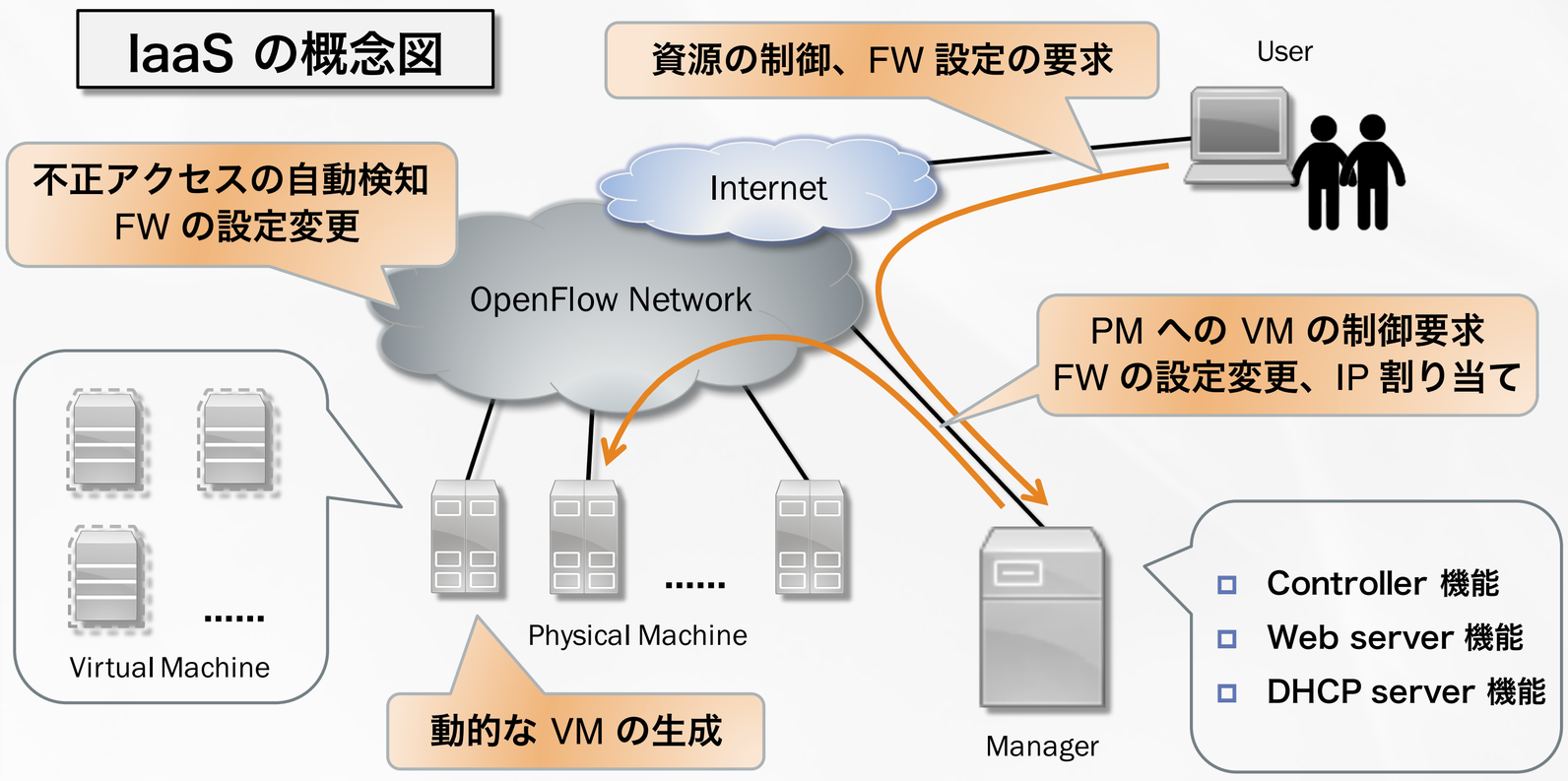
OSAKA UNIVERSITY

不正アクセス検知機能を持つ仮想ファイアウォールを備えた IaaS の実装

概要と目的

- FW (FireWall) 機能を持つ IaaS の開発
  - WUI (Web User Interface) による簡便な利用システム
  - ユーザ毎に個別のコンピュータ資源を柔軟に割り当て
  - FW によるアクセス制限
    - ユーザの要求によるルールの追加と削除
    - 不正アクセスの自動検知によるルールの追加と削除

アクセス制御と不正アクセス対策機能を兼ね備えた、柔軟で簡便なコンピュータ資源の提供が可能に！！



実現方法

IaaS システムの実現

Web server 機能

- ユーザに対し WUI で要求受付
  - ユーザ管理、VM の生成/削除/編集/起動/停止、FW の設定変更
- ユーザ情報を管理（ID + パスワード）

⇩ Controller に要求を伝達

Controller 機能

- Web server からの要求を処理
  - ユーザ登録：スライス生成
  - FW の設定変更：ファイアウォール機能の実現

⇩ PM に VM 管理の命令を伝達

PM 機能

- Controller からの命令を PM (Windows) 上で実行
  - VM の生成/削除/編集/起動/停止

⇩ DHCP server に IP アドレスの要求

DHCP server 機能

- PM の要求に対して VM に IP アドレスを動的に割り当て

ファイアウォール機能の実現

- OpenFlow のフローテーブルを ACL として活用

1. ユーザからの要求に対する設定変更
   - ユーザの指定に従いフローの生成 / 削除 / 編集
2. 不正アクセスの検知からの設定変更
   - パケットのヘッダを監視し、異常を検知
   - 該当ヘッダの特徴に対応するアクセス遮断用のフローをVSI に追加
   - 同ルールを適用すべき他の VSI にフローを共有

工夫点

- 資源の要求と FW の設定変更に WUI を利用
  - ユーザ・フレンドリーなシステムの実現
  - インタフェースの統一による手続の一元化
- 不正アクセス検知に基づく、フィルタリングルールの自動生成と共有
  - ユーザや管理者の手を煩わせずに適切にアクセス制御
  - OpenFlow / SDN の特性を活かした親和性の高い設計

デモ内容

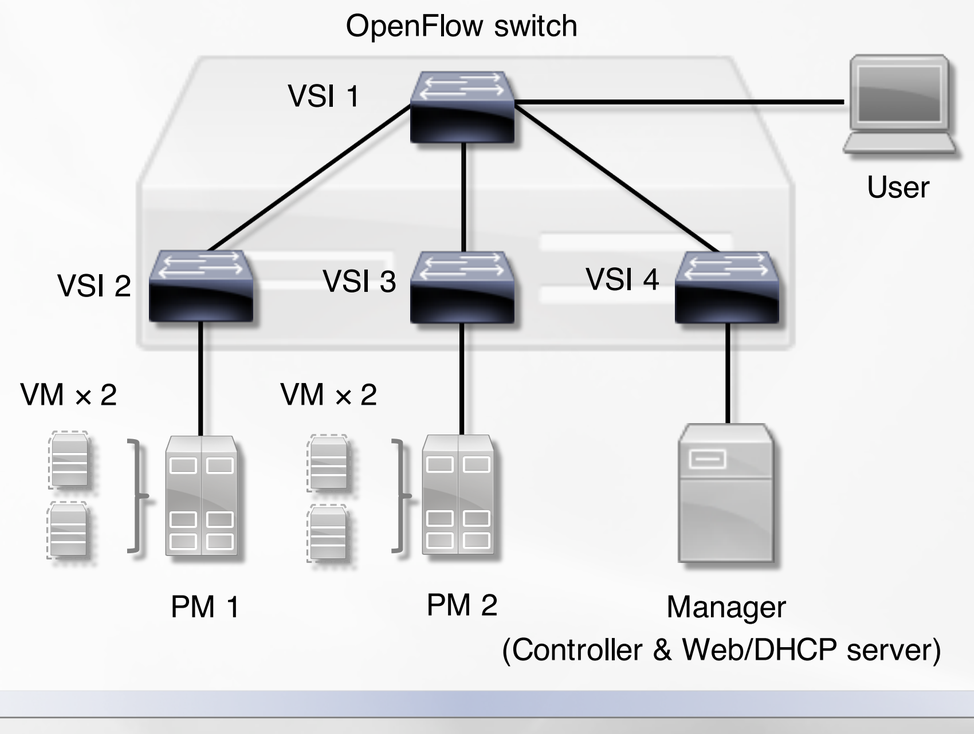
- シナリオ

1. WUI 上のユーザ要求による VM 資源の割り当て
   - ユーザの登録と削除
   - VM の生成 / 削除 / 編集 / 起動 / 停止

2a. WUI 上のユーザ要求による FW の設定変更
   - 外部からの VM1 に対するアクセスを遮断

2b. 不正アクセスの自動検知と FW の設定変更
   - VM1 に対する ICMP Flood を実施
   - Controller が攻撃を検知し、 攻撃者の IP からのアクセスを遮断するルールを VSI に適用

- ネットワーク構成



まとめ

- 単独での動作確認に成功
  - ユーザー要求による VM 資源の生成 / 削除 / 編集
- 仮想マシン上での動作確認に成功
  - ユーザー要求による FW の設定変更
  - 不正アクセスを自動的な検出と、FW の設定変更
- OpenFlow との共存に失敗
  - Trema の起動にはネットワークの切断が必要であるのに対し、IaaS の運用にはネットワーク接続が必要である