

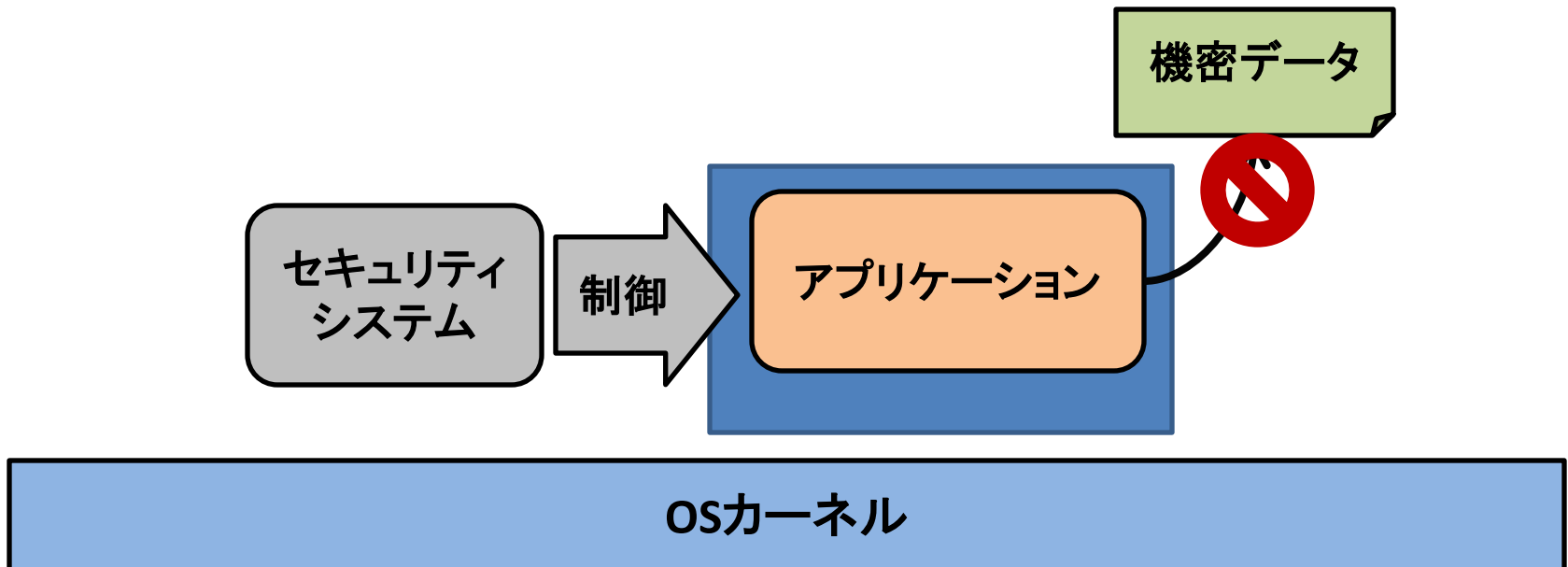
仮想マシン内のシステムコール制御 とアプリケーションのデータ保護

尾上 浩一* 大山 恵弘** 米澤 明憲*

* 東京大学 ** 電気通信大学

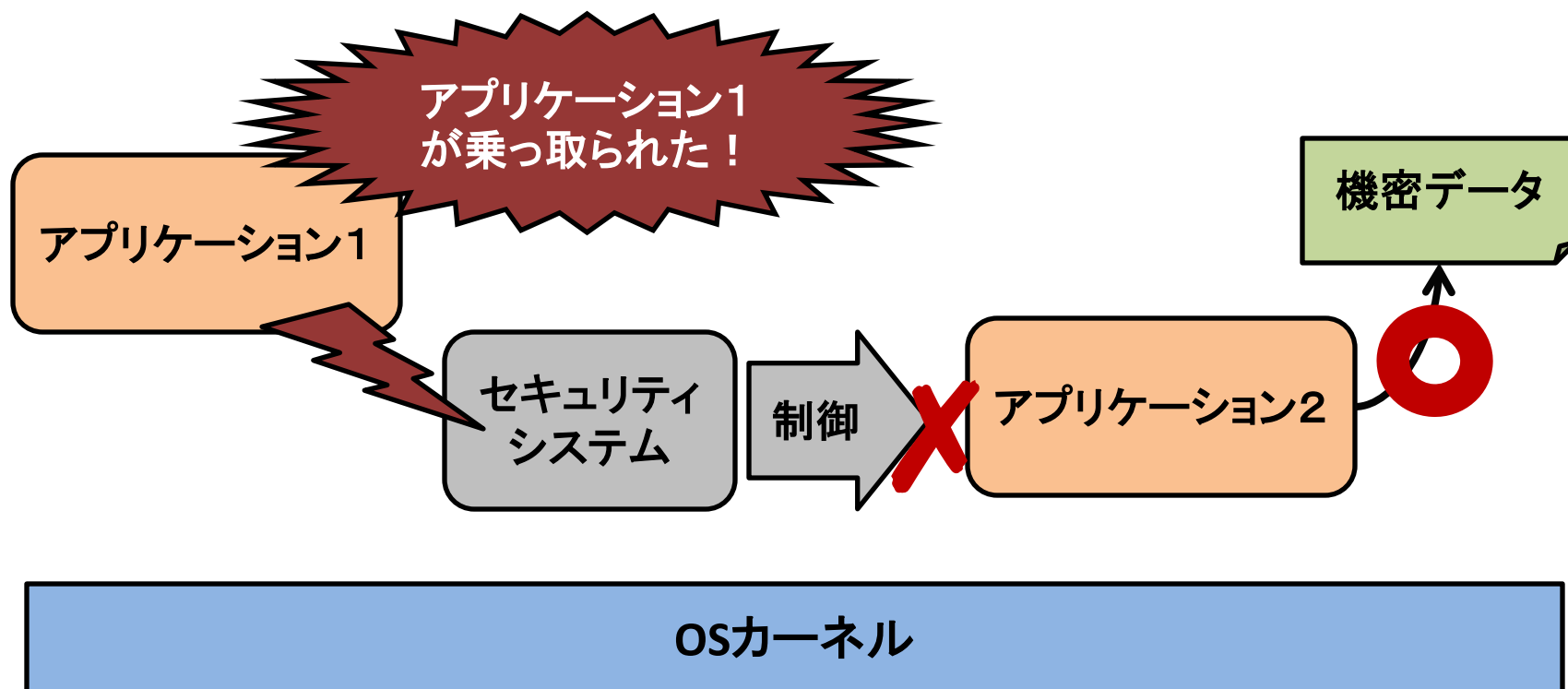
アプリケーションの保護

- セキュリティシステムの適用が一般に普及
 - サンドボックスシステム
 - 侵入検知・防止システム (IDS・IPS)
 - アンチウイルスシステム



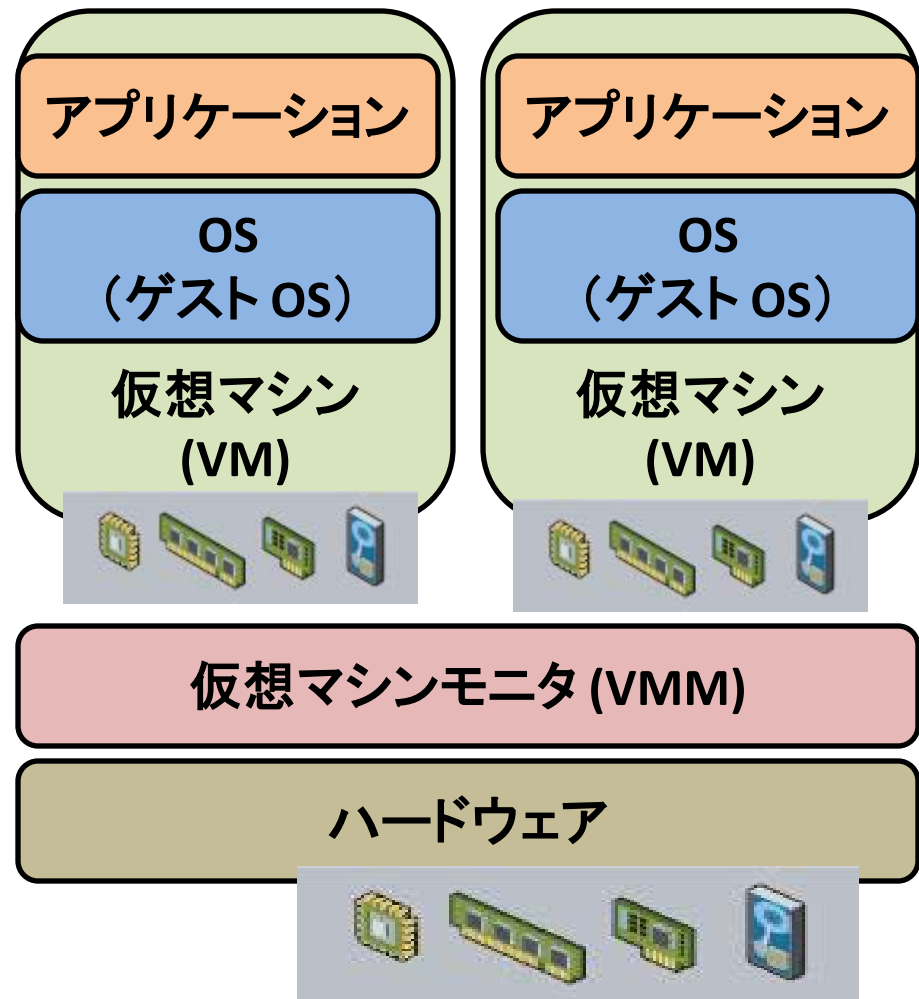
セキュリティシステムも攻撃され得る！

- 他のアプリケーションと同じ実行空間で稼働



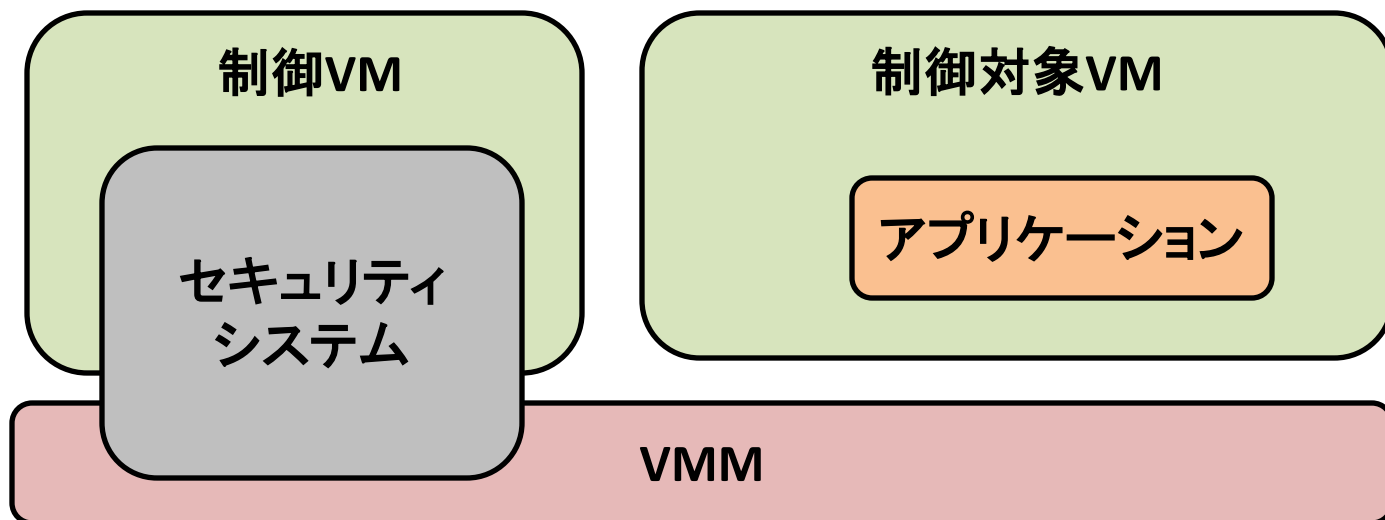
仮想マシンモニタ (VMM) を 利用することが効果的

- VM単位の隔離
 - たとえあるVMが奪取されても、VMMや他のVMを奪取することは困難
- VMの物理メモリやディスクなどの物理計算資源への操作を制御
 - VMMはVMよりも高い特権レベルで稼働



本研究の目標

- VMの外側からアプリケーションの安全性を向上させたい
 - VMMとセキュリティシステムを協調させ、アプリケーションの振る舞い制御とアプリケーションに関連するデータの保護を実現したい



本研究のアプローチ

- 制御対象VMの外側からアプリケーションが発行したシステムコールの実行を制御
 - アプリケーションプロセス単位で実行を制御
 - VMMと制御VMが、アプリケーションに関連するメモリ・ファイル操作を制御
 - メモリ上、仮想ディスク上のアプリケーションに関連するデータの漏洩・不正改竄の防止
- ✓ 利用者が指定したアプリケーションのみ実行を制御

準仮想化を利用した Xen を用いて提案システムを構築

制御対象VMの外側からの システムコールの実行制御

セキュリティシステムの運用比較

	VMを使わない 場合	VMの外側で 稼働させる場合
セキュリティシステム への攻撃	X 容易	○ 困難
セキュリティシステム の制御単位	○ OSレベル	X ハードウェアレベル

システムコールの実行制御の目標

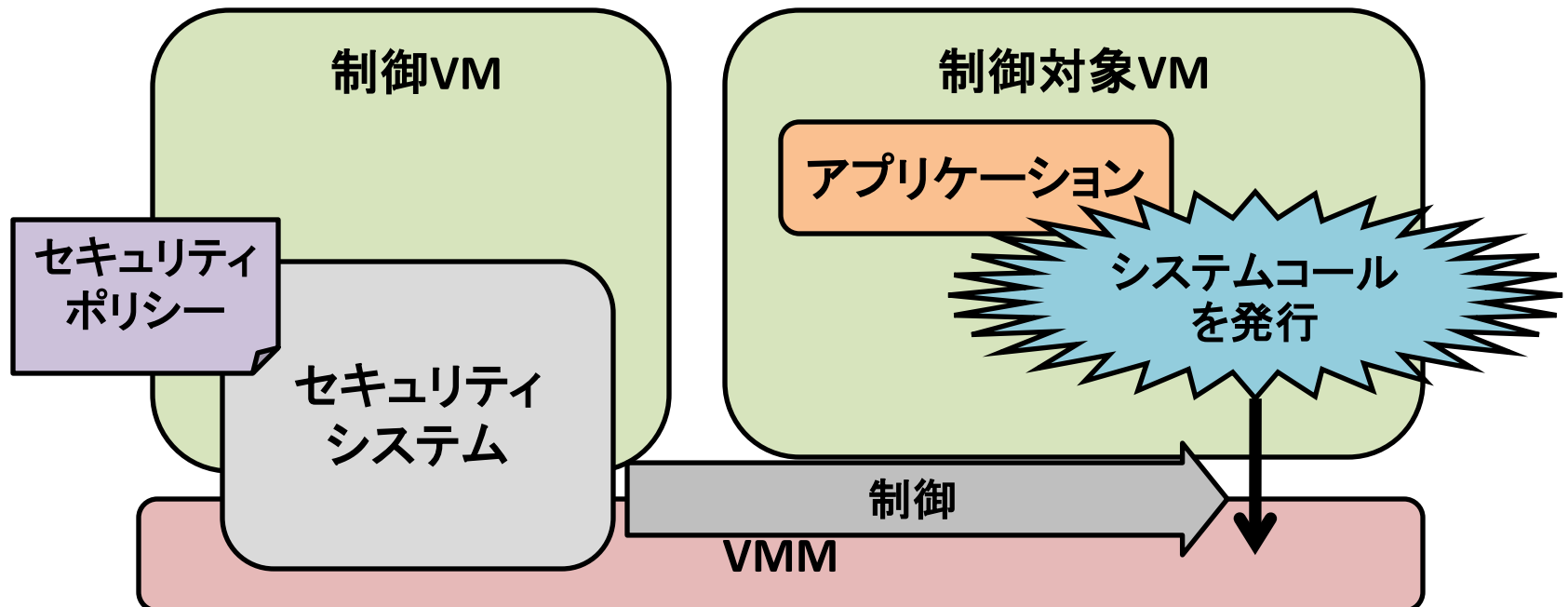
	VMを使わない場合	VMの外側で稼働させる場合
セキュリティシステムへの攻撃	X 容易	○ 困難
セキュリティシステムの制御単位	○ OSレベル	X ハードウェアレベル

Semantic gap

本研究の目標

本研究のアプローチ

- VMの外側からシステムコールの実行を制御
 - ゲスト OS カーネルの情報を利用
- セキュリティポリシーに基づいた制御



アプリケーションの実行状態の取得

- VMMが捕捉時に取得できるイベント・実行状態
 - イベント : 特権命令、割り込みなど
 - 実行状態 : レジスタ、メモリ上の値



- セキュリティシステムが必要とする情報
 - イベント : システムコール
 - 実行状態 : プロセス、システムコール番号など

本研究におけるセキュリティポリシー

- システムコール名と引数情報を用いたパターンマッチ

...

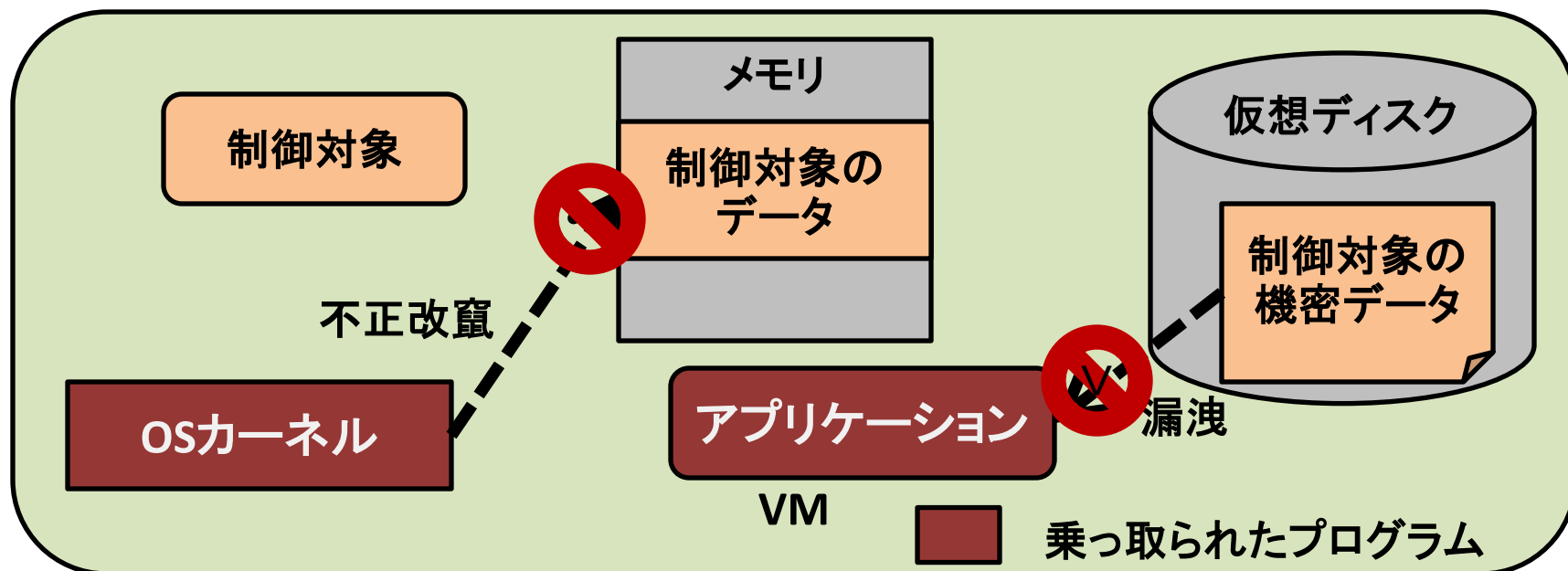
```
open default: allow
  fileEq("/etc/passwd")
  or filePrefixEq("/etc/cron.d")
  deny(EPERM)
```

...

アプリケーションに関連する メモリ・ファイル操作制御

アプリケーションのデータ保護の目標

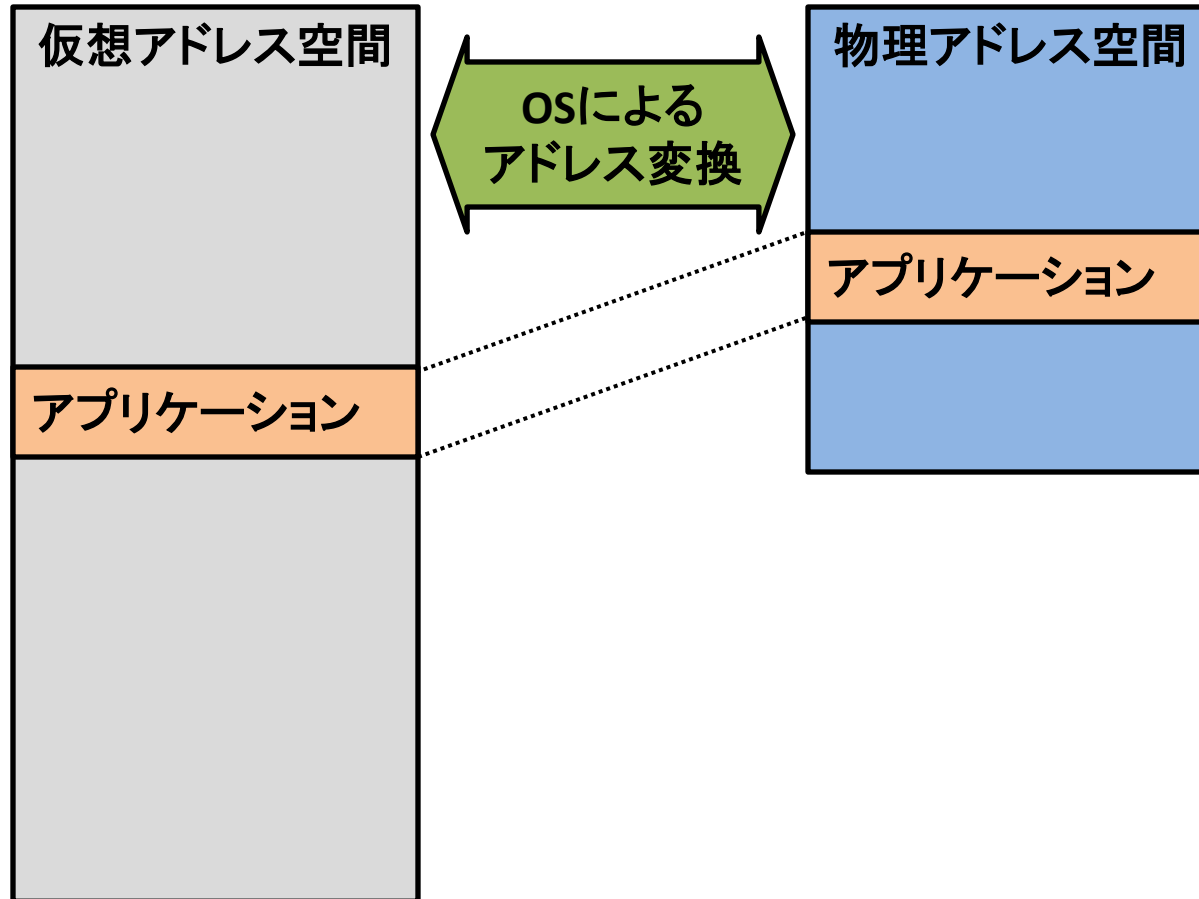
- 制御対象のアプリケーション(制御対象)のデータの漏洩・不正改竄の防止
 - ptraceやカーネルモジュールなどを利用した攻撃



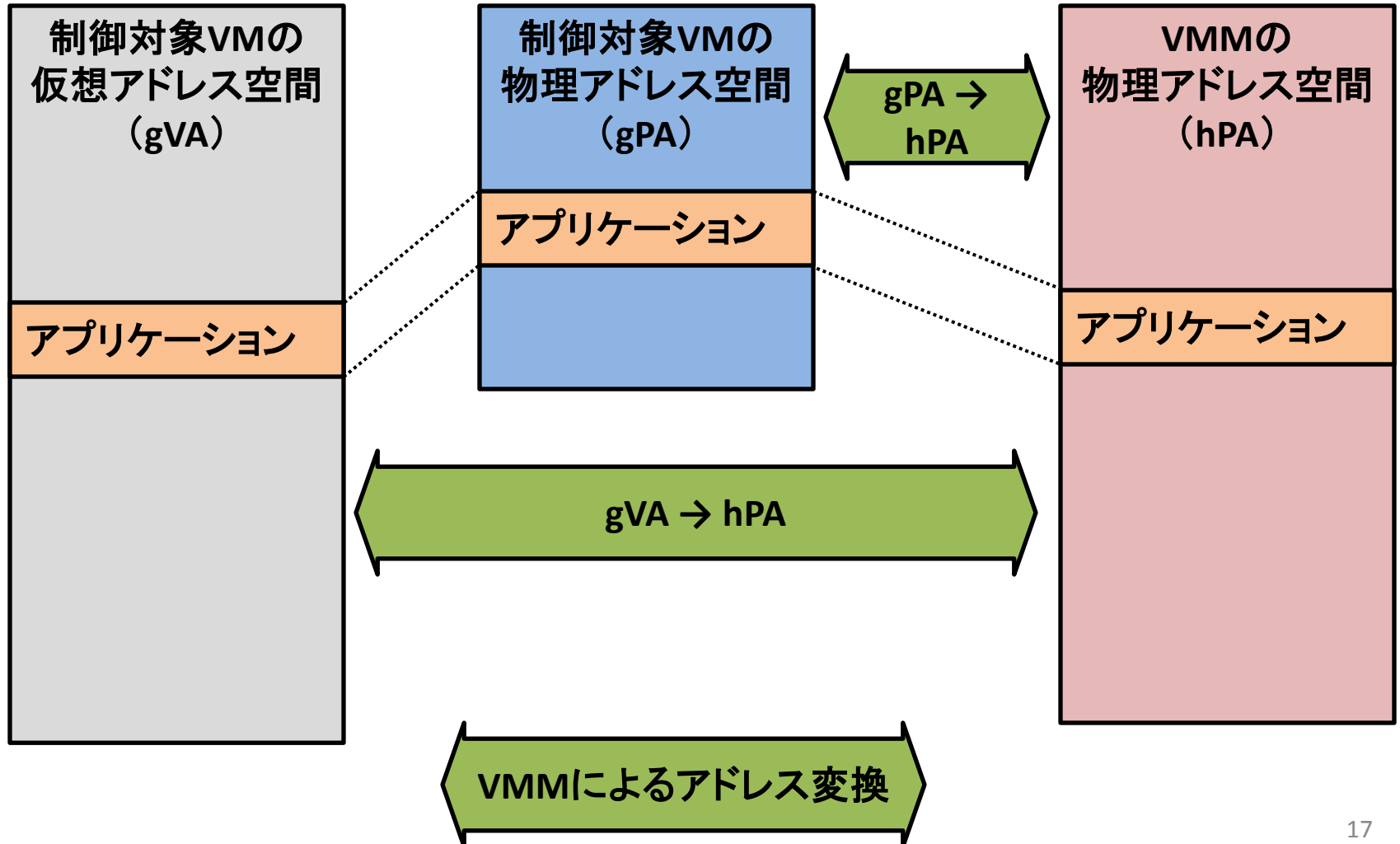
本研究のアプローチ

- 制御対象のメモリ・ディスク上の実体を制御対象外のプログラム(制御対象外)から隠蔽
 - OSカーネルも制御対象外に含まれる
- メモリ上のデータ
 - コード、データ、スタック領域など
 - 制御対象の物理メモリ領域を多重化
 - Overshadow[Chen et al., 2008]
 - [Rosenblum et al., 2008]
- ディスク上のデータ
 - 実行ファイル、設定ファイルなど
 - 異なるVMで管理

OSによるメモリ管理

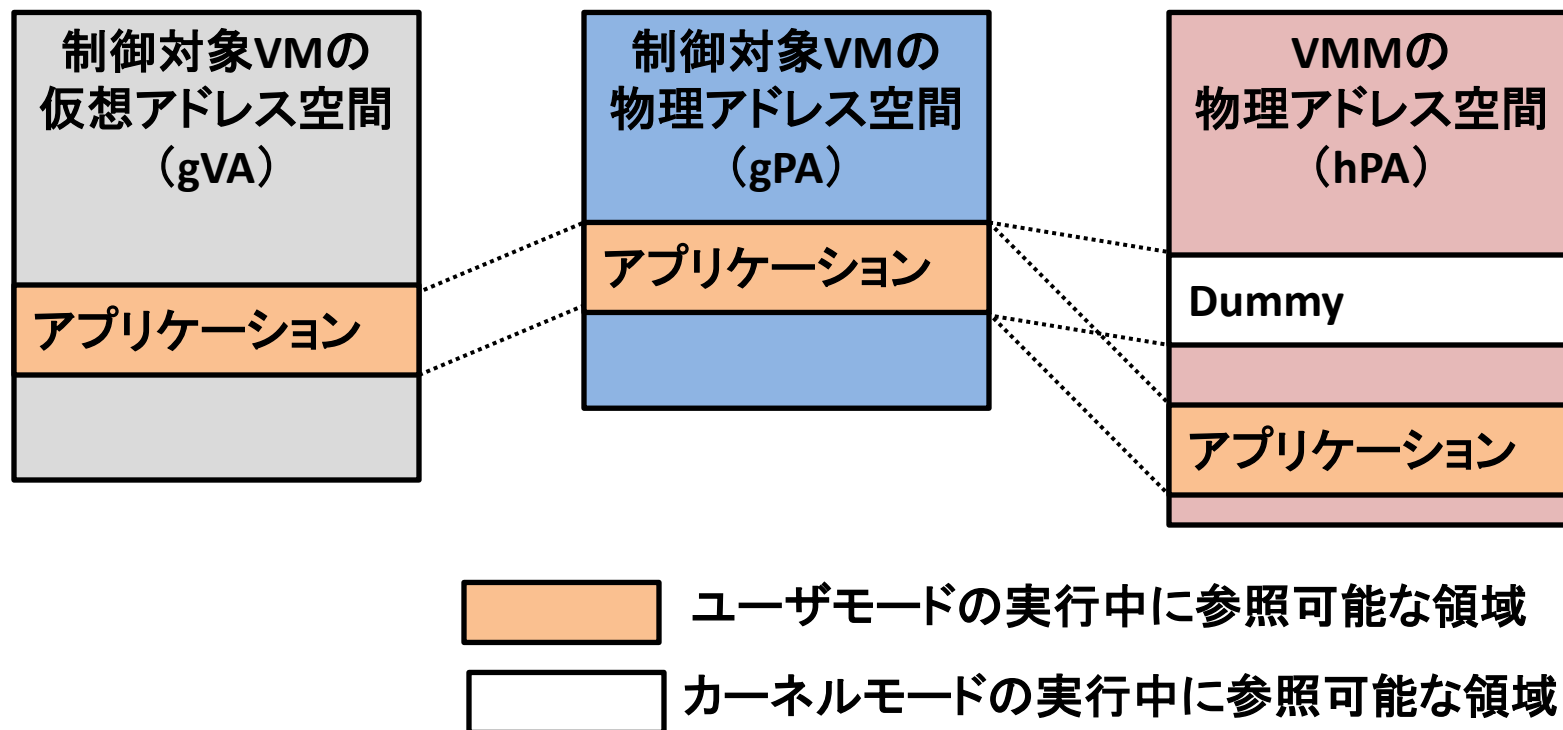


VMMによるメモリ管理



本研究におけるメモリ上のデータ保護 (1/2)

- カーネルモード・ユーザモードで異なる物理アドレス領域を見せる

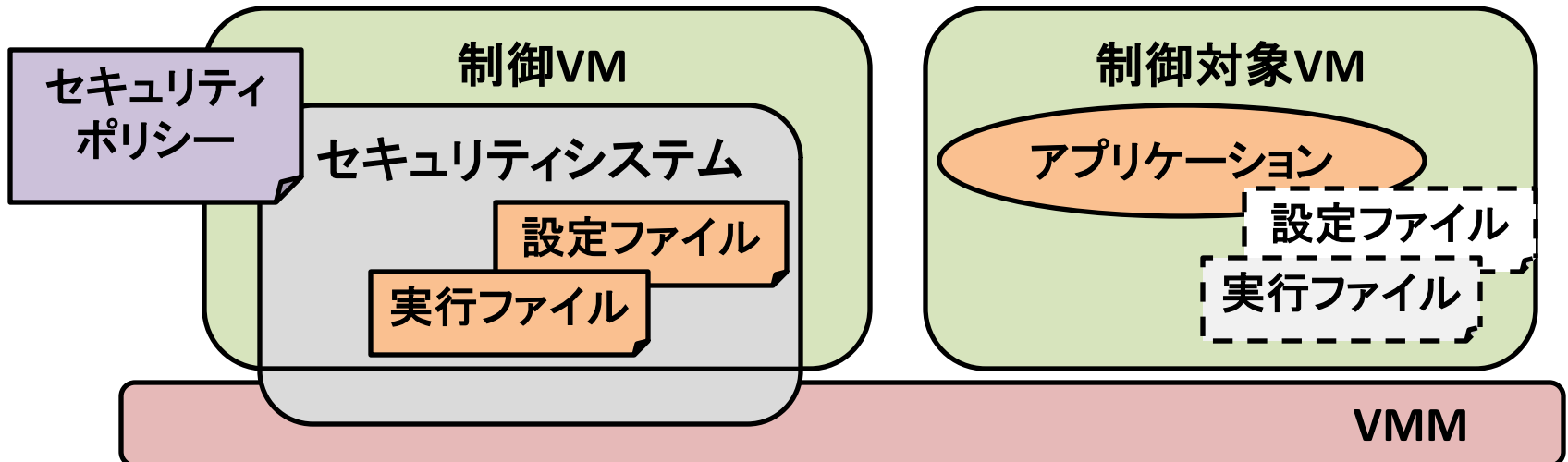


本研究におけるメモリ上のデータ保護 (2/2)

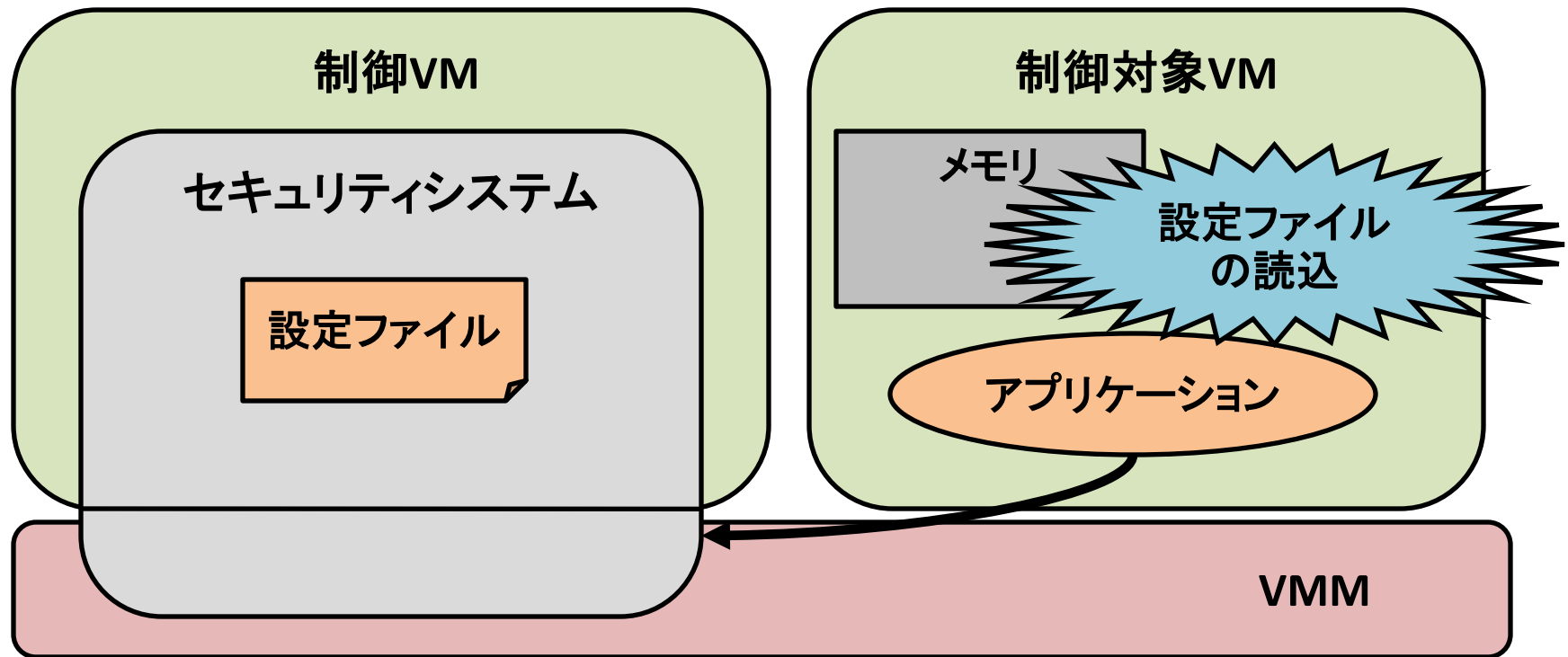
- 制御対象アプリケーションに関する
カーネルモード・ユーザモード間の切り換えが
発生したとき、ページテーブルを切り換える
 - 例外・割り込み処理
 - システムコール処理

本研究におけるディスク上の データ保護(1/5)

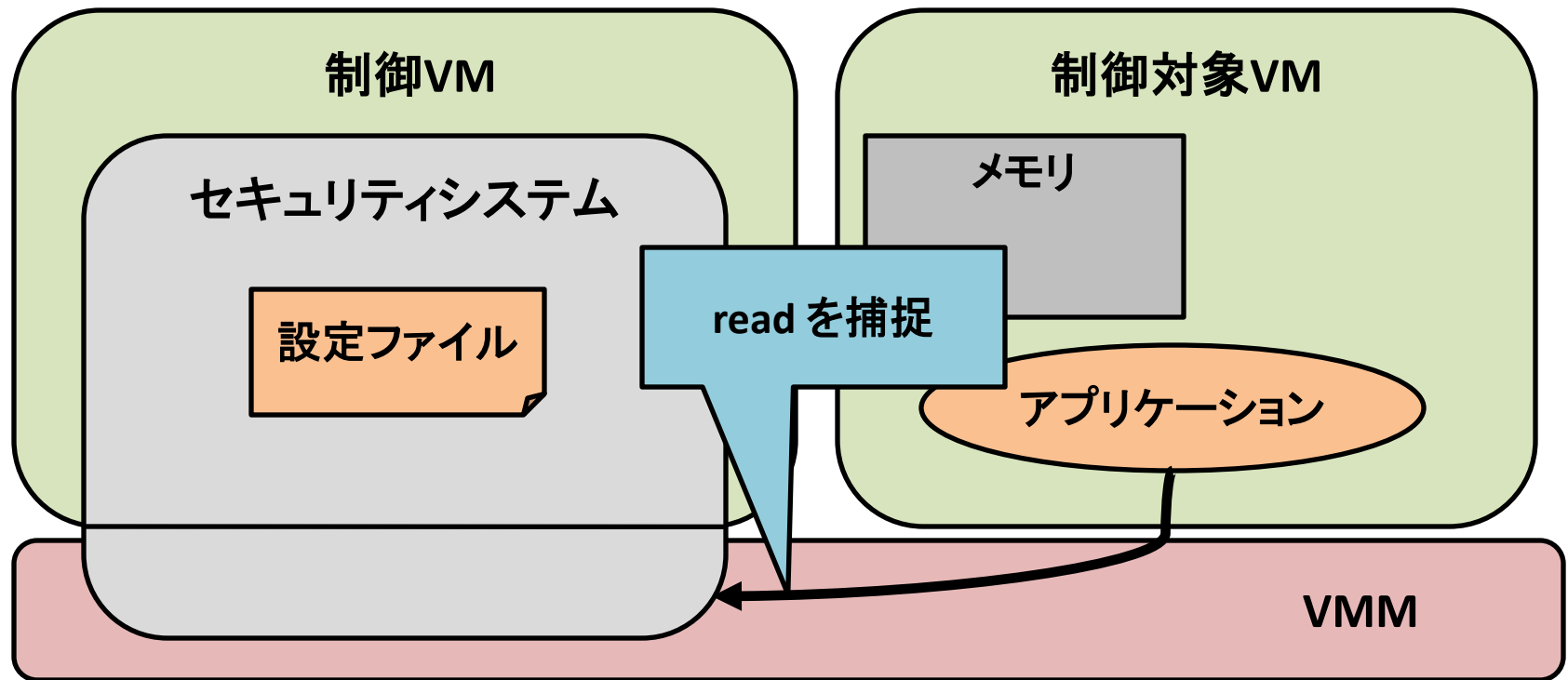
- 異なるVMで制御対象ファイルの実体を管理
 - 実行ファイル、設定ファイル、データベースファイルなど
 - 制御対象はセキュリティポリシーで指定



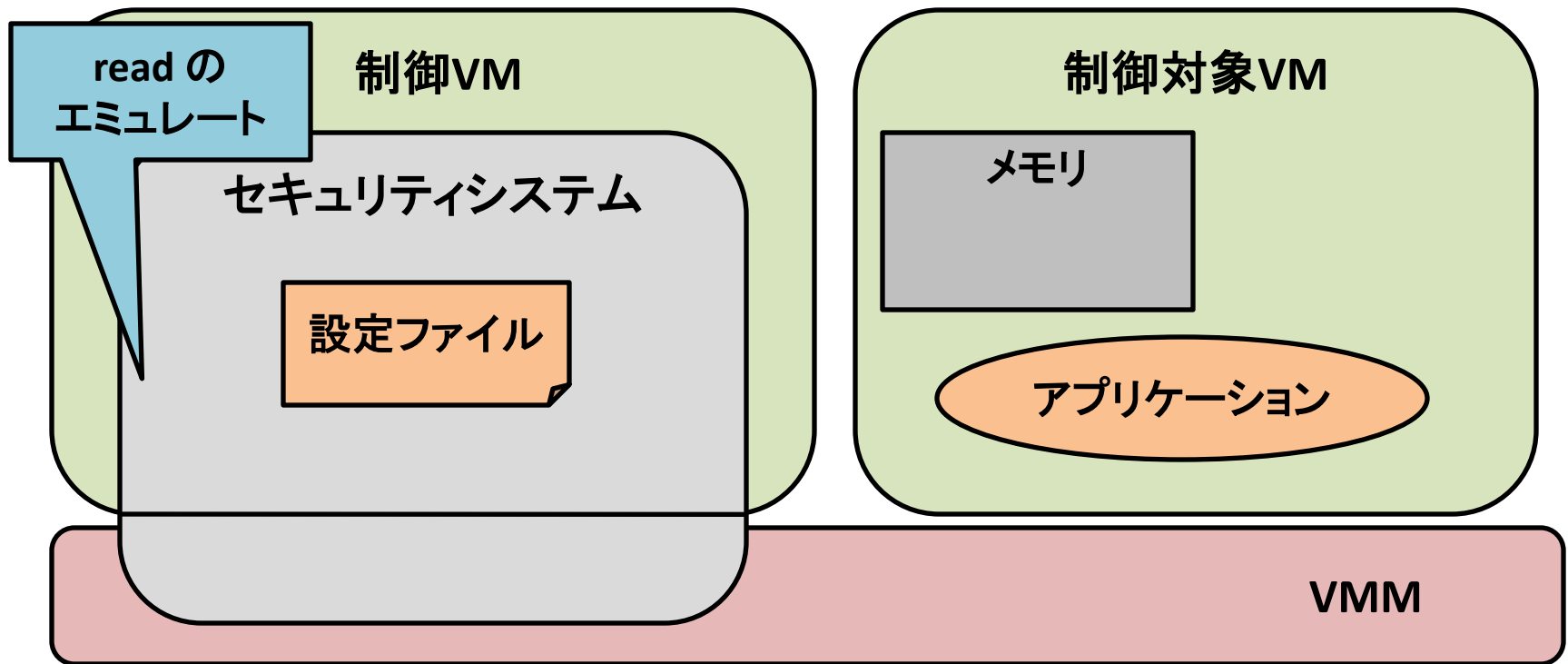
本研究におけるディスク上の データ保護(2/5)



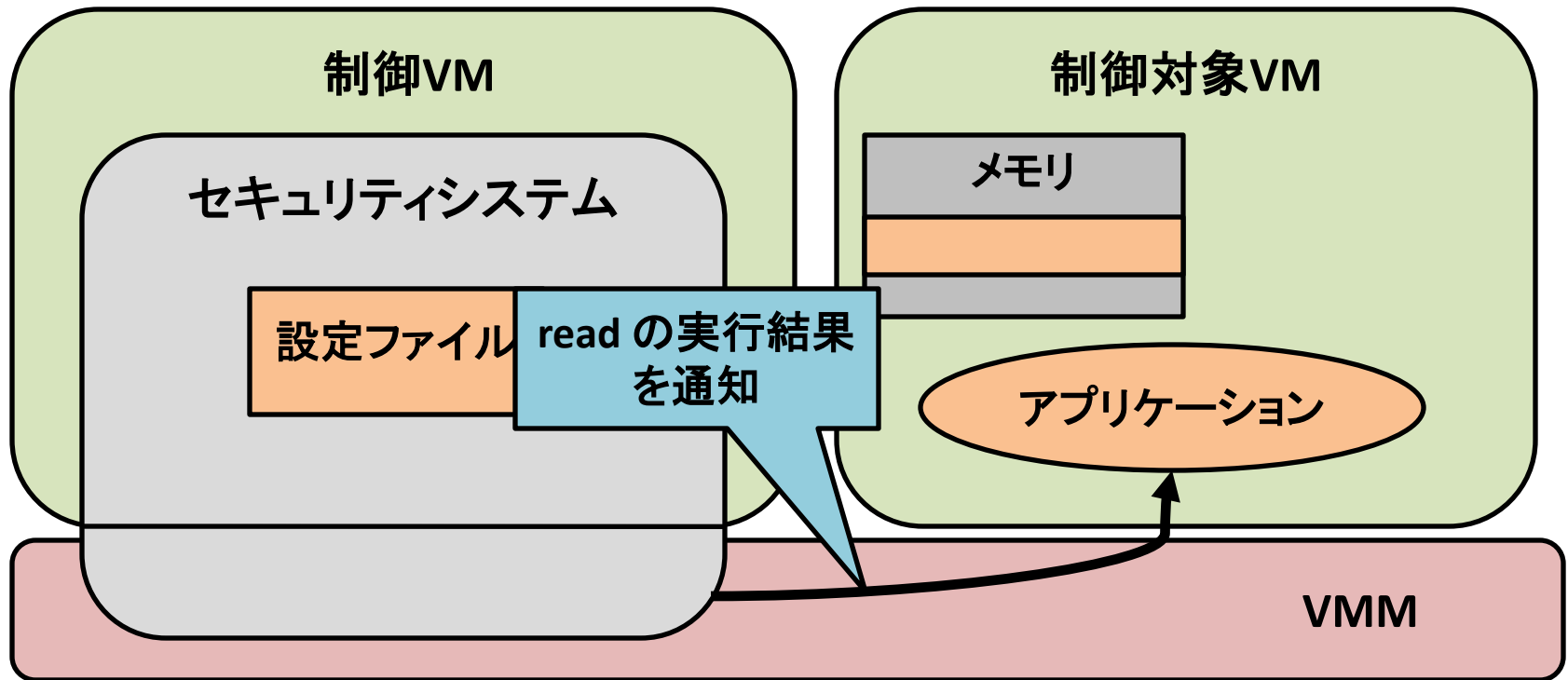
本研究におけるディスク上の データ保護(3/5)



本研究におけるディスク上の データ保護(4/5)



本研究におけるディスク上の データ保護(5/5)



まとめ

- VMの外側からアプリケーションを保護するセキュリティシステムの提案
 - アプリケーションの振る舞いの制御
 - システムコールの実行制御
 - メモリ・ディスク上のデータの保護
 - メモリ上のデータ: VMMによる物理メモリ領域の多重化
 - ディスク上のデータ: 異なるVMで管理

ご清聴ありがとうございました