オープンソース　保護OS

メモリ保護と時間保護を有する自動車向けリアルタイムOS

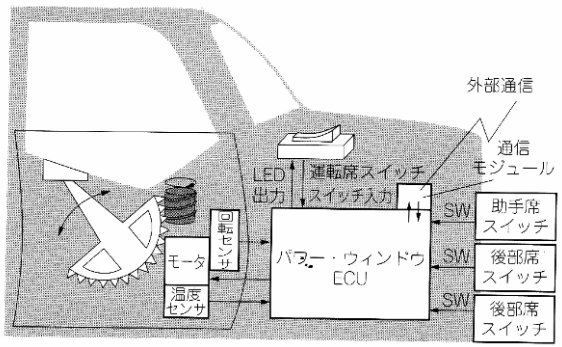
株式会社ヴィッツ
服部博行

自動車に使われているコンピュータ

80年代：エンジン制御、トランスミッション制御

90年代：ナビ、ブレーキ制御、ハイブリッド（HV）

2000年～：HV化、先進安全システム、IT・ITS連携システム



従来モータとスイッチで構成されていた機能にもECUは使われている。

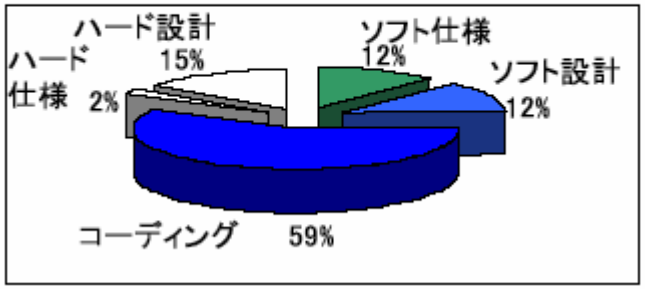
これは安全性を確保するため、挟み込みを防止したり、快適性をえるためにエアコンなどと協調する場合がある

ＥＣＵ間は通信をして複雑な連携が必須

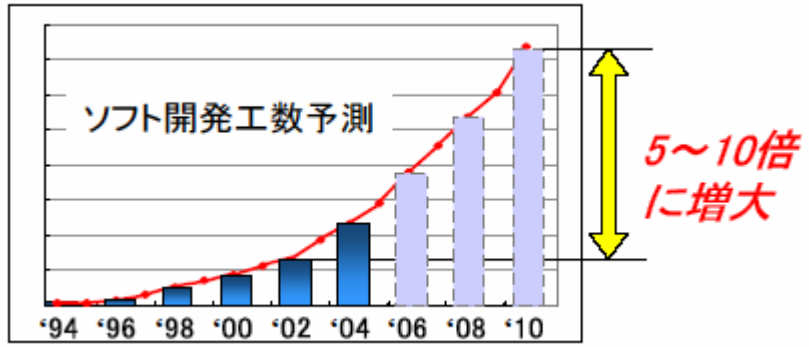
自動車制御システムが抱える問題点

株式会社 ヴィッツ

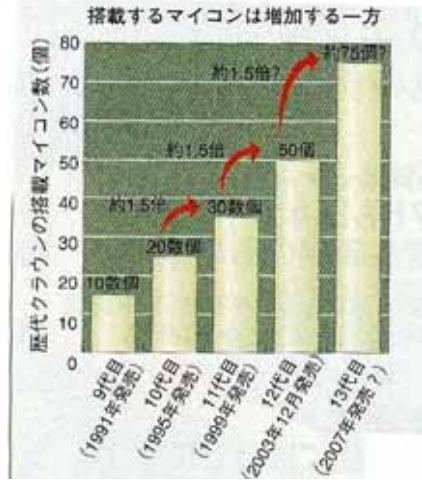
ECU開発工数の 8割以上がソフトウェア開発



引用：2005/1/24 JasPar 自動車制御ソフト・車載LAN標準化活動　トヨタ自動車　谷川浩
日経エレクトロニクス 2004/3/1 トヨタインサイド



- ECU数増大
  ⇒ 車両への搭載限界（ｽﾍﾟｰｽ、W/H・バス負荷等）
- ソフトウェア開発工数の増大
  ⇒ 車両開発の**ボトルネック化懸念**



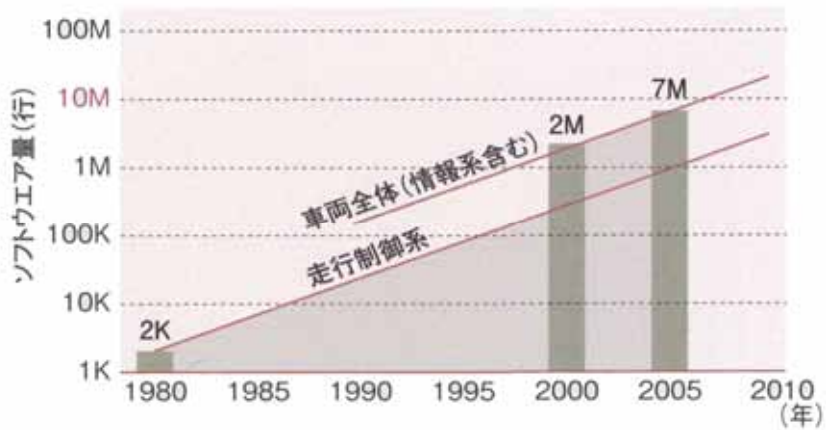
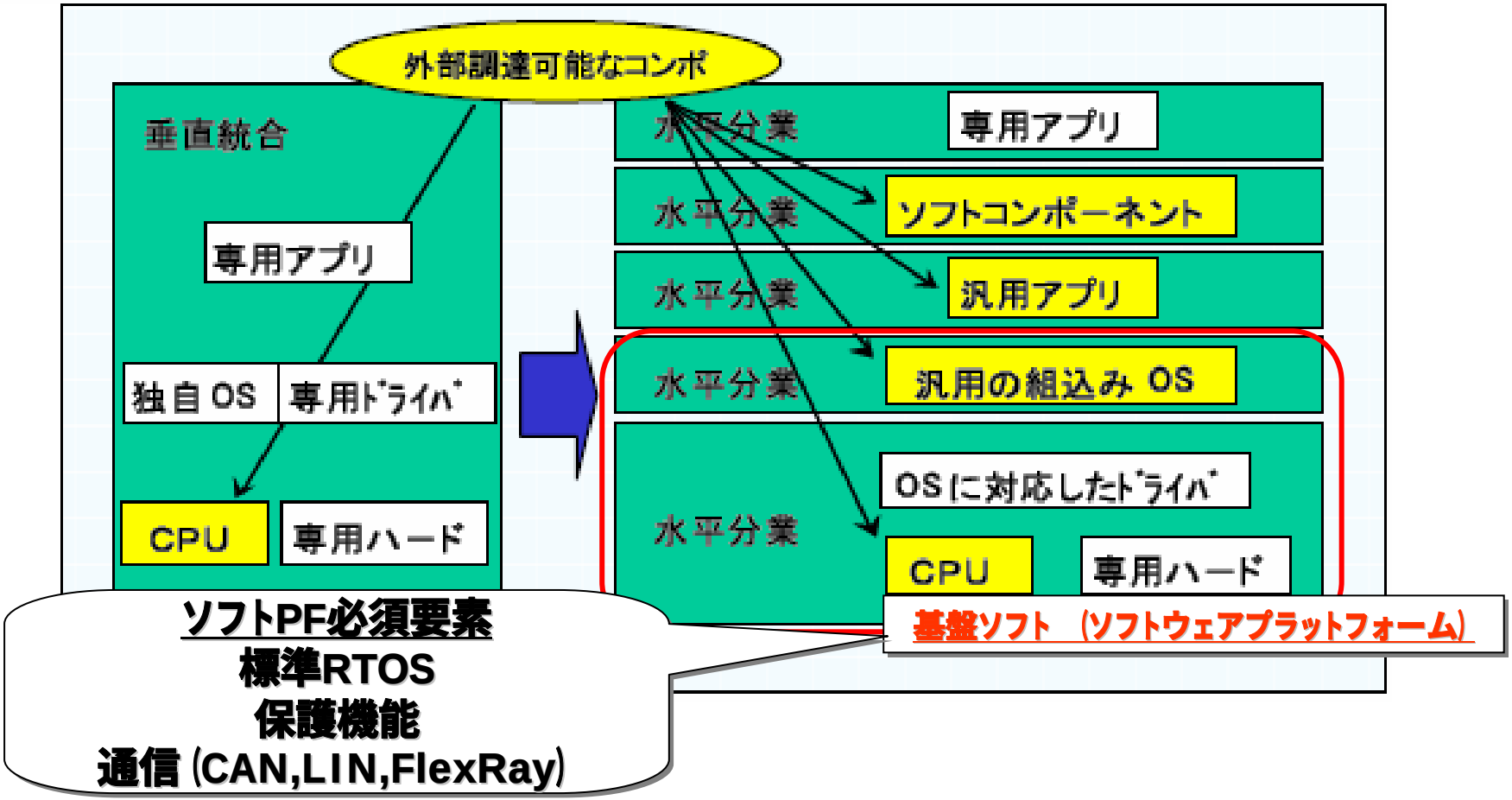


図1　クルマ1台当たりのソフトウエア量（日産自動車の場合）
1980年はECUのソフトウエアだけで2000行程度だった。ソフトウエア量の多いカーナビが登場したことで、2000年には制御系ECUと合わせて200万行にまで増えた。20年で約1000倍に膨れ上がった。今後もソフトウエア量は増え続ける。

ソフトウェア開発量を抑えるソフトウェアプラットフォーム (SFP) 化

株式会社 ヴィッツ



SFP化によるメリット

ソフトウェア部品流通

ソフトウェアの部品化による開発コードの抑制

SPF化だけでは解決できない問題点

株式会社 ヴィッツ

SFP化で解決もしくは軽減できる問題

・ソフトウェアの部品化促進、共通化、標準化

！ソフトウェアの専用開発、テスト工数などの抑制が可能となる

ECU数の増加問題はSPFでは解決もしくは軽減できない

ECU問題はECU統合で解決する

トヨタ自動車　レクサスLS460では、3つのECU統合を実施

以下は、その統合例

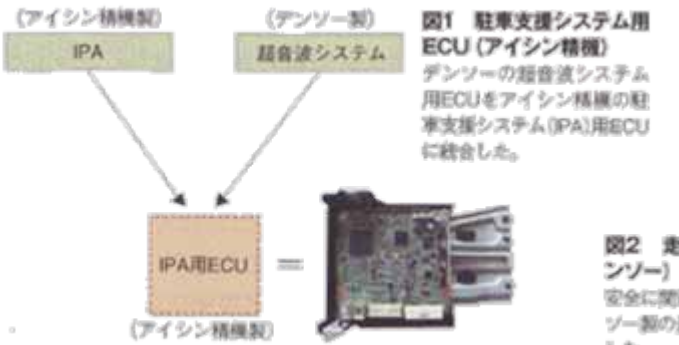


図1　駐車支援システム用ECU（アイシン精機）
デンソーの超音波システム用ECUをアイシン精機の駐車支援システム（IPA）用ECUに統合した。

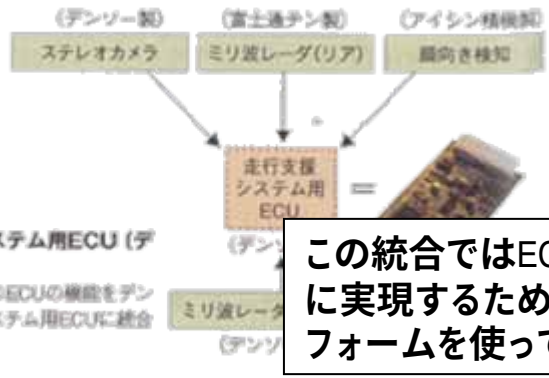
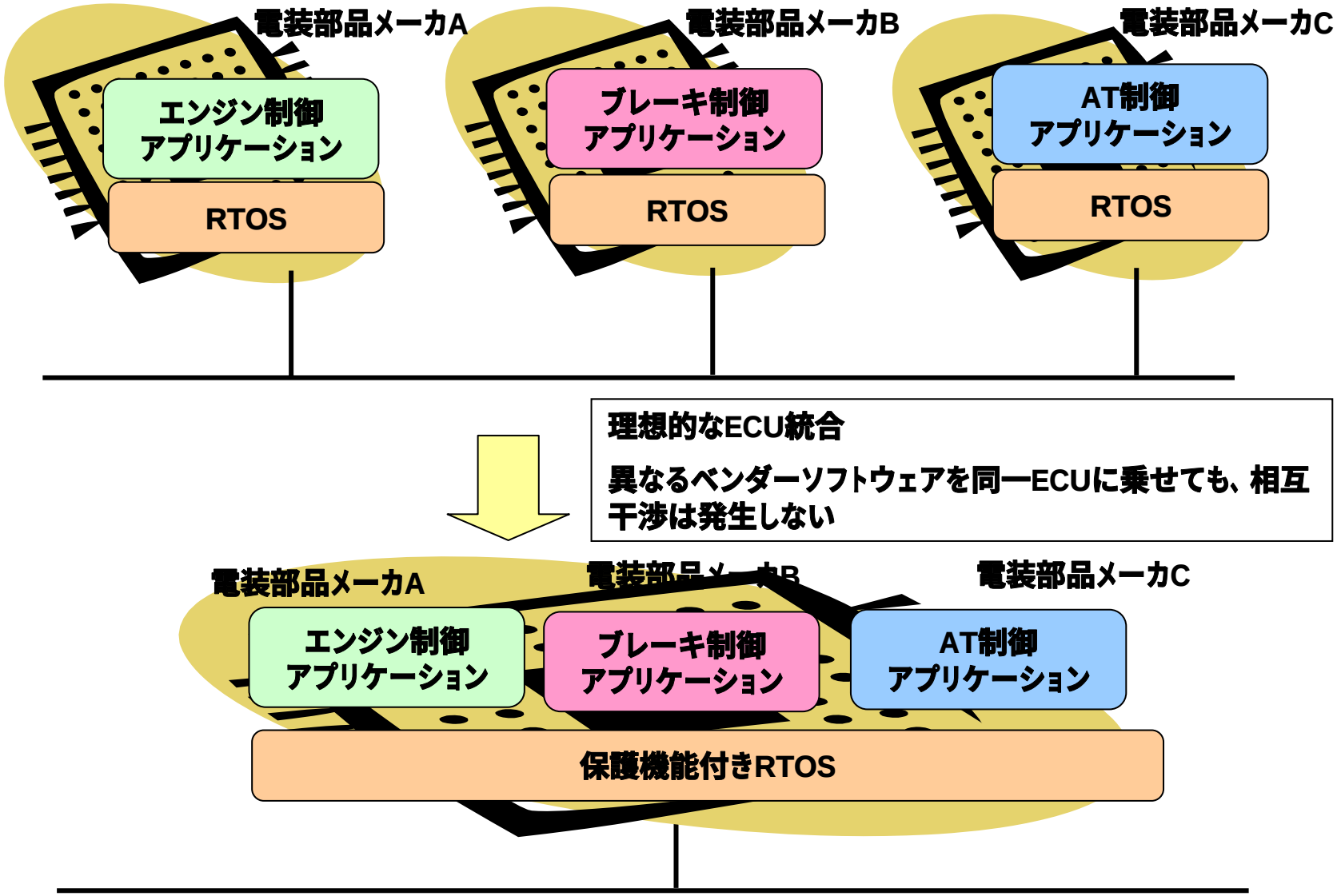


図2　走行支援システム用ECU（デンソー）
安全に関連する複数のECUの機能をデンソー製の走行支援システム用ECUに統合した。

この統合ではECU統合を安全且つ容易に実現するための保護機能付きプラットフォームを使っているとの発表はない

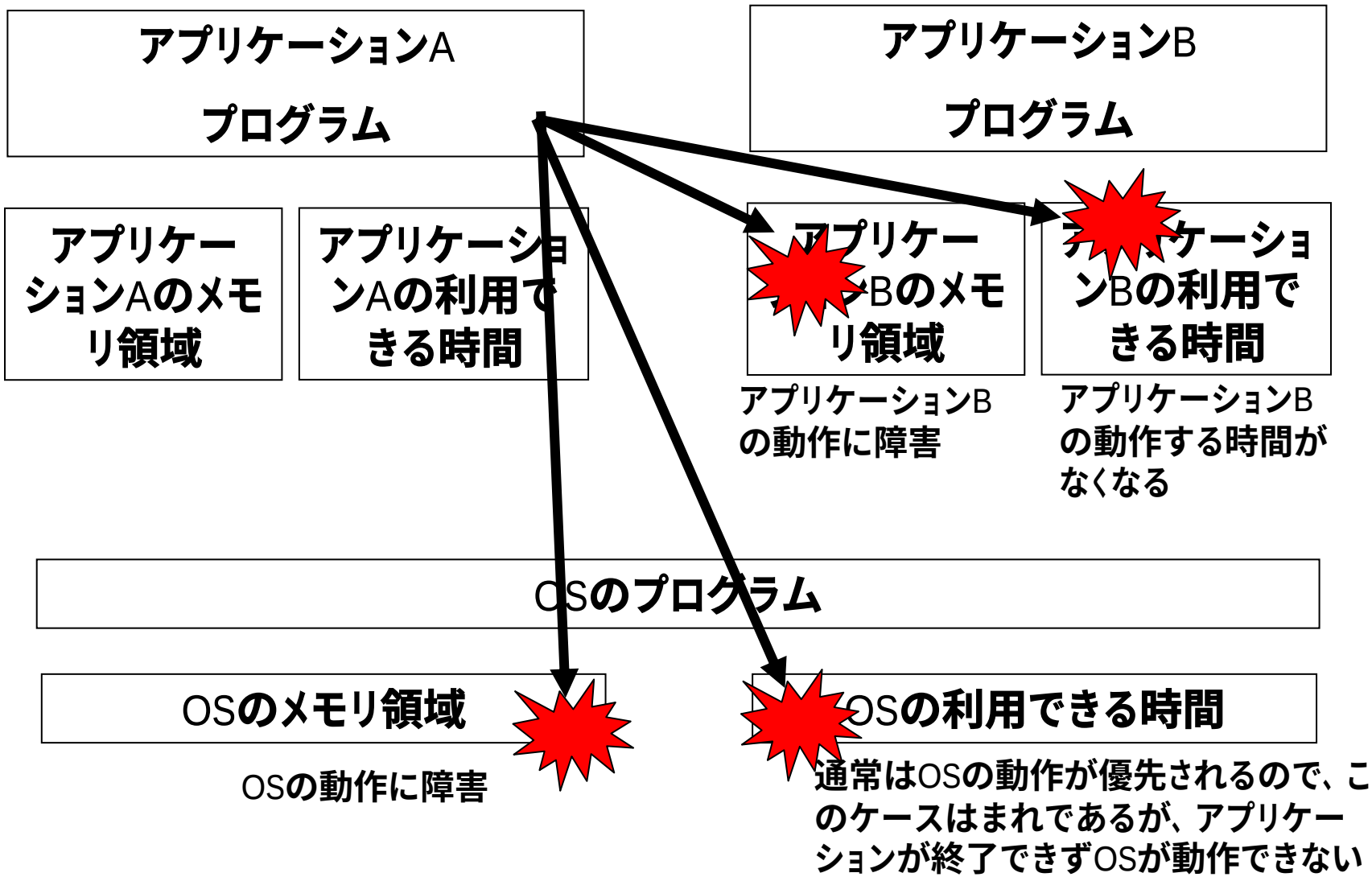
出展:　日経 Automotive Technology 2007/11

ECU統合とは


電装部品メーカA
エンジン制御
アプリケーション
RTOS
電装部品メーカB
ブレーキ制御
アプリケーション
RTOS
電装部品メーカC
AT制御
アプリケーション
RTOS
理想的なECU統合
異なるベンダーソフトウェアを同一ECUに乗せても、相互干渉は発生しない
電装部品メーカA
電装部品メーカB
電装部品メーカC
エンジン制御
アプリケーション
ブレーキ制御
アプリケーション
AT制御
アプリケーション
保護機能付きRTOS

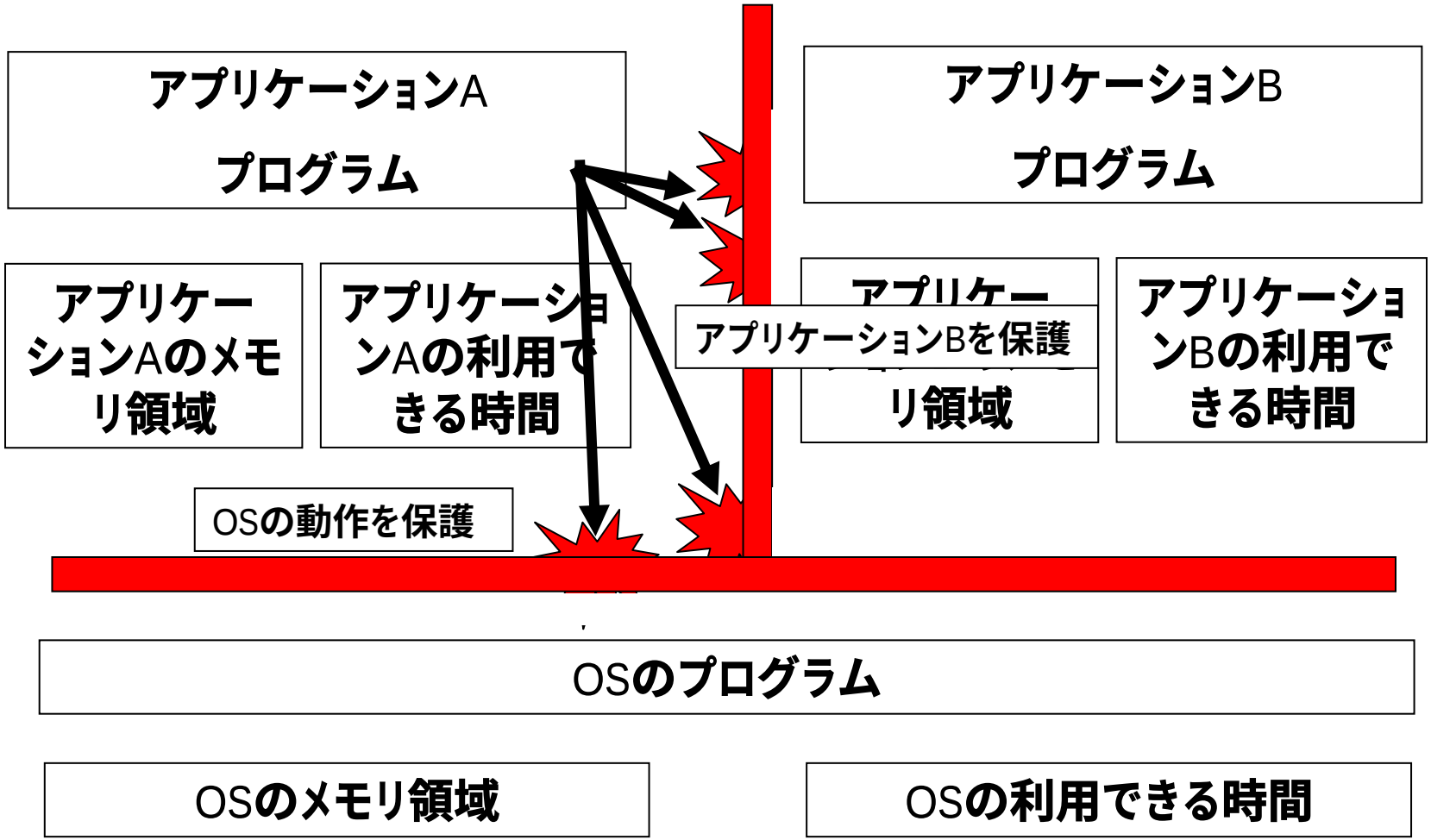
ECU統合に必要な保護機能

株式会社 ヴィッツ



ECU統合に必要な保護機能

株式会社 ヴィッツ

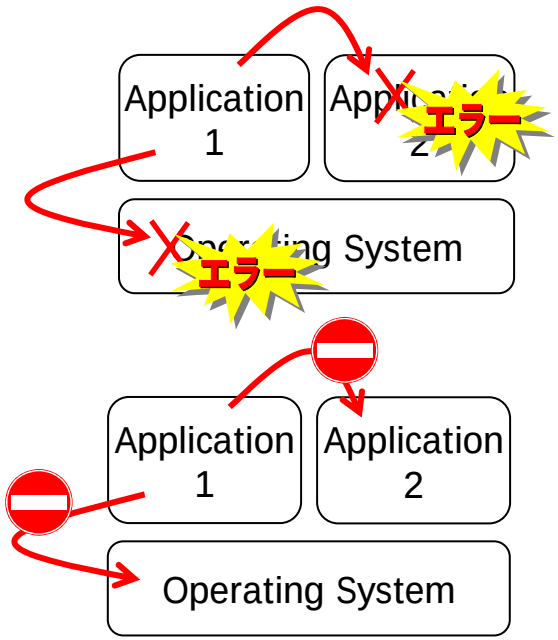


メモリ保護 機能概要

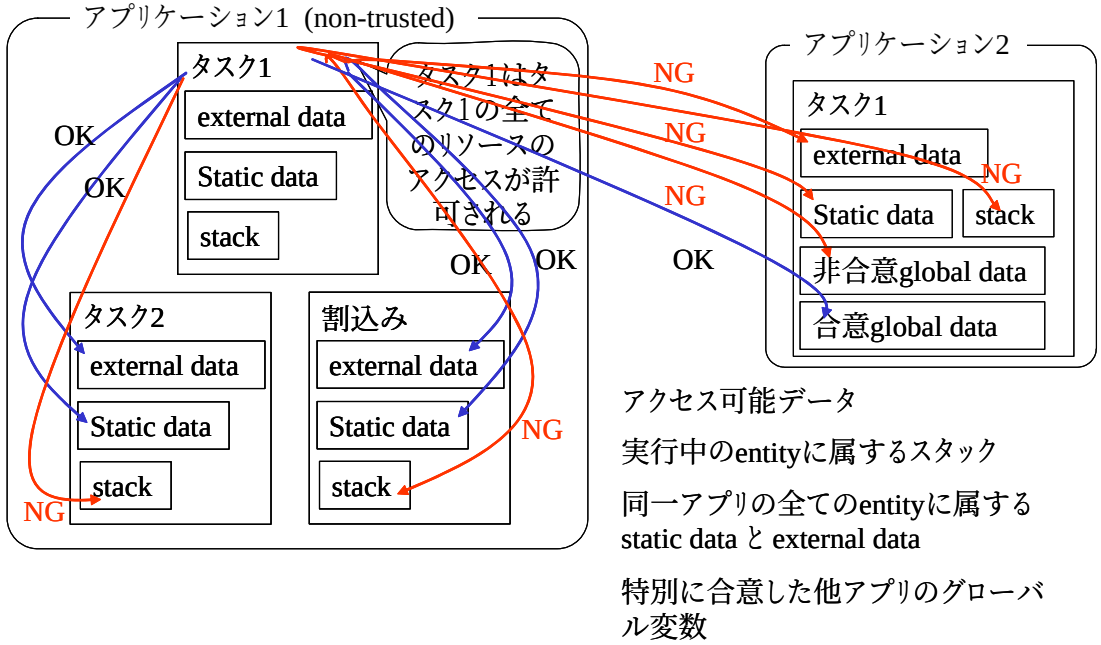
株式会社 ヴィッツ

＜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



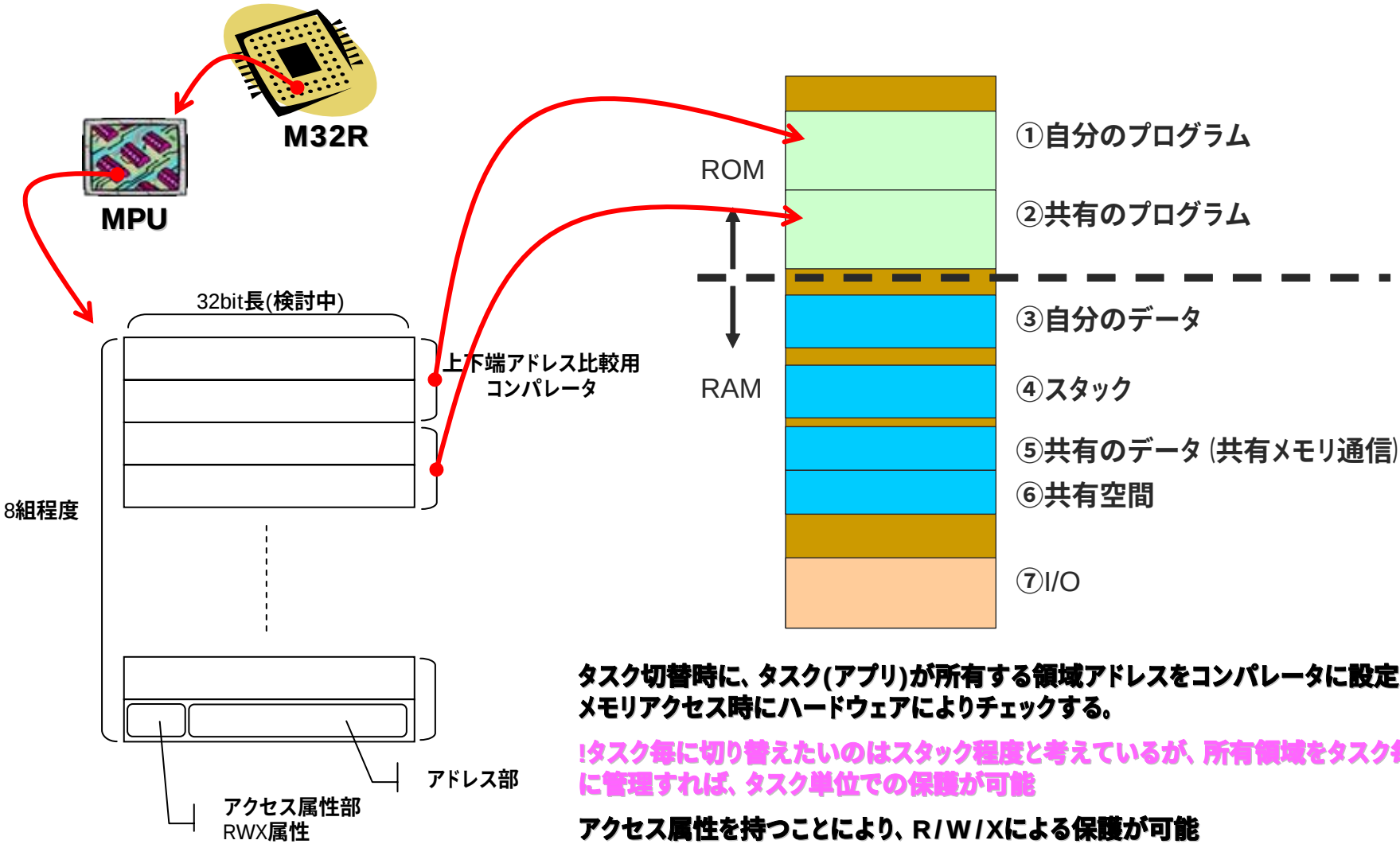
HISのメモリ保護 (HISの保護は書込みのみ)

HISの保護を拡張し、Writeに加え、
Rread,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)

メモリ保護 の実現方法

株式会社 ヴィッツ



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

時間保護

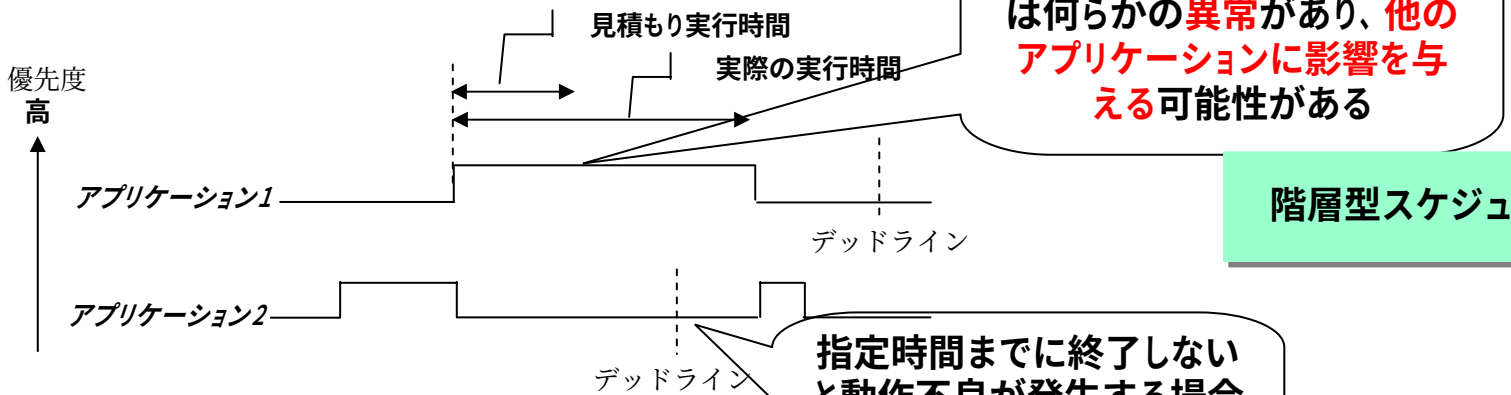
時間保護：処理単位のプロセッサ実行時間を保護（保証）すること

ECU統合時のアプリケーション開発の注意点

・他のアプリケーション実行時間に影響をあたえてはいけない

・処理要求から完了までの時間を守らないとシステムが破綻する場合がある

時間保護には上記2種類の要求を満たすために、以下の2種類が必要



見積もり実行時間を越えるのは何らかの異常があり、他のアプリケーションに影響を与える可能性がある

階層型スケジューラ

指定時間までに終了しないと動作不良が発生する場合など、デッドラインまでの終了を確認するのは重要

HIS
デッドラインモニタリング

ただし、デッドラインモニタリングは監視機能であり、厳密な時間保護とは言えない

デッドラインモニタリングによる時間保護

株式会社 ヴィッツ

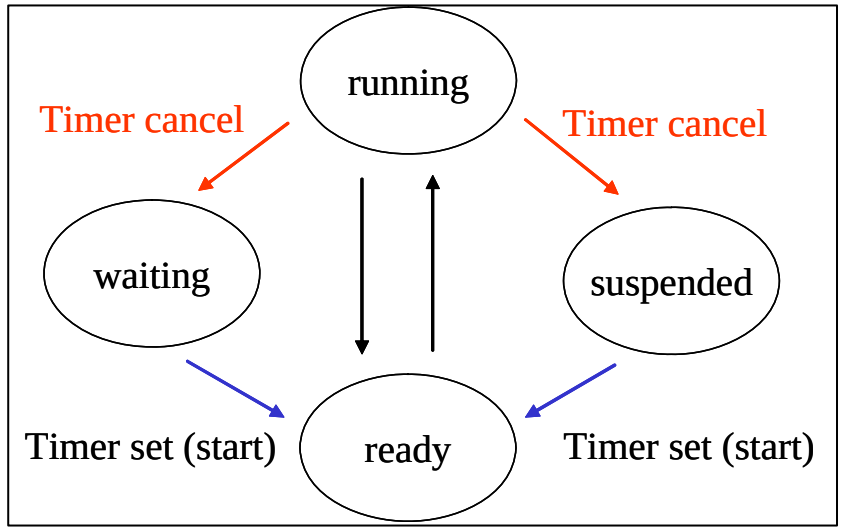
＜時間監視機能＞

・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 (エクスパイヤ)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

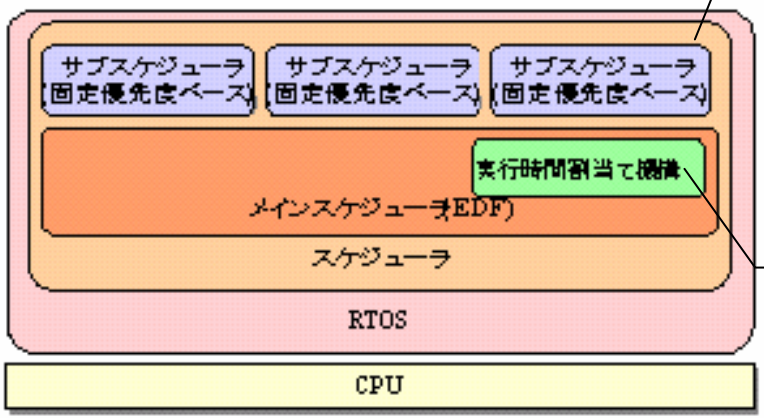
この方式は、デッドラインまでに処理の完了を確認するには良い方法。しかし、保護という意味はほとんどない。

階層型スケジューラによる時間保護

株式会社 ヴィッツ

＜時間保護＞

・多段ディスパッチャー方式



サブスケジューラ：
プリエンプティブな固定優先度ベーススケジューラ
アプリケーション内のタスク起動を管理する
(アプリケーション毎に用意される。また、アプリケーション毎に異なるスケジューラでも良い)

メインスケジューラ：
EDF (Earliest Deadline First) によるアプリケーションへのプロセッサ時間を割り当てる
(プロセッサ利用率に応じた実施的プロセッサ時間)

・RTOSに組込むことにより、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

保護機能OSの実証実験

株式会社 ヴィッツ

実証実験

実証実験計画；ヴィッツ

アイシン精機と東海理化が完全バックアップ

-2007年4月17日に実証実験開始をプレスリリース

-2007年10月30日にアイシン精機藤岡試験場で試験完了

関連記事

中日新聞 (2007/4/18)

日刊工業新聞 (2007/4/18)

読売新聞 中部版 (2007/4/18)

毎日新聞 (2007/4/28)

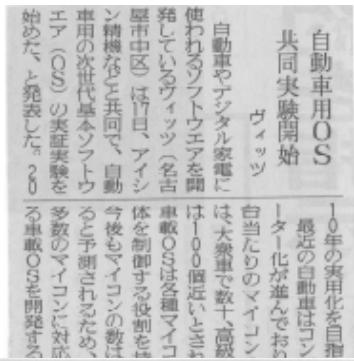
車の電子装置 統合制御
アイシンなど 新OS開発

電子化が進む自動車を、統合制御できるOSの効率的に制御できる基本ソフト（OS）の開発に成功したと発表した。

取り組んでいるアイシン精機やソフト開発のヴィッツ（名古屋市）などの共同研究チームは十七日、複数の電子装置を

仕事を割り付けることができる。また車の運転動作に即時に応答できるよう、個々のECUに一定時間内に仕事を完了させる監視機能も持つ。

研究チームは今回のOS開発で「車載ECUの数を二分の一から三分の一に減らしたい」としており、秋までに実証実験を続け、二〇一一年ごろの実用化を目指す考えだ。



自動車用OS
共同実験開始
ヴィッツ

自動車やデジタル家電に使われるソフトウエアを開発しているヴィッツ（名古屋市中区）は17日、アイシン精機などと共同で、自動車用の次世代基本ソフトウエア（OS）の実証実験を始めた、と発表した。20

10年の実用化を目指す。最近の自動車はコンピューター化が進んでおり、1台当たりのマイコンは、大衆車で数十、高級車は100個近いときもある。車載OSは各種マイコンを制御する役割を担う。

今後もマイコンの数は増えると予測されるため、多数のマイコンに対応する車載OSを開発する

トッパーズプロジェクト

保護機能付きOSを開発

組み込みシステム向けのオープンソース（設計図を無償公開するソフト）を開発する産学官グループの「トッパーズプロジェクト」（高田公章会長＝名古屋大大学院教授）は17日、自動車制御システム向けの保護機能付き基本ソフト（OS）を開発したと発表した。電子制御ユニット（ECU）統合時に有効なメモリー保護機能などを搭載。今後、機能検証のためアイシン精機と東海理化で実証実験を行う計画。将来的には一般公開する。保護機能付き車載OSのオープンソースは世界初。

高田 会長

アイシン精機・東海理化で実証

ECU統合促す

車制御システム向け

新OSは、トッパーズプロジェクトが04年に開発したカーネル（OSの中核部分）「トッパーズOSEKカーネル」をベースに、メモリー保護や時間保護機能などを追加開発した。開発は経済産業省「地域新生コンソーシアム研究開発事業（06～08年度）」の採択を受け、同プロジェクトの会員企業を中心に行われた。

現在、電子制御技術はエンジンやブレーキなどの制御に加え、ECUの搭載数は高級車で70個前後に及ぶ。今後もクルマの電子化が進む中で、車内の制御システムはますます高度化、複雑化する恐れがある。

このため開発効率化やコスト削減などの観点から、従来、制御システムごとに用意していたECUを、複数システムがECUを共有する形にする、ECUの統合が必要になると見られている。

だが、一つのECUに複数のシステムを乗せた場合、各システムが相互干渉し合い、不具合を起こす可能性が出てくる。

対策として、検証テストを繰り返しながらそのリスクをつぶしていく方法があるものの、その分、設計負担が大きくなってしまう。そこで新OSは、干渉のリスクのある部分を隔離する保護機能を搭載。OSレベルで相互干渉を避ける仕組みをつくった。またソフト単位で問題が起こった際に、他のソフトに影響が及ばないように、任意の単位でソフトを分離できる機能も搭載した。

今回のコンソーシアム事業にも参画したアイシン精機と東海理化は今後、保護機能の有効性の検証に取り組み、今年秋を目標に最終的な検証を終える計画。またアイシン精機は今後、同OSの自社製品への適用も検討していく方針だ。

プレーキ・アクセル一括管理

自動車用基本ソフト開発

アイシンなど 年内無料開放へ

トヨタ自動車グループのアイシン精機や名古屋大学などの研究チームは17日、自動車の複数の機能をまとめて管理する基本ソフト（OS）を開発したと発表した。自動車の高性能化にともない部品の電子化が進み、ブレーキやアクセルなど多機能を個別に管理する電子制御装置（ECU）は高級車には50個以上、大衆車でも30個程度搭載されている。開発された基本ソフトを使えば搭載するECUを減らし、コストを削減して軽量化もできるという。

研究チームは年内にも基本となっている。

ソフトをインターネット上で無料開放し、国内自動車メーカーなどと連携して各社が共通で使用できる国内初の標準化を目指す。

自動車は現在、ブレーキとハンドルを連動させて横滑りを防ぐといった複雑な動きをするためには、ECU同士を配線でつないで連動させるのが基本。

ECUの搭載数を減らすには、統合して個々のECUに複数の機能を管理させる必要がある。

が、不用意に統合するとプログラムの誤作動につながる恐れがあると指摘されていた。研究チームが開発した基本ソフトは、この誤作動を防ぐ仕組みを盛り込んだのが特徴だ。

自動車の機能をまとめて管理する基本ソフトの開発では、BMWを中心とした独自動車メーカーなど欧州勢が先行。国内でもトヨタが4月から独自の基本ソフトの開発も視野に入れて開発部門を立ち上げるなど、競争が本格化してきた。

研究チームは基本ソフトの無料開放で内外の幅広い知恵を集めて高性能な基本ソフトに仕上げ、「将来は欧州側に提案していきたい」（アイシン精機）と世界標準化も念頭に置いている。

注目度　主要自動車関連情報誌で紹介

株式会社 ヴィッツ

ヴィッツ:「信頼性向上のために保護機能を開発する」

独立系ソフトウエアベンダーのヴィッツは、名古屋大学などと共同で、ソフトウエアプラットフォームに必要となる保護機能を開発している(図8)。

保護機能は、アプリケーションごとに使用するメモリー領域やアプリケーションを決めてアクセスを制限する「メモリー保護」と、CPUを占有する時間を決める「時間保護」がある。

メモリー保護機能は、許可していないアプリケーションからメモリーへのアクセスを制限もしくは禁止する。アプリケーションが、禁止した動きをした場合はエラーを返すことで、問題の特定を容易にする。

一方の時間保護は、アプリケーションごとにCPUの占有時間を割り当てる機能。占有時間を過ぎて使用した場合、ほかのアプリケーションがCPUを使えなくなるなどの影響が考えられる。決められた処理時間内に処理が終わらなかった場合は、原因となるアプリケーションに通知する。

同社はソフトウエアプラットフォームの導入でECUの統合が進み、現在100個近くあるECUが2012年には30個程度にまで減ると予想している。

ECUの統合で、異なるメーカーのアプリケーションが一つのECUに搭載されると最も難しいのは、不具合が発生した場合の検証だ。「メーカーが異なると開発も検証の手法も異なる。同じメーカー内では問題がなくても、全く気が付かない要因で不具合が発生することがある」(ヴィッツ取締役の服部博行氏)という。

同社は、開発中の保護機能を、組み込み分野のオープンソースのソフトウエアを開発する団体「TOPPERSプロジェクト」を通して公開し、標準化団体「JasPar」に提案する計画だ。TOPPERSはすべてをオープンにするわけではない。標準化後は、保護機能に関するビジネスなどを見込んでいる。

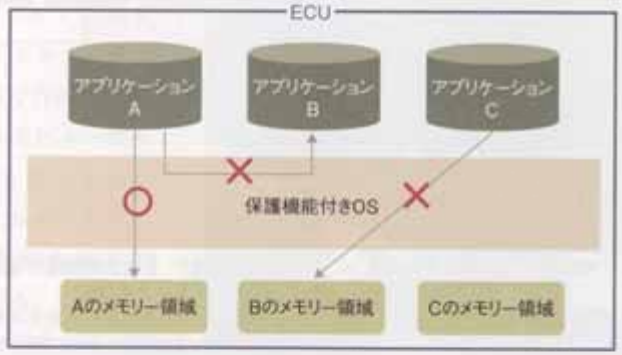
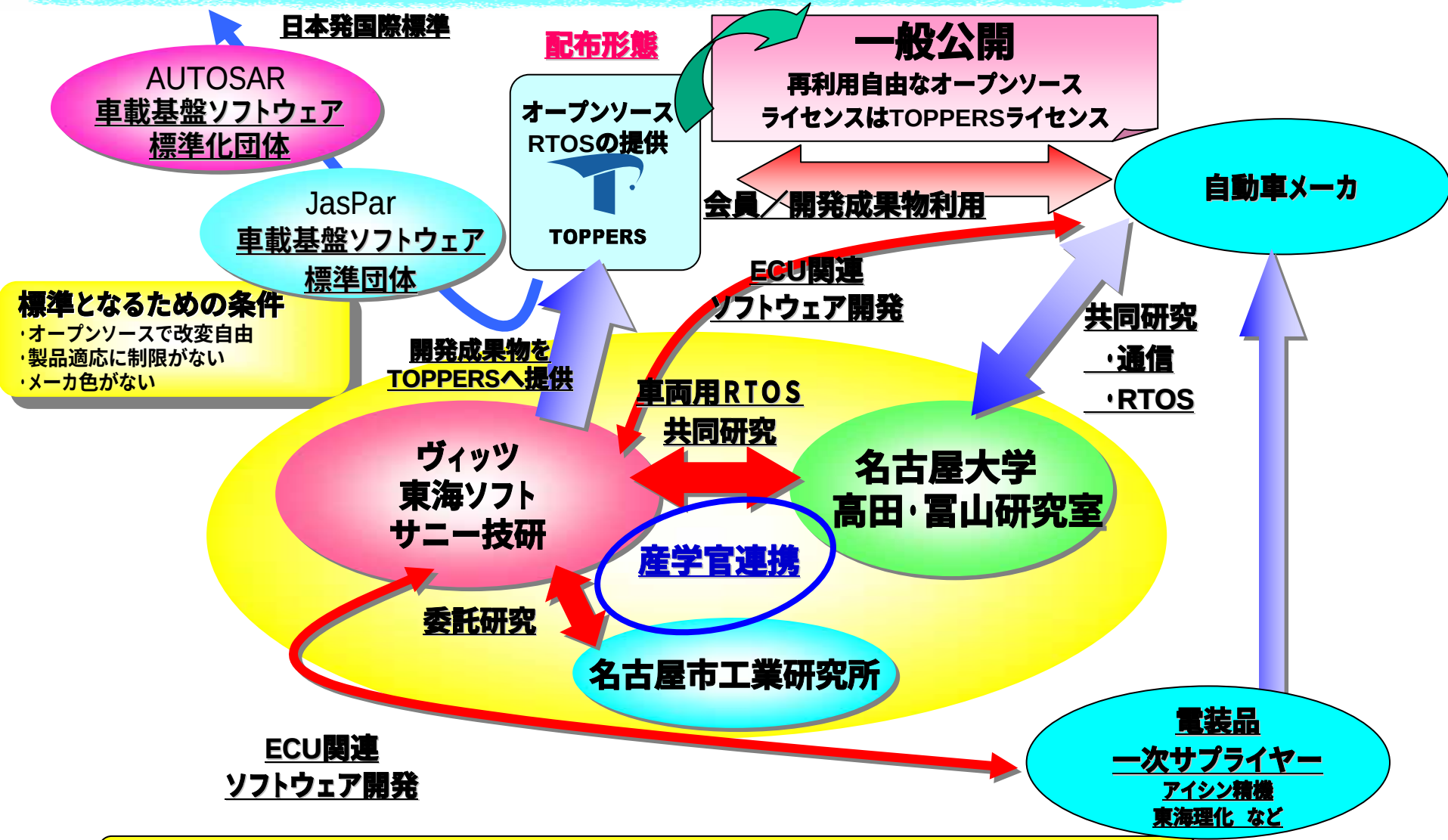


図8　保護機能の仕組み
ECUに複数のアプリケーションが搭載されても、アクセス可能なメモリー領域やアプリケーションを指定することで不具合を未然に防ぐ。たとえ不具合が発生しても問題の特定を容易にする。

目標は自動車向けSPFの標準化

株式会社 ヴィッツ



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に等へ販売

自動車制御SPFへのロードマップ

株式会社 ヴィッツ