2012年12月4日（火）
筑波大学 東京キャンパス文京校舎

BitVisor Summit

【主催】
（社）情報処理学会
システムソフトウェアとオペレーティングシステム研究会
（第24回コンピュータシステム・シンポジウム 併設イベント）

開催趣旨

BitVisor Summit は、BitVisor に興味を持つ幅広い層の方々に交流や情報交換の場を提供することを目的としています。

BitVisor は純国産の仮想マシンモニタですが、BitVisor のように日本国内において研究開発されており、なおかつ高い完成度を持つ低レイヤのシステムソフトウェアはそれほど多くはないのではないかと思われます。

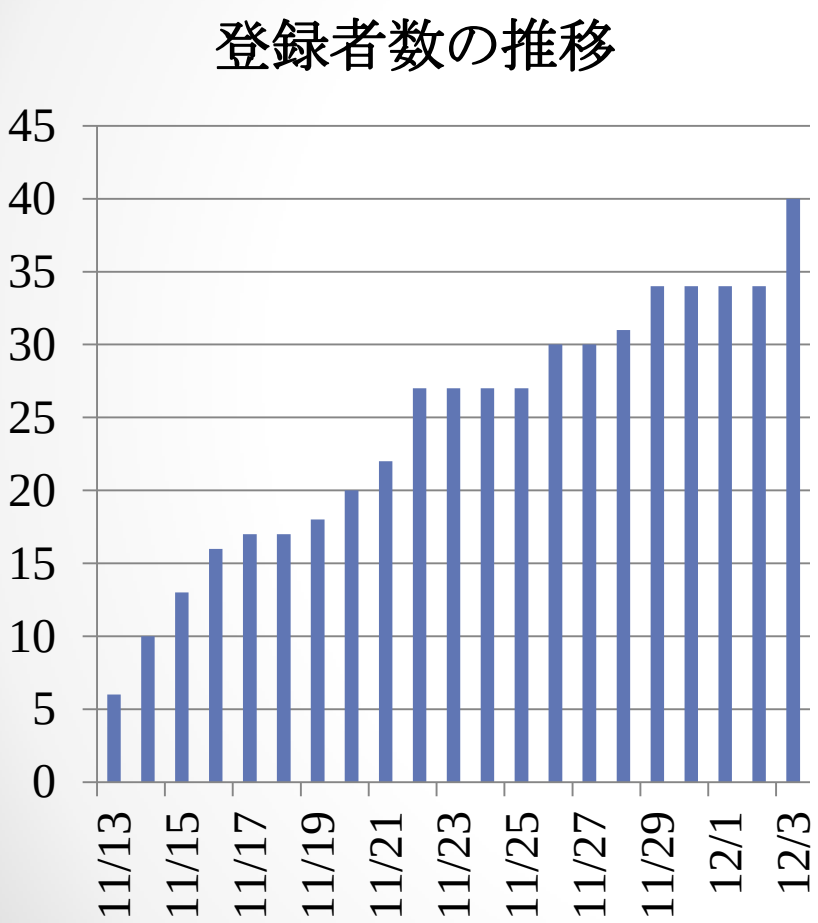
本 Summit では、BitVisor に関する最新の技術的な情報の交換の場を提供するほか，仮想化技術やOSカーネルなど、高度な基盤システムソフトウェア全般に興味を持った研究者・開発者・ユーザが交流する稀少な機会として有益な場となることを期待しています.

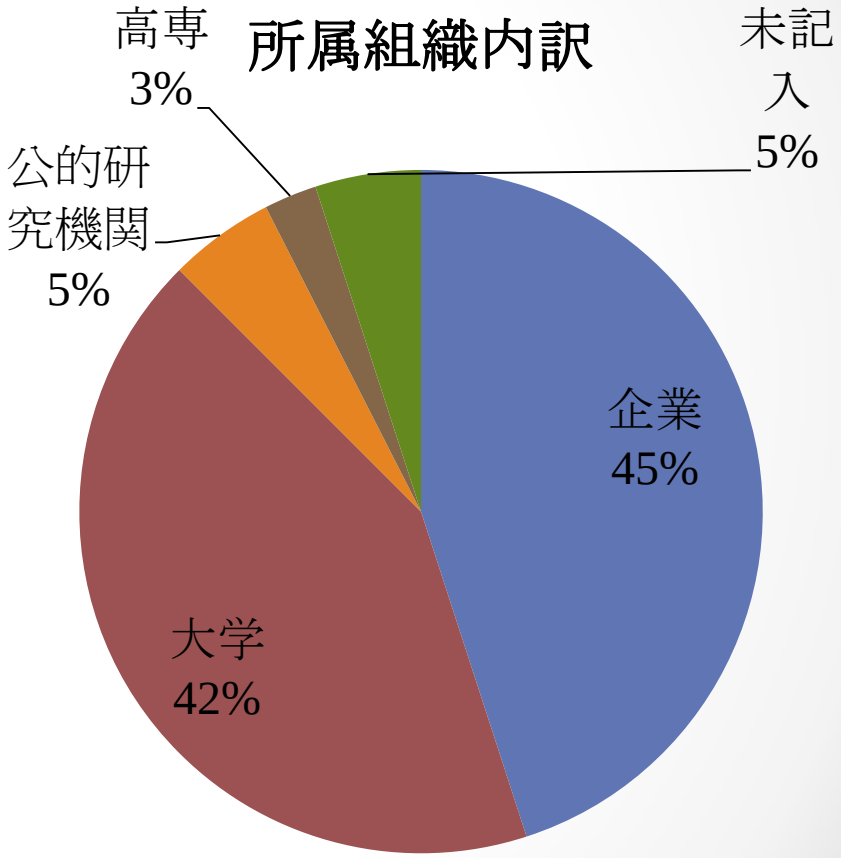
講演者内訳

- 招待講演×３件
  - 榮樂 英樹 様（株式会社イーゲル）
  - 松原 克弥 様（株式会社イーゲル）
  - 村上 純一 様（フォティーンフォティ技術研究所）

- 一般講演×６件
  - 産業技術総合研究所×1件
  - 筑波大学×2件
  - 電気通信大学×2件
  - 立命館大学×1件

参加登録者


登録者数の推移
45
40
35
30
25
20
15
10
5
0
11/13
11/15
11/17
11/19
11/21
11/23
11/25
11/27
11/29
12/1
12/3


所属組織内訳
高専
3%
未記入
5%
公的研究機関
5%
企業
45%
大学
42%

BitVisorの現状と今後

品川高廣（東京大学）

BitVisorの歴史

- 2006年：セキュアVMプロジェクトで研究開発開始
- 2008年 3月：BitVisor 0.2公開
- 2009年 3月：BitVisor 1.0公開
  - VMMコア、ディスク・ネットワーク暗号化、ICカードによる鍵管理
- 2010年 6月：BitVisor 1.1公開
  - 保護ドメイン機能、AHCI対応、Realtek NIC対応、...
- 2011年10月：BitVisor 1.2公開
  - Suspend/Resume対応、ATA Piggyback、TCB BIOS対応、...
- 2012年 9月：BitVisor 1.3公開
  - バックグラウンド暗号化（特許出願済）、EPT/NPT、ADvisor機能、...

BitVisorを支えた競争的資金

- 平成18年度～20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
  - 「高セキュリティ機能を実現する次世代OS環境の開発」
  - 研究代表者：加藤和彦（筑波大学）

- 平成21年度～23年度
  - 総務省 戦略的情報通信研究開発推進制度（SCOPE）
    - ICTイノベーション促進型研究開発
  - 「ディペンダブルな自律連合型クラウドコンピューティング基盤の研究開発」
  - 研究代表者：加藤和彦（筑波大学）

- 平成22年度
  - JST 研究成果最適展開支援事業（A-STEP）
    - フィージビリティスタディ【FS】ステージ・シーズ顕在化タイプ
  - 「高セキュリティを実現する仮想マシンモニタ（BitVisor）の実用化検証」
  - 企業責任者：松原克弥（株式会社イーゲル）、研究責任者：品川高廣

BitVisorを支える(支えた)人

チーフアーキテクト
品川(東京大学)
ATA, PCI

松原氏 (イーゲル)
USB(UHCI,EHCI)

NTT Com
IDman (PKCS #11)

登氏 (ソフトイーサ)
VPN (IPsec)
Intel Pro 100

榮樂氏 (イーゲル)
VMMコア
Intel Pro 1000
保護ドメイン
AHCI
EPT/NPT
その他全般

北村氏 (イーゲル)
Suspend/Resume

保理江氏(NTTデータ)
VT-d (IOMMU)

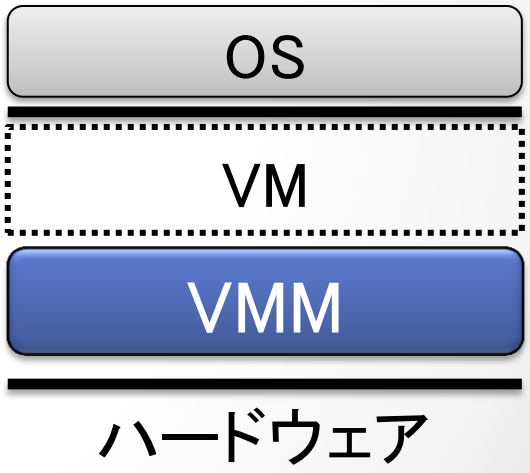
大山氏 (電通大)
ADvisor

表氏 (筑波大学)
バックグラウンド暗号化

サイエンスパーク
Realtek NIC

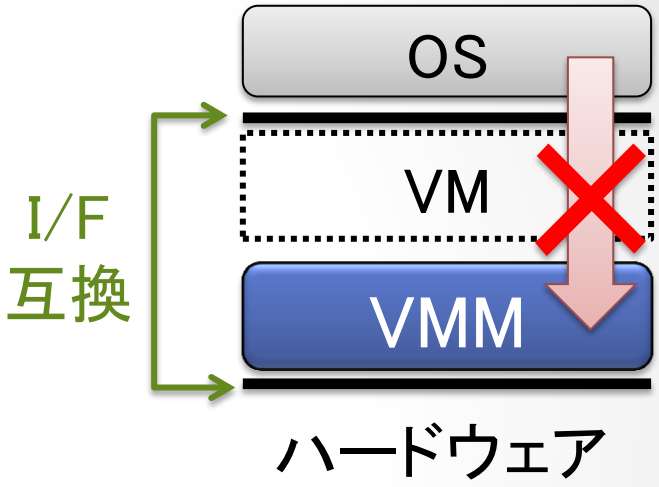
BitVisorとは

- 仮想化ソフトウェアの一種
  - 仮想マシンモニタ ＝ Virtual Machine Monitor (VMM)
    - ハイパーバイザ ＝ Hypervisor (Type I VMM)
      - ホストOSに頼らずハードウェア上で直接動作
  - OSとハードウェアの間で動作する
    - 仮想マシン ＝ Virtual Machine (VM) を作り出す
  - Single-VM仮想化
    - ある時点で動作するOSは一つだけ

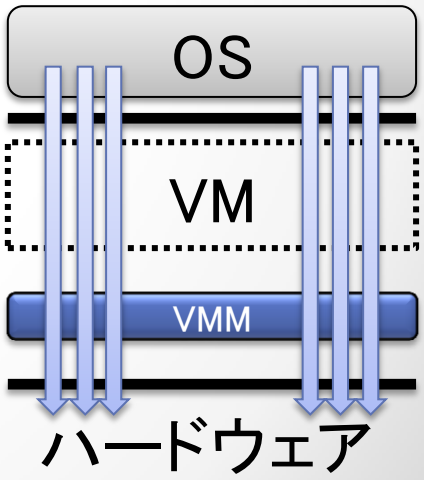


Single-VMの利点

- 仮想化の利点を活用できる
  - セキュリティ
    - ゲストOSより高い特権レベルで動作する
  - 互換性
    - ゲストOSを修正せずに機能追加を行える



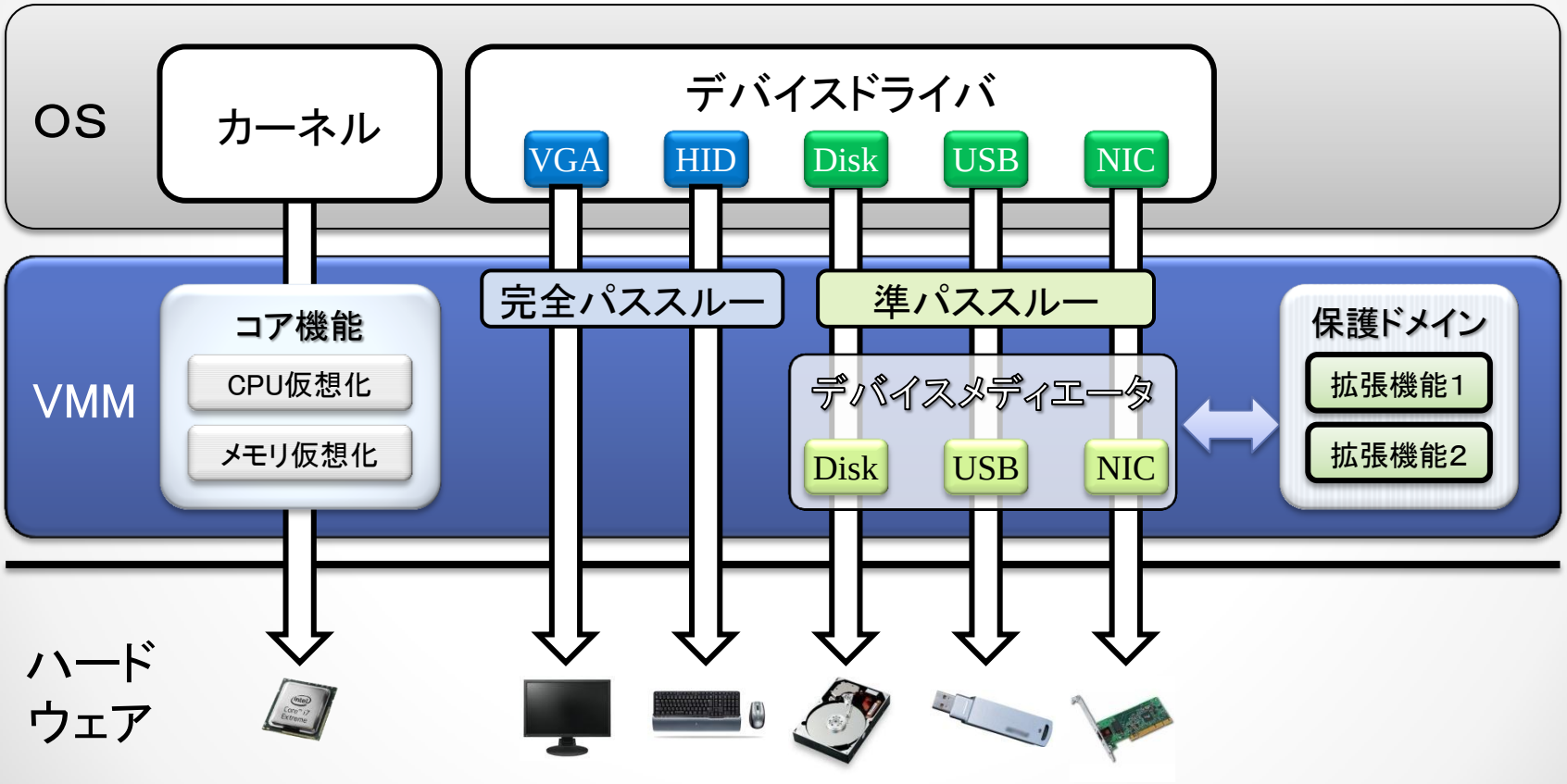
- VMMを小さく出来る
  - セキュリティ
    - Trusted Computing Base (TCB)のサイズ削減
      - 一般にプログラムは小さいほど安全とされている
  - オーバーヘッド
    - 仮想化に伴うコストを削減できる



BitVisor の基本アーキテクチャ

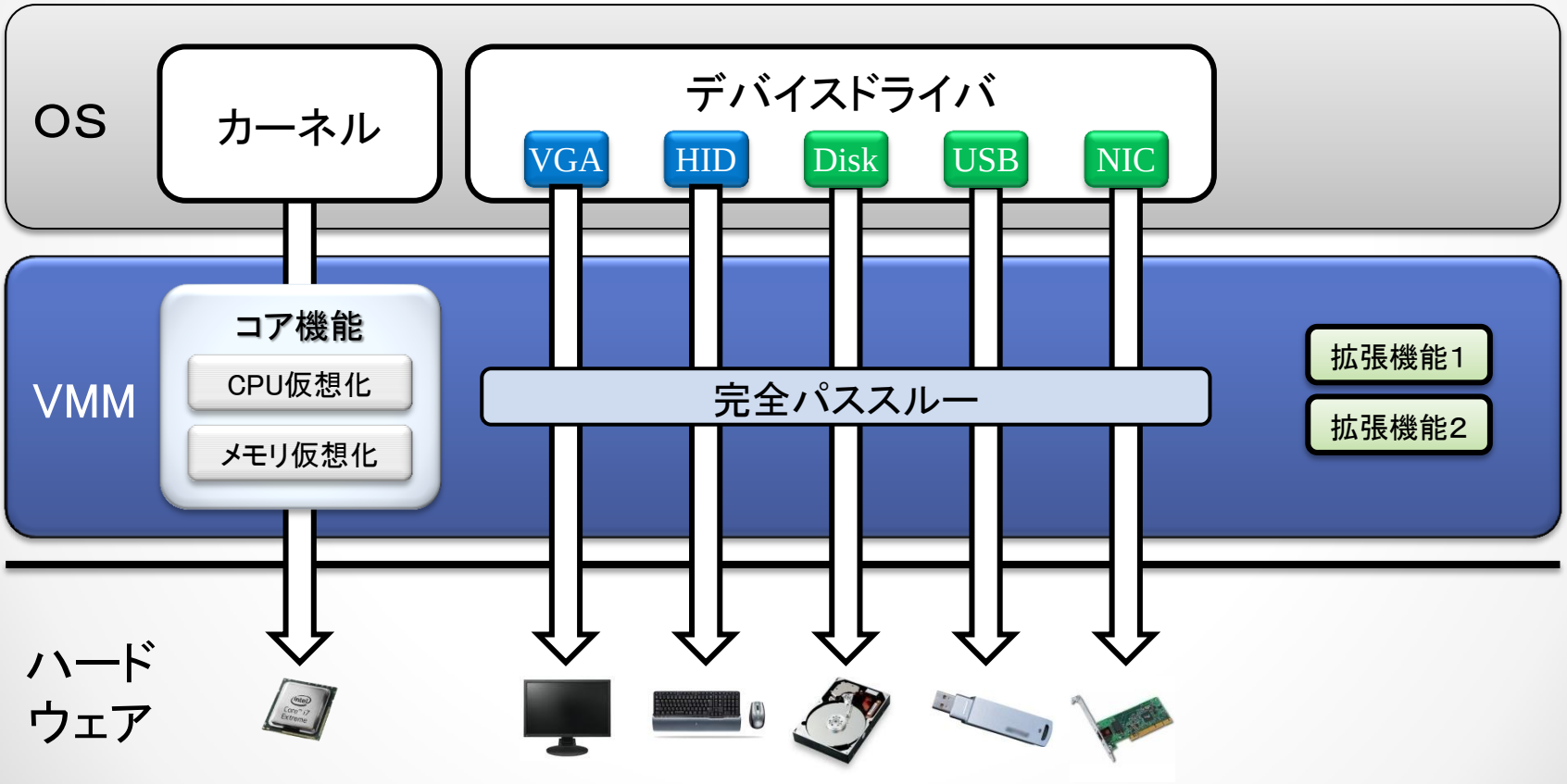
準パススルー型(↔準仮想化)

[Shinagawa et al. VEE '09]



BitVisor の応用型(1)

「コア機能」のみ

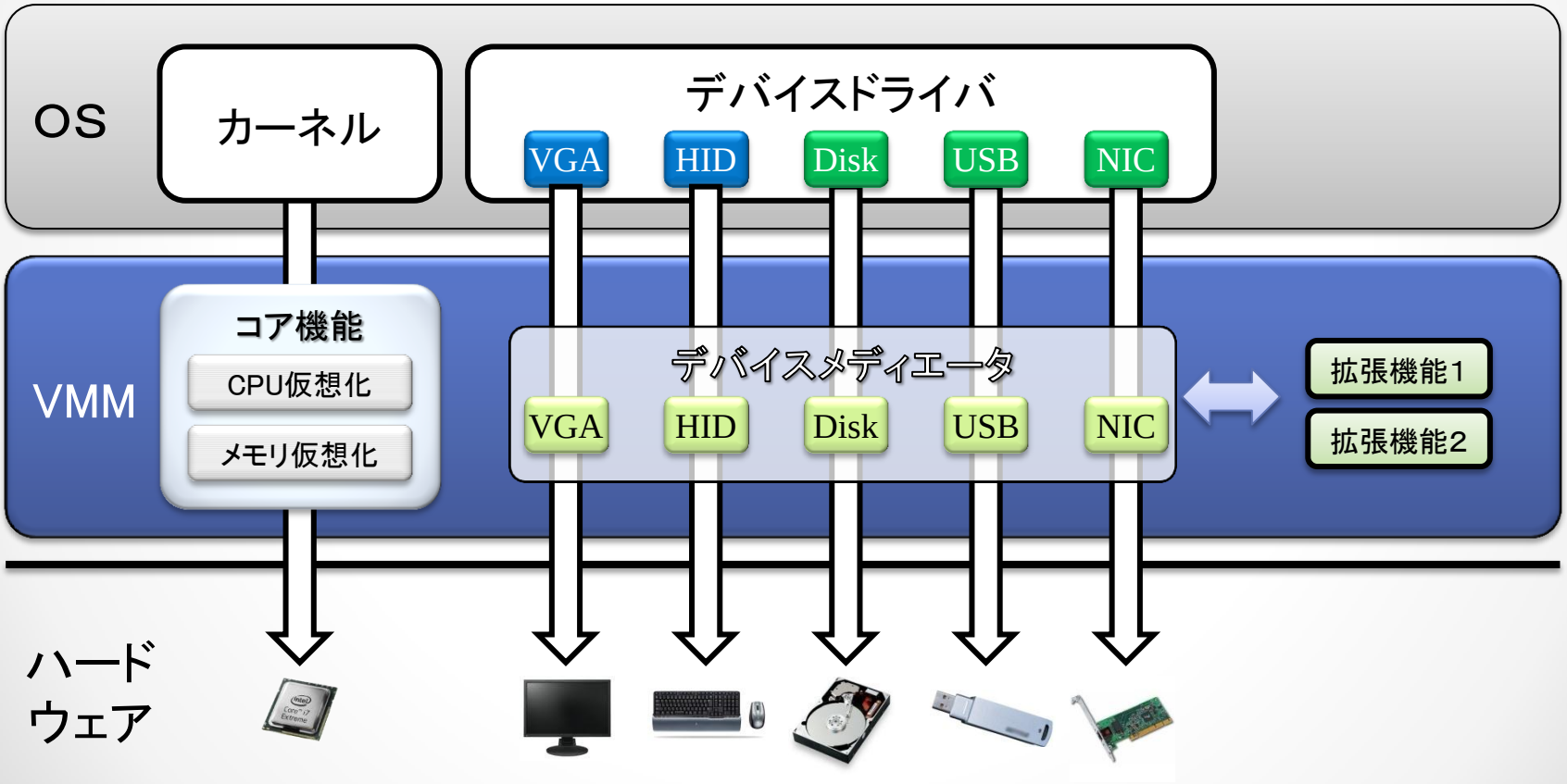


コア機能の仮想化レベル

- CPU仮想化
  - VMM に制御が戻る条件の On/Off
    - 割り込み、システムレジスタ、制御関係、メモリ関係、I/O関係
  - BitVisor の機能の On/Off
    - タイマースレッド、保護ドメイン
- メモリ仮想化
  - ページ保護の On/Off
    - Shadow Paging 無し／有り、EPT（+Unrestricted Guest）
  - MMIOの捕捉

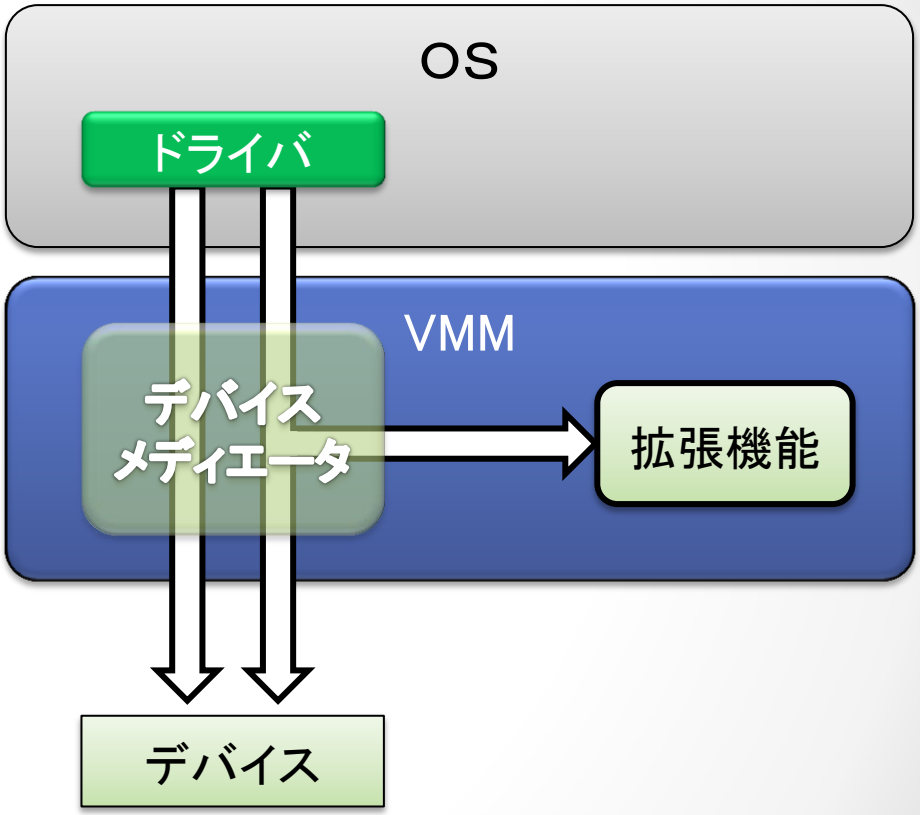
BitVisor の応用型(2)

「コア機能」＋ n ×「準パススルードライバ」



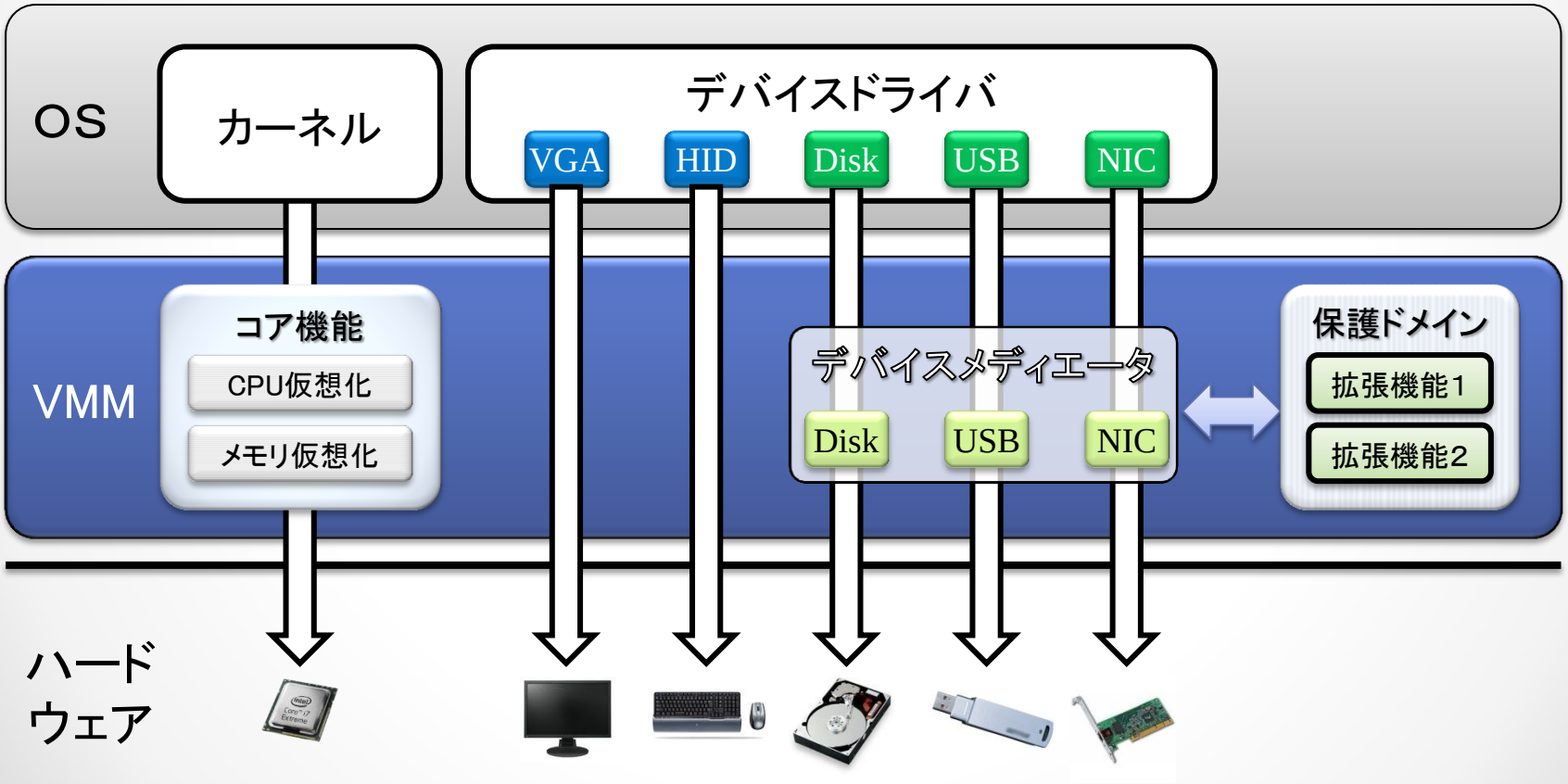
準パススルーのレベル

- 監視のみ
  - IDSなど
- 監視＋変換
  - アクセス制御
  - 暗号化
- 多重化（Piggyback）
  - VMMによる機能追加
    - Disk, USB, NIC



BitVisor の応用型(3)

保護ドメイン(Process)



BitVisor の応用研究の例

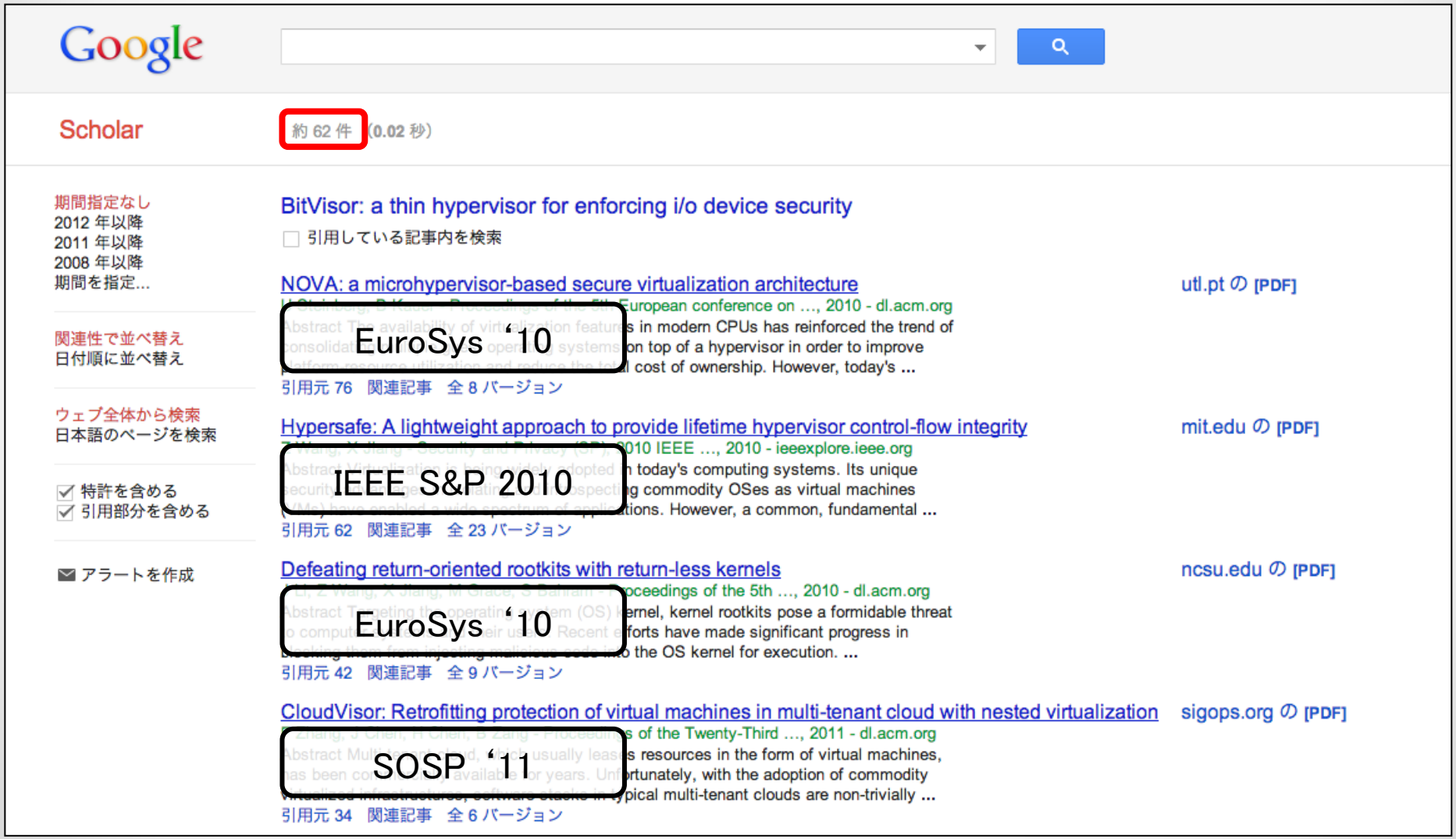
加藤(筑波大学)・品川(東京大学)の共同研究

	VMM コア	Disk	USB	NIC	保護ドメイン
セキュアVM	☑	☑	☑	☑	
システムファイル保護	☑	☑			
透過的VPN切り替え	☑			☑	
透過的ネットワークブート	☑	☑		☑	
ボランティアコンピューティング	☑			△	☑
デバドラ検証	☑	○	○	○	

BitVisor を使った世界の研究

- TCVisor [Rezaei *et al.*, ICITST '10]
  - ユーザ毎に特定のストレージ領域のみを見せる仕組み
    - TPM, password, security tokenの組み合わせで実現
- HyperSafe [Wang *et al.*, IEEE S&P '10]
  - Hypervisor自身の完全性を維持する仕組み
    - Hypervisor を書き換えられなくする
- "Return-less" VMM [Li *et al.*, EuroSys '10]
  - ret命令のないカーネル・VMMを実現
    - ROR (Return-Oriented Rootkit)対策

論文の参照数


Google
Scholar
約 62 件 (0.02 秒)
期間指定なし
2012 年以降
2011 年以降
2008 年以降
期間を指定...
関連性で並べ替え
日付順に並べ替え
ウェブ全体から検索
日本語のページを検索
特許を含める
引用部分を含める
アラートを作成
BitVisor: a thin hypervisor for enforcing i/o device security
引用している記事内を検索
NOVA: a microhypervisor-based secure virtualization architecture
utl.pt の [PDF]
European conference on ..., 2010 - dl.acm.org
EuroSys '10
in modern CPUs has reinforced the trend of
on top of a hypervisor in order to improve
cost of ownership. However, today's ...
引用元 76 関連記事 全 8 バージョン
Hypersafe: A lightweight approach to provide lifetime hypervisor control-flow integrity
mit.edu の [PDF]
2010 IEEE ..., 2010 - ieeexplore.ieee.org
IEEE S&P 2010
today's computing systems. Its unique
commodity OSes as virtual machines
tions. However, a common, fundamental ...
引用元 62 関連記事 全 23 バージョン
Defeating return-oriented rootkits with return-less kernels
ncsu.edu の [PDF]
roceedings of the 5th ..., 2010 - dl.acm.org
EuroSys '10
ernel, kernel rootkits pose a formidable threat
forts have made significant progress in
the OS kernel for execution. ...
引用元 42 関連記事 全 9 バージョン
CloudVisor: Retrofitting protection of virtual machines in multi-tenant cloud with nested virtualization
sigops.org の [PDF]
of the Twenty-Third ..., 2011 - dl.acm.org
SOSP '11
resources in the form of virtual machines,
rtunately, with the adoption of commodity
ypical multi-tenant clouds are non-trivially ...
引用元 34 関連記事 全 6 バージョン

TinyVisor

SOURCEFORGE.JP オープンソース・ソフトウェアの開発とダウンロード

ログイン アカウント作成 ヘルプ

MY SF.JP | ソフトウェアを探す | Magazine | 開発

Wiki 検索

SourceForge.JP > ソフトウェアを探す > TinyVisor > Wiki > **TinyVisorの機能**

TinyVisor

概要 | ニュース | ダウンロード | ソースコード | Wiki | メーリングリスト | チケット

編集 | PDF | ページ一覧 | 最近の更新 | 検索

TinyVisorの機能

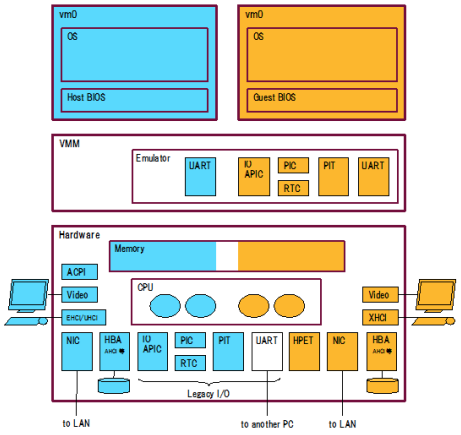
1. CPU、メモリ、I/OのVMへの割り当て

TynyVisorは、PCに内蔵されているCPU、メモリ、I/OをVMに割り当て、OSから使用可能にします。

CPU、メモリ、I/Oを割り当てる単位は次の通りです。

要素	割り当て単位	備考
CPU	論理プロセッサ単位(Hyper-ThreadingのThread単位)	BSPは必ずvm0に割り当てられる。Intel VT-xまたはAMD SVMを使用して仮想化している。
メモリ	ページ単位(4KB単位)	Intel VT-xのEPTまたはShadow Pagingを使用して仮想化している。
I/O	PCIe Root Port単位(PCIeスロット単位)	MSIまたはMSI-Xに対応していないI/Oデバイスをvm0以外のVMに割り当てると、割り込みを使えない。Intel VT-d(IOMMU)を使用して仮想化している。AMD IOMMUには未対応。

CPU、メモリ、I/Oの割り当ての概念図を次に示します。



CPU、メモリ、I/Oの割り当ての概念図

vm0のOSからは、水色のCPU、メモリ、I/Oを使用することができます。 vm1のOSからは、橙色のCPU、メモリ、I/Oを使用することができます。

Legacyl/Oは、OSの動作に必要不可欠なI/Oデバイスですが、PCに一組しかありません。そのため、二組あるかのようにVMMがエミュレートして、OSから使用可能にします。

Wiki目次

- FrontPage
- TinyVisorの機能
- 動作実績のあるハードウェア
- 動作実績のあるOS
- TinyVisorのインストール方法
- TinyVisorの使い方

最近の更新 (Recent Changes)

2012-10-07
- FrontPage

2012-09-29
- SideBar
- 動作実績のあるOS

2012-07-16
- 動作実績のあるハードウェア

2012-07-15
- TinyVisorの機能

2012-06-23
- TinyVisorの使い方

最新リリース情報

tinyvisor (0.7) 2012-09-29

BitVisorの今後の課題

- 機能向上
  - デバイス対応
    - USB 3.0（xHCI），NIC（Marvell, Broadcom），無線LAN, RAIDカード, ...
  - マシン・OS対応
    - EFI（Mac対応）, Nested Virtualization, MMConfig, ...
  - 開発者向け対応
    - 依存関係対応Config, API整理，ドキュメンテーション
  - オーバヘッド削減
    - EPT, スレッド, Preemption Timer
- 商業化
  - セキュアVM, ネットワークブート，...

まとめ

- BitVisorの現状と今後
  - 準パススルー型アーキテクチャ
    - VMMコア機能
    - デバイス・メディエータ
    - 保護ドメイン
  - 応用研究・開発
    - 加藤・品川研究室
    - 世界の研究
    - TinyVisor
  - 今後の課題
    - デバイス対応，マシン対応，開発者向け対応，オーバーヘッド削減
    - 商業化

BitVisor の宣伝

- BitVisor に関する情報
  - ホームページ
    - http://www.bitvisor.org/
  - メーリングリスト（@bitvisor.org）
    - bitvisor-user（日本語）, bitvisor-user-en（英語）
    - bitvisor-devel（日本語）, bitvisor-devel-en（英語）
  - ソースコード
    - http://sourceforge.net/projects/bitvisor/
- 有償サービス
  - （株）イーゲルが提供