標的型攻撃の
侵入拡大経路推定に関する研究

名古屋大学　情報基盤センター
山口　由紀子

サイバーセキュリティの現状

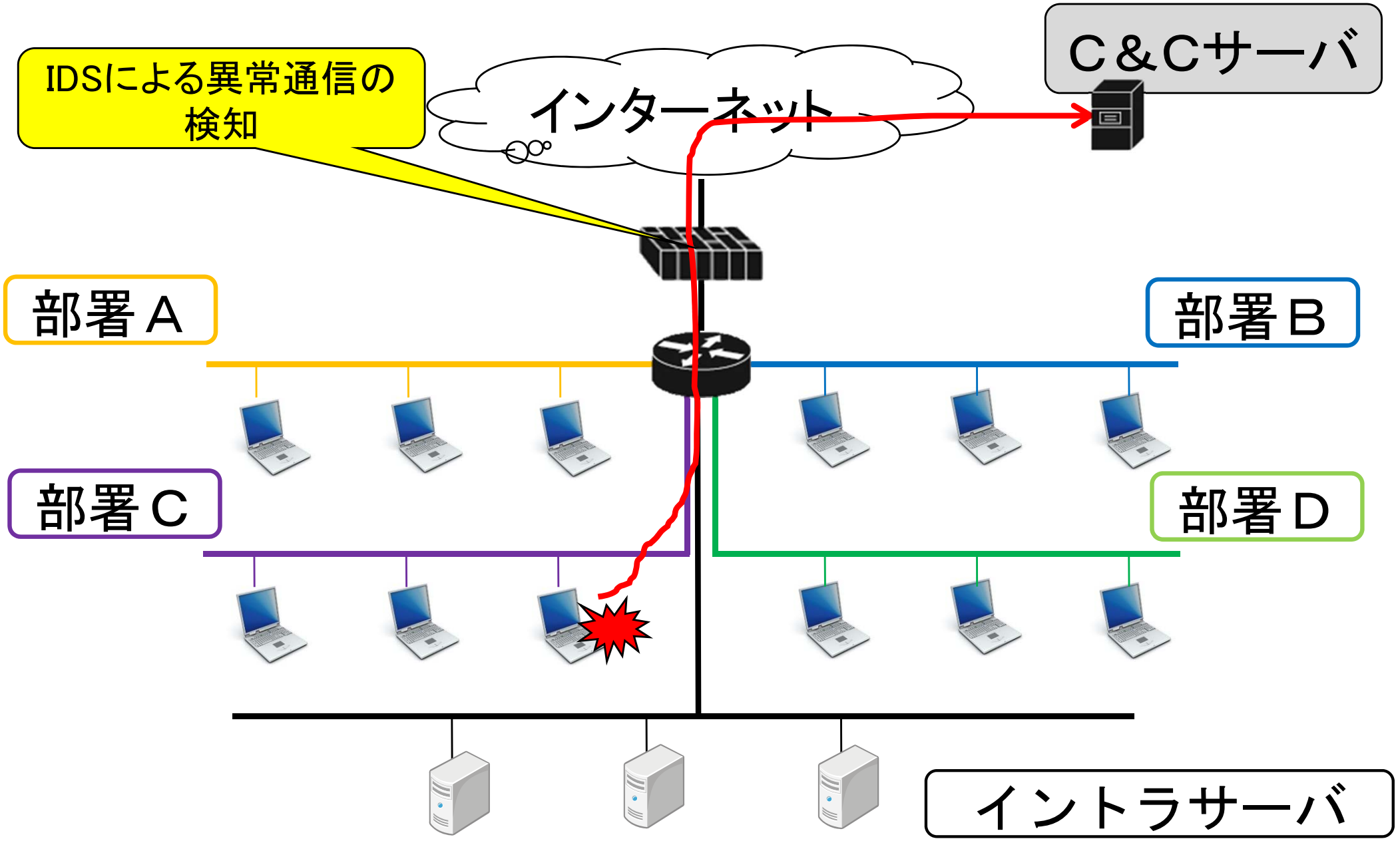
- サイバー攻撃の増加、巧妙化
  - フィッシングメール
  - 水飲み場攻撃

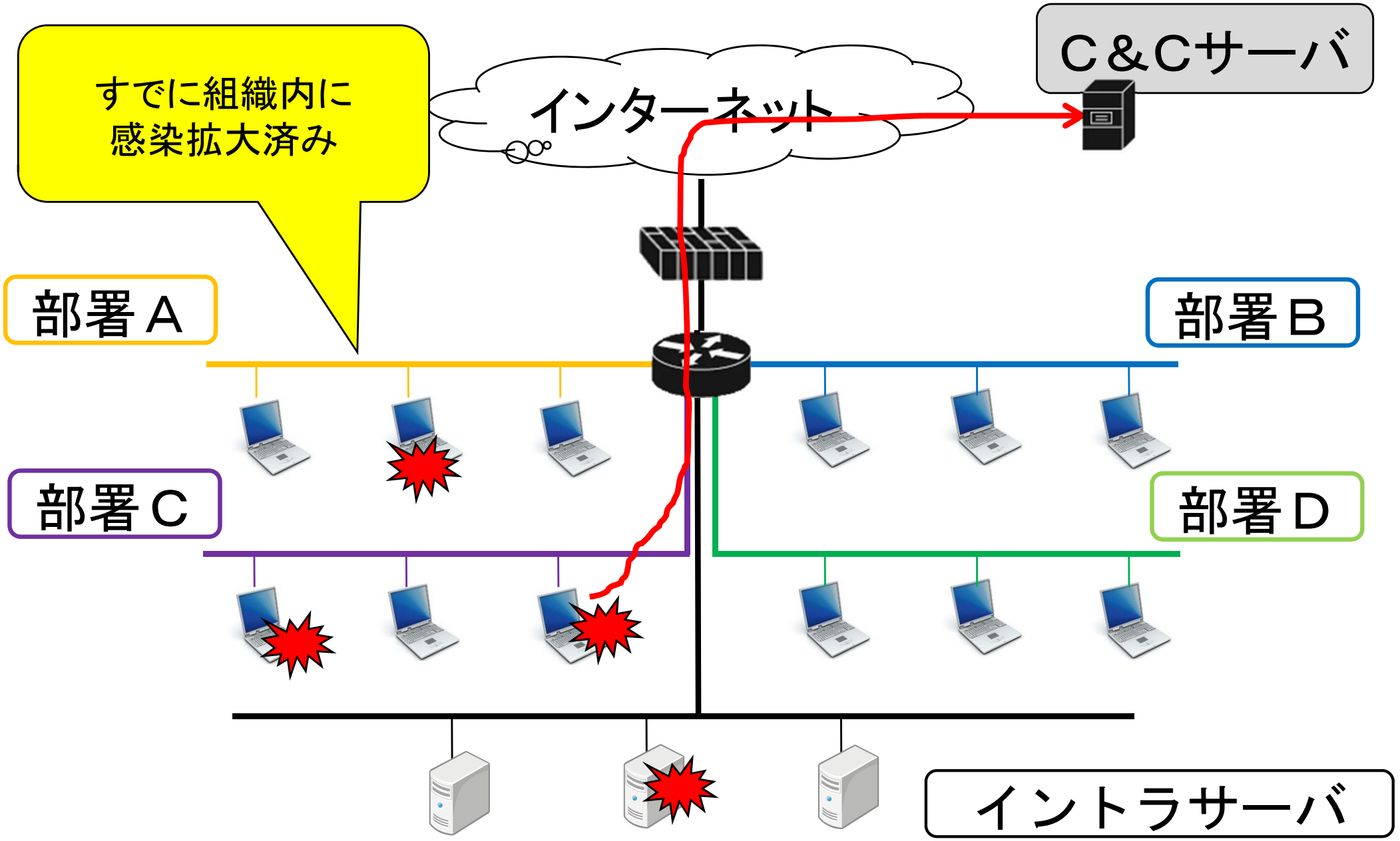
- 代表的な脅威：標的型攻撃
  - 特定の組織への明確な目的のもとに行われる攻撃
  - 入念な事前調査と計画立案
  - 組織に合わせて攻撃手法をカスタマイズ

標的型攻撃の手順*

手順１　計画立案: 攻撃目標選定、偵察
手順２　攻撃準備: 攻撃用サーバ準備（C＆C）
手順３　初期潜入: 標的型メールの送付
手順４　攻撃基盤構築:
　　コネクトバック開設、端末情報入手、
　　ネットワーク構成把握
手順５　内部調査侵入:
　　サーバ不正ログイン、管理サーバ乗っ取り、
　　他端末へ攻撃範囲拡大
手順６　目的遂行: 情報窃取、情報破壊

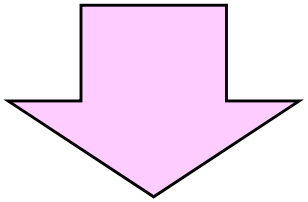
*)「高度標的型攻撃対策に向けたシステム設計ガイド」 https://www.ipa.go.jp/files/000052614.pdf.


IDSによる異常通信の検知
インターネット
C&Cサーバ
部署A
部署B
部署C
部署D
イントラサーバ


すでに組織内に
感染拡大済み
インターネット
C&Cサーバ
部署A
部署B
部署C
部署D
イントラサーバ

侵入発覚後の対策

- 感染検知した端末の隔離と調査だけでは不十分
- すべての感染疑い端末の検査が必要



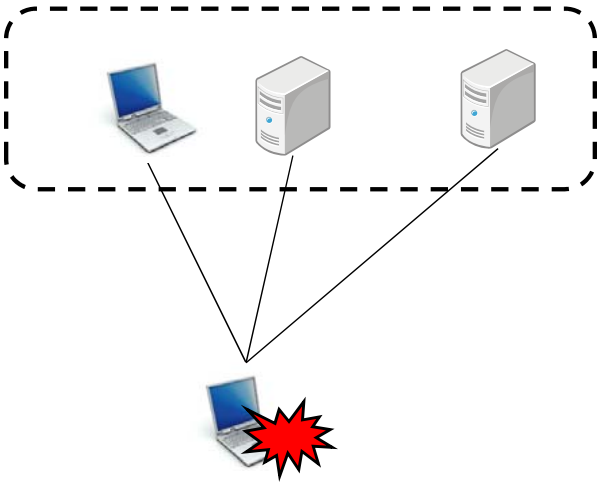
本研究の目的

侵入発覚後の感染経路を推定
調査対象の感染疑い端末を削減
ネットワーク管理者の負担軽減

アプローチ

再帰的に感染経路を探索

端末Aを宛先とする通信を行った端末群

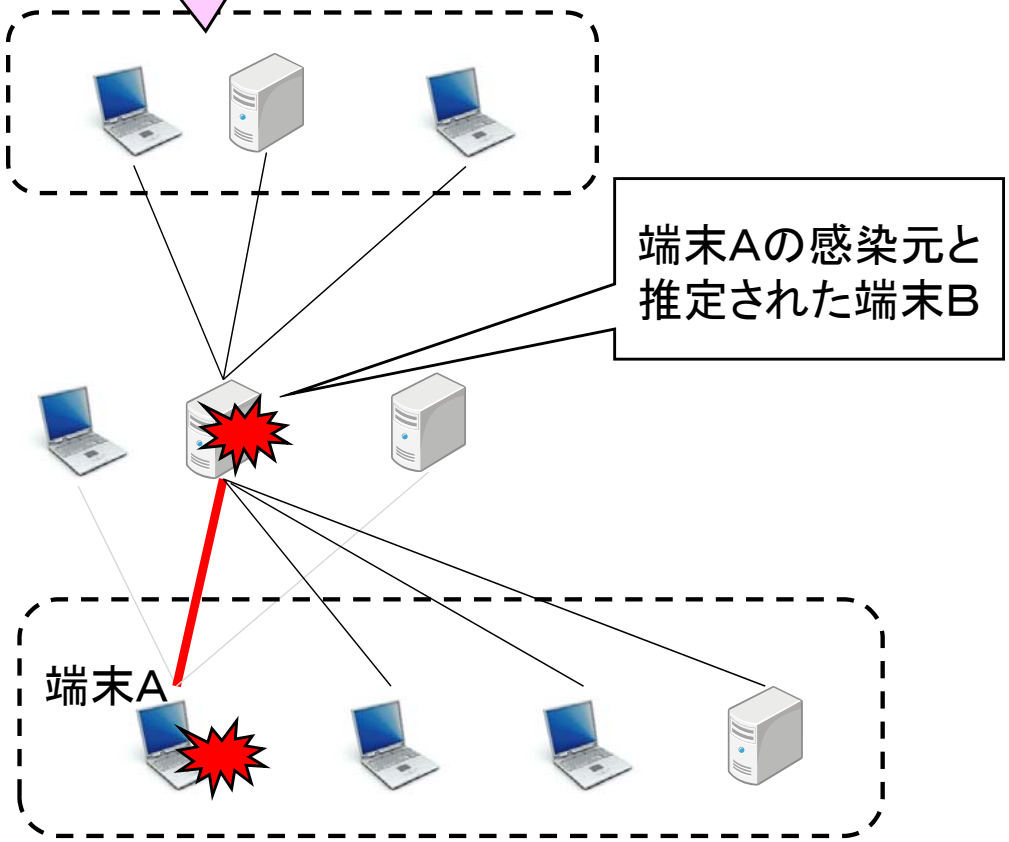


第1発見感染端末A

手順1　感染元推定

時間経過

端末Bを宛先とする通信を行った端末群



端末Bを発信元とする通信を行った端末群

手順2　感染経路推定

機械学習による異常通信の検知

- 検知手法：教師なし機械学習による分類器の生成
  - DBSCAN
- 学習用データ（正常データ）
  - イントラネットの日常的な通信
  - インターネットとの通信に比べて大量
    ⇨パケットデータではなくフローデータを利用
- 検知用データ
  - 分類器への入力期間の調整