仮想化技術によりログを保護する機構の研究

岡山大学大学院自然科学研究科　山内研究室

1.研究背景

ログは，計算機の動作を正確に把握するために重要
(例) 企業のサーバが攻撃を受けた際の犯人の特定

⇒ ログへの攻撃や過失により，ログが改ざんまたは喪失する問題

＜ログの改ざんの例＞
(1) ログファイルの改ざん
(2) ログ収集プログラムへの攻撃によるログの改ざん
＜ログの喪失の例＞
(1) リングバッファの上書きによるカーネルログの喪失

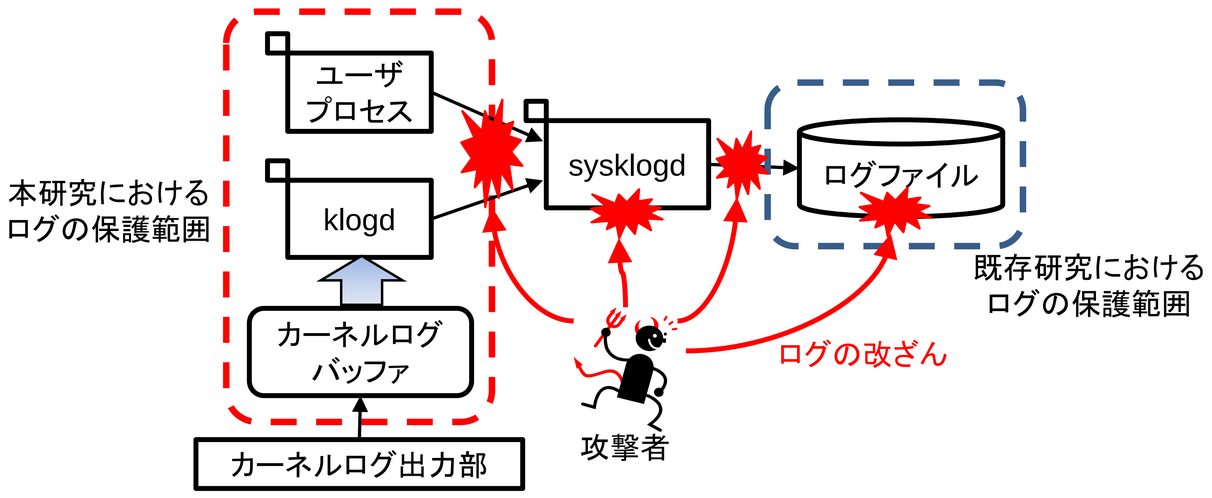
ログが改ざんまたは喪失した場合，犯人の特定や被害の把握が困難

⇒ 確実にログの改ざんや喪失を防止する技術の開発が重要な課題

仮想計算機モニタ（Virtual Machine Monitor, VMM）によりログの改ざんと喪失を防止するシステムを提案

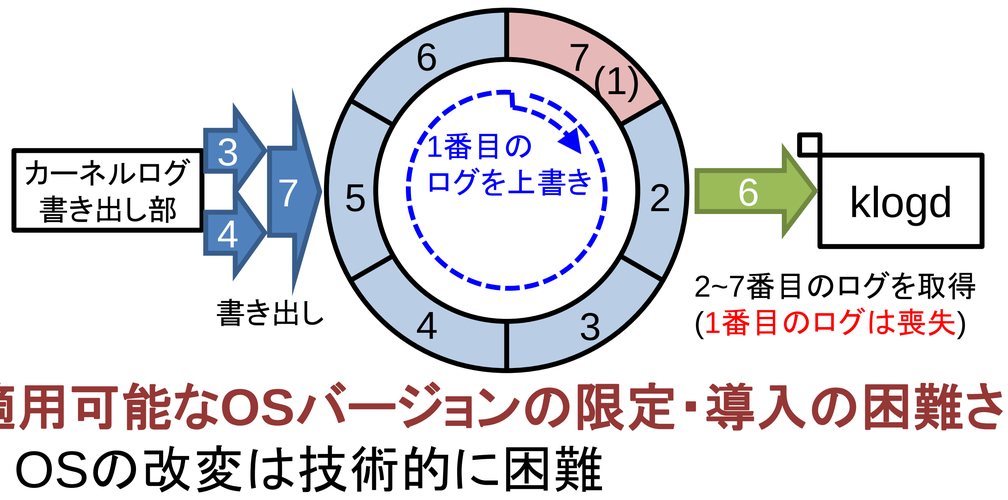
2.既存のログ管理方式の問題

(1) **ログへの攻撃**
既存研究はログファイルの保護を目的としているが，ファイルに保存される前のログが改ざんされる可能性



(2) **ログの保護機構への攻撃**
保護機構自体が攻撃の被害 ⇒ ログの信頼性の低下

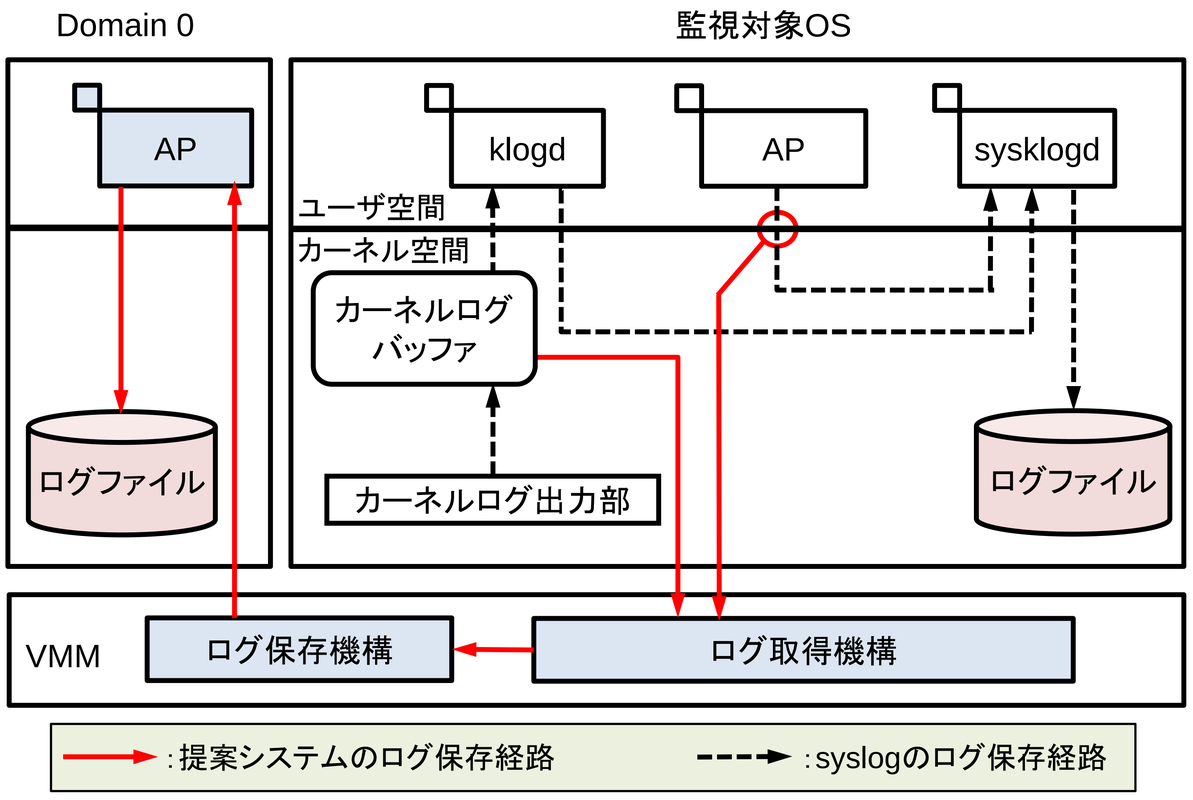
(3) **カーネルログの喪失**
古いログが新しいログにより上書きされ，喪失



(4) **適用可能なOSバージョンの限定・導入の困難さ**
(A) OSの改変は技術的に困難
(B) OSが更新される度に修正する必要あり

⇒ **VMMを利用することで問題を解決**
(1) 出力直後に保護することでログへの攻撃を防止
(2) 仮想化技術を利用してログを隔離
(3) OSから独立した機構の実現

3.VMMによるログの保護機構



(1) **監視対象OS上のログ出力のVMMによる検知・取得**
- 監視対象OSの改変無しでログの取得が可能
- 監視対象OSとVMMは独立
  ⇒ 攻撃の困難なログの保護機構の実現

(2) **Domain 0(特権OS)の要求に応じ，監視対象OSとは異なる仮想計算機(VM)上にログを保存**
- 取得したログはVM単位で隔離
  ⇒ 監視対象OSからログへの攻撃は困難

4.VMMによるログ出力の検知

(1) **応用プログラム（AP）の出力したログの検知**
- ログを出力するシステムコールをVMMにより検知
- システムコールに利用されるレジスタを操作

(2) **カーネルの出力したログの検知**
- メモリ上に読み込まれたカーネルにブレークポイントを設定
- ブレークポイント例外の発生をVMMにより検知

⇒ OSやAPのソースコードに依存しない

様々な種類のOSへ適用可能

5.動作例

```
May 19 10:52:26 debian kernel: [   11.890364] EXT3-fs: mounted filesystem with ordered data
mode.
May 19 10:52:26 debian kernel: [   14.043270] eth1: link up, 100Mbps, full-duplex, lpa 0x05E1
May 19 10:53:21 debian kernel: th world.
May 19 10:53:21 debian kernel: [  241.698031] Hello    ld.
May 19 10:53:21 debian kernel: [  241.699593] Hello    52th wor
                                      ⋮
May 19 10:53:21 debian kernel: [  249.187210] Hello 3498th world.
May 19 10:53:21 debian kernel: [  249.187973] Hello 3499th world.
```

実験で出力したカーネルログが不自然な位置から始まっている

監視対象OS上のカーネルログ

```
(XEN) KERNLOG:<6>[   11.890364] EXT3-fs: mounted filesystem with ordered data
mode.
(XEN) KERNLOG:<6>[   14.043270] eth1: link up, 100Mbps, full-duplex, lpa 0x05E1
(XEN) KERNLOG:<4>[  241.646670] Hello    0th world.
(XEN) KERNLOG:<4>[  241.646670] Hello    1th world.
                                      ⋮
(XEN) KERNLOG:<4>[  241.698069] Hello   50th world.
(XEN) KERNLOG:<4>[  241.698031] Hello   51th world.
(XEN) KERNLOG:<4>[  241.699593] Hello   52th world.
                                      ⋮
(XEN) KERNLOG:<4>[  249.187210] Hello 3498th world.
(XEN) KERNLOG:<4>[  249.187973] Hello 3499th world.
```

監視対象OS上のカーネルログでは途切れている部分もすべて取得できている

VMMにより保護したログ