サイバー攻撃の脅威と攻撃パターン

高倉弘喜
名古屋大学

巷で言われる標的型攻撃対策

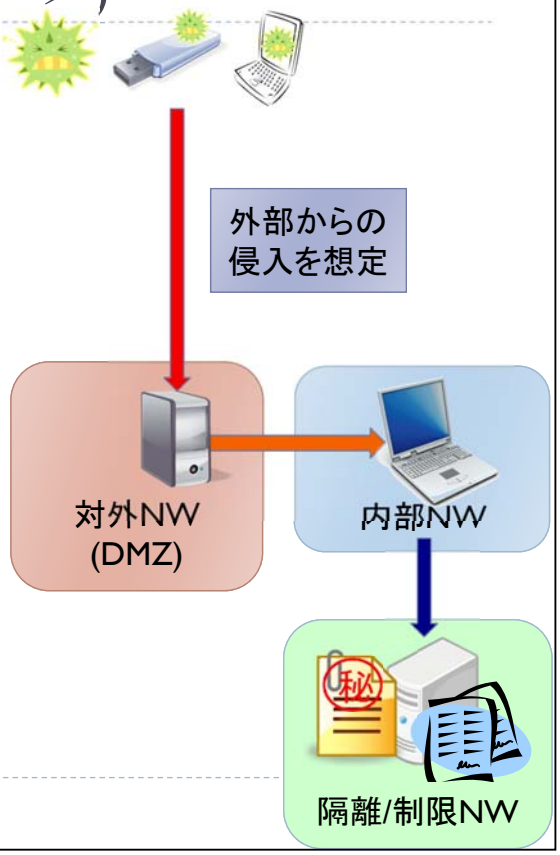
- 攻撃の全貌把握
  - 的確な判断には
    - 正確、かつ、網羅性の高い情報が必要不可欠
- 感染情報機器の完全な措置
  - 一台でも取り残すと、そこから、攻撃再発
- 漏洩情報の把握
  - 機微情報漏洩の際の速やかな対応が必須
- 攻撃を許した原因を特定
  - 再発防止策
  - 社員の教育
    - 「覚えの無いメール」対策
- 迅速な対応が要…なので新製品を

これまでの情報セキュリティ対策

- 新たな攻撃手法が見つかる度に新ソリューション
  - Firewall
  - IDS/IPS
  - Anti-Virus/Anti-spam
  - 情報漏洩対策(DLP)
  - 統合脅威管理(UTM)
- 新たに登場するディバイス達
  - BYOD/BYON
  - さらに新たな対策の必要性
- 結局、イタチごっこの繰返し
    - 様々な機器のアンバランスな導入

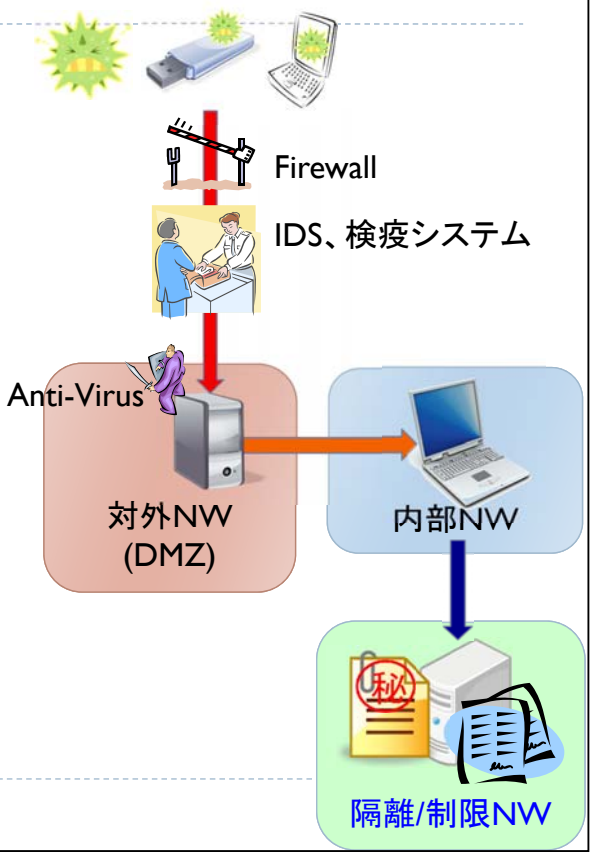
従来対策(階層型ネットワーク)

- 対外ネットワーク(DMZ)
  - 外部と内部との通信を仲介
    - 内部NWへの直接通信を防止
    - 各種セキュリティ対策(次スライド)
- 隔離/制限ネットワーク
  - 内部NWからのアクセスも制限
    - スタンドアロンマシンによる保護
- 内部ネットワーク
  - 比較的緩やかな制御
    - 一番管理し難い部分



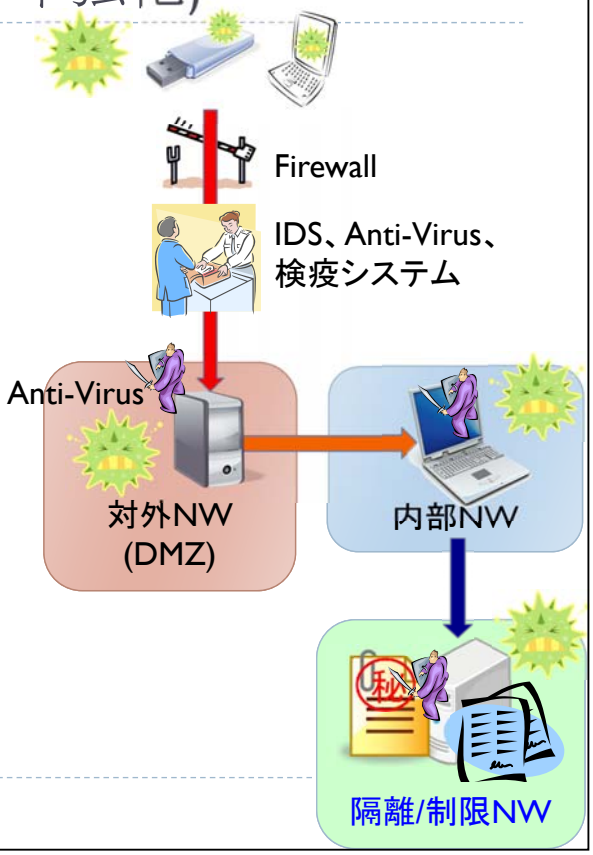
従来対策(入口対策)

- DMZで不正侵入を阻止
  - Firewall
    - 許可された通信のみ通過
    - 通信内容は関知しない
  - IDS(IPS)
    - 攻撃を行う通信を検知(阻止)
  - Anti-Virus
    - マルウェアの侵入を阻止
- 未知の攻撃には効果が薄い
  - Zero-Day攻撃



従来対策(内部セキュリティ強化)

- とは言っても…
  - 内部NWにセキュリティソフト導入
    - DMZでの対策と基本的に同じ
      - ✓ 多くの組織で同一メーカ製品
- 多様な侵入経路
  - メール添付
  - Webアクセスによる感染
    - 水飲み場型攻撃
  - USBメモリ送付/持込み
- 見逃しの可能性
  - 一旦入られてしまうと…



目立たない偵察活動

- 第一波攻撃成功後：
  - 感染PCを前線基地とした「偵察」活動
    - 利用者の活動を観察
      - ✓ 認証サーバは？
        - 認証の仕組みに注目
        - キャッシュログオンの有無
      - ✓ ファイルサーバは？
        - 業務ファイルの取得(目的の情報で無くて良い)
      - ✓ メールの送受信状態
        - 人間関係の把握(ソーシャルエンジニアリング)

  - 「夜中にこっそりと家捜し」や「派手な調査活動」はない
    - 正規の認証手順で、いつものファイルサーバにアクセス
      - ✓ NTハッシュさえあれば…パスワード不要
    - いつもの同僚に業務メール
      - ✓ 組織内部への侵食開始

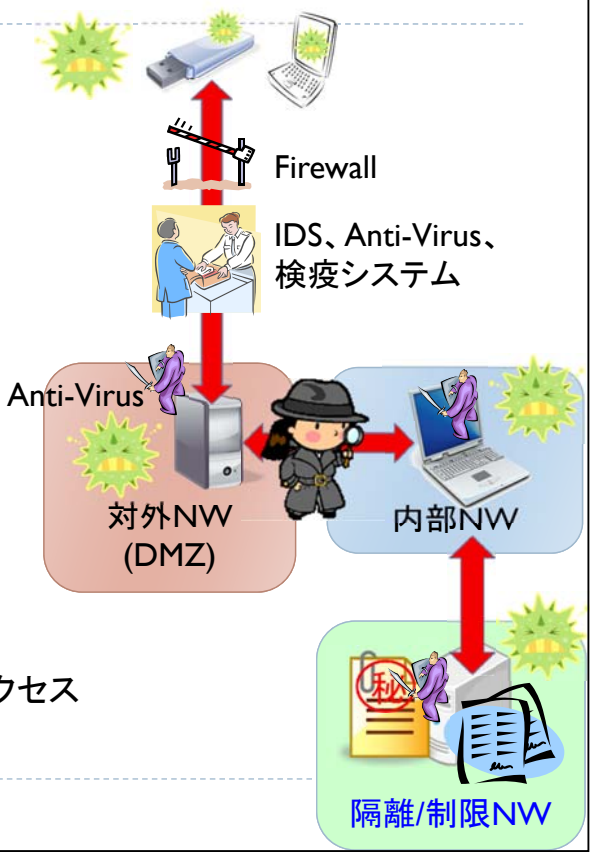
前線基地からの攻撃には脆い内部NW

- 内部NWの管理・監視体制
  - 部署毎にVLAN分割・アクセス制御している事例は稀
    - 設計・構築・運用コストの高騰
      - ✓ 部署間の通信可否を事前把握するのは困難
      - ✓ 機器追加による設定変更
      - ✓ 組織変更に伴う設計変更
  - 内部NWを隅から隅まで監視する体制にはなっていない
    - 組織内で何が起きているのかを把握するのは困難
      - ✓ 農水省の例
        - 2012年1月から4月：発生
        - 2012年3月末：情報流失の可能性は無い
          - 調査委員会発足
        - 2013年5月24日：124点の行政文書流出(機密性2以下)

真面目に調査すると1年はかかる

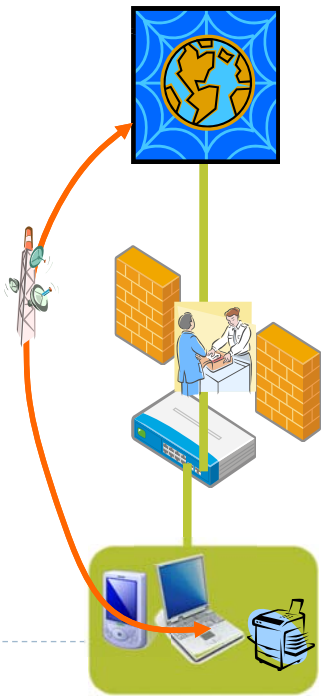
従来対策(出口対策)

- 外向き通信の監視
  - 攻撃者指令サーバ情報
    - ブラックリスト方式
    - ホワイトリスト方式
- 情報漏洩対策(DLP)
  - コンプライアンス
    - 一種のホワイトリスト方式
- 監視回避へ…
  - 暗号通信
    - 情報持出し/指令受信 by https
  - 監視回避
    - 正規ユーザを装った正しい手順でアクセス



BYODによるBOYN

- BYONによる監視対象外ネットワークの持込み
  - テザリング
  - MITM攻撃
  - 気付き難いネットワーク環境
    - LTEの方が企業ネットワークより快適…
- 不正な「ネットワーク持ち込み」
  - 入口/出口対策の無力化
    - アンチウィルス
    - 不正アクセス検知(IDS/IPS)
    - 情報漏洩対策(DLP)



不正ネットワーク持ち込みの例(IPv6)

- BYODによるアドレス乗っ取りの試み

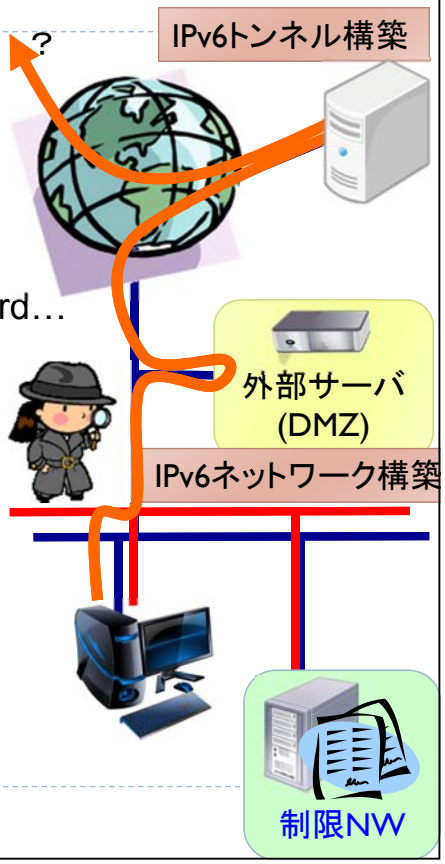
観測日時	IPアドレス	MACアドレス	FQDN	検出結果
2012-07-11 16:34:05 +0900	2001:2f8:2[redacted]:7cd4:2366:2b4f:2a51	14:5a:05[redacted]:a7		DAD の連続送信
2012-07-11 16:34:05 +0900	2001:2f8:2[redacted]:7cd4:2366:2b4f:2a51	14:5a:05[redacted]:a7		DAD の連続送信
2012-07-11 16:28:56 +0900	2001:2f8:2[redacted]:566:1d12:d154:a89f	14:5a:05[redacted]:a7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

複数のIPアドレスに成り済まし

同じMACアドレス

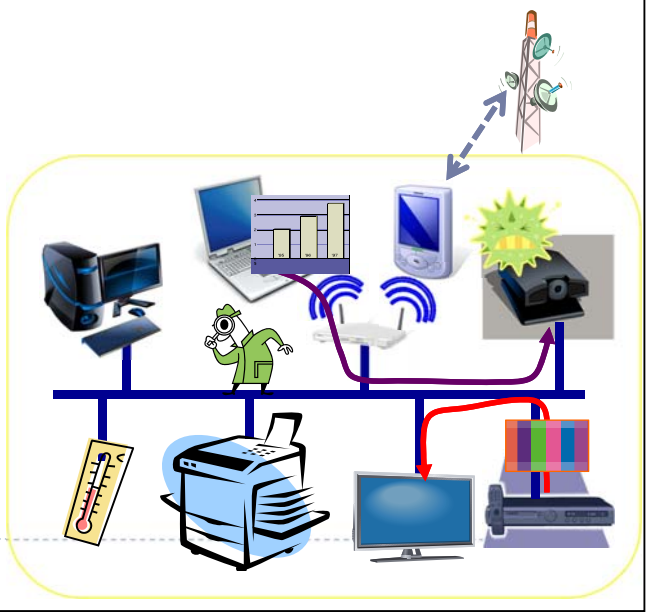
監視対象外NWの構築

- NW管理者のPCも陥落済み
  - ネットワーク構成を変更
    - 出口対策を回避する通信経路の構築
    - IPv6網を構築
      - ✓ 自由に掘れるトンネル by 6to4, Teredo, 6rd…
      - ✓ 自動的にトンネルを張るWindows製品
- 多くの組織
  - 入口/出口/漏洩対策
    - 自社内ネットワークアドレスのみを監視対象
  - 監視対象外ネットワーク
    - インターネット直結な状態



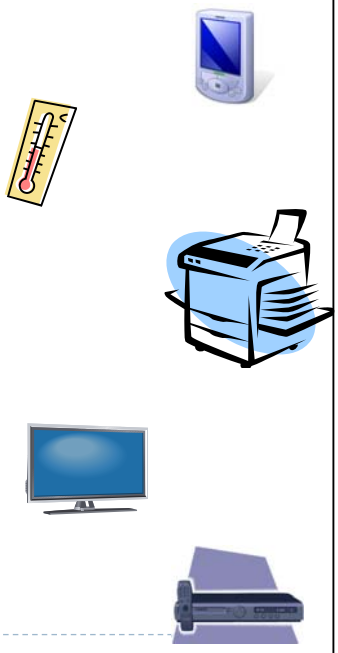
様々なディバイスがネットワークに

- OA機器
  - プリンタ、スキャナ…
  - プロジェクタ
    - サーバ機能を搭載
- 情報家電や建物設備
  - インターネットとの連携
    - 外部データに基づいた制御
- 少ないバリエーション
  - 攻撃の標的としては最適
    - 幅広い普及台数
  - 前線/中継基地として活用
    - 重要情報を最初から保持



多くのネットワーク対応機器

- OSは…
  - Linux, FreeBSD, Windowsの限定機能版
    - 場合によっては、フルスペック版を搭載
- アプリは…
  - PC用アプリの流用
  - メーカ独自開発
- いずれにせよ、PCと同じセキュリティリスク
  - PCと同レベルのパッチ適用が可能か？
  - PC同様のアンチウィルス
    - CPU・メモリ資源の制限



意外なものにまで発生する脆弱性

見直しが求められるサイバー攻撃対策

- 内部NWへの侵入を想定
  - 多くの攻撃は仕事を請け負ったプロ集団
    - 追い出しても追い出しても侵入して来る
      - ✓ どんどんステルス化
  - 攻撃が見えている方がなんぼかマシ
    - 把握できなくなったほうが怖い
- 保護対象情報(人物)の特定
  - 全ての情報を最高レベルで保護するのは不可能
    - どんだけコストをかけても…
  - 重点的なセキュリティ投資
- 業務継続を意識した防御手法
  - 攻撃に曝されていない業務への影響を極小化
    - 完全停止を極力回避
  - 不完全な情報下における防御戦略決定
    - 並行して情報収集とその精度向上

侵入の試みを察知するのは困難

- 第一波攻撃
  - 人事担当、広報担当、苦情担当などが標的に
    - 不特定多数からのメール
  - 一般社員も標的に
    - 取引先からの業務メールに偽装
      - ✓ 取引先を先に攻略
  - 「覚えの無いメールは開かない」が有効ではない
  - ゼロデイ攻撃…調査済みのセキュリティ対策
    - 入口対策だけでは防ぎきれない
      - ✓ 着弾を想定せざるを得ない
    - 出口を見張れば良い訳でもない
      - 暗号化
      - 細切れデータの持出し

現時点の情報に基づく暫定判断

- 「情報が揃うまで待つ」は最悪の選択肢
  - 不確定情報下における意思決定
    - という科目まである諸外国
  - 辻褄の合わない情報の出現
    - 攻撃の意図を察知されないために散蒔かれる偽情報
- 情報収集を継続しつつ新たな対策を検討
  - 情報の精度向上
    - 情報収集による偽情報の排除
  - 現判断を補強 or 否定
    - 新たな判断をいつすべきか？
      - ✓ 継続 or 撤回
  - 定期的な判断記録の保全

再発防止策の立案と実施

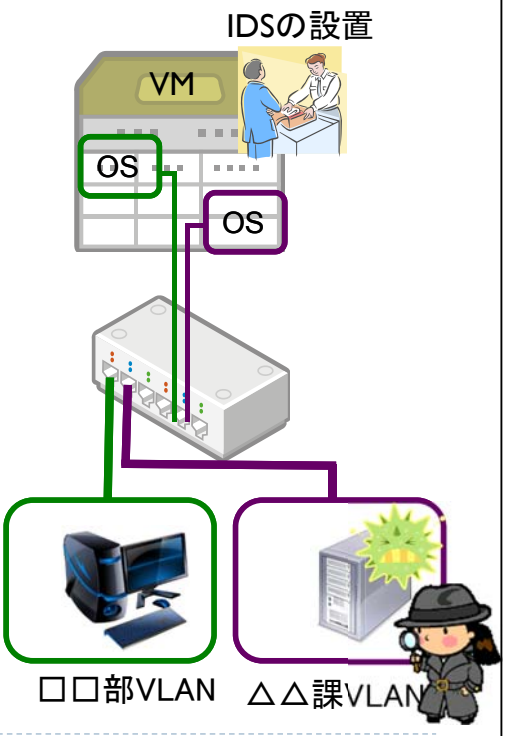
- 原因が全て判明することはまずありえない。
  - 誰が、どの脆弱性が、どの情報が…狙われた？
  - どんなに調査しても断片的な情報
    - 不足分は推理力で勝負→役員を説得できるか？
- 全ての情報システム・資産を守ることは困難
  - 情報セキュリティ対策にもROI
    - 狙われやすい所を重点的に防護
  - 必要な措置はリピータ対策
    - 直ちに追い出す作戦が正しいとは限らない
      - ✓ 依頼された情報を執拗に探索
        - 狙われている情報を把握した方が得策
      - ✓ そこに網を張って待つという選択肢も

新たなセキュリティ対策の必要性

- あらゆるリスクを想定するのは不可能
  - コスト的に折り合わない
- 守るべきは何か？
  - インターネットからの攻撃
  - 社内からの攻撃
- どこで守るか？
  - 対外接続点
    - 入口対策/出口対策
  - 組織内部

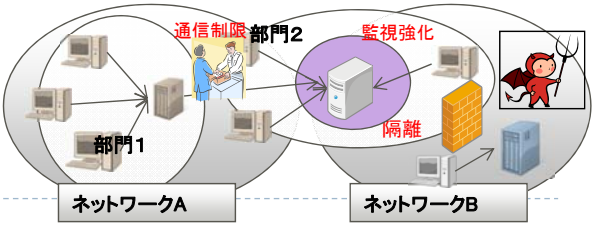
攻略し難いネットワークへの移行

- アクセス区画の整備
  - 部署毎にVLANを構築
    - VLAN間の通信を制限
      - ✓ 偵察活動の阻止
  - VLAN越え通信の監視
    - 通常存在しない部署間アクセスの存在
- 内部NWの監視体制強化
  - 巡回監視が基本
    - 常時監視よりも低コスト
    - 広く薄い監視
  - 通信量から得られる情報
    - 高頻度通信=重要(かも知れない)業務
- VM化サーバの監視
  - 監視ポイントの大幅集約



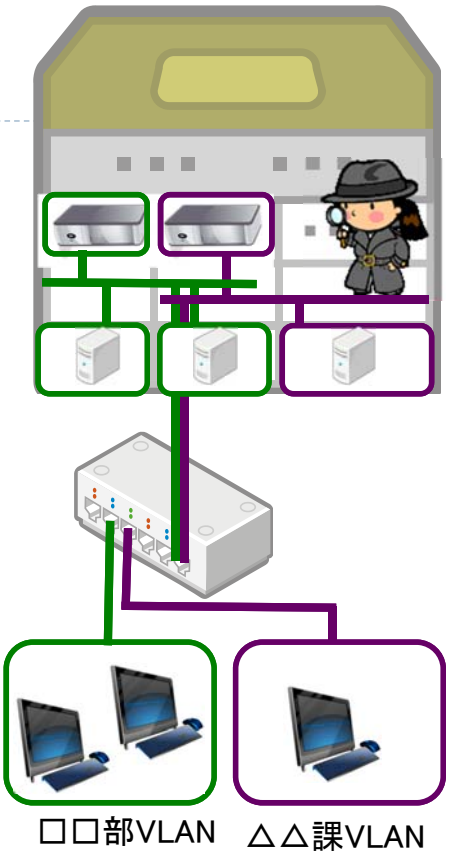
万が一の内部浸食対策

- VLAN/SDN化より監視ポイントを集約
  - 末端のトラフィックを監視装置まで転送
    - 至る所にセンサーを置くより格安
- VLAN毎にざっくりと監視
  - 普段は存在しない通信の発生
    - VLAN越え通信の試みに注視
- 不審な通信発見時
  - 段階的アクセス制限
    - 通信の発生元
    - データの重要度
    - 業務の重要度



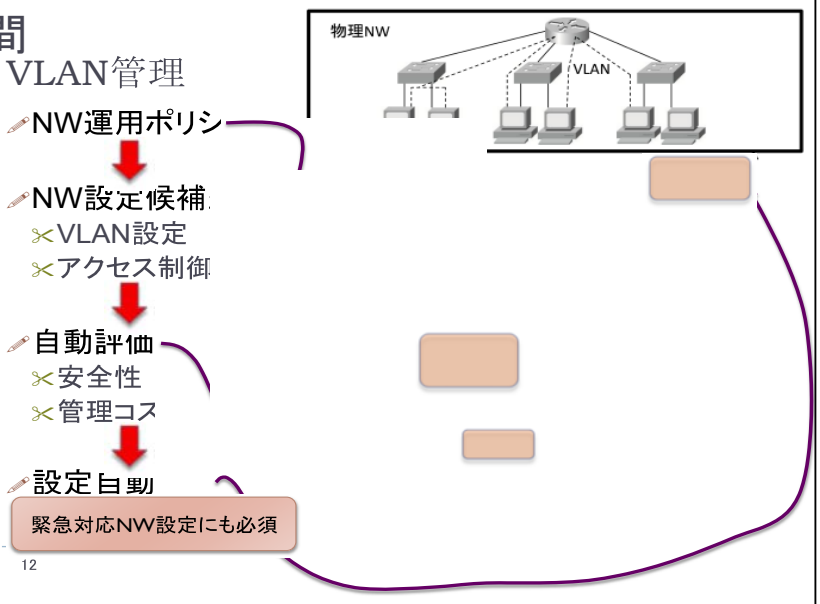
さらなる仮想化の促進

- サーバを仮想化
- クライアントも仮想化
  - VDI(Virtual Desktop Infrastructure)
- サーバークライアント間のネットワーク
  - 論理的ネットワーク
    - VM間通信
    - SDNによるアクセス制御
- 監視ポイントの大幅集約
  - ホストマシン上で全てを監視
    - 巡回監視も容易に実現
    - VMがマルウェア感染しても影響を受け難い
    - 不審な通信の早期発見
    - ピンポイントで防御対策実施



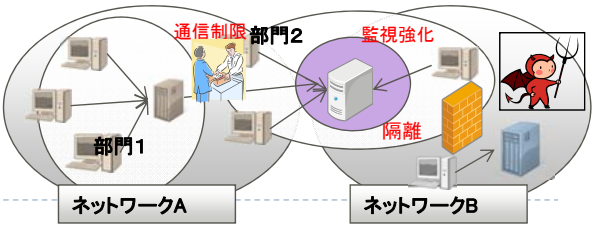
ネットワーク構築の(半)自動化

- 最初は大雑把なVLAN分割
  - 緩いアクセス制御
- ネットワーク監視による再設計
  - 通信の無いVLAN間
    - 遮断ACL提案
  - 再設計の評価
    - 安全性
    - 利便性
- 設計データ投入
  - config自動生成
    - 半自動化



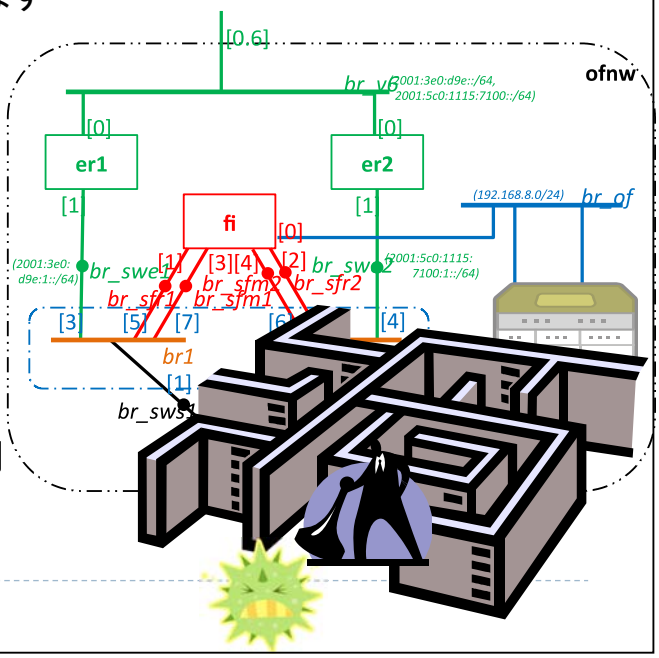
緊急対応下での業務継続のための情報収集

- 普段の通信状態の把握
  - 緊急対応により影響を受ける業務の洗い出し
  - 業務の影響度を考慮した緊急対応案
    - 隔離/遮断
      - ✓ 業務への影響小　or 隔離状態で業務継続可能
        - データの授受は安全な方法で
    - 通信制限
      - ✓ 業務への影響中
        - 通信量の多い部門のみ
        - 不審な通信が観測されていない部門のみ
    - 監視強化
      - ✓ 業務への影響大
        - 読み出しのみ可
        - 別VMで囮サーバ
          - アクセス状況を監視



緊急用ネットワークによる攻撃追跡

- ネットワークのアクセス制御を強化
  - 通常の通信
    - アクセスの挙動は変化しないはず
  - 攻撃/調査活動
    - 挙動変化の可能性あり
      - ✓ スキャン
      - ✓ 迂回
      - ✓ 沈黙
- 挙動変化からの目的推測
  - どのサーバに向っている？
- 攻撃の目的に対応した防御

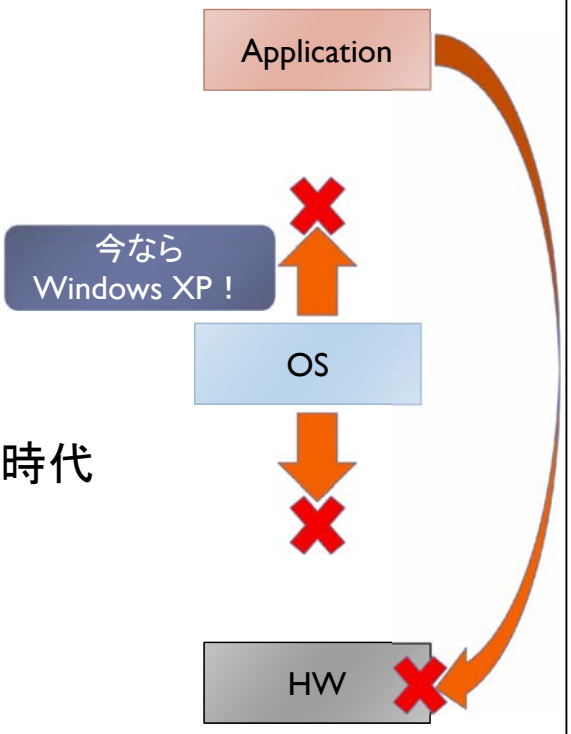


簡易ハニーポットの構築

- 不審な通信をハニーポットに誘導
  - VLAN+SDNであれば容易に実現
    - 一般的なネットワークでもPolicy Based Routingで対応可能
  - VMであればcloneを使える
    - 本物と同じ構成/動作による正確な情報を収集
    - 攻撃者が気付き難いハニーポット
      - ✓ 目的の情報の特定
- 保護対象の絞り込み
  - 人物
  - ネットワーク
  - サーバー
    - 情報の精度向上による、更なる対策 or 対策変更

システム更新の無限ループ

- OS更新…
  - ハードウェアのスペック不足
  - 新型機へ更新
    - 現用OSに非対応
  - 最新OSの導入
    - 現用アプリケーションに非対応
  - 結局、全リプレースへ
- 長期のシステム稼働を想定する時代
  - 長期間の負荷増の見積困難
  - 運用開始時に更新計画
  - 止められないシステムの存在



まとめ

- ステルス化するサイバー攻撃への備え
  - 早期発見&迅速対応…のためには
    - 怪しい情報の収集と解析
      - ✓ 情報が揃わなくても暫定措置
  - 攻撃者の目的把握
    - 保護対象の絞り込みと集中的な対策
    - 被害範囲と影響度の推定
      - ✓ 業務継続を意識した段階的な対応
      - ✓ 対策による攻撃の挙動変化を追跡
- ネットワーク構成の見直し
  - VLAN化とアクセス制御
    - 細かすぎないことも重要
  - 緊急対応も意識したネットワーク管理

できるだけコストをかけずに！