JPCERT/CCが見た、標的型攻撃の実態

一般社団法人JPCERTコーディネーションセンター
インシデントレスポンスグループ
久保啓司

JPCERT/CC とは

一般社団法人 JPCERT コーディネーションセンター

Japan Computer Emergency Response Team / Coordination Center

- https://www.jpcert.or.jp/
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウエアや情報システム・制御システム機器等の脆弱性への対応など**我が国における「セキュリティ向上を推進する活動」**を実施
- **サービス対象:**

  日本国内のインターネット利用者やセキュリティ管理担当者ソフトウエア製品開発者等（主に、情報セキュリティ担当者）
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**我が国の窓口となる「CSIRT」**
  ※各国に同様の窓口となる　CSIRTが存在する
  (例、米国のUS-CERT, CERT/CC, 中国のCNCERT, 韓国のKrCERT/CC)

経済産業省からの委託事業として、**サイバー攻撃等国際連携対応調整事業を実施**

JPCERT/CCの活動

インシデント予防 → インシデントの予測と捕捉 → 発生したインシデントへの対応

脆弱性情報ハンドリング

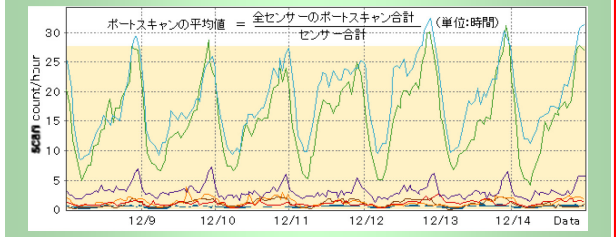
- 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- 関係機関と連携し、国際的に情報公開日を調整
- セキュアなコーディング手法の普及
- 制御システムに関する脆弱性関連情報の適切な流通

JVN Japan Vulnerability Notes

情報収集・分析・発信

定点観測（TSUBAME）

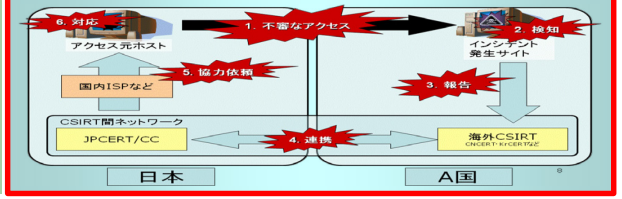
- ネットワークトラフィック情報の収集分析
- セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



インシデントハンドリング

（インシデント対応*調整*支援）

- マルウエアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- 再発防止に向けた関係各関の情報交換及び情報共有



早期警戒情報	重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信
CSIRT構築支援	海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援
制御システムセキュリティ	制御システムに関するインシデントハンドリング、情報収集・分析発信
アーティファクト分析	マルウエア（不正プログラム）等の攻撃手法の分析、解析
国内外関係者との連携	日本シーサート協議会、フィッシング対策協議会の事務局運営等
国際連携	各種業務を円滑に行うための海外関係機関との連携

標的型攻撃とJPCERT/CC

標的型攻撃への取り組み

- 国内外から標的型攻撃の情報提供
  - 海外セキュリティベンダーから
  - 被害組織から
  - 被害組織の分析結果から
- 認知できるのは攻撃の断片のみ（些細な情報）
  - C2との通信
  - マルウエア検知情報
- 被害組織にリスクを認識してもらうまでがミッション
  - 被害組織の調査に協力
    - ログ解析、フォレンジック、マルウエア解析
  - 被害組織がリスクを認識すればセキュリティベンダーへ引き継ぐ

ところで

標的型攻撃 ≒ APT攻撃？

- 今日のテーマは「APT攻撃」です
  - 攻撃者の目的は情報窃取
    - いわゆるespionage
  - 攻撃者は見つからないように行動
  - システム運用・ネットワーク運用に障害は発生しない

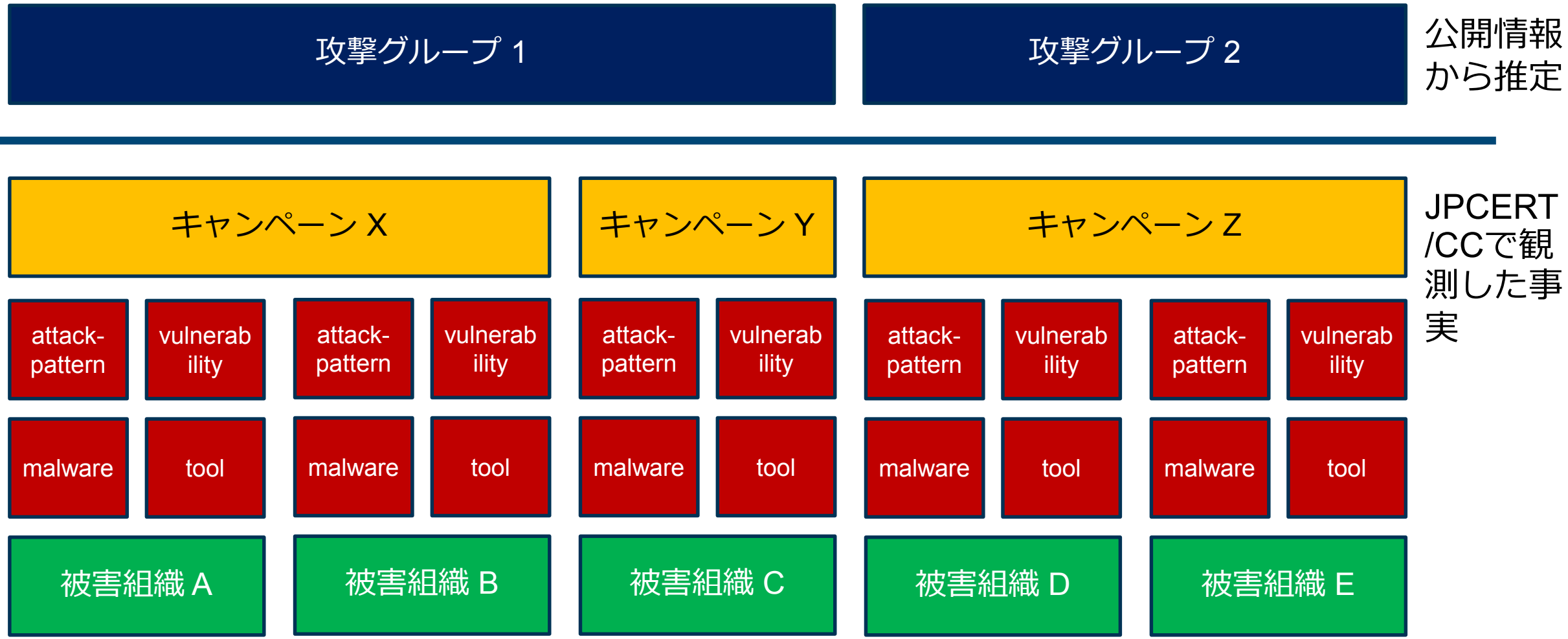
  ∴対応が非常に難しい

APT攻撃キャンペーン

2017年にJPCERT/CCが対応した
おもなAPT攻撃キャンペーン

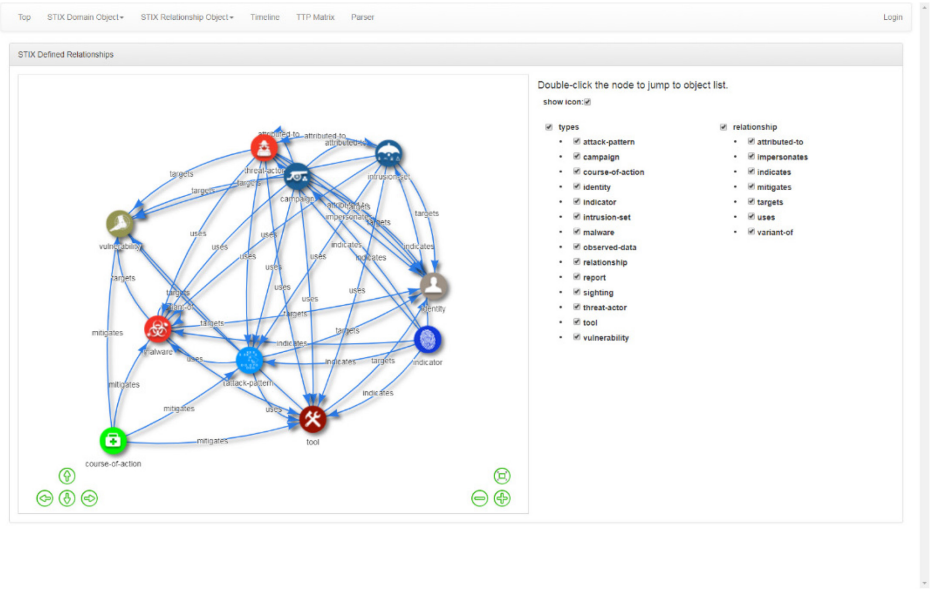
- Tick/Daserf
  - Tick (Symantec)
  - BRONZE BUTLER (Secureworks)
  - REDBALDKNIGHT (TrendMicro)
- Winnti
  - Winnti (Kaspersky)
  - Axiom (Novetta)
- APT10
  - APT10 (FireEye)
  - menuPass (PaloAlto)
  - Cloud Hopper (PwC)

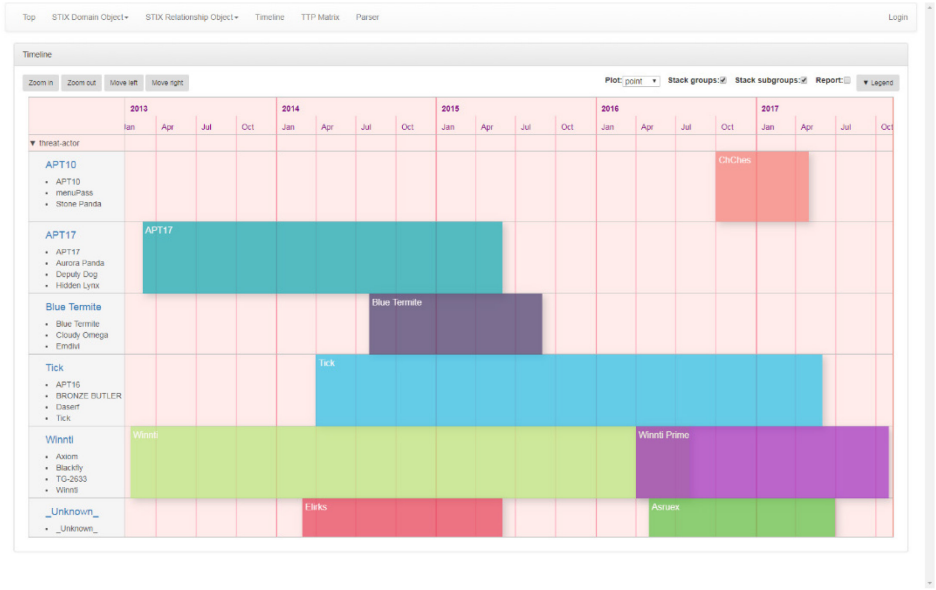
攻撃グループとキャンペーン



デモ 1: 攻撃キャンペーン、被害組織

- APT攻撃インシデント可視化システム
  - JPCERT/CCが対応したAPT攻撃インシデントをインプット
    - 攻撃キャンペーン、被害組織をタイムラインで表示
    - 被害組織の業種分類
      - 日本標準産業分類を参考に分類





攻撃手法の分析

TTP Matrix

被害組織で起こっていること（Kill Chain Phase）

侵入

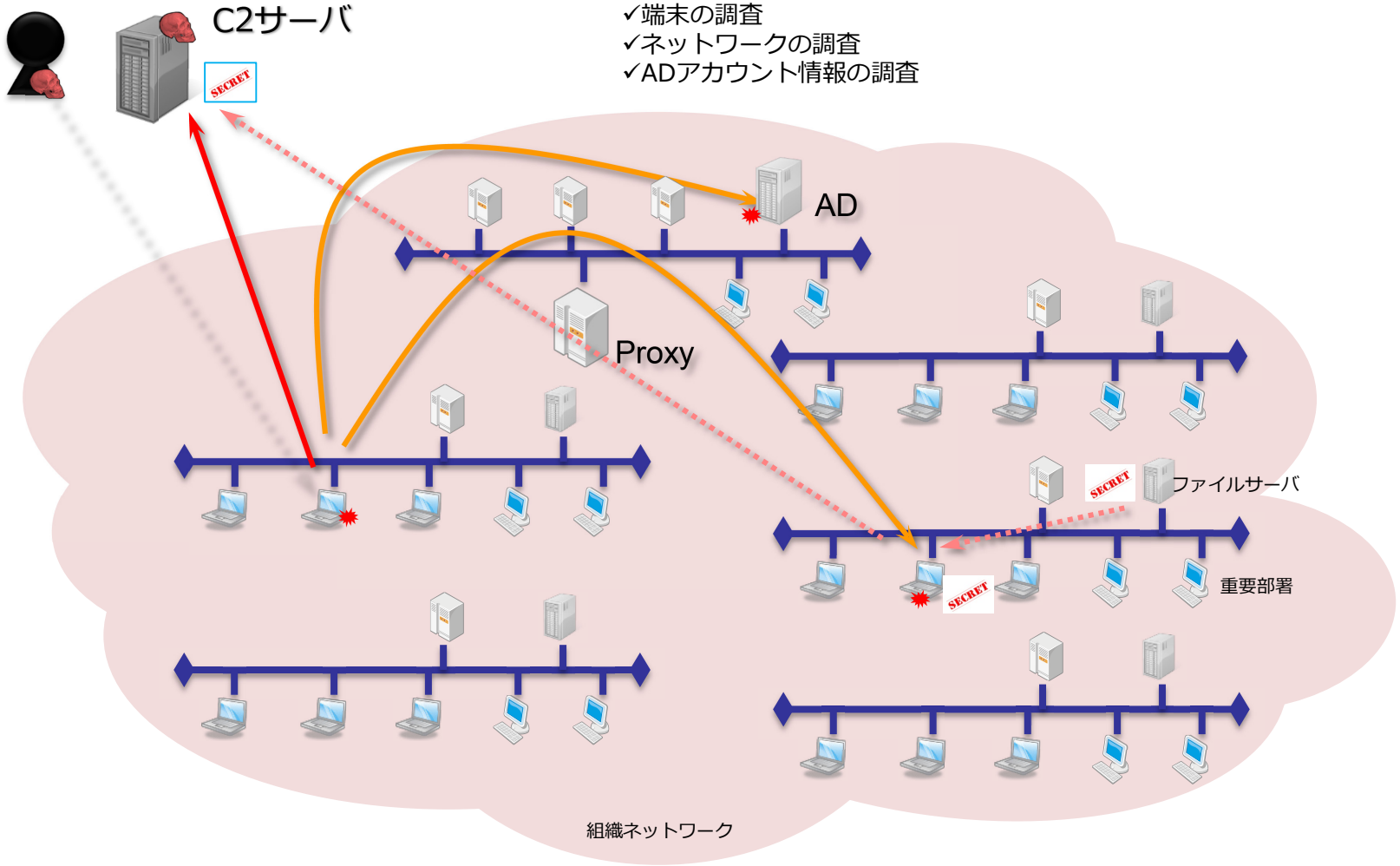
C2

偵察

Lateral Movement
権限昇格

情報窃取

潜伏



被害組織で起こっていること（Kill Chain Phase）

侵入

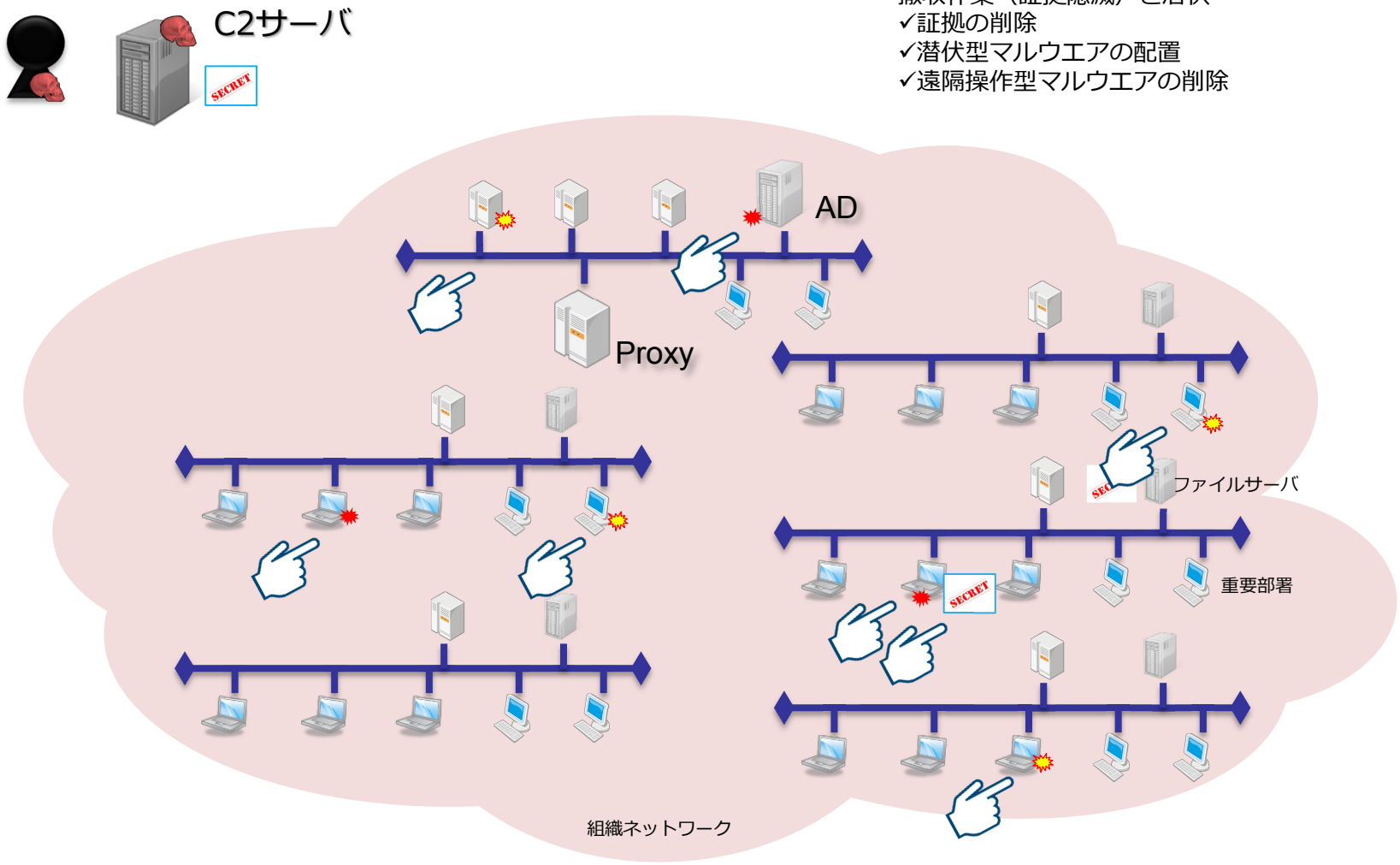
C2

偵察

Lateral Movement
権限昇格

情報窃取

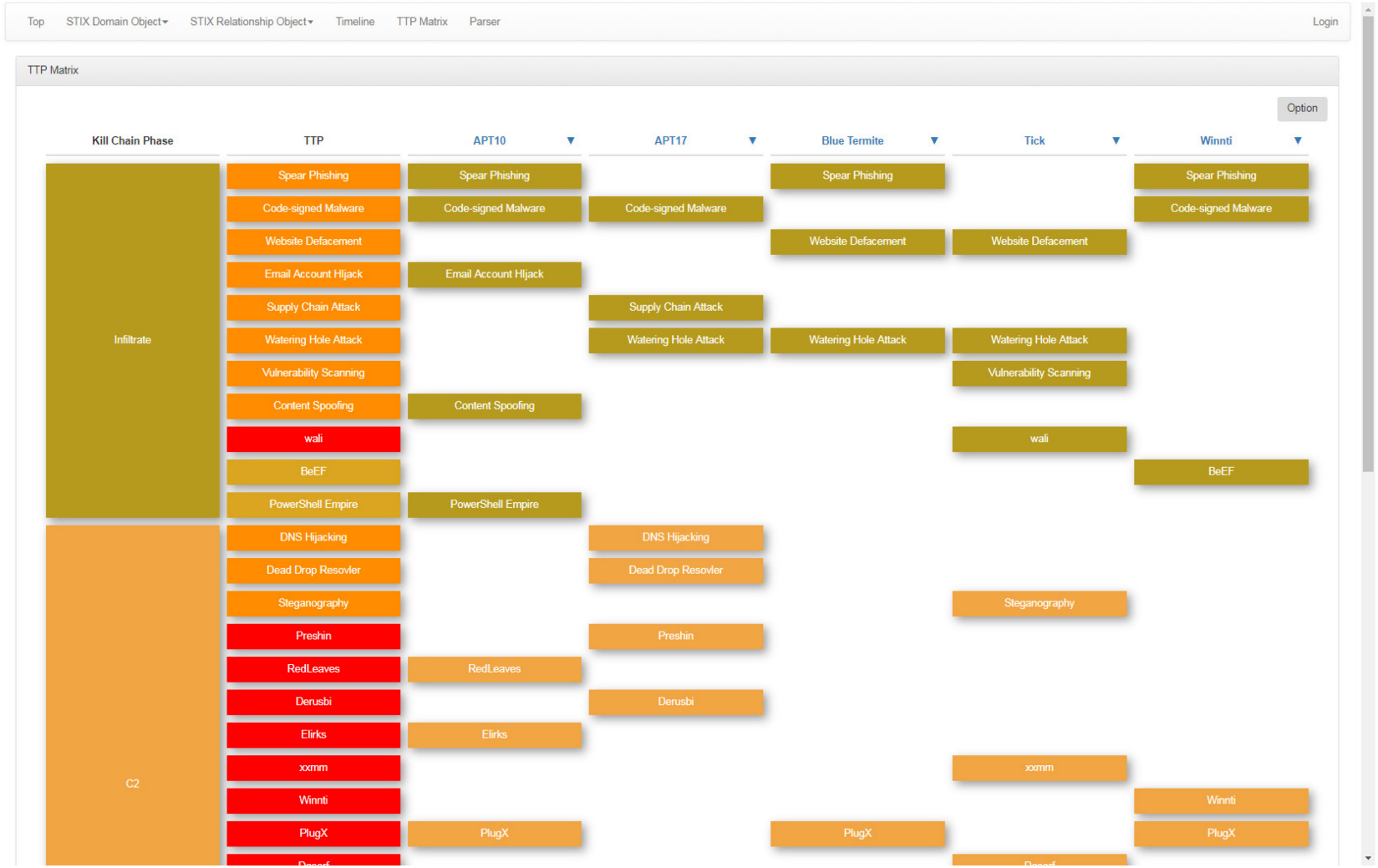
潜伏



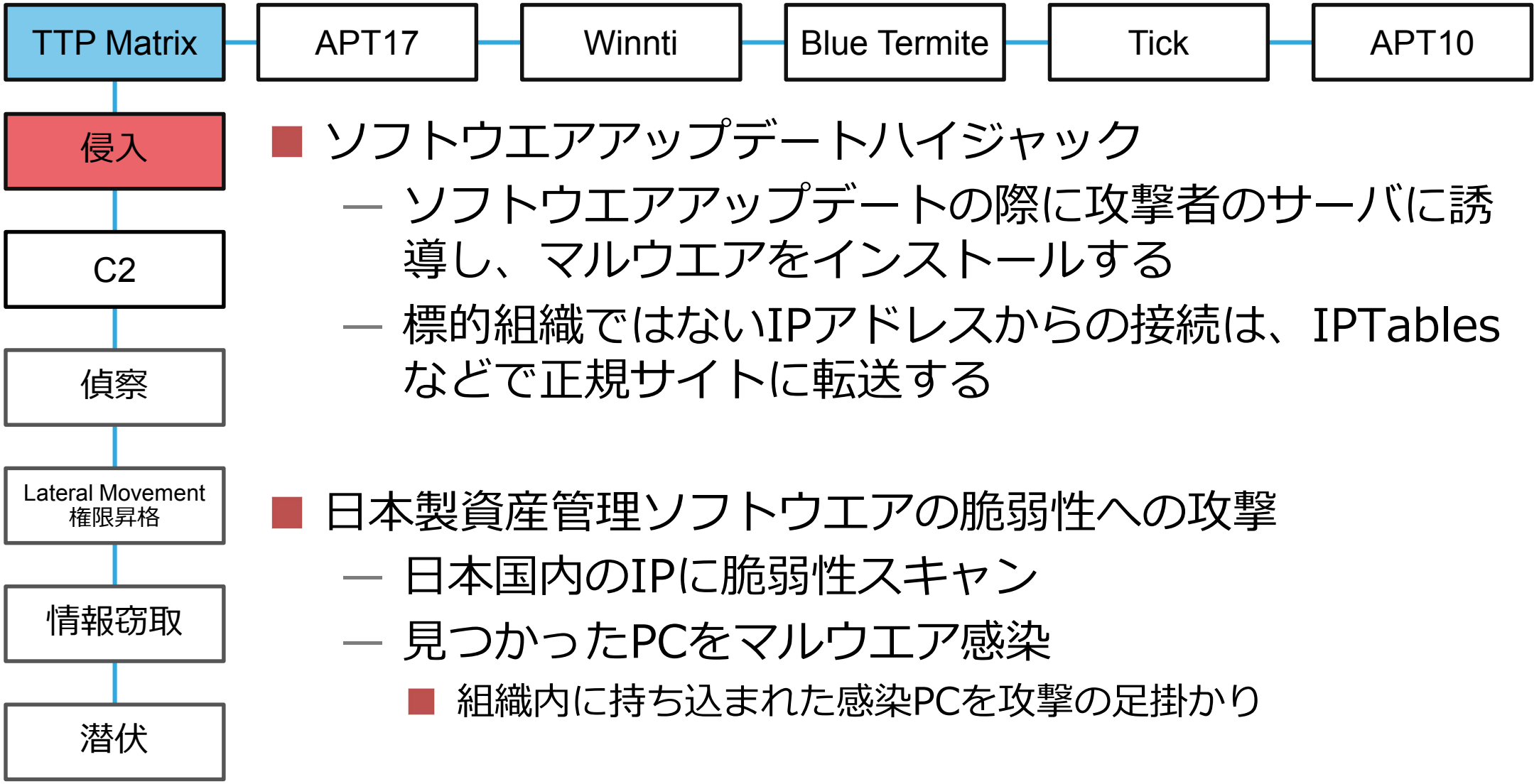
攻撃手法の分析 （TTP: Tactics, Techniques and Procedures ）

- 攻撃手法
  - 侵入の手口
  - 悪用する脆弱性
  - ツール
  - マルウエア
  - etc.
- 攻撃手法の分析
  - どの攻撃者がどの段階で何を使うか
    - TTP x Kill Chain Phase = 攻撃グループ？
  - 攻撃者間で類似性は見えるか
    - 同一の攻撃者である可能性は？

デモ 2: 攻撃手法の分析 （TTP Matrix）



侵入: 特徴的な攻撃手法



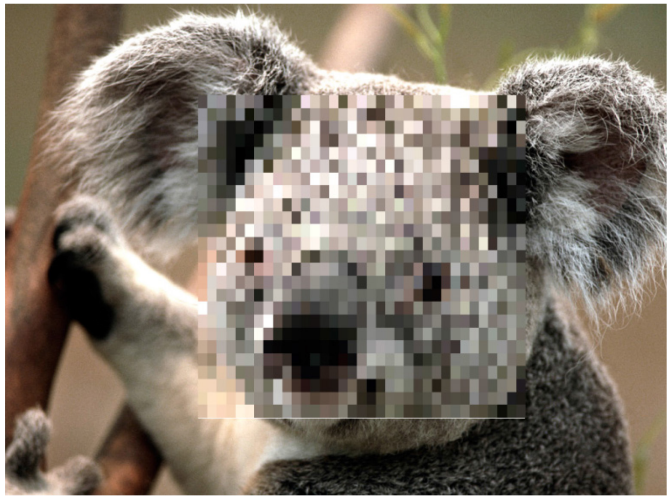
- ソフトウエアアップデートハイジャック
  - ソフトウエアアップデートの際に攻撃者のサーバに誘導し、マルウエアをインストールする
  - 標的組織ではないIPアドレスからの接続は、IPTablesなどで正規サイトに転送する
- 日本製資産管理ソフトウエアの脆弱性への攻撃
  - 日本国内のIPに脆弱性スキャン
  - 見つかったPCをマルウエア感染
    - 組織内に持ち込まれた感染PCを攻撃の足掛かり

C2: 特徴的な攻撃手法

TTP Matrix | APT17 | Winnti | Blue Termite | Tick | APT10

- 侵入
- C2
- 偵察
- Lateral Movement 権限昇格
- 情報窃取
- 潜伏

- 通信先の隠ぺい
  - Steganography
    - Webサイトの画像に通信先を埋め込み



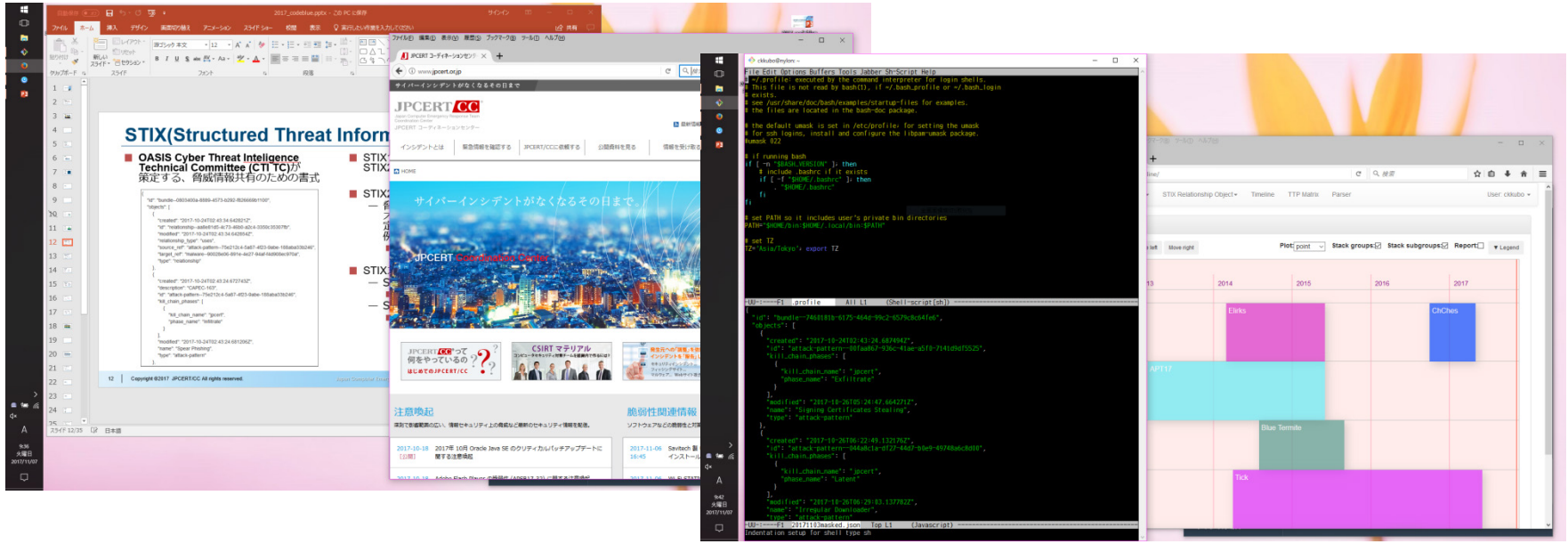
```
00c06f0: 989b 436e a9de 65c2 ba21 8816 cc64 aa6a  ..Cn..e..!...d.j
00c0700: dda7 ccbe eeea ee12 002e 1131 7761 787a  ...........1waxz
00c0710: 7371 3233 3452 4d36 4a52 4a58 4a53 4831  sq234RM6JRJXJSH1
00c0720: 4952 3947 6a42 3936 5953 6841 5852 4721  IR9GjB96YShAXRG!
00c0730: 2120 3433 3271 737a 7861 7731 2a45 5b7d  ! 432qszxaw1*E[}
00c0740: 9c6e d1cf f07f 14f2 58a1 7934 acb2 bc56  .n......X.y4...V
```

偵察: 特徴的な攻撃手法

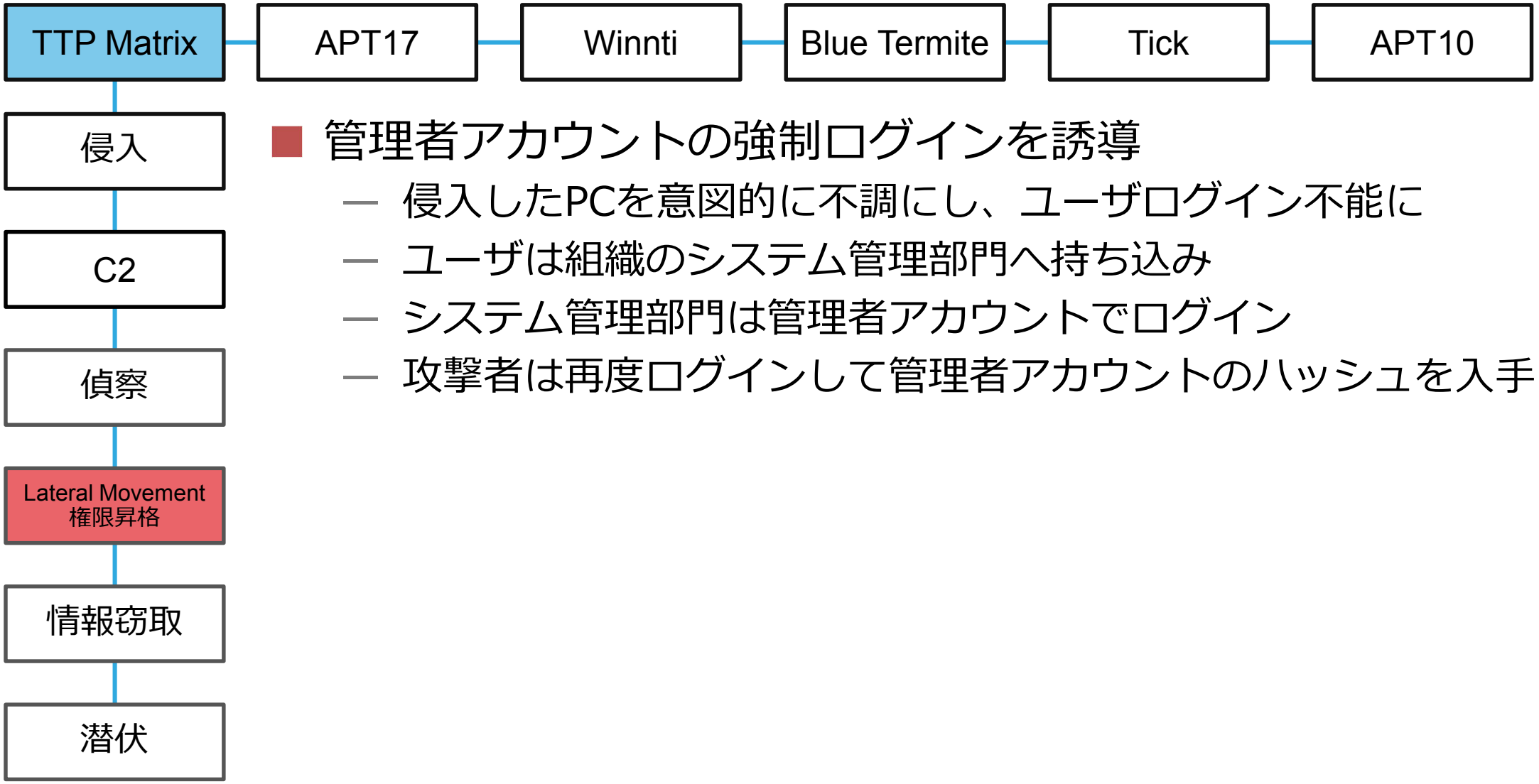
TTP Matrix | APT17 | Winnti | Blue Termite | Tick | APT10

- 侵入
- C2
- 偵察
- Lateral Movement 権限昇格
- 情報窃取
- 潜伏

- インシデント対応メンバーのPCへの侵入
  - 被害組織のインシデント対応状況の把握
  - デスクトップ操作画面の動画録画マルウエア

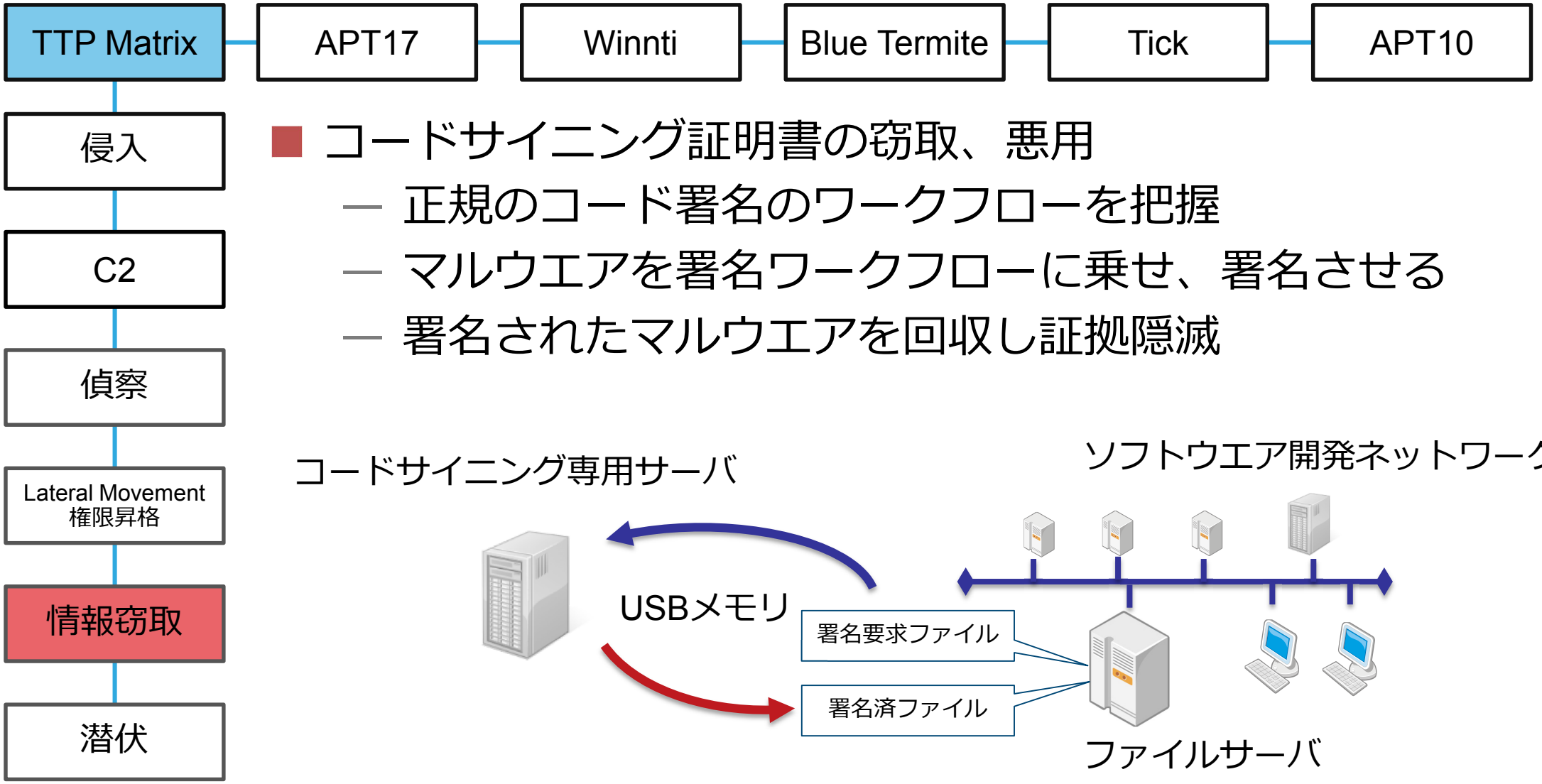


Lateral Movement, 権限昇格: 特徴的な攻撃手法



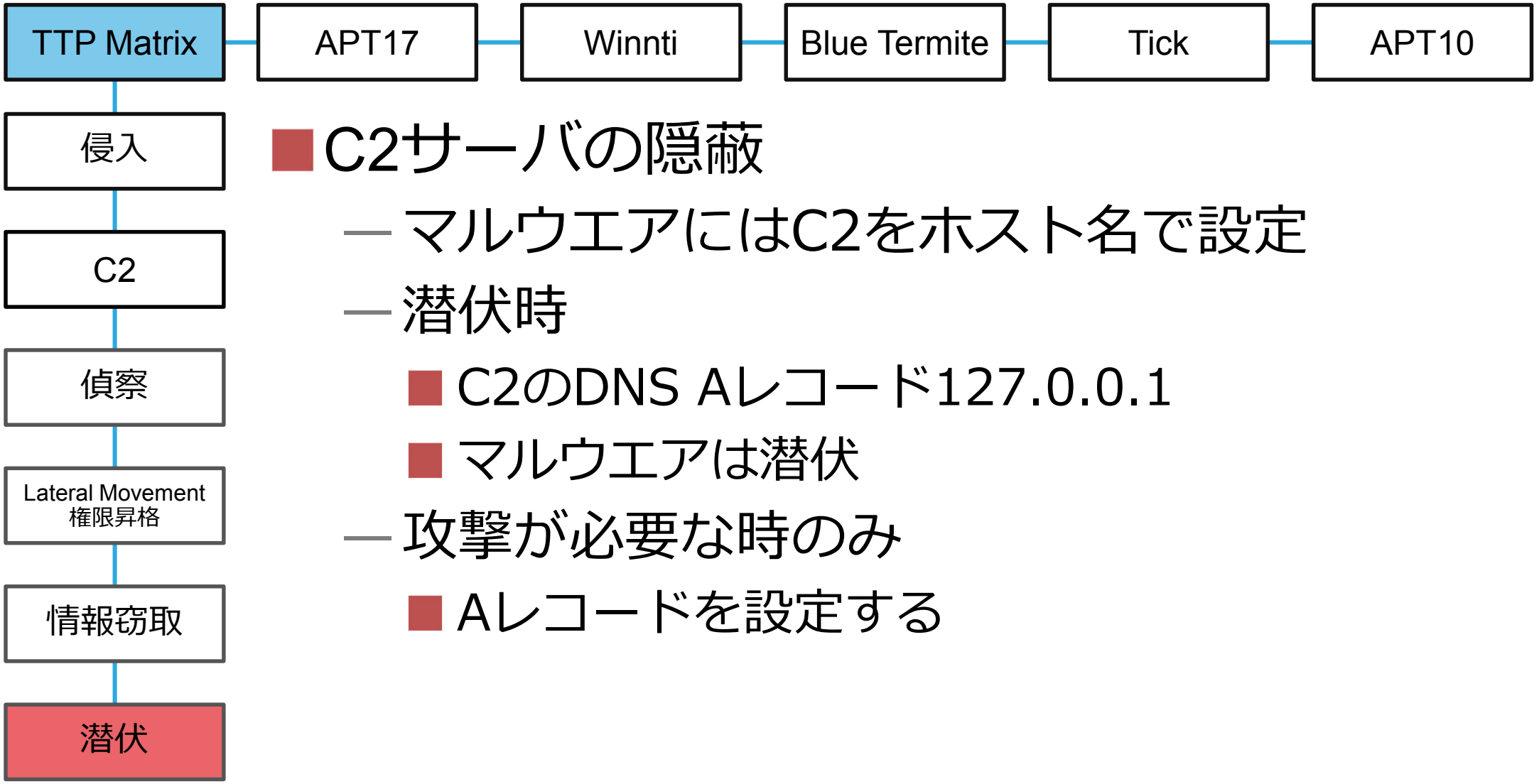
- 管理者アカウントの強制ログインを誘導
  - 侵入したPCを意図的に不調にし、ユーザログイン不能に
  - ユーザは組織のシステム管理部門へ持ち込み
  - システム管理部門は管理者アカウントでログイン
  - 攻撃者は再度ログインして管理者アカウントのハッシュを入手

情報窃取: 特徴的な攻撃手法



- コードサイニング証明書の窃取、悪用
  - 正規のコード署名のワークフローを把握
  - マルウエアを署名ワークフローに乗せ、署名させる
  - 署名されたマルウエアを回収し証拠隠滅

潜伏: 特徴的な攻撃手法



- C2サーバの隠蔽
  - マルウエアにはC2をホスト名で設定
  - 潜伏時
    - C2のDNS Aレコード127.0.0.1
    - マルウエアは潜伏
  - 攻撃が必要な時のみ
    - Aレコードを設定する

APT攻撃対応の
ベストプラクティス

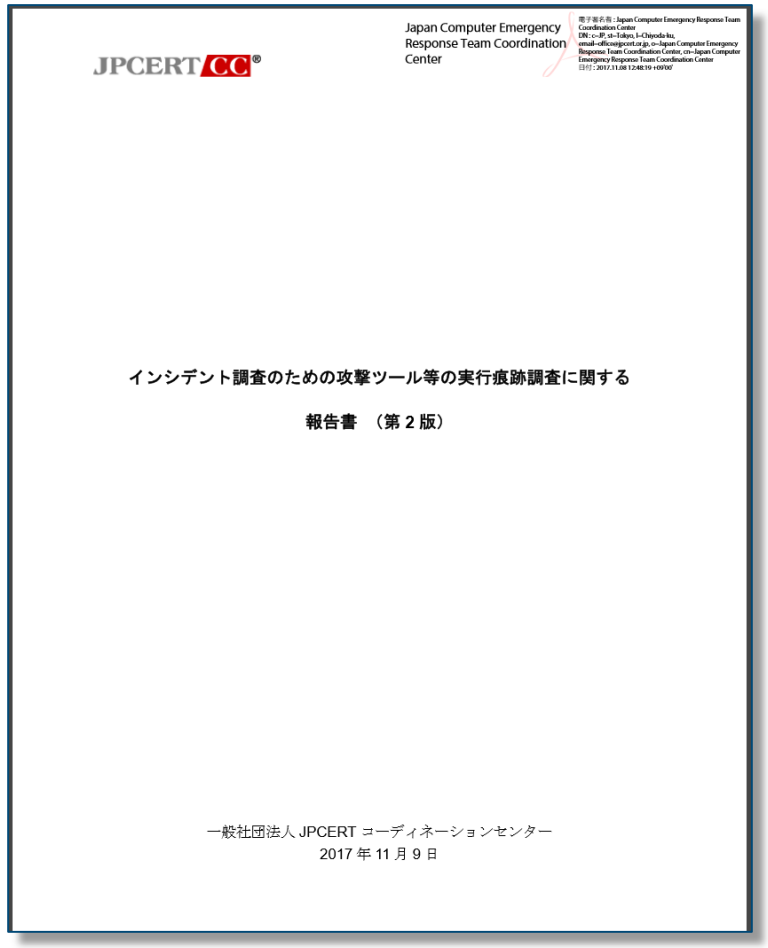
インシデントレスポンスの目的

事実に基づいて、
影響範囲と原因を排除すること

事実の認識：インシデント調査

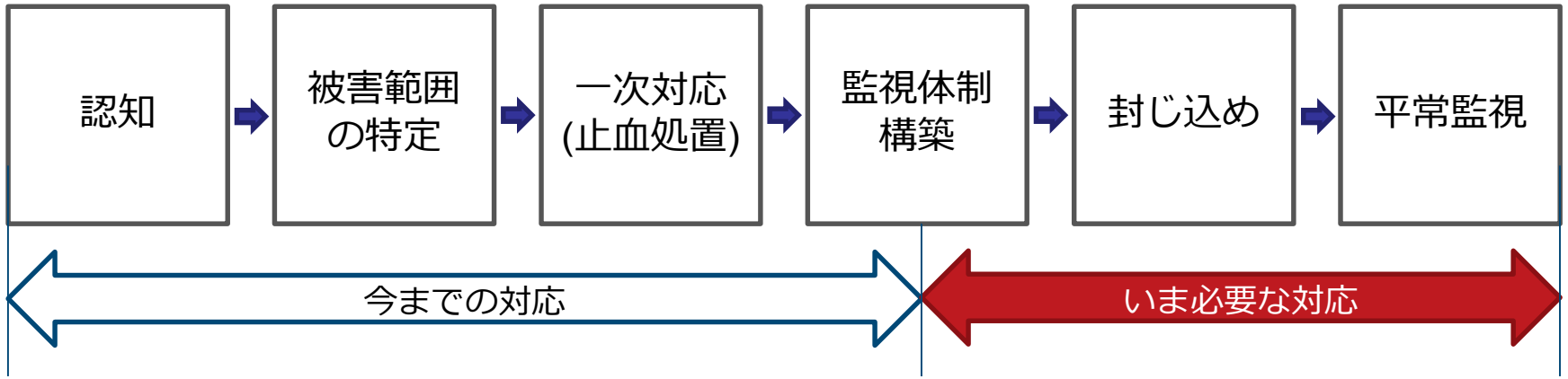
- インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書（第2版）（11月9日公開）
  - Windowsにおける、コマンドおよびツール実行時に作成される痕跡を調査
  - Sysmonと監査ポリシーを利用

- ツール分析結果シート
  - https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/



インシデント調査のための攻撃ツール等の実行痕跡調査に関する報告書
JPCERT/CC
https://www.jpcert.or.jp/research/ir_research.html

APT攻撃対応ベストプラクティス



- 今までの対応
  - 被害範囲を想定した対応
- 必要な対応
  - 監視体制を構築、リアルタイムで事実確認を可能に
  - テクノロジー・メソッドの導入
  - 対応戦略も重要

認知

- 外部からの連絡
  - JPCERT/CC
  - 警視庁サイバー攻撃対策センター
  - NCAなどのコミュニティ
  - 海外セキュリティ組織
- 異常検知
  - アンチウイルスソフトウエア
  - セキュリティ製品
  - データベースの異常負荷
  - etc…

自組織で発見：外部からの連絡

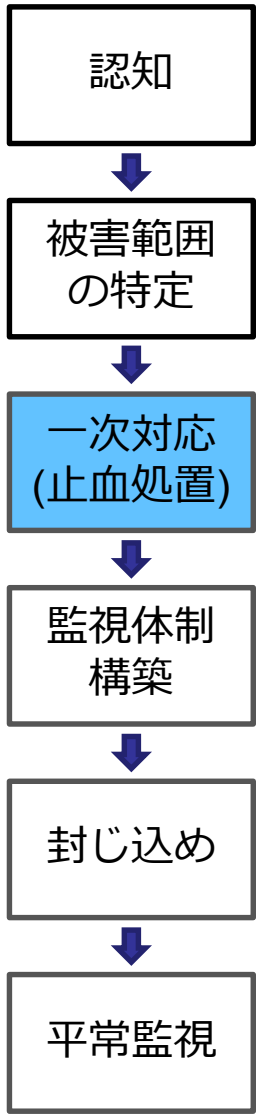
47%：53%

FireEye M-Trends2016
https://www2.fireeye.com/WEB-M-Trends-2016-JA.html

被害範囲の特定

- 経営層への説明を意識
  - PC何台が感染という情報では不足
  - 「誰の何が」という情報が重要
  - 対応費用の稟議決済のための作業
- 短期間で投入リソースの決済が必要
  - 費用・工数をかけないと事実確認できないというジレンマ
- 成功事例
  - ファイルサーバのアクセスログ（何が）
  - ADのログ（誰の）

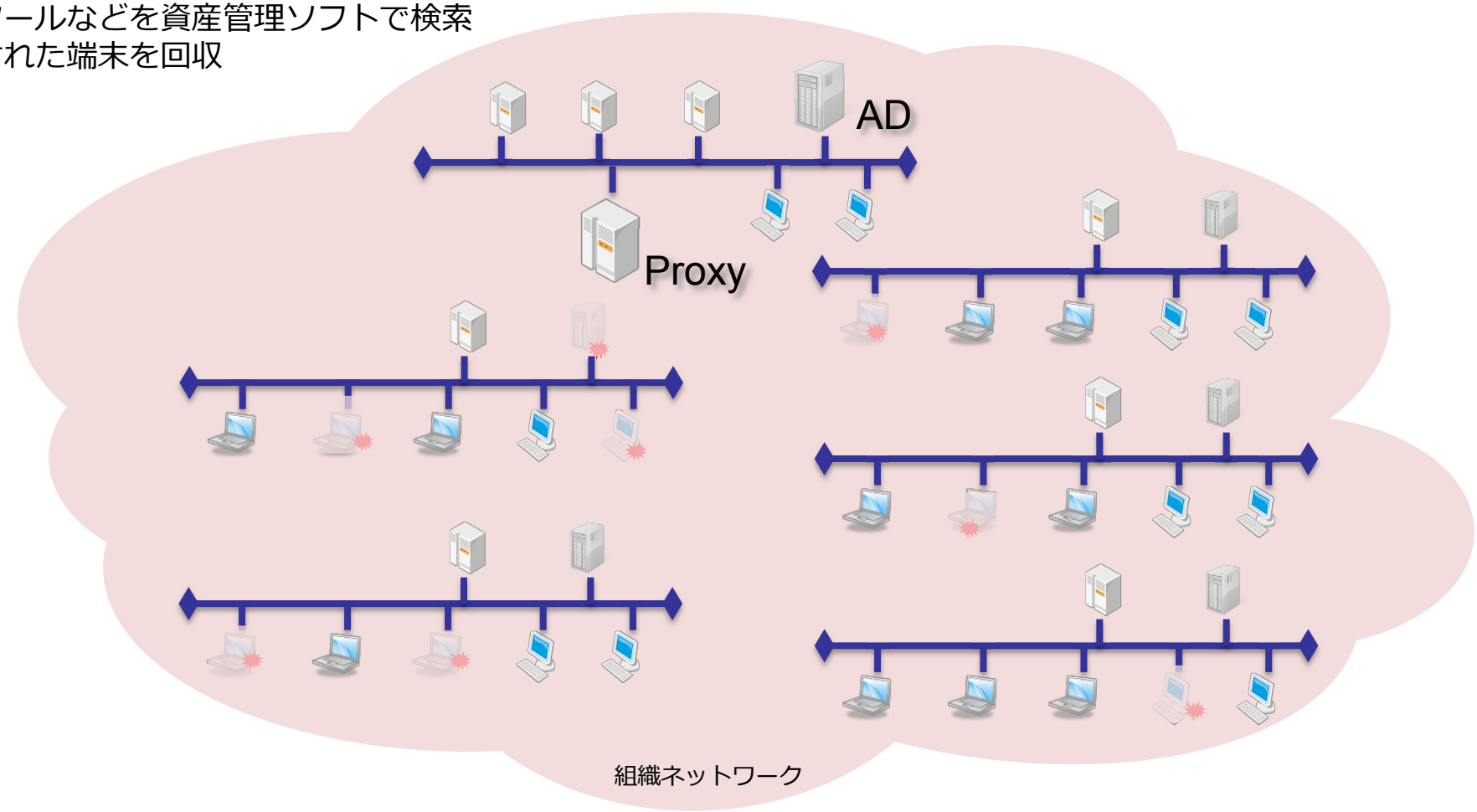
一次対応（止血処置）



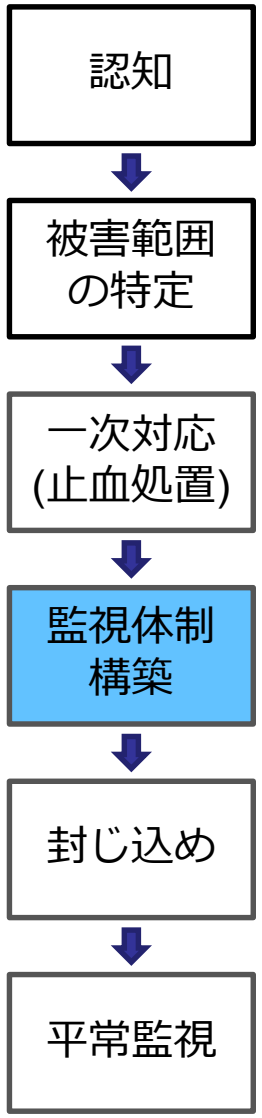
- 過剰反応気味に対応すべき
  - 被疑PCの回収（定型オペレーションに）
  - 可能な限り証拠保全（ディスクイメージ）
  - 必要に応じてフォレンジック調査
    - マルウエアの特定、攻撃グループの特定
      - アンチウイルスソフトのパターン作成
      - 資産管理ソフトも活用
        - 被疑PC回収のサイクル
  - ユーザアカウントのパスワード変更
  - ドメイン管理者のパスワード変更
    - ゴールデンチケット、シルバーチケットへの対応
  - 組織内の脆弱ポイントへの対策
    - セキュリティパッチ適用
    - ドメイン管理権限の運用見直し
    - PC管理用アカウントの見直し

一次対応（止血処置）

1. Proxyの通信ログから端末を特定し、回収分析
2. 検体をアンチウイルスベンダーに提供、パターン化
3. アンチウイルスソフトで検出した端末を回収分析
4. 設置されたツールなどを資産管理ソフトで検索
5. ツール設置された端末を回収



監視体制構築



- 組織ネットワーク全体の把握
  - ログの保存期間の確認
    - ADサーバ、ファイルサーバ
    - Proxyサーバ、ファイアウォール
    - DHCPサーバなど
  - ログの可読化・可視化
    - Windowsイベントログの可読化
    - ADの認証アカウンティング
  - ログ管理の統合
    - 各サーバのイベントの相互タイムライン追跡

- ユーザPCの監視、管理
  - 通信プロセスの記録
  - プロセス起動の追跡
  - レジストリ変更など

テクノロジー導入の検討
SIEM製品・EDR製品

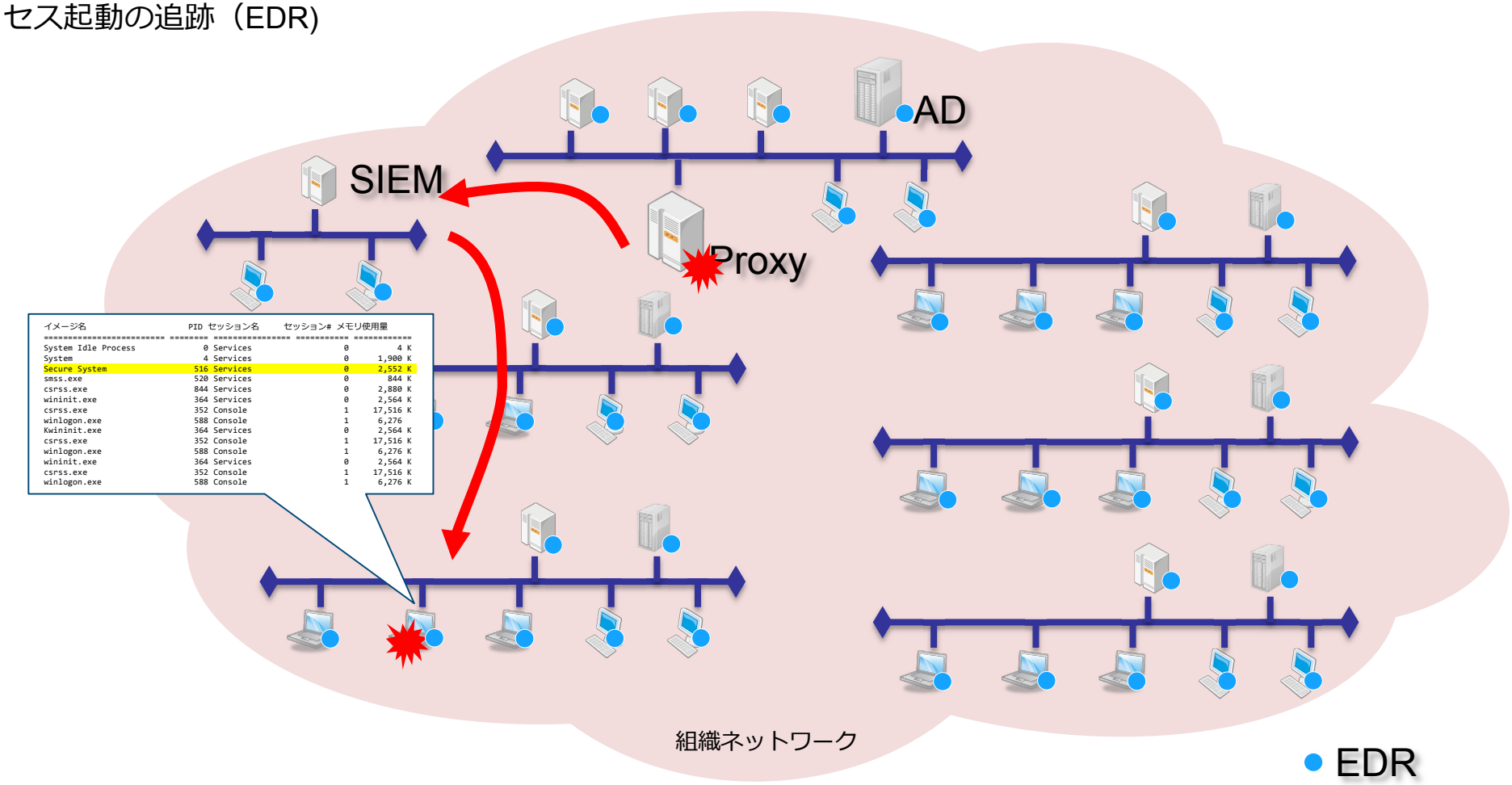
監視体制構築

- インシデントレスポンス視点で実現すべきこと
  - SIEM製品
    - 各種ログの可読化・可視化、検索
    - 異常認知から該当PC、ユーザの特定
      - プロキシログから該当通信のPC特定
      - 異常データベースクエリのPC、ユーザ特定　など
  - Endpoint Detection and Response(EDR) 製品
    - 通信プロセスの特定
    - 当該プロセス起動の追跡

フォレンジック調査の必要のない監視体制

監視体制構築

1. 監視体制の構築（SIEM,EDR）
2. Proxyの異常通信からPCの特定（SIEM）
3. PCの通信プロセスを特定（EDR)
4. プロセス起動の追跡（EDR)



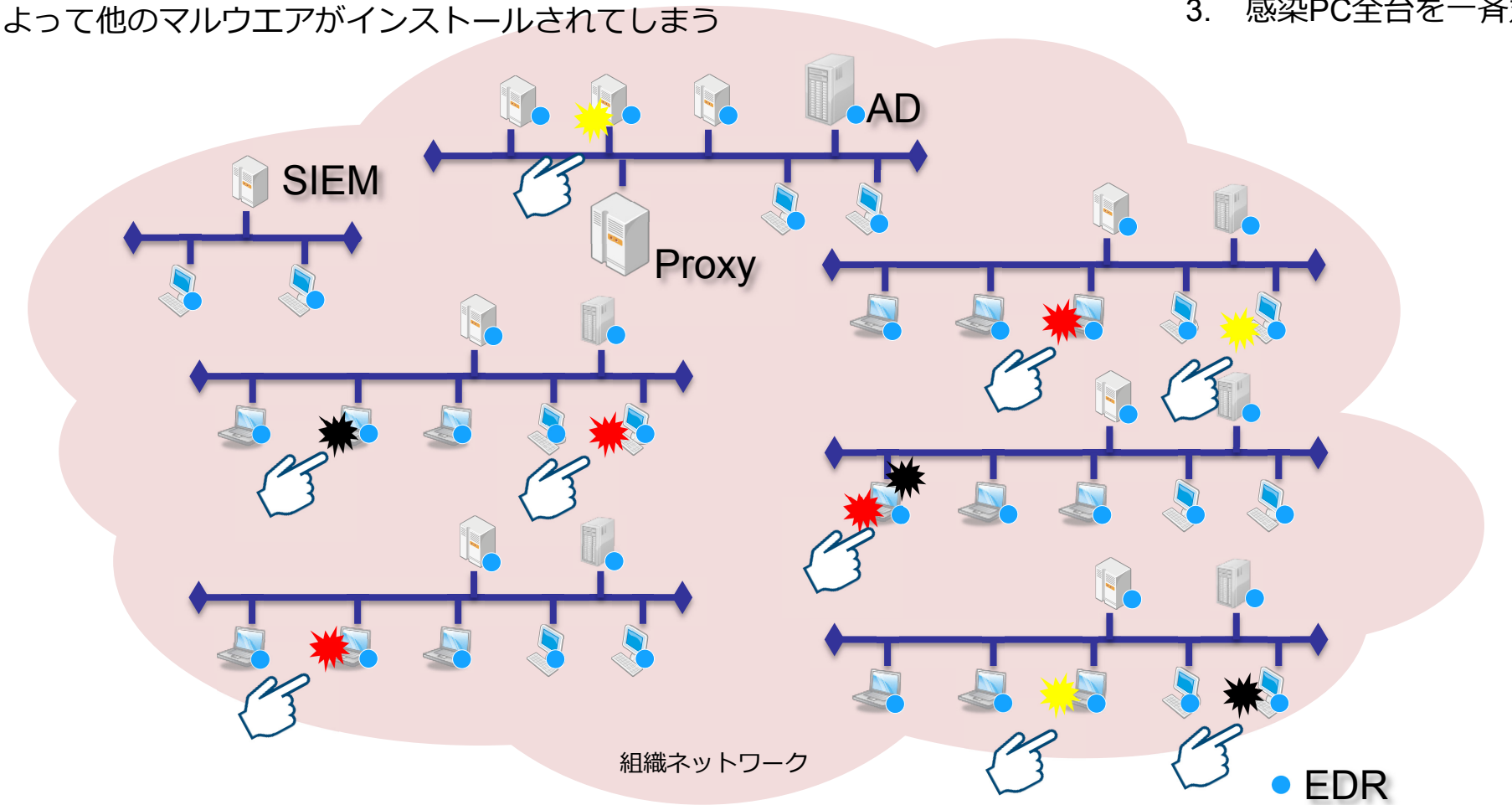
封じ込め

- 構築した監視体制を活用
- 戦略
  - 監視期間を設定
    - 監視期間には過剰反応しない
    - 侵害を確認できた範囲を攻撃者に悟られないように
      - ネットワーク全体を把握できていることが前提
    - 深刻な被害を確認した場合は即対応
      - 監視期間を再設定
  - 対応日を決めて一斉に対応

封じ込め

間違った戦略
1. 感染PCの確認
2. 見つかったものから対応
3. 攻撃者によって他のマルウエアがインストールされてしまう

正しい戦略
1. 感染PCの確認
2. 感染状況の全体把握
3. 感染PC全台を一斉対応



まとめ

- 標的型攻撃への対応
  - 事実の認識が最も重要
  - 体制
    - CSIRT
      - 事業部門の参加が必須
    - 経営層がリード
      - 決済できる体制
  - 技術
    - 体制だけでは対応できない
    - EDR、SIEMなどの技術の導入
  - メソッド（オペレーション）
    - 事実確認を可能に
      - 事実に基づいて対応することが重要
    - 一次対応の手順化（ルーティン化）
    - 専門家への協力依頼
      - セキュリティ事業者、JPCERT/CC

- 組織ネットワークの変化への対応
  - ネットワーク形態の変化
    - モバイル端末
    - リモートオフィス
  - 組織利用サーバ形態の変化
    - クラウドサービスの利用

ネットワークセキュリティだけの対応は困難

エンドポイントの監視
ユーザ認証・サービスの監視が重要

参考文献

- Application for STIX v2.0 objects management and analysis STrelok
  https://github.com/jpcertcc/strelok/
- インシデント調査のための攻撃ツール等の実行痕跡調査報告書
  https://www.jpcert.or.jp/research/ir_research.html
- ツール分析結果シート
  https://jpcertcc.github.io/ToolAnalysisResultSheet_jp/
- ログを活用したActive Directoryに対する攻撃の検知と対策
  https://www.jpcert.or.jp/research/AD.html
- 高度サイバー攻撃(APT)への備えと対応ガイド～企業や組織に薦める一連のプロセスについて
  https://www.jpcert.or.jp/research/apt-guide.html

お問合せ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- Tel：03-3518-4600
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form