

Xen Summit Tokyo 2008

品川 高廣(筑波大学)

Introduction to BitVisor and Comparison with Xen

BitVisor とは？

- セキュリティ機能を備えた仮想マシンモニタ
 - 「セキュアVMプロジェクト」で開発中
 - 政府サポートに基づく研究開発プロジェクト
 - 内閣官房情報セキュリティセンター(NISC)が主導
 - 文部科学省 科学技術振興調整費による財政支援
- ゼロから開発(純国産)
 - 筑波大学を中心とした複数の大学・組織で開発
 - プロジェクトの期間は3年間(2006～2008)

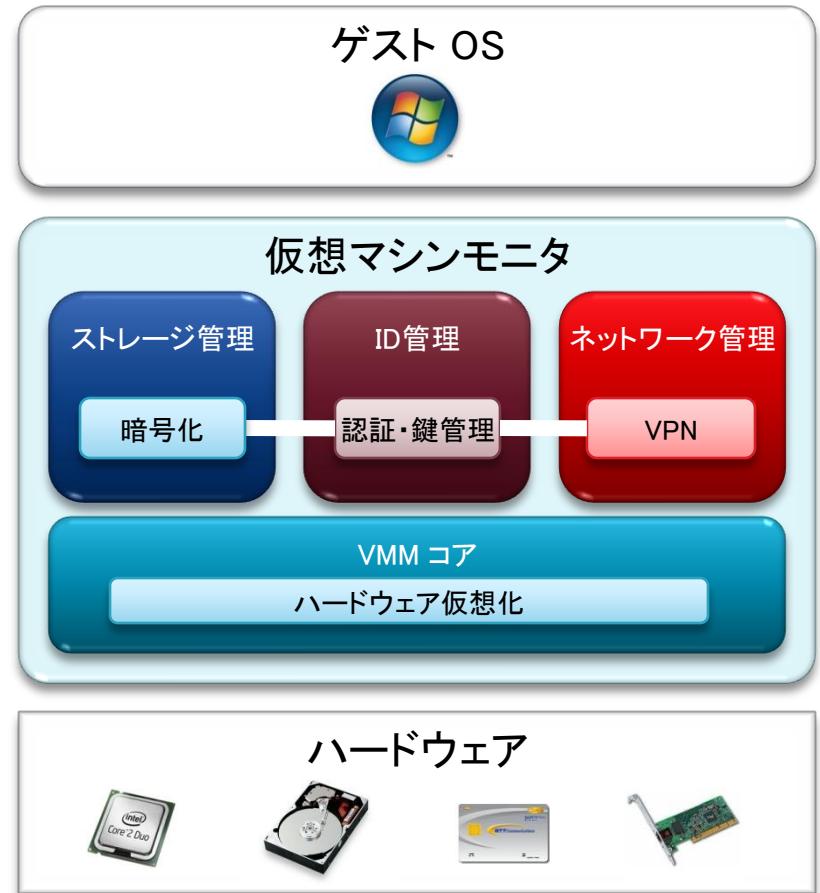


背景と目的

- 情報漏洩事件の増加
 - PC・USBメモリ等の紛失・盗難
 - インターネット経由
 - ウィルスやファイル交換ソフトなど
- 仮想マシンモニタを用いた情報漏洩の防止
 - 暗号化・認証を仮想マシンモニタで強制する
 - ストレージ及びネットワークの暗号化
 - ICカードによる認証・鍵管理

BitVisorの機能

- ストレージ管理
 - HDD及びUSBメモリの暗号化
- ネットワーク管理
 - IPsecによるVPN接続
- ID管理
 - ICカードによる鍵管理・認証
- VMMコア
 - CPU及びメモリの仮想化

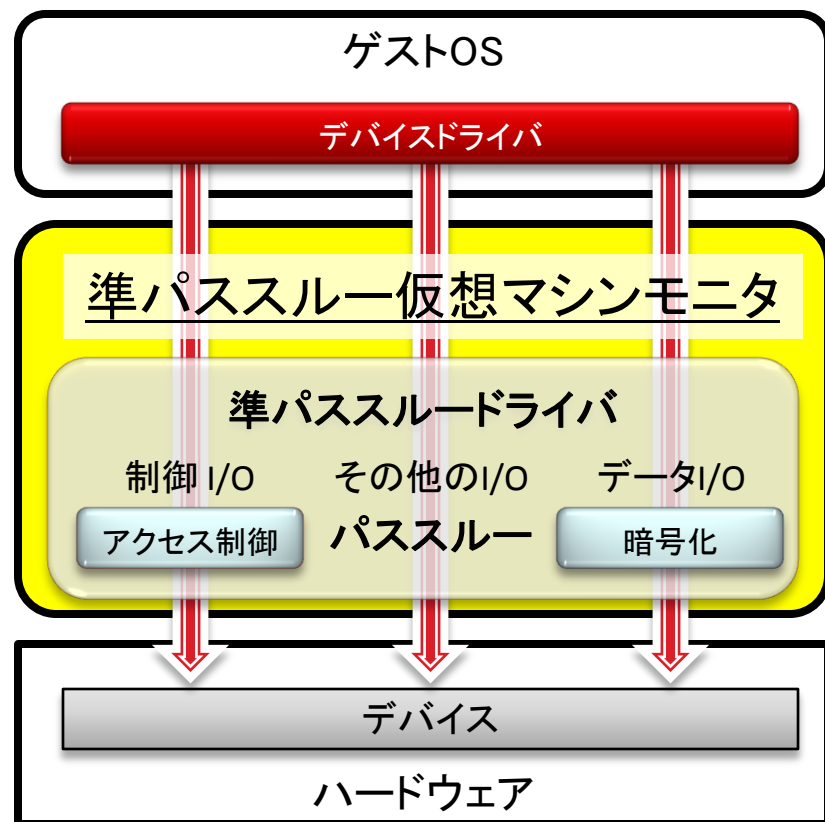


設計時の前提条件

- 仮想マシンモニタ自身のセキュリティが重要
 - 仮想マシンモニタを可能な限り小さくすべき
- デスクトップ環境での使用が前提
 - Windowsを安全に動作させることが目標
- 限られた開発コスト・期間
 - 3年間, 常駐研究員5名, 限られた予算
 - サポートするハードウェアは限定してよい

準パススルー型アーキテクチャ

- 多くのI/Oをパススルー
 - ゲストがデバイスを制御
 - デバイスは仮想化しない
- 一部のI/Oだけを捕捉
 - 制御I/Oの監視
 - アクセス制御
 - データI/Oの変換
 - データの暗号化



利点

- 仮想マシンモニタを小さく出来る
 - CPU & メモリの仮想化を簡略化可能
 - 仮想マシン間の保護やスケジューリングが不要
 - ドライバを簡略化可能
 - 制御I/O及びデータI/Oのみを処理すればよい
- オーバーヘッドの低減
 - 多くのI/Oをパススルーする
 - Windows Vista の Aero も動作
- 開発コストの削減
 - 仮想マシンモニタ及びドライバのコード行数削減
 - ゲストOSのデバイスドライバの機能を活用して実現

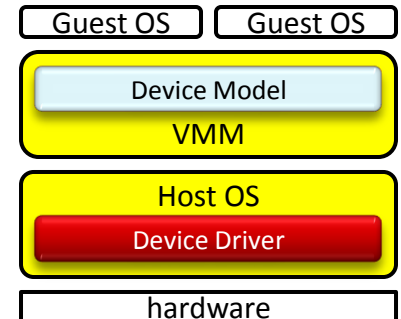
弱点

- 複数のゲストOSが同時には稼動しない
 - 1つのゲストOSがデバイスを直接制御している
⇒ デスクトップ環境を想定しているため許容可能
- ハードウェアサポートが限定される
 - 監視・変換するデバイスごとにドライバが必要
⇒ (政府の) オフィス環境に限定しており許容可能

他の仮想マシンモニタとの比較

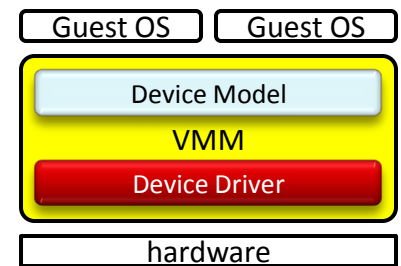
■ Type II VMM

- TCB = ホストOS + VMM
 - 例: Linux(56MLOC)+QEMU(310KLOC)



■ Type I VMM

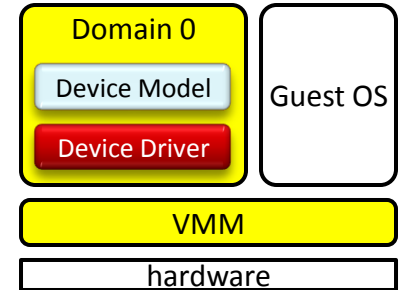
- デバイスモデルとドライバを持つ
 - 例: VMWare ESX hypervisor は 200 KLOC



Xenとの比較(サイズ)

■ Xen

- VMM(ハイパーバイザ)は比較的小さい
 - 約100 KLOC [Murray et al. VEE2008]
- TCBは必ずしも小さくない
 - ドメイン0を含む



■ BitVisor

- VMMは小さい
 - VMMコアは約20KLOC
 - 準パススルードライバは通常のドライバの約10分の1程度
- 必要最小限の機能のみ実装
 - 複数VM間の資源共有や保護は不要

Xenとの比較(オーバーヘッド)

	Xen	BitVisor
VM間のスケジューリング	必要 (複数ゲストOSに対応)	不要 (ゲストOSは1つのみ)
シャドウページング	必要 (VM・VMM間の保護と アドレス変換のため)	必要 (VMMの保護のため)
- シャドウページングの実装	高度に最適化	初期の実装 (EPT/NPTで改善が期待)
デバイスドライバの構造	準仮想化	準パススルー
- ドライバが必要なデバイス	ほぼ全てのデバイス (特定のデバイスはパ ススルーで利用可能)	一部のデバイス (ストレージ及びネット ワーク)
- デバイス毎の監視するI/O	全て or なし	部分的
- デバイスとのインターフェイス	抽象化されている	物理デバイスと同一

- VEE 2009での発表予定の論文を参照ください
 - T. Shinagawa, H. Eiraku, K. Tanimoto, K. Omote, S. Hasegawa, T. Horie, M. Hirano, K. Kourai, Y. Ohyama, E. Kawai, K. Kono, S. Chiba, Y. Shinjo and K. Kato. BitVisor: A Thin Hypervisor for Enforcing I/O Device Security. In Proc. 2009 ACM SIGPLAN/SIGOPS International Conference on Virtual Execution Environments (VEE 2009), Mar, 2009. To appear.

実験環境

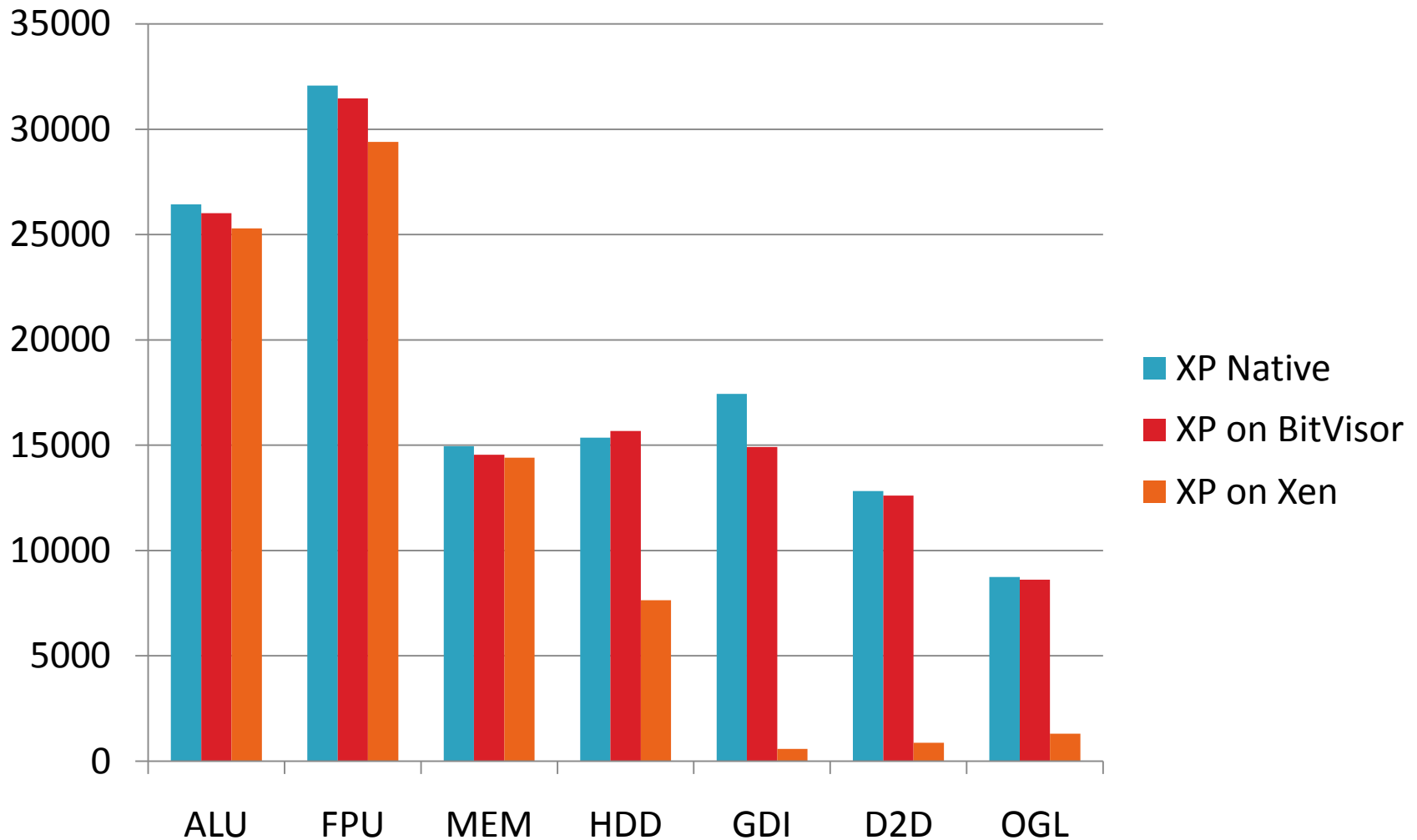
■ ハードウェア

- CPU: Intel Core 2 Duo E6850 (3.0GHz)
- Memory: PC5300 2GB (XenのVMでは1.5GB)
- HDD: Velocity Raptor 300GB (10,000rpm)
- VGA: ATI RADEON X1950

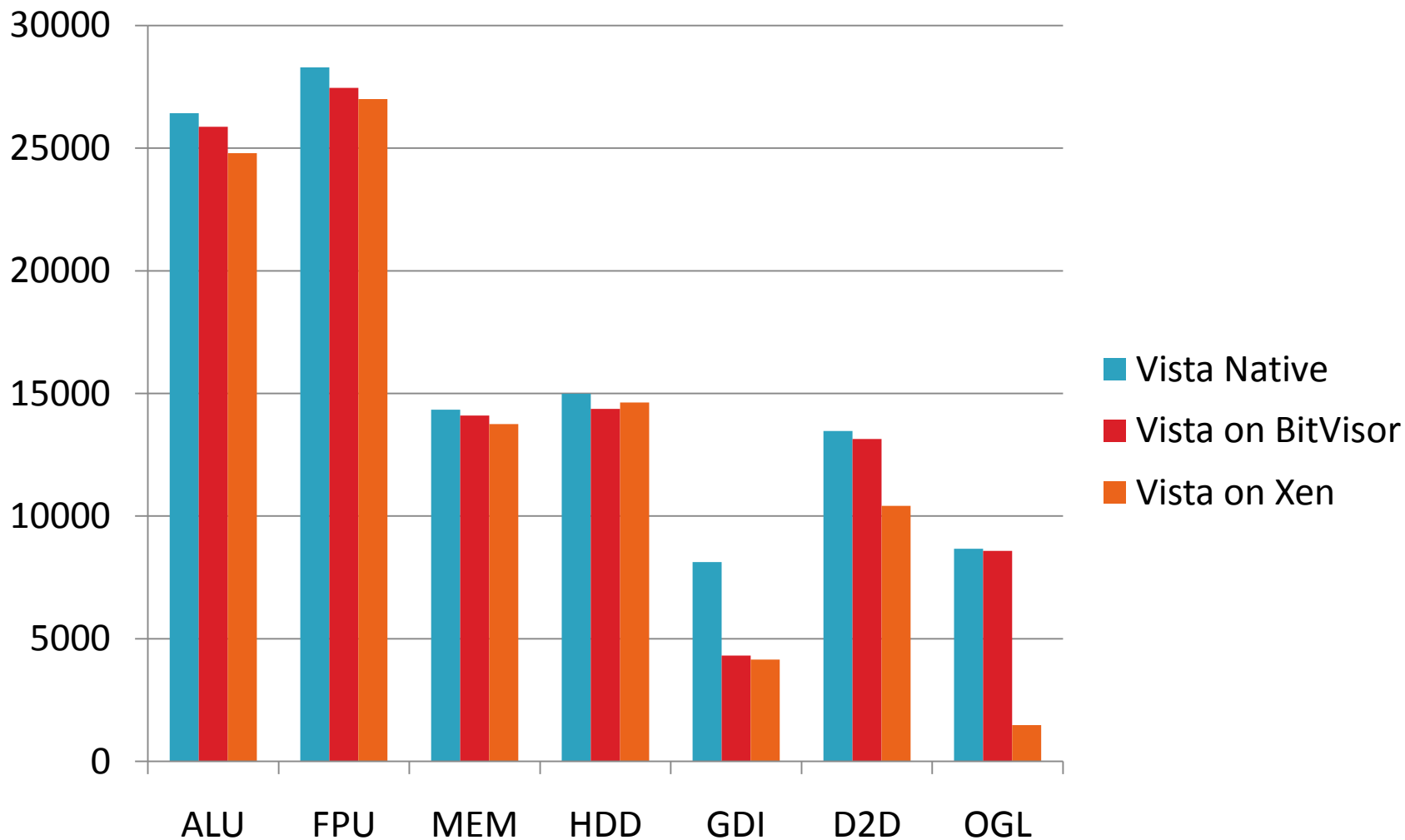
■ ソフトウェア

- VMM: BitVisor 0.3 (64bit), Xen 3.0.3 (CentOS 5.2)
- ゲストOS: Windows XP SP3, Windows Vista

Crystal Mark 2004R3 (XP)



Crystal Mark 2004R3 (Vista)



まとめ

- セキュアVMM「BitVisor」を紹介
 - ストレージ及びネットワークの暗号化
 - ICカードによる認証及び鍵管理
- Xen との比較
 - アーキテクチャ上の違い
 - 準仮想化 v.s. 準パススルー
 - パフォーマンス上の違い

現在の実装状況

- BitVisor 0.7 をリリース(予定)
 - Intel VT, 32/64bit, SMP/Multicore
 - AMD SVM も限定的サポート(シングルプロセッサのみ)
 - 多くのメジャーなOSに対応
 - Windows Vista/XP, Linux, FreeBSD, ...
 - HDD 暗号化(ATA のみ)
 - USB メモリの暗号化(UHCIのみ)
 - Type B の ICカード
 - 国家公務員身分証明書ICカード
 - IPsec VPN (Intel PRO100 のみ)

ダウンロード



セキュアVMプロジェクト

<http://www.securevm.org/>