A-4.
標的型サイバー攻撃の調査と対応（PC編）

金城学院大学
西松　高史

このセッションの目標

標的型サイバー攻撃を受けた時の「PCの痕跡調査」と
対応を学び、実習にて確認する

（1） ログ取得の準備をし、確認することができる
（2） 被害範囲の予測・調査を行うことができる
PCの調査・対応が行えるようになる

標的型攻撃の流れ

① 計画立案
② 攻撃準備

標的となる組織の情報を収集、準備を行う。

③ 初期潜入

標的型メール等でウィルス(主にRAT)を送信、感染。SNSやUSBメモリを使う場合も

④ 基盤構築

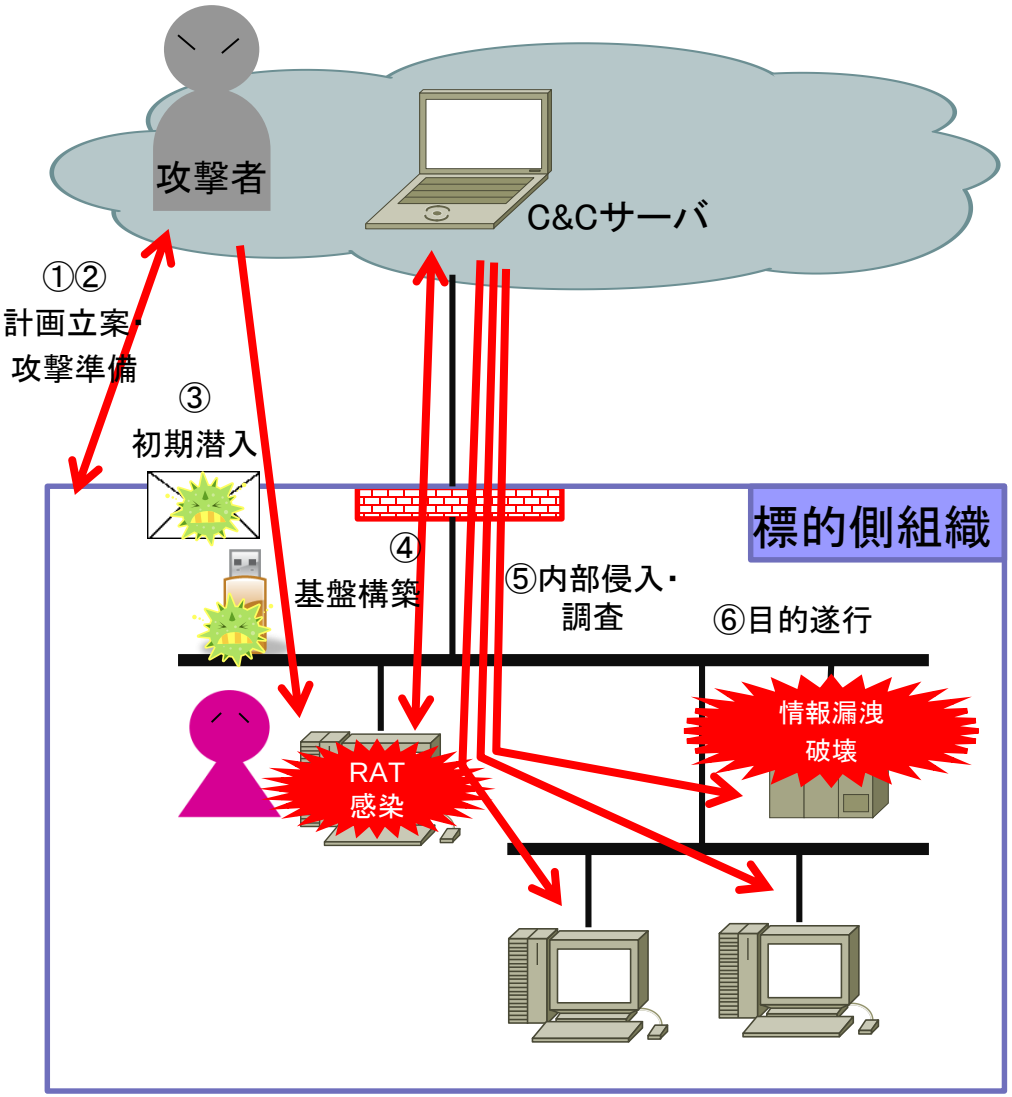
RAT経由で各種ハッキングツールを送信

⑤ 内部侵入
調査

④のツールを用いてさらに内部システムの侵入を行い調査を進める

⑥ 目的遂行
⑦ 再侵入

最終目的の達成



インシデント対応フローチャートに沿った対応

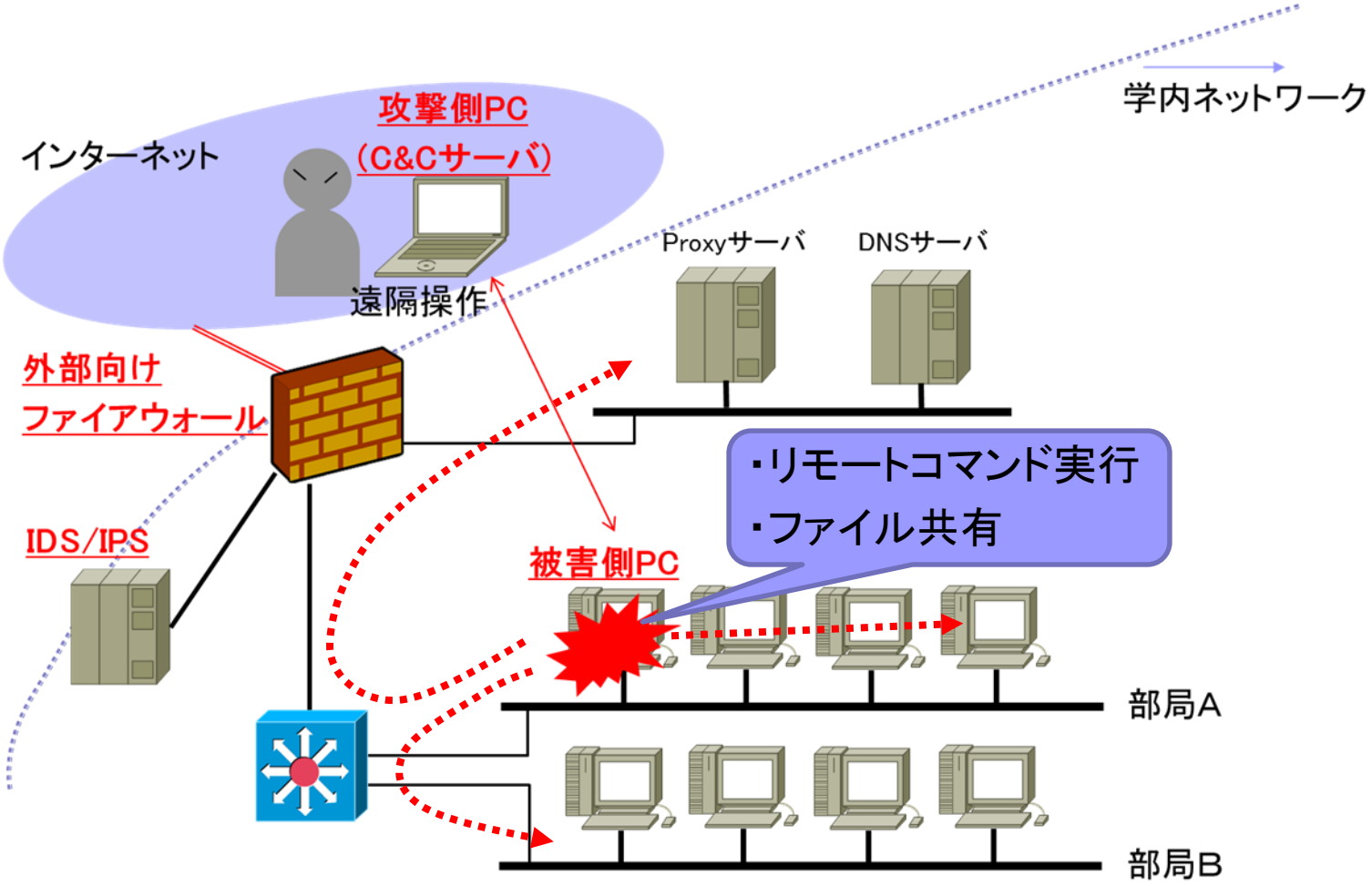
1. 外部からの指摘
2. 事実の確認・一次対応
    1. ネットワークレベルでの調査・対応
    2. PCレベルでの調査・対応
3. インシデント対応に関する体制、手順の確認
4. インシデント情報の集約
5. 被害（情報漏えい）の調査・予想
6. 対外的窓口の設置
7. インシデント情報公開の時期と公開内容の検討
8. 再発防止計画

A−4

「PCの痕跡調査」

PCの痕跡調査

- 調査結果を元に侵入を進める（横展開）



PCの痕跡調査

- どんな痕跡調査ができるのか？（理想）
  - フォレンジック（外部業者へ委託）
    - 被害状況によっては必要だが、状況の確認と費用の見積が必要

学内に状況を説明するためにも、
ある程度の痕跡調査が必要

PCの痕跡調査

- 痕跡調査結果
- イベントログ、実行履歴、レジストリエントリ
  - 専用のフォレンジックソフトウェアやフォレンジックに関する知識がなくても可能
  - イベントビューアを利用
- 攻撃手法の研究
  - 攻撃者によって使われることが多い代表的なツールを実行した痕跡を探す

JPCERT/CC
「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」
最終更新: 2016-06-28
https://www.jpcert.or.jp/research/ir_research.html

PCの痕跡調査

- 痕跡調査結果
  - 44種類のツールについて痕跡調査結果を解説している。

JPCERT/CC
「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」
最終更新: 2016-06-28
https://www.jpcert.or.jp/research/ir_research.html

3.1. 本章の構成

以降では、44 種類の各ツールについて、以下のような表形式で解説している。

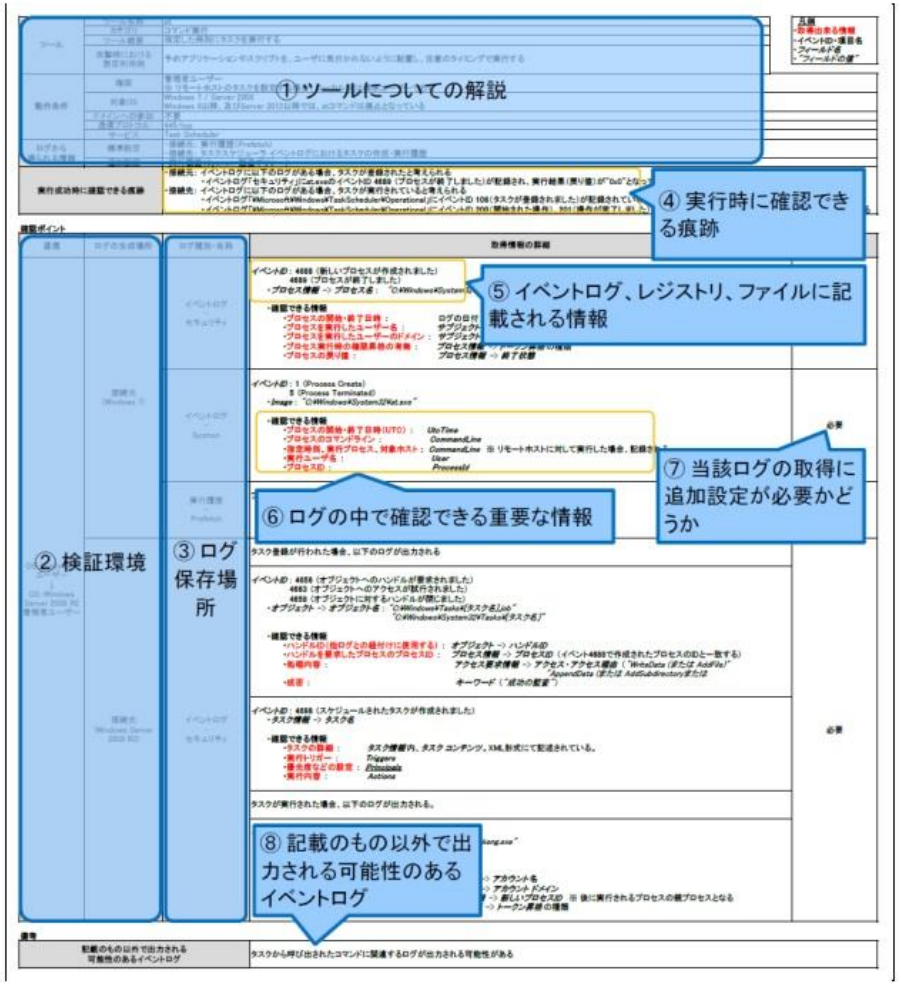


図 3-1: 次節以降の記載内容

PCの痕跡調査

- 前準備（各PCの設定）
  - ログ収集の設定
    - 監査ポリシーの有効化
      - Windowsに標準で搭載されている詳細なログを取得するための設定
    - Sysmonのインストール
      - マイクロソフトが提供するツールで、プロセスの起動、ネットワーク通信、ファイルの変更などをイベントログに記録する
    - ログの保存期間確認
      - 保存期間は1年程度必要
    - 時刻の同期
      - 複数のサーバやPCのログの関連性を相関分析するために重要

ログが増えるため
ディスク容量と
保存期間に注意！

「PCの痕跡調査」実習

実習

1. PCの痕跡調査

- 攻撃者がよく使うWindowsコマンド
  - PsExec
  - net系コマンド
  - Power Shell（リモートコマンド実行）
- 攻撃者がよく使うコマンド
  - wce
- ログの確認（痕跡調査）
  - イベントビューア

PsTools(PsExec)

- Windows管理ユーティリティ
- Microsoftがフリーで配布
  - https://technet.microsoft.com/ja-jp/sysinternals/bb897553
- コマンド
  - PsExec・・・リモートでプロセスの実行を行う
  - PsKill・・・リモートでプロセスの強制終了を行う
  - PsShutdown・・・リモートでシステムのシャットダウンを行う
- サーバ側で、ファイル共有サービスが動いていれば動作。
  - SMBのプロセス間通信機能を使用
  - 感染端末と同じドメインであれば、パスワードも不要。

net系コマンド

- ファイル共有サービス制御
  - net share
    - 公開しているファイル共有の一覧を表示する
  - net use x: ¥¥192.168.1.xxx¥share
    - ネットワーク共有に接続する
  - net use
    - 接続しているネットワーク共有一覧
  - net view
    - 共有を公開しているサーバの一覧
  - net view ¥¥192.168.1.xxx
    - サーバが公開している共有の一覧

Power Shell（リモートコマンド実行）

- Windowsを管理するための新しいシェル
- ネットワークを介して他のホストに対してコマンドを実行することも可能

イベントビューアー

- イベントログを見るためのツール
- [Win]+[R]キーを押して「eventvwr」を入力
- 最大ログサイズを設定
  - コンソールツリーで管理するイベントログまで移動して選択
  - [操作]メニューの[プロパティ]をクリック
  - [最大ログサイズ(KB)]でスピンボックスコントロールを使用して必要な値を設定し、[OK]をクリック

「フォレンジックの概要」

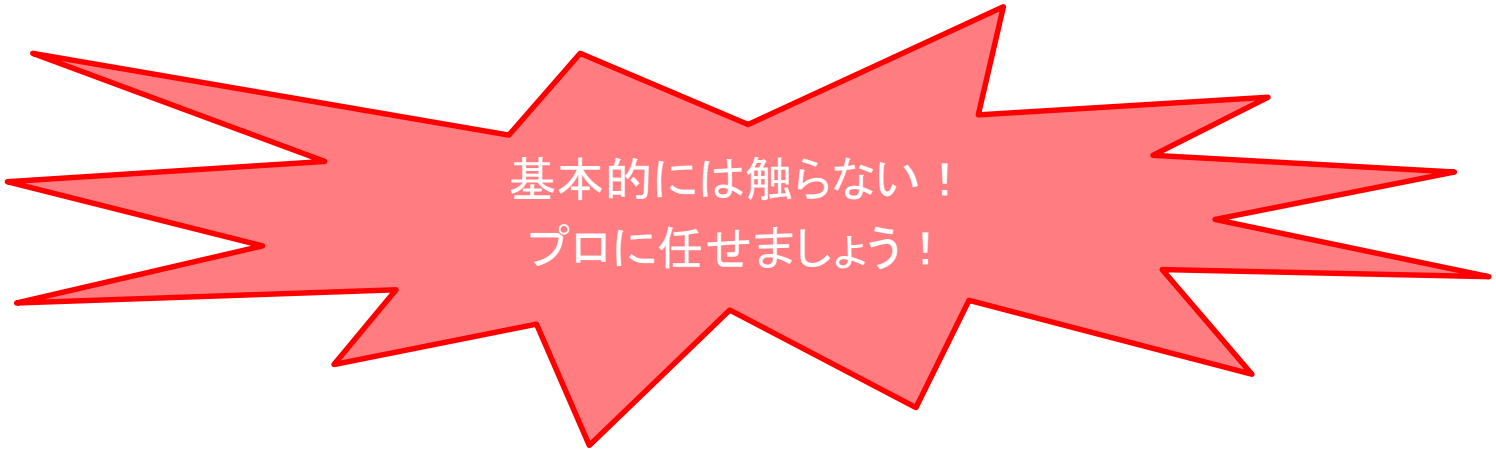
フォレンジックの概要

- 証拠の保全
  - 証拠保全の重要性
    - 稼働中のシステムで調査を行えば、不正なプロセスやネットワーク情報を検出することが出来る可能性が高い。特に「日時情報」「一時ファイル」「ログ」などの情報が重要。
    - マルウエアは何らかのきっかけで自己消去してしまう可能性も想定される

詳しく書かれている資料
「証拠保全ガイドライン　第5版」 2016年4月21日
特定非営利活動法人　デジタル・フォレンジック研究会
「証拠保全ガイドライン」改訂ワーキンググループ

フォレンジックの基本

- 初動対応
  - PCの電源を切らない
    - 電源「ON」のまま
    - 再起動もダメ
  - ネットワークケーブルを抜く
    - 端末間での侵害拡大と情報流出の防止



【参考】ネットワークケーブルを抜かない対応

- トレンドマイクロ社ウイルスバスターCorp.を利用している場合
  - PCの電源を切らない
    - 電源「ON」のまま
    - 再起動もダメ
  - ネットワークケーブルを抜かない
    - サポートに連絡し手順の確認
    - パーソナルファイアーウォールの設定を行い対象PCの隔離
    - 対象PCへToolBox ATTKを配信し実行、調査ログを収集
    - 取得した調査ログをTrendLabへ解析を依頼
    - 対象PCへToolBoxファイル収集ツールを配信し実行、不審ファイルを収集
    - 取得した不審ファイルをTrendLabへ解析を依頼
    - 駆除可能な場合、駆除パターンファイル作成してもらい配信もしくは、本格的なフォレンジック

まとめ

- 事前準備
  - 監査ポリシーの有効化とsysmonのインストール
  - ログの容量と時間同期の確認
- 連絡があれば、イベントビューアで確認
  - 攻撃者がよく使うコマンドの実行履歴
- 無理をせず、プロにフォレンジックを依頼
- 対策製品の導入
  - 対費用効果

参考資料

- JPCERTコーディネーションセンター（JPCERT/CC）
  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
  - https://www.jpcert.or.jp/research/ir_research.html
- マクニカネットワークス

  標的型攻撃の実態と対策アプローチ　第1版
  - http://www.macnica.net/security/report_01.html/