研究室紹介

最所研究室

https://air.eng.kagawa-u.ac.jp

目次

- はじめに
- 研究紹介
  - 脆弱性情報に基づいたセキュリティ対策
  - 試行錯誤できるセキュリティ演習
  - コンテナセキュリティ
  - Webサービスのオートスケーリング
- おわりに

はじめに

最所研究室とは

Webサービスの品質向上を
目的とした研究を行なっています

研究内容：
　ネットワーク，セキュリティ，
　クラウド
場所：
　1号館10階北側
ゼミ：
　週1回(現在は木曜13:00～)
就職先傾向：
　ITインフラ系，Web系，SI系

例えば…

サイトにアクセスしづらい状態が発生!!
⇨サーバ増やせば解決するけど，
　無駄にサーバを増やしたくない
⇨どうすれば効率良く増減できる？

メリット

開発経験，運用経験を積める
⇨就活で**有利**に働く

研究を自由に進められる
⇨**自力で進める力**が身に付く

院生が多い
⇨**手厚いサポート**を受けられる

脆弱性情報に基づいたセキュリティ対策

目的

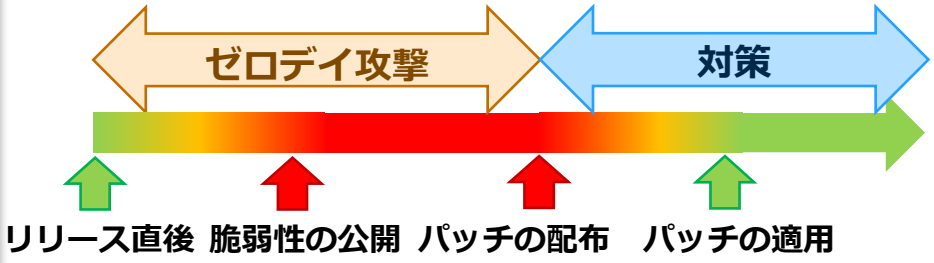
ゼロデイ攻撃による被害が甚大
標的型攻撃と組み合わされる

インターネット上に公開されている脆弱性情報などを用いて，組織内の脆弱性を検出．ネットワークから排除することで組織内の**重要な資産を守る**

キーワード

情報セキュリティ,ゼロデイ攻撃,
標的型攻撃,脆弱性,BYOD

ゼロデイ攻撃



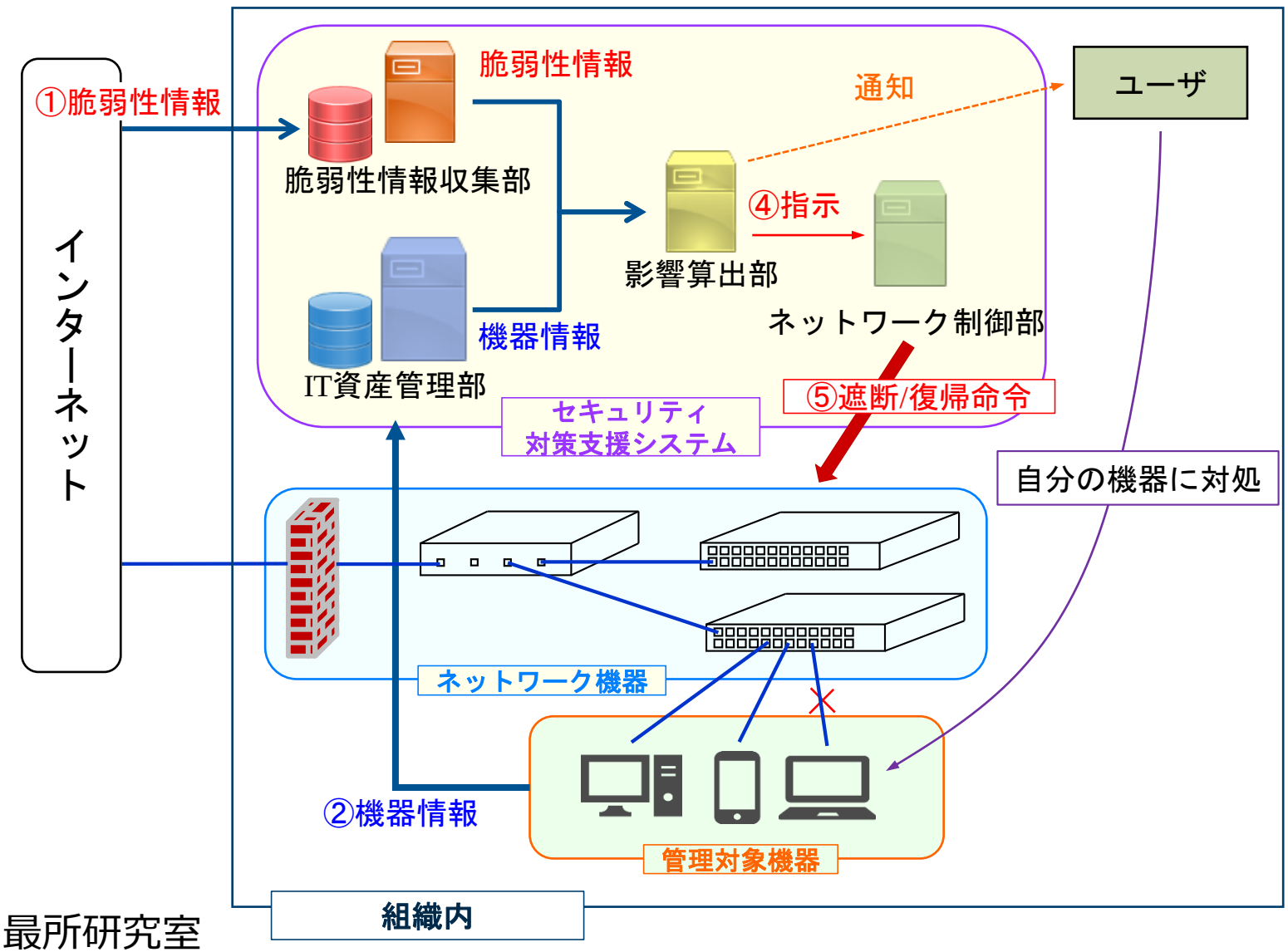
標的型攻撃

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW

引用 : IPA, 情報セキュリティ10大脅威 2021,
https://www.ipa.go.jp/security/vuln/10threats2021.html

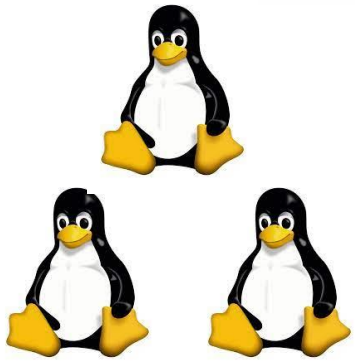
最所研究室
https://air.eng.kagawa-u.ac.jp

脆弱性情報に基づいたセキュリティ対策



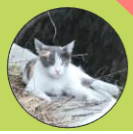
こんなことに興味がある人

- ✓ゼロデイ攻撃対策
- ✓標的型攻撃対策
- ✓脆弱性対策
- ✓サーバ
- ✓ネットワーク



試行錯誤ができるセキュリティ演習

NEW!



目的

知識と経験を持つ**セキュリティ人材**が**不足**している.

防御演習を**試行錯誤**することで，**セキュリティ人材の育成**を目指す.

セキュリティ教育 + 試行錯誤 = ?
セキュリティ人材の育成

サイバー攻撃から防御する
- 防御手法の調査 (調査)
- 防御手法の選別 (選別)
- 防御手法の試行錯誤 (試行)

サイバー防御の演習を試行錯誤
"ぷろてっくん"

最所研究室
https://air.eng.kagawa-u.ac.jp

試行錯誤ができるセキュリティ演習

NEW!

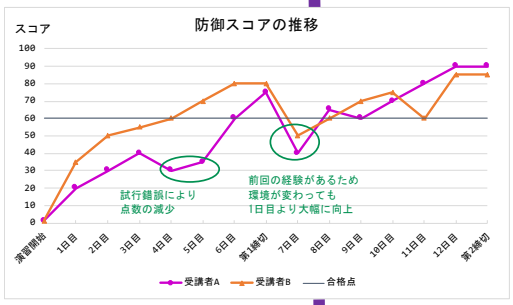
PURCHASE

購入

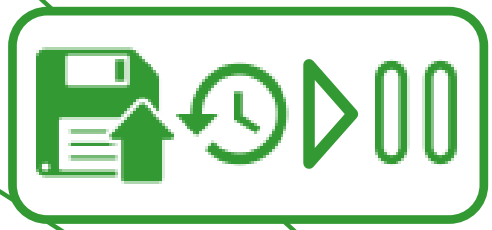
EC

攻撃

ATTACK




```
# less /var/log/files
This app is faild.
# system stop ec
# port block http
# port che
```



管理

ぷろてっくん

受講者

- root
  - saveA
    - saveB
    - saveC
    - saveD
  - attack
    - allPortDown
    - telnetDown

MSR
Machine-Save-Restore

試行錯誤ができるセキュリティ演習

NEW!

防御スコア

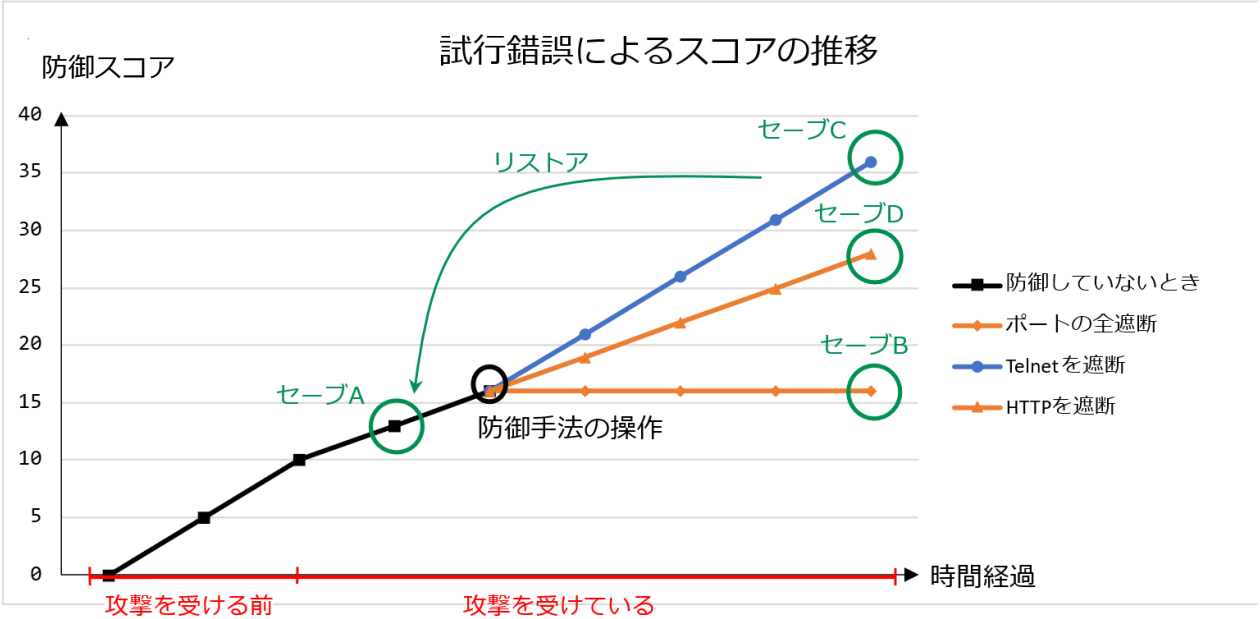
- 成功度合い
- 他の受講者と共有
- 対抗意識を促す

試行錯誤

- セーブ&リストア
- 防御手法を何度も実践
- 最適な防御手法を検討

単独で自宅演習

- 手を動かせる
- 自宅で長期間
- COVID-19でも安心



最所研究室

https://air.eng.kagawa-u.ac.jp

試行錯誤ができるセキュリティ演習

NEW!

技術

セキュリティ，ハードニング，仮想マシン，シェルスクリプト，
✚ More … ？

NEW!

まだまだ発展の余地がたくさん！

いろいろ足りていないとも




コンテナセキュリティ

目的

コンテナ型仮想環境内で
マルウェアの実行を防ぎたい

↓

システムコールをフィルタ

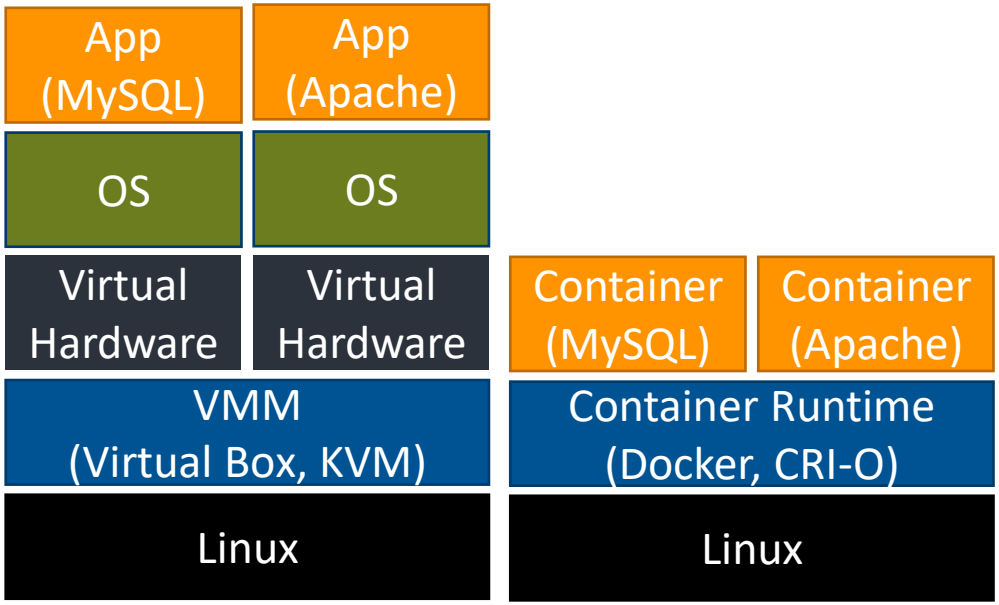
↓

コンテナで使用するシステムコール
をリストアップするシステムを開発

OS, コンテナ型仮想化,
システムコールフィルタ

コンテナ型仮想化

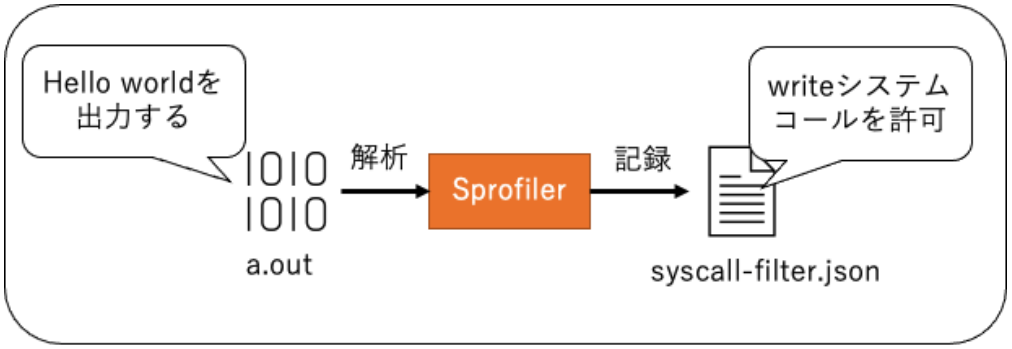
仮想化手法の1つ
仮想マシン(VM)より軽量かつ高速
システムコールの攻撃に脆弱

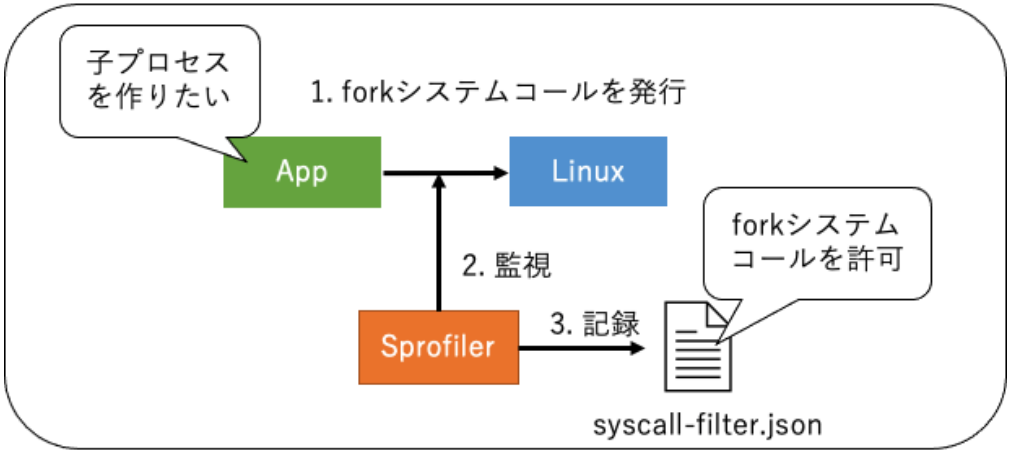


https://github.com/sai-lab/sprofiler

最所研究室
https://air.eng.kagawa-u.ac.jp

コンテナセキュリティ





実行を許可する
システムコール

```
"syscalls": [
  {
    "names": [
      "close",
      "fcntl",
      "mmap",
      "munmap",
      "readlinkat",
      "write"
    ],
```

課題

人間がアプリの使用するシステムコールをすべて把握するのは困難

解決策

システムコールを自動で解析

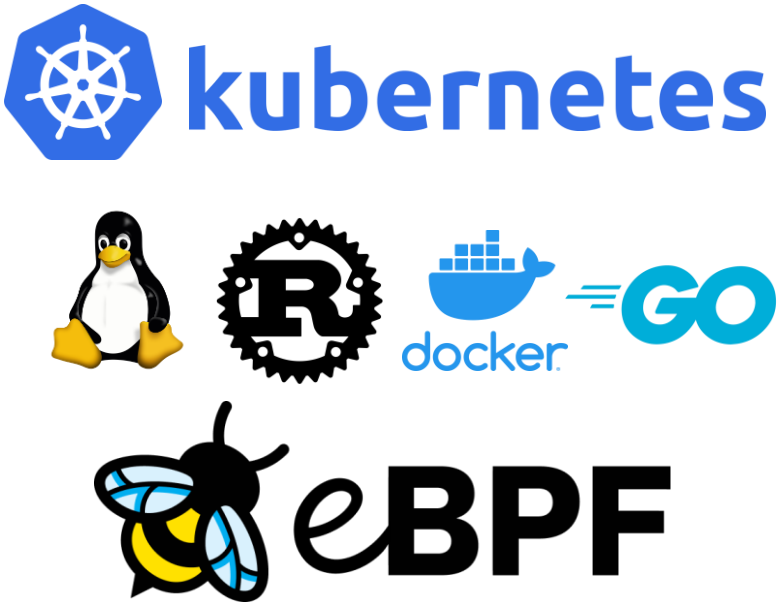
1. 実行形式バイナリファイルから解析
2. アプリケーションを実行して使用されたシステムコールを記録

最所研究室
https://air.eng.kagawa-u.ac.jp

https://github.com/sai-lab/sprofiler

身につく技術

- 低レイヤー(OS, 仮想化技術)の知識
- コーディング力
- 最新の技術の動向を追いかける力
  - Linuxカーネルの最新技術
  - Kubernetesなどのコンテナ技術



進路

- 業種: 情報通信
- 職種: ソフトウェアエンジニア
- 業務: クラウドサービスの開発

Webサービスのオートスケーリング

目的

インターネットの普及により，Webサーバへのアクセスが多様化し，アクセス数の予測が難しくなっている．本研究では，**クラウド(仮想化技術)**を用い，アクセス数に応じてWebサーバの増減を行うことで，**快適なWebサービス**を提供するオートスケーリング機構を開発する．

分散Webシステム,
オートスケール,
負荷分散, 仮想化技術

用語

・オートスケール

仕事量に応じてサービス能力を動的に変更する仕組み．

・クラウド

ユーザがインフラやソフトウェアを持たなくても，インターネットを通じて，サービスが必要なときに必要な分だけ利用できる仕組み．

・キャッシュサーバ

Webサーバのデータの複製し，そのサーバに代わって応答するサーバ．

・ロードバランサ

サービスにかかる負荷を複数のサーバに振り分ける装置．

最所研究室
https://air.eng.kagawa-u.ac.jp

背景

- クラウドを用いたキャッシュサーバ
  - クラウド環境の発展
  - クラウド上の仮想マシンを用いて**キャッシュサーバ**を構築
  - 負荷分散によって、より安定したWebサービスを提供
- キャッシュサーバを用いる場合の問題点
  - 負荷に対して用意したキャッシュサーバ数が

  ⇨少ない ： 過負荷の場合に**応答性の改善が不十分**

  ⇨多い ： リソース過剰で**余分なコスト発生**

目的

- 大量のリクエストがあっても応答性を維持
- 負荷量に対してサーバ数を最適化し余剰なコストを削減

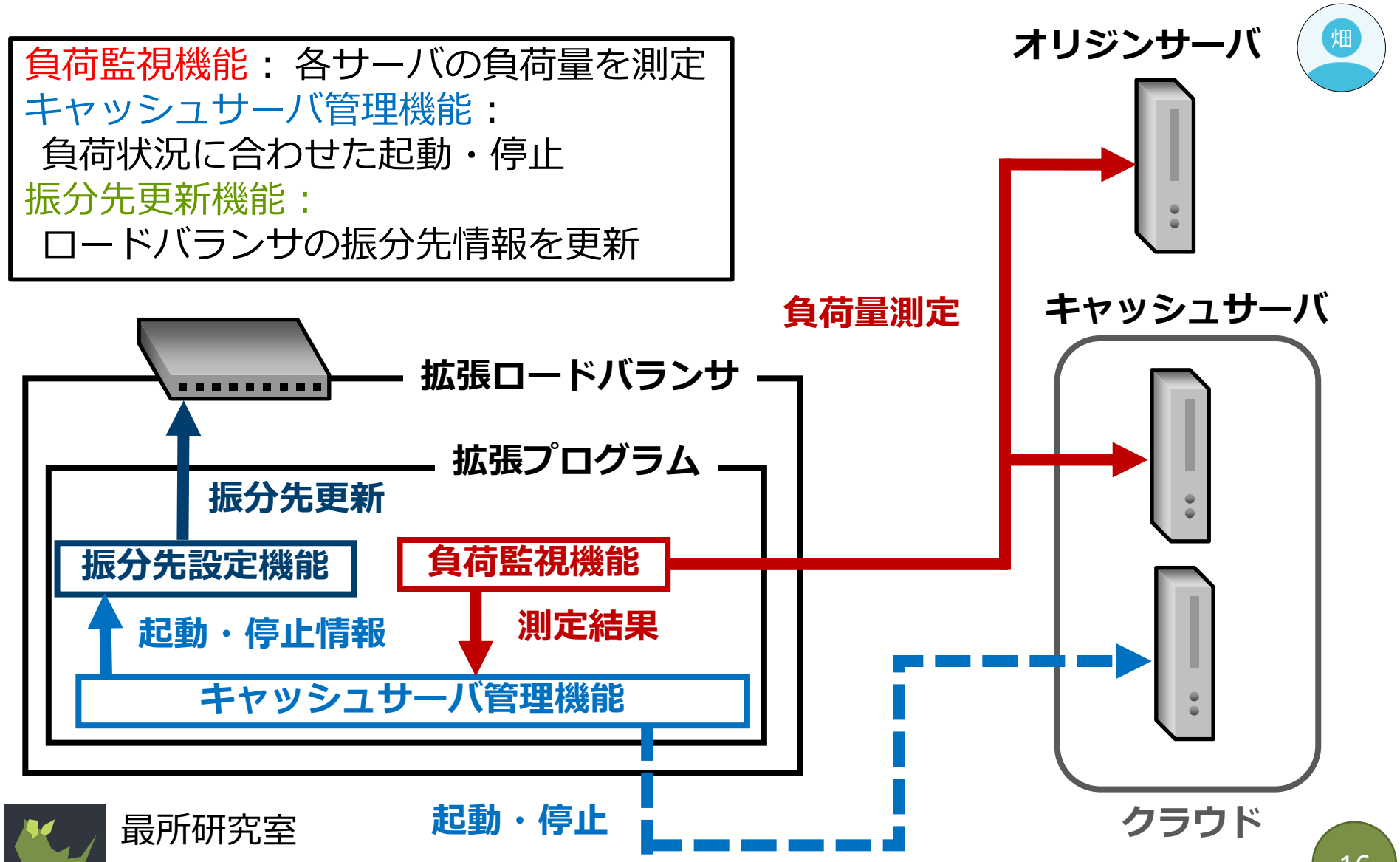
  ⇨**オートスケール**

  (負荷の監視 + 動的な起動(スケールアウト)・停止(スケールイン))

システムの概要

Webサービスのオートスケーリング

負荷監視機能： 各サーバの負荷量を測定
キャッシュサーバ管理機能：
負荷状況に合わせた起動・停止
振分先更新機能：
ロードバランサの振分先情報を更新



おわりに

最所研究室とは？

- **Webサービスの品質向上**
- **1号館10階**
- **contact@air.eng.kagawa-u.ac.jp**

研究テーマ	目的	技術
脆弱性情報に基づいた セキュリティ対策	組織のセキュリティ向上	ゼロデイ攻撃, 標的型攻撃,脆弱性
試行錯誤できる セキュリティ演習	セキュリティ人材の育成	仮想マシン, シェルスクリプト, ハードニング
コンテナセキュリティ	マルウェアからのコンテナ保護	OS, コンテナ型仮想化, システムコールフィルタ
Webサービスの オートスケーリング	Webサービスの可用性向上	分散Webシステム, 負荷分散, 仮想化技術

最所研究室

https://air.eng.kagawa-u.ac.jp

求ム！
自分の腕と技術に
自信がある学生！
Mr. Takehara

OSや仮想化技術に
興味がある学生は
一緒に勉強しましょう！
Mr. Iiguni

セキュリティに
興味がある人，
一度研究室まで
来てみて下さい！
Mr. Nishioka

システムに興味がある人，
気軽に来てください！
Prof. Saisho

困りごとあれば
いつでも相談に
来てください！！
Mr. Goto

ぜひ，
お話しましょう！
Ms. Ishizuka

Welcome to Sai-Lab.

Special Thanks!

Prof. Saisho, Mr. Iiguni, Mr. Takehara, Mr. Nishioka, Mr. Hata, Mr. Goto, Ms. Ishizuka