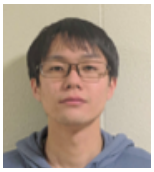
# 脆弱性情報を用いたアクセス制御に基づく ゼロデイ攻撃対策セキュリティシステム



香川大学大学院工学研究科信頼性情報システム工学専攻　最所研究室　竹原一駿
連絡先 s20g470@stu.kagawa-u.ac.jp

## ゼロデイ攻撃の増加

○ 標的型攻撃と組み合わせることが多い
○ ゼロデイ攻撃自体を防ぐことは難しい

○ 個人情報や営業資料の流出
○ コンピュータの乗っ取り

## BYODの増加

○ 個人端末を講義や業務に用いる
○ 情報資産が個人端末に依存する

○ 組織のネットワークに接続
○ 脆弱性が存在する機器

## 個人情報など情報資産の保護

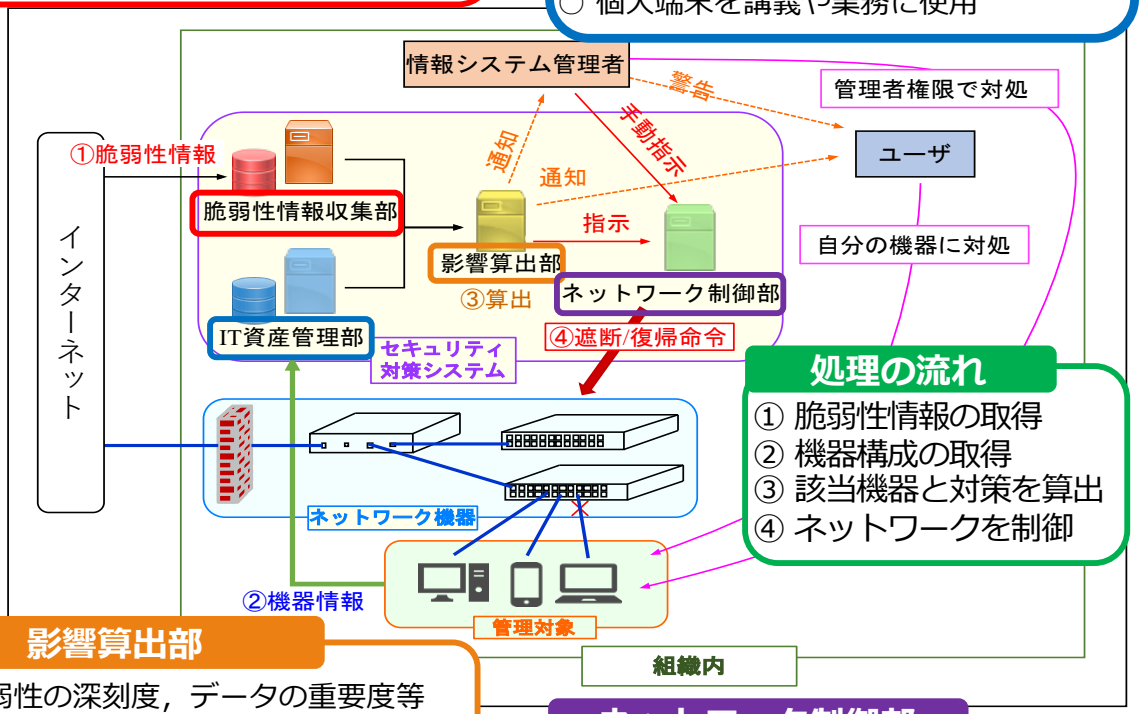
## 脆弱性情報と機器情報を用いてアクセス制御を行う ゼロデイ攻撃対策セキュリティシステム

### 脆弱性情報収集部

○ 公開された脆弱性情報をDBに保存
○ 対象製品，ソフトウェア，ベンダ
○ 脆弱性の深刻度
○ パッチ配布に関わらず速やかに

### IT資産管理部

○ 組織の機器を個人で紐付け
○ DBにて一元管理
○ 個人情報の有無などで重要度を設定
○ エージェントを機器に導入
○ 個人端末を講義や業務に使用




### 処理の流れ

① 脆弱性情報の取得
② 機器構成の取得
③ 該当機器と対策を算出
④ ネットワークを制御

### 影響算出部

○ 脆弱性の深刻度，データの重要度等
○ 外部との接続の遮断やアクセス制限
○ 制御方針と制御方法を算出

### ネットワーク制御部

○ 該当機器のMACアドレスを取得
○ 外部ネットワークからの遮断と復帰
○ 内部ネットワークからの隔離と復帰
○ 機器の接続箇所の変更への対応
○ VLANを使用
○ 無線LAN環境へも対応予定

### 今後の予定

□ 各部間の連携
□ 関係学会での発表
　○ ISEC情報セキュリティ研究会
　○ 情報処理学会　全国大会

[1] 楠目幹, 喜田弘司, 最所圭三. “脆弱性情報を利用したゼロデイ攻撃対策システムにおける構成情報収集機能の実装及び脆弱性評価機能の設計”. 電子情報通信学会技術研究報告, Vol. 119, No. 140, pp. 1~6, 2019.
[2] 西岡大助. “BYOD に対応したIT 資産管理システムの開発". 学士論文, 香川大学, 2020.
[3] 竹原一駿. ”脆弱性情報を用いたセキュリティシステムにおけるネットワーク制御機構に関する研究”. 学士論文, 香川大学, 2020.