仮想マシンによる
セキュアシステムの実現

大山 恵弘
電気通信大学 情報工学科

自己紹介もかねて: Project VINCS

- Virtual Infrastructure for Networked ComputerS
  - http://www.yl.is.s.u-tokyo.ac.jp/projects/vincs/
- 次世代の仮想化技術を研究している
  - 先進的なVM
    - Virtual Multiprocessor
  - VMの応用
    - Quasar

情報関連業界におしよせる仮想化の波

- 仮想化支援機構を擁するCPUの出荷開始
- 仮想マシンソフトウェアの品質向上
  - 性能、安定性、使いやすさ
- 仮想マシンソフトウェアの低価格化
  - 戦略的な価格設定も

「仮想化」は今後数年のキーテクノロジー

仮想化に関連した過去の動き（1）

- 1998: VMware社設立
- 1998: VMware’s US patent #6397242 出願（2002年特許付与）
- 1999: VMware Workstation発売
- 2003: Xenの論文がSOSP 2003にて発表
- 2003: MicrosoftがConnectixを買収、VirtualPC 2004米国発売

仮想化に関連した過去の動き（2）

- 2005: VT, Pacificaの仕様発表
- 2005/10: VMware Player無料公開
- 2005/12: Xen 3.0リリース
- 2006/1: SWSoftがOpenVZの発表
- 2006/2: VMware GSX Server無料公開
- 2006/4: MicrosoftがVirtual Server 2005 R2の無償提供を発表

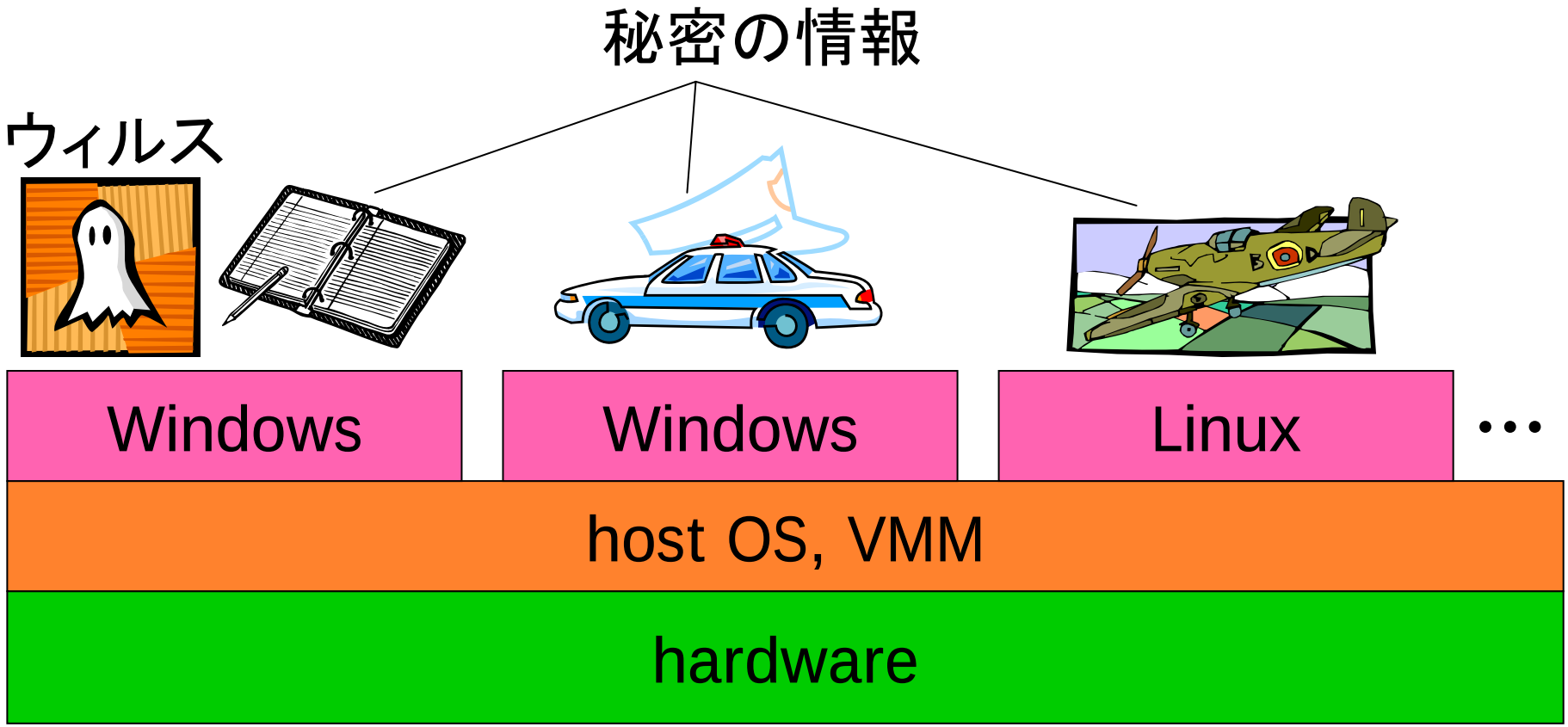
なぜ仮想マシンが重要か？

- 仮想マシンの普及がOS構築法の見直しを迫っている
  - 従来のOSの仕事を仮想マシンが行う可能性
    - ハードウェア管理
    - 低レベル資源を仮想化して上層に提供
- 上層のソフトウェアは、下層のソフトウェアの仕様を意識して実装される必要があることが多い
  - 仮想マシンの仕様を意識したOS開発

セキュリティの文脈において仮想化技術に注目する理由

- わかりやすい隔離の提供
  - ハードウェア・ソフトウェアコストの減少に伴う、管理コストの相対的増加
  - 仮想マシンはいわば大味な隔離技術
- 強い隔離の提供
- Trusted Computing Base (TCB) の縮小
- 仮想化システム・計算機の速度向上
- 資源に余裕がある計算機の増加

悪意/脆弱ソフトウェアの仮想マシンによる隔離



仮想化システムの恩恵（1）

- 実行環境の隔離
  - 攻撃および障害による影響範囲を分割
  - 資源割り当て単位・スケジューリング単位を提供
- 実行環境を外から制御できる層の提供
  - プログラムの動作の監視
    - 自動システム管理に道を開く
  - 実行環境のバックアップ・複製・サスペンド
    - OS全体の「アプライアンス化」
  - 再実行による攻撃解析・障害解析・デバッグ
  - ロールバックによる障害からの回復

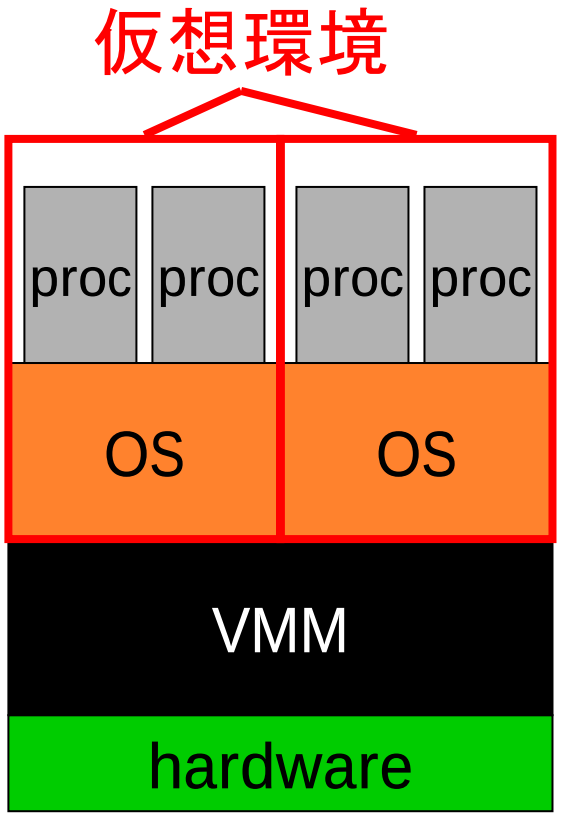
仮想化システムの恩恵(2)

- 資源の多重化
  - サーバの統合
  - 1物理計算機上での複数種OSの同時利用
- 実環境間の差異の隠蔽
  - 物理計算機間マイグレーション
  - 仮想デバイスのドライバによる実デバイスの制御
- 所有していないハードウェアの提供
  - 開発中のハードウェア
  - 生産が打ち切られたハードウェア

仮想化システムの分類

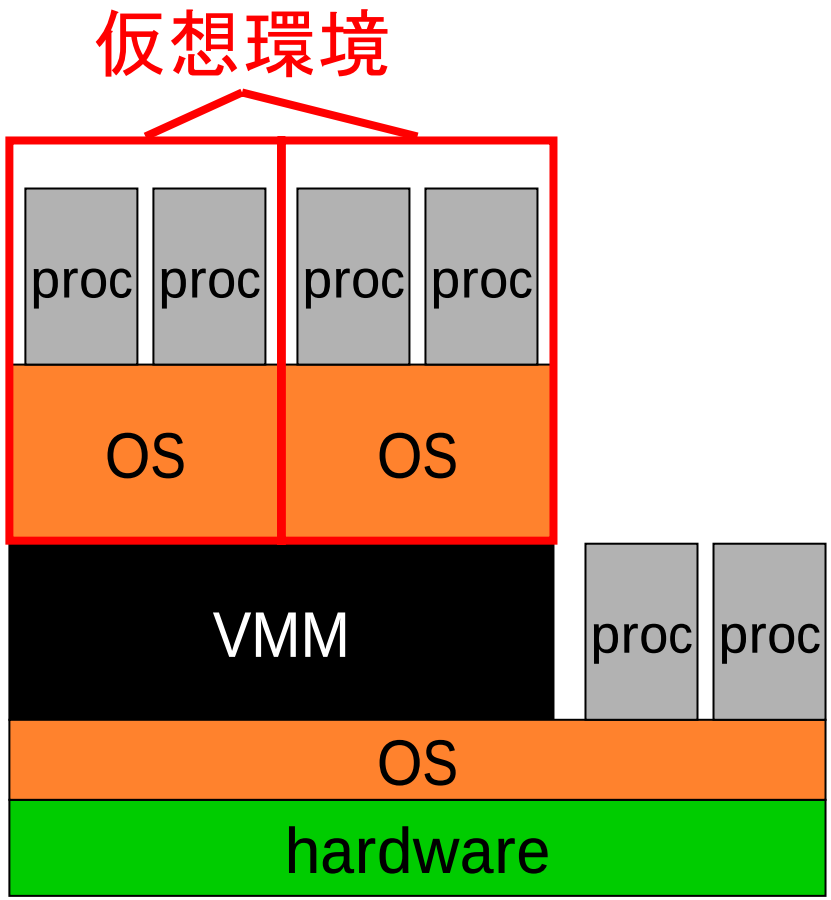
- 仮想マシンモニタ（VMM）
  - Type Ⅰ (hypervisors)
  - Type Ⅱ
  - Hybrid
- 資源ビュー仮想化システム
- 言語VM

Type I VMMs



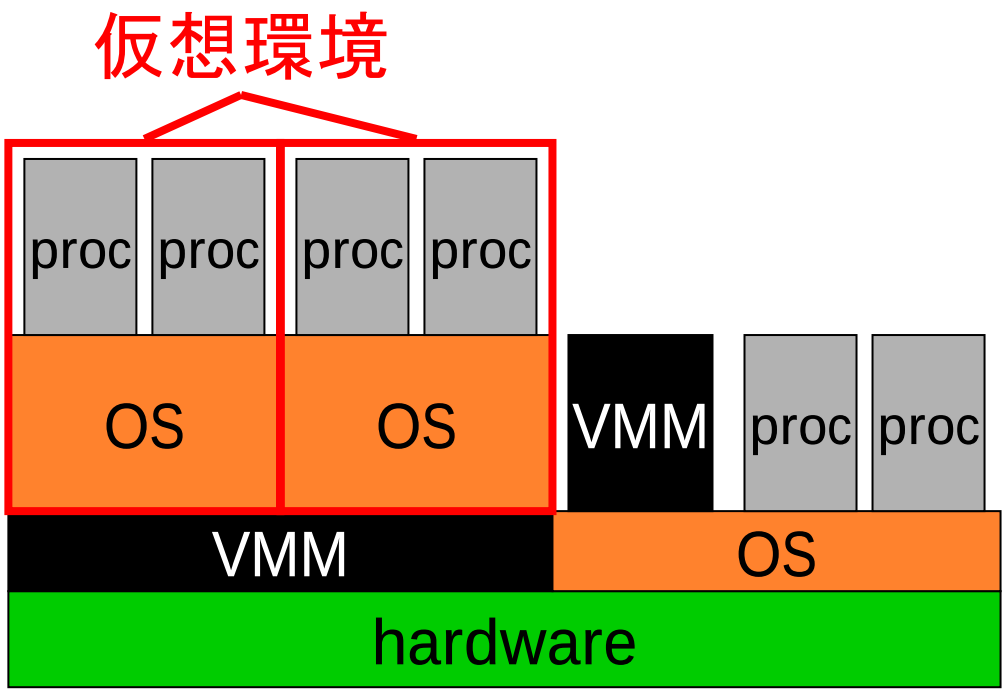
- VMMはハードウェアのすぐ上に位置
  - ホストOSなし
- VMMの古典
- 例：VMware ESX Server, Xen, VM/370, Windows Hypervisor?

Type II VMMs



- VMMはホストOSの上でユーザプロセスとして動作
- 例：User-Mode Linux (tt mode)

Hybrid VMMs



- VMMはハードウェアのすぐ上に位置
- ホストOSは存在
- ゲストOSのI/Oにホスト OSを利用
- 例：VMware Workstation

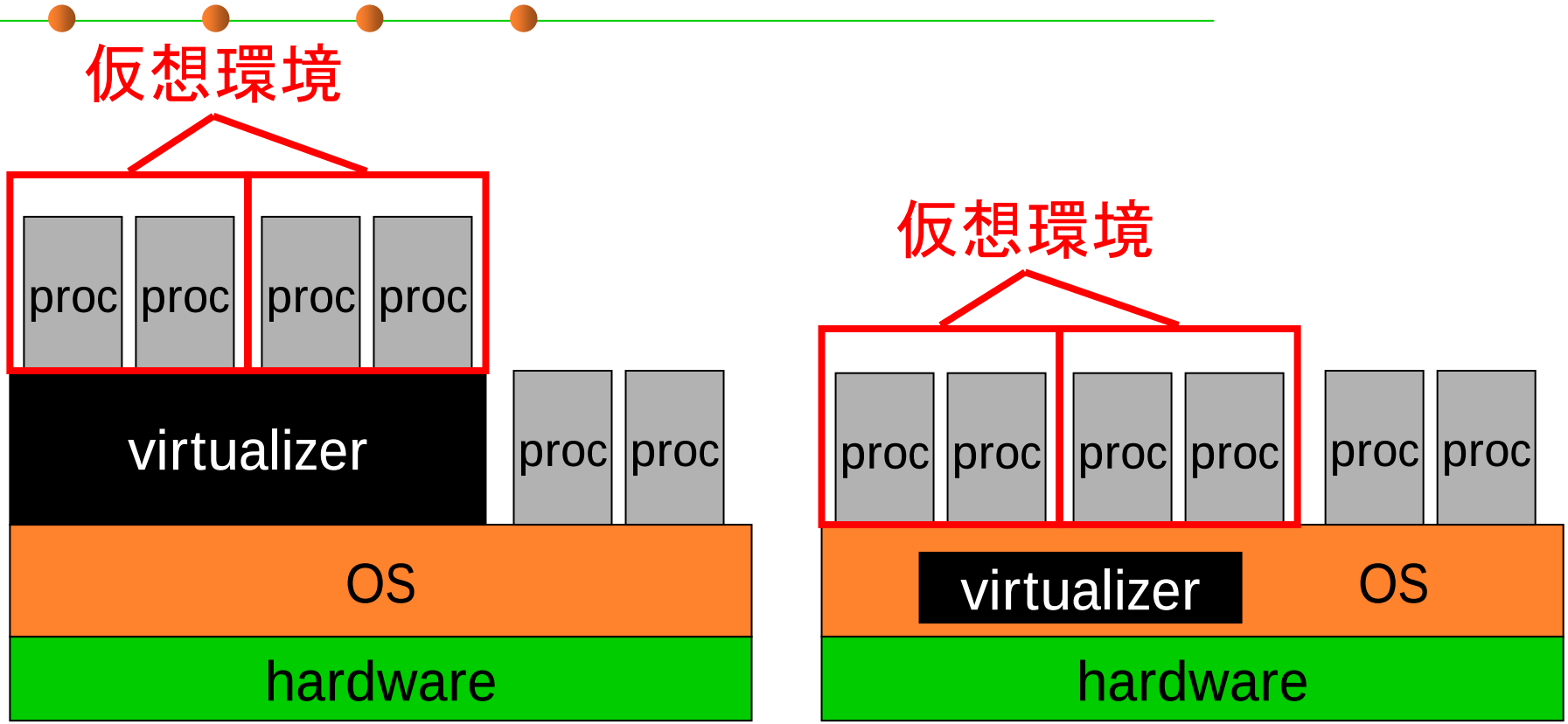
3種のVMMの比較

- Type I VMM
  - 高い性能を実現しやすい
  - ホストOSに影響されない資源消費制御が実現可能
- Type II VMM
  - 導入の敷居が低い
  - ゲストOSおよびVMMの異常や脆弱性がホストOSに影響を与えにくい
  - ホストOSの資源管理・デバイス管理を利用できる
- Hybrid VMM
  - Type IとType IIの特徴を併せ持つ

VMMの利点と欠点

- 利点
  - 「別のPC上でプログラムを実行した」状態に近い度合いの隔離
- 欠点
  - 無視できない資源消費量、オーバヘッド（程度は実装による）
    - SOSP 2003論文発表の時点で、Xenの性能は既にかなり高い

資源ビュー仮想化システム（1）



例：Solaris containers (zones), FreeBSD jail, Linux VServer, Virtuozzo

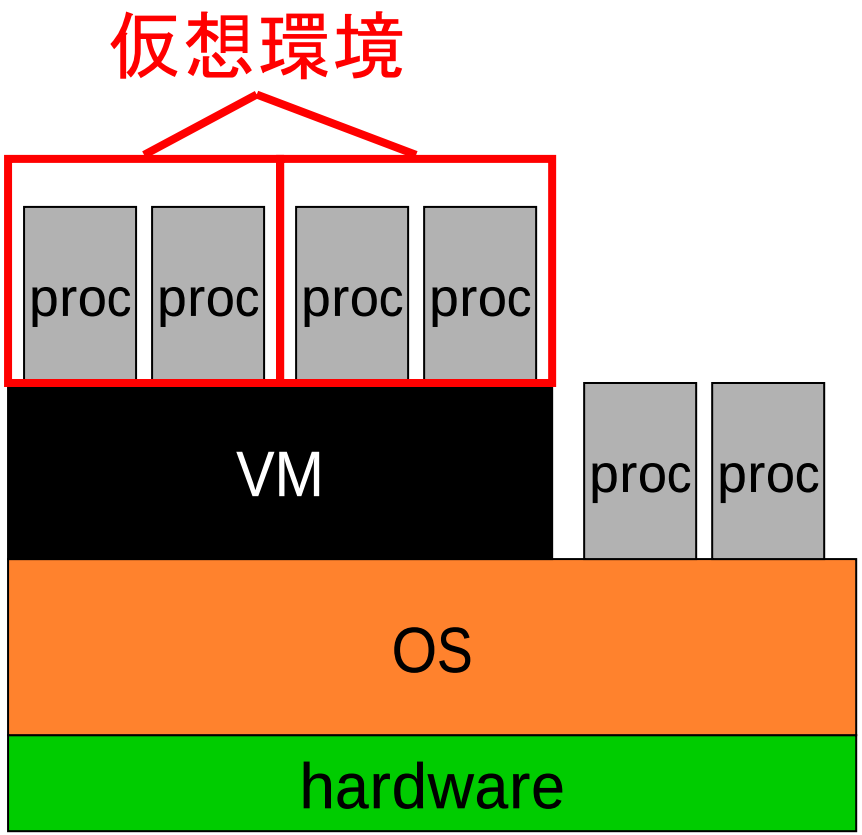
資源ビュー仮想化システム(2)

- 一つのOS上に複数の仮想環境を構築
- 資源の見え方・名前空間を仮想化
  - ファイル木、プロセス空間、etc
  - 仮想ネットワーク機能も提供されることが多い
- カーネルは仮想環境と実環境で共有
- 仮想環境内のプロセスの動作には制限がかかるのが普通
  - shutdownやinsmodを実行できないなど

資源ビュー仮想化システム（３）

- 利点
  - 小さい消費資源量とオーバヘッド
- 欠点
  - 仮想「マシン」でないことからくる制限
    - 仮想環境ではホストOSと同じOSしか使えない
    - 仮想環境でできる処理に制限
      - シャットダウン、デバドラのインストール

言語VM



- 独自のISAおよびOSサービスAPIを提供
- 例：JVM, .NET CLI
- 利点：実環境への依存が小さい仮想環境を作れる
- 欠点：独自ISA/APIの採用からくる制限
  - レガシーアプリの実行
  - APIがない処理の実行

命令実行を仮想化するための基本方式

- ゲストOSを低い特権レベルで動かし、特権命令でトラップさせる
  - トラップしたら、さも特権命令が実行されたかのようにゲストOSのメモリ/レジスタを、ホストOSが書き換える

命令実行の仮想化に関するx86の問題

- 「Pentiumにはsensitiveな非特権命令（non-virtualizableな命令）が250個中17個存在する」
  - “Analysis of the Intel Pentium’s Ability to Support a Secure Virtual Machine Monitor”, Robin and Irvine, USENIX Security Symposium, 2000.
  - Sensitive命令：エミュレーションが必要
  - 非特権命令：特権不足による例外が発生しない
  - 例： PUSHF, POPF, PUSH, POP, STR

Sensitiveな非特権命令の問題を解決するための技術

- Non-virtualizableな命令を別の命令に書き換える
  - 割り込みが発生する命令　or　VMMのコードを呼び出す命令に書き換える
  - VMMの実装が複雑化する一要因

CPUによるVMMのサポート (VT-xの例)

- x86の仮想化しにくいという欠点を解消
- rootモードとnon-rootモードを導入
  - 従来のring 0, 1, 2, 3に“ring –1”を付加
  - VMMをrootで、VMをnon-rootで実行
  - Non-rootモードでの実行では、多くの命令やイベントでrootモードへの遷移が発生
    - 遷移の発生のさせ方をソフトウェアで制御可能

VM(M)を利用した侵入検知

- HyperSpector [Kourai&Chiba ’05]
  - VM上でIDSとサーバを動かす
  - Inter-VM monitoring機構の提供
  - サーバやIDSが乗っ取られてもホストOSは安全
- Livewire [Garfinkel&Rosenblum ’03]
- Revirt [Dunlap et al. ’02]

ハードウェア仮想化機構の普及

- 今後のVMMはVT, Pacificaの存在が前提
  - x86の仮想化しにくい仕様と格闘する時代が終焉へ
  - x86を仮想化するための各種技法の価値が下落か
- セキュリティ問題の解決のために仮想マシンを利用することがさらに現実的に
- VMM技術の研究・開発の方向が変化
  - 差別化には「高性能なVMMをIntel系CPU上に作りました」以上の何かが必要になる可能性が高い
  - 今後の研究・開発はVMMの応用が中心か

Interoperabilityの向上

- 複数システムの相互乗り入れ
  - 例：VirtualPC上のLinuxをXenにマイグレーション
- 現在は様々な仕様が乱立
  - Para-virtualization (hypercall) interface
  - VM management interface
  - VM image format

国内での最近の動き

- 次世代OS環境「セキュアVM」の開発
  - 筑波大ほか多くの大学、企業、政府機関
  - VM、ID管理、暗号化、VPN
- 組み込みシステムのセキュリティを強化する仮想化技術の開発
  - 早稲田大、筑波大、エルミック・ウェスコム
  - マイクロカーネル上に仮想化したLinuxとITRONを実装