

セキュアVMワークショップ
「開発者自らが語るVMの作り方」

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11月18日

富士ソフト アキバプラザ

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.
 - ❖ セキュアOS機能
- 最近の問題はむしろクライアント
 - ❖ 「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)
 - ❖ 「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」

さらに根深い問題

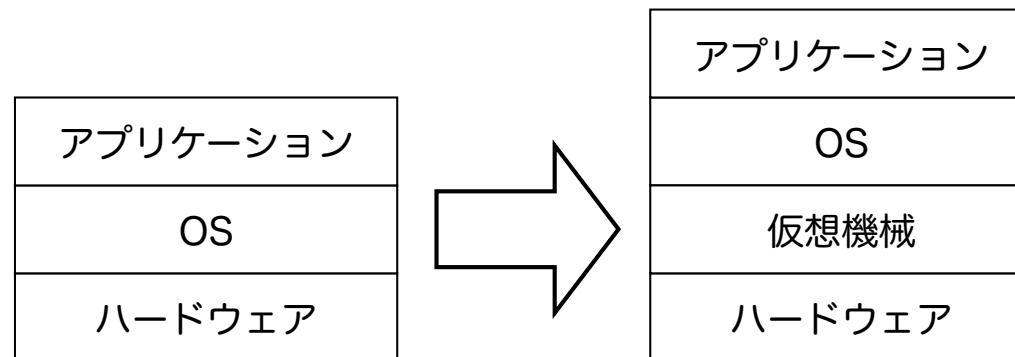
- 基盤システムソフトウェアの基本設計は米国を中心とした海外陣営に抑えられてしまった。
 - ❖ 基盤ソフトウェアレベルに容易には手が出せなくなっている。
- 以前は多くいた産業界の基盤システムソフトウェア技術／技術者が失われつつある。
 - ❖ 某企業幹部：「50代以上ならいますが若い人は本当に少ないんです」
 - ❖ 参考図書を探すと、80年代、90年代
 - ❖ 某ハードウェア会社：「マニュアルの日本語版も昔は沢山ありましたが、今はなくなりましたね」

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

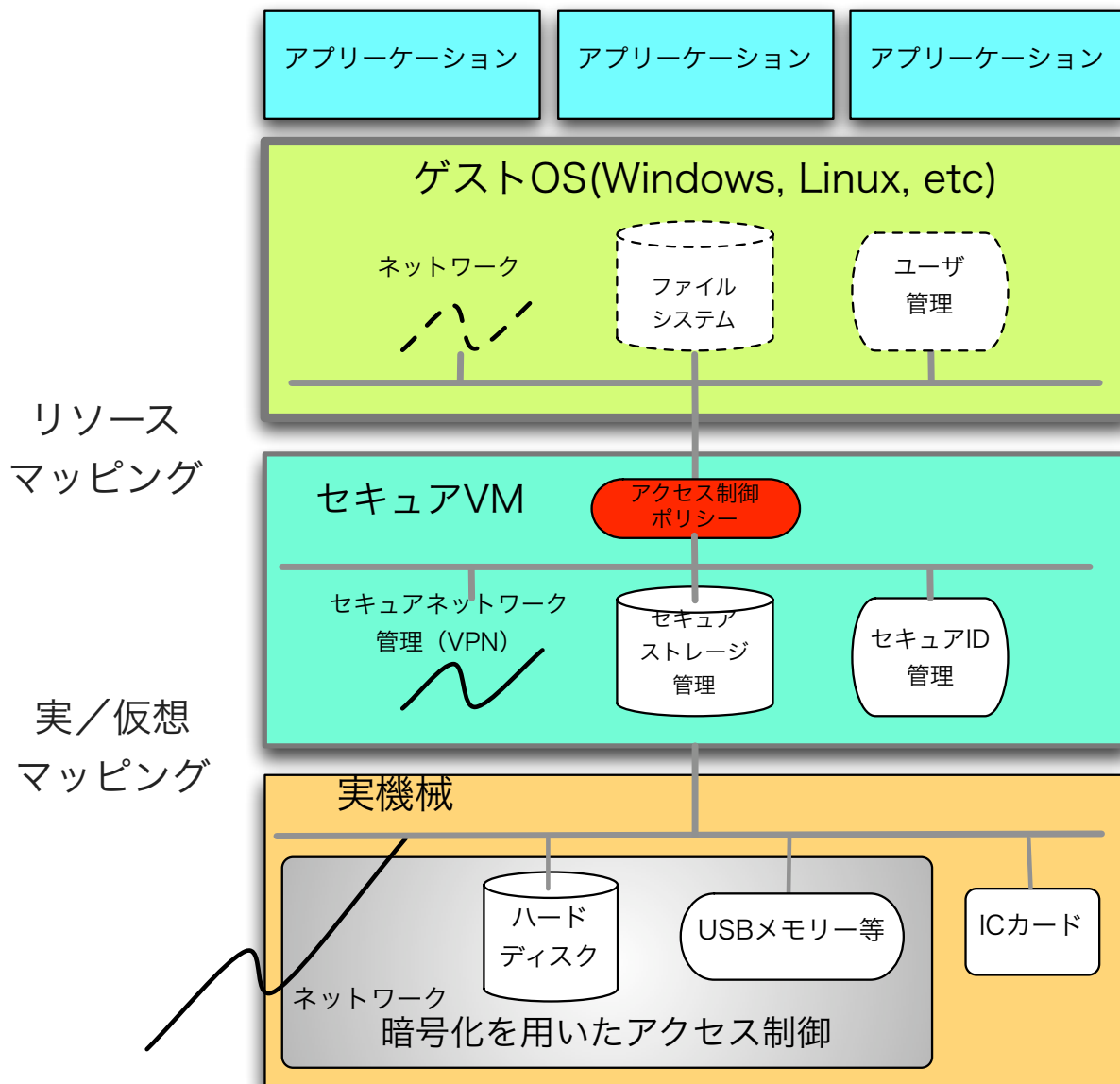


振興調整費

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

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。

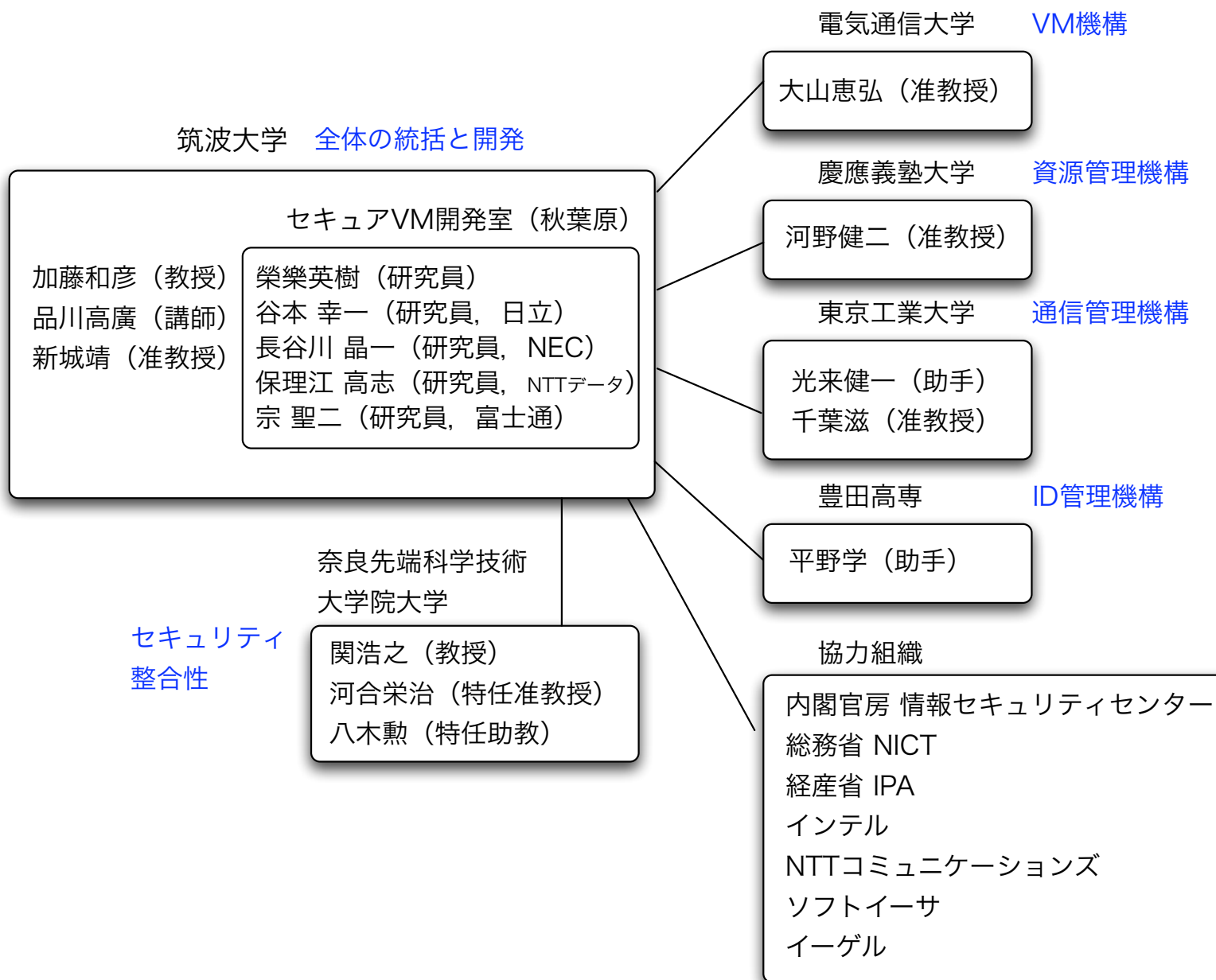
セキュアストレージ管理

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。

主要開発メンバー



運営委員会 (半年に1回)

加藤 和彦	筑波大学 教授 (委員長)	山口 英	内閣官房 情報セキュリティセンター 情報セキュリティ補佐官 奈良先端科学技術大学院大学 教授
品川 高廣	筑波大学 講師		
大山 恵弘	電気通信大学 准教授	大久保 明	内閣府 政策統括官
河野 健二	慶應義塾大学 准教授	新井 孝雄	総務省 情報通信政策局 情報セキュリティ対策室長
光来 健一	九州工業大学 准教授		
千葉 滋	東京工業大学 教授	八尋 俊英	経済産業省 商務情報政策局 情報処理振興課長
関 浩之	奈良先端科学技術大学院大学 教授	篠田 陽一	情報通信研究機構(NICT) 情報通信セキュリティ研究センター長
平野 学	豊田工業高等専門学校 助教	田代 秀一	情報処理推進機構(IPA) オープンソースソフトウェアセンター長
		坂村 健	YRPユビキタス・ネットワーキング研究所長 東京大学 教授

科学技術振興機構(JST)

田浦 健次郎	プログラムオフィサー (研究領域主管) 東京大学 准教授
林原 光男	プログラムオフィサー (プログラム主管)
北村 義男	主任調査員

セキュア VM を実現するソフトウェア「BitVisor」の開発初期版を公開

国立大学法人 筑波大学(学長:岩崎洋一)は、高セキュリティ機能を持った次世代 OS 環境「セキュア VM」を実現するソフトウェアである「BitVisor」の開発初期版の公開を 3 月 19 日より開始しました。

BitVisor とは

BitVisor とは、筑波大学を中心とするセキュア VM プロジェクトにおいて開発中の仮想マシンモニタ(VMM^{*1})と呼ばれるソフトウェアです。BitVisor では、クライアント PC における情報漏洩を防止するために、仮想マシン(VM^{*2})の技術を利用して Windows^{*3}や Linux 等の OS からは独立した形でセキュリティ機能を実現します。具体的には、ストレージやネットワークの暗号化、ID 管理などの機能を仮想マシンで実現することにより、PC や USB メモリの盗難や紛失、ウィルス感染等による情報漏洩を防止します。

セキュア VM プロジェクトは現在、文部科学省の平成 18 年度科学技術振興調整費^{*4}で採択された研究課題「高セキュ

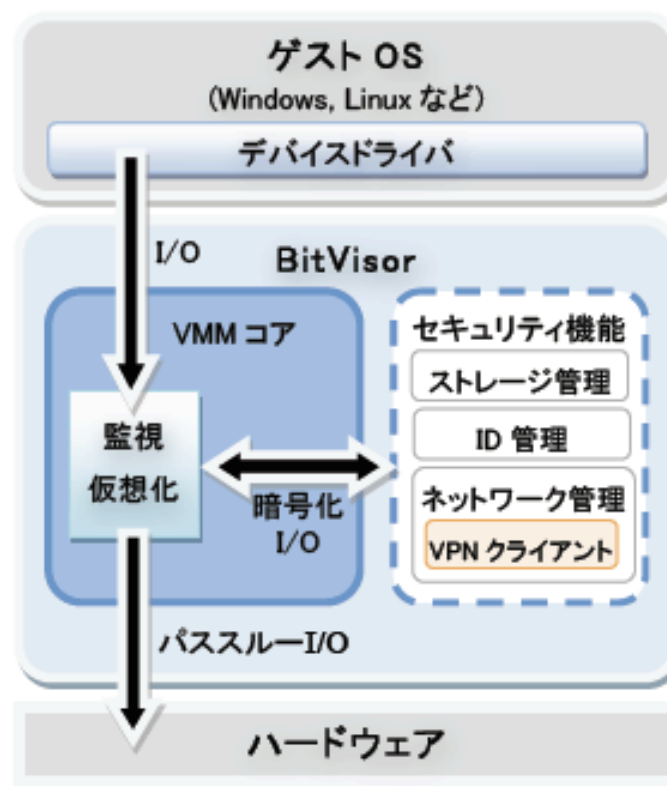


図 1: BitVisor 概要

シンポジウム

- 第1回セキュアVMシンポジウム
 - ✓ 2007年3月20日13:00~17:10
 - ✓ 東京グランドホテル
- 第2回セキュアVMシンポジウム
 - ✓ 2007年3月20日13:00~17:10
 - ✓ 富士ソフト アキバプラザ
- セキュアVMワークショップ
「開発者自らが語るVMの作り方」
 - ✓ 2008年11月18日（本日）
 - ✓ 富士ソフト アキバプラザ

BitVisorホームページ <http://www.securevm.org/>



セキュアVMプロジェクト

Google™ サイト検索:

検索

更新日: 2008年6月19日(木)

ホーム

プロジェクト

アウトリーチ

BitVisor

リンク

仮想マシンモニタ

技術情報

報道関係

その他

日本発! 国産セキュア仮想マシンモニタ

HDD暗号化、USBメモリ暗号化、TypeB ICカード認証、
64bitゲスト/ハイパーバイザー、Intel VT/AMD-V対応、...

BitVisor (ビットバイザー) 0.7

近日公開予定

ニュース

2008年11月1日 (土)

BitVisorに関する論文がVEE 2009に採録決定

- BitVisor に関する論文 "BitVisor: A Thin Hypervisor for Enforcing I/O Device Security" が、国際会議 VEE 2009 (The 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments) に採録されることが決定しました。

2008年10月23日 (木)

セキュアVMワークショップを近日開催予定

- 11月18日 (火) にセキュアVMワークショップ「開発者自らが語るVMの作り方」を富士ソフトアキバプラザで開催予定です。定員は先着80名となっておりますので、お早めにお申し込みください。

2008年8月7日 (木)

SWoPPにおいて研究成果を発表

- 2008年並列/分散/協調処理に関する『佐賀』サマー・ワークショップ (SWoPP佐賀 2008) において、BitVisorに関する研究発表をおこないました。

アウトリーチ

ご意見・ご要望など

メールで下記のアドレスまでお願いします。
svm-support@oss.cs.tsukuba.ac.jp

アウトリーチ

セキュアVMワークショップ

日時: 2008年11月18日(火)
場所: 富士ソフト アキバプラザ

ソフトウェア

BitVisor 0.3

バイナリ&ソースコード

ダウンロード

アクセス数: 28264



BitVisor ダウンロード

免責事項

- 本ソフトウェアは開発途上のα版（試作版）です。一切の動作は保証しません。
- 本ソフトウェアを使用したことにより、いかなる損害が生じても、一切の責任を負いません。

公開ソフトウェア

現在公開しているソフトウェアは、以下のとおりです。

BitVisor 0.3

- BitVisor 0.3 バイナリ: 既存のOSをゲストOSとして起動して動作を確認していただけます。
※セキュリティ機能は搭載されていません。
- BitVisor 0.3 ソースコード: BitVisor 0.2に安定性向上、高速化のための修正等を行いました。BitVisor 0.2からの主な変更点は、以下の通りです。
 - BIOS 呼び出しをマルチプロセッサ初期化前におこない、起動時の安定性を向上させました。
 - 4GiB以上のアドレスを扱えるようにしました。
 - 対応ゲストOSに次のOSが追加されました。
 - FreeBSD 7 (32bit版)
 - Windows XP x64 SP2, Windows Vista x64
 - Debian GNU/Linux (64bit版)
 - FreeDOS EMM386.EXE
 - シャドウページングを高速化しました。
 - IEEE1394デバイスをゲストOSから不可視としました。
 - VMMで確保するメモリを32MiBから64MiBに拡大しました。

BitVisor 0.2

- BitVisor 0.2 バイナリ: 既存のOSをゲストOSとして起動して動作を確認していただけます。
※、セキュリティ機能は搭載されていません。
- BitVisor 0.2 ソースコード: VMMコア及びディスク暗号化機能の開発初期版が含まれています。ディスク暗号化はデフォルトではOFFに設定されています。
- VPNクライアントモジュール (IPv4, IPv6): OSに依存せずにIPSecを利用できるモジュールです。現時点ではまだBitVisorに組み込まれていませんが、汎用IPSecモジュールとしてご活用下さい。

※BitVisor は準バススルー型アーキテクチャを採用しており、動作するゲストOSは1つのみです。

ソフトウェア

BitVisor 0.3

バイナリ&ソースコード

[ダウンロード](#)

BitVisor バイナリのダウンロード

- [bitvisor-0.3.elf](#)
- [bitvisor-0.2.x86.elf](#) (32bit版)
- [bitvisor-0.2.x64.elf](#) (64bit版)

※ディスク暗号化は無効になっています。インストール済のOSを起動できます。

BitVisor ソースコードのダウンロード

- [bitvisor-0.3.tar.gz](#) (md5sum: ba6db1fb995de29bdaafae887c4d6643)
- [bitvisor-0.3.tar.bz2](#) (md5sum: d945142c8125511075c9bf0ae0d0a3f8)
- [bitvisor-0.2.tar.gz](#)
- [bitvisor-0.2.tar.bz2](#)

VPN クライアントモジュールのダウンロード

現時点ではまだBitVisorに組み込まれていませんが、OSに依存しないIPSecモジュールとしてご活用下さい。

- VPN クライアントモジュール(IPv4版)
 - ソースコード ([vpn_ipv4_only.tar.gz](#))
 - ビルドマニュアル ([build_ipv4.pdf](#))
 - テストマニュアル ([test_ipv4.pdf](#))
- VPN クライアントモジュール(IPv6版)
 - ソースコード ([vpn_ipv6_only.tar.gz](#))
 - ビルドマニュアル ([build_ipv6.pdf](#))
 - テストマニュアル ([test_ipv6.pdf](#))

アクセス数: 6512



アウトリーチ：出前講義

- 2007年12月20日 13:15~15:05
 - ✓ 茨城県立並木高等学校
- 2008年2月1日 10:20~12:10
 - ✓ 筑波大学附属中学校
- 2008年10月25日 11:00~12:50
 - ✓ 神奈川県立弥栄高等学校

テレビ番組

- Just Japan! (ジャストジャパン)
 - ✓ 制作：テレビ神奈川（提供：内閣府）
 - ✓ H20.3.1(土) 放送(TVK他, UHF局14局ネット)
- サイエンスチャンネル
 - ✓ 制作：科学技術振興機構(JST)
 - ✓ SKY PerfecTV! 76ch でインターネット放送中

Just Japan (ジヤスト・ジャパン)

- 内閣府が提供する, 政府広報番組. 放送局は, 全国のUHF局14局.

とちぎテレビ 日 9:30~10:00

群馬テレビ 日 8:30~9:00

テレビ埼玉 日 8:30~9:00

千葉テレビ 土 8:00~8:30

東京MXテレビ 土 7:30~8:00

テレビ神奈川 土 22:00~22:30

テレビ和歌山 土 9:00~9:30

岐阜放送 土 9:00~9:30

三重テレビ 土 10:30~11:00

びわ湖放送 日 11:30~12:00

京都放送 土 9:00~9:30

サンテレビ 火 8:00~8:30

奈良テレビ 土 7:55~8:25

セキュアVMワークショップ 「開発者自らが語るVMの作り方」

日時：平成20年11月18日（火） 主催：筑波大学

会場：富士ソフト アキバプラザ（秋葉原駅近く） 参加費：無料

参加申し込み：<http://www.securevm.org/svmw.html>

【プログラム】

13:00-13:20 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 教授）

13:20-14:00 セキュアVM「BitVisor」のアーキテクチャ概要

品川 高廣（筑波大学大学院 システム情報工学研究科 講師）

14:00-14:40 PCの仮想化支援機能とBitVisorコア技術詳細

榮樂 英樹（筑波大学大学院 システム情報工学研究科 研究員）

14:40-15:00 休憩

15:00-15:40 BitvisorとI/O仮想化技術

保理江 高志（筑波大学大学院 システム情報工学研究科 研究員）

15:40-16:20 BitVisorにおけるUSBの仮想化方式

松原 克弥（（株）イーゲル シニアアーキテクト）

16:20-17:00 BitVisorにおける透過的なVPN処理の設計と実装

登 大遊（ソフトイーサ（株）会長）