SVirt

レッドハットが実現するセキュアな仮想化環境

Red Hat K.K. Senior Solution Architect: Ryo Fujita <rfujita@redhat.com>

V1.0: 20th. Jan 2010

Agenda

- The Fact
- RH with SELinux
- SELinuxとは
- KVM on SELinux
- 新たなる脅威
- Svirt
- 利用状況

The Fact

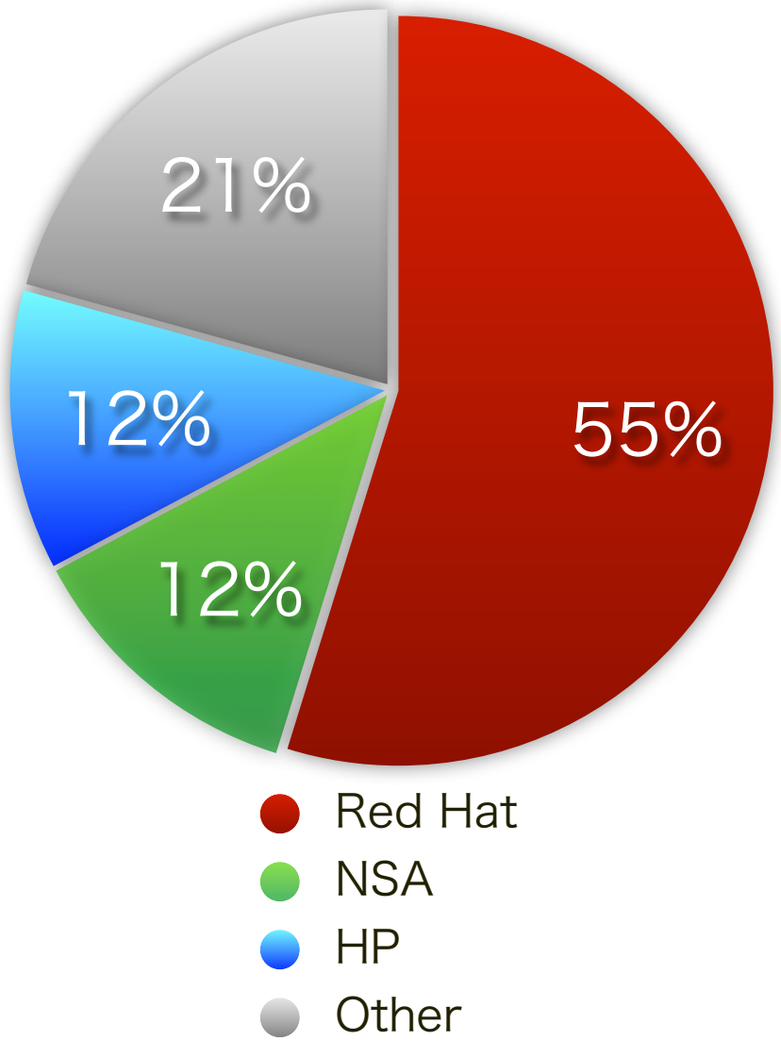
- rootパスワードとともに公開されているサーバ
  - http://www.coker.com.au/selinux/play.html
  - To access my Debian play machine ssh to play.coker.com.au as root, the password is "SELINUX".
  - SELinuxコミュニティのRussell Coker（元Red HatのSELinuxのメンテナ）が運用
- rootパスワードを公開してもクラック・ハックされないのがSELinux!

RH with SELinux

- RHEL
  - FC2：SELinuxを導入（2004年5月）
  - RHEL4：SELinuxを導入（2005年2月）
    - targetedポリシー（約13ターゲット）
- RHEL5：SELinuxを強化（2007年3月）
  - targetedポリシー（約80ターゲット）
  - MLS/MCSの導入

RH with SELinux(続き)

- SELinuxの開発・サポート
  - Red Hat：286（55%）
    - gitログ522パッチセット中
      - git：Linuxのバージョン管理システム
  - nsa：65、hp：63
  - oracle：1



SELinuxとは

- Security Enhanced Linux
  - 強制アクセス制御（MAC）と最小特権を実装したLinux（≠TrustedOS）
  - NSA（米国国家安全保障局）とSecure Computing社による10年来の研究成果
  - 実装はLSM
    - Linux Security Module

DACとMAC

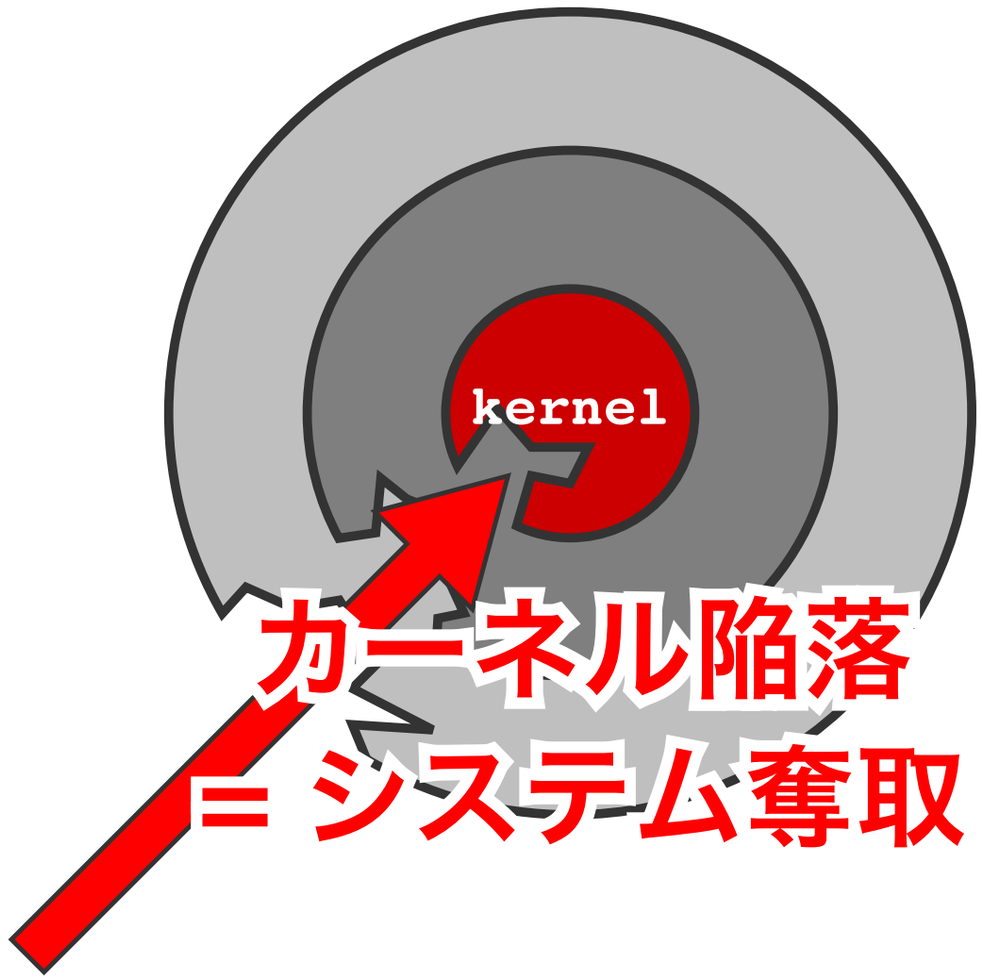
- Discretionary Access Control
  - 任意アクセス制御
    - リソースの所有者が任意に決定
- リソース操作に対する制御は`rwx`のみ
  - 特権ユーザになれば、全ての操作が可能
- 従来のOSの実装

DACとMAC(続き)

- Mandatory Access Control
  - 強制アクセス制御
    - セキュリティ管理者がポリシーを強制
  - リソース操作に対する制御の粒度が向上
    - 操作＝アクセス・ベクター
    - 全てのリソースを制御可能

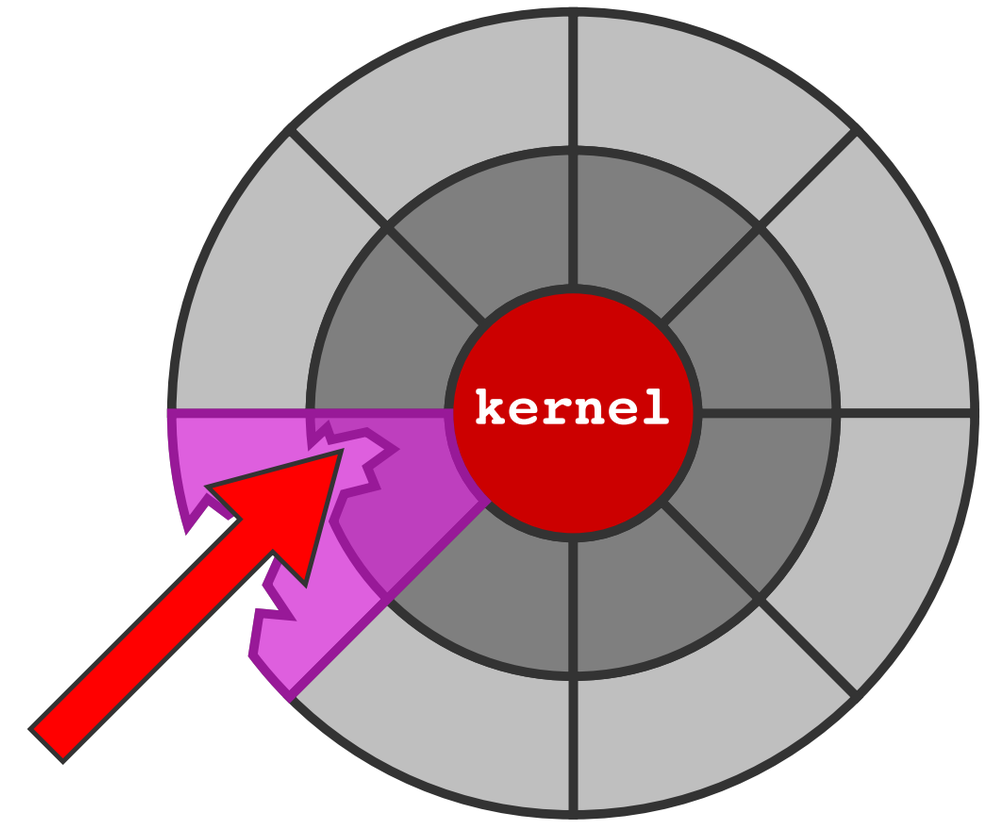
DACとMAC(続き)

- DACで脆弱性のあるhttpdが攻撃されると...
  - 子プロセス
    - apacheユーザ
  - 親プロセス
  - rootユーザ



DACとMAC(続き)

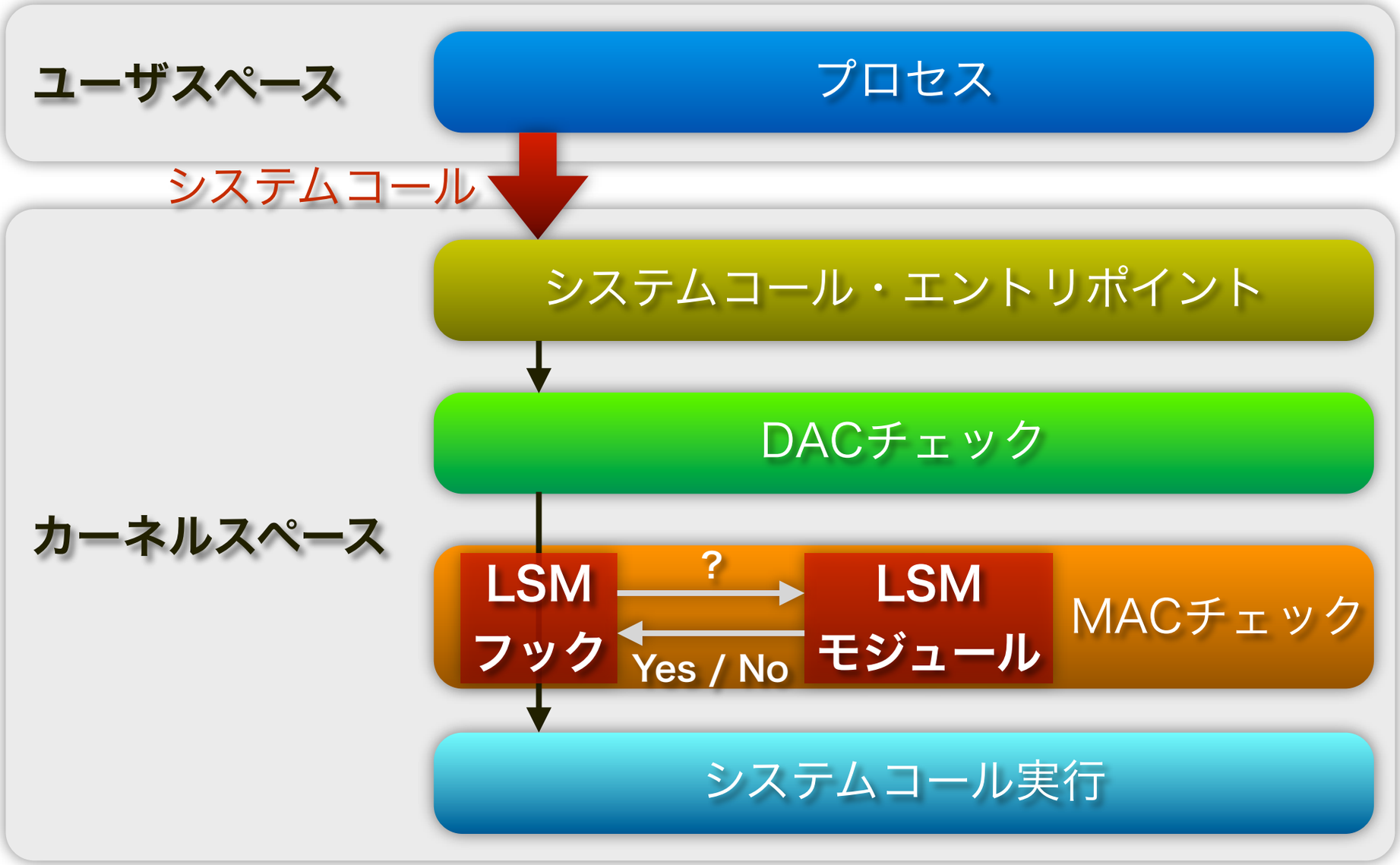
- MACで脆弱性のあるhttpdが攻撃されると...
  - 被害は最小限



ドメインに留まる

DACとMAC(続き)

- SELinuxはDAC・MACの組み合わせ



最小特権

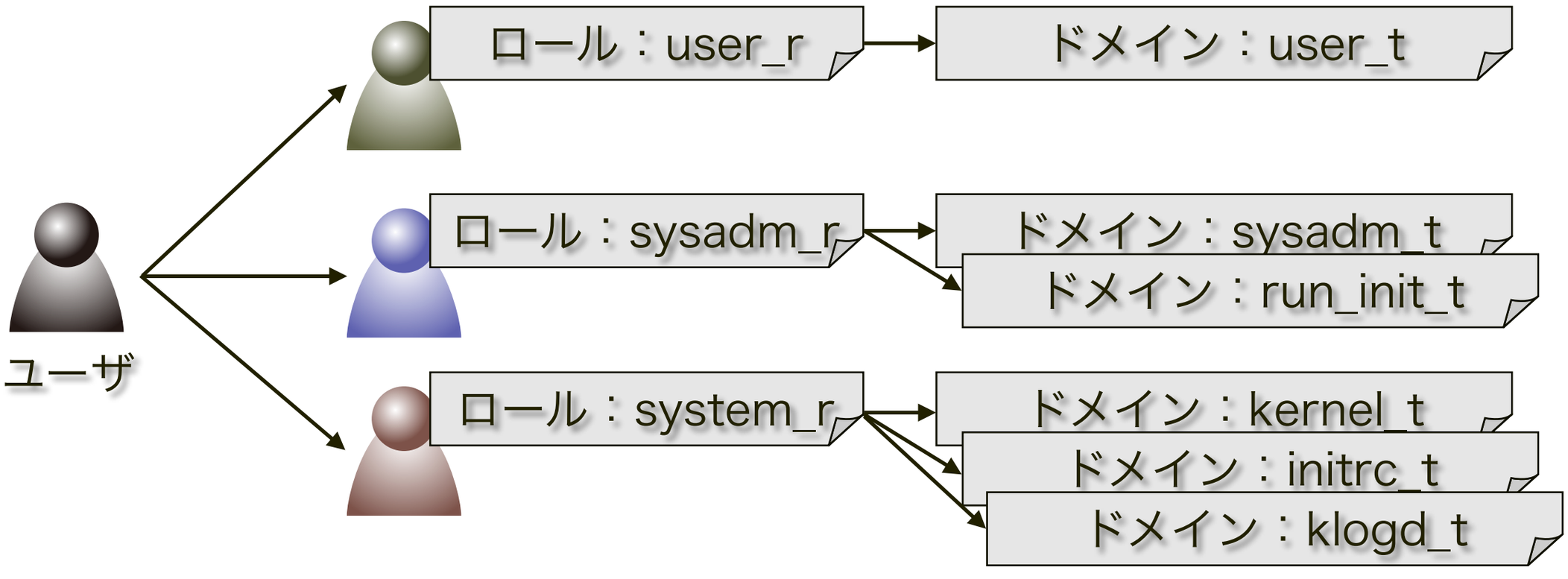
- プロセスやユーザに不要な特権を与えない
  - TE（Type Enforcement）
  - RBAC（Role Based Access Control）
  - MLS/MCS

TE

- 英語のSVO構文と同じ
  - S：プロセス、V：アクセスベクタ、O：リソース
- プロセスにはドメイン、リソースにはタイプ
- 許可するSVOを定義＝セキュリティポリシー

RBAC

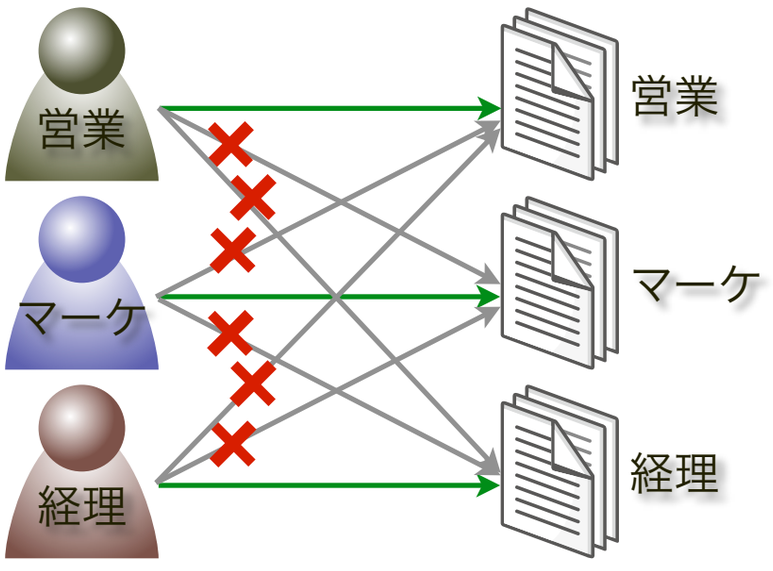
- ロールに必要な権限だけを設定
  - ユーザにあるロールになることを許可
  - ロールに利用できるドメインを設定



MLS/MCS

- Multi Level Security
  - セキュリティコンテキストにレベルを追加

- Multi Category Security
  - セキュリティコンテキストにカテゴリを追加



セキュリティポリシー

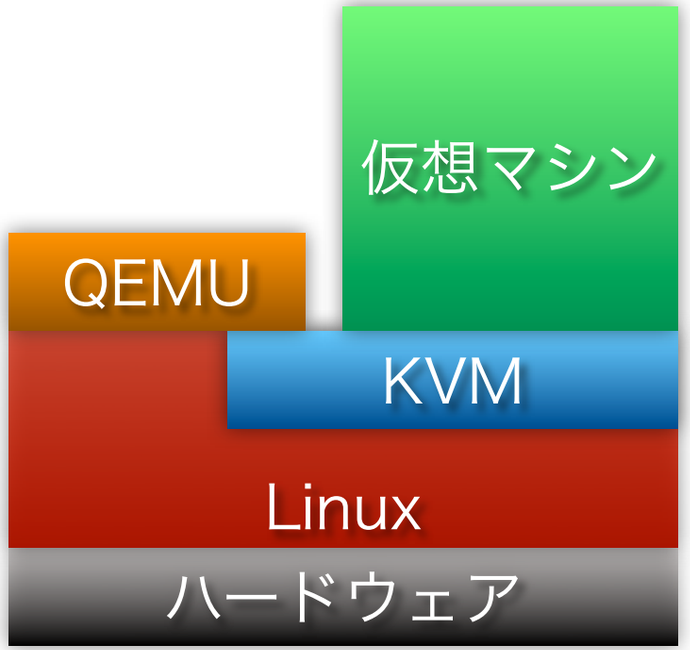
- strict
  - デフォルト：全て拒否
  - 最小権限の原則の徹底
  - 汎用的なサーバでは適用が難しい
- targeted
  - デフォルト：全て許可
  - unconfined_tドメインの追加
  - エッジサーバを保護
    - httpd, dhcpd, mysqld, named...

3つのモード

- disabled
  - SELinuxは無効
- permissive
  - ポリシーチェックが行われロギングされるが、アクセスベクターの停止は行われない
- enforcing
  - アクセスベクターが強制停止される

KVM

- KVM：Kernel-based Virtual Machine
  - CPUの仮想化支援機能を利用するためのカーネルモジュール
- Intel VT / AMD-Vが必須
- ハイパーバイザを高速化
  - 現在の実装ではQEMUを高速化

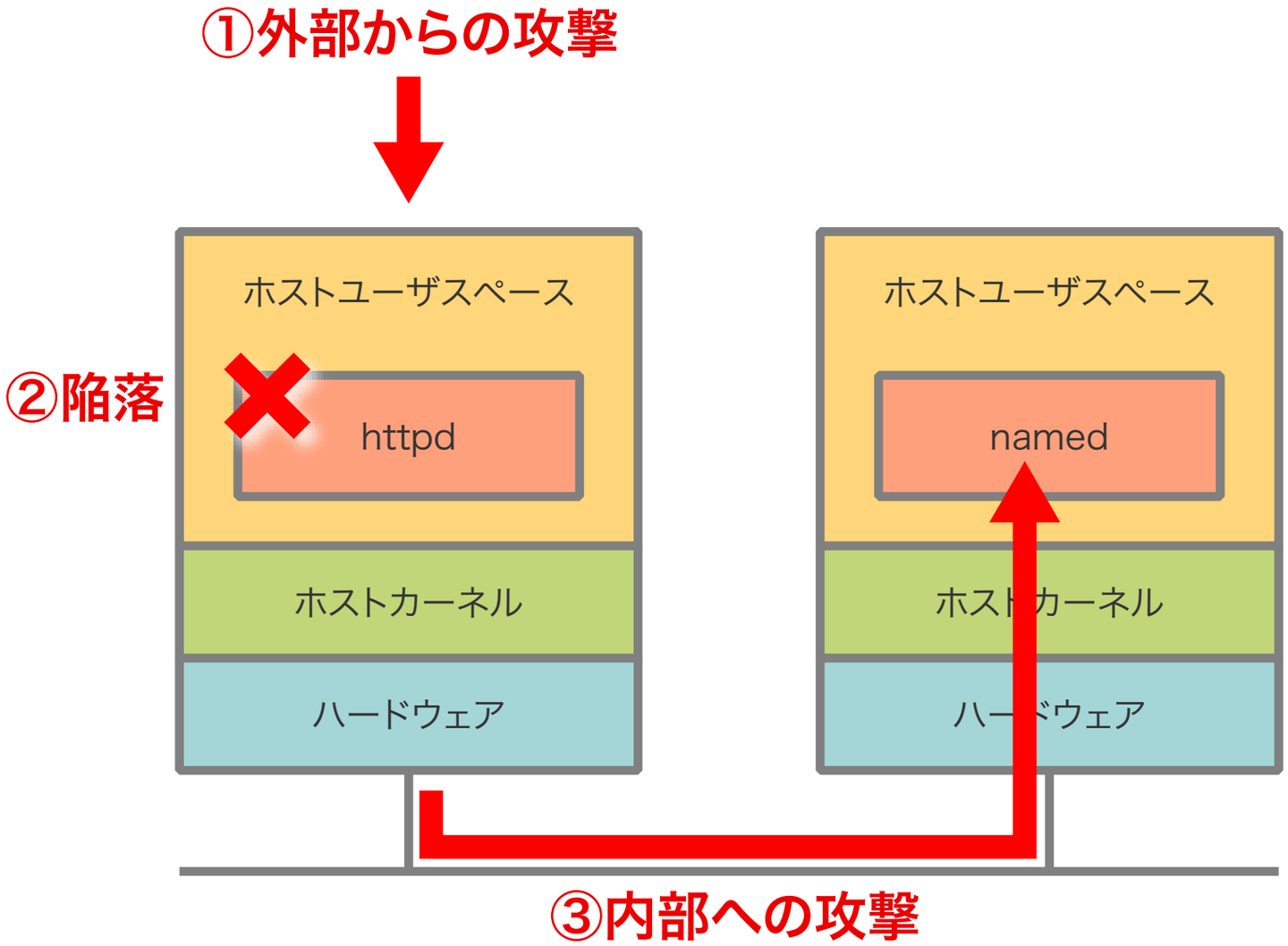


KVM(続き)

- QEMU
  - KVM以前から開発・利用
  - 多種のOSで動作
    - 命令を動的に変換
    - x86(_64)、ia64、ARM、SPARC...
- 各種H/Wのエミュレーションを提供
- ユーザプロセス
  - SELinuxでは1ドメインとして扱われる

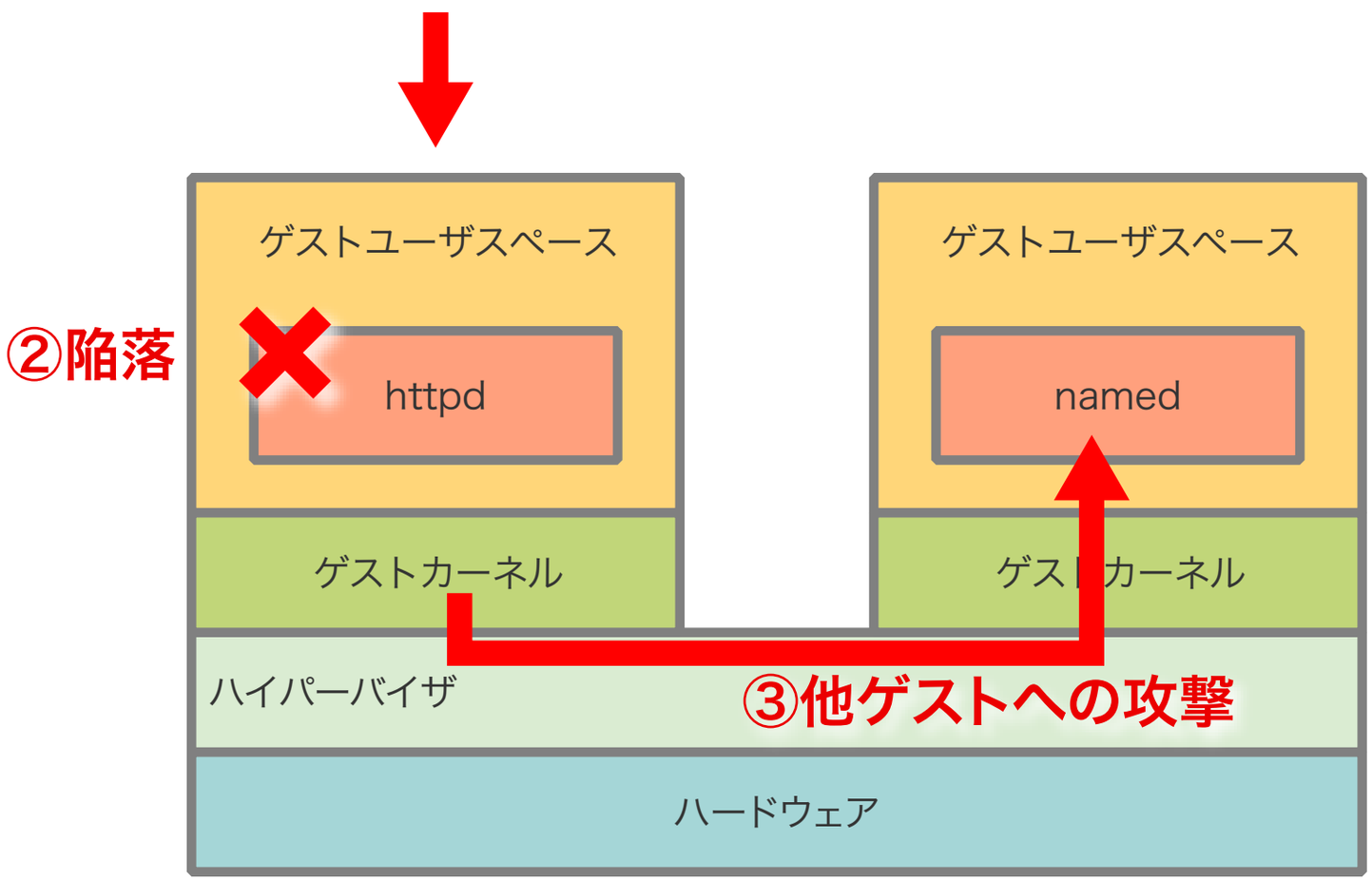
新たなる脅威

- 従来の攻撃はネットワーク経由



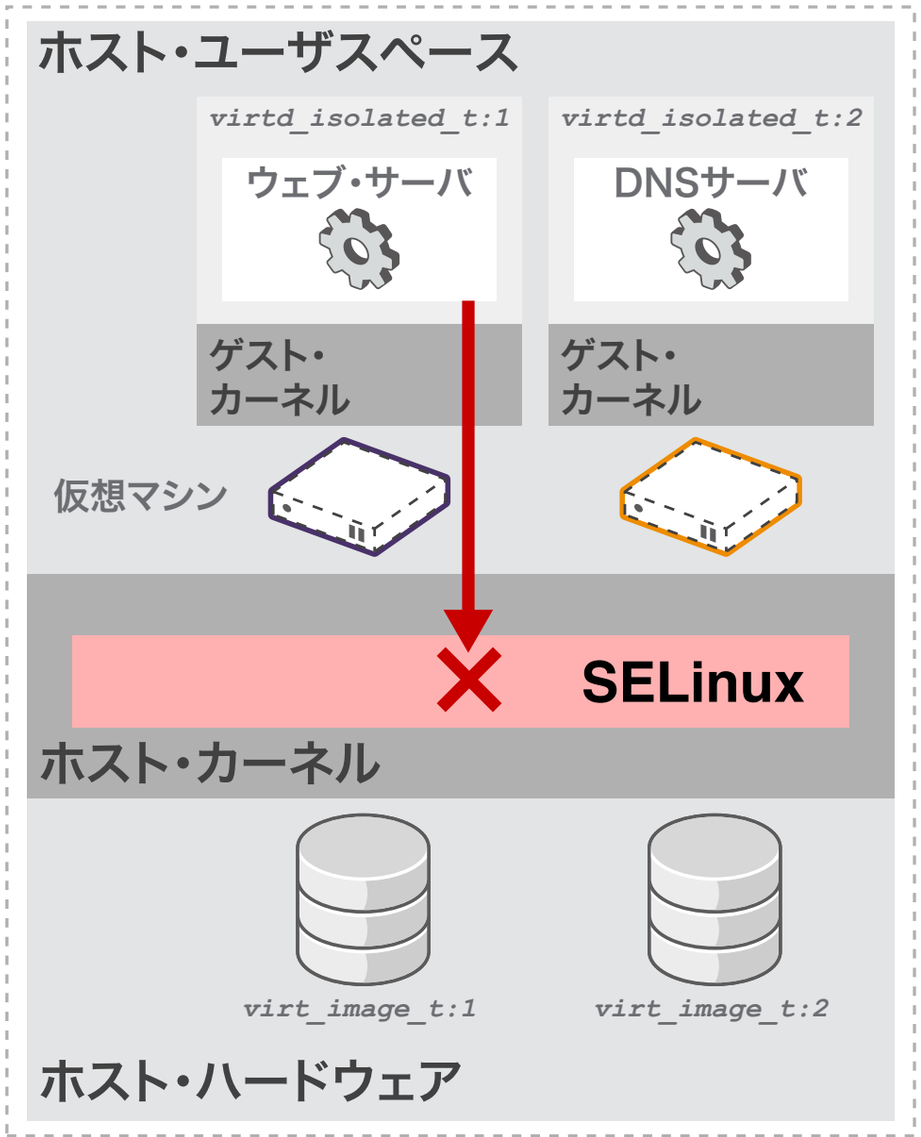
新たなる脅威(続き)

- 新たな攻撃はハイパーバイザ経由



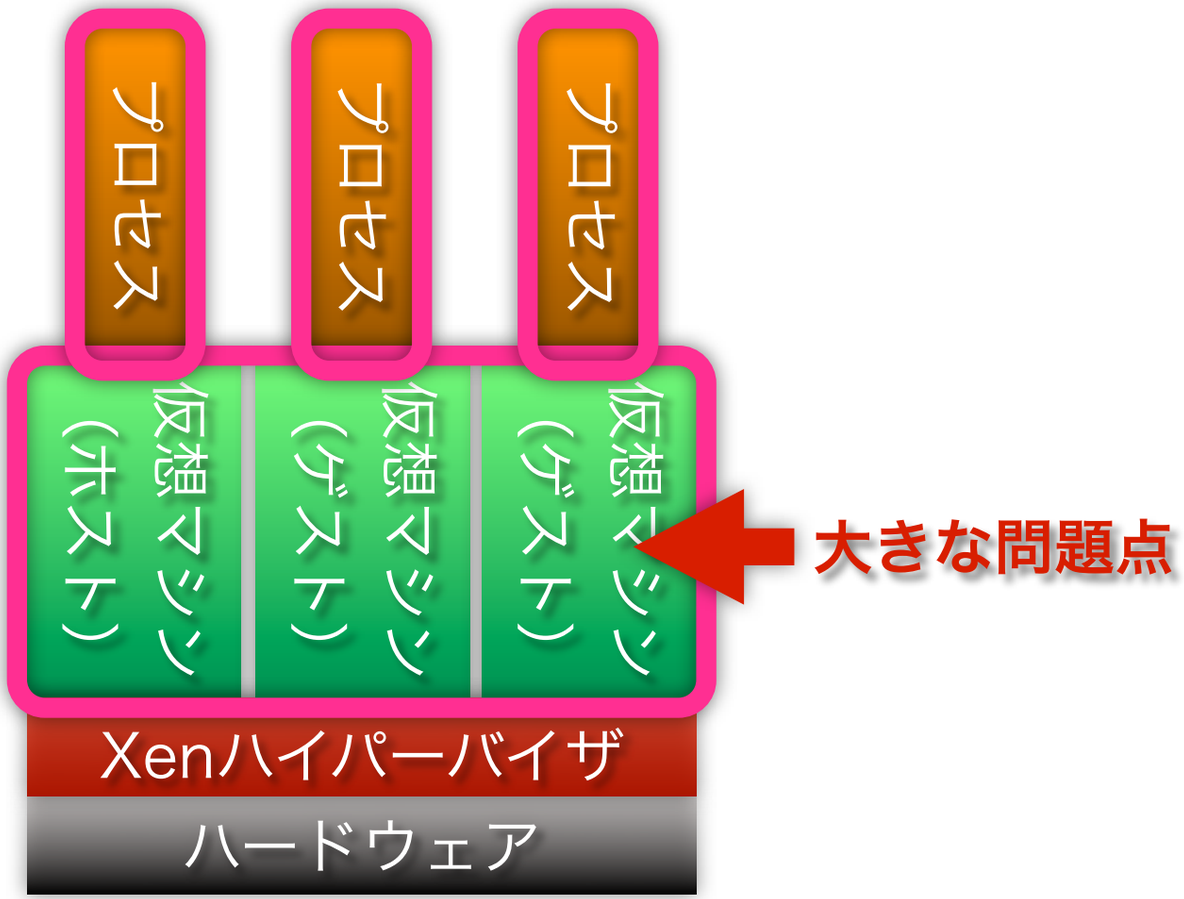
Svirt

- SELinuxを仮想化に適用
  - セキュリティポリシーをハイパーバイザに
- libvirtを拡張
  - 仮想ゲストやリソース
  - ラベル・virtd_isolated_t:<UUID>を付与

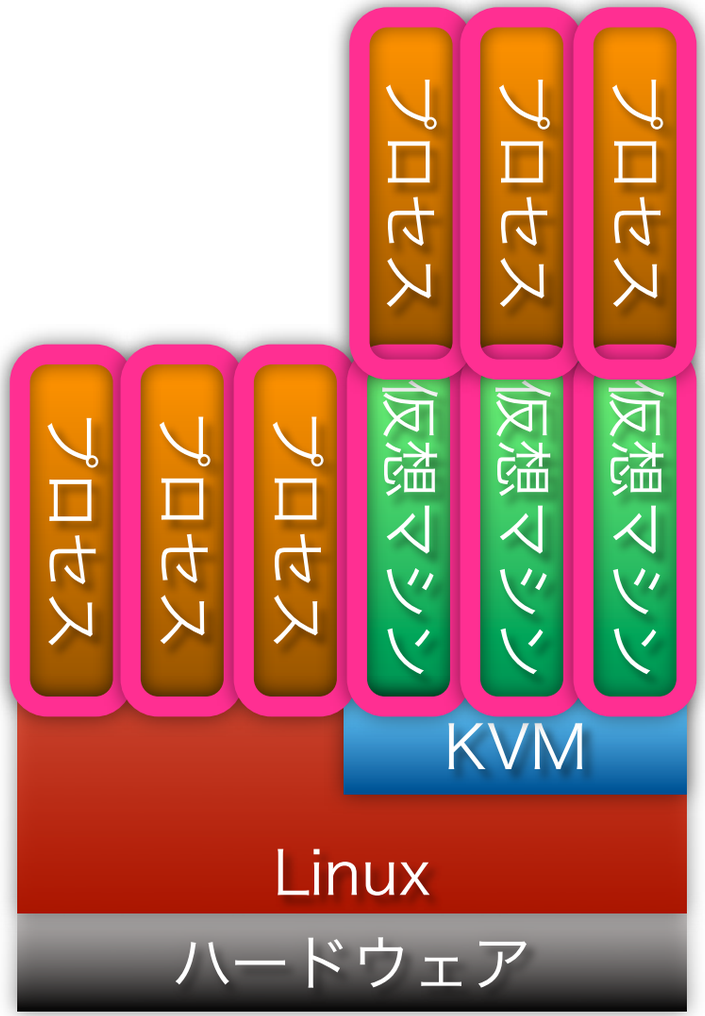


Xenとの比較

- KVMでは孤立させられる



Xenにおけるドメイン



KVMにおけるドメイン

利用状況(米)

- 米政府
  - ミリタリーとシビリアンで標準を区別
  - ミリタリー
    - DISA（国防情報システム局）が管轄
    - NIAPがポリシーを管理：CCが用いられる
      - PL-1～3ではSELinuxは不要
      - 最高レベルではSELinuxが必須

利用状況(米-続き)

- シビリアン
  - NIST（国立標準技術研究所）が管轄
  - FISMAがポリシーを管理
  - FDCC（Federal Desktop Core Configuration）を用いる
- Red Hatも参加し策定作業中
  - SELinuxが必要
  - 近々公開される予定

利用状況(米-続き)

- 利用している組織
  - NAVY
    - MLS（SELinux）を利用
  - Marines / Coast Guard
    - NAVYと同様
  - いくつかの情報部（非公開）
    - SELinuxを利用

利用状況(米-続き)

- 利用予定の組織
  - FISMAのポリシーを利用する全部局
  - NASA、農務省、司法省など

利用状況(オーストラリア)

- オーストラリア国防軍
  - 全てのサービスでSELinuxを利用
  - “Australian Defense Force uses it in all Services. None of them ever turn SELinux off.” by Ross Ford, Federal Territory Manager in Australia