Mintオペレーティングシステムにおけるヘルスチェック機能の実現

岡山大学 工学部 情報工学科
天野 正博

研究背景

インターネットの普及に伴い，計算機に対する攻撃が増加

⇨ TwinOSにおけるヘルスチェック機能

＜TwinOS＞

シングルコア上で2つのOSを動作

＜ヘルスチェック機能＞

監視用OSがサービス用OSを検査

＜TwinOSにおけるヘルスチェック機能＞

(1) 先行OSが共存OSのメモリを検査

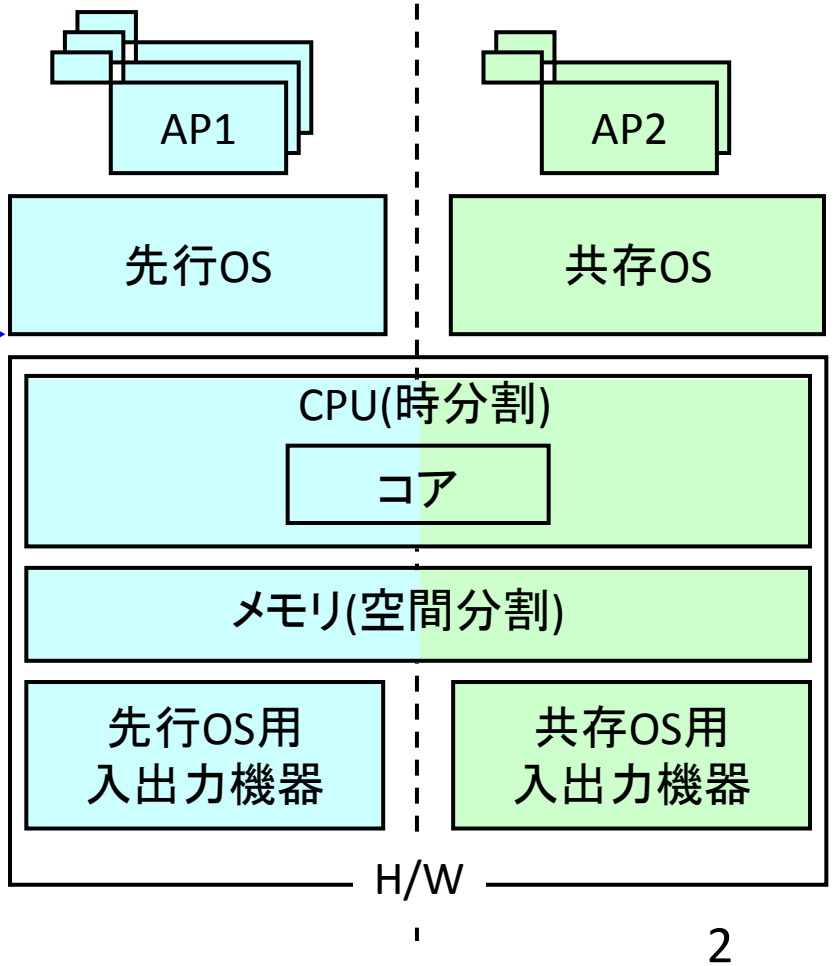
(2) 共存OSが改ざんされている場合

OS切替の停止によって共存OSを停止

＜要求＞

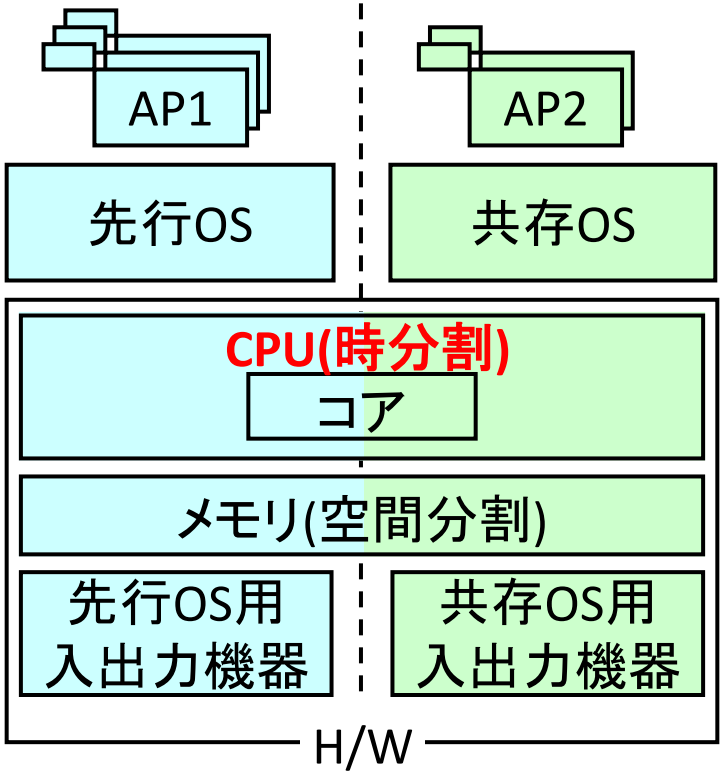
Mint上でヘルスチェック機能を実現

⇨ TwinOSにおけるヘルスチェック機能を参考

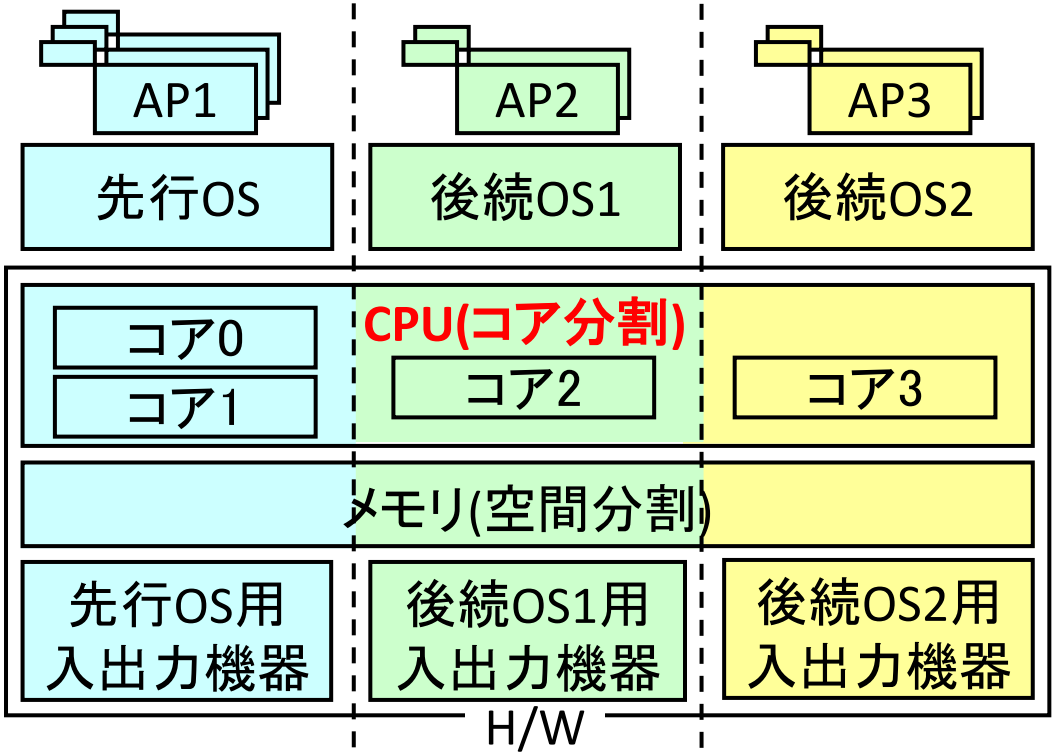


TwinOSとMint

＜TwinOS＞



＜Mint＞



＜TwinOSとMintの違い＞

(1) コアの分割方法

TwinOS: 時分割，2つのOSが共有　Mint: コア毎に分割，各OSが占有

(2) OSの走行方式

TwinOS: OSを切り替えながら走行　Mint: 各OSが同時に走行

課題

(課題1) 監視用OSによるサービス用OSの停止・再開

TwinOSにおけるヘルスチェック機能と停止・再開方法が異なる

(課題2) 検査範囲や検査契機の検討

十分な検査が行える検査範囲や検査契機の検討する必要がある

(課題3) 攻撃者によるサービス用OS停止の妨害

異常なサービス用OSを確実に停止する必要がある

(課題4) HDDを1台しか持たない計算機上ではヘルスチェック機能が利用できない

TwinOSやMintは走行させるOSの数だけHDDが必要である

(課題1)と(課題4)について対処

対処

(対処1) IPIの送信により，サービス用OSの停止・再開

IPI(Inter-Processor Interrupt): プロセッサ間割り込み

任意のコアへ割り込みを発生可能

⇨ IPIの送信により，コアへ停止・再開させる割り込みを発生

監視用OS上にサービス用OS停止・再開機能を実装

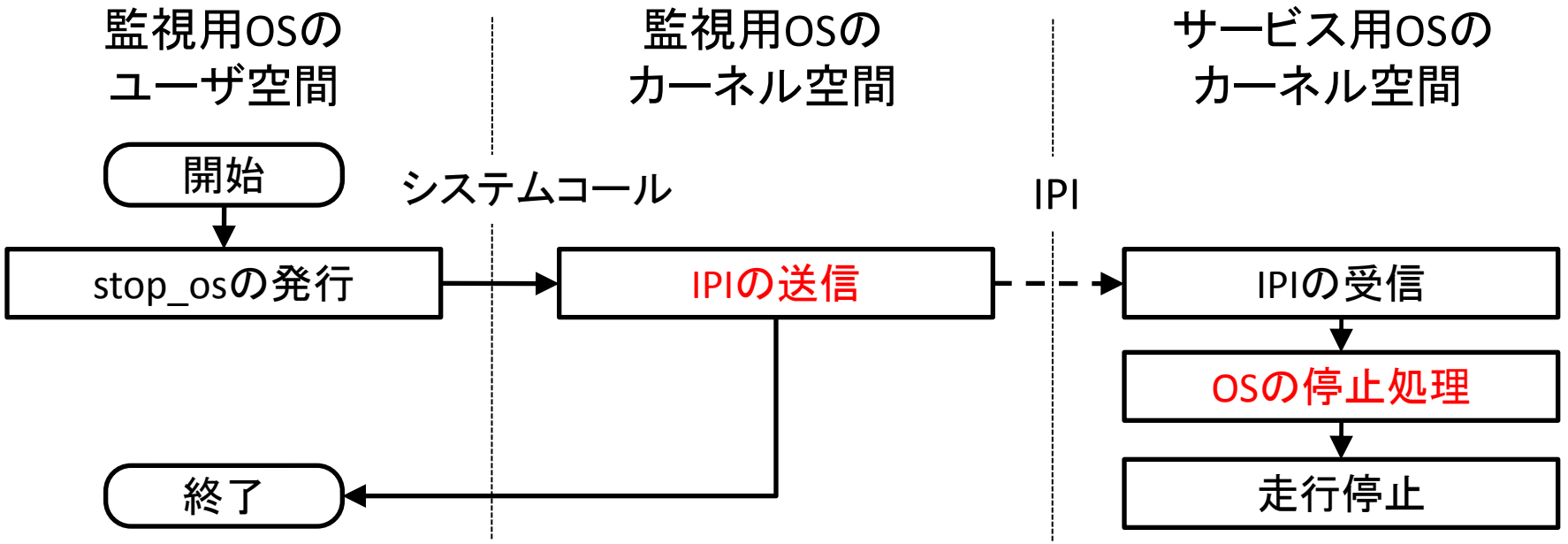
(対処2) 先行OSをHDDの占有なしで起動

先行OSをinitrdだけで動作させることでHDDの占有なしで起動

initrd(initial ramdisk): 初期ルートファイルシステム

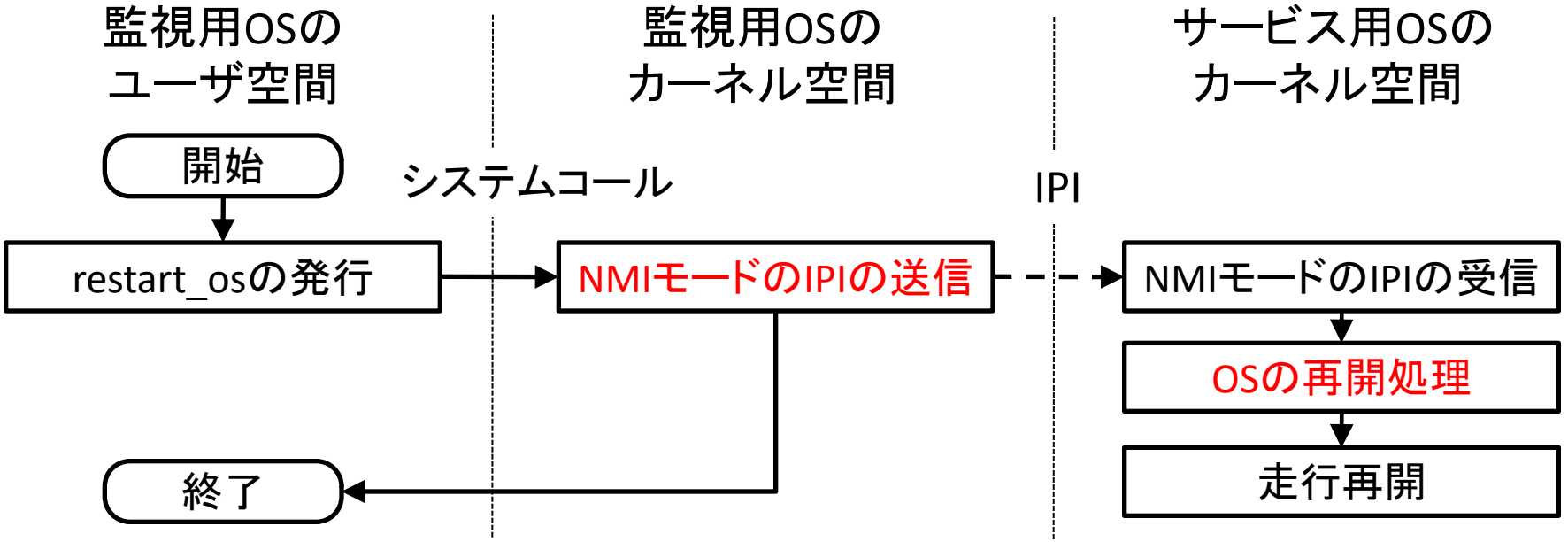
(対処1)のサービス用OS停止・再開機能について説明

サービス用OS停止機能



(1) システムコールの発行
(2) IPIの送信
(3) IPIの受信
(4) OSの停止処理
　(A) 割り込みの無効化
　(B) hlt命令を実行し，コアを停止
　　hlt命令: 割り込みを受け取るまでコアを一時停止
(5) サービス用OSの走行停止

サービス用OS再開機能



(1) システムコールの発行
(2) NMIモードでIPIを送信
NMI(Non-Maskable Interrupt): マスク不可割り込み
サービス用OSは割り込みを無効化した状態でhlt命令により停止
⇨ マスク不可な割り込みを発生させ，再開
(3) NMIモードのIPIの受信
(4) OSの再開処理
(5) サービス用OSの走行再開

本発表のまとめ

＜実績＞

(1) サービス用OS停止機能の実装
(2) サービス用OS再開機能の実装
(3) 先行OSのHDDの占有なしでの起動を実現

＜残された課題＞

(1) 検査範囲と検査契機の検討
(2) 攻撃者によるサービス用OS停止の妨害
(3) 残りの機能の実装