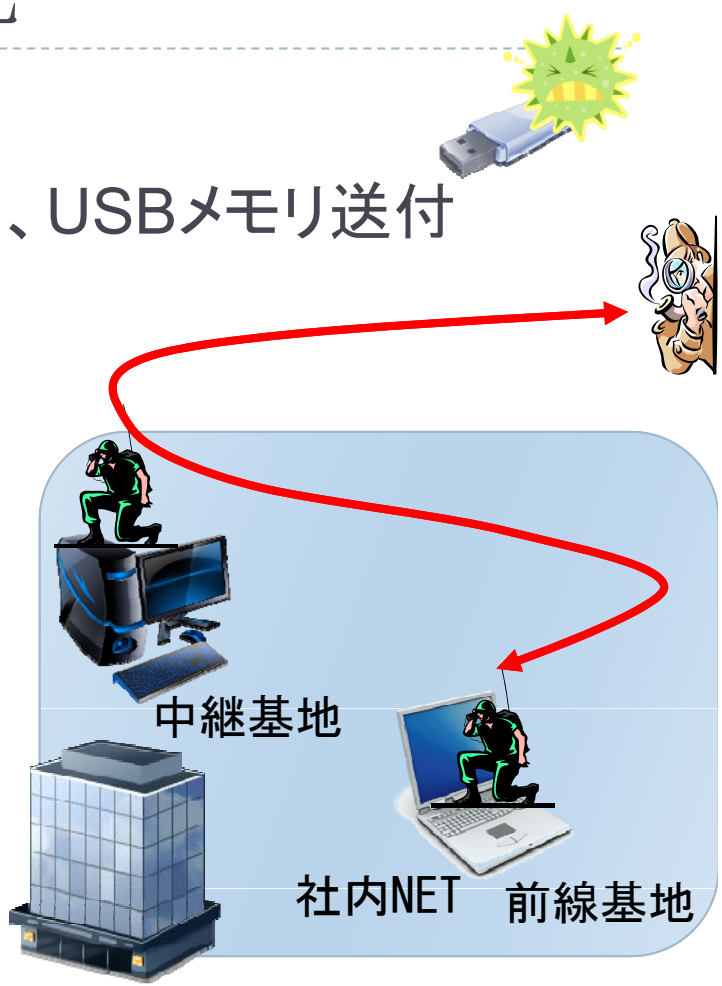
巧妙化するサーバ攻撃に備えた ネットワーク運用

高倉弘喜
名古屋大学

標的型攻撃の巧妙化と長期化

- 社内NWに侵入
  - メール添付ファイル、Webサイト誘導、USBメモリ送付
- 前線基地となる感染PC
  - 偵察活動
    - NW構成の調査
    - サーバ情報の調査
      - ✓ IPアドレス、重要情報の有無
    - メール
      - ✓ 通信宛先、メール本文、添付ファイル
  - 浸食活動
    - 社内での標的型メール送信
- ミッション完了後、中継基地化



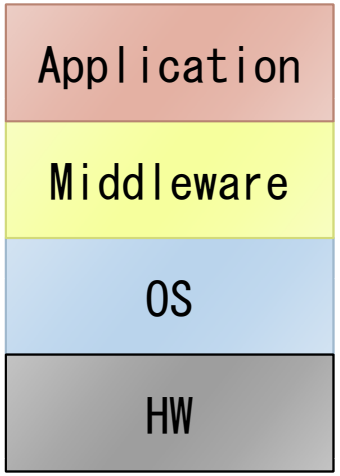
年単位の活動も

従来対策の限界

- セキュリティ対策は調査済み
  - マルウェアはAnti-virus未検知
  - 攻撃はIDS未検知 or 誤検知
    - 対策済みのはずのシグネチャが反応
    - アノマリ検知の可能性はあるが…
- 隔離NWも攻撃対象
  - 情報の運搬媒体を活用
    - USBメモリ
- 全ての情報システム・資産を守ることは困難
  - 情報セキュリティ対策にもROI
    - 狙われやすい所、狙われやすい所を重点的に防護

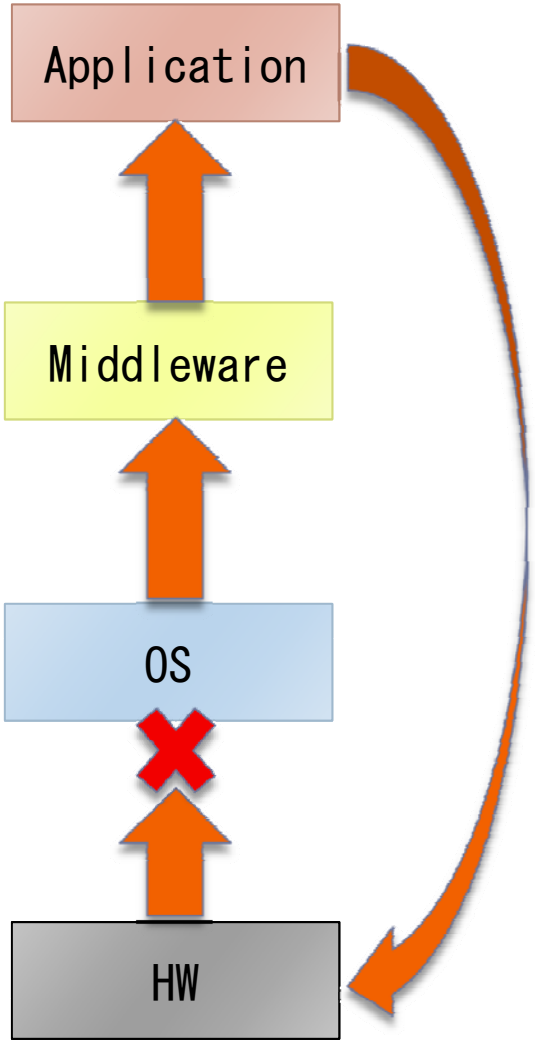
狙われる認証系

- 全ての社内マシンからアクセス可能
  - 全社員の認証情報
    - 各社員の使用PC＆アクセス権限
    - システム管理者、ネットワーク管理者の情報も
- 認証系のパッチ適用
  - ミドルウェア/アプリケーション
    - DBMS
    - 処理言語(java, perl, python, ruby, php…)
    - サーバ(Web、メール, …)
    - CMS
  - 重要になればなる程、OS更新に即応できず
    - 運用開始後、一度も更新されないOS, Middleware, Application



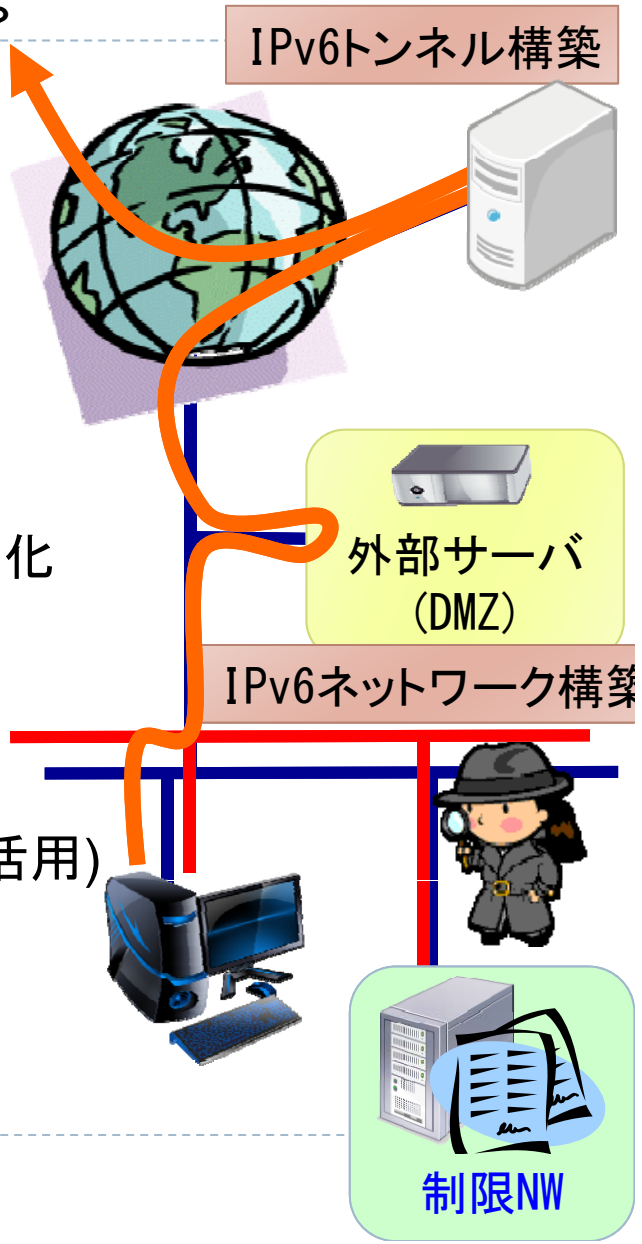
更新の無限ループ

- OS更新
  - Middleware, Applicationの更新
  - 各種設定の微修正
- ハードウェアのスペック不足
  - 新型機への更新
  - 現行機OS非対応
- 最新OS導入
  - ミドルウェア、アプリケーションの大幅改修
- 認証系の稼働期待期間：10年以上
  - 長期利用で生じる負荷増の見積ミス
  - 運用開始後、1度も更新されず…



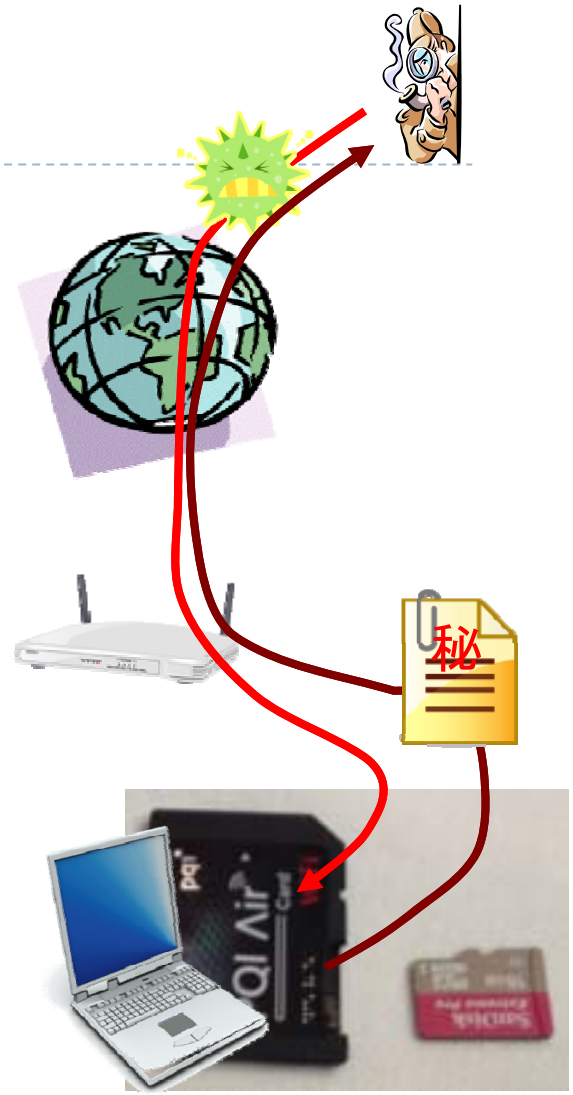
意表を突く攻撃

- 一般的な監視体制
  - 入口対策
    - Firewall, IDS, anti-virus
  - 出口対策
    - RAT/bot通信検知…コンプライアンス系
    - NAT/proxy…送信情報監視
      - ✓ HTTPS：一旦平文に戻す→検査→再暗号化
    - 多くの組織でIPv4のみ利用している…つもり
      - ✓ IPv4限定な監視体制
- 監視ポイント回避
  - 別経路NW構築 by NW管理者(認証情報の活用)
    - ✓ IPv6網を無断構築
    - ✓ 各種トンネリング：6to4, Teredo, 6rd



可搬メモリまで…CPU内蔵

- 元々はデジカメ用
  - CPU: ARM 200MHz程度
  - 主記憶：数十MB
  - 二次記憶: 数百MB
  - Wi-Fi搭載
    - ARM Linux
- 組込み機器+メモリ
  - 十数年前のPC並の性能
    - Malwareの持ち込み
    - 情報の持出し
- 一番の問題
  - 普通のメモリと見分けがつかない
    - 発熱などの差はあるが…



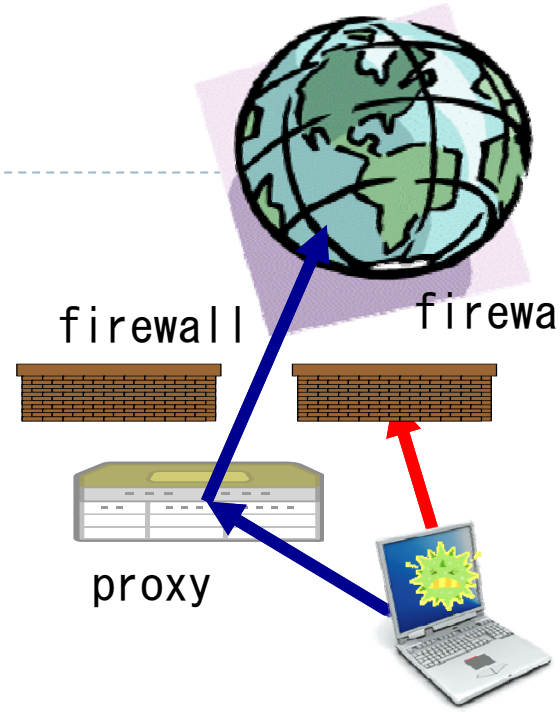
http://linux.slashdot.jp/story/12/04/11/0954236/telnetでログインできるSDメモリーカード

IPv6 readyなディバイス達

- PC、OA機器、家電…センサー
  - IPv6アドレス自動設定
  - 一つのNICに複数のIPアドレス
    - 同時使用可能
      - ✓ IPv4は通常一つのみ
- IPアドレス重複割り当ての警告なし
  - 仕様
    - 偶然発生するIPアドレス重複
    - 先着者優先の法則
  - 気付きにくいMITM

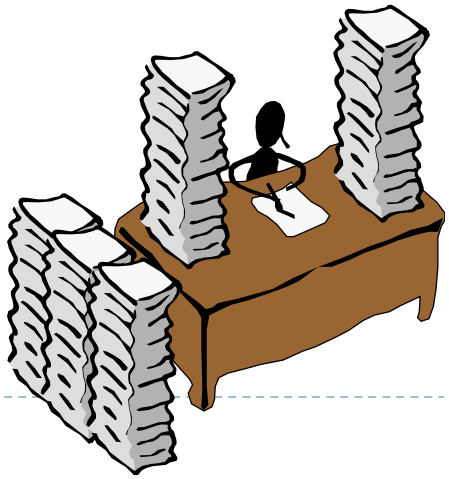
ログ保存が重要に

- 標的型攻撃では後追いを想定
  - ある程度の侵入は許容
- 異変の早期察知
  - 定常的なログ検査
  - 不自然な記録を抽出
- 様々なログ
  - 各種セキュリティシステム：firewall、IDS/IPS、ハニーポット
    - 未知の攻撃そのものを言い当てる事は稀だが…
  - サーバログ：proxy、VPN、メール
    - アクセス失敗、通信中継
- ログはログサーバに集約
  - サーバ、セキュリティシステム、NW機器の乗っ取りを想定



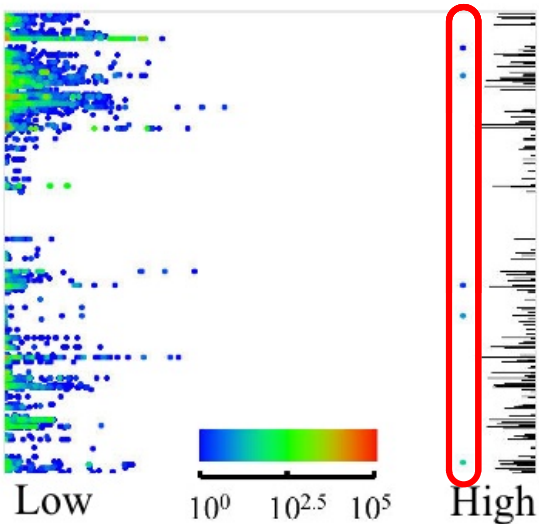
ログ取り過ぎ注意！

- ログの用途
  - 事後調査
    - できるだけ詳細なログが必要
      - ✓ LAN内の全トラッフィックを保存してくれれば…
    - 「現実的な」容量が必須
      - ✓ 攻撃の全容解明に3年かかる見込み？
  - 攻撃の早期発見
    - 定期的なログ検査
      - ✓ 1時間、1日、1週間
    - 1時間分のログ解析に1日かかる？
  - 用途に応じた適正なログ採取
    - 闇雲に何でも集めれば良い訳ではない



ログ解析

- 単体のログだけでは異変察知は困難
  - 複数ログの相関分析
  - 膨大な攻撃 or 異常を示すログ
    - その中から特に怪しいものに絞り込む
    - 目視での確認は困難→相関分析ツール必須
- 新たな異常検出手法が必要
  - 過去には見られなかったログの出現パターン
    - いつも発生しているアクセス失敗の記録
      - ✓ 設定ミスの可能性大(それはそれで問題ですが…)
    - 過去ログの学習が必要
      - ✓ 定期的な再学習と処理時間の見積(1週間かかりますじゃダメ)
      - ✓ 早期発見のためのログはさらに絞り込みが必要

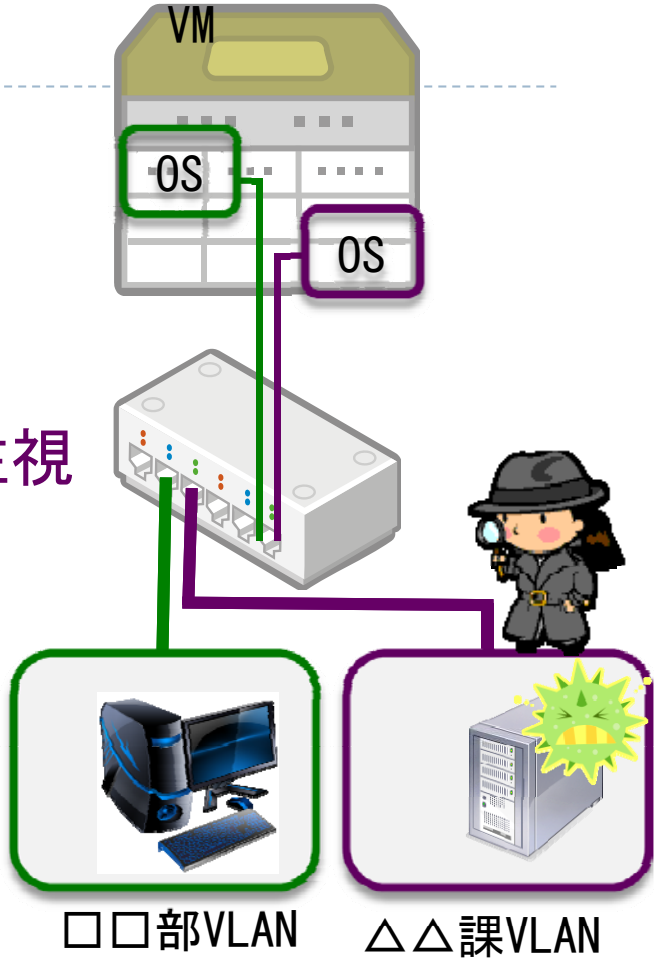


監視対象の選定

- サーバ
  - アクセス失敗、管理者権限取得状況
- NW機器
  - 設定変更履歴
- セキュリティ機器
  - できるだけ上流で監視
    - 監視のコスト削減
    - 監視機器への物理的攻撃を回避
- 万が一に備えて…
  - ハニーポット
  - 末端でのパケットキャプチャ
    - ミラーリング機能付きL2 SW

適切なアクセス制御

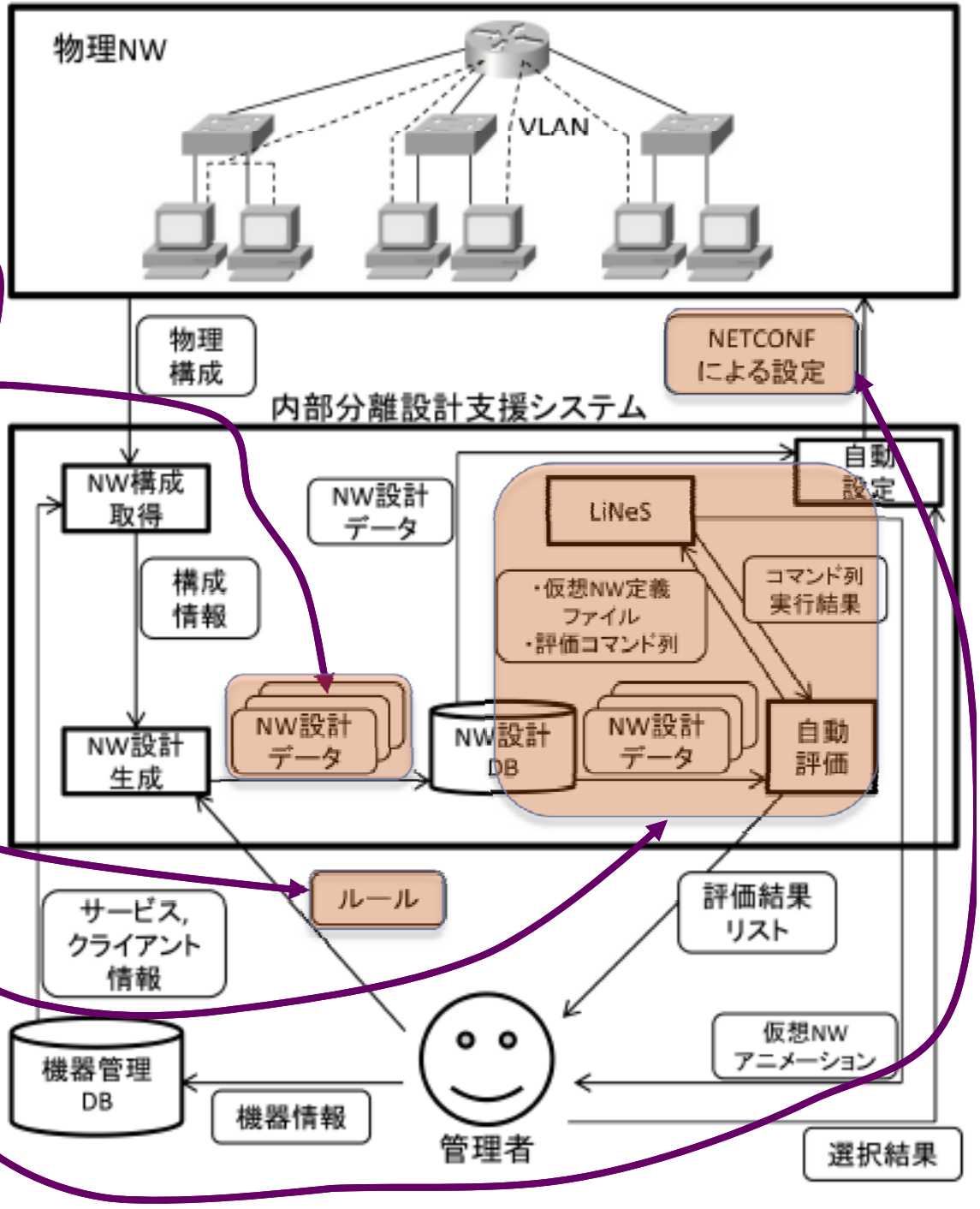
- 想定外のアクセスを防止
  - 異なる部署のPC間の通信
    - VLANによる切り分け
    - VLAN間のアクセスを制限
  - アクセス制御を超えようとする挙動に注視
- 緊急時のネットワーク監視強化
  - 監視対象のトラッフィク量削減
  - 監視機器のコストに影響
    - 100Mbps << 1Gbps <<<<<< 10Gbps
  - 緊急時アクセス制限
    - 攻撃対策＆事業継続の両立
    - 侵入者の挙動解析→目的推定→保護対象の絞り込み



VLAN管理

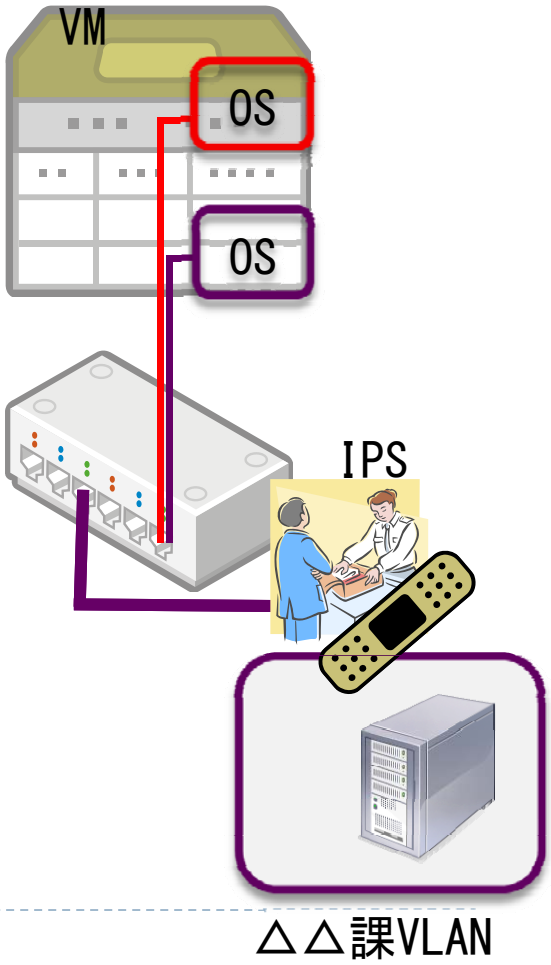
- NW運用ポリシ
- NW設定候補生成
  - VLAN設定
  - アクセス制御
- 自動評価
  - 安全性
  - 管理コスト
- 設定自動投入

緊急対応NW設定にも必須



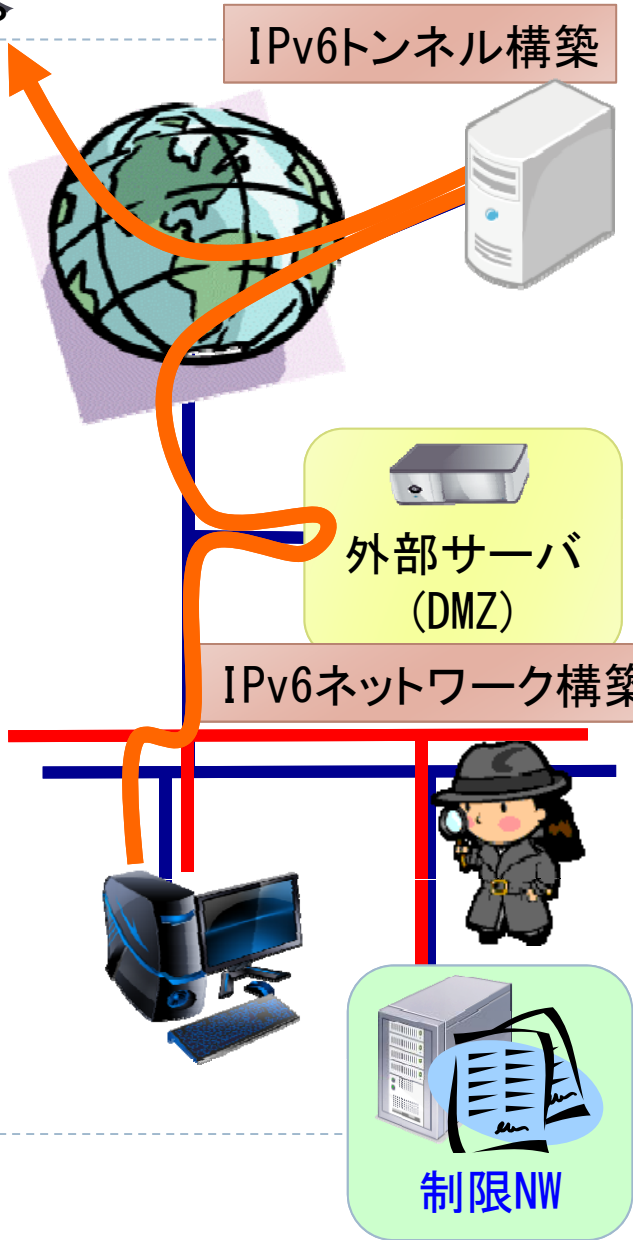
パッチ適応問題への対応

- OS更新に追従できないミドルウェア・アプリケーション
  - firewall/アプリケーションfirewallで保護
  - IPSによる仮想パッチ
    - 非対応の脆弱性を狙った攻撃をdrop
    - 完璧ではない
- 長期展望を見据えたシステム構築
  - 設計時に運用期限を設定
    - システム選定
      - ✓ 期限内の動作/互換性保証が確実なもの
  - 依存関係把握
    - 重要なシステムほど高い被依存度
    - リプレースが及ぼす影響把握



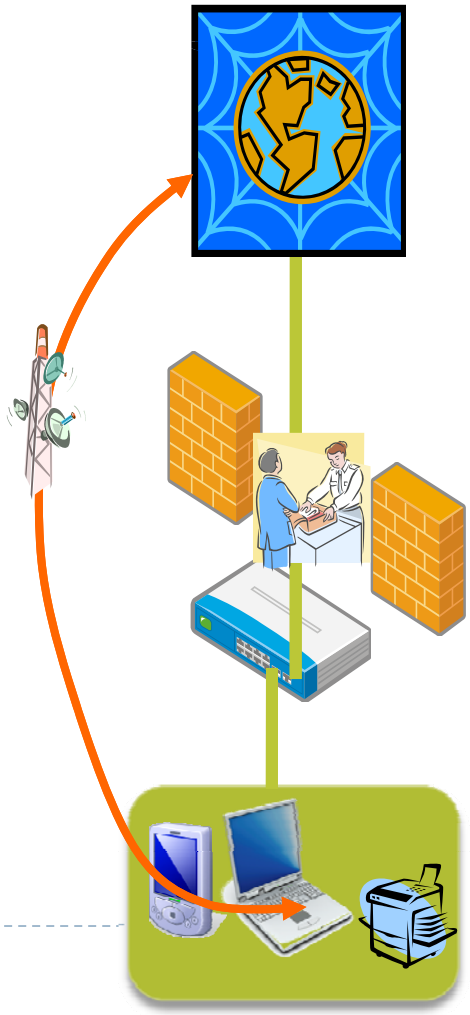
ネットワーク機器での攻撃対策

- NW管理者に成り済まして設定変更
  - 裏口ネットワークの構築
  - 監視網の回避
- NW機器の変更履歴を保存
  - VLAN管理ツールとの連携
  - 第三者による設定変更を検知
    - NW設定の更新頻度は低い
- 新しい技術の導入
  - OpenFlowとか
    - 正規のパケット以外は全てdrop



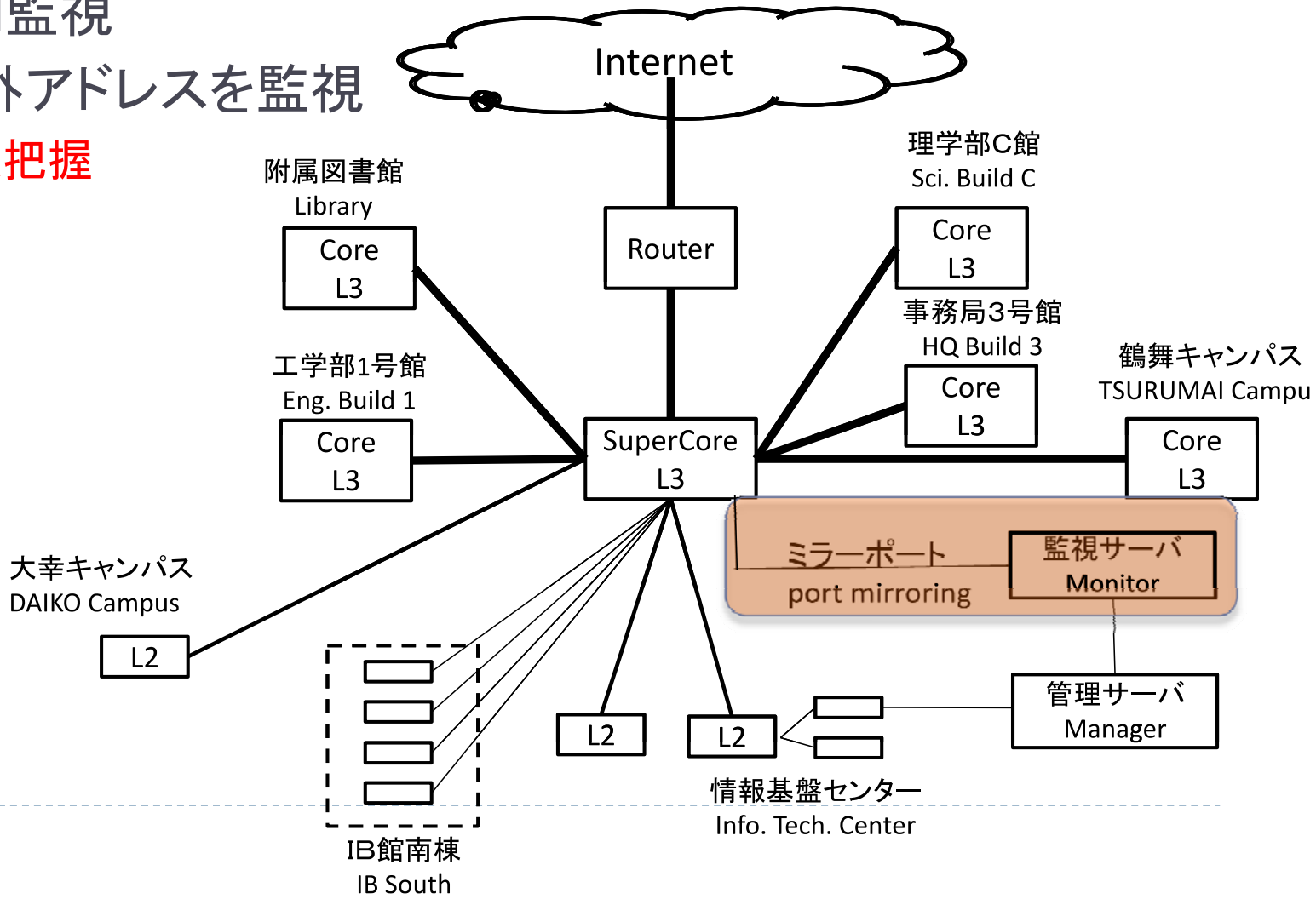
BYOD対策

- BYODもこれからの脅威
  - マルウェア拡散
  - 別ネットワークの持ち込み
    - テザリング
    - 各種トンネリング
  - MITM攻撃
- 不正な「ネットワーク持ち込み」
  - 監視と早期検知が重要に
    - 特にIPv6



不正ネットワーク持ち込み対策例

- L3 SW
  - VLAN監視
  - 管理外アドレスを監視
    - 兆候把握



不正ネットワーク持ち込みの例

- BYODによるアドレス乗っ取りの試み

観測日時	IPアドレス	MACアドレス	FQDN	検出結果
2012-07-11 16:34:05 +0900	2001:2f8:2f:1c29:7cd4:2366:2b4f:2a51	14:5a:05	a7	DAD の連続送信
2012-07-11 16:34:05 +0900	2001:2f8:2f:1c29:7cd4:2366:2b4f:2a51	14:5a:05	a7	DAD の連続送信
2012-07-11 16:28:56 +0900	2001:2f8:2f:1c29:566:1d12:d154:a89f	14:5a:05	a7	正常
2012-07-11 16:28:56 +0900	2001:2f8:2f:1c29:566:1d12:d154:a89f	14:5a:05	a7	正常
2012-07-11 16:28:09 +0900	2001:2f8:2f:1c29:d4bf:9491:9d2f:5ce7	14:5a:05	a7	DAD の連続送信
2012-07-11 16:28:09 +0900	2001:2f8:2f:1c29:d4bf:9491:9d2f:5ce7	14:5a:05	a7	DAD の連続送信
2012-07-11 16:25:54 +0900	2001:2f8:2f:1c29:d1a3:924a:85a8:a762	14:5a:05	a7	DAD の連続送信
2012-07-11 16:25:54 +0900	2001:2f8:2f:1c29:d1a3:924a:85a8:a762	14:5a:05	a7	DAD の連続送信
2012-07-11 15:40:24 +0900	2001:2f8:2f:1c29:9d88:28c2:1214:6963	14:5a:05	a7	DAD の連続送信
2012-07-11 15:40:24 +0900	2001:2f8:2f:1c29:9d88:28c2:1214:6963	14:5a:05	a7	DAD の連続送信
2012-07-11 15:38:15 +0900	2001:2f8:2f:1c29:8024:762d:7e2e:702a	14:5a:05	a7	正常
2012-07-11 15:38:15 +0900	2001:2f8:2f:1c29:8024:762d:7e2e:702a	14:5a:05	a7	正常
2012-07-11 15:38:14 +0900	2001:2f8:2f:1c29: a7	14:5a:05	a7	DAD の連続送信
2012-07-11 15:38:14 +0900	2001:2f8:2f:1c29: a7	14:5a:05	a7	DAD の連続送信

まとめ

- 標的型攻撃に備えて
  - 早期発見&迅速対応
    - ある程度の侵入は許容
  - 攻撃者の目的把握
    - 保護対象の絞り込み
    - ログ収集の重要性
      - ✓ 収集コストと解析コストを考慮
  - ログの相関分析
    - 自前ツール or 外注監視
- ネットワーク構成の見直し
  - 自動設定ツール
    - 緊急時の対応もできるだけ自動化

できるだけコストをかけずに！