高セキュリティ機能を実現する
次世代OS環境構築を目指して

加藤和彦
筑波大学大学院 システム情報工学研究科

2006年6月

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
  - 政府・行政機関からの個人情報，機密情報の漏洩
  - 民間企業からの個人情報等の漏洩

実社会での対策

- 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)

問題点(1/2)

- 現在広く使われているOSは，**インターネット以前**（＝クローズシステム時代）に基本設計が行われた.
  - Unix：1970年代に基本設計された少人数グループ用TSSシステム.
  - Windows, Mac：最初の設計はパーソナルOS.
- OSの基本機能として，システム**内部**の共有と保護機能を有するが，**外部**世界をも考慮した保護（すなわちセキュリティ）は未だ発展途上.
  - 外部環境に接続したネットワーク（e.g. インターネット）
  - 外部環境と交換される移動可能記憶メディア（e.g. CD-ROM, USBメモリ）

問題点(2/2)

- **サーバシステム**をターゲット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」

クライアント環境の難しさ

- 一般OS（Windows, Linux）は任意(discretionary） アクセス制御
  - ユーザ（≒管理者）が自在にアクセス制御を設定可能.
  - システム全体の管理者がアクセス制御を強制できない.
  - つまり，自己責任ベース.
- もはや集中型システム環境，独自・専用システム環境には戻れない.
  - コモディティハードウェア＋共通汎用システム利用による大幅コスト減効果.
  - サーバシステムよりも選択肢は狭いという現実.

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.
  - 継続的な人材／技術の維持ができていない.
- IT技術者は多くいるが（数的には世界有数），国産オリジナルのIT製品，IT文化を作り出せなくなっている.
  - ITに関して輸出できる技術，文化がない.
  - 「施工技術者」になってしまっている.

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.

文部科学省 科学技術振興調整費

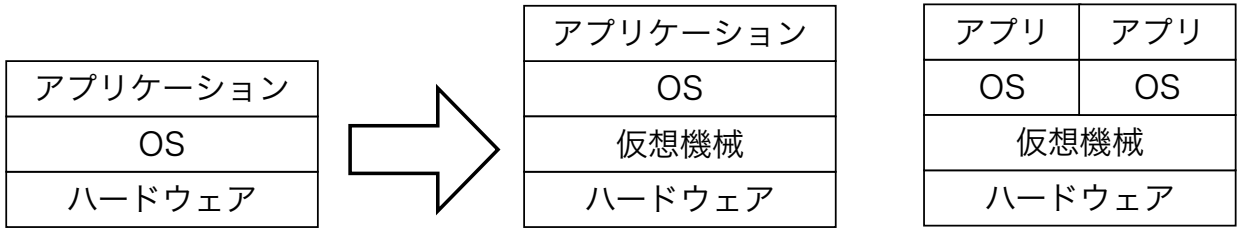
- 科学技術振興調整費とは
  - 総合科学技術会議(議長：内閣総理大臣)の方針に基づく科学技術の振興に必要な重要事項の総合推進調整のための経費として文部科学省の予算として計上された、政策誘導型の競争的資金.
- 重要課題解決型研究とは
  - 国家的、社会的に重要な政策課題であって、単独の府省では対処が困難であり、政府として速やかに取り組むべき政策目標及び課題について、産学官の複数の研究機関による総合的な推進体制の下で、具体的な達成目標を設定し研究開発を推進する。

平成18年度
文部科学省 科学技術振興調整費

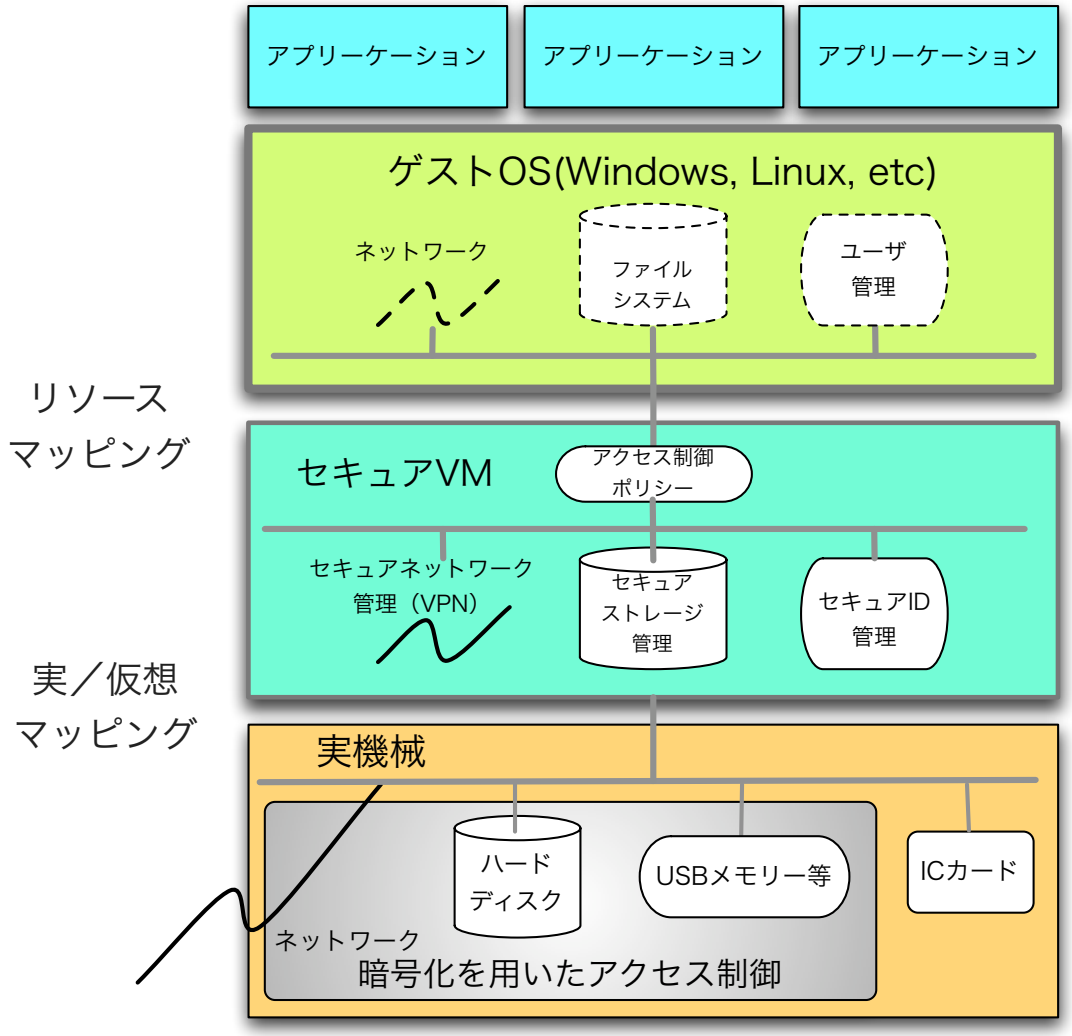
- 重要課題解決型研究
  - 情報セキュリティに資する研究開発
- 課題名
  - 高セキュリティ機能を実現する次世代OS環境の開発
- 研究期間
  - 2006年度から３年間

アプローチ

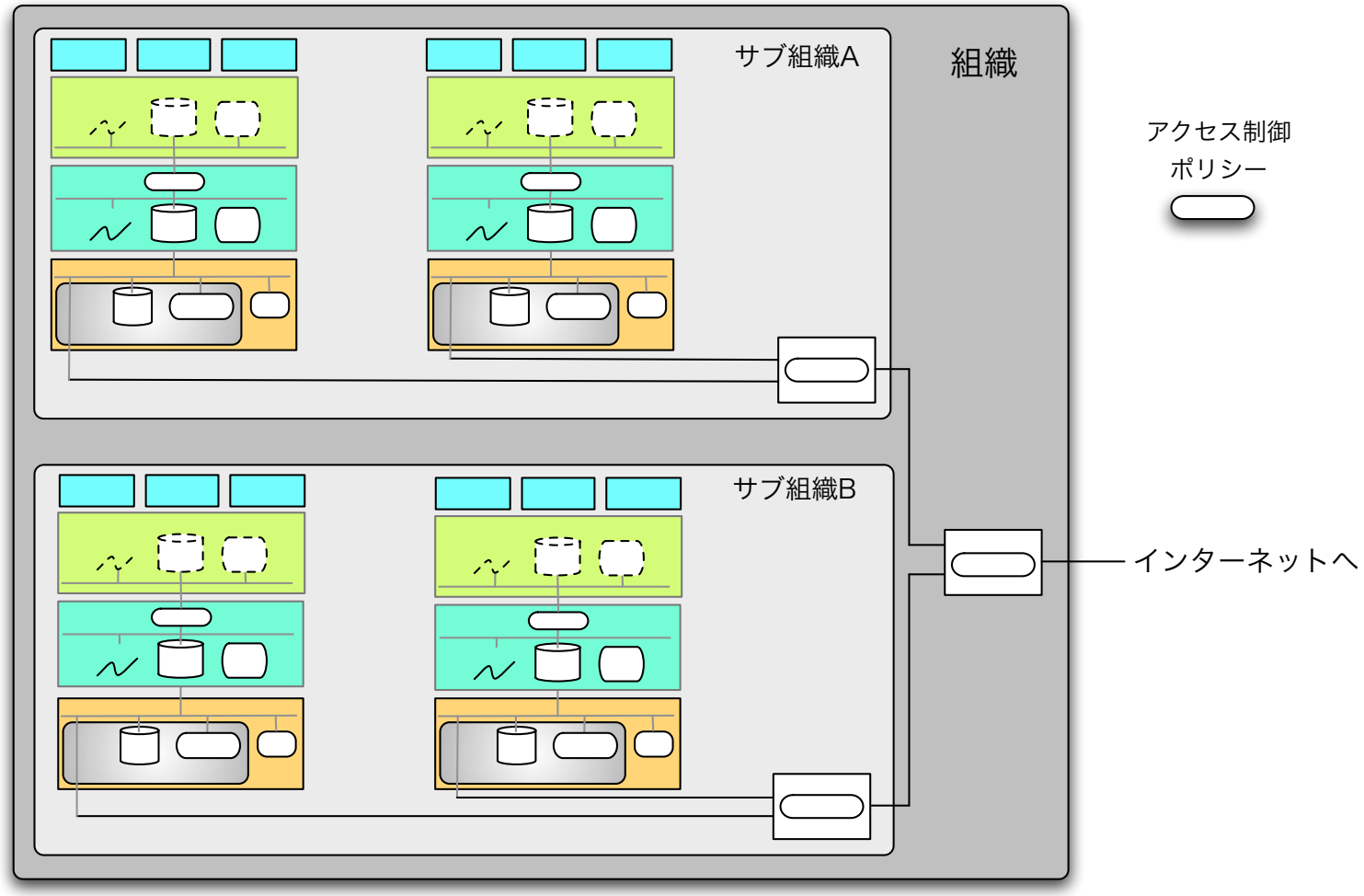
- 仮想機械技術に着眼
  - 大型計算機システムにおいては1960年代より知られる技術.
  - 近年，パソコンにおいても利用可能となってきた.
  - 仮想機械をサポートするマイクロプロセッサが登場.
    (インテル社VT技術搭載CPUが2005年11月より発売).
- セキュア機能を組み込んだ仮想機械によりOS環境ごと制御
  - 隔離とマッピングにより，現状環境との互換性を確保しつつ，高セキュリティを達成.
- クライアント，エンドユーザ環境のセキュア化



システム構成 (1/2)


アプリーケーション
アプリーケーション
アプリーケーション
ゲストOS(Windows, Linux, etc)
ネットワーク
ファイル
システム
ユーザ
管理
リソース
マッピング
セキュアVM
アクセス制御
ポリシー
セキュアネットワーク
管理（VPN）
セキュア
ストレージ
管理
セキュアID
管理
実／仮想
マッピング
実機械
ハード
ディスク
USBメモリー等
ICカード
ネットワーク
暗号化を用いたアクセス制御

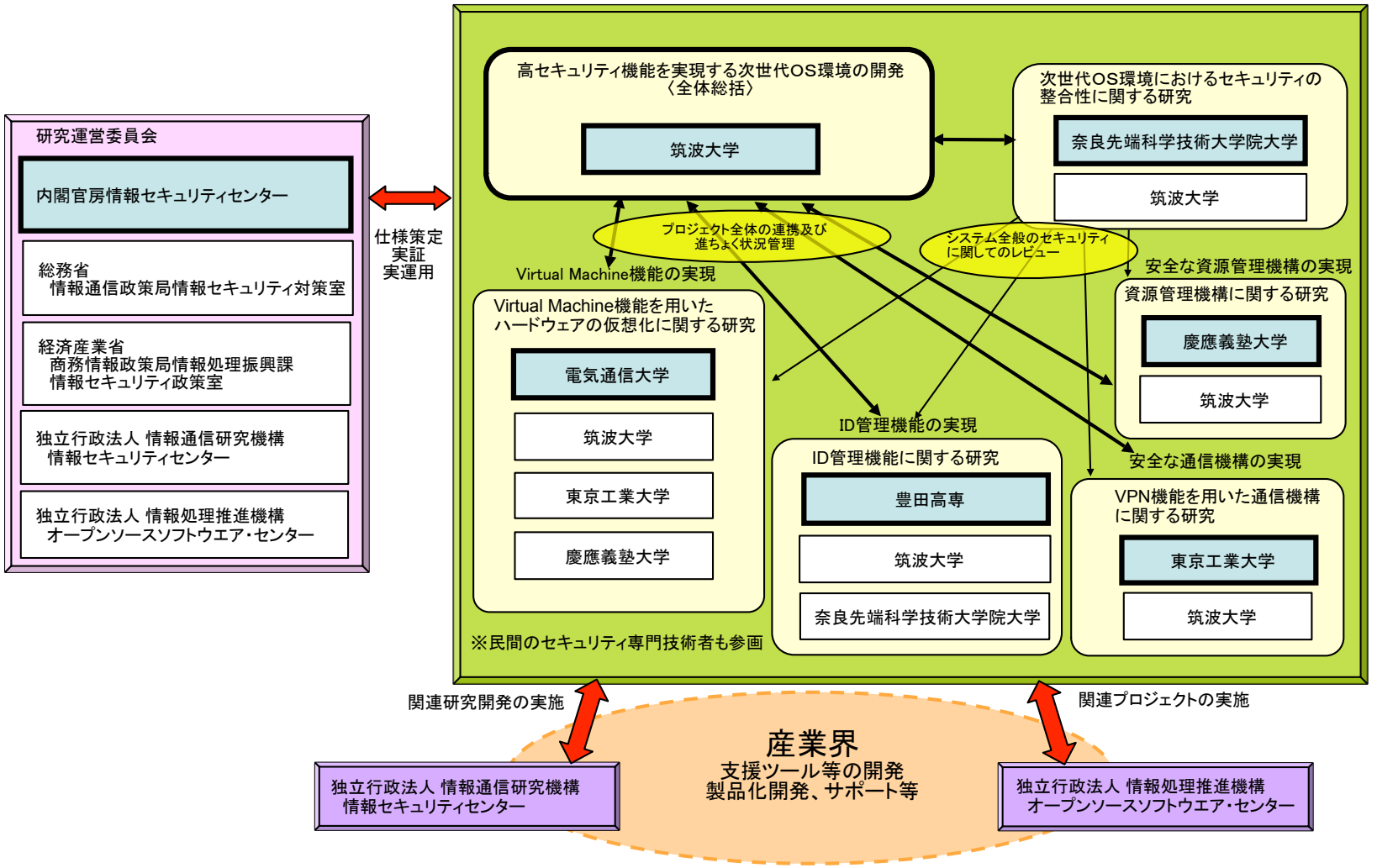
組織による統一アクセス制御ポリシー



研究開発体制

- ユーザ（政府）と開発者（学＋産）の密なコラボレーションによる設計と実装
  - 政府：内閣官房情報セキュリティセンター
  - 学：筑波大，電通大，東工大，慶大，奈良先端大，豊田高専
  - 産：富士通，NEC，日立製作所，NTT，NTTデータ，ソフトイーサ
- IT関連省庁との横断的連携
  - 総務省，経済産業省
  - IPA, NICT, AIST
- 産業界との連携
  - セキュアIT基盤開発推進コンソーシアム

研究開発体制


研究運営委員会
内閣官房情報セキュリティセンター
総務省
情報通信政策局情報セキュリティ対策室
経済産業省
商務情報政策局情報処理振興課
情報セキュリティ政策室
独立行政法人 情報通信研究機構
情報セキュリティセンター
独立行政法人 情報処理推進機構
オープンソースソフトウエア・センター
仕様策定
実証
実運用
高セキュリティ機能を実現する次世代OS環境の開発
〈全体総括〉
筑波大学
次世代OS環境におけるセキュリティの
整合性に関する研究
奈良先端科学技術大学院大学
筑波大学
プロジェクト全体の連携及び
進ちょく状況管理
システム全般のセキュリティ
に関してのレビュー
Virtual Machine機能の実現
Virtual Machine機能を用いた
ハードウェアの仮想化に関する研究
電気通信大学
筑波大学
東京工業大学
慶應義塾大学
安全な資源管理機構の実現
資源管理機構に関する研究
慶應義塾大学
筑波大学
ID管理機能の実現
ID管理機能に関する研究
豊田高専
筑波大学
奈良先端科学技術大学院大学
安全な通信機構の実現
VPN機能を用いた通信機構
に関する研究
東京工業大学
筑波大学
※民間のセキュリティ専門技術者も参画
関連研究開発の実施
関連プロジェクトの実施
産業界
支援ツール等の開発
製品化開発、サポート等
独立行政法人 情報通信研究機構
情報セキュリティセンター
独立行政法人 情報処理推進機構
オープンソースソフトウエア・センター

まとめ

- 仮想機械技術を用いて，互換性を確保しつつ，高セキュリティを達成.
  - 今が好機
- 開発者（学＋産）とユーザ（政府機関）の密なコラボレーション.
  - 産業界との連携も推進
- 基盤ソフトウエアの優れた研究開発能力を有する若手研究者，技術者の育成.