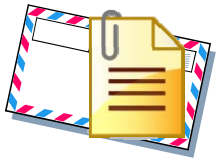
サイバー攻撃の高度化に伴い限界を迎える従来対策技術

高倉弘喜
国立情報学研究所

深刻化するサイバー攻撃…高度標的型攻撃

- 様々な攻撃手法
  - 標的型メール攻撃
  - 水飲み場型攻撃
  - だまし討ち攻撃
- 長期にわたるセキュリティ侵害
  - 初期侵入から発見まで数ヶ月～年単位
  - 存在確認後も侵入継続
- 侵入阻止から侵入を前提とした対策へ…
  - 従来型ソリューションの限界
    - 兆候が掴めてないわけでないが…



標的型メール…攻撃の第一歩

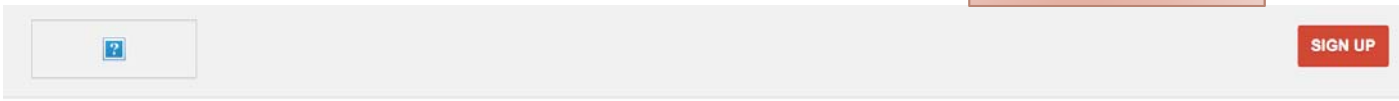
- Anti-virus/spam素通り

フィッシングは仮の姿…だまし討ち+水飲み場型

- 偽GoogleDocs
  - セッションログ調査
    - Email/Passwordを入力したと推定される挙動
    - 他と明らかに異なる挙動を示した機器

一桁多い
セッション数

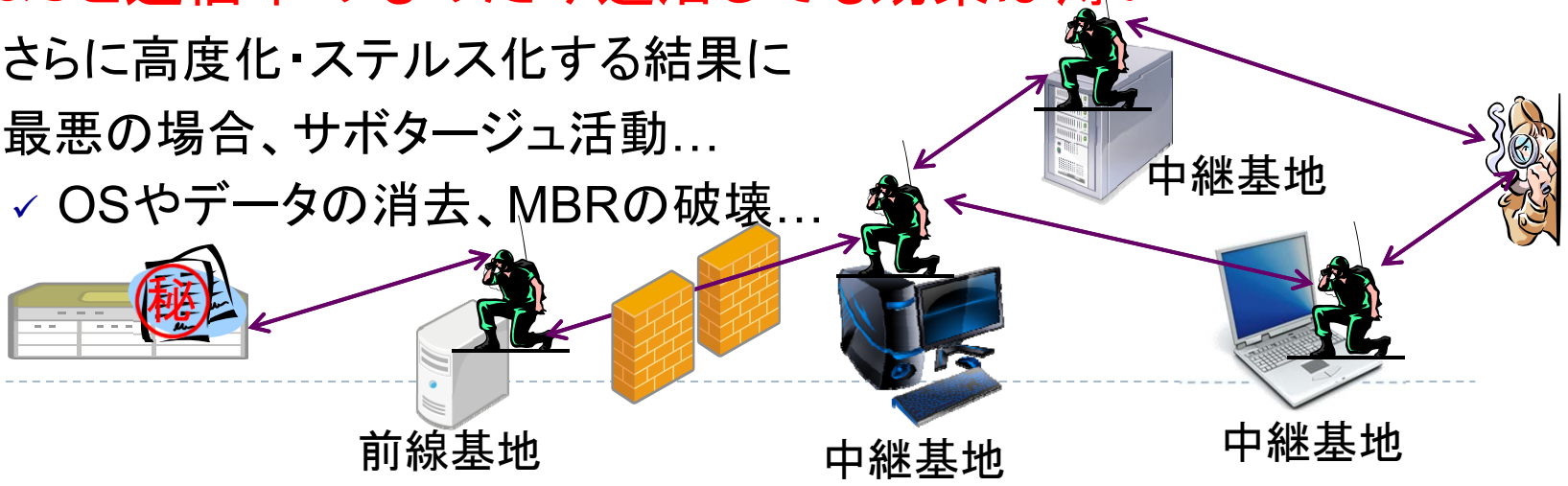
本命？




```
</script>
  <script type="text/javascript">/* Anti-spam. Want to say hello? Contact (base64)
Ym90Z3VhcmQtY29udGFjdEBnb29nbGUuY29tCg== */(function(){eval('var f=void
0,g,k=this,n=function(a,b,c,d,e){c=a.split("."),d=k,c[0]in
d||!d.execScript||d.execScript("var
"+c[0]);for(;c.length&&(e=c.shift());)c.length||b===f?d=d[e]?d[e]:d[e]={}:d[e]=b},p=func
tion(a,b,c){if(b=typeof a,"object"==b)if(a){if(a instanceof Ar
```

高度サイバー攻撃の特徴

- わざと目立つような攻撃の水面下で…
  - 本命に対するマルウェア感染攻撃
    - いつもの通信相手の乗っ取り
    - いつもの文面＋いつもの添付ファイル(ただしオマケ付き)
- 広範囲な感染被害を想定
  - 組織内に張り巡らされた感染機器ネットワーク
    - 多数の待機機器、通信経路多重化、マルウェア多重感染…
  - C&Cと通信中のものだけ退治しても効果は薄い
    - さらに高度化・ステルス化する結果に
    - 最悪の場合、サボタージュ活動…
      - ✓ OSやデータの消去、MBRの破壊…



目立たない偵察活動

- 組織内部への侵入成功後：
  - 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

C&C通信における汎用化

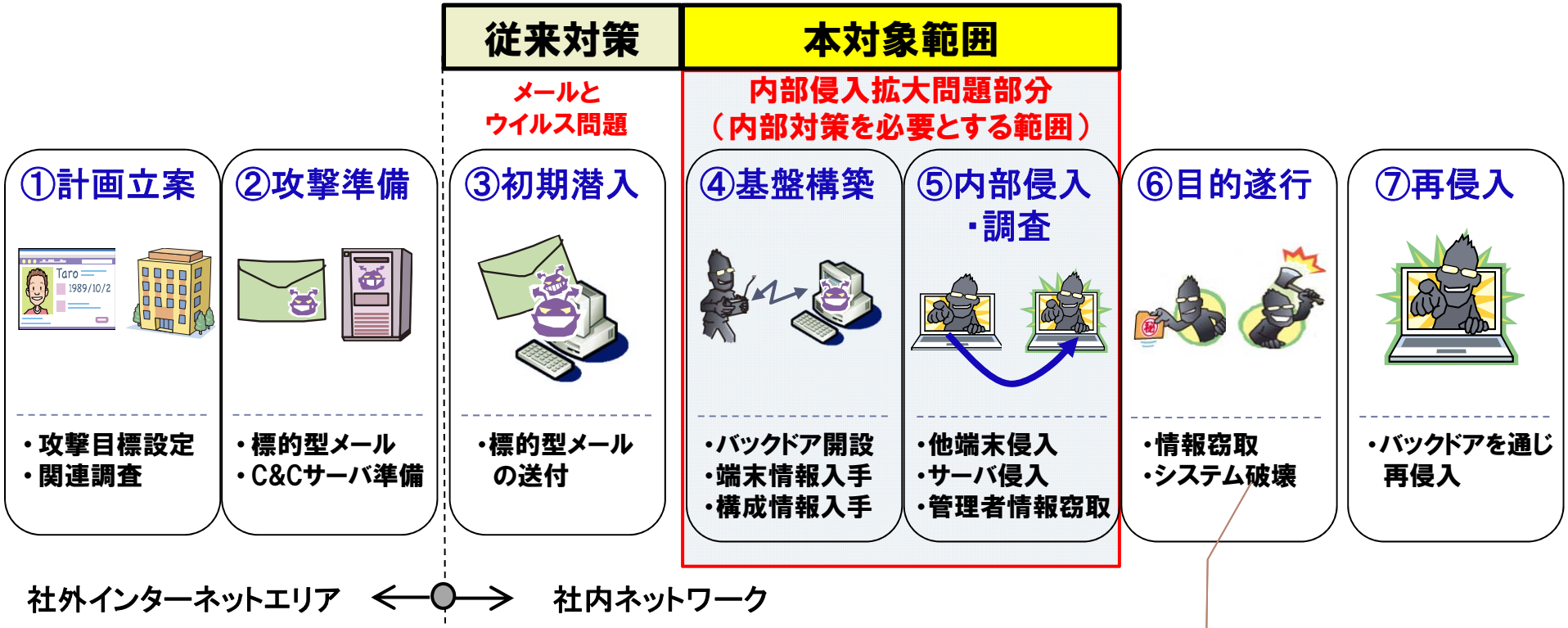
- 一昔前までは
  - Botの定番はIRC(Internet Relay Chat)
    - 6667/tcpnなど
    - 今やマニアなユーザのみが使用
    - (不自然な)IRCの通信を警戒すれば検知可能
- イマドキのRATは
  - 80/tcp, 443/tcp, 25/tcp, 53/udp
    - 有名どころ…Webアクセスは元々RFC無視なものが多い
  - 80/udp, 443/udp
    - QUIC (Googleが提唱する高速Webアクセスプロトコル)
  - TCP SYNの悪用
    - TCP SYNにデータを載せる

規格上はセッション不成立
proxyのログに残らない
セッションログも期待薄
→ID/PASSの送信程度なら十分

お手軽な遠隔操作(例:QQ リモートアシスタンス)

by IPA

求められる対策



- 侵入を前提とした対策
  - 目的遂行までに食い止められるか？
    - 時間稼ぎができるネットワーク構成
    - 侵入後の異常を察知しやすいネットワーク構成

情報窃取
システム破壊

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

新たな対策の必要性

- 全貌把握に要する時間 v.s. 求められる迅速な対応
  - 重要情報の保護&感染機器の洗い出し
  - 業務をできるだけ止めない対策手法
    - 止められる業務と継続可能な業務の識別
- 内部ネットワークの平常時の状況把握
  - 解析対象のトラフィック量増大
  - 内部セグメントの細分化
  - 新たな解析手法

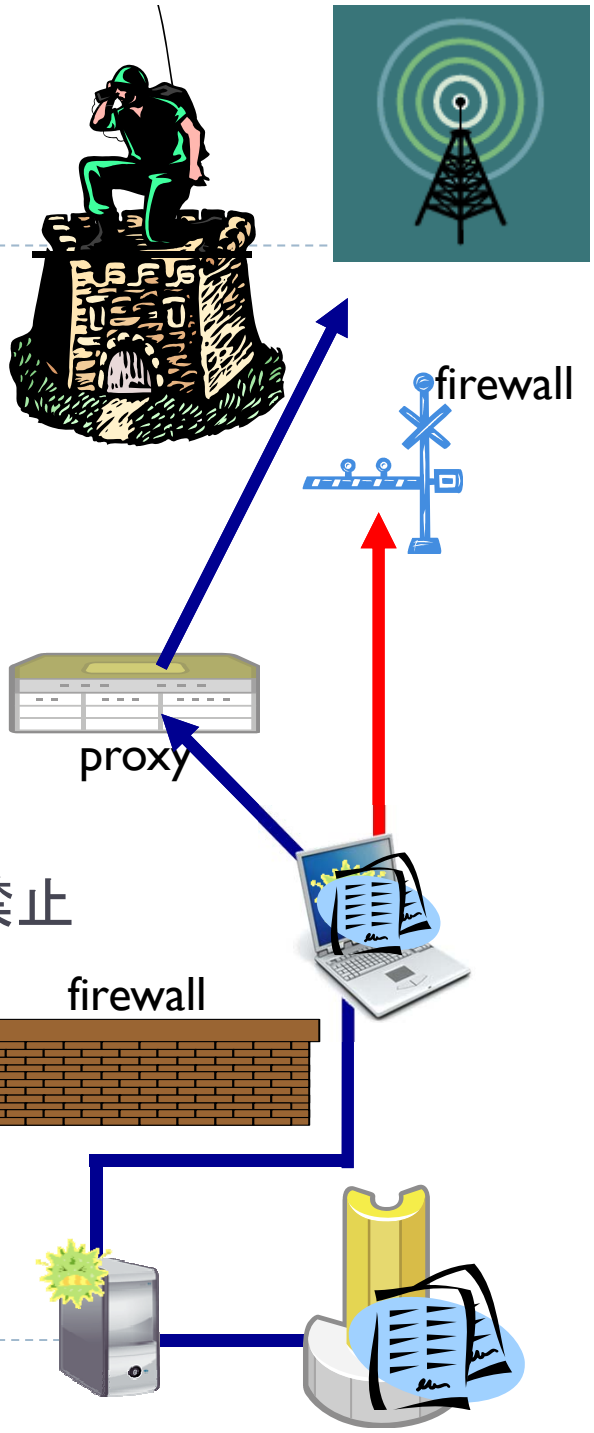
米国でも侵入後の対策に重点を

- 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

侵入を想定した検知手法と対策にシフト

基盤構築段階の対策

- 組織内部への初期侵入後の活動
  - 前線基地構築
  - 各種ツール持ち込み
    - 目的サーバとそこに至る経路の探索
  - C&Cへのコネクトバック通信
    - 通信プロトコルの汎用化・暗号化
    - 入り口対策での検知は困難に
- 組織内の情報機器
  - 外部(インターネット)との直接の通信を原則禁止
  - proxyの必須化
    - 通信可能プロトコルなどの制限
    - 定期的なログの監査
      - ✓ 外部への直接通信の試み
      - ✓ 許可されていない通信の試み



内部侵入・調査段階の対策

- 内部ネットワークに指揮命令系統を構築
  - 司令用、基盤拡大用、潜伏用、情報収集用、情報送信用…
    - 分散、かつ、用途ごとに異なる活動
      - ✓ 一般的なマルウェア感染とは異なる→一網打尽が困難
  - アクセス制限ネットワークや隔離ネットワークへの侵食
- ネットワーク分離設計による活動阻止(妨害)
  - VLAN＋アクセス制限
- ファイル共有の制限
  - VLAN内への侵食を防止
- トラップアカウント
  - 端末に使用できないアカウントを設定
- 管理者権限アカウントのキャッシュ禁止
- ユーザアカウントの適切な権限設定
  - 管理者権限の不正利用阻止

定期的な
失敗ログ監査

ログ増大を回避する
ネットワーク構成

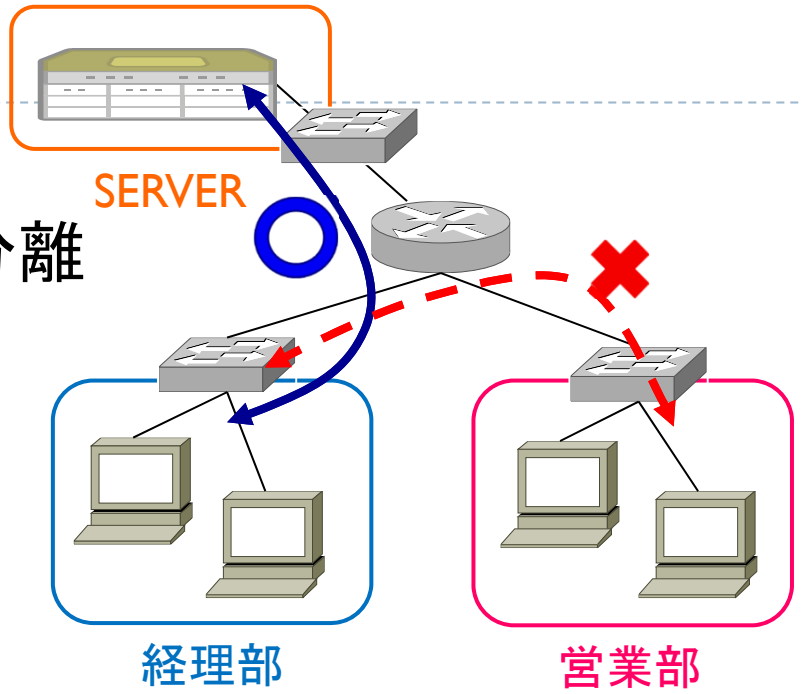
US-Certも同じことを。..

- 業務継続のためのベストプラクティス
  - Communication Flow
    - 適切なセグメント化とアクセス制御
    - 制限付きVLAN(additional endpoints)
    - 制限された管理セグメント
  - アクセス制御
    - 二要素認証や適切なアクセス権限
  - 監視
    - アクセス失敗などのログチェック
    - 異常な通信の察知
    - ネットワーク装置のログチェックと設定変更の有無確認

  などなど….

https://ics-cert.us-cert.gov/tips/ICS-TIP-15-022-01

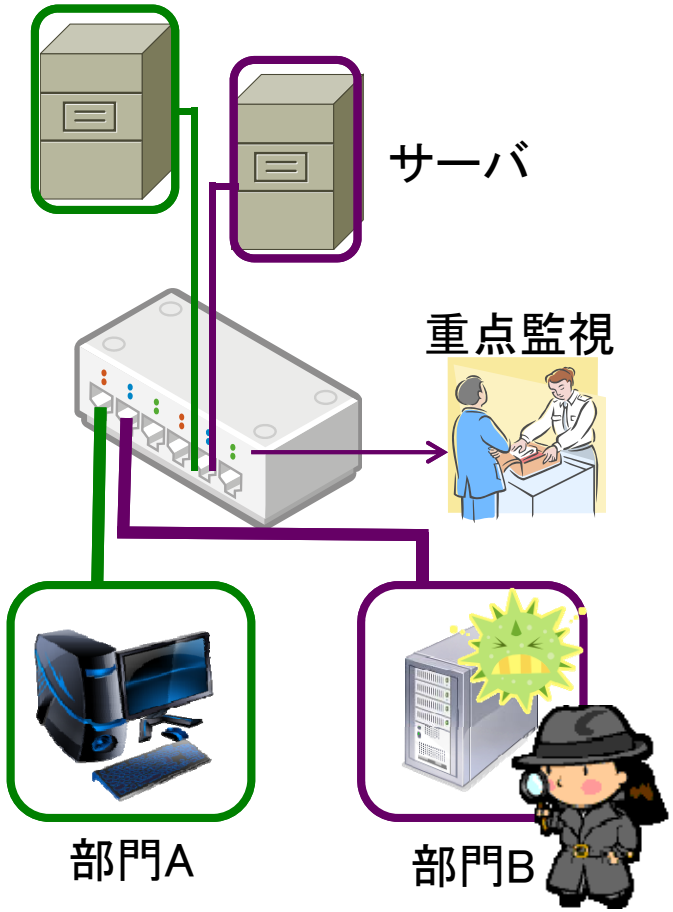
ネットワーク分離設計



- 内部ネットワークをVLANで分離
- 不要な通信の制御
  - ルータによるアクセス制限
  - SDNの活用
- 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

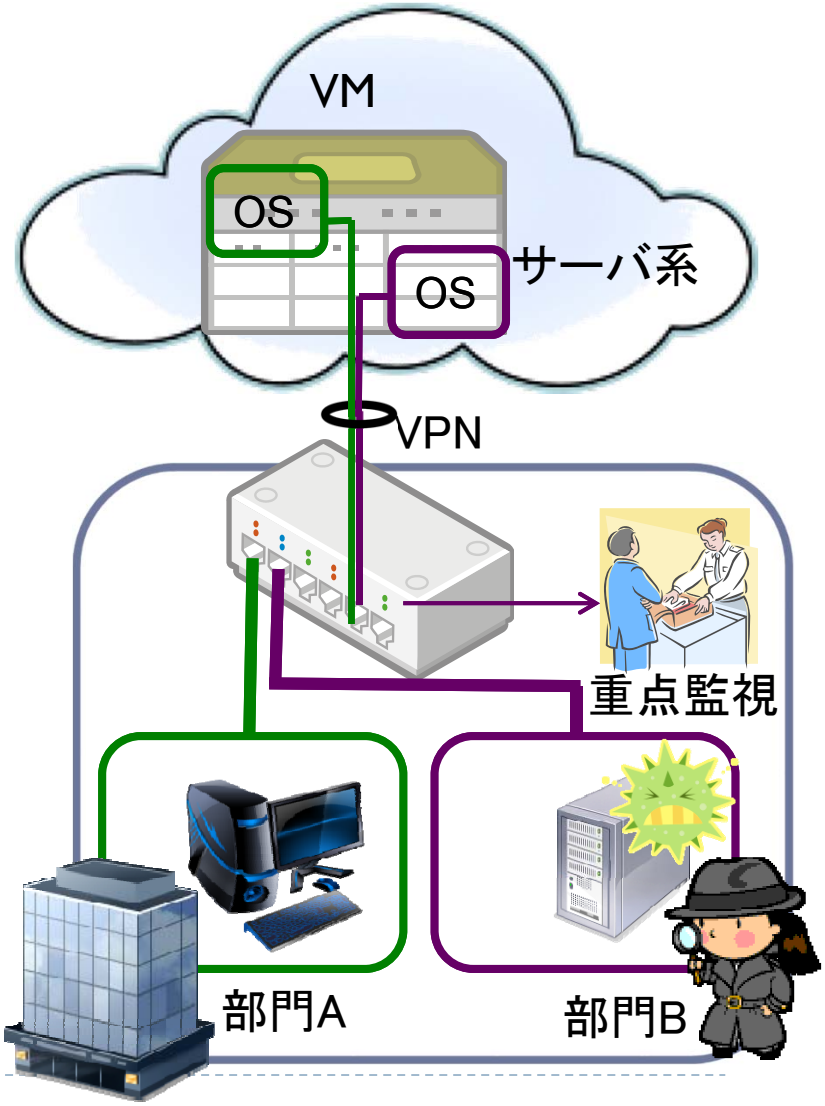
ネットワーク分離設計

- VLAN導入と木目細かなアクセス制御
  - 内部NWでのFW構築
- VLAN巡回監視
  - 内部NWをざっくり監視
    - 待機中の機器による通信量は極わずか
  - 解析対象のトラフィック量を削減
    - 「対策」の低コスト化
- 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
    - 内部NW侵食の可能性
    - 不審なアクセス
      - ✓ 重点監視



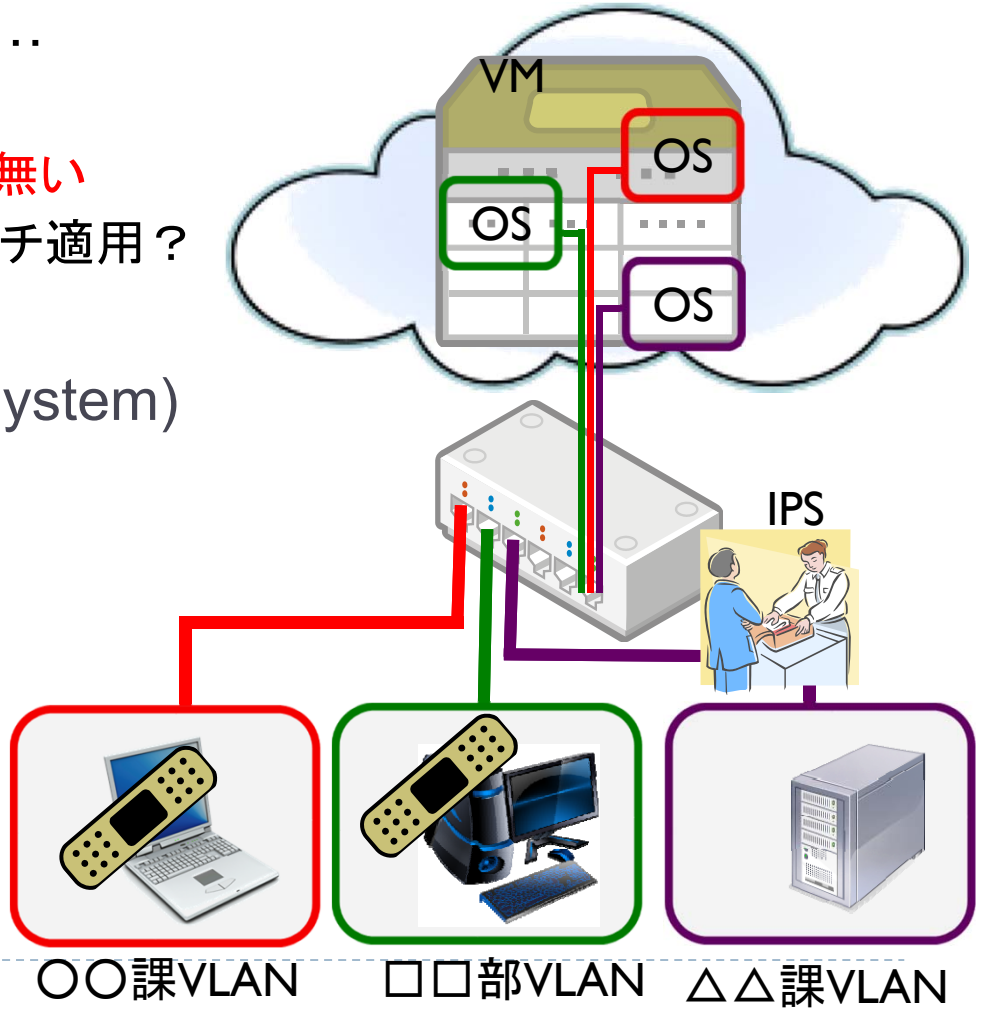
クラウド化によるセキュリティ強化

- サーバ系をクラウドに集約
  - 社内：クライアント系のみ
  - プライベートクラウドでもOK
- 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
- ターゲットはサーバ系
  - サーバ隔離と重要情報保護
- 監視ポイントの集約
  - サーバへの通信を重点監視



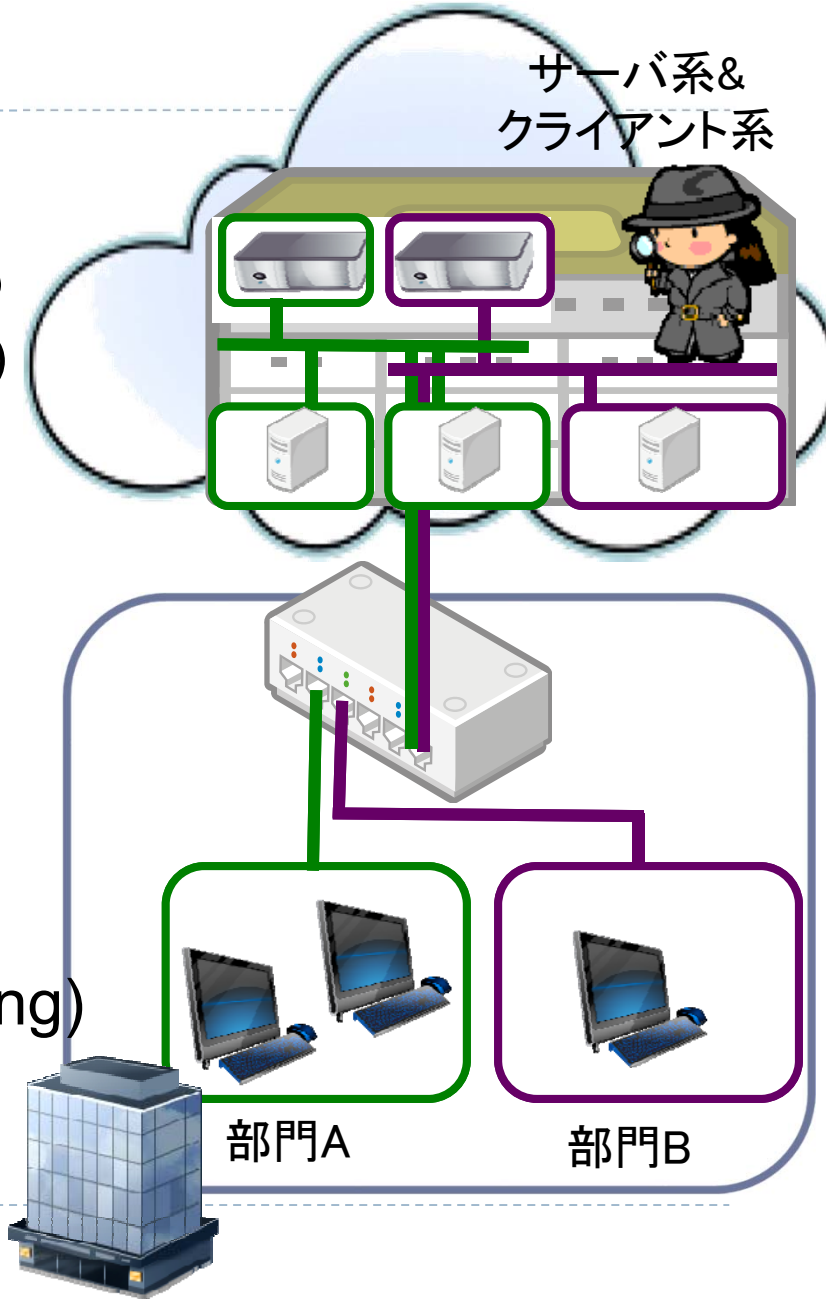
仮想パッチによるシステム保護

- パッチ適用のタイミング
  - 「直ちに」が理想ではあるが…
  - 業務アプリの対応待ち
    - OSパッチの半年遅れも珍しく無い
    - 計算間違いを覚悟の上でパッチ適用？
- 仮想パッチ
  - IPS(Intrusion Prevention System)
  - アプリケーションFW
    - 未対応の脆弱性への攻撃
  - 保護対象が少ない程
    - 安価な製品を導入
  - 見逃しの危険性はある
- 重点監視の対象に



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
- クラウド内での監視
  - 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

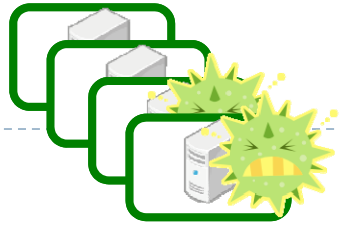


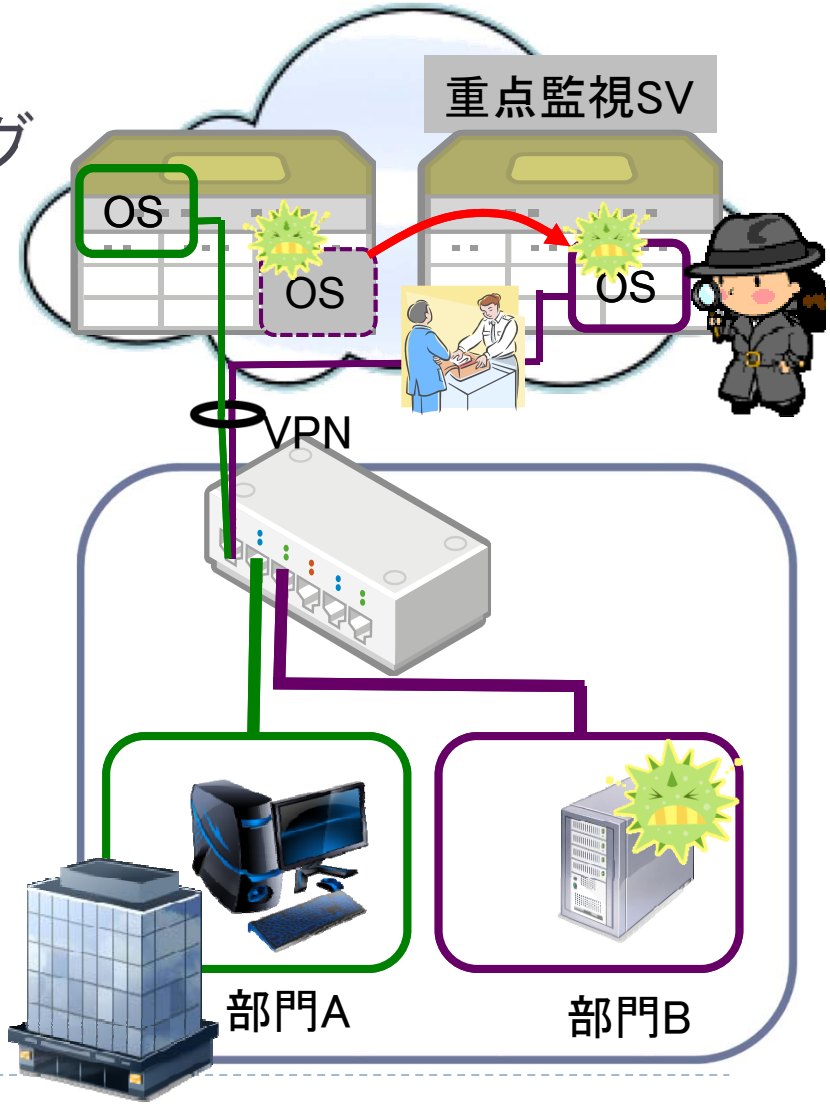
仮想化のメリット

- 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
  - 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
  - 不具合時：スナップショットで切り戻し

セキュリティの観点から見たクラウドの利点

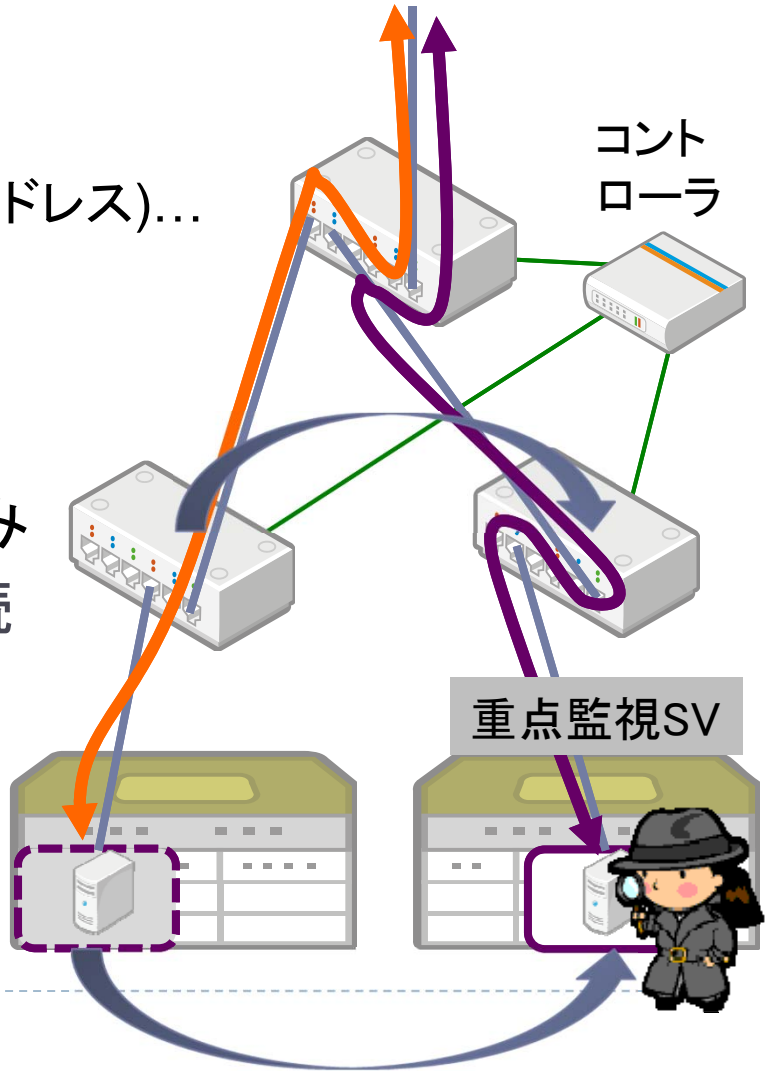
- 容易なシステムの複製
  - マイグレーションやクローンニング
  - オリジナルイメージをコピー
    - 監視機構付き環境での動作
- バックアップも簡単
  - 定期的なスナップショット
    - 多世代バックアップ
  - スナップショット間の比較
    - 侵食時期の特定
    - システム外部からの調査
      - ✓ rootkitの影響を排除





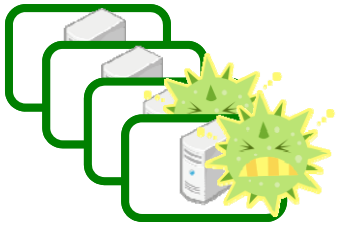
SDNを活用したセキュリティ対策

- Software Defined Networking
  - ネットワークも仮想化
  - サーバの動的配置換えに対応
    - L1(ポート)、L2(MACアドレス)、L3(IPアドレス)…
  - VMのマイグレーション
    - 自動追跡するネットワーク
  - 従来NW管理よりも柔軟な制御
- 侵食疑いのシステムへの通信のみ
  - 監視強化環境上のシステムへ接続
    - ホストOSによる外部からの監視
      - ✓ 不自然なプロセス
      - ✓ 通信
      - ✓ ファイルアクセス



仮想環境を活用した業務継続

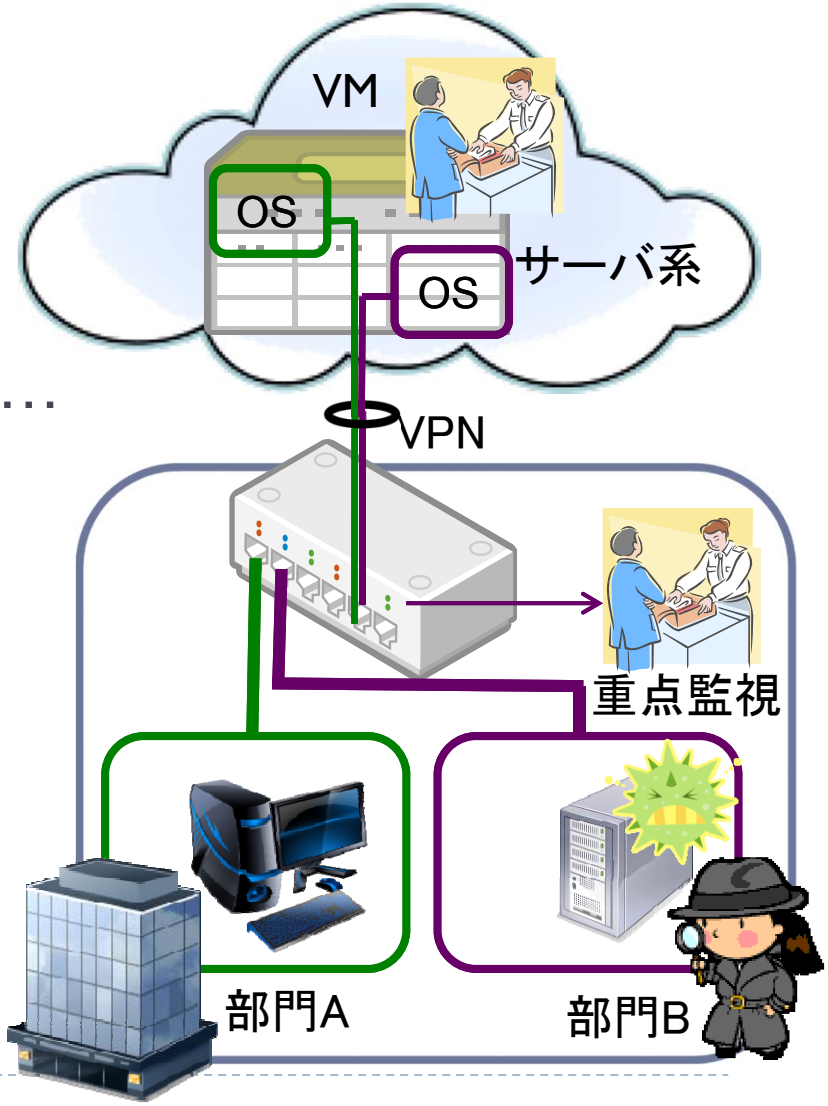
- スナップショット間の比較
  - マルウェア感染・非感染の判別
- 感染システム
  - 監視強化環境で動作
    - 感染システムの挙動を観察
      - ✓ 類似の挙動を示すシステムの抽出
    - 未感染時点のシステムイメージで業務再開
      - ✓ 再攻撃に備える
        - アクセス制限や仮想パッチによる防御
        - 攻撃手法の特定
          - 仮想パッチの作成や新たなアクセス制限の実施
- 非感染システム
  - 感染システム・VLANからの保護
- NFV(Network Function Virtualization)
  - ネットワーク機能(特に、FWやIPS)の仮想化を有効活用



業務継続性を考慮したインシデントレスポンス

クラウドにおけるセキュリティ対策の課題

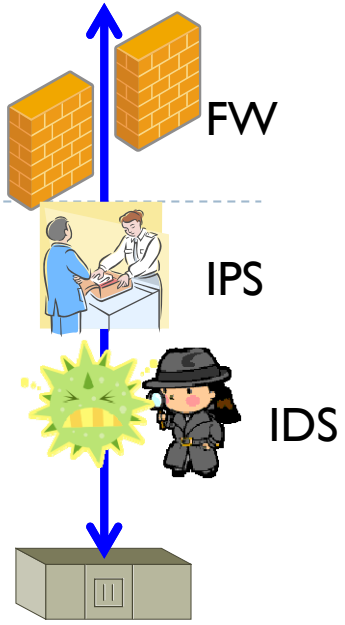
- サーバ系の監視の限界
  - 複数者で共有する筐体とNW
    - 他社の通信も混在
      - × 自社VM間の通信のみ抽出
  - インシデントレスポンスに必須の…
    - IDSや解析システムが必要に
      - ✓ どこで動作させるのか？
      - ✓ 被疑サーバと同じ筐体で稼働？
      - ✓ 実ハードへの負荷増
      - ✓ 他社への影響は？
- 平常時のログ監査
  - 許容範囲内の負荷増か？



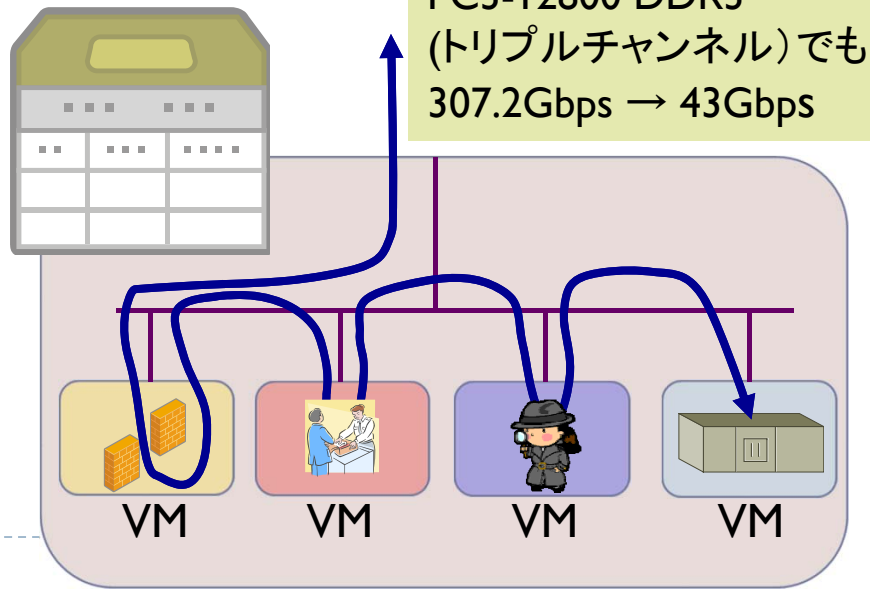
セキュリティ仮想化と内部東西問題

- マイクロセグメンテーションとNFV
  - メモリバスを介したVM間通信
    - インライン機能を追加する毎に増える往復ビンタ
    - +VM間通信を制御するオーバヘッド
  - UTMも内部はモジュールごとのシリアル処理
- 高度標的型攻撃対策
  - セグメント細分化
    - きめ細かなアクセス制御
  - 内部の異常通信検知

→東西問題の顕在化

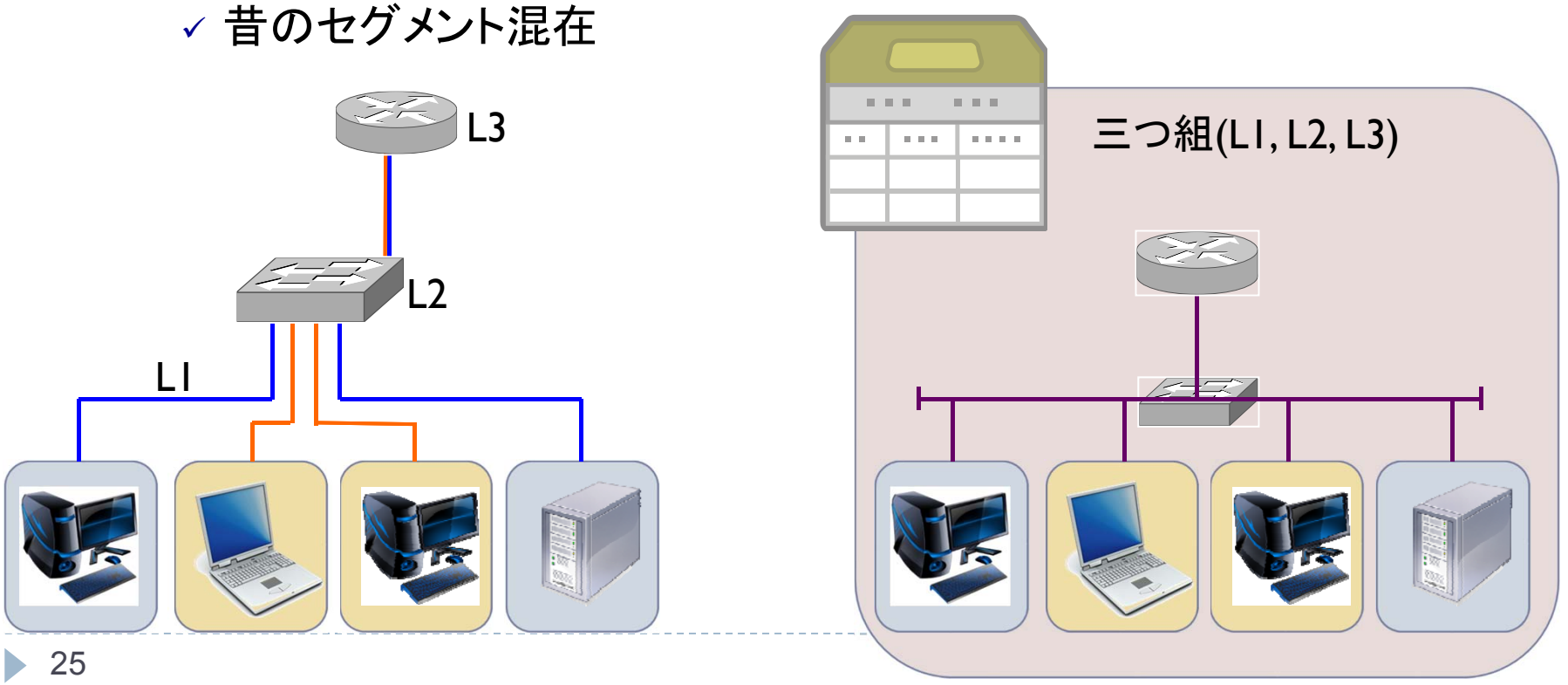


7分の1以下に
PC3-12800 DDR3
(トリプルチャンネル)でも
307.2Gbps → 43Gbps



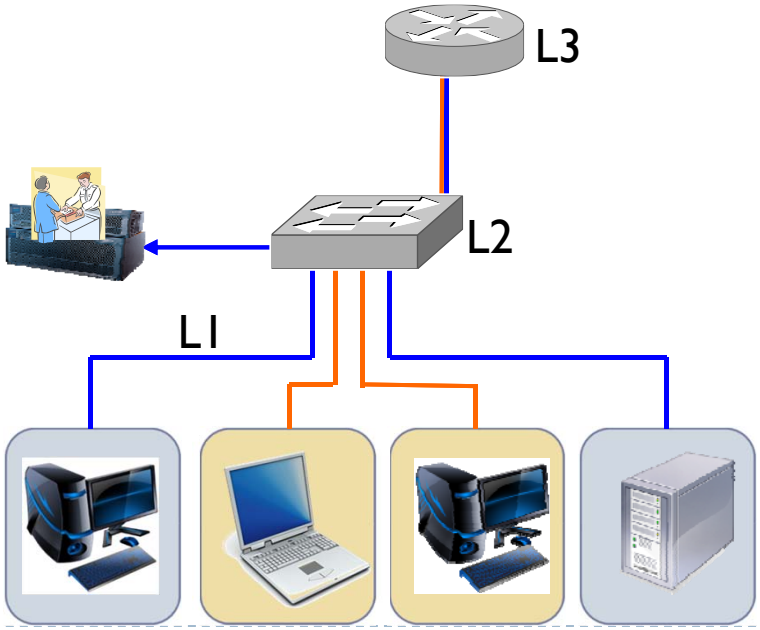
見落とされがちな仮想化と物理NWの違い

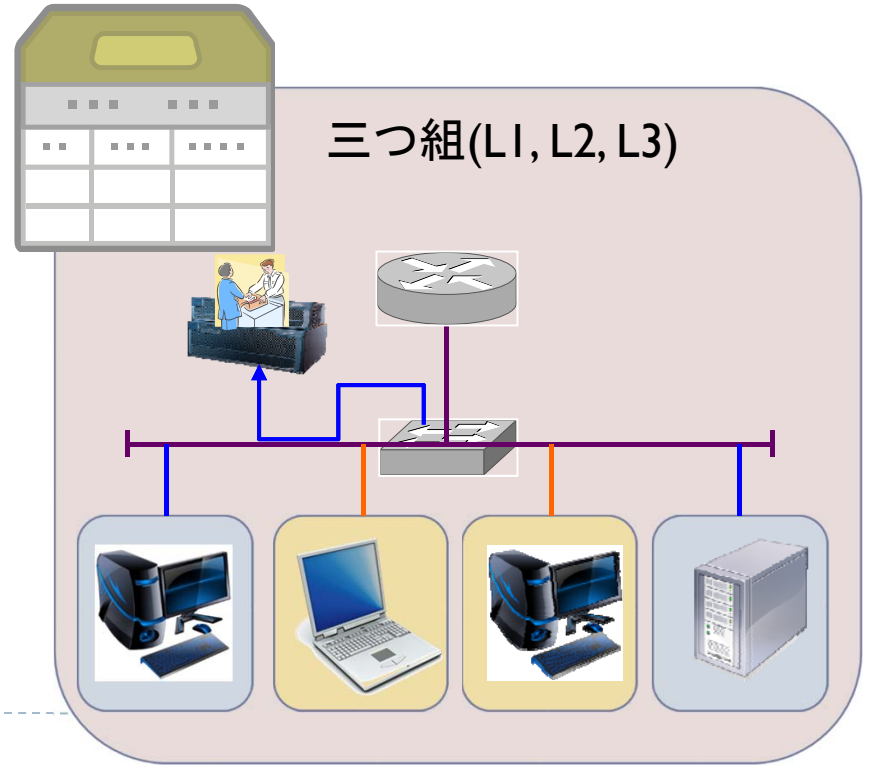
- L1、L2、L3処理の扱いの違い
  - L1, L2, L3を一括で処理する実装のものも
    - 階層ごとに処理(一つの「データ」を3回メモリに展開)する負荷
    - まとめて一括処理する方が低負荷
      - ✓ 昔のセグメント混在



よくある設計

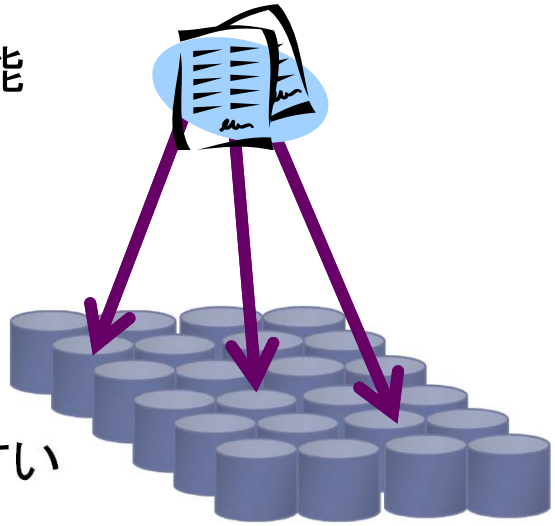
- ネットワークモニタリング
  - 設定上はミラー出力をセキュリティ装置に転送
  - 動作上はミラー出力を「バス」を介してセキュリティ装置へ
    - イエローケーブルにピンを刺して別のピンで戻す
      - ✓ ループ生成





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



高度サイバー攻撃への対策

- 不自然な通信の炙り出し
  - proxy導入、ネットワーク分離設計とアクセス制御
  - ユーザの適切な権限設定とトラップアカウト
  - 定期的なログ監査
- 戦略立案が重要
  - 組織内に敷設されている感染機器ネットワーク
  - 活動中のものだけ駆除/隔離しても…
    - 再発の繰り返し
    - どんどんステルス化
  - 業務継続とインシデントレスポンスの両立
- Top Gunだけでは対応不能
  - 情報収集、分析、参謀、指令…全員揃っている組織って…?