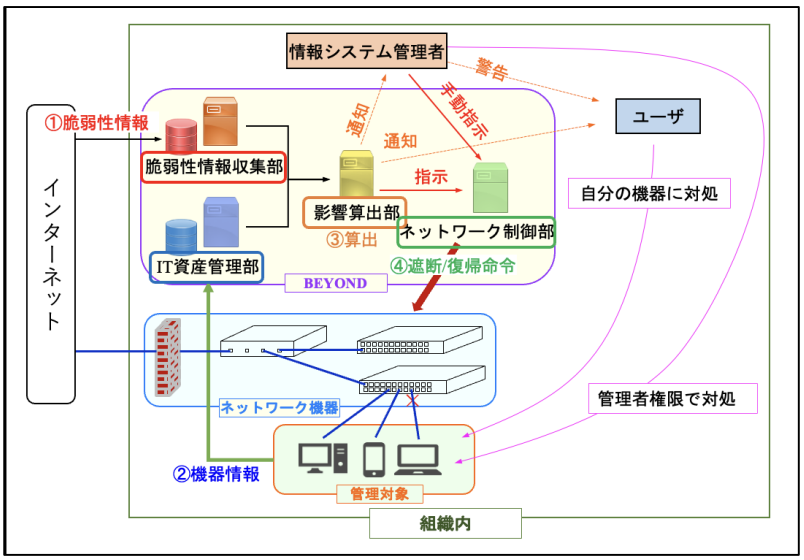
BEYOND:セキュリティ対策システム



背景

- 脆弱性を利用した攻撃は標的型攻撃と組み合わせると甚大な被害が出る
- 大学等で，個人の端末を組織のネットワークに接続して業務に使用するBYODが増加

課題

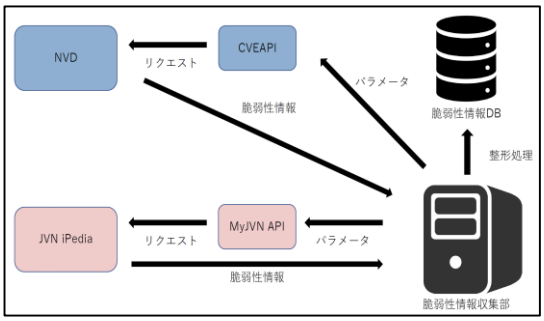
- BYODに脆弱性が存在する場合，その機器を介して組織の情報資産の漏洩が起きる

目的

- 脆弱性情報と機器情報を用いて脆弱性を検知し，アクセス制御を行うことで組織の情報資産を保護

脆弱性情報収集部

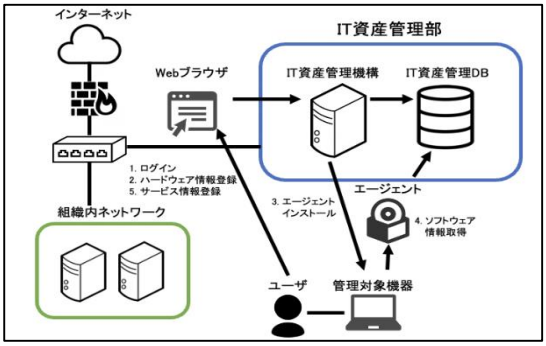
- インターネット上から脆弱性情報を収集
- 脆弱性の深刻度，脆弱性をもつ製品，対策方法
- 収集してきた情報は整形処理をすることで扱いやすく



創発科学研究科創発科学専攻 中村友昭

IT資産管理部

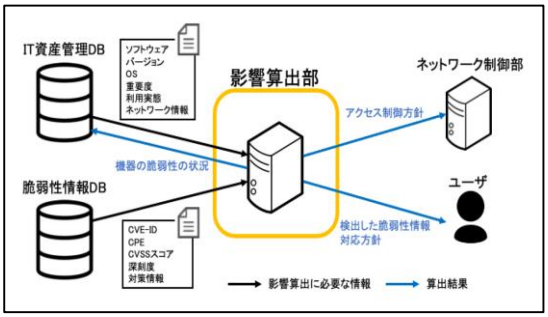
- Webブラウザとエージェントを用いて機器情報を収集
- エージェントを用いることでBYODにも対応
- APIを用いてアクセス権限を割り振る



工学研究科 信頼性情報システム専攻 西岡大助

影響算出部

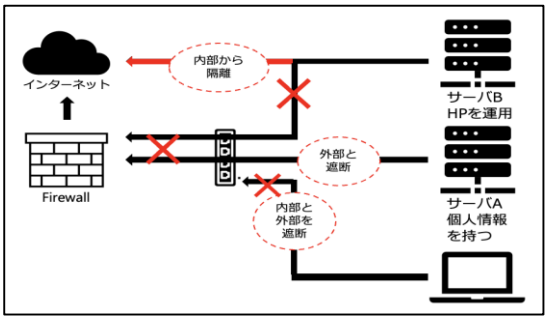
- 脆弱性情報収集部のDBとIT資産管理部のDBから機器に存在する脆弱性を検出する
- 脆弱性の内容，サービス情報などから制御方針を算出し，ネットワーク制御部とユーザに通知



電子･情報工学科 細川洋輔

ネットワーク制御部

- 影響算出部から通知された内容に従ってアクセス制御
- 機器が接続しているネットワーク機器を操作
- 接続しているネットワーク機器の移動にも対応



工学研究科 信頼性情報システム専攻 竹原一駿