脆弱性情報を利用したゼロデイ攻撃対策セキュリティシステム

Zero-Day Attack Prevention Security System Using Vulnerability Information

竹原一駿，楠目幹，西岡大助
最所研究室

目次

[付録]A-1. 用語解説

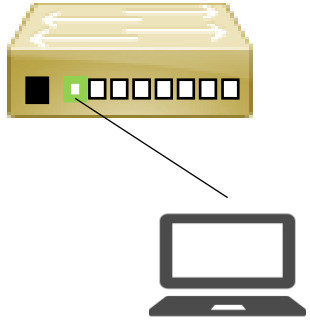
■ BYOD (Bring your own device)
- 個人保有の携帯機器を職場に持ち込み，業務に使用する
- 香川大学の学生にも義務づけられている

■ ソフトウェア
- コンピュータを動作させるためのプログラム(命令)を記述したデータのまとまり．Windows，Excel，Word

■ Firewall (ネットワーク機器)

- 外部とのネットワーク接続の間で検問する
- 防火壁と言われる

■ L2スイッチ (ネットワーク機器)
- ネットワークの接続を分割する
- 宛先を見て判断する機能がついている



[付録]A-2. 用語解説

■ 脆弱性 (セキュリティホール)

- プログラムの不具合や，設計上のミスが原因となって発生した情報セキュリティ上の欠陥
- 設定ミスや監査の不備なども脆弱性と成りえる

■ パッチ

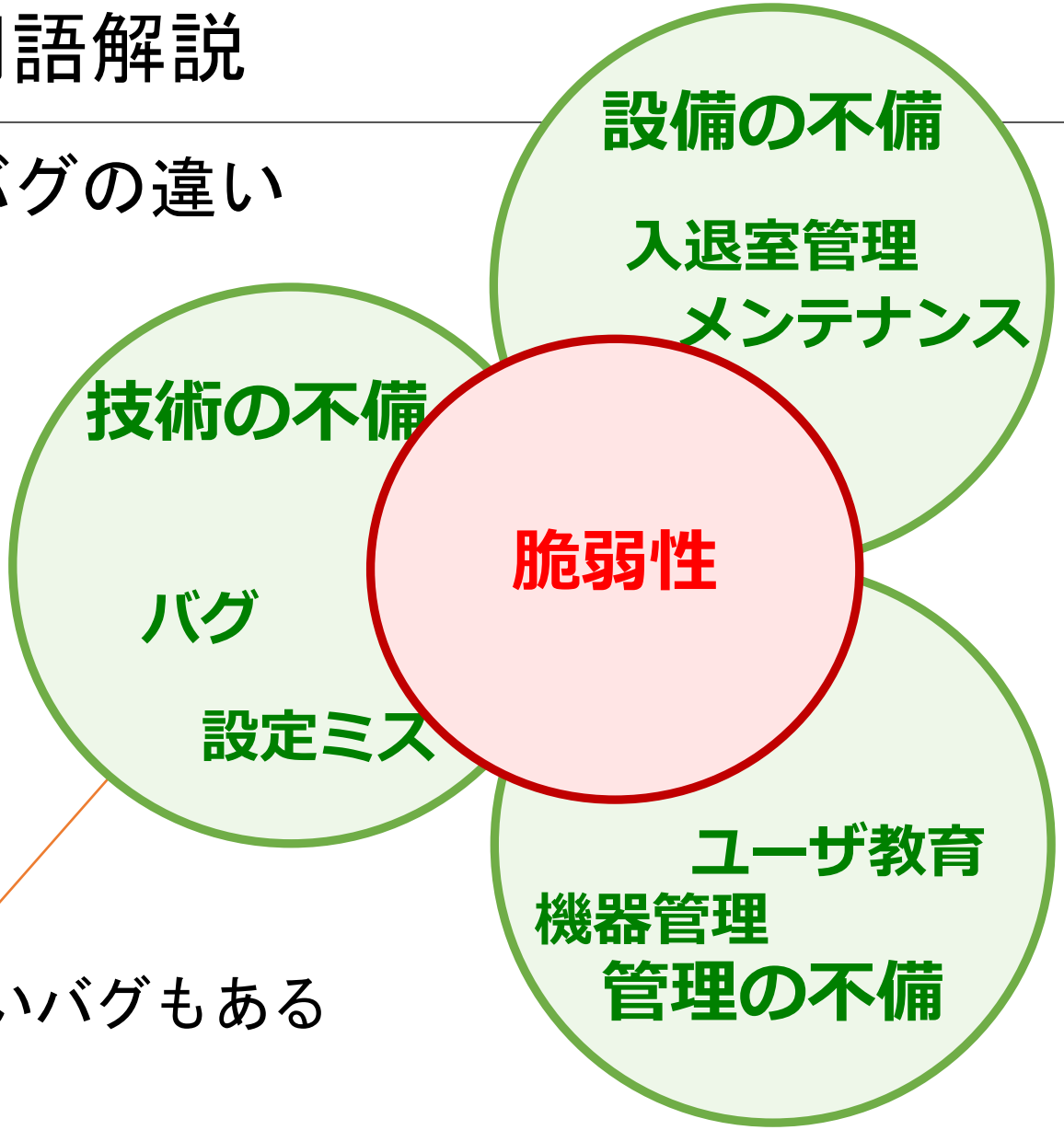
- 脆弱性やバグを修正するためのファイルやプログラム
- しばしば，Windows Updateで配信されている中身の一部

■ 情報資産

- 組織にとって守るべき価値をもつ情報
  (顧客情報，製品情報，マーケティング情報など)
- それを取り扱う一連の情報システム
  (必要なハードウェア，ソフトウェア，ネットワーク)

[付録]A-3. 用語解説

■ 脆弱性とバグの違い

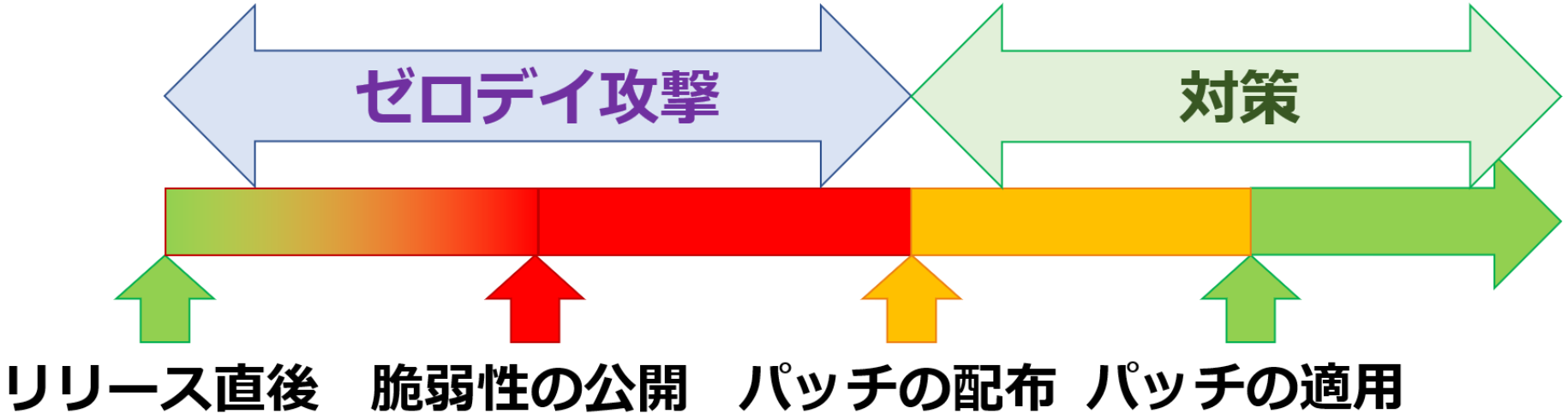


脆弱性とならないバグもある

[付録]A-4. 用語解説

■ ゼロデイ攻撃

- ソフトウェアに存在する脆弱性を発見
- ベンダによるパッチ配布前に行う攻撃
- 基本的な対策は，パッチの配布を待つ
- それまでの攻撃には，対応できない



[付録]A-5. おすすめ書

- 増井敏克, おうちで学べるセキュリティのきほん, 翔泳社
- 上原孝之, 情報処理教科書 情報処理安全確保支援士 2020年版, 翔泳社

[付録]B-1. 過去の発表実績

- 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.
- 竹原一駿, 最所圭三. “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”. 先端工学研究会2020, pp.49, 2020. (http://www.kagawa-u.ac.jp/kagawa-u_ead/topics/event/2020/)

1-1. はじめに

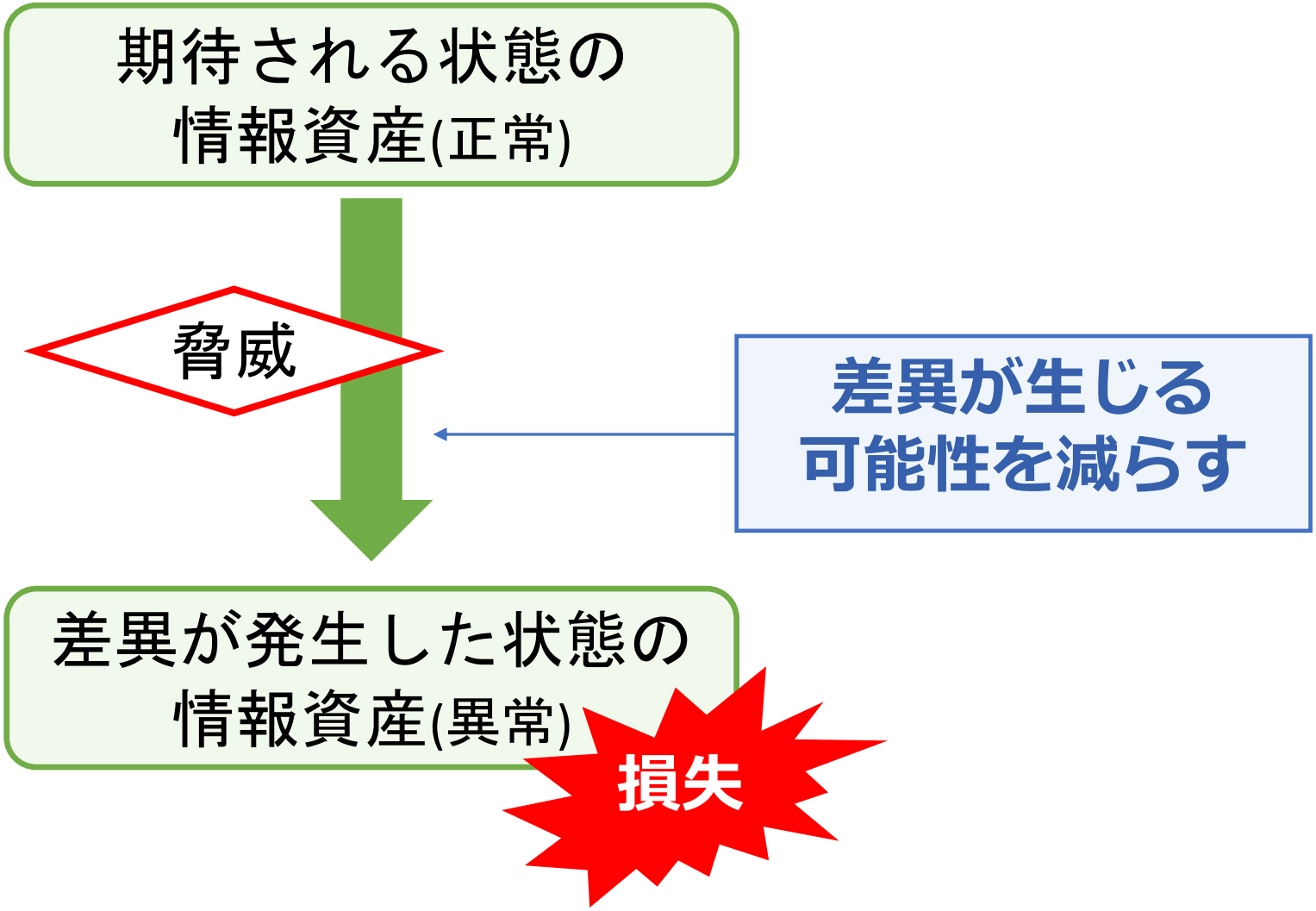
■ ゼロデイ攻撃による被害が増えている
- 標的型攻撃を組み合わせた攻撃
- ゼロデイ攻撃自体を防ぐことは難しい

■ 企業や大学におけるBYODが増えている
- 自らの機器を持ち込み，業務に使用する
- 組織のネットワークに接続することが多い

個人情報を始めとした情報資産を守る

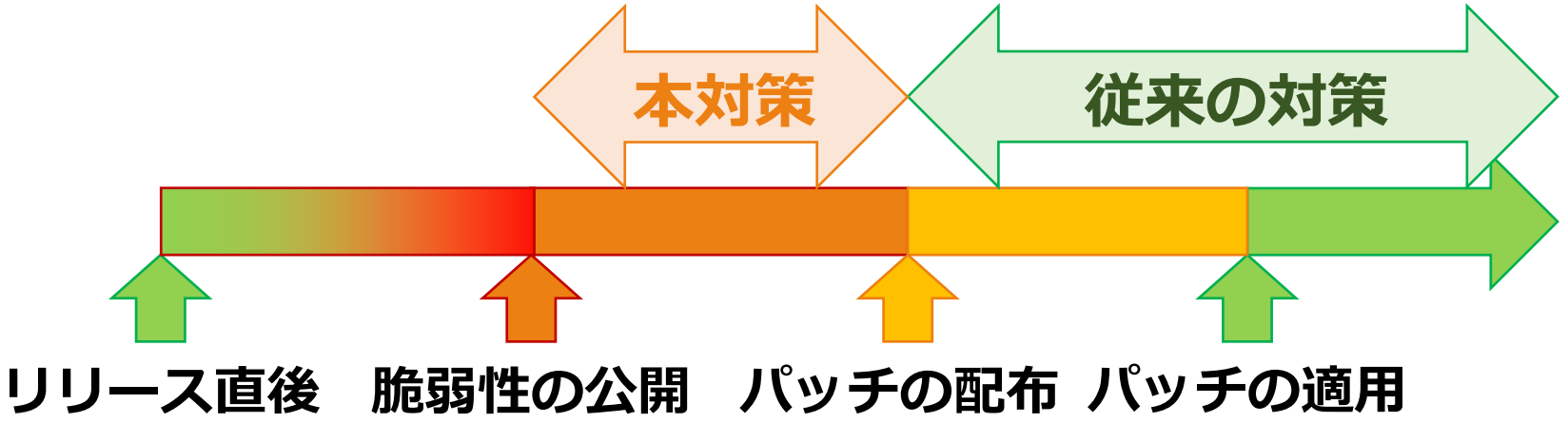
脆弱性情報と機器情報を用いて
ネットワーク制御を行う
ゼロデイ攻撃対策セキュリティシステム

1-2. 情報資産を守る

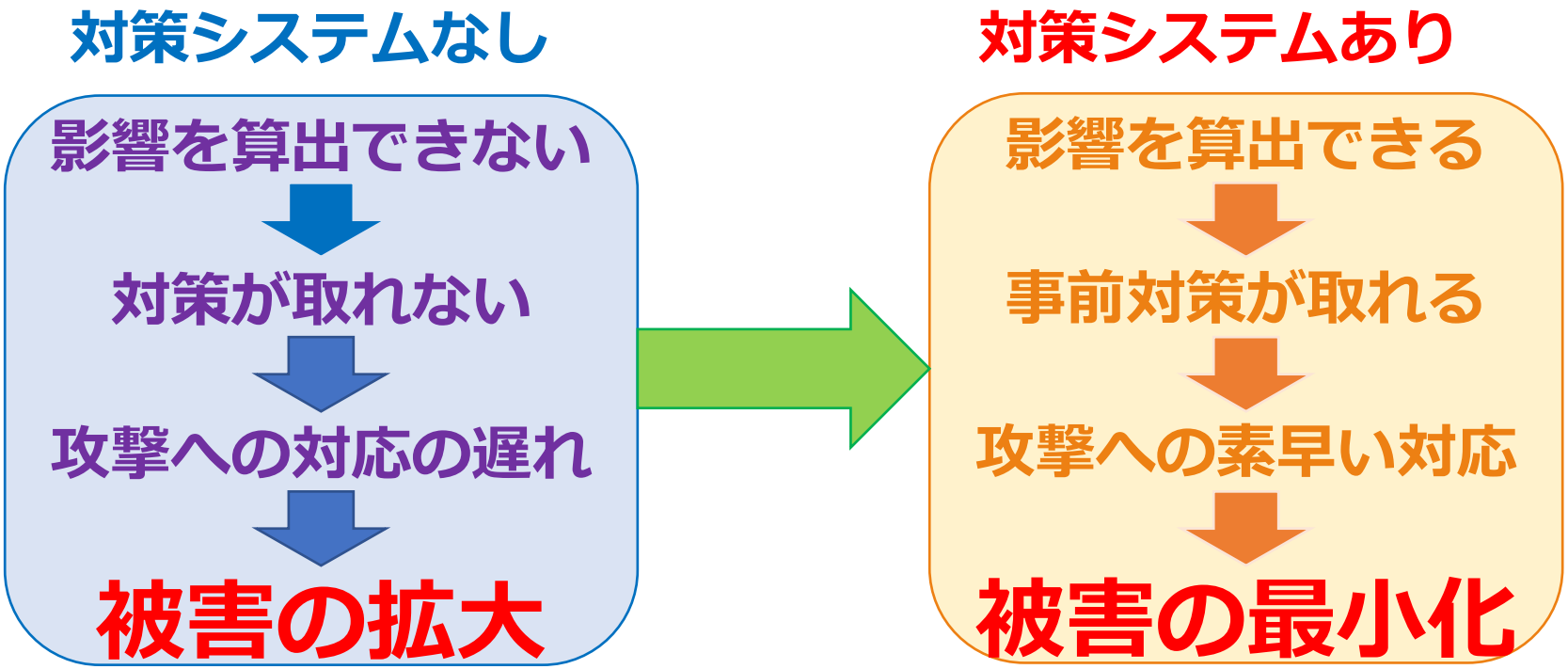


1-3. 本提案の狙い

パッチの配布に**依存しない**かつ
ソフトウェアの**脆弱性情報**を利用した対策



1-4. 本システムの効果



管理者が適切な対策を取れるように
影響範囲や**対策**を提供

s20g470@stu.kagawa-u.ac.jp

1-5. 影響範囲の予測

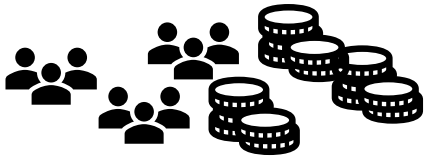
影響範囲を予測し、**事前対策**

- **影響の有無**
- **影響するマシン**
- **影響するマシン数**
- **マシンの管理者**
- **緊急性の有無**　等

→ **事前対策が取れる**

1-6. 本システムの目標

大企業



人材や資金が豊富

十分な対策が可能

大学や病院

人材や資金が不足

対策の不足や
属人化

大学や病院等の **小さな組織における**
セキュリティ対策の向上を目指す

対策が全く
取れていない

少しでも対策が
取れている

より対策が
取れている

2. 近年のゼロデイ攻撃による被害

■ Internet Explorer
- ライブラリの脆弱性を悪用
- 対策パッチ配布までは，アクセスしないことを推奨
- 被害を確認している

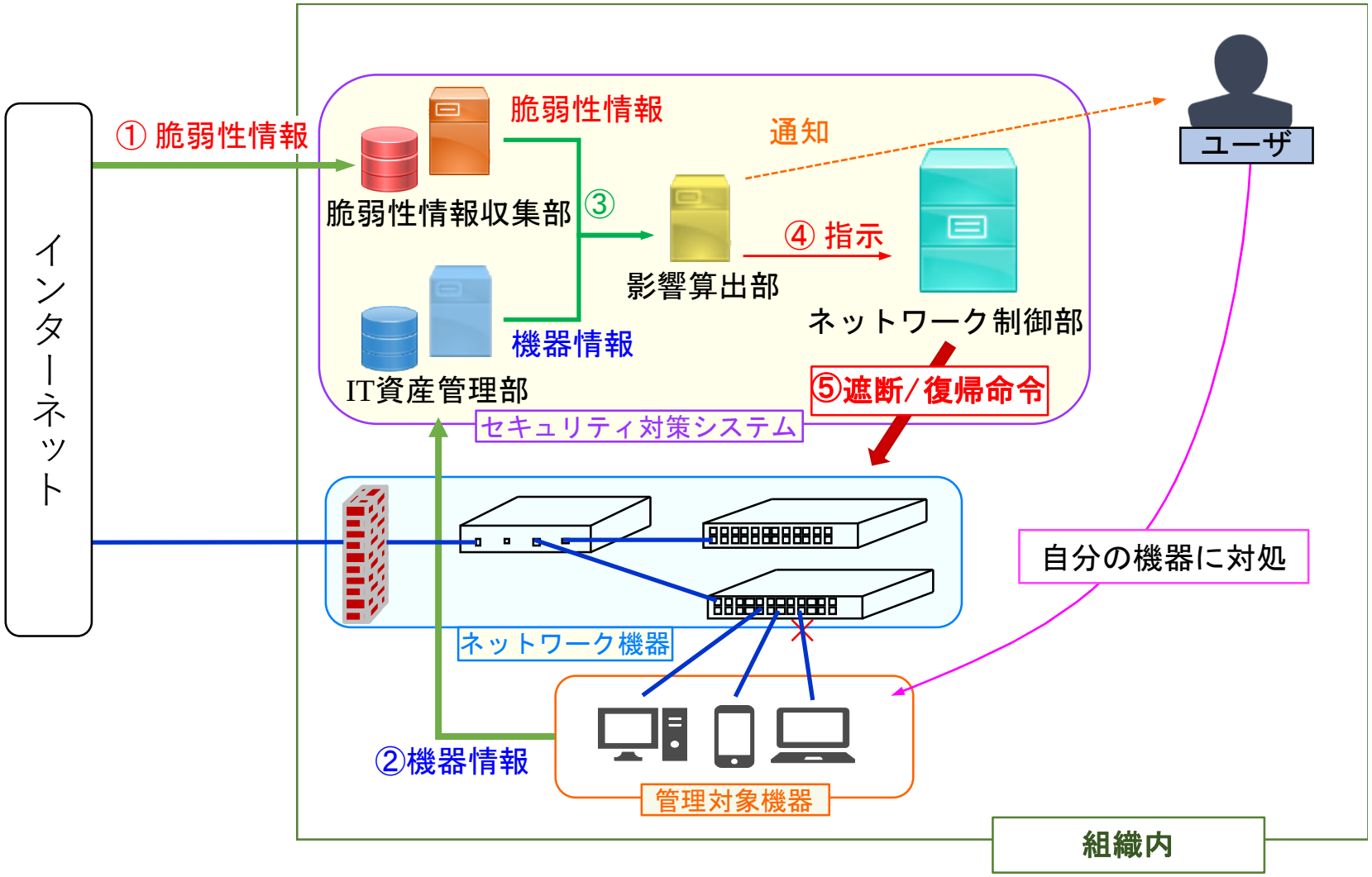
“Microsoft Internet Explorer の脆弱性対策について (CVE-2019-1367):IPA 独立行政法人 情報処理推進機構”
https://www.ipa.go.jp/security/ciadr/vul/20190924-ms.html，2020/01/29

■ 三菱電機
- ウイルス対策ソフトの脆弱性を悪用
- 8000人超えの個人情報，技術資料，営業資料が流出

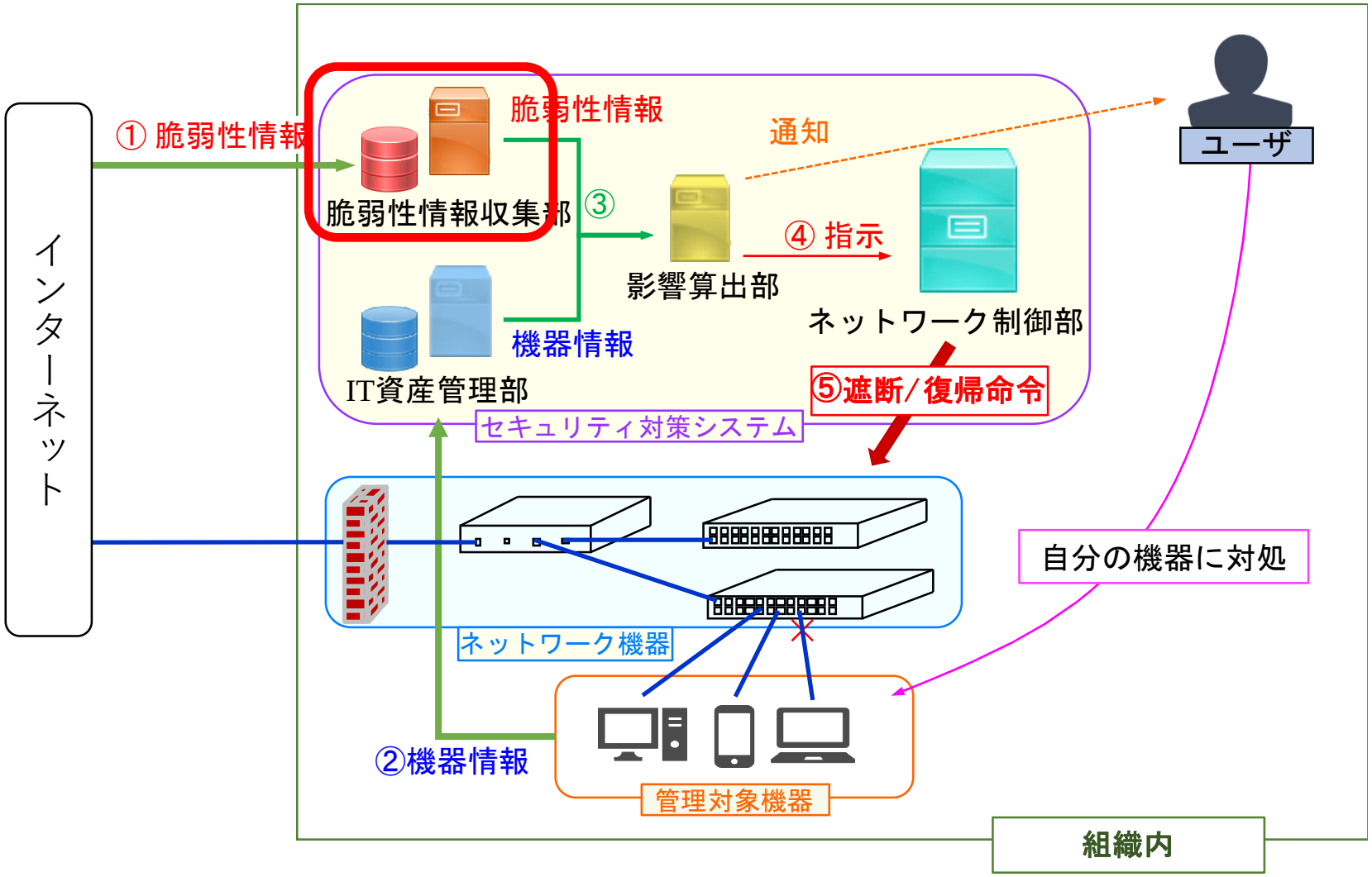
“三菱電機、約 8000 人の個人情報流出か ウイルス対策システムにゼロデ イ攻撃 - ITmedia NEWS”
https://www.itmedia.co.jp/news/articles/2001/21/news083.html, 2020/01/23

身近なソフトの脆弱性を悪用

3-1. システム全体の流れ

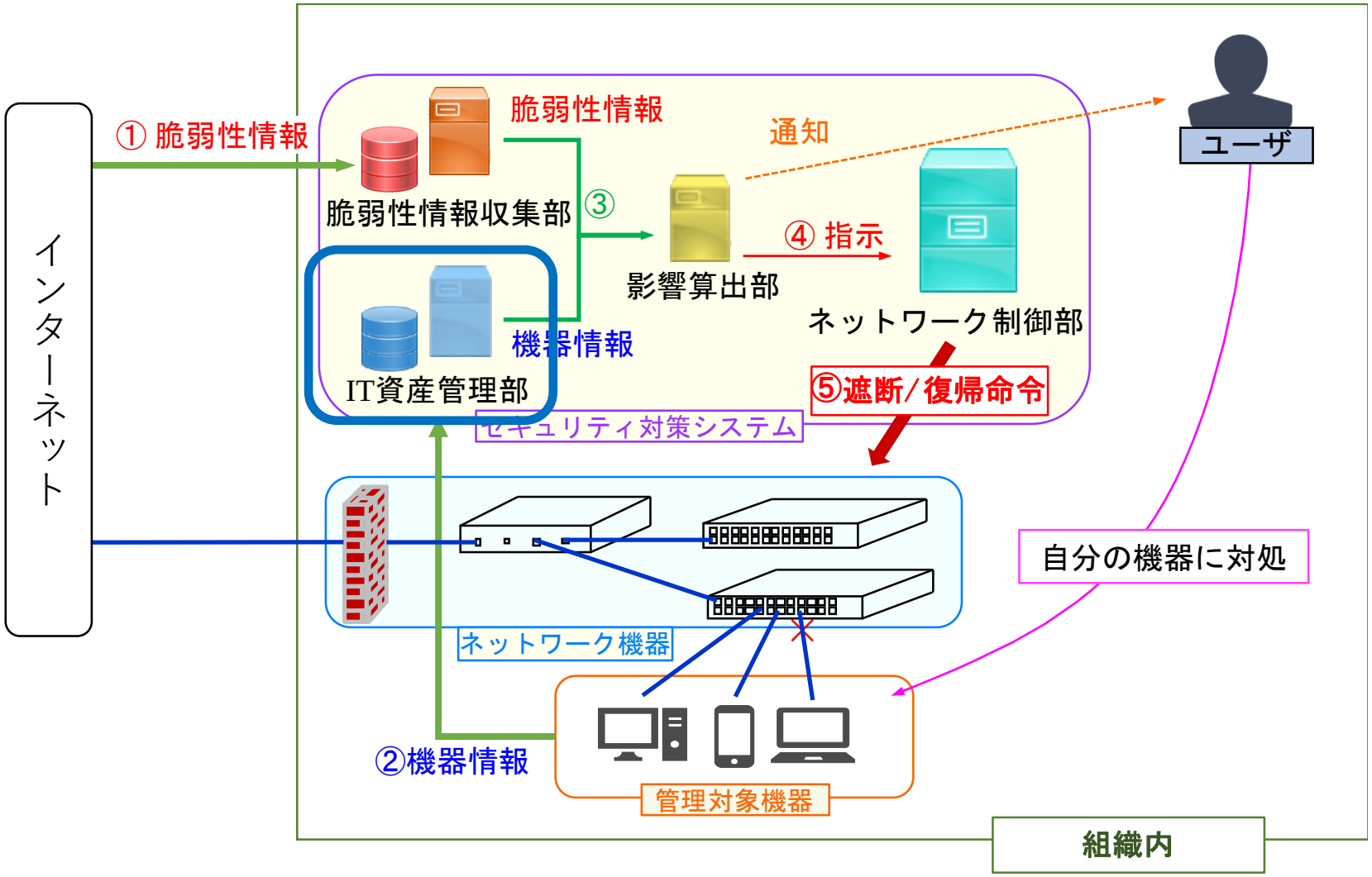


3-2. 脆弱性情報を収集



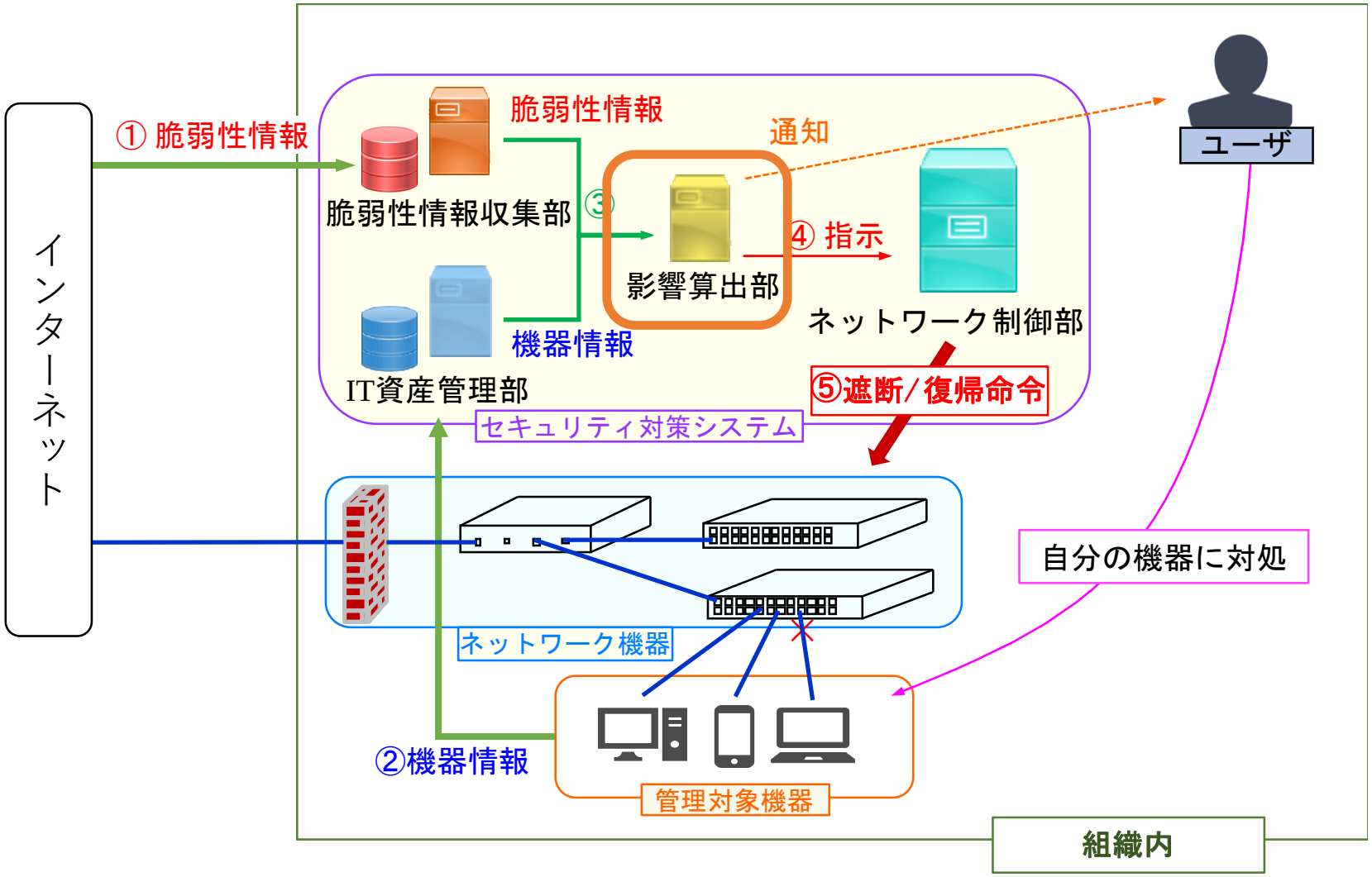
s20g470@stu.kagawa-u.ac.jp

3-3. 組織の機器情報を収集



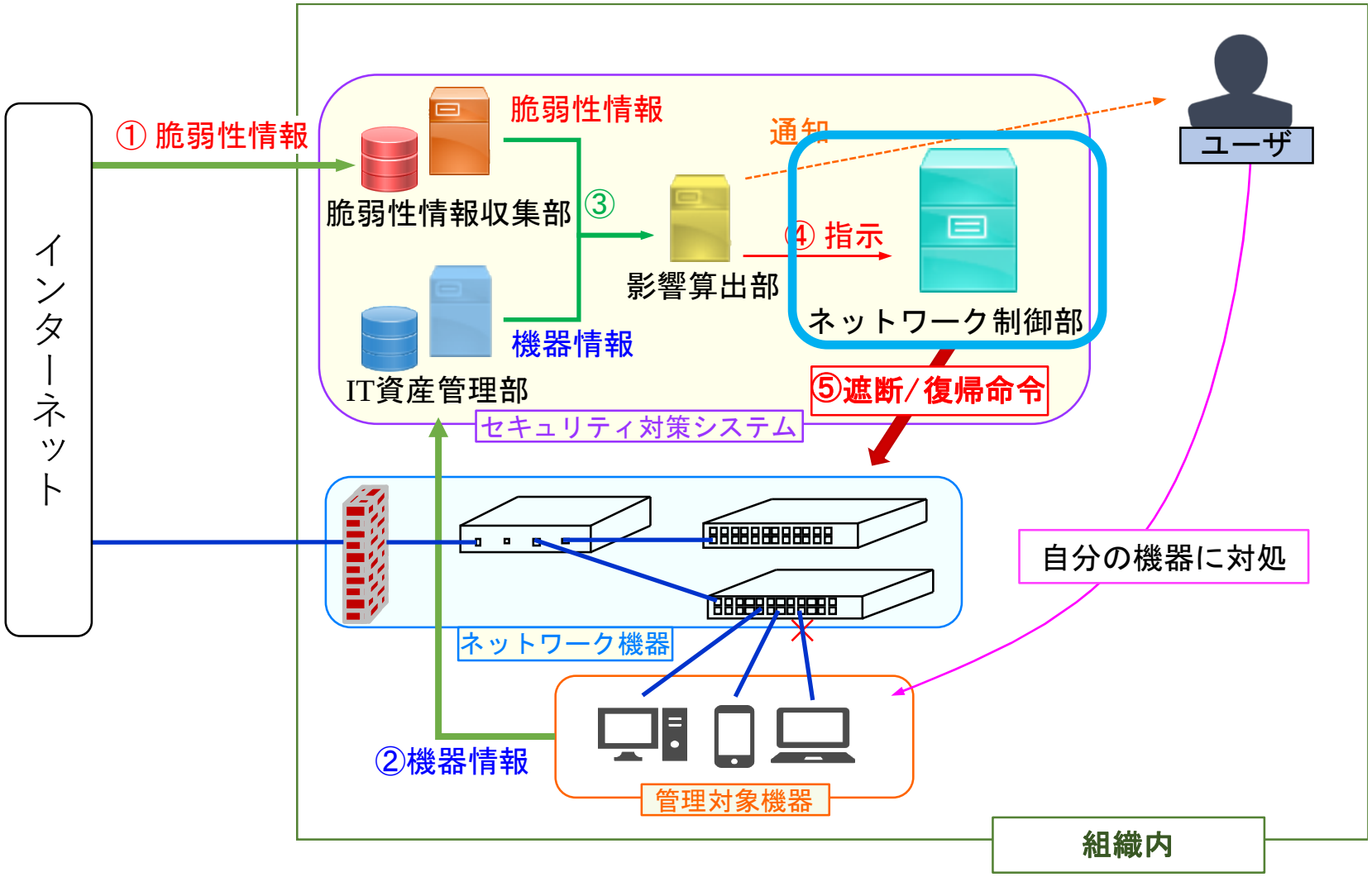
s20g470@stu.kagawa-u.ac.jp

3-4. 組織ネットワークへの影響を算出

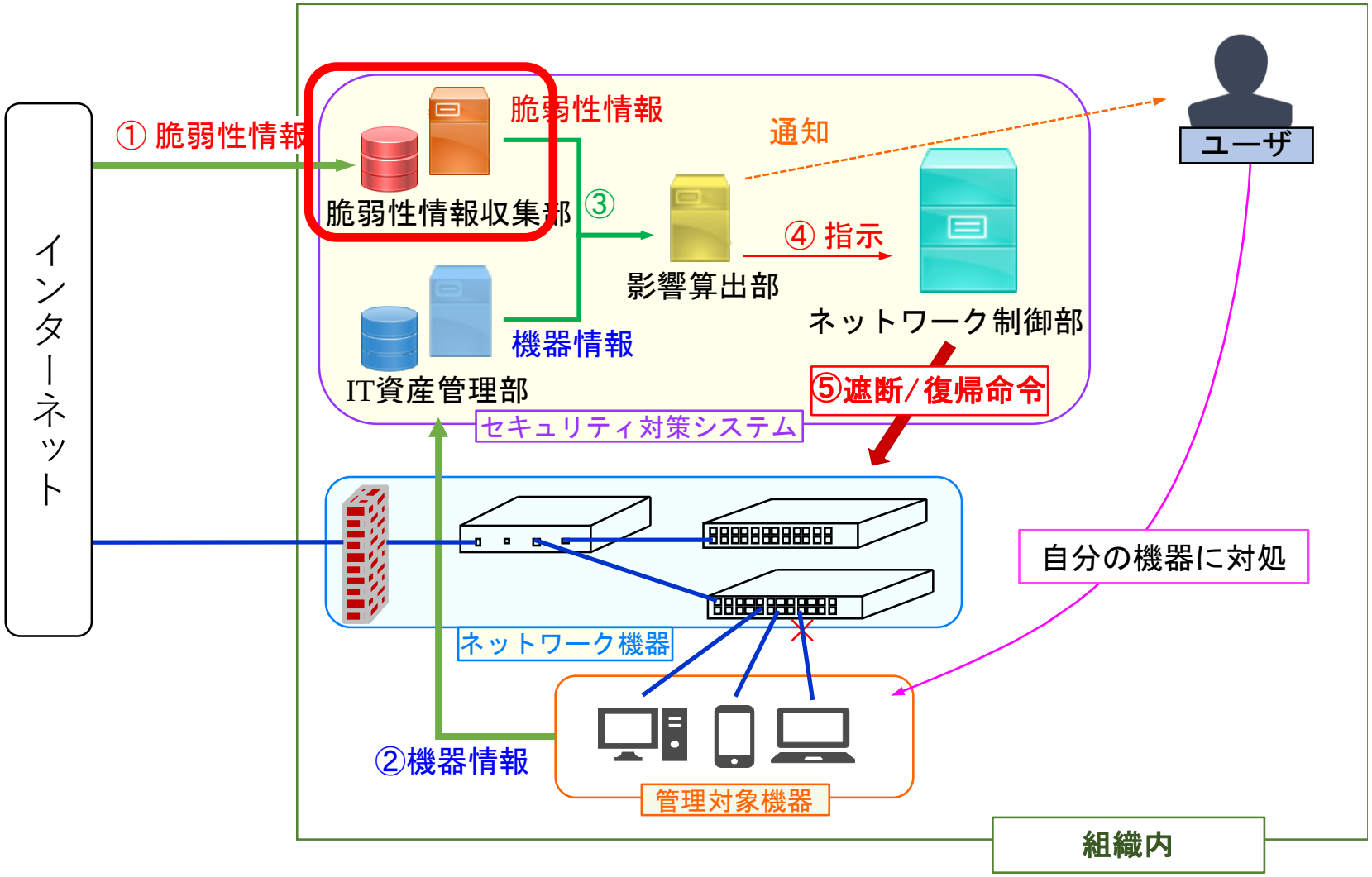


s20g470@stu.kagawa-u.ac.jp

3-5. 結果をもとにネットワークを制御



4-1. 脆弱性情報収集部

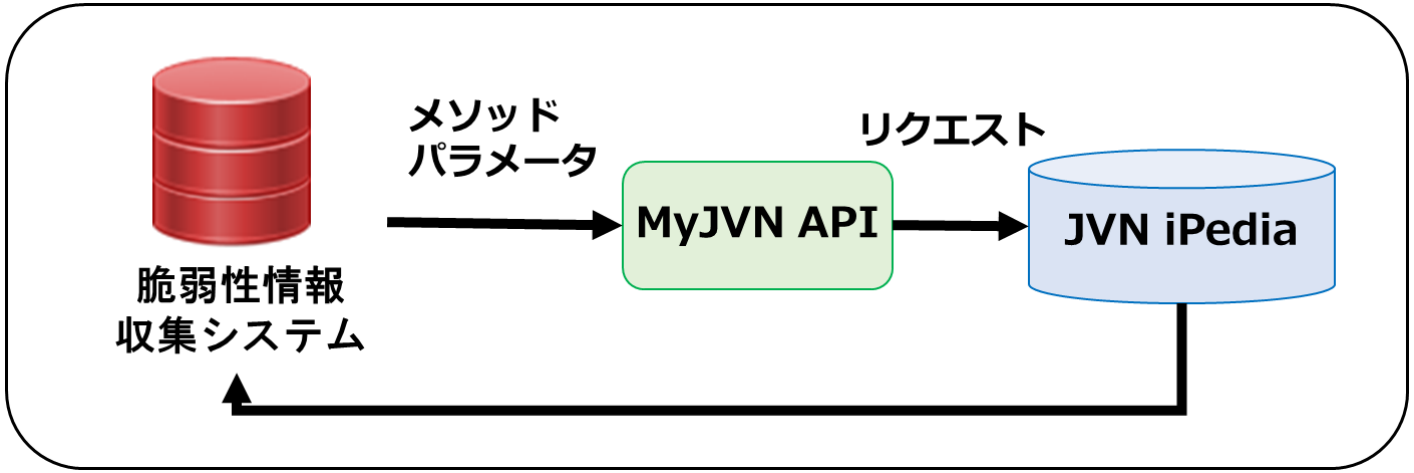


s20g470@stu.kagawa-u.ac.jp

4-2. 脆弱性情報収集部

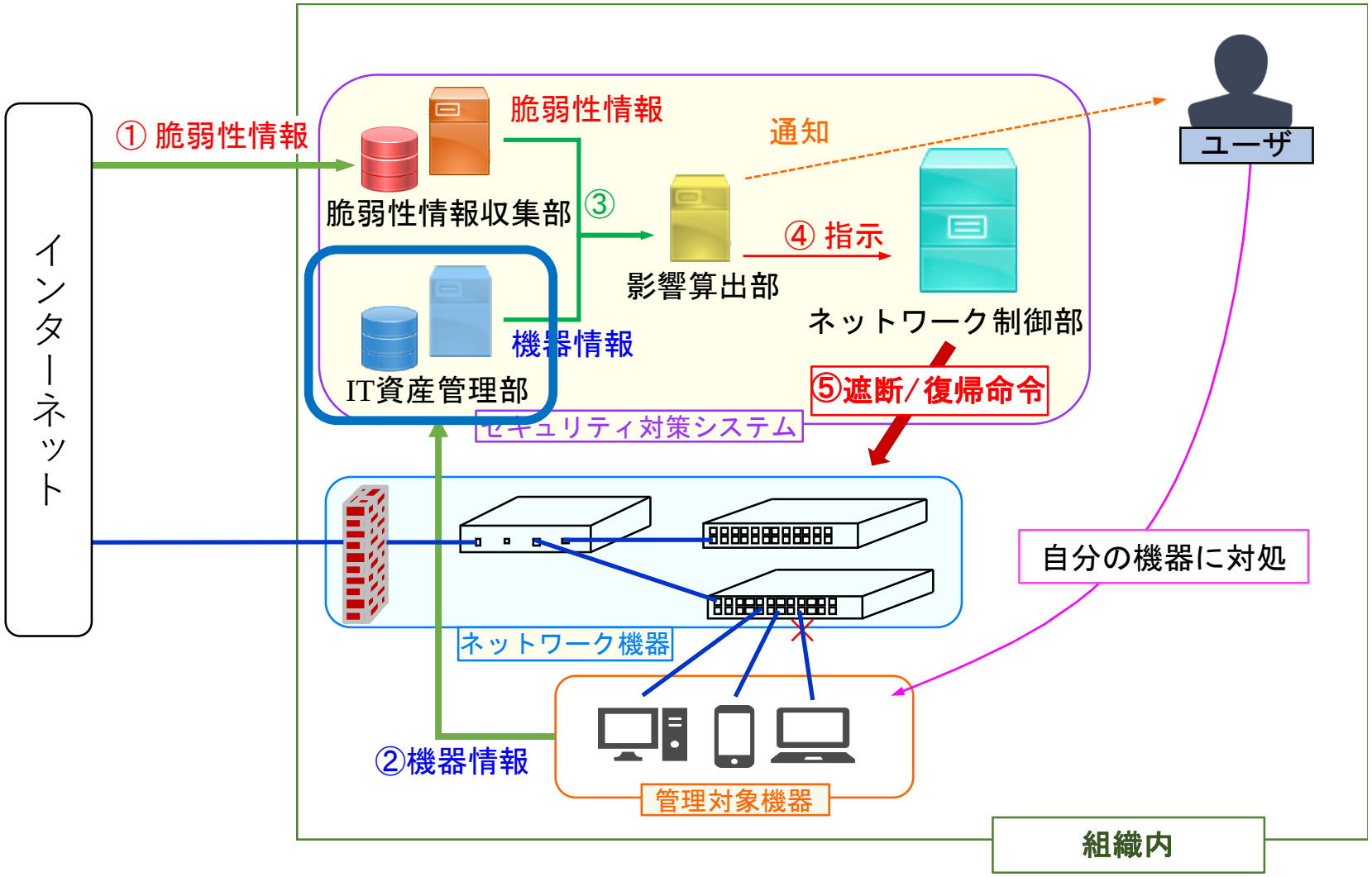
■ 脆弱性情報を利用したゼロデイ攻撃対策システムの考案と DB 構築

- JVN iPediaで公開された脆弱性情報をDBに格納
- 対象製品，ソフトウェア，ベンダ，深刻度
- ベンダのパッチ配布に依存せず，公開後速やかに集約



JVN iPedia - 脆弱性対策情報データベース https://jvndb.jvn.jp/
“脆弱性情報を利用したゼロデイ攻撃対策システムの考案と DB 構築”
楠目幹，本学部電子・情報工学科2018年度卒業論文

5-1. IT資産管理部

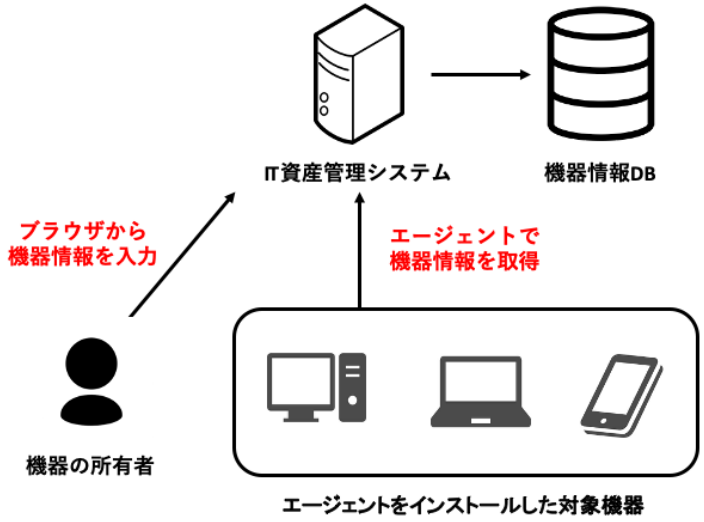


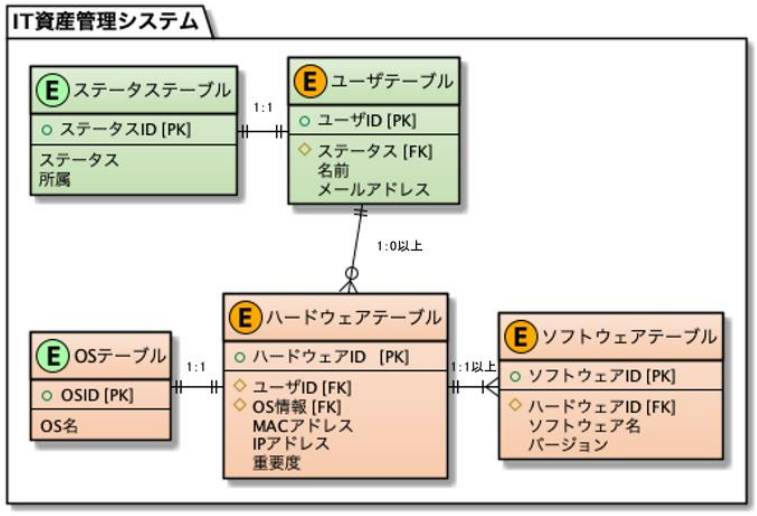
s20g470@stu.kagawa-u.ac.jp

5-2. IT資産管理部

■ BYODに対応したIT資産管理システムの開発

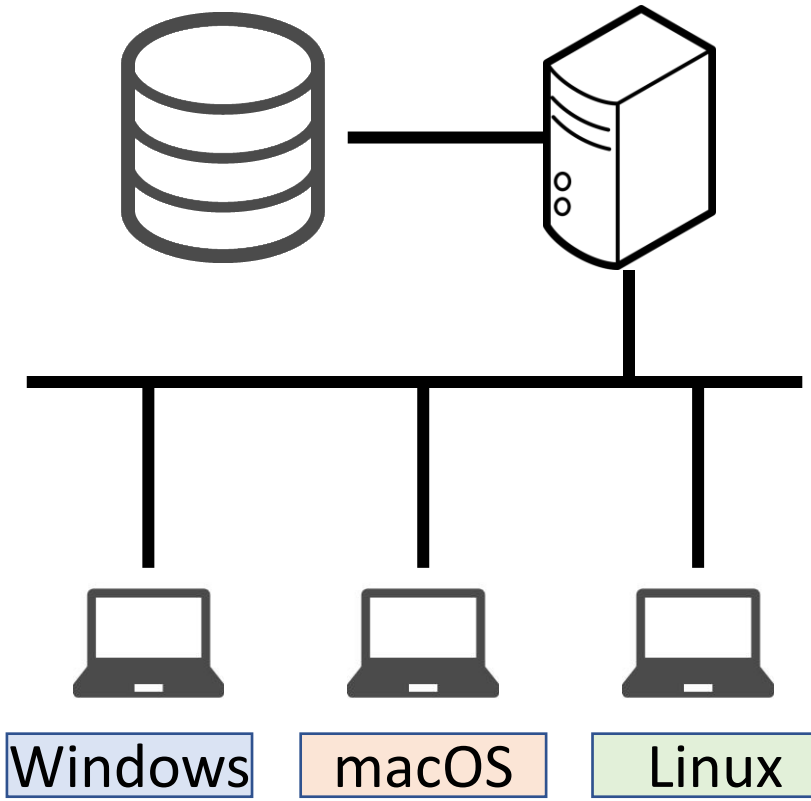
- 持ち込まれた機器をユーザと紐付けし，DBで管理
- 機器の重要度を登録　(重要度:個人情報の保存)
- エージェントの導入を行う
- 未導入の機器は，ネットワーク接続を未許可に





”BYODに対応したIT資産管理システムの開発”
西岡大助，本学部電子・情報工学科2019年度卒業論文

5-3. 情報取得の流れ



① ログイン認証

② ハードウェア情報の取得

③ エージェントのインストール

④ ソフトウェア情報の取得

5-4. 管理する情報

ユーザ情報

- ユーザID
- 氏名
- メールアドレス
- 所属
- ステータス

LDAPと連携
各自入力

ハードウェア情報

- MACアドレス
- 固定IPアドレス
- OS情報
- 重要度

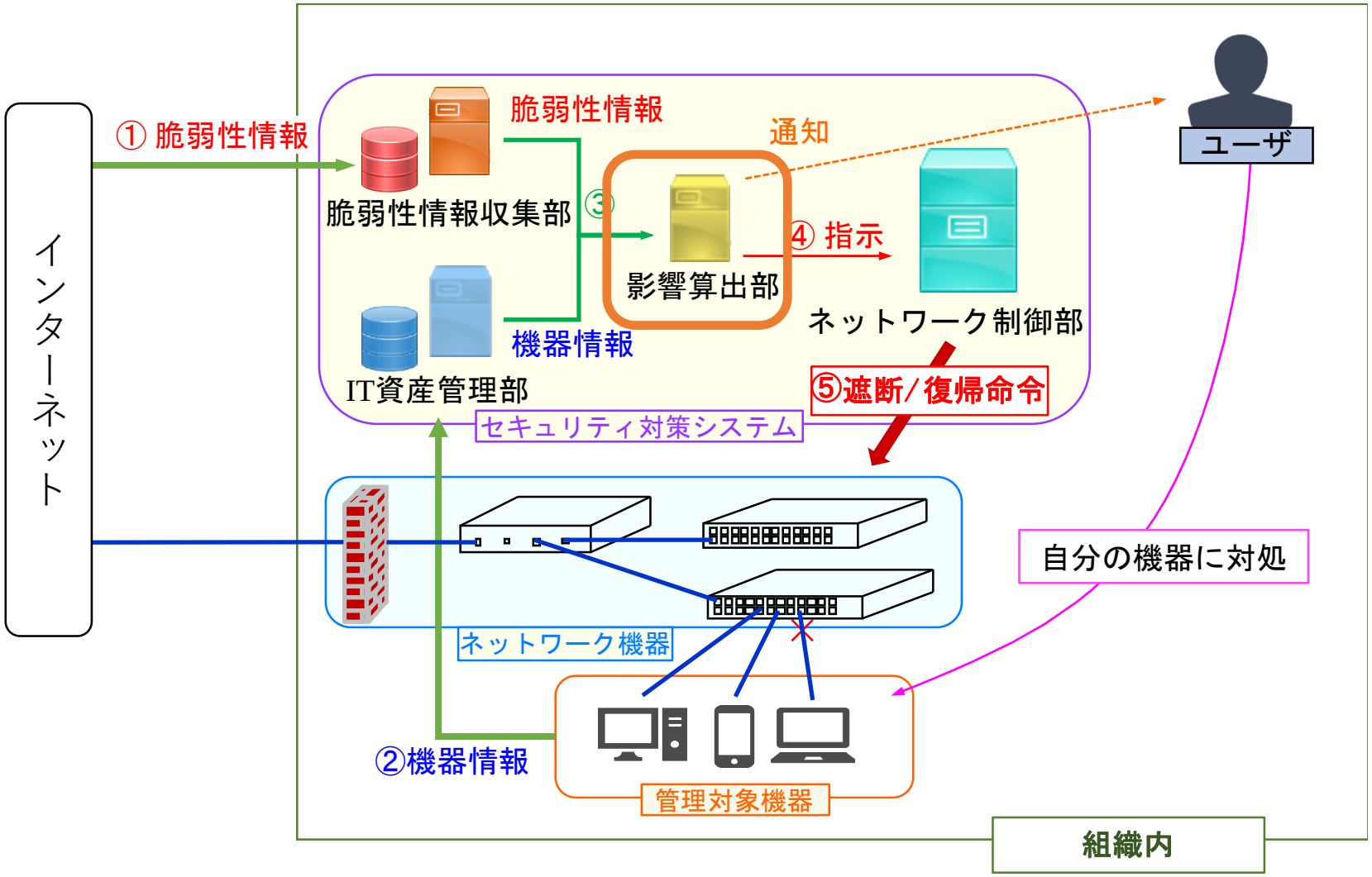
ログイン認証時に
取得

ソフトウェア情報

- ソフトウェア名
- バージョン

エージェントで
各端末から取得

6-1. 影響算出部



s20g470@stu.kagawa-u.ac.jp

6-2. 影響算出部

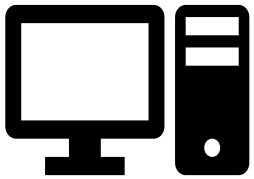
■ 組織にどのような影響がでるのか算出

● パラメータ
- 脆弱性の深刻度
- 情報資産(データ)の重要度
- 機器資産(HardWare)の価値
- 攻撃状況
- 通信実績
- サービス形態(内向，外向)
- 可用性　…etc

● 制御方針
- 管理者に警告
- 外部との接続を遮断
- 検疫ネットワークへ隔離
- アクセス制限

● 判定結果
- 制御方針
- 制御対象 (MACアドレス)

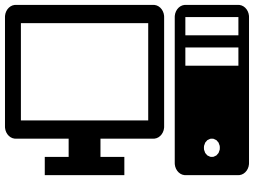
6-3. 緊急度算出の例



- 脆弱性が存在
- 稼働しているサービスや使用するソフトウェアに関係

緊急度は高い

直ちに隔離が必要

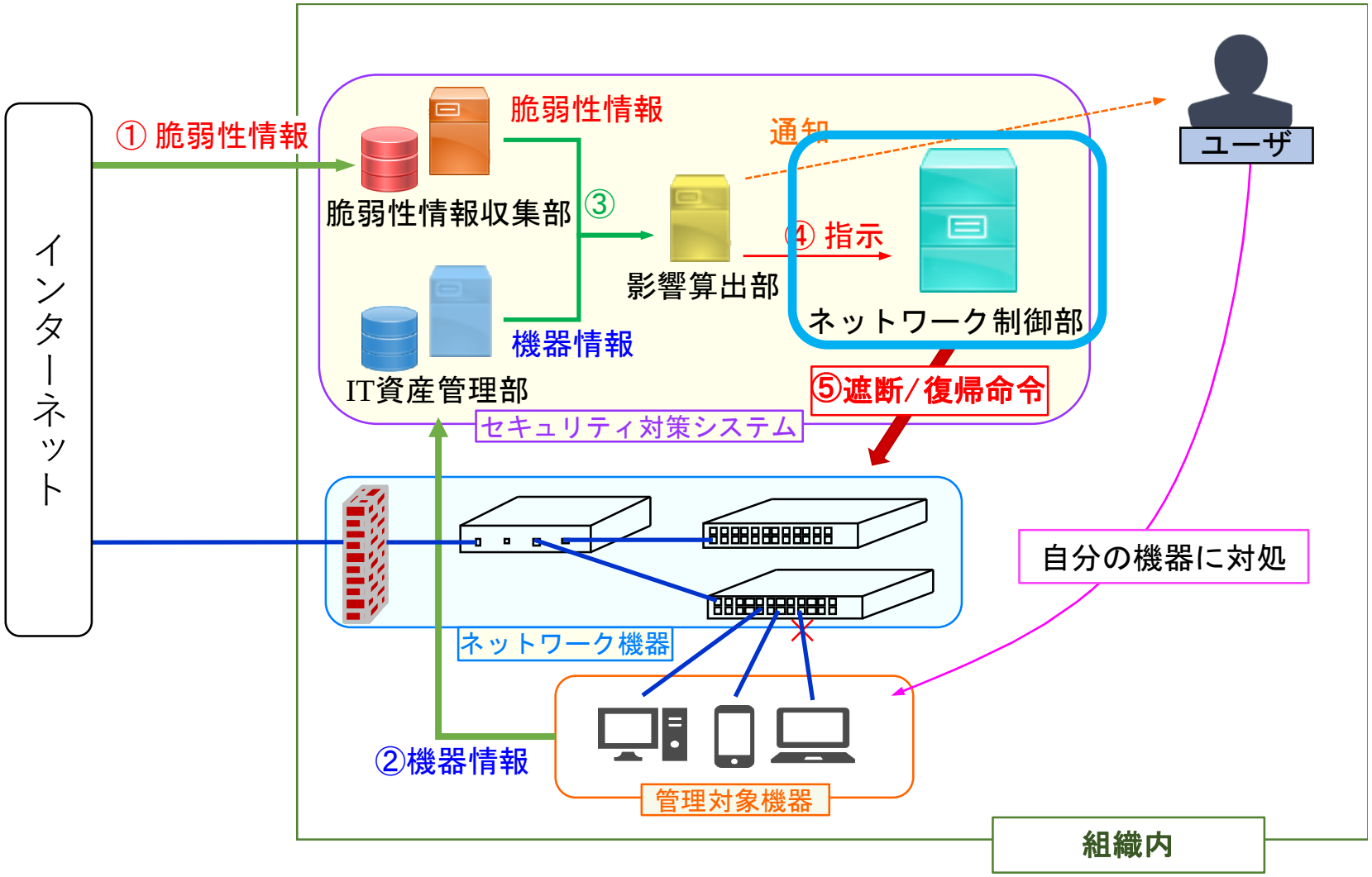


- 脆弱性が存在
- 稼働しているサービスや使用するソフトウェアに無関係

緊急度は低い

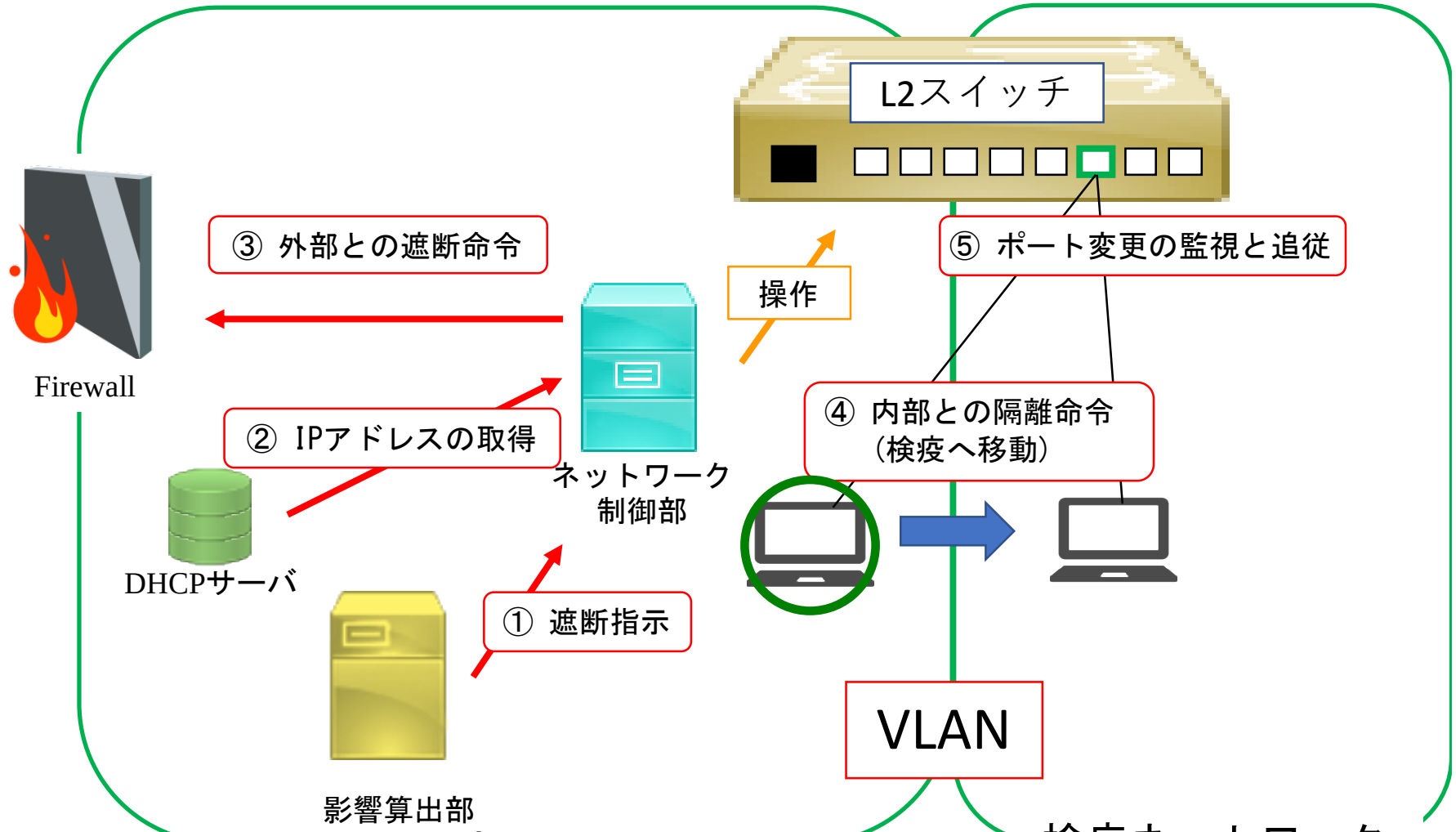
担当者に警告

7-1. ネットワーク制御部



s20g470@stu.kagawa-u.ac.jp

7-2. ネットワーク制御部

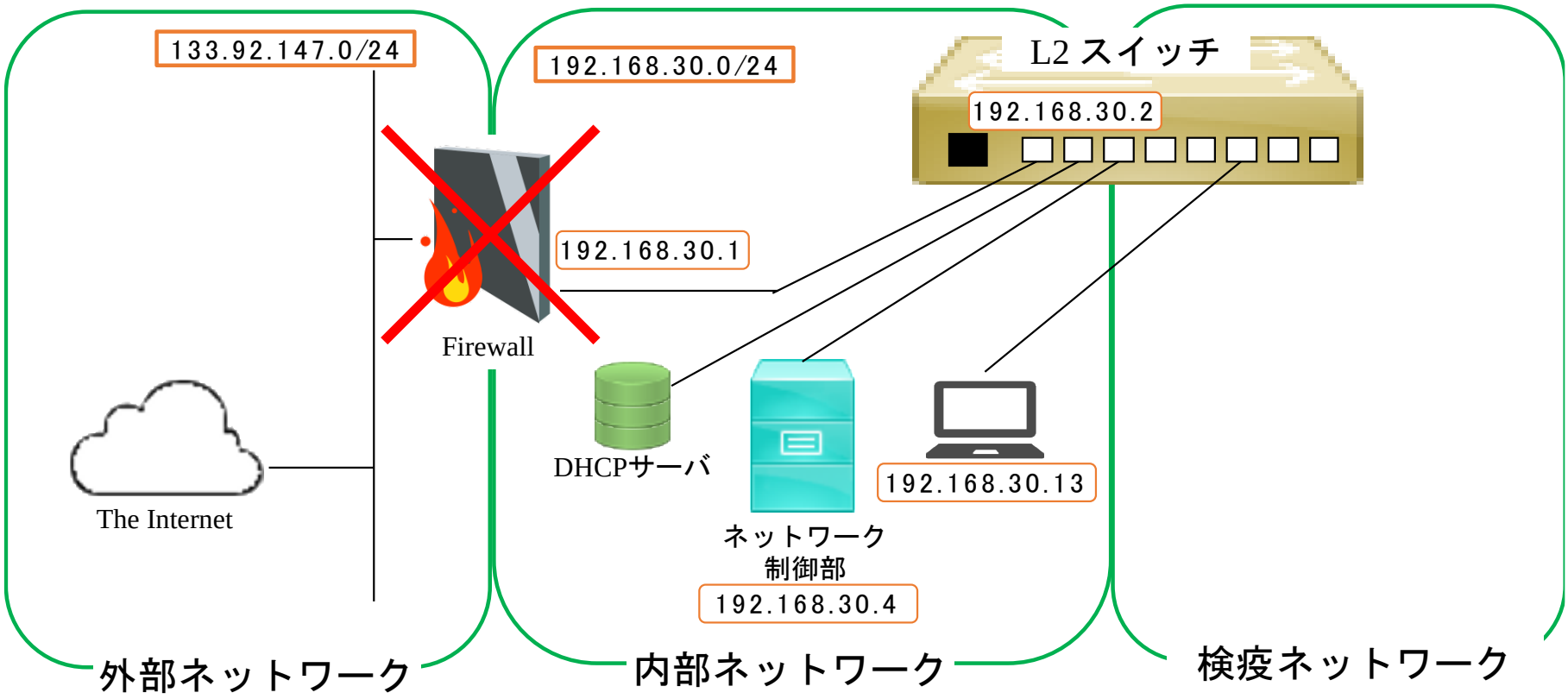


7-3. 機能評価

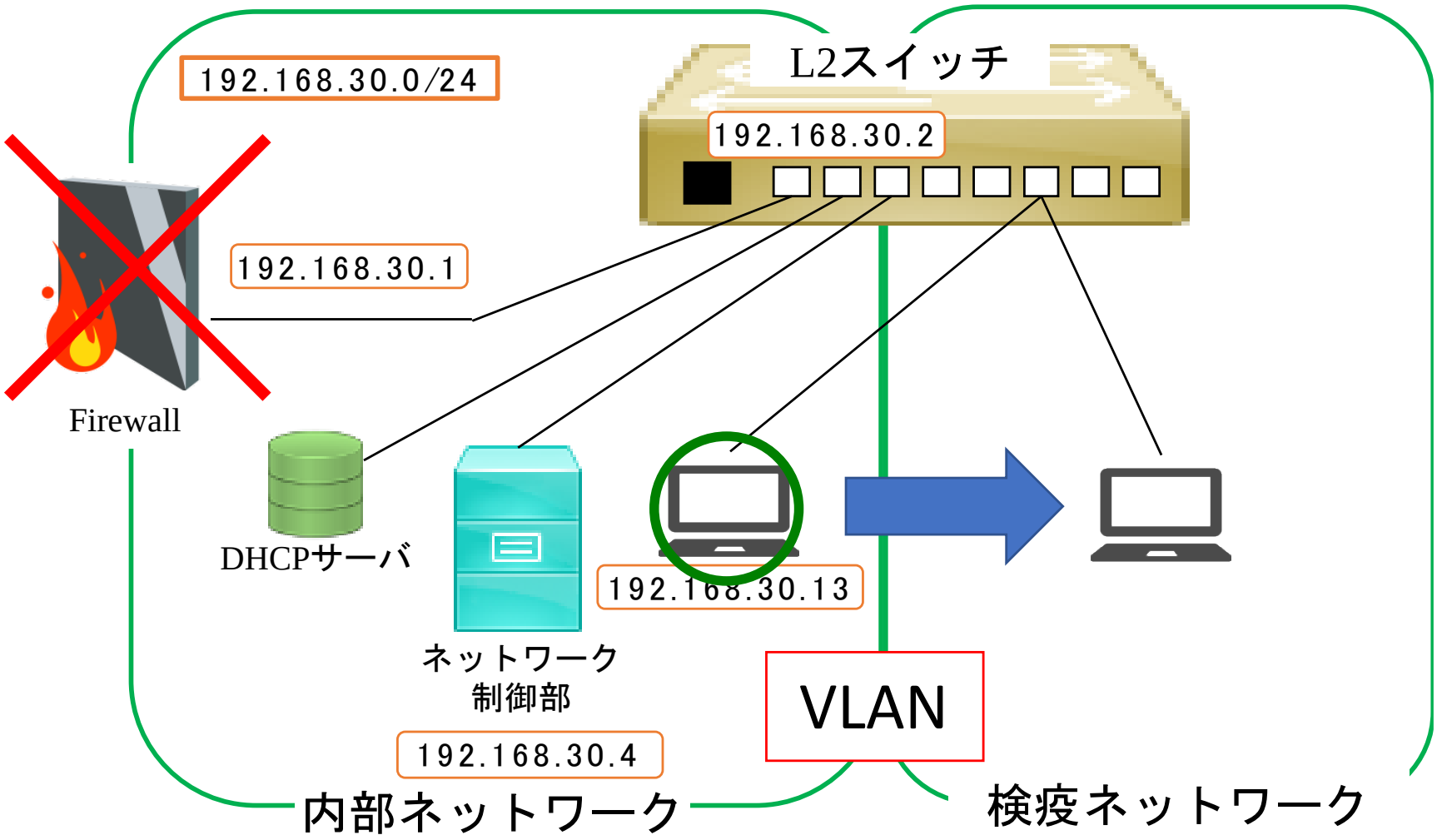
- 実装機能の動作を評価
  - 影響算出部による該当機器を想定
  - 外部ネットワークからの遮断と復帰
  - 内部ネットワークからの隔離と復帰
  - L2スイッチへの接続しているポート変更の監視と追従

- ”ping” (ICMPパケット) の通信中の遮断を確認
  - 20回送る途中に遮断する
  - 外部ネットワークとの通信
  - 内部ネットワークとの通信

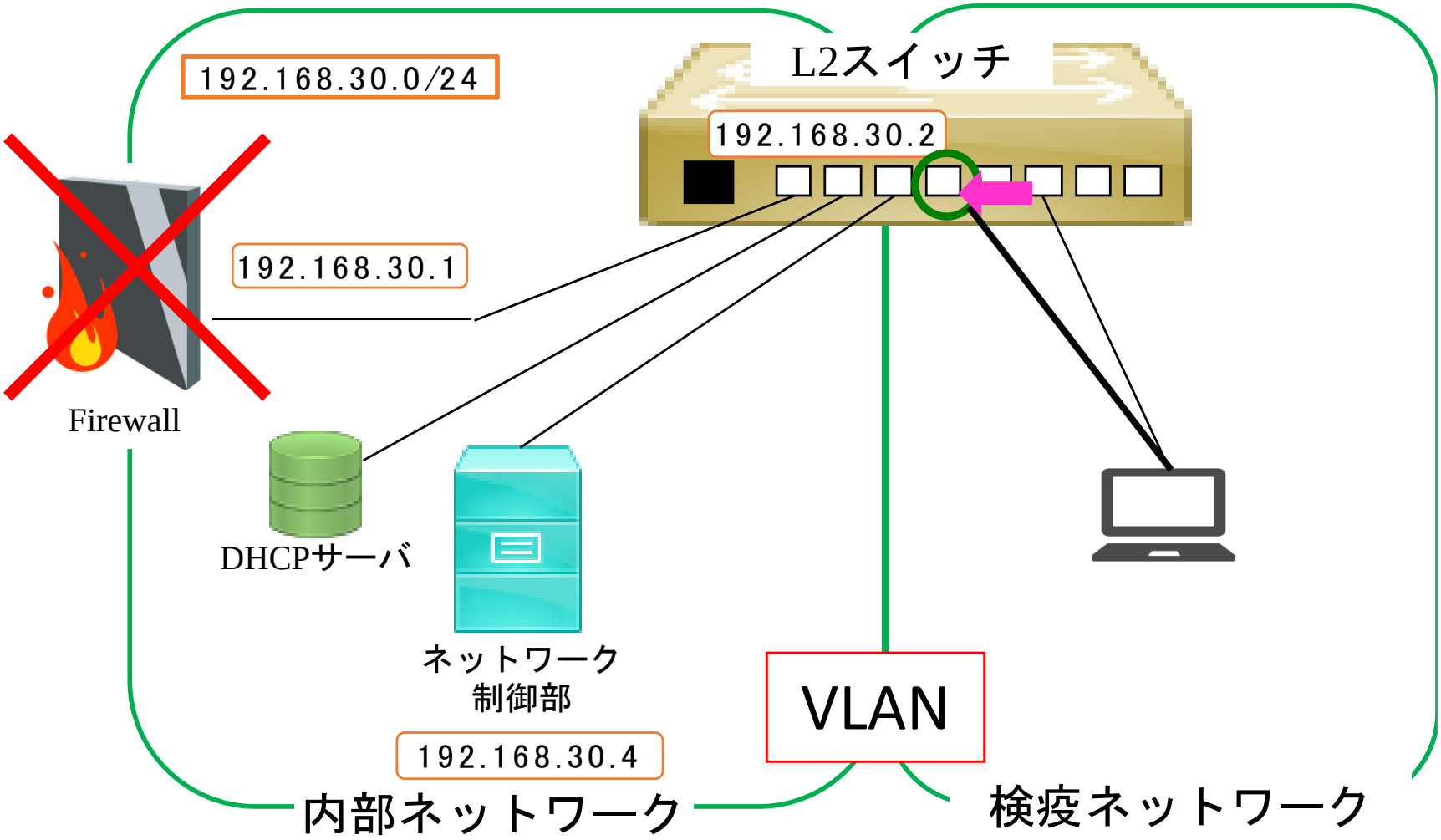
7-4. 外部ネットワークからの遮断



7-5. 内部ネットワークからの隔離



7-6. 接続ポートの監視と追従



8. おわりに

■ まとめ

- 組織に存在する情報資産を守る
- 大学や病院など小さな組織を対象とする
- 組織のネットワークに対する影響を算出する
- 脆弱性情報と機器情報を用いてネットワーク制御を行うゼロデイ攻撃対策セキュリティシステム

■ 問題点と課題

- 影響算出部の開発
- 無線LAN環境や異なる機種への対応
- エージェントの機能拡張
- 機器の重要度の算出方法について検討

9-1. 他学校の導入システム

KWIINS

- 2000年度より京都女子大学にて導入
- 学内ネットワーク接続へのユーザ認証
- 一定時間の無通信時の再認証
- ウイルス等への振る舞い検知と隔離機構
- ⇒　不正な活動の検知や隔離
- ⇒　これらの対策とした通信制限を不要に
- (※ セグメントを超えたICMPの禁止など)
- 未知のウイルスにおいても検知が可能

- 我々のシステムとの併用でセキュリティ向上を期待

宮下健輔. “学内ネットワークの安全性向上を目指したアクセス制御と脅威検知の導入”. 情報処理学会インターネットと運用技術シンポジウム 2008, pp. 73–79, 2008.

9-2. 他社製品

■ SKYSEA Client View

- 機器の一元管理を行う
- ベンダーが配布したパッチのキャッシュを行う
- パッチ配布前には対策しない

SKYSEA Client View Ver.14 | SKYSEA Client View | Ｓｋｙ株式会社
https://www.skyseaclientview.net/ver14/#tabs-2

■ IoT向け脆弱性情報管理サービス

- 脆弱性情報に対して，通知を行う
- 通知まで，数日を要する
- ネットワーク制御までは行わない

ActSecure IoT向け脆弱性情報管理サービス | NEC
https://jpn.nec.com/act/acts_iotvms.html#servicemenu