# サイバー攻撃の脅威と最新攻撃パターン

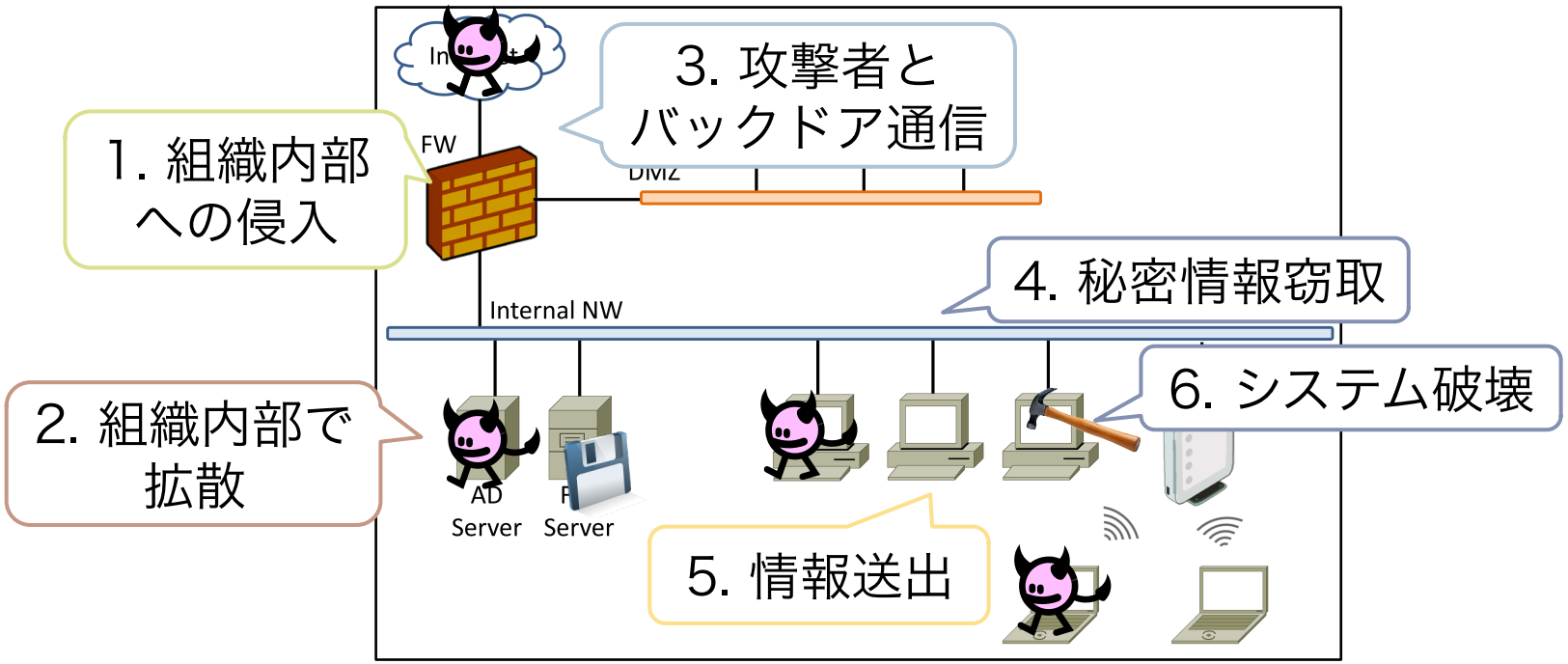
高倉弘喜
名古屋大学

# 今回の内容

- 標的型攻撃の概要
  - 侵入を前提とした対策
    - 被害範囲の特定、事後対応や再発防止策
- クラウド活用の利点と注意点
  - 安全性向上
  - 迅速な状況解析と被害範囲特定
  - インシデントレスポンスのための追加負荷
- 今後検討すべき事項
  - ビル設備のネットワーク化
- 進みつつある対策
  - 大学間CSIRT

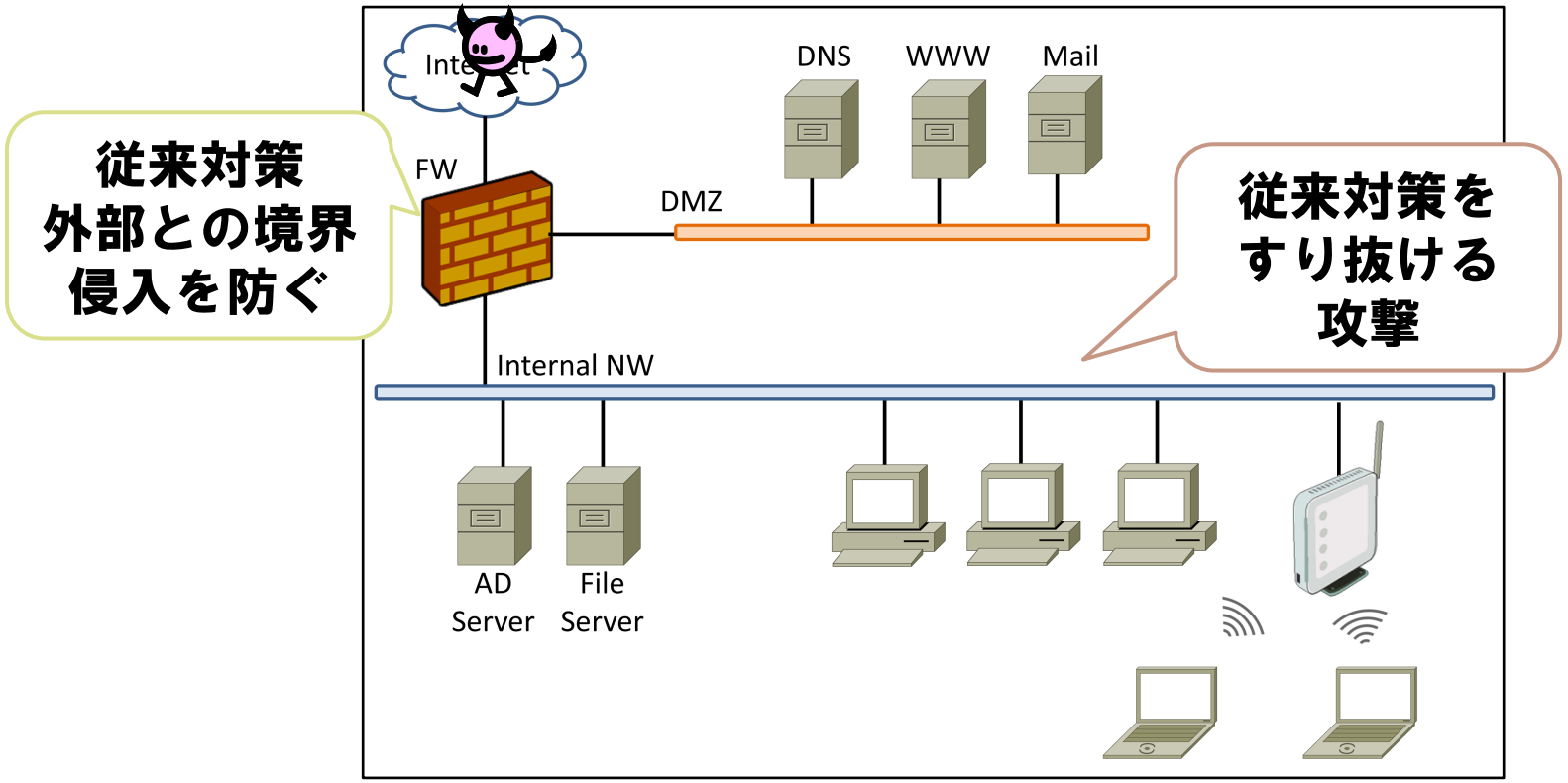
# 近年のサイバー攻撃

- 特定の攻撃対象、情報窃取などの目的→巧妙な手口
  - 事前の調査活動
  - 攻撃対象専用の、標的型メール攻撃や組織のNWに特化した攻撃
  - 長期間の潜伏



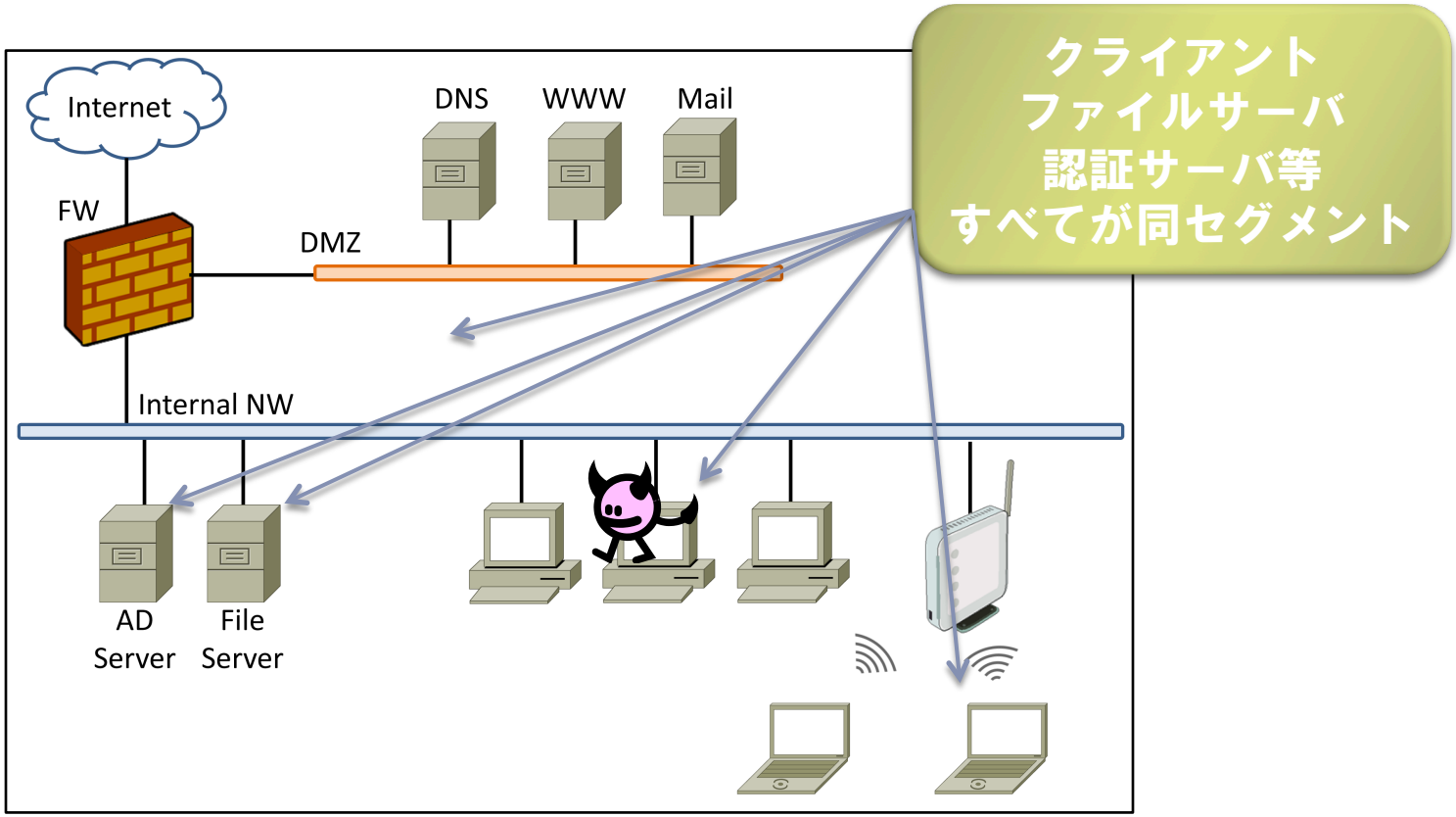
# 従来からのセキュリティ対策

- ファイアウォール、侵入検知システム、ウイルス対策ソフト
  - 組織の入口で侵入を防ぐための対策



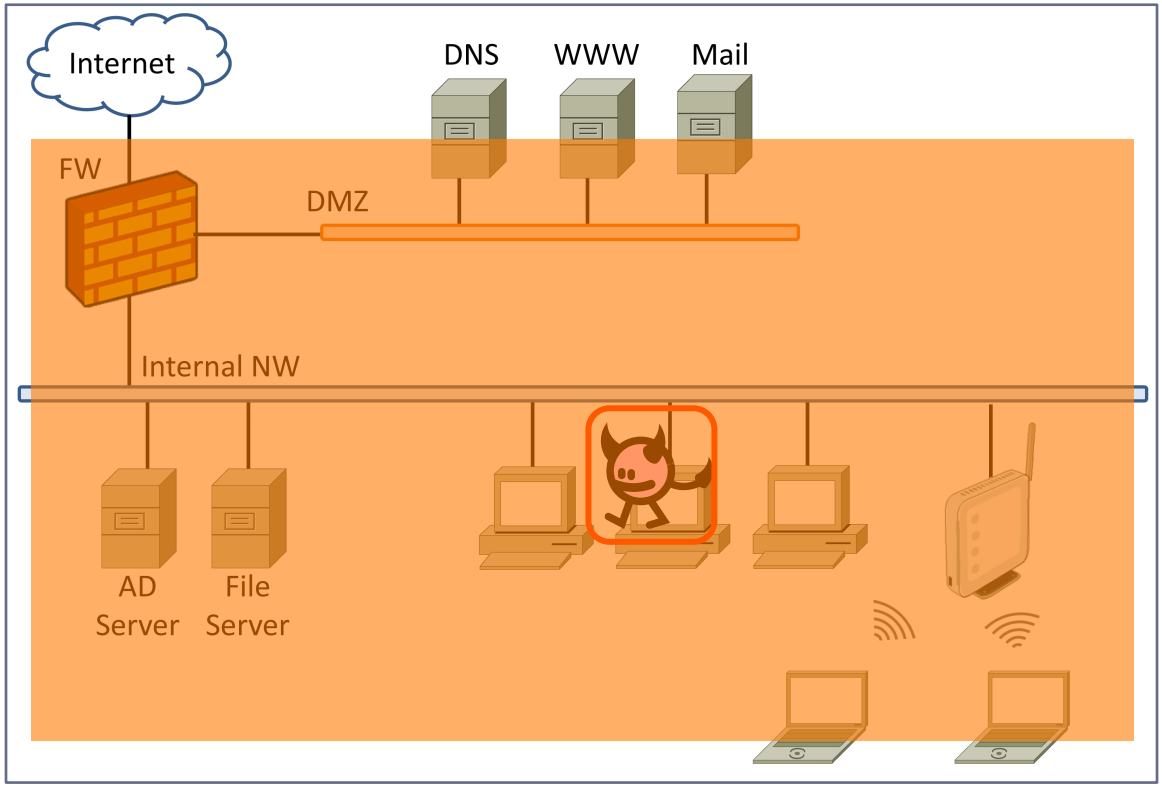
# 一般的な企業内部ネットワーク

- すべての機器が同一セグメント
  - マルウェアは内部で自由に活動



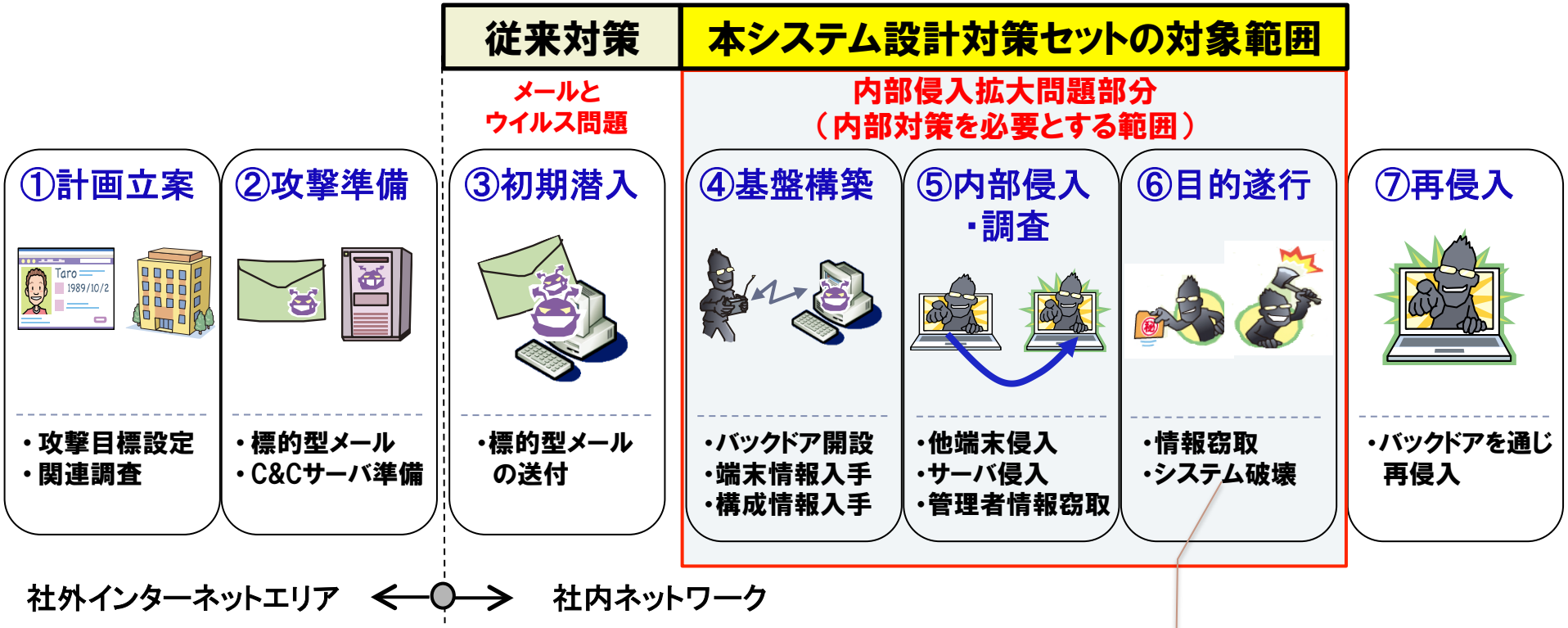
# インシデント時の対応

- マルウェア感染を発見した場合
  - 組織ネットワーク全体を停止 or 何もしない



# 侵入を前提とした対策の必要性

by IPA




- 内部ネットワークでの対策必須
  - 解析対象のトラフィック量増大
  - 新たな解析手法が必要に

情報窃取
システム破壊



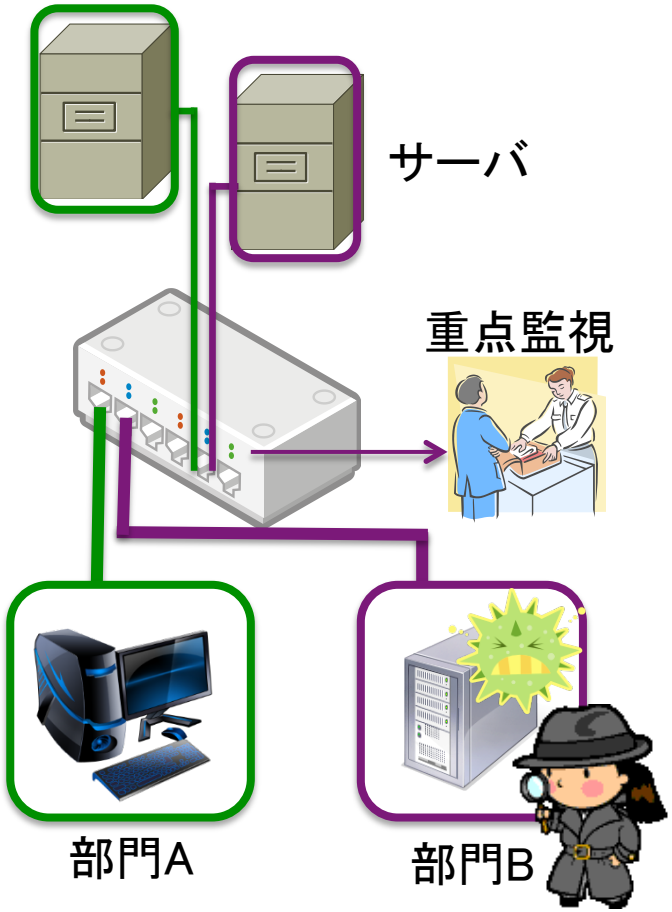
http://www.ipa.go.jp/security/vuln/newattack.html

# 海外でも、侵入後の対策に重点を

- NIST SP 800-61が求める対策
  - Preparation
    - ✓ Secure systems, networks, application against attacks
      - e.g., security patches
  - Detection & **Analysis**(検知&**分析**)
    - ✓ Detect sign of an incident.
      - e.g., various types of countermeasures
  - **Containment**/Eradication & Recovery(**封込め**/根絶&回復)
    - ✓ Mitigate damage
      - Few solutions
  - Post-Incident Activity

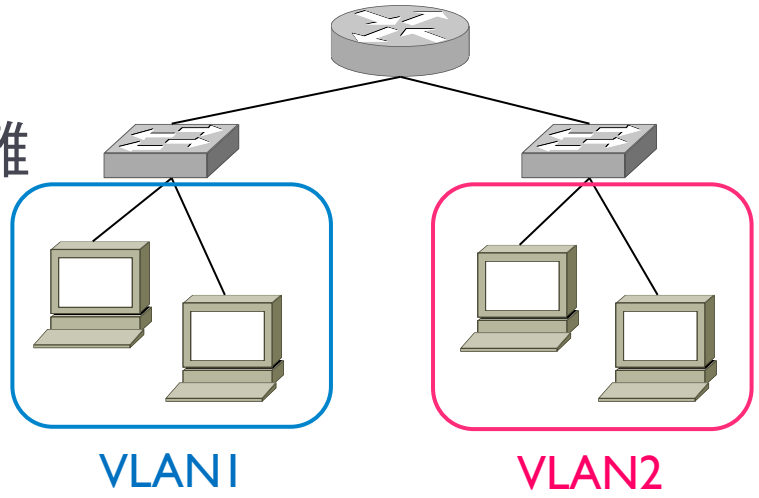
# 攻撃を受け難いネットワークの構築

- VLAN導入と木目細かなアクセス制御
  - 内部NWでのFW構築
  - VLAN間の無許可アクセスを監視
    - アクセスの存在検知
      - ✓ 設定ミス・異常動作
        - それはそれで問題
      - ✓ ステルス攻撃進行中の可能性
      - ✓ 不審なアクセスのみ重点監視
- VLAN巡回監視
  - 内部NWをざっくり監視
    - ステルス攻撃は凝視しても…
  - 解析対象のトラフィック量を削減
    - 「対策」の低コスト化



# 巧妙な攻撃への対策

- ネットワーク分離設計
  - 内部ネットワークをVLANで分離
  - 不要な通信の制御

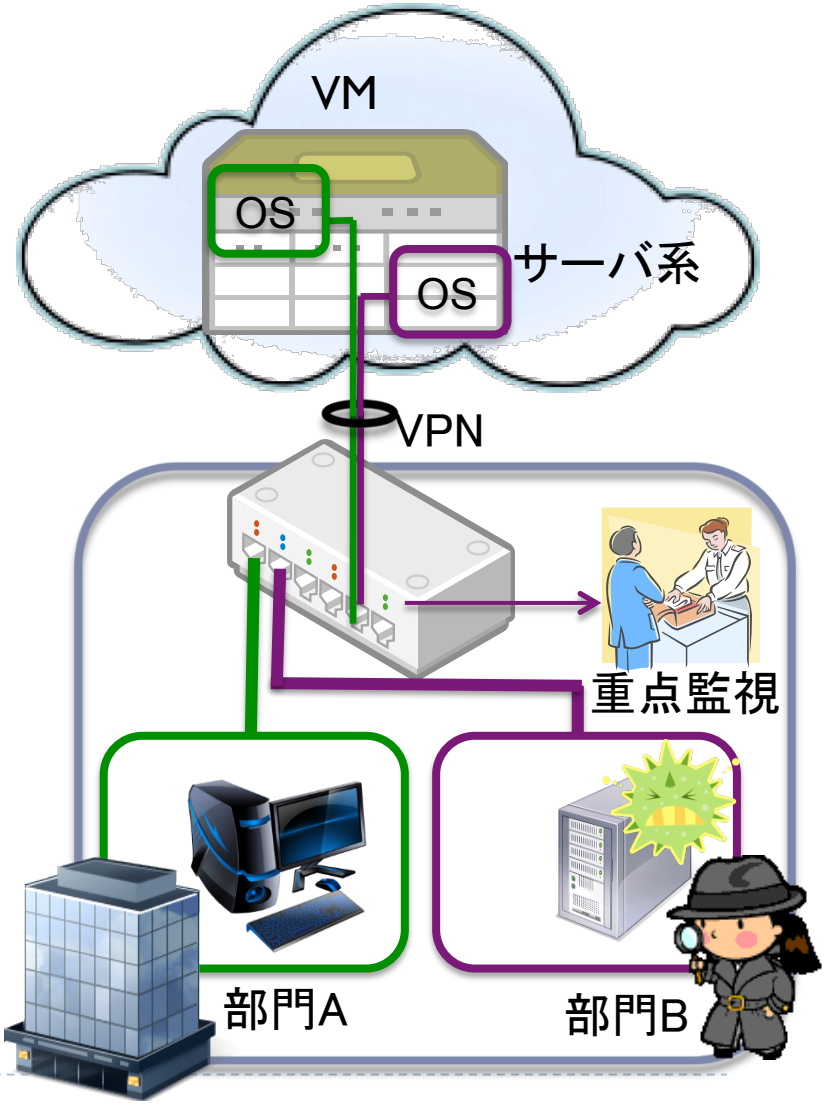



- ネットワーク自動設計
  - ネットワーク分離設計の応用
  - ネットワーク構成算出、アクセス制御を自動化
  - 異常時の動的なアクセス制御

# クラウド化によるセキュリティ強化

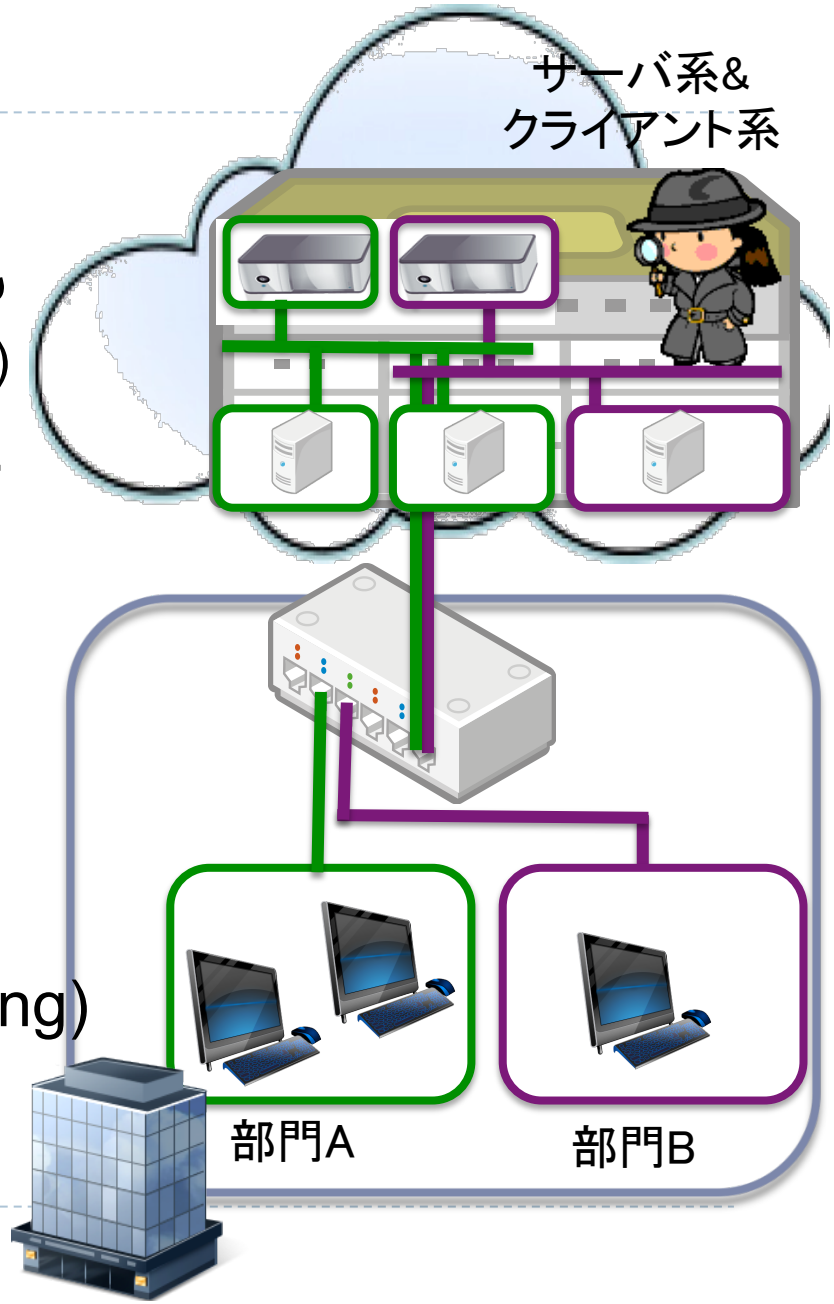
- サーバ系をクラウドに集約
  - 社内：クライアント系のみ
- 標的型攻撃の目標
  - 重要情報の摂取
  - NW・システムの破壊
    - サーバ系攻撃の可能性大
- サーバ系の隔離
  - 重要情報の保護
- 監視ポイントの集約
  - サーバ系への回線を重点監視

プライベートクラウドでもOK



# 次世代環境

- 完全仮想化環境
  - サーバだけじゃなくクライアントも
    - VDI(Virtual Desktop Infrastructure)
- 全てのトラフィックが監視可能に
  - Server – client間
  - Client – client間
- DC内での監視
  - VLAN巡回監視の容易化
  - 迅速なインシデントレスポンス
- SDN(Software Defined Networking)
  - 柔軟なネットワーク運用

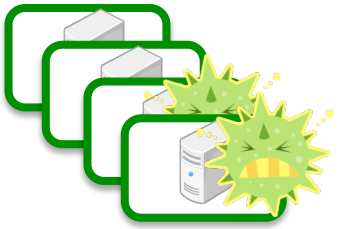


# 完全仮想化のメリット

- ハードウェアとソフトの寿命のミスマッチから脱却
  - HWの陳腐化/劣化：4、5年後
  - OS/アプリケーションのサポート期間：10年程度
    - 最新OSではサポートされない旧型マシンや周辺機器(プリンタとか)
- 統一されたセキュリティ対策
  - OS/アプリケーションの更新状況把握
    - 更新が遅れがちになるサーバ問題への対応
      - ✓ 不具合時：スナップショットによる切り戻し
  - アンチウイルスソフトによる一括スキャン
    - 外部からのVMディスクイメージに対するスキャン
- スナップショットによる迅速な業務継続
  - HW障害による業務停止を最小限に

# VDI環境に適したインシデントレスポンス

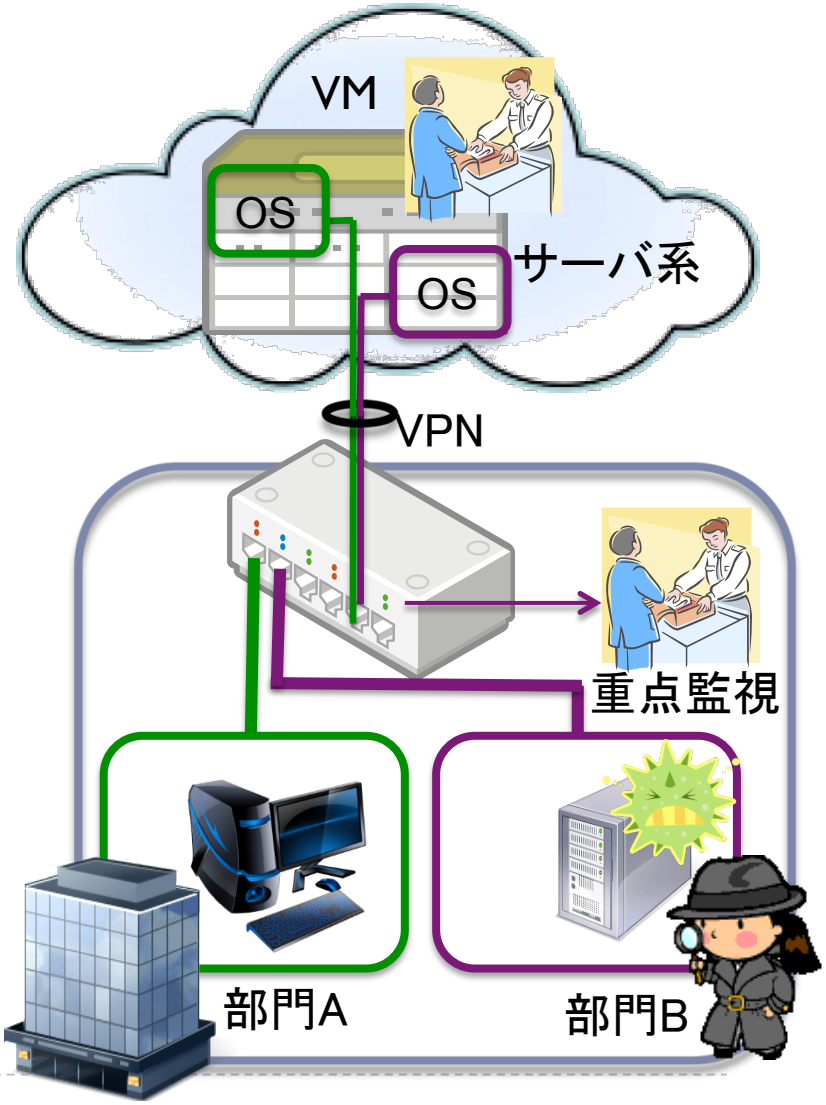
- 仮想マシン
  - 定期的なスナップショット
    - 多世代バックアップ



- インシデント確認時
  - インシデント発生時期の迅速な特定
    - マルウェア感染と被害範囲
- スナップショット間の比較
  - 最終更新後の実行ファイル・ライブラリ入れ替わり
  - 外部によるファイルシステム全体の調査
    - rootkitの影響排除
- 感染前の仮想マシンで業務継続
  - 監視強化は必須

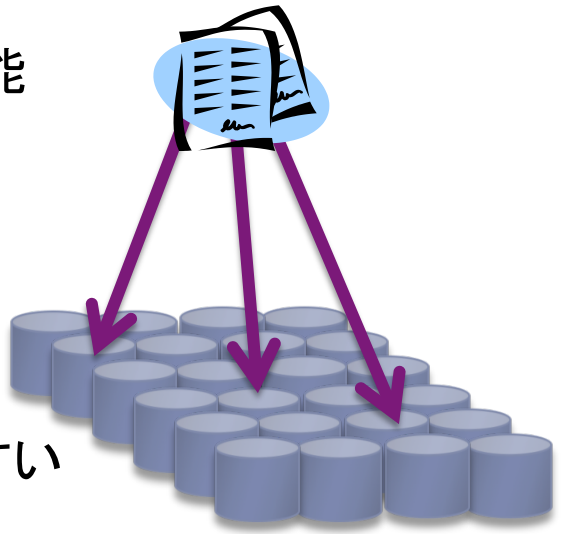
# クラウドにおけるセキュリティ対策の課題

- サーバ系の監視の限界
  - VMの物理的な位置
    - 複数の筐体…DCに分散
  - VM間の通信
    - どこを通っているのか？
- 複数者で共有する筐体とNW
  - 自社のVMの通信のみ抽出
  - インシデントレスポンスの為に…
    - IDSや解析システムが必要に
      - ✓ どこで動作させるのか？
- 平常時の巡回監視
  - 許容範囲内の負荷増



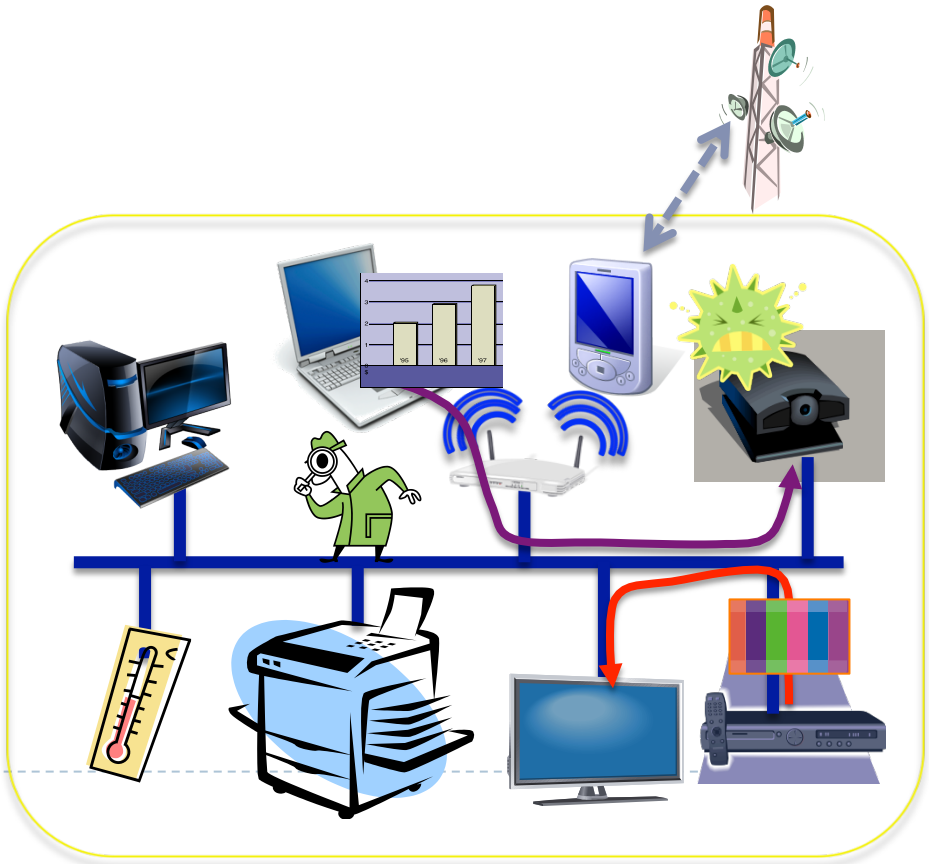
# フォレンジックスへの影響も大

- ネットワークフォレンジックスの負荷増
  - 実ネットワーク不在 or 超高速実ネットワーク
- コンピュータフォレンジックスが困難に
  - VMのファイルシステム
    - OS+アプリ＋αが一つのファイルに
    - VM上のファイルの追加、削除、変更
      - ✓ ファイルシステム内の論理的位置は特定可能
      - ✓ 実際にはどこにマップされるのか？
  - ホストマシンの実ディスクシステム
    - HW　RAID
      - ✓ 消されたファイルの磁気情報はどこに？
      - ✓ サボータージュ(破壊)活動の影響を受けやすい



# 様々なディバイスがネットワークに(去年の再掲)

- 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



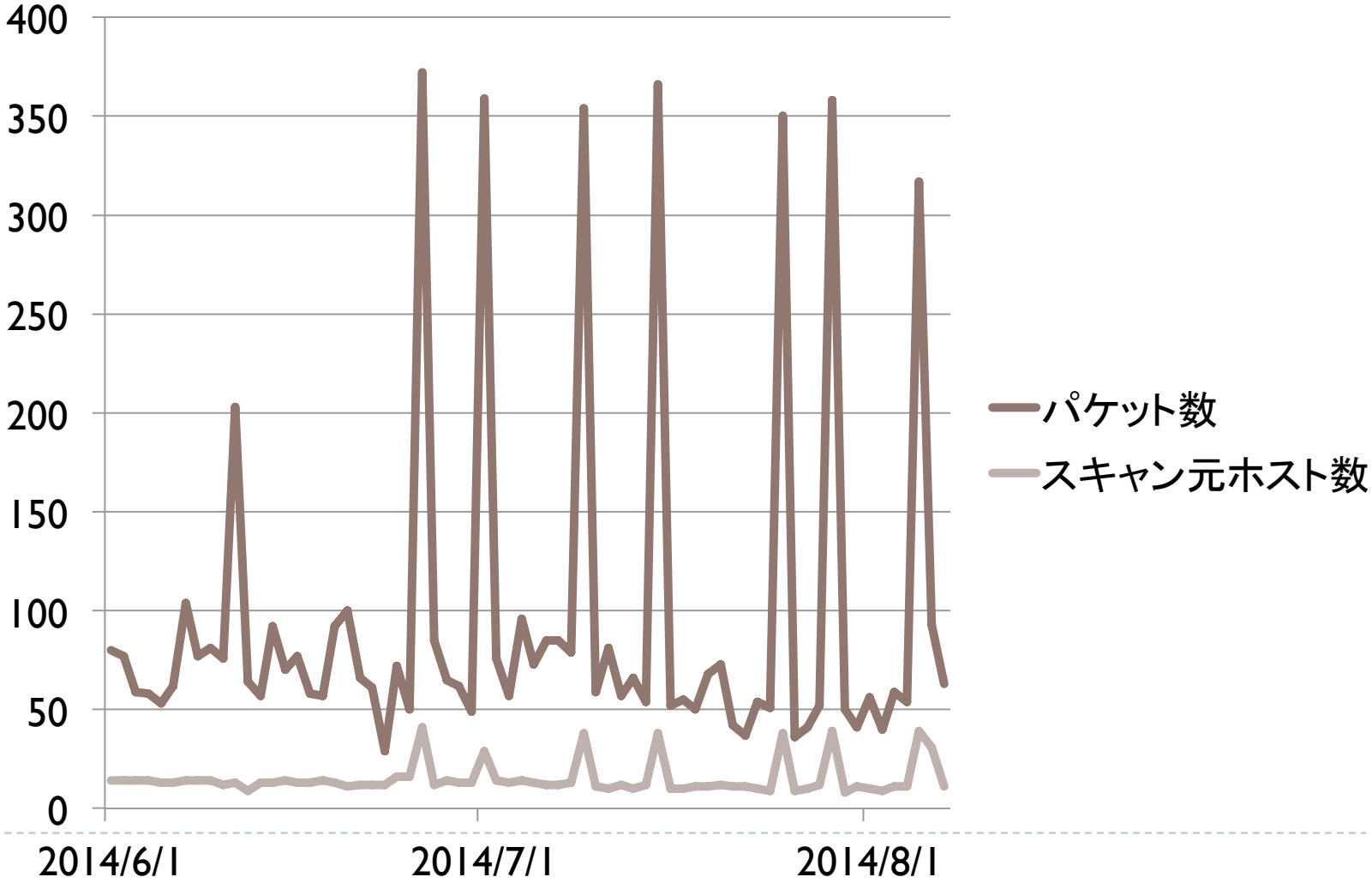
# 狙われ始めたビル設備制御

- BACnet (Building Automation and Control Network)

| Receive Time | Type | Source | Source Country | Destination | From Port | To Port | IP Protocol | Application |
|---|---|---|---|---|---|---|---|---|
| 08/07 15:09:07 | end | 82. 5.7 | IS | 133.6. 140 | 40000 | 47808 | udp | bacnet |
| 08/07 15:08:34 | start | 82. 5.7 | IS | 133.6. 140 | 40000 | 47808 | udp | bacnet |
| 08/07 15:06:29 | end | 82. 5.6 | IS | 133.6. 38 | 40000 | 47808 | udp | bacnet |
| 08/07 15:06:19 | end | 93. .62 | RO | 133.6. 211 | 40000 | 47808 | udp | bacnet |
| 08/07 15:06:06 | end | 82. 5.6 | IS | 133.6. 225 | 40000 | 47808 | udp | bacnet |
| 08/07 15:05:56 | start | 82. 5.6 | IS | 133.6. 38 | 40000 | 47808 | udp | bacnet |
| 08/07 15:05:53 | end | 82. 5.7 | IS | 133.6. 9 | 40000 | 47808 | udp | bacnet |
| 08/07 15:05:46 | start | 93. .62 | RO | 133.6. 211 | 40000 | 47808 | udp | bacnet |
| 08/07 15:05:33 | start | 82. 5.6 | IS | 133.6. 225 | 40000 | 47808 | udp | bacnet |
| 08/07 15:05:20 | start | 82. 5.7 | IS | 133.6. 9 | 40000 | 47808 | udp | bacnet |
| 08/07 15:03:26 | end | 82. 5.6 | IS | 133.6. 30 | 40000 | 47808 | udp | bacnet |
| 08/07 15:02:53 | start | 82. 5.6 | IS | 133.6. 30 | 40000 | 47808 | udp | bacnet |
| 08/07 15:02:19 | end | 82. 5.7 | IS | 133.6. 26 | 40000 | 47808 | udp | bacnet |
| 08/07 15:01:47 | start | 82. 5.7 | IS | 133.6. 26 | 40000 | 47808 | udp | bacnet |
| 08/07 15:00:06 | end | 93. .62 | RO | 133.6. 0 | 40000 | 47808 | udp | bacnet |
| 08/07 14:59:33 | start | 93. .62 | RO | 133.6. 0 | 40000 | 47808 | udp | bacnet |
| 08/07 14:59:28 | end | 82. 5.7 | IS | 133.6. 25 | 40000 | 47808 | udp | bacnet |
| 08/07 14:58:55 | start | 82. 5.7 | IS | 133.6. 25 | 40000 | 47808 | udp | bacnet |
| 08/07 14:58:40 | end | 93. .62 | RO | 133.6. 211 | 40000 | 47808 | udp | bacnet |
| 08/07 14:58:08 | start | 93. .62 | RO | 133.6. 211 | 40000 | 47808 | udp | bacnet |

# 増加傾向にあるBACnet探索

- 基本的に、何かが見つかりそうになると活発化



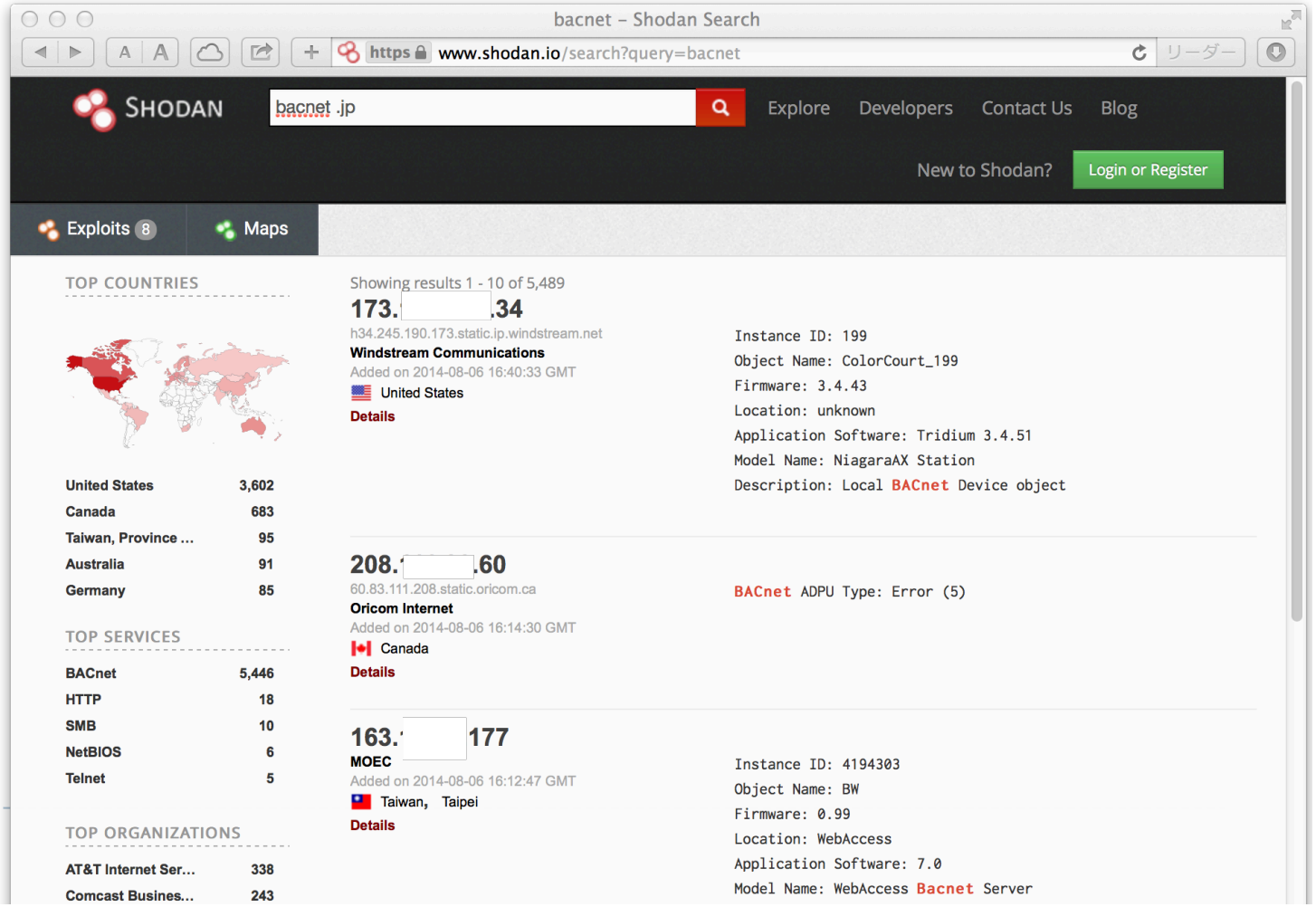
# shodanによる探索活動

- 日々調査

| Receive Time | Type | Source | Source Country | Destination | From Port | To Port | IP Protocol | Application |
|---|---|---|---|---|---|---|---|---|
| 08/07 15:11:05 | start | 71. .142 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:11:04 | end | 198 0.114 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:11:00 | start | 198 0.114 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:49 | end | 66. 92.138 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:46 | start | 66. 36.119 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:40 | start | 71. .142 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:38 | start | 66. 92.138 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:32 | start | 198 0.114 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:24 | end | 71. .142 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:21 | end | 71. .200 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:20 | end | 198 9.74 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:20 | end | 71. .131 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:20 | end | 71. .131 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:19 | end | 71. .142 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:17 | start | 66. 92.138 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:09 | end | 198 9.98 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:10:01 | end | 71. .142 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:09:51 | start | 71. .142 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:09:49 | start | 71. .200 | US | 133.6. | 40000 | 47808 | udp | bacnet |
| 08/07 15:09:48 | start | 198 9.74 | US | 133.6. | 40000 | 47808 | udp | bacnet |

# 一般公開される調査情報

- 脆弱な機器の情報も検索可能
  - 様々な目的で利用されている



# 動き出した大学での対策(案)

- 各大学の自己努力
  - ✓ 著しい体力差(教職員)
- 乏しい情報共有
  - ✓ 類似被害の多発
- 多様化するネットワーク利用
  - ✓ 在宅学習環境の普及
  - ✓ モバイル機器の持ち込み
  - ✓ OA機器などのネット接続

→困難な自力対策

- SINETのセキュリティ監視
  - ✓ 商用・海外接続での攻撃防止
  - ✓ 各大学のセキュリティ監視支援
- 情報共有の枠組み構築
  - ✓ 関係機関の連携促進
- セキュアな接続環境提供
  - ✓ 攻撃防止能力の向上
  - ✓ 速やかな事故対応

→学術機関全体の底上げ

# 大学CSIRTの立ち上げ支援と連携

- SINET5による接続形態の変更
  - 全ての大学が各県のDCに接続
  - DCで流量監視→不審な動きの察知→当該大学に連絡
- 原則として、当該大学のCSIRTが現場対応
  - 運用委託企業との連携が重要
    - 守秘義務/契約による自主的対応への足かせ
  - 一つの企業が複数の大学の運用を担当
    - 類似事案を把握している可能性大
- 大学間の直接の情報交換は難しい
  - 私情協やSINETを通じた情報交換
  - 運用委託企業の技術レベルの底上げ

# まとめ

- 標的型攻撃
  - 第一波攻撃の検知と被害防止は極めて困難
    - 一人でも突破されると組織内NWへの侵食開始
    - 内部NWの監視が必須に
      - ✓ VLAN＋アクセス制御＋巡回監視
  - クラウド時代の到来
    - サーバだけでなくクライアントもVM化
    - どこのHWで稼働しているのか？
    - バランスの取れたインシデントレスポンス耐性の確立
- 新たなディバスのネットワーク接続急増
  - 悪意の無い探査活動の急増
- 新たな大学間連携の枠組み構築