第2回セキュアVMシンポジウム

セキュアVMプロジェクトの概要

加藤和彦
筑波大学大学院 システム情報工学研究科

2008年3月19日

背景

- ITシステムの**脆弱性**を突いた，深刻なセキュリティ上の問題が発生
  - Webサーバの乗っ取りや停止
- 深刻な**情報漏えい**問題
  - 政府・行政機関からの個人情報，機密情報の漏えい
  - 民間企業からの個人情報、産業情報等の漏えい

問題

- **サーバシステム**をターゲットとしたセキュリティ機能向上が図られてきたが．．．
  - サーバシステムは，台数が限られ，専門家が集中的に管理可能.
  - サーバシステムは，セキュアOS機能を駆使した設定が可能.
- 最近の問題はむしろ**クライアント**
  - 「事件は会議室（サーバー）で起きているんじゃない，**現場**（クライアント）で起きているんだ」

Thanks to「踊る大捜査線」

現行の対策

- 不具合修整を含むソフトウェア・**バージョンアップ**や**パッチ**適用
  - バグ，脆弱性に対するアドホックな修正がほとんど.
  - 問題が判明しないと，修正が行えない.
- **ウィルス検知**ミドルウェアの導入
  - 基本的に既知の問題に対応.
  - ヒューリスティック（経験的手法）の積み重ね.
- **アナウンス**
  - 「情報漏えいを防ぐ最も確実な対策は，パソコンでWinnyを使わないことです．この点について，私からも国民の皆さんにお願いしたいと考えております．」 (2006.3.15 首相官邸　官房長官記者発表)

クライアント環境の難しさ

- 一般OS（Windows, Linux）は，ユーザの**使い勝手の良さ**（自由度）に重点を置いた設計，設定がされている.
  - しばしば，エンドユーザが管理者.
- セキュリティ対策に関して，アナウンス，周知徹底しか有効な**手だてがない**ことも多い.

さらに根深い問題

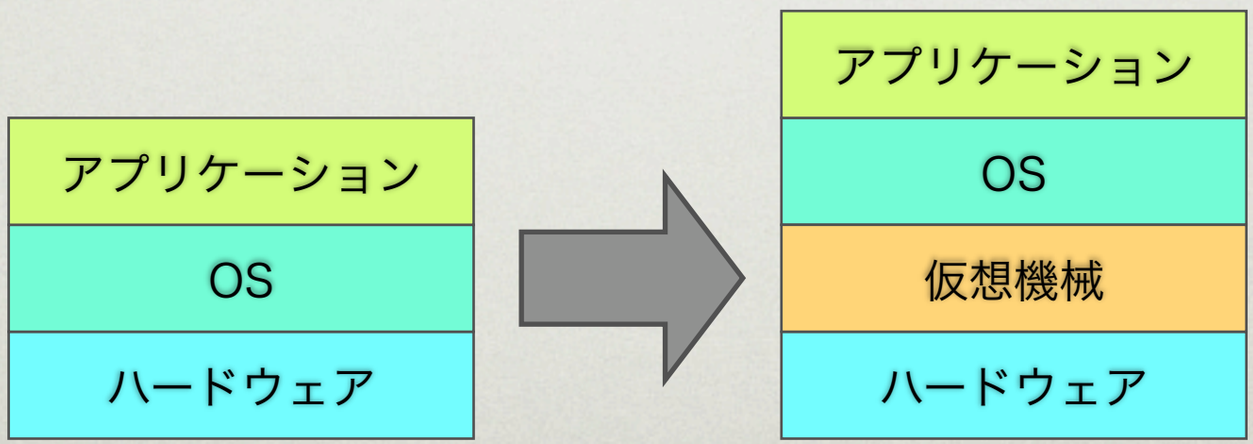
- 基盤システムソフトウェアの基本設計は米国を中心とした**海外陣営**に抑えられてしまった.
  - 基盤ソフトウェアレベルに容易には手が出せなくなっている.
- 以前は多くいた産業界の基盤システムソフトウェア技術／技術者が**失われつつある**.
  - 某企業幹部：「50代以上ならいますが若い人は本当に少ないんです」
  - 参考図書を探すと，80年代，90年代
  - 某ハードウェア会社：「マニュアルの日本語版も昔は沢山ありましたが，今はなくなりましたね」

目指したいこと

- **クライアント**環境へ高セキュリティ機能を提供したい.
- エンドユーザによる設定, 操作をできるだけ**簡単**にしたい.
- **共通汎用OS**(Windows, Linux等)に適用可能としたい.
- 組織による統一アクセス制御ポリシーの徹底を技術的に行えるようにしたい.

アプローチ

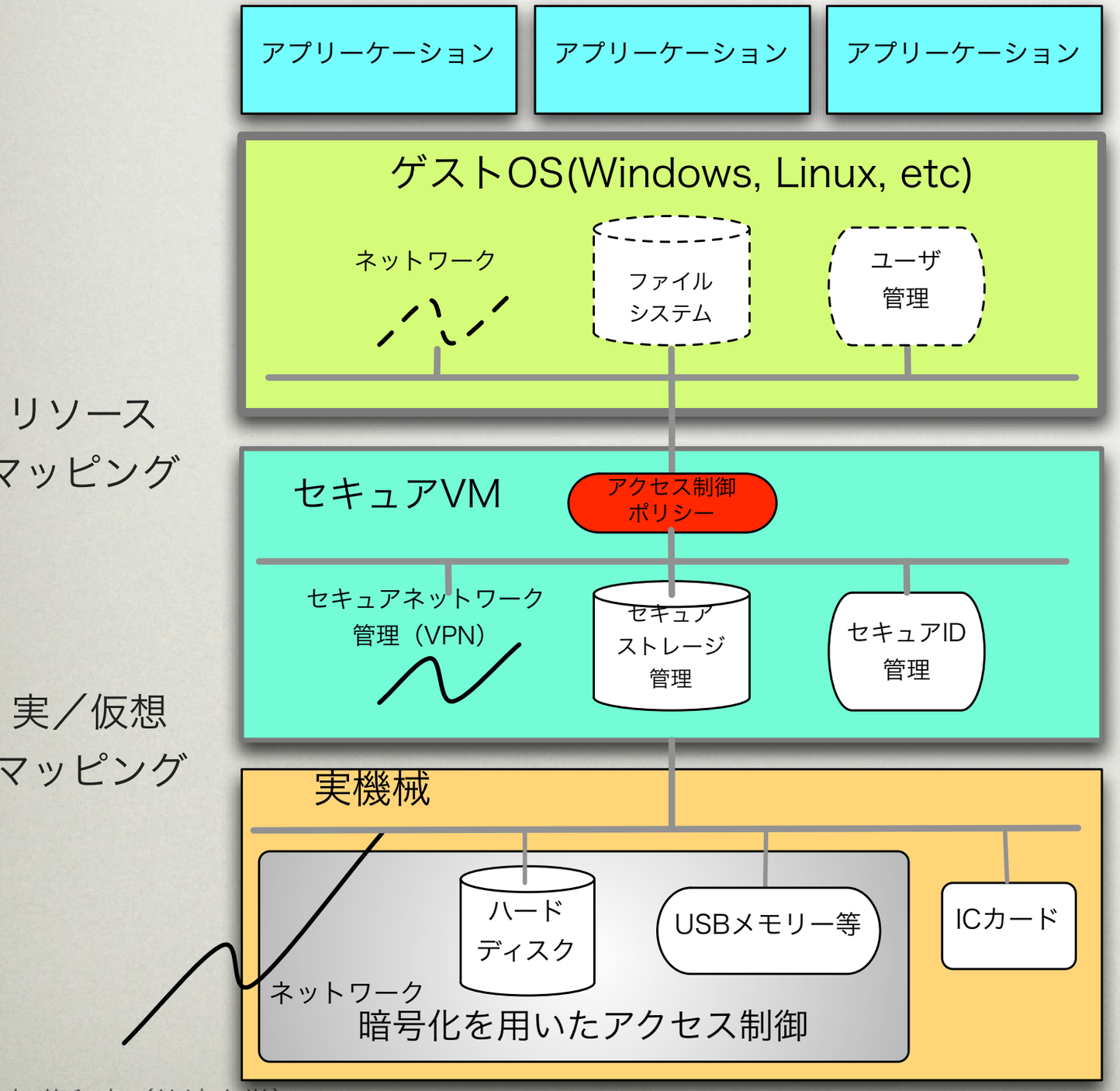
- **仮想機械技術**に着眼
  - 大型計算機システムにおいては1960年代より知られる技術.
  - 近年，パソコンにおいても利用可能となってきた.
  - 仮想機械をサポートするマイクロプロセッサが登場.
    (インテル社VT技術搭載CPUが2005年11月より発売).
- 仮想機械レベルで可能なセキュリティ機能の導入



文部科学省 科学技術振興調整費
(平成18年度採択)

- 重要課題解決型研究
  - 情報セキュリティに資する研究開発
- 課題名
  - 高セキュリティ機能を実現する次世代OS環境の開発
- 研究期間
  - 平成18 (2006)年度から３年間

BitVisorのシステム構成



セキュアネットワーク管理

暗号化した仮想ネットワーク(VPN)により，通信を自動的に暗号化.

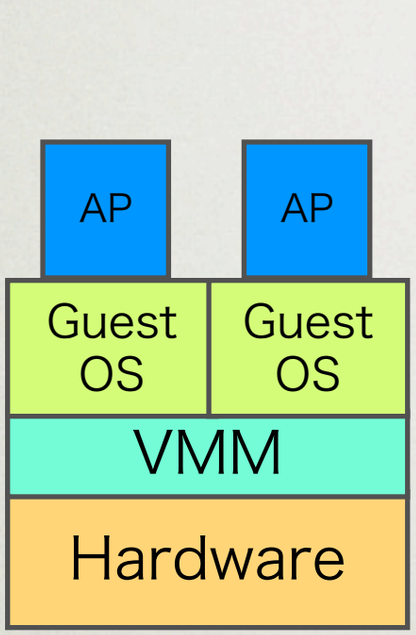
セキュアストレージ管理

ハードディスクやUSBメモリを暗号化．PCの盗難・紛失等が発生しても，セキュアIDなしには読み取り不能.

セキュアID管理

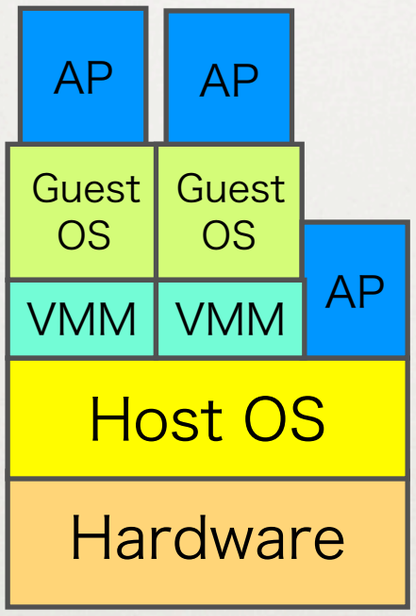
ユーザや利用目的を，政府職員ICカード等を用いて認証.
IDごとに利用環境を制御し、必要に応じて通信やファイル入出力を暗号化.

仮想マシンモニタの種類



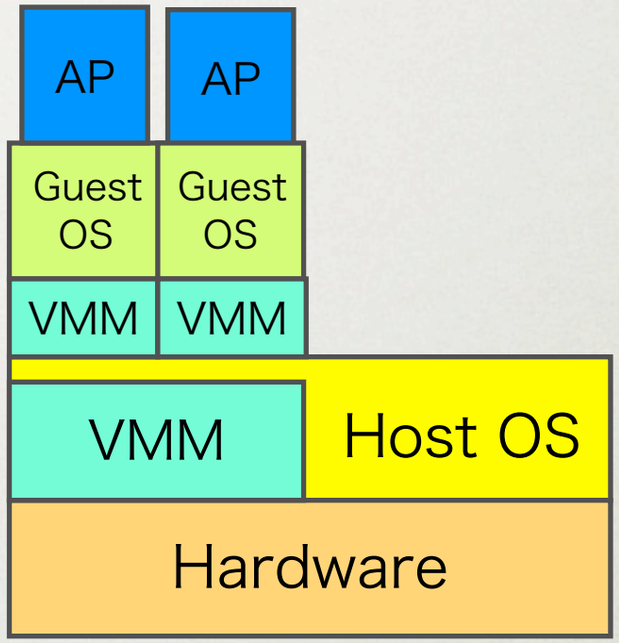
Type I
(hypervisor)

例　Xen, BitVisor



Type II

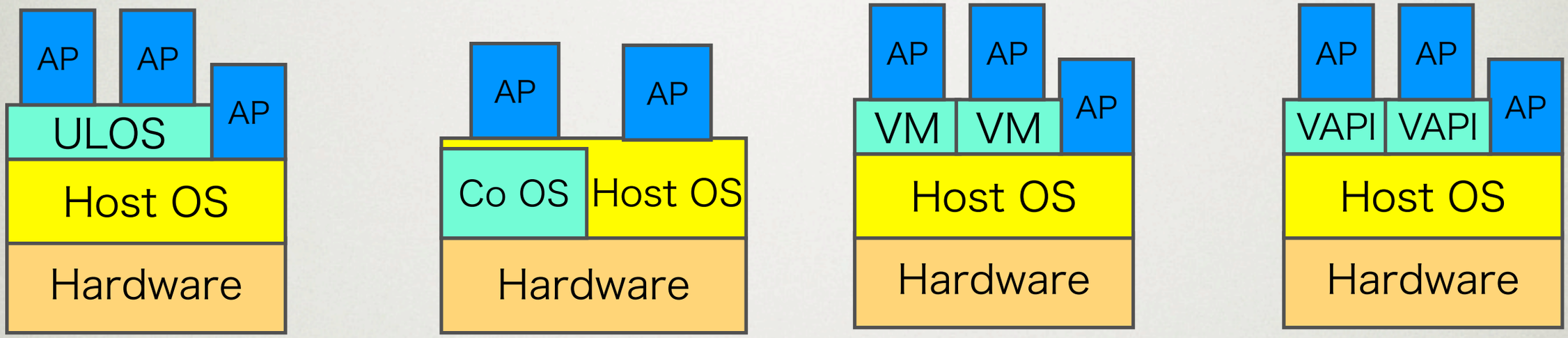
QEMU
LilyVM-U



Hybrid VMM

VMware workstation,
LilyVM-K

仮想マシンモニタ以外の仮想計算環境



ユーザレベルOS

User-Mode Linux

共存OS

CoLinux

プログラミング言語層VM

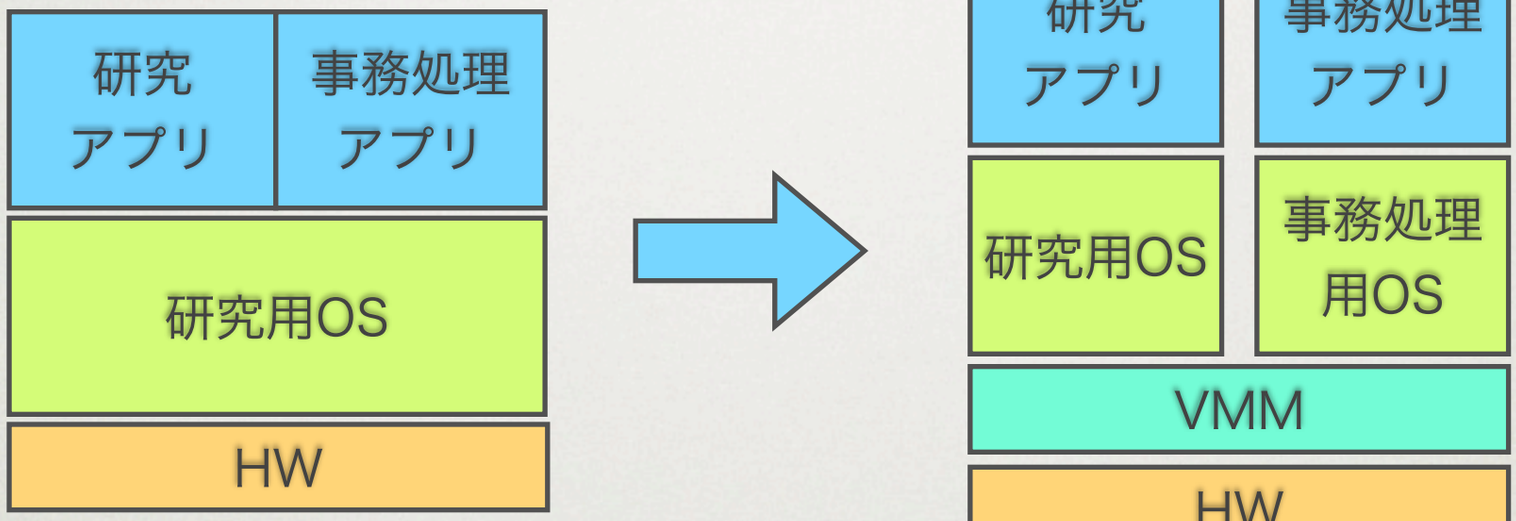
Java VM,
.NET CLI

仮想OS API

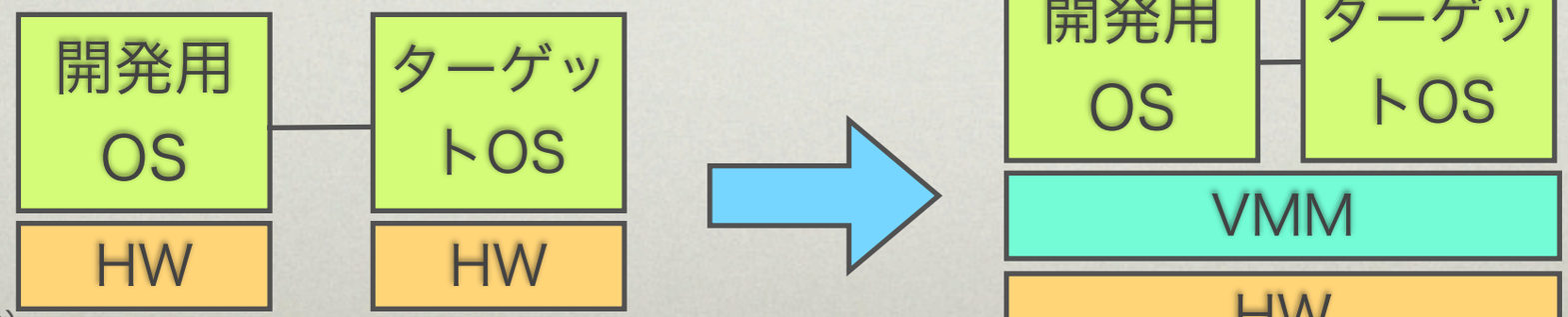
SoftwarePot

VMの利用法 (1/3)

	利用法	目的
1	**隔離** isolation	セキュリティ

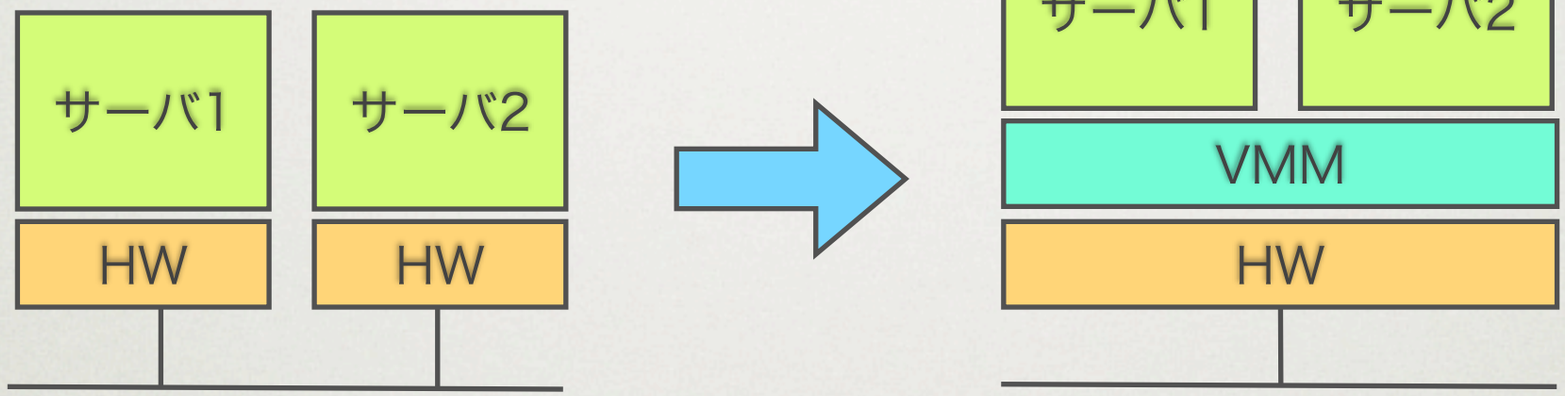


	利用法	目的
2	**ソフトウェアマシン** software machine	経済性 利用効率

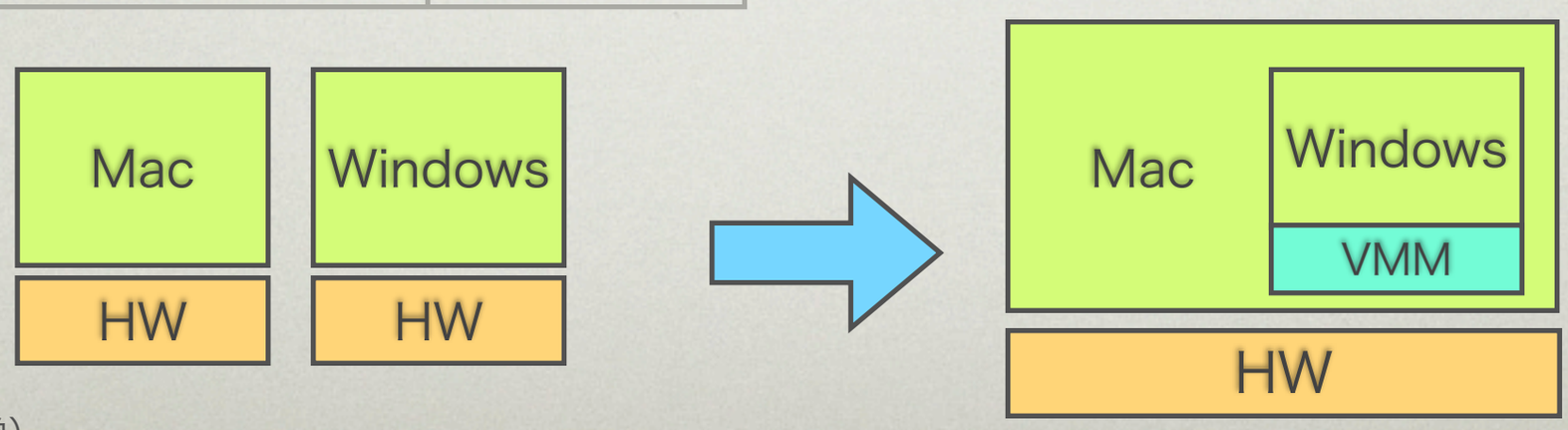


VMの利用法 (2/3)

	利用法	目的
3	**統合** consolidation	経済性 管理効率

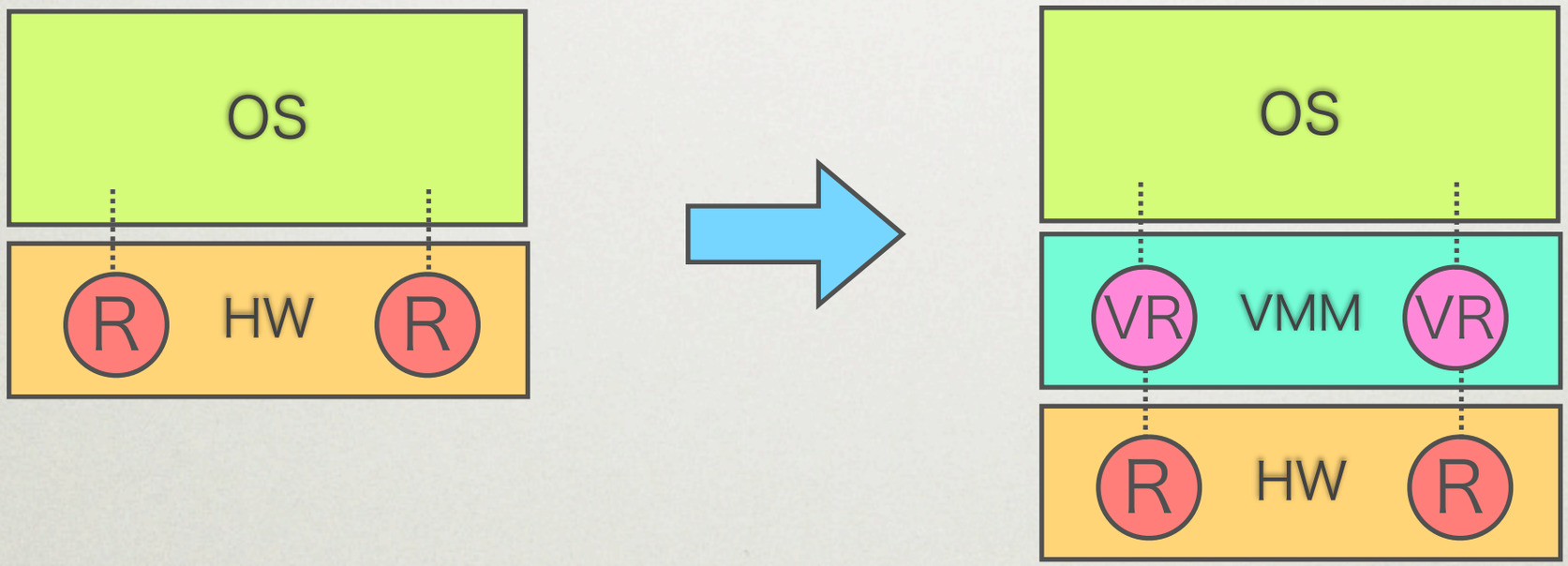


	利用法	目的
4	**複数OS** multiple OSs	開発効率

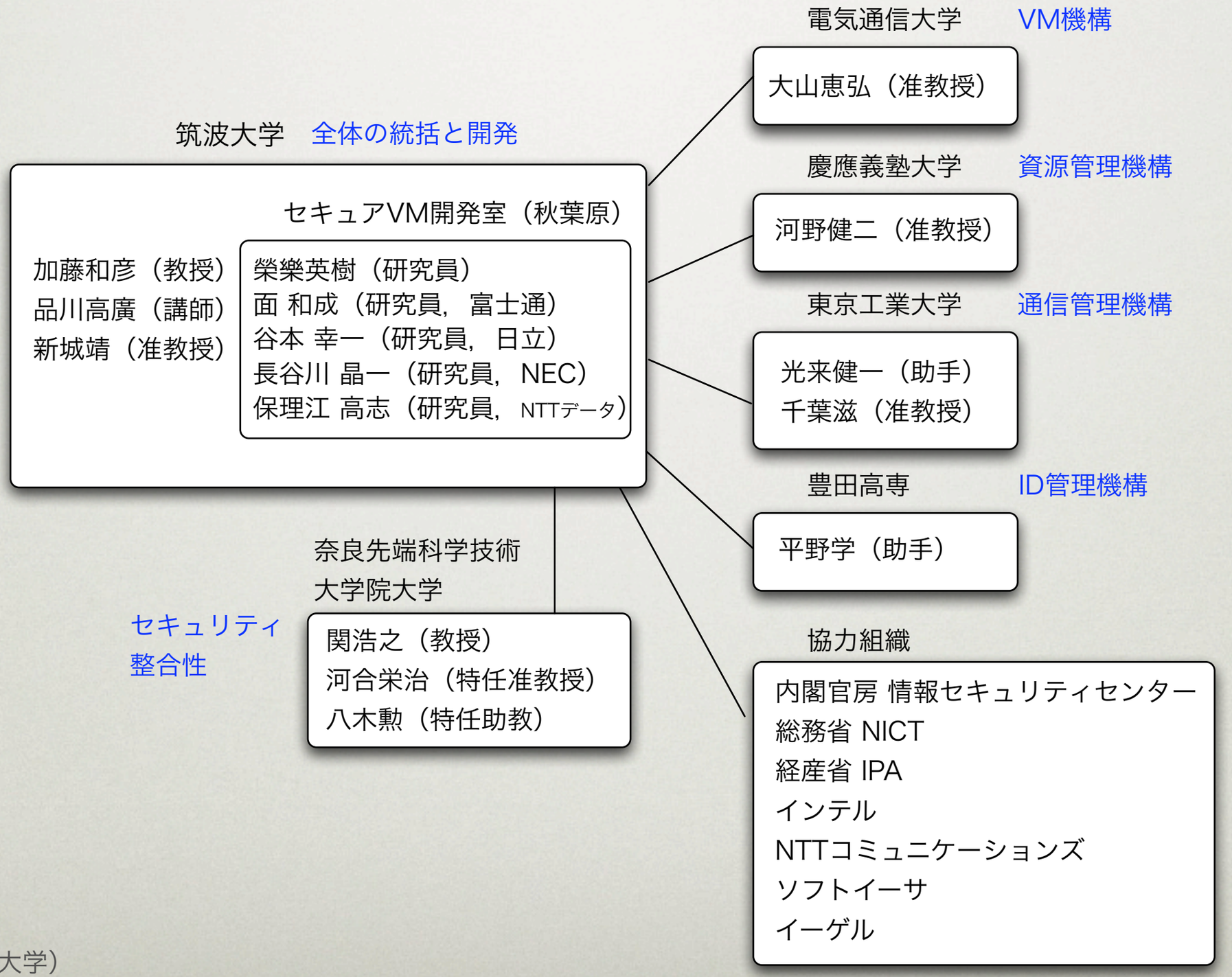


VMの利用法 (3/3)

	利用法	目的
5	**資源制御** resource control	セキュリティ



主要開発メンバー



チャレンジ

- 限られた時間とマンパワー
- フルスクラッチ
- デバイスドライバの取扱い
- ゲストOSとしてLinux & Windows XP/Vista
- 抑制されたソースコード量とオーバーヘッド

祝! 本日公開
BitVisor α版

- **公開サイト**
  http://www.securevm.org/
- **公開ソフトウェア**
  1. VMMコアのバイナリ及びソースコード
  2. VPNクライアント(IPv4, IPv6対応IPsec機能)のソースコード