# TOPPERSプロジェクトの最近の成果と今後の活動指針

2011年6月10日

高田 広章

NPO法人 TOPPERSプロジェクト 会長

名古屋大学 大学院情報科学研究科 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/

# TOPPERSプロジェクトとは?


TOPPERS = Toyohashi Open Platform for
Embedded and Real-Time Systems

## プロジェクトの活動内容

- 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
- それ以前は，名古屋大学(2002年度までは豊橋技術科学大学)高田研究室を中心とする任意団体として活動

# TOPPERSプロジェクトの狙い

2010年8月に見直し

## 決定版のITRON仕様OSの開発

ほぼ完了

- ITRON仕様がかかえる過剰な重複投資と過剰な多様性の問題を解決（または軽減）

## 次世代のリアルタイムOS技術の開発

- 組込みシステムの要求に合致するし，ITRONの良さを継承する次世代のリアルタイムOS技術を開発

  ***Linuxと類似のOSをもう１つ作っても意味がない！***

- オープンソースソフトウェア化により産学官の力を結集

## 組込みシステム開発技術と開発支援ツールの開発

- 高品質な組込みシステムの効率的な開発を支援

## 組込みシステム技術者の育成への貢献

- オープンソースソフトウェアを用いた教育コースや教材を開発し，それを用いた教育の場を提供

# 重点的に取り組んでいるテーマ

## 次世代のリアルタイムカーネル技術

! 高信頼性・安全性・リアルタイム性を追求

- TOPPERS新世代カーネル（ITRON仕様からの発展）
- 次世代車載システム向けRTOS（OSEK/VDX, AUTOSAR仕様をベースに）

## 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プラットフォームと開発支援ツール

- 各種のミドルウェアや仮想化技術
- 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ロボコン向けプラットフォームと教材の提供

# TOPPERS新世代カーネルの開発状況

# TOPPERS新世代カーネルの必要性

*μITRON4.0仕様が公表されてから，すでに10年が経過*

組込みシステムにおける要求の変化

- システム/ソフトウェアの一層の大規模化・複雑化
- これまで以上に高い信頼性・安全性
- 小さい消費エネルギーで高い性能

μITRON4.0仕様以降の各方面の技術開発成果

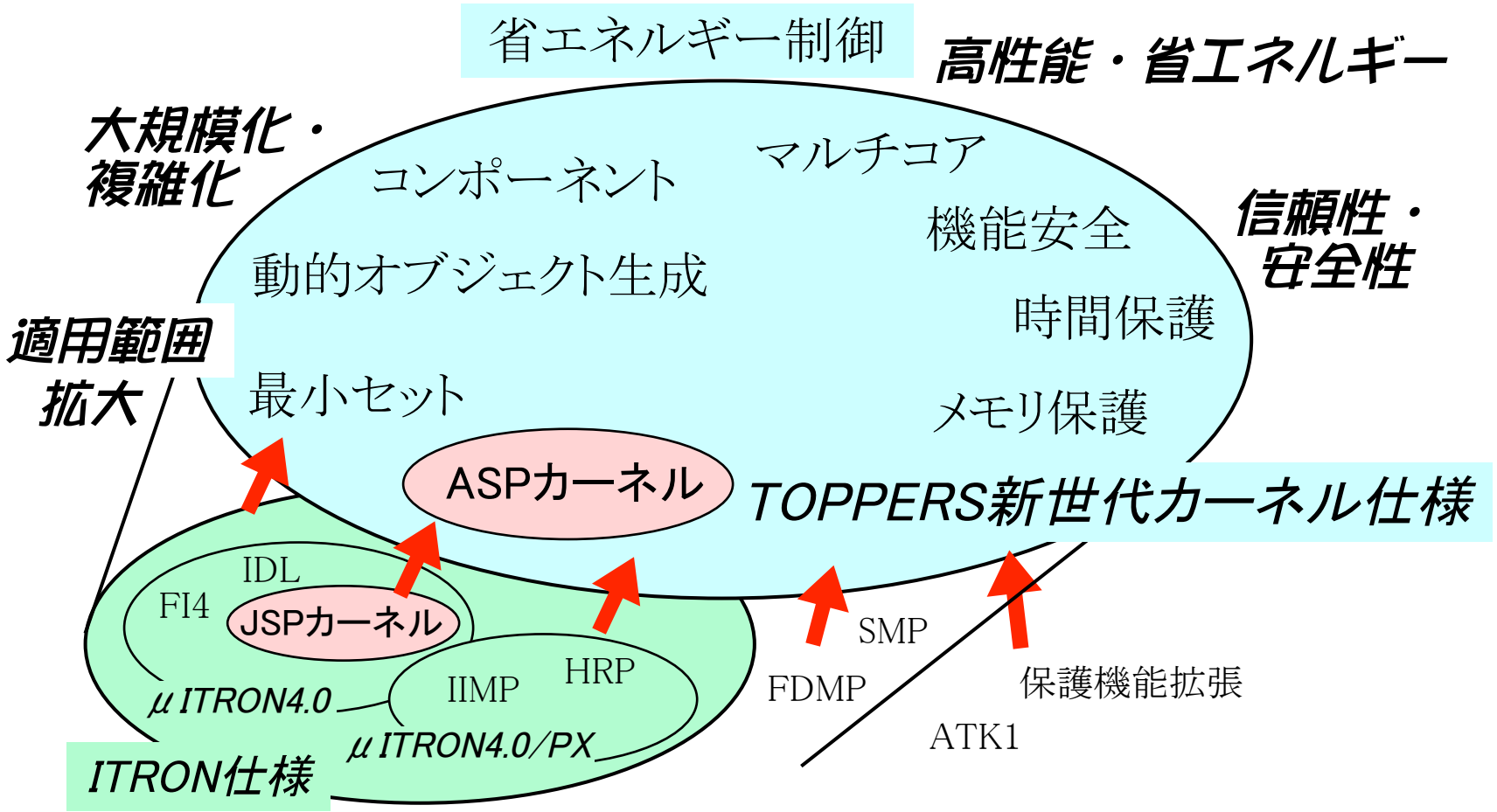
- マルチコアプロセッサ対応
- 保護機能（メモリ保護，時間保護）
- 機能安全対応，省エネルギー制御
- コンポーネントシステム対応

μITRON4.0仕様で完成度が低かった箇所の改良

- システムコンフィギュレーション手順など

*➔これらの要求にこたえる新しいカーネル仕様が必要*

# TOPPERS新世代カーネル仕様の位置付け ～ ITRON仕様からの発展



# TOPPERS新世代カーネル仕様の設計方針

(1) μITRON4.0仕様をベースに拡張・改良を加える

- 多くの実績があるμITRON4.0仕様をベースに
- μITRON4.0仕様の不十分な点は積極的に拡張・改良

(2) ソフトウェアの再利用性を重視する

- ソフトウェアの再利用性向上のために，少々のオーバヘッドがあっても，ターゲット依存項目を減らす

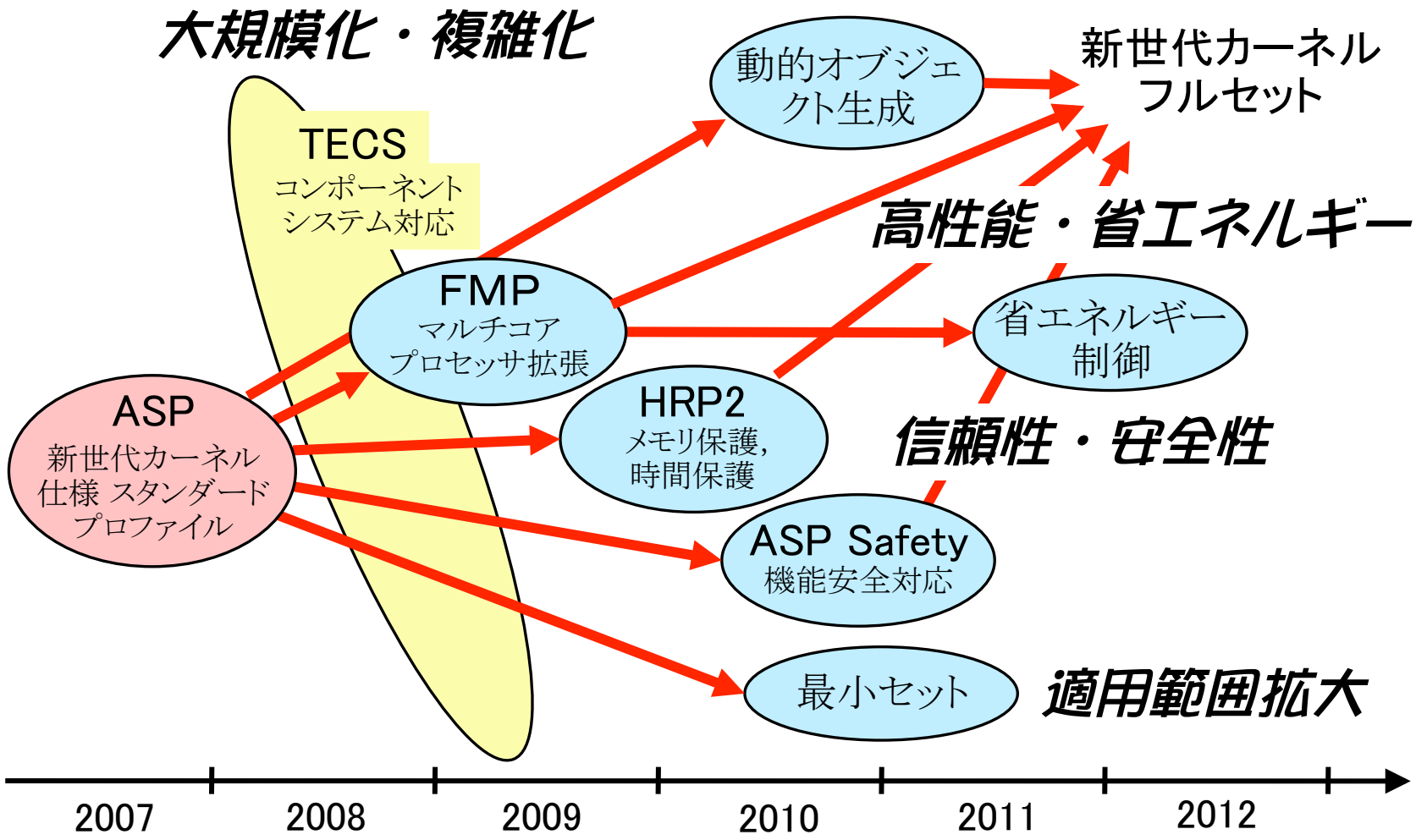
(3) 高信頼・安全なシステム構築を支援する

- アプリケーションに誤用されにくい仕様とする
- 妥当なオーバヘッドで救済できる誤用は救済する

(4) アプリケーション構築に必要な機能は積極的に取り込む

- 多くのアプリケーションに共通に必要な機能を実装
- ただし，(1)～(3)の方針を満たすことが前提

# TOPPERS新世代カーネル開発ロードマップ




※ リリース前のカーネルの名称は仮称

# TOPPERS新世代カーネルの開発状況

## TOPPERS/ASPカーネル

- TOPPERS新世代カーネルの出発点（基盤）となるリアルタイムカーネル
- TOPPERS/JSPカーネル（μITRON4.0仕様 スタンダードプロファイル）に対して，信頼性・安全性・ソフトウェアポータビリティ向上のための各種の拡張・改良
  - 割込み処理機能を「TOPPERS標準割込み処理モデル」によりプロセッサによらず標準化
  - 信頼性・安全性の向上については細かな改良の積み重ね
  - いくつかの独自の機能拡張
- 5月にRelease 1.7.0の配布を開始
  - 拡張パッケージにより，オブジェクトの動的生成機能や制約タスクをサポート

## TOPPERS組込みコンポーネントシステム（TECS）

- 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
- 2009年6月に仕様書とツールを配布開始
- 6月に配布開始予定のバージョンでは，分散システム開発を支援するための遠隔手続き呼出しをサポート

## TOPPERS/FMPカーネル

- マルチプロセッサ対応のリアルタイムカーネル
- すでに携帯電話機に採用された事例
- TTSP（後述）による検証がほぼ完了
- 近日中に配布開始予定のRelease 1.2.0は，さらに安定性を増したものに

## TOPPERS/HRP2カーネル

- 高信頼システム向けに，各種の保護機能（メモリ保護機能とオブジェクトアクセス保護機能，オーバランハンドラ機能など）を持ったリアルタイムカーネル
- 現在，開発の最終段階
- 近日中に正式版（Release 1.0）の会員向けの早期リリースを開始する予定

## TOPPERS/ASP Safetyカーネル（機能安全対応）

- （株）ヴィッツが機能安全規格IEC 61508のSIL 3に準拠したソフトウェアプロセスに基づいて開発
- ASPカーネルの機能を徹底的な検証が可能な範囲にサブセット化したもの
- 2010年12月から会員向けに早期リリース

## 動的オブジェクト生成

- ASPカーネル Release 1.7.0の拡張パッケージの形で，5月にリリース
- 追加した静的APIとサービスコール
  - AID_*YYY* … 割付け可能なオブジェクトIDの数の指定
  - acre_*yyy* … オブジェクトの動的生成
  - del_*yyy* … オブジェクトの削除
  - def_*yyy* … オブジェクトの定義
- 動的に変更できないもの
  - 割込みハンドラの定義（def_inhはサポートしない．割込みサービスルーチンの動的生成・削除は可能）
  - CPU例外ハンドラの定義（def_excはサポートしない）
  - 割込み要求ラインの属性（cfg_intはサポートしない）

## TOPPERS/SSPカーネル（最小セット）

- 機能を最小限に絞り込んだリアルタイムカーネル
  - 制約タスク（待ち状態を持たないタスク）のみ
  - 優先度毎のタスク数を1つに制限
- TOPPERS公募型事業の採択テーマとして開発中
- 近日中に早期リリースを開始する予定

## 省エネルギー制御

- 名古屋大学 組込みシステム研究センター（NCES）が中心になって実施した組込みシステムの消費エネルギー最適化の研究において，TOPPERS新世代カーネルに省エネルギー制御機構を組み込む方法を提案
- 今後，実用化できる技術へと発展させていく計画

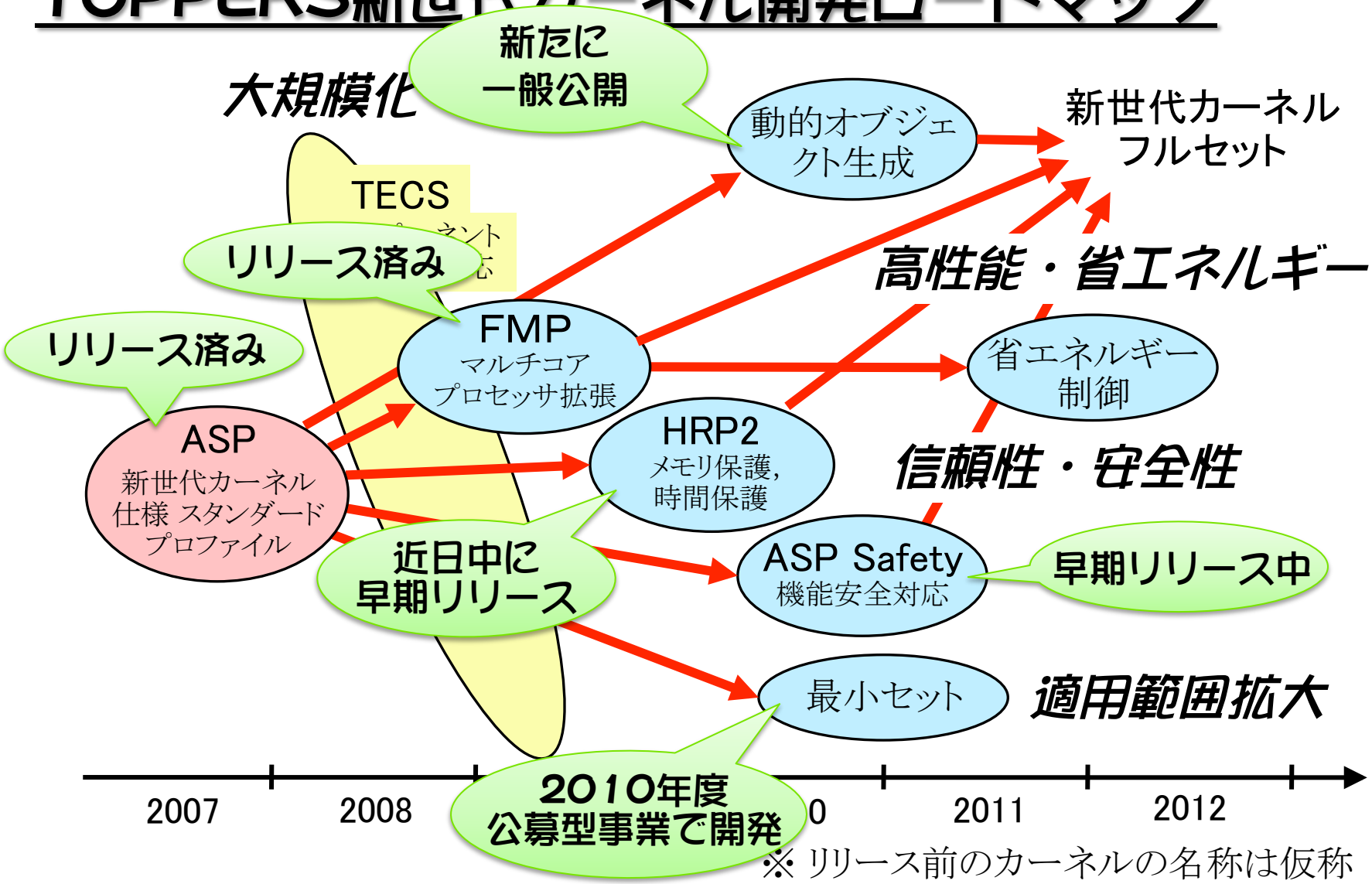
## TOPPERS新世代カーネル統合仕様書

- TOPPERS新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
- 5月に配布を開始したRelease 1.3.0で，ASP（拡張パッケージを含む），FMP，HRP2の3つのカーネルの仕様をカバー
  - すでにμITRON4.0仕様書を越えるボリュームに
- 今後の計画
  - SSPカーネルの仕様記述を追加
  - 要求事項にタグを付与する（トレーサビリティのため）
  - マルチコア，保護機能，動的生成の組み合わせについて未検討部分が残っている

## TOPPERSテストスイートパッケージ（TTSP）

- TOPPERS新世代カーネルのテストスイート
- テスト品質と保守性を向上させるために，独自の記法によるテストシナリオから，ツールによりテストプログラムを生成する形態
- 本日付けで，ASPカーネルの仕様を網羅するためのテストシナリオと，テストプログラム生成ツールを含むパッケージの配布を開始
  - 1779件のテストケースを含む
  - 統合仕様書やASPカーネルの不具合発見に貢献
- FMPカーネルに対するテストスイートの開発も完了しており，1年後に配布開始する予定

# TOPPERS新世代カーネル開発ロードマップ



# 組込みシステムの今後と TOPPERSの今後の活動指針

# TOPPERSプロジェクトのこれまでと現状

## 第１期：ITRON仕様の実装

- 1999年頃：μITRON4.0仕様に準拠したリアルタイムカーネルの開発を開始
- 2000年11月：JSPカーネルとして公開
- 2003年9月：NPO法人 TOPPERSプロジェクト発足
- 2004年4月：FI4カーネル，ATK1（OSEK仕様）

## 第２期：TOPPERS新世代カーネル

- 2006年頃：TOPPERS新世代カーネルの開発を開始
- 2007年11月：ASPカーネルを早期リリース，TOPPERS新世代カーネル開発ロードマップを公表
- 2011年6月（現在）：開発ロードマップの大部分を達成

***第３期へ進むべき時期に来ている***

# 組込みシステムの今後の変化

！組込みシステムの社会インフラ化

## 制御と情報処理の統合（統合システム）

- 持続可能な社会の実現を目指して，情報通信技術と組込みシステム技術を活用したスマート社会を構築することが世界的な流れ
  - スマートグリッド，エネルギーITS，スマート…
- 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（System of Systems）の構築が重要に
  - 欧米の学会では，Cyber Physical Systemと呼ばれている
- このようなシステムは，社会インフラ化すること，物理的な世界とつながることから，より高いディペンダビリティが要求される

➔日本が強みが生かせる分野なのでは？

## ネットワークによる機能再配置 ← クラウドコンピューティング

- 個々のサービスの高度化・複雑化はさらに進むと思われる
- すべての機器がネットワーク接続されれば，すべての機器が汎用・多機能である必要はない
  - 機器に求められる機能（サービスのアーキテクチャ）が大きく変わる可能性

! パラダイムチェンジの時期の見極めが難しい

  - 中途半端にネットワーク接続されている状態では，パラダイムチェンジは起こらない

## 消費電力あたりの性能の向上

- 組込みシステム自身の消費エネルギー削減も求められる
- そのためには，新しいハードウェア技術の導入が必要

# 次の10年を見据えた活動指針

## 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

# Safety & Security

## 確認）情報セキュリティ（information security）とは？

- 情報の機密性，完全性および可用性の維持（JIS X 5080）
- 機密性（confidentiality）
  - アクセスを認可された者だけが情報にアクセスできることを確実にすること
- 完全性（integrity）
  - 情報及び処理方法が，正確であること及び完全であることを保護すること
- 可用性（availability）
  - 認可された利用者が，必要なときに，情報及び関連する資産にアクセスできることを確実にすること
- さらに，真正性，責任追跡性，否認防止，信頼性などの特性の維持を含める場合も（ISO/IEC 27001）

## 組込みシステムにおける安全性とセキュリティ

- 制御系組込みシステムにおいては，安全性（safety）が重視されてきた一方で，情報セキュリティはあまり重視されてこなかった

## 今なぜ情報セキュリティか？

- 進むネットワーク接続
  - ネットワークを通じたセキュリティ上の攻撃は，原因と影響の範囲を絞りにくい
- 部品（ソフトウェアプラットフォーム，ネットワーク，マイコン）の標準化
  - 技術情報が入手しやすく，攻撃が容易に
- 個人情報や企業秘密の流出に対する社会意識の変化
  - 個人情報流出は，大きな損害につながる

## 組込みシステムに対する情報セキュリティ上のリスク

- セキュリティ攻撃によるシステムの誤動作
  - システムの脆弱性を利用して，システムを誤動作させる（ソフトウェアを不正に書き換えて誤動作させることも）
  - 安全に関わる制御系組込みシステムでは，安全性にかかわる事態につながるおそれ
- 個人情報の流出，価値のある情報の流出
  - 組込みシステムの中には，個人情報を保持しているものも多い（携帯電話機，カーナビ，…）
  - 例えば，工場の稼働状況の情報が流出したら…
- その他の脅威の例
  - セキュリティ機器の機能喪失（誤動作の一種と捉えることも）
  - 組込みシステムをセキュリティ攻撃の踏み台に利用

## 安全性とセキュリティの両立の困難

- 安全性は厳密なリスク評価を要求する
- セキュリティリスクの厳密な評価は難しい

  $$リスク = 重大度 \times 脆弱性 \times 脅威$$

  - 脆弱性（セキュリティ上の問題を起こす可能性のあるシステムの弱点）と脅威（脆弱性を利用してリスクを現実化させる手段）の評価手法が確立していない
  - 脅威は時間とともに変化する

## 安全性とセキュリティの両立に向けて

- セキュリティリスクの評価手法の確立
- システムのアーキテクチャからの考慮
- セキュリティ対策に対する相場観の醸成
- 変化する脅威に対応する仕組みの導入

# Ecology（高エネルギー効率）

## マルチコア，（さらには）メニーコアへ

- 高速なプロセッサはエネルギー効率が悪い
  - 1GHzのプロセッサ1つよりも，200MHzのプロセッサ5つの方が消費電力が小さい
  - 50MHzのプロセッサ20個の方がさらに小さい
- アプリケーションをどのように開発するかが最大の課題
  - OSだけでなく，ソフトウェア開発環境/ツールの研究開発も重要

## 省エネルギー制御

- 急いで処理する必要がない場合には，ゆっくり処理をする
  - （状況にもよるが）消費エネルギーを小さくできる
- システム全体の状況を把握できるのはOSなので，OSでサポートすることが必要

# Connectivity

## Smart Futureの大前提

- 小さいコスト，小さい消費エネルギー，高いディペンダビリティでのネットワーク接続が，Smart Futureに重要
- ソフトウェアプラットフォームと開発技術も，ネットワークを前提としたものに
- 各種のネットワークへの対応が必要
  - インターネット
  - リアルタイム制御系ネットワーク
  - 無線系ネットワーク

# 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

## これまでのソフトウェア開発形態と課題

- ソフトウェアやその部分毎に，プロジェクトメンバ（研究教育機関 or 企業 or 個人）が担当
- 組込みソフトウェアの大規模化・複雑化により，1つの組織だけで開発するのが難しい状況が増えている

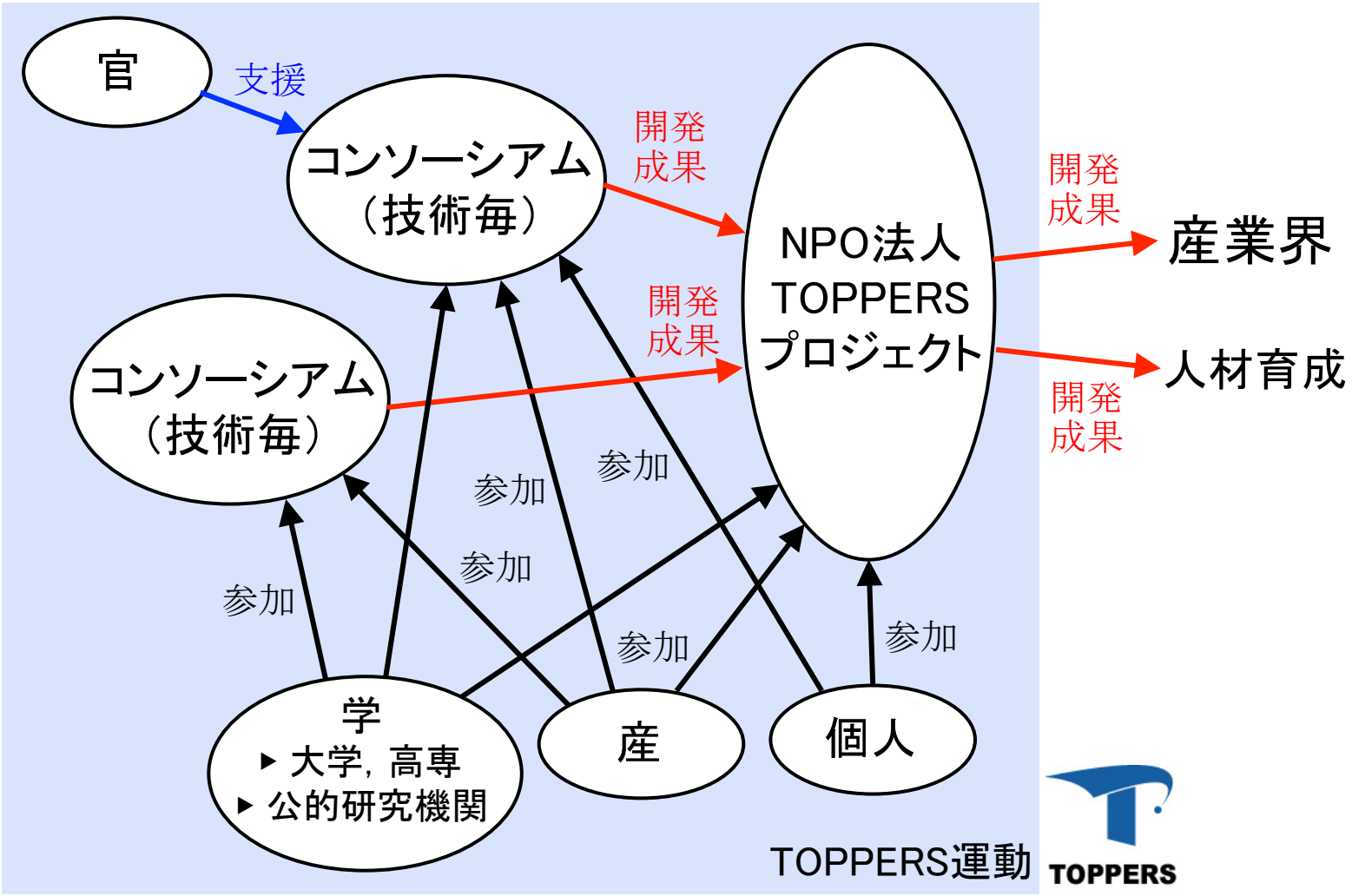
## コンソーシアムによるソフトウェア開発

- 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
- できたソフトウェアは，TOPPERSプロジェクトからOSS化

## NPO法人 TOPPERSプロジェクトの役割

- 産業界へ提供・普及する窓口
- プロジェクト全体の枠組みや方向性を定めるハブ

# コンソーシアムによるOSS開発

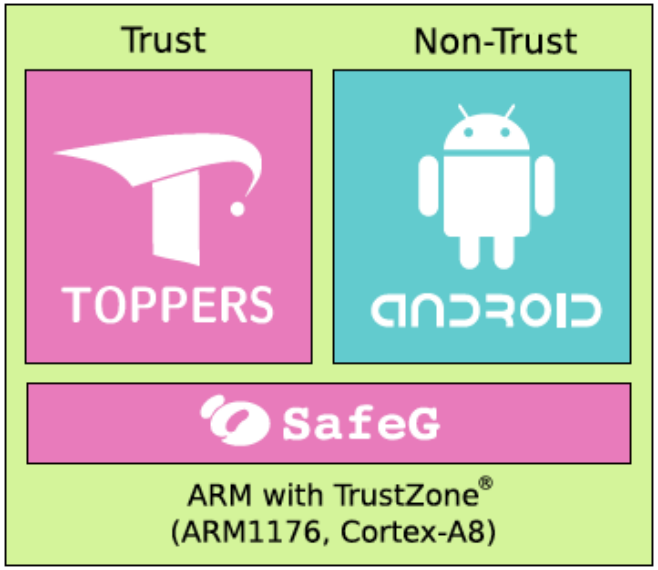


# 今後の活動指針に沿った活動事例

# SafeG：高信頼組込みシステム向けデュアルOSモニタ

## SafeGとは？

- 1つのマイクロプロセッサ上で，汎用OSとRTOSを安全に共存して動作させるデュアルOSモニタ
- 名古屋大学 組込みシステム研究センター（NCES）と，高田研究室で開発




## SafeGの最大の特徴

- ARM TrustZone技術を用い，RTOSをTrust状態，汎用OSをNon-Trust状態で実行し，RTOSと汎用OSを時間的・空間的に分離
- 汎用OSにバグやセキュリティホールがあり，汎用OSのカーネルが誤動作したり，特権モードで不正なプログラムが動作しても，RTOS側を保護できる

## 開発の背景

- 最近の組込みシステムは，ネットワークに接続することで豊富な機能を提供することが求められる一方で，高い安全性やリアルタイム性が必要な処理も実行する必要
- ネットワーク接続による豊富な機能の実現と高信頼性の確保という相反する要求に，1つのOSだけで応えることは難しい
- LinuxやWindowsのような汎用OSと，ITRON仕様やAUTOSAR仕様のようなRTOSを併用するアプローチが有効
- 仮想マシン（VM）やハイブリッドOSの技術は，実行時オーバヘッドが大きいという問題や，OS自身の不具合には対処できないという問題がある

## SafeGのその他の特長

- RTOS側のリアルタイム性を保証
  - RTOS側の割込みが常に優先され，それによりOSの切換えを行うため，汎用OSの実行によって，RTOS上で動作するアプリケーションのリアルタイム性が阻害されない
- 小さい実行時オーバヘッド
  - ARM TrustZone技術を活用することによって，OS間の切換え時間が1～2μ秒程度（ARM1176JZF-S，210MHzで測定）
- 汎用OSに加える修正が少ない
  - 汎用OSのバージョンを上げる必要がある場合にも，容易に追従することができる
- SafeG自身は小規模で信頼性確保が容易
  - SafeG自身は，コードサイズ（バイナリ）が1.5KB以下と小規模なソフトウェアで，信頼性を確保することが容易

## 今回リリースするSafeG

- シングルコアプロセッサのみに対応
- 汎用OSとしてLinuxおよびAndroidを，RTOSとしてTOPPERS/ASPカーネルを用いている

## 今後の開発計画

- OS間通信機能，より柔軟なスケジューリング機構，マルチコアプロセッサのサポートなどの開発が進行中
  - 順次リリースする計画
- NCESでは，NCESと共同でSafeGの開発を進める企業を募集中．SafeGをテーマにコンソーシアム型共同研究を実施することも検討

# 次世代車載システム向けRTOSに関するコンソ

## 活動の位置づけと名称

- 名古屋大学 組込みシステム研究センター（NCES）が設定した研究開発テーマに，複数の企業の参加を得て研究・開発を進めるコンソーシアム型共同研究
- 次世代車載システム向けRTOSの仕様検討および開発に関するコンソーシアム型共同研究（略称：ATK2コンソ）

## 参加企業（2011年5月時点，五十音順）

- （株）ヴィッツ
- （株）OTSL
- （株）サニー技研
- （株）デンソー
- （株）東芝
- トヨタ自動車（株）
- 日本電気通信システム（株）
- パナソニック アドバンストテクノロジー（株）
- 富士ソフト（株）
- 富士通VLSI（株）
- ルネサス エレクトロニクス（株）

## 研究開発の内容

- AUTOSAR OS仕様をベースとした次世代の車載組込みシステム向けのRTOS仕様の策定
- 策定した仕様に基づいたRTOSの実装と評価
- 検証スイートの開発

## ベースとする研究開発成果

- TOPPERS新世代カーネル
- NCESで開発したAUTOSAR仕様ベースのRTOS仕様と実装
  - マルチコアプロセッサにも対応．国際的にも最先端の技術であると自負
- NCESを中心とするコンソ型共同研究で開発したRTOSの検証支援ツールと検証スイート（TTSP）

## 研究開発体制

- 参加企業から，計12名の技術者がNCESに常駐（内2名はハーフタイムでの従事）
- 名古屋大学の教員・研究員8名が参加（内1名がフルタイムで従事）

## プロジェクトの期間

- まずは，2011年4月～2012年3月
- 進捗や成果を見て，次年度以降の継続について検討
  - できれば，3年程度継続して，RTOSのみではなく，COM等のミドルウェアの開発も行いたい

## 研究開発成果の取扱い

- 開発したRTOS（検証スイートを除く）は，開発終了後，TOPPERSプロジェクトより，TOPPERS/ATK2の名称でオープンソースソフトウェアとして一般公開

# おわりに

# まとめとこれからの課題

## 今後の活動指針を提示

- 運営委員会等での議論を踏まえて，TOPPERSプロジェクトの今後の活動指針を策定・提示
- ご意見は大歓迎

## これからの課題

- 活動指針から開発項目への落とし込み
  - ニーズ調査が必要
  - ご意見は大歓迎
- ソフトウェア開発体制の強化
  - 開発に参加する会社が儲かる仕組み作り

# (共同) 開発者を募集

- TOPPERSのソフトウェア開発に参加して下さる会社を募集
  - コンソーシアム型開発への発展の可能性も

## 具体的な開発案件(現時点での主なもの)

- 次世代のリアルタイムOS
  - TOPPERS新世代カーネル
  - 次世代車載システム向けRTOS
- 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プラットフォームと開発支援ツール
  - SafeG
  - TLV(トレースログ可視化ツール)
  - ScheSim(スケジューリングシミュレータ)
- 技術者育成のための教材開発