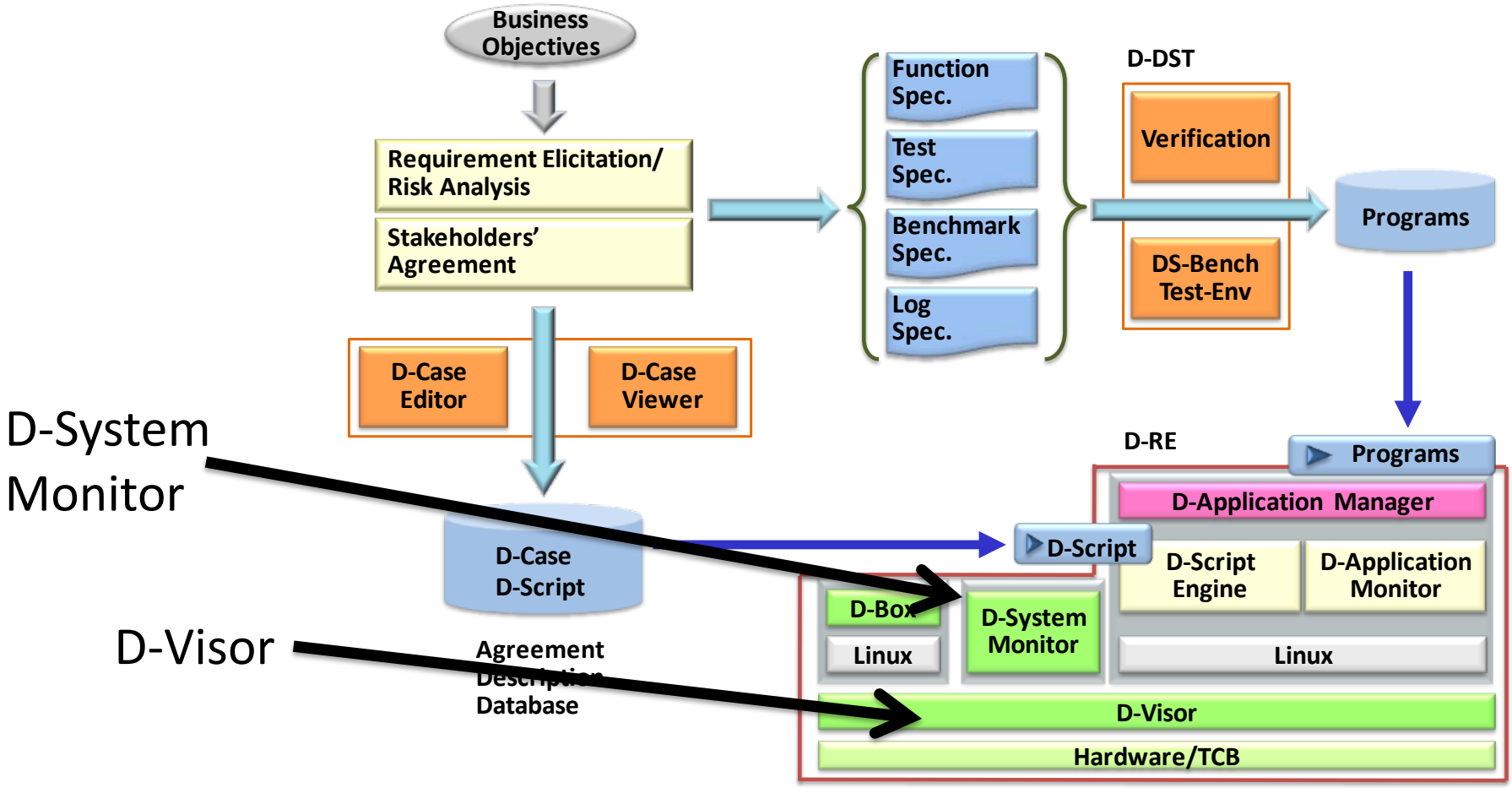
D-Visor: ディペンブルシステムにおけるVMの役割

早稲田大学
基幹理工学部　情報理工学科
中島　達夫

OSの整合性、障害監視

- システムが定義された通りに動作することを保証するためには，OSカーネル自体が正しく動作していることを保証する必要がある.
  - OSカーネルが満足すべき性質が常に満足していることを保証する.
  - Linuxカーネルのような巨大なOSを検証を用いて問題を取り除くことは不可能である.
- 特に，セキュリティ面での攻撃を考えると，OSカーネルが定義されたように動作していることを監視するための機能がディペンダブルシステムでは必用不可欠となる.

D-VisorとD-System Monitor



D-VisorとD-System Monitor

- D-Visor: 仮想化層
  - XEN, KVM: サーバ向け仮想化層
    - 複雑で仮想化支援機能が必須
  - SPUMONE, ART-Linux: 組込みシステム向け仮想化層
    - 軽量で仮想化支援機能が不要
  - 組込み／リアルタイムシステム向けのフリーなD-Visorとして利用出来るものはないので，DEOSプロジェク内で開発した.
- D-System Monitor:
  - モニタリングサービス： 汎用的なカーネルデータ構造の整合性管理
  - FoxyKBD, Rootkit Libra： 河野先生の講演で説明
- D-System Monitorランタイム API

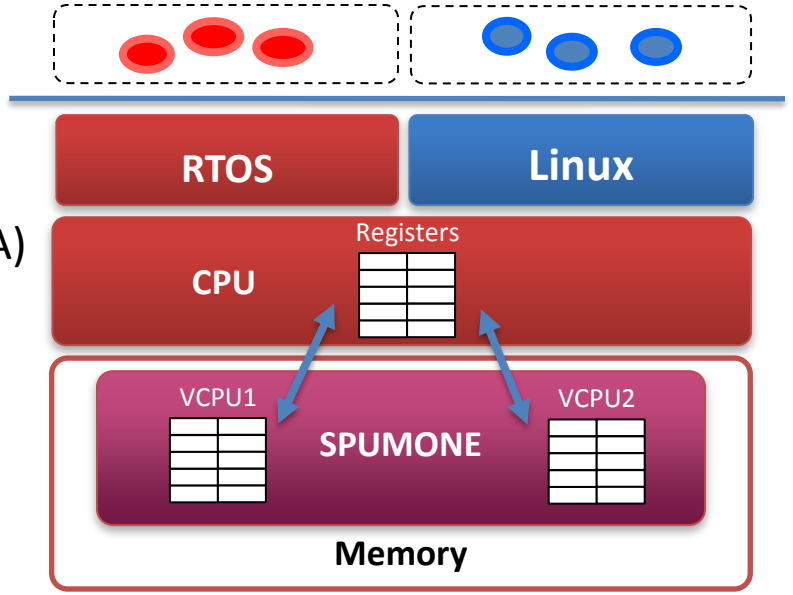
マルチコア組込みシステム向けD-Visor

- 仮想化支援ハードウエアが存在しない場合でも効率よく動作する必要がある.
- 効率を犠牲にせず，Linuxカーネルの変更を最小にする必要がある.
  - 組込みシステムにおいては重要な要件
- 負荷に応じてLinuxが利用する物理コアの数を動的に変更することが可能である.
  - 低消費電力と効率／リアルタイム性のトレードオフ
- RTOSのリアルタイム性を犠牲にせずに複数のOSを動作させることが可能である.

組込みマルチコアプロセッサ向け D-Visor: SPUMONE

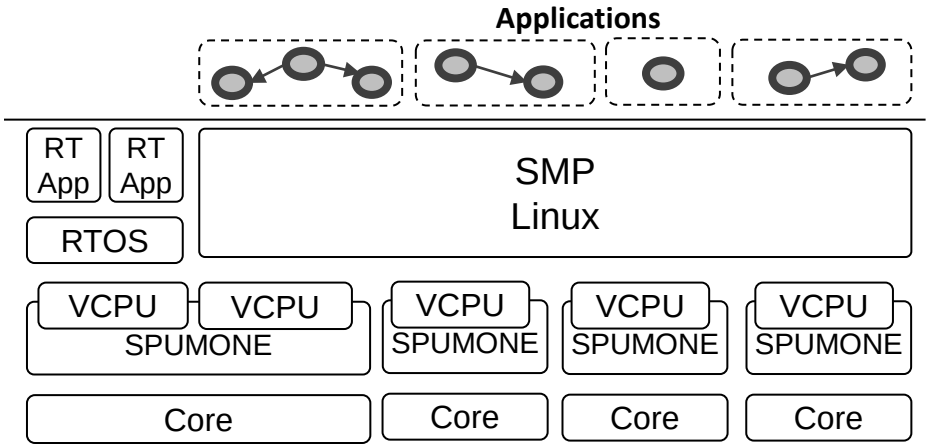
- OSカーネル(Linux, RTOS)とSPUMONEの両方が同一のカーネルアドレススペースに存在する.
- SPUMONEは仮想CPUという抽象化をLinuxやRTOSに提供する.
- SPUMONEは仮想CPUを利用して，複数のOSを同一の物理コア上で動作することを可能とする.
- CPU: Super H(SH-4A ISA)

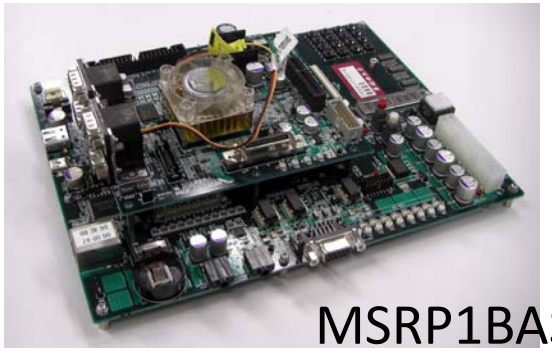
SH7780 400MHz (ISA: SH-4A)
2 serial channels
6 timer channels
128MB DDR-SDRAM
100Mbps Ethernet x 2
CF card adapter
2.5inch IDE adapter



マルチコアプロセッサの支援

- 分散カーネルモデルの利用
  - 各コア毎に独立したSPUMONEを配置する.
  - 各SPUMONEは仮想CPUを用いて複数のOSを同一の物理コア上で動作させる
  - 各SPUMONEはプロセッサ間割り込みを利用して通信をおこなう.

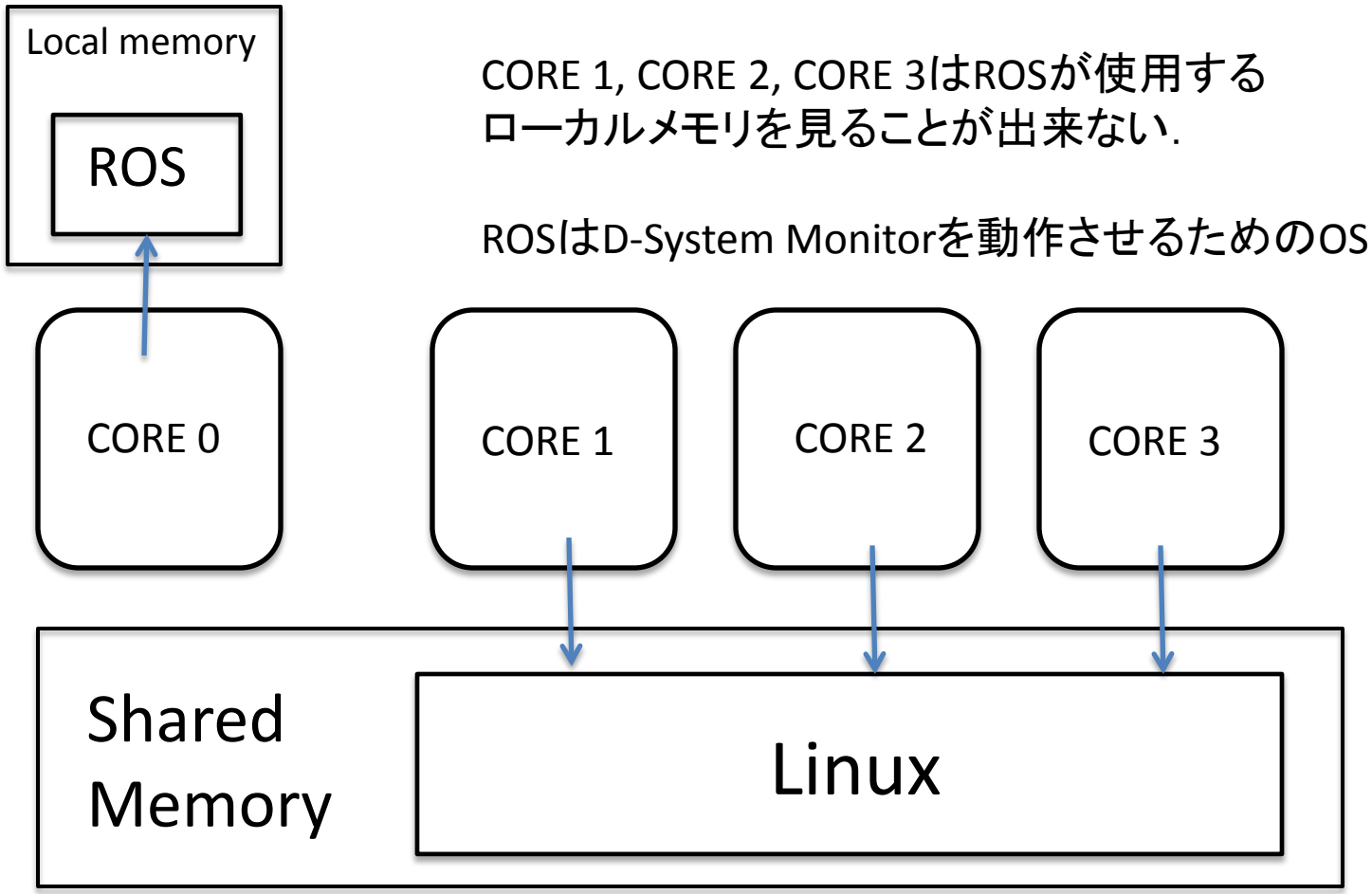




MSRP1BASE02

RP1 (SH-4A MP ISA)
600MHz x 4
128MB DDR-SDRAM

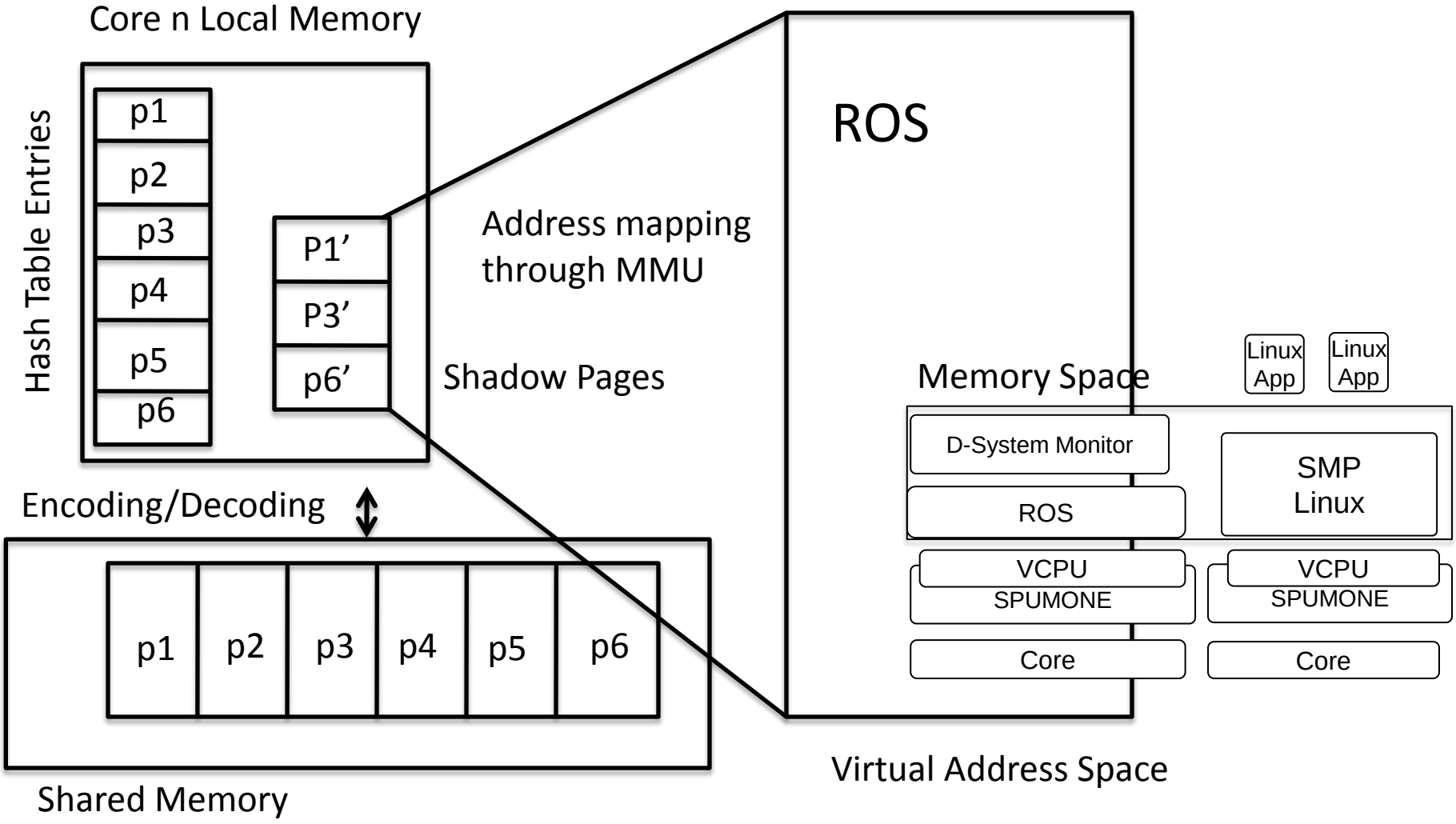
SPUMONEにおけるD-System Monitorの保護



CORE 1, CORE 2, CORE 3はROSが使用するローカルメモリを見ることが出来ない.

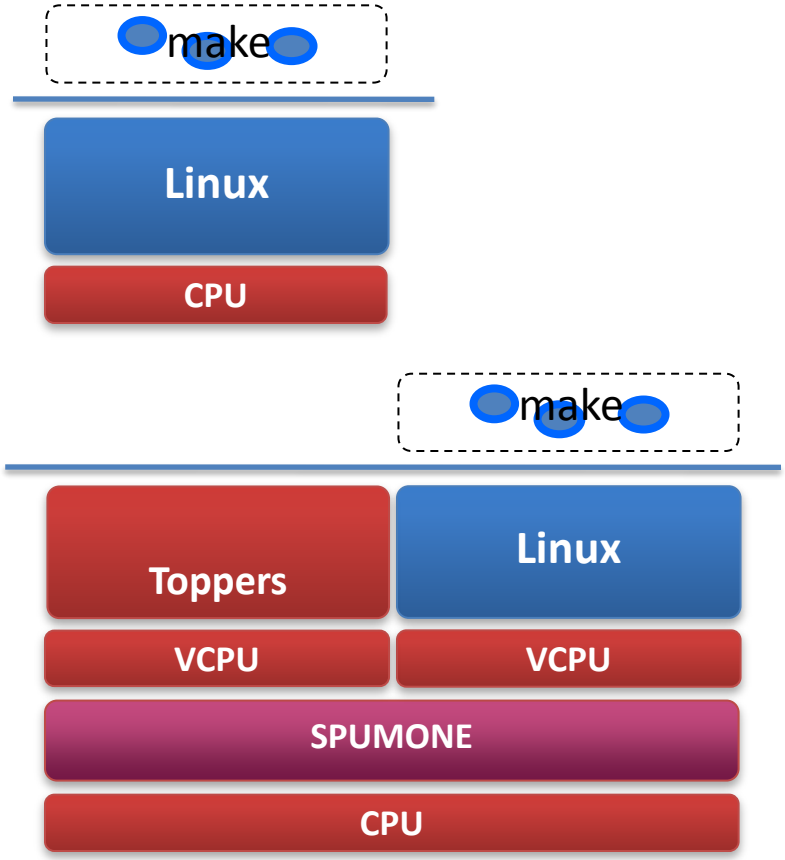
ROSはD-System Monitorを動作させるためのOS

複雑なD-System Monitorの保護



オーバヘッドの評価

- ネイティブLinuxとSPUMONE上のLinuxの性能差を示す



Linuxカーネルビルドタイム

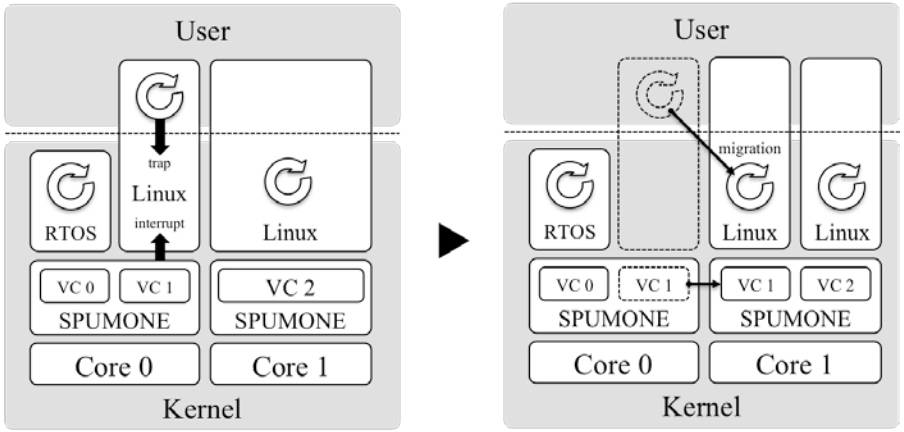
Configuration	Time	Overhead
Linux only	68m5.898s	-
Linux and TOPPERS on SPUMONE	69m3.091s	1.4%

- オーバヘッドはToppers上のタイマ処理のオーバヘッドも含む

RTOS: TOPPERS/JSP 1.3
- kernel and applications reside in the same address space
- 64MB
- Devices
  - Serial channel 0
  - Timer channel 3

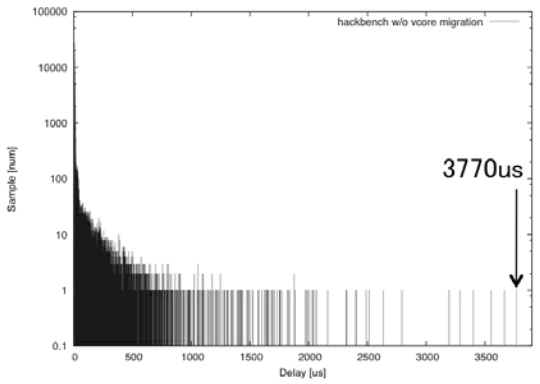
GPOS: Linux 2.6.20.1
- 64MB
- Devices: All the other
- Root FS: NFS share (Fedora Core 5)

リアルタイム性の評価

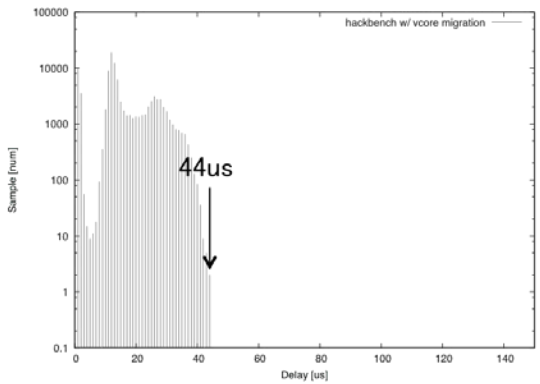


- システムコールを呼び出す毎に，仮想CPUが他の物理CPUに移動する
- Linuxカーネル内のアクティビティがRTOSのアクティビティと干渉しない．

- RTOSディズパッチレーテンシが大幅に改善



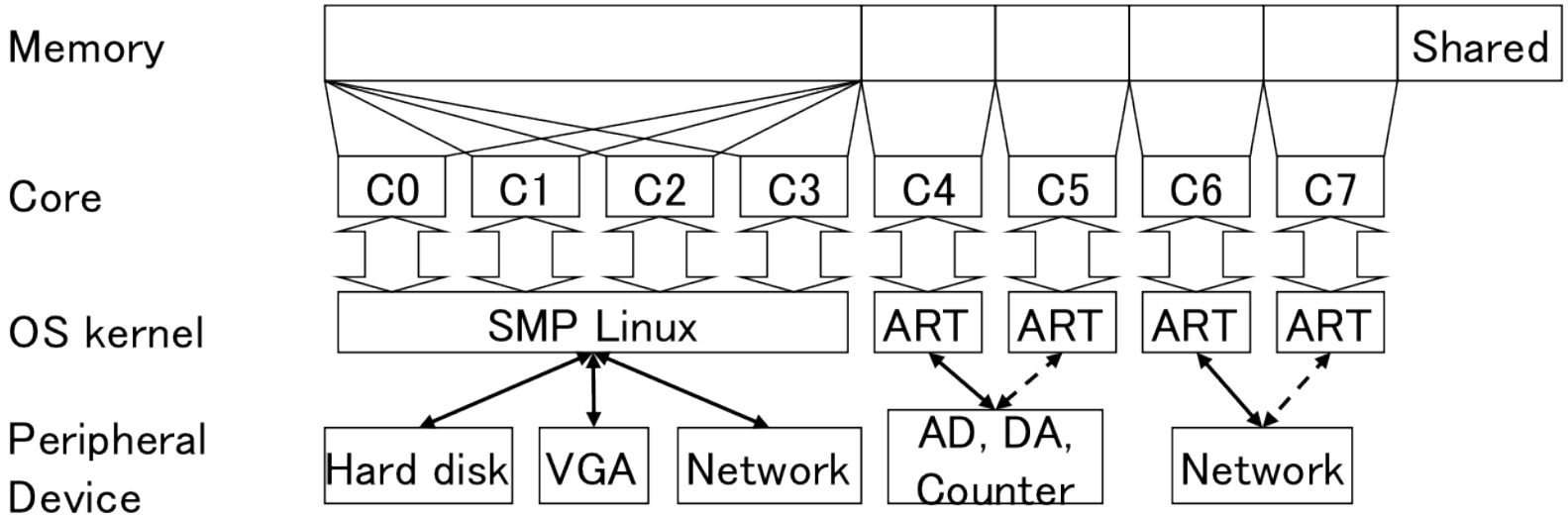
Delay without VCPU migration



Delay with VCPU migration

ART-Linux概要

- ART-Linuxはリアルタイム拡張したLinuxである.
- 複数のコア上で動作する軽量の仮想化層を持っている.
- D-System Monitorを保護出来ないので，セキュリティよりもリアルタイム性が従事される場合に利用する.

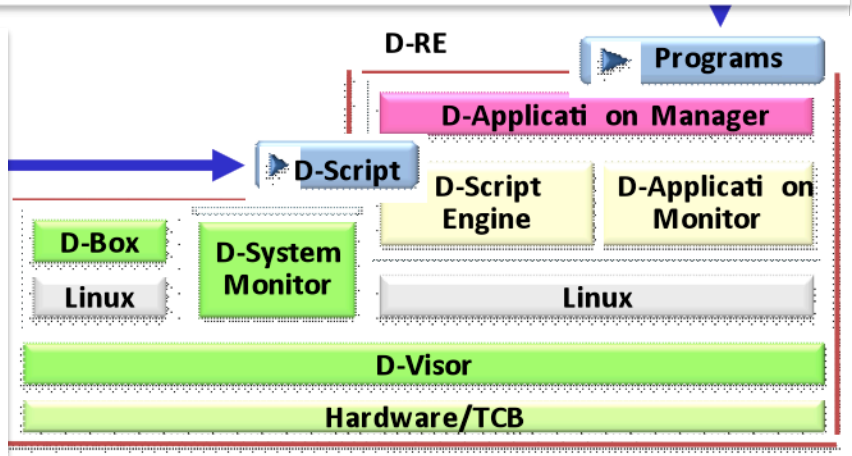


DEOSにおけるD-System Monitor

- 環境の変化に応じて，新しいD-System Monitorを追加したり，既存のD-System Monitorを変更することが可能である.
  - 例えば，新しい攻撃方法が見つかった場合は，新しいD–System Monitorを追加する
- 各D-System Monitorはカーネルのある部分の整合性管理をおこなう.
  - Linuxを変更せずにD-System Monitorの追加，変更だけで新しい要求に対応可能である.

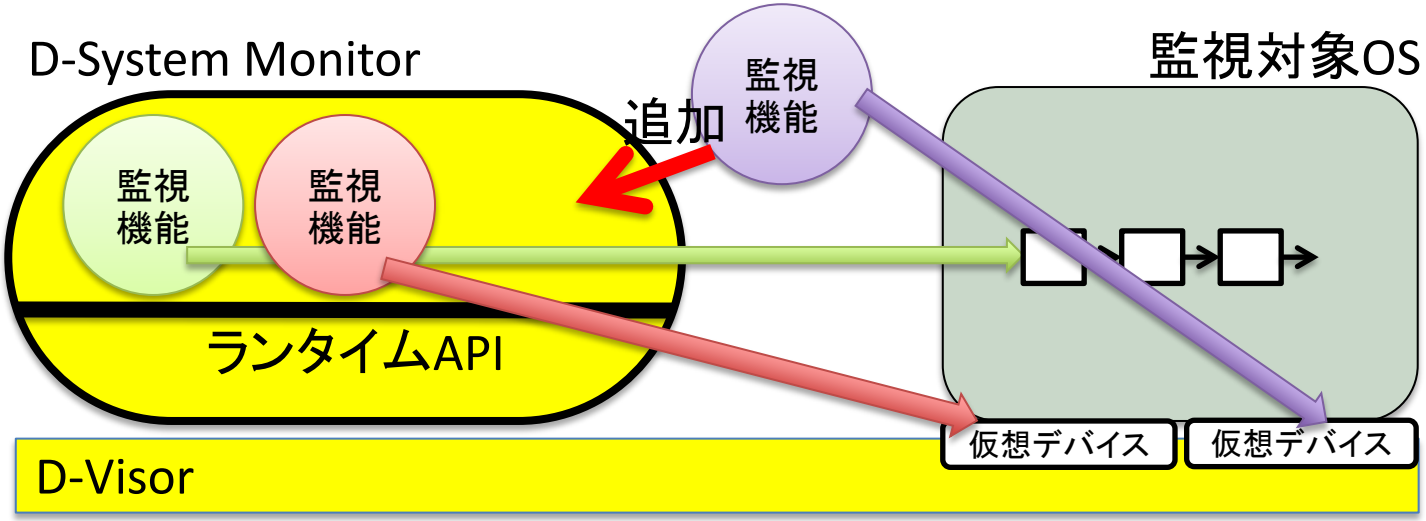
D-System Monitorの例: モニタリングサービス

- Linuxカーネル内のすべてのデータ構造の整合性を監視するためのシステム
  - 従来のシステムはどのデータ構造をどう監視するかを記述する必要があった.
  - ソースコードを解析して，データ構造に関する仕様を自動的に抽出し，学習機能により整合性のための条件を自動生成する.
  - 整合性監視によりカーネルルートキットが検出可能であることは実証している.
  - Linuxのバージョンアップによりデータ構造が変更されても簡単に適応出来る.
  - ソースコードがあればRTOSの整合性監視にも利用出来る.



D-System MonitorランタイムAPI

- D-System Monitorとして監視対象OSを検査するためのAPI
  - APIを策定することで、D-System Monitorの監視機能がD-Visorの実装に依存しなくなる
    - APIを用いた監視機能は複数のD-Visorで利用可能
  - 新たな脅威に対応する監視機能の迅速な開発を支援
    - APIを使用すればD-Visorの内部設計の詳細を知る必要はない



最後に

- D-VisorとしてのD-Visorの１つである
- SPUMONE(SH4a, x86版)とD-System Monitorのモニタリングサービスを年度内に評価版として利用可能
- 検証を利用することによりD-Visorの複雑な箇所の安全性の保証をおこなっている.
- D-Visor上ではLinuxが動作するため，D-REが容易に動作可能である.
- 展示ブースにてマルチコアプロセッサ上で動作するSPUMONEのデモをおこなっている.