANノード、LINノード) を意識させない通信
- ・非OS対応 CAN/LIN通信ミドルウェアとの接続互換
- ・非OS対応 CAN/LIN通信ミドルウェアとデバイスドライバを共有(目標)
- ・非OS対応 通信ミドルウェアと共通のNetwork Management を利用



＜機種依存対応＞

- ・メモリ保護はルネサス製M32Rを利用するため、TOPPERS/OSEKカーネルをM32R対応する

＜System Generator＞

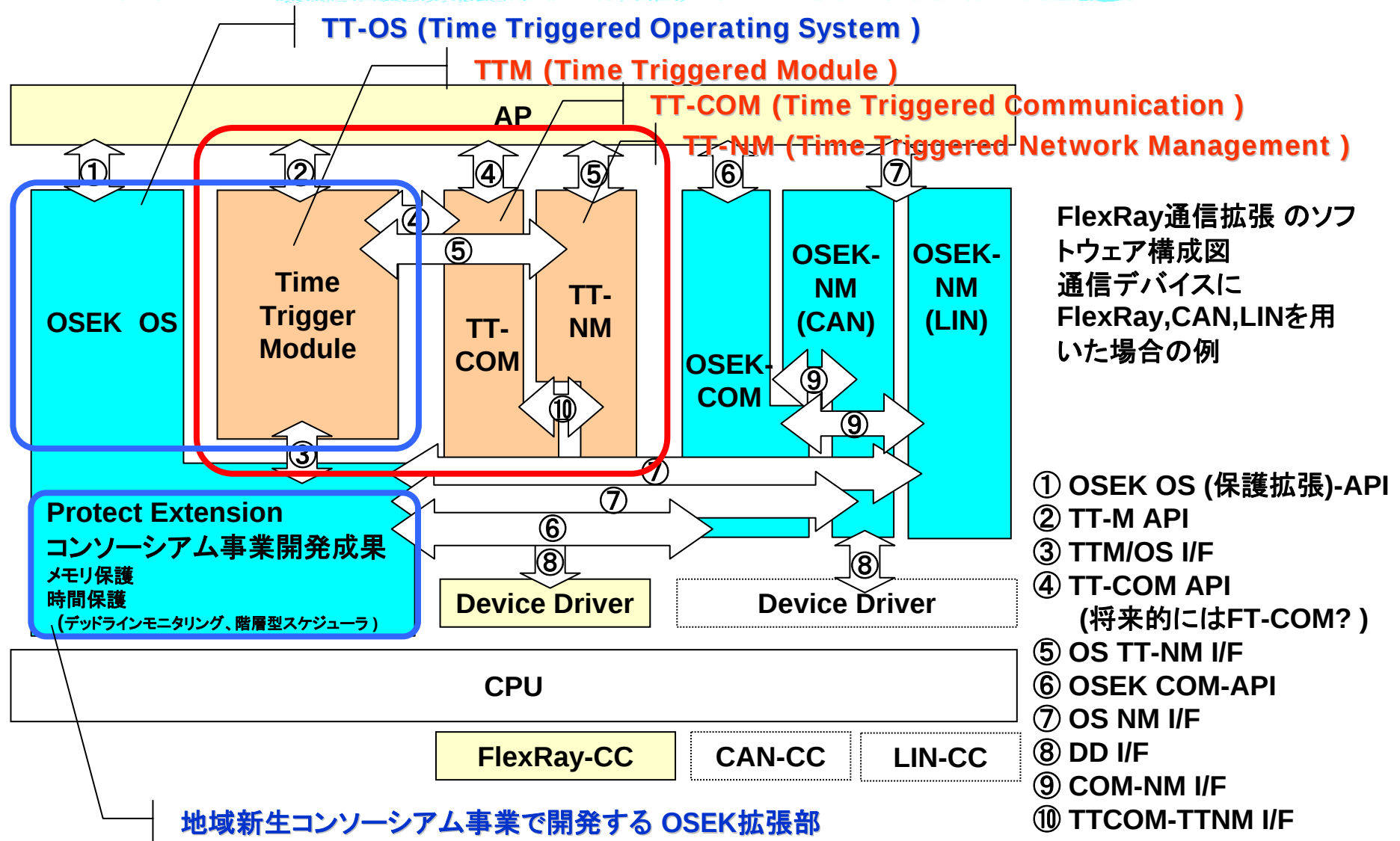
- ・記述言語は、OSEK Implementation Language Ver.2.5 (OIL仕様) を基本仕様とする
- ・OIL仕様に、メモリ保護、時間保護、通信ミドルウェア拡張に伴う、記述言語を拡張する
- ・拡張OIL仕様に対応した実装コードを生成する

＜検証スイート＞

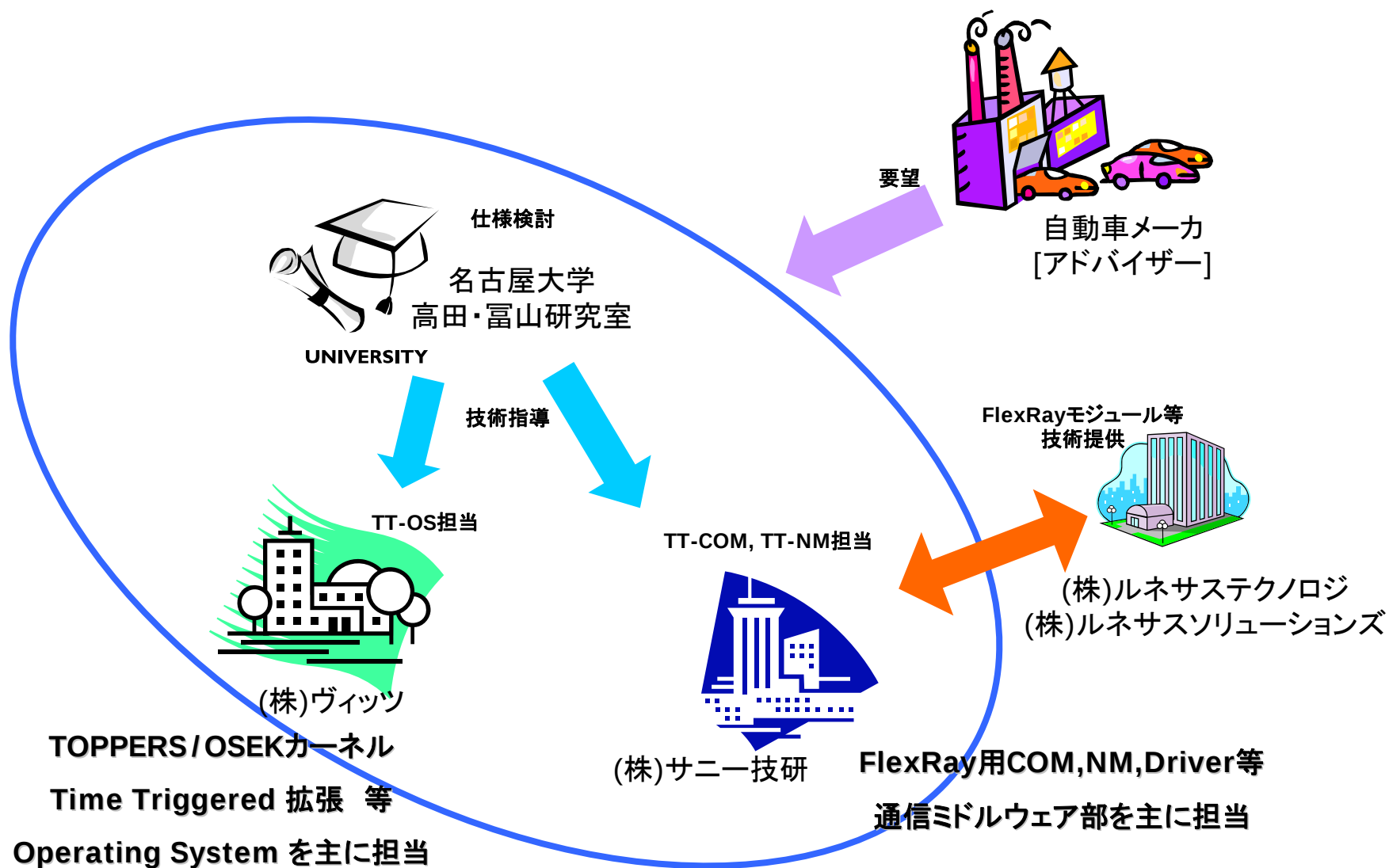
- ・メモリ保護、時間保護等実現機能妥当性を検証するテストプログラムを作成する
- ・通信ミドルウェアの接続検証、異常処理時の動作妥当性を検証するテストプログラムを作成する

FlexRay通信拡張について

FlexRay通信拡張 ソフトウェア構成図



FlexRay通信拡張開発体制

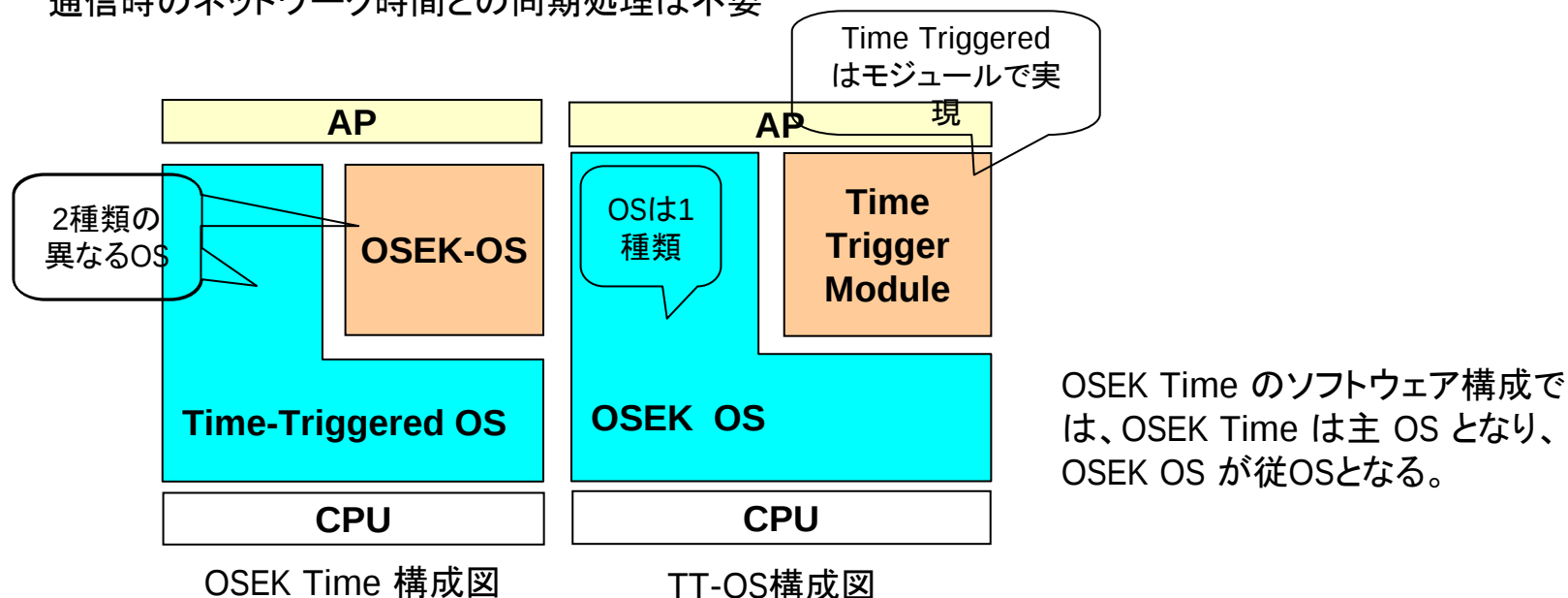


TT-OS (Time Triggered OS) の特徴

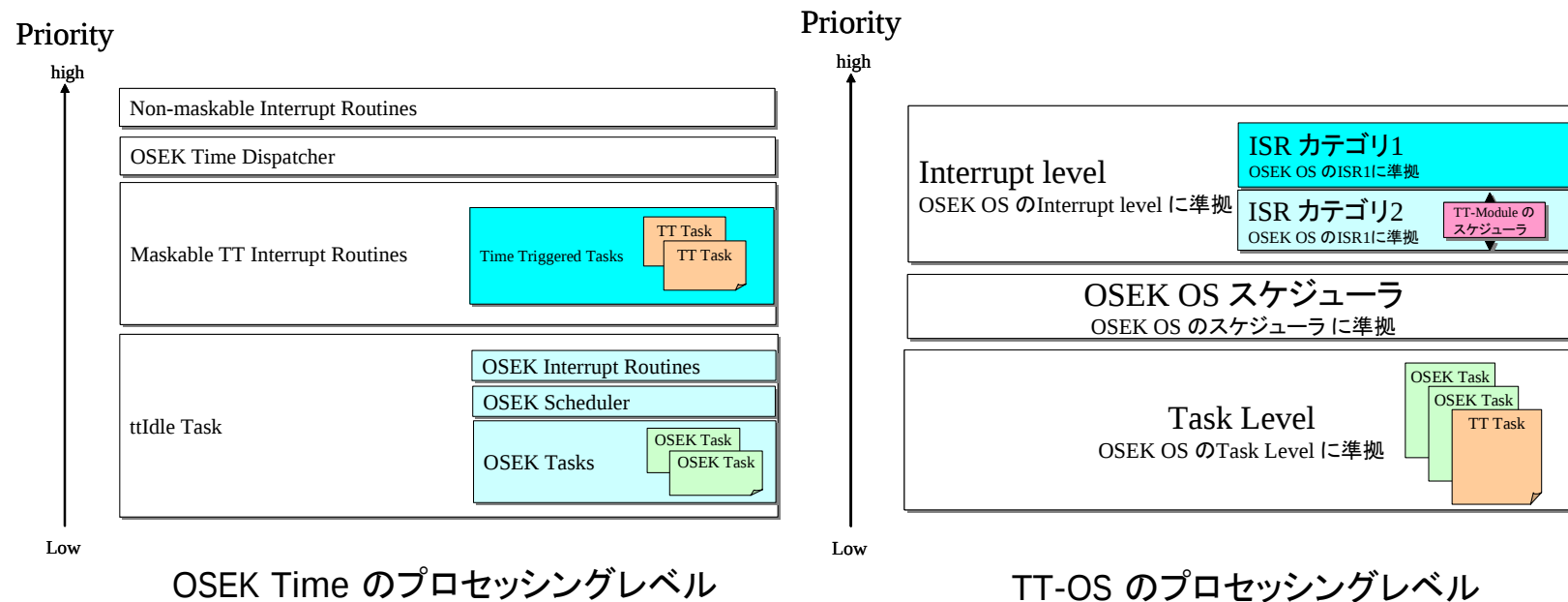
- ・ 自動車メーカーの利用想定を調査し、仕様を新規作成
- ・ OSEK仕様OSにTime Triggered Module の追加で、Time Triggered 処理を実現
- ・ OSEK/VDX Time-Triggered Operating System 仕様を参考に仕様を検討
- ・ Time Triggered Task と OSEK Task の優先度は自由に決定可能
- ・ Time Triggered Task の起動トリガはFlexRay-IPからの割込みを利用する。

ネットワーク時間との時間誤差は発生しない

通信時のネットワーク時間との同期処理は不要



TT-OS (Time Triggered OS) の特徴



OSEK Time 環境では、OSEK OS 管理下のタスク、割り込み処理は、Time Triggered タスクが稼動していないアイドル時に動作をする。

→ 非Time Triggered 処理の時間制約を保障することは難しい

一方、TT-OS はすべてのタスクがOSEK OS 管理下であり、優先度に従い、OSEK OS がタスク起動を行う。
(TTMは、Time Triggered Task の起動要求を行うのみ)

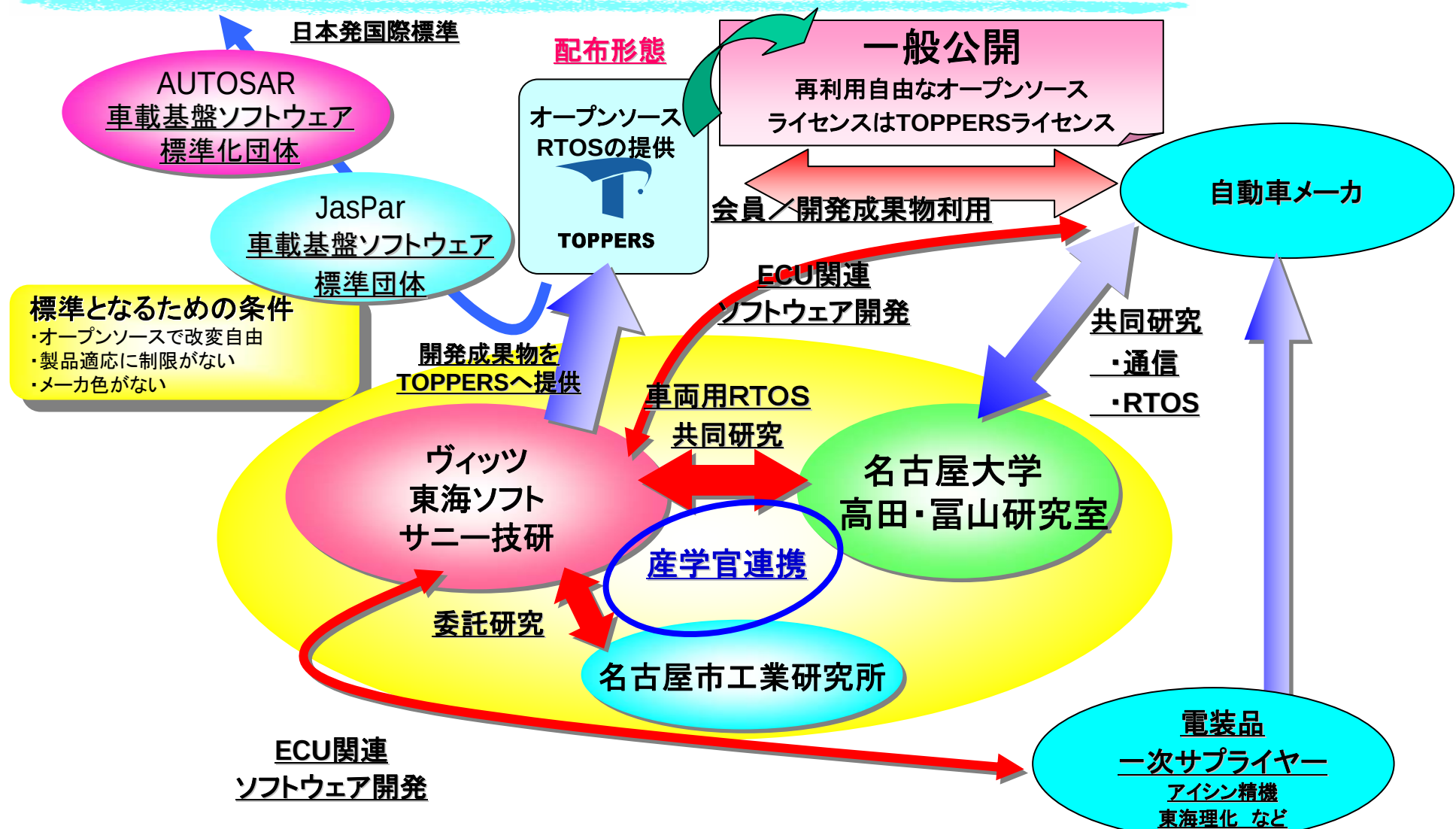
→ Time Triggered 処理と、非Time Triggered 処理部の共存が可能

例：ネットワーク同期通信処理と回転軸同期など

- FlexRay通信を目的とした、通信ミドルウェア
- DRV(実装依存部)、COM/NM(非依存部)で構成
- OSEK/VDX Fault-Tolerant Communication 仕様を参考に仕様を規定
- データ送信方法は、イベント (Qued)、状態(UnQued)が選択可能
- メッセージのPack / UnPack をサポート
- エンディアン変換をサポート
- 通信途絶・送信途絶検出機能をサポート
- Network Management 機能をサポートし、ノード管理、起動、WakeUP、Sleep を管理

デモンストレーション映像

普及計画図



技術面 ; **次世代車両用OS** の仕様を提案

営業面 ; 先進的ソフト機能部品などの開発成果物を自動車メーカーに等へ販売