一般社団法人CySecPRO
デジタル・フォレンジック・トレーニングについて

プロフィール

氏名	川崎 隆哉 (かわさき たかや)
所属	株式会社リクルートテクノロジーズ
略歴	2015年 8月～ リクルートテクノロジーズ 入社 / 現職 2012年 4月～ 株式会社UBIC(現フロンテオ)
業務	不正及びマルウェアに関するインシデント発生時の コンピュータフォレンジック及び執務環境の監視

関連書籍

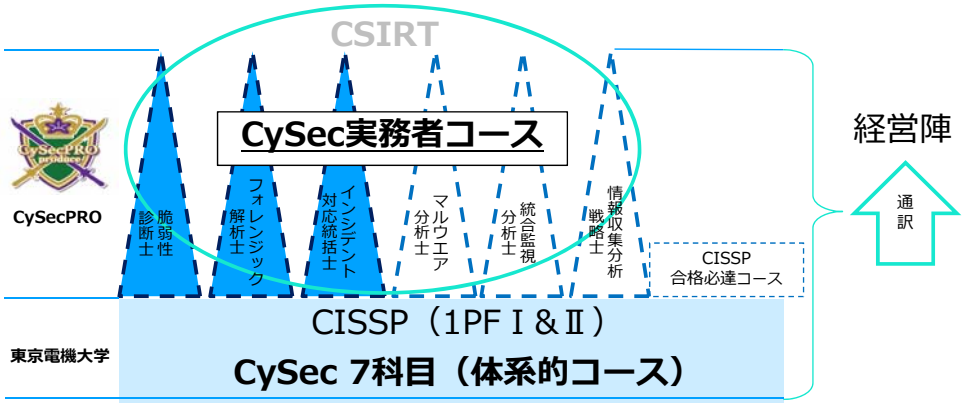
本日のアジェンダ

- 本団体の概要
- 本コースの概要
- コース作成時に重要視したこと

本日のアジェンダ

- 本団体の概要
- 本コースの概要
- コース作成時に重要視したこと

本団体(CySec PRO)の概要



本日のアジェンダ

- 本団体の概要
- 本コースの概要
- コース作成時に重要視したこと

本コースの概要

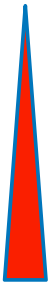
- **学問としてのデジタル・フォレンジックではなく、**
  実践的な「デジタル・フォレンジック調査手法」を学ぶ講義(初心者向け)

  ✓ **目的：**
  フォレンジック調査の助手となれるスキル(後述のLevel 2)を身につける
  (職人の弟子になれる様な教養を身につける)

  ✓ **手法：**
  実際に仮定の調査案件を想定し、一緒に調査を実施していく中で調査の考えや
  フォレンジックのアーティファクトを学んでいく

フォレンジッカーの3レベル

- **フォレンジッカーを下記の3つのレベル(役割り)に分類し、**
  責任や調査の範囲を分離する考え



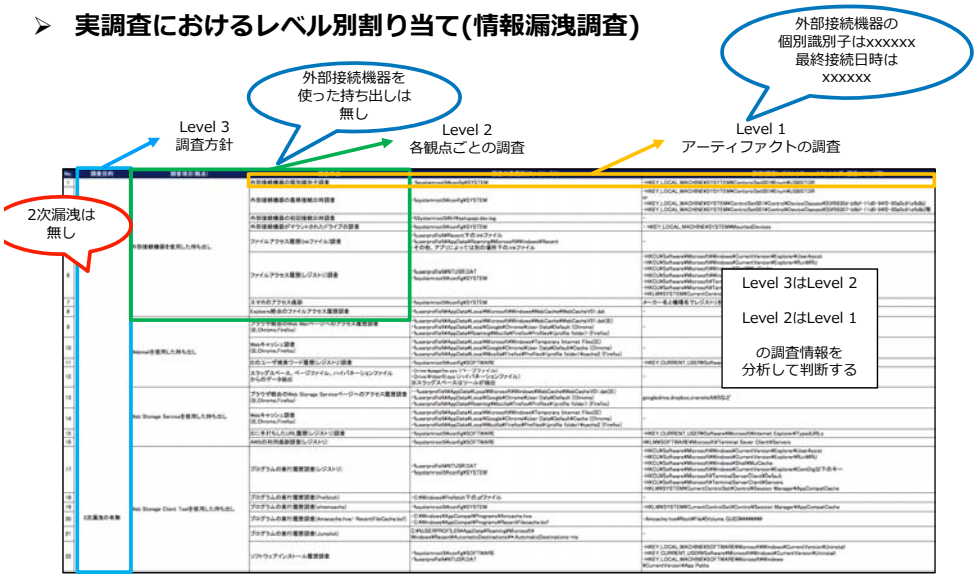
✓ **Level 3：**
ヒアリング、調査方針・範囲の策定や報告(特に非IT人材に説明するスキル)
(方針策定・報告(・再発防止))

✓ **Level 2：**
取得したデータを総合解析する実践的な保全・調査スキル(応用保全・2調査)

✓ **Level 1：**
基礎事項の理解と調査に必要なデータの保全の
ダブルチェック等・調査準備(初級保全・１次調査)

フォレンジッカーの3レベル(補足)

- **実調査におけるレベル別割り当て(情報漏洩調査)**



CySecPRO

スコープ

- **本講義のスコープとしては下記の通り**

✓ **OS：**
Windows 7,10

✓ **系統：**
不正調査、サイバーセキュリティ

✓ **範囲：**
ディスクフォレンジック、メモリフォレンジック

✓ **到達目標レベル：**
Level 2（調査方針があれば、調査ができるようにする
=型にはまった案件なら一定レベルの調査ができるようにする）

CySecPRO

本日のアジェンダ

- 本団体の概要
- 本コースの概要
- コース作成時に重要視したこと

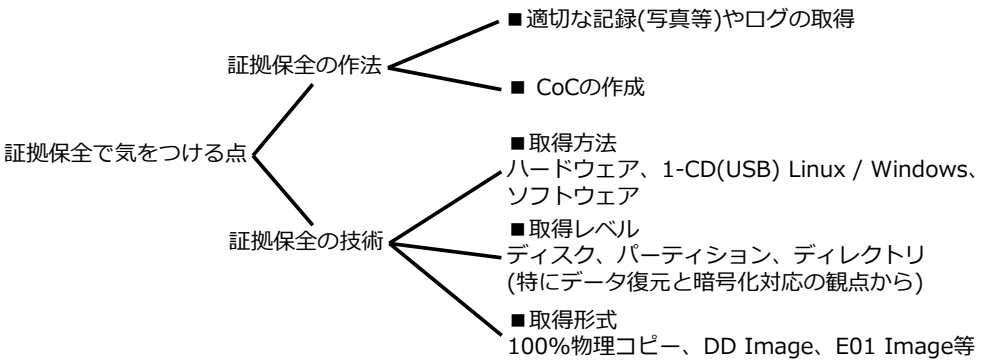
コース作成時に重要視したこと

- **自分がこう教えて欲しかったを形にする**
  - ✓ 架空の調査案件をベースに案件の最初から最後まで通して
    疑似的に体験することでフォレンジック調査全体の雰囲気を掴む
    (ヒアリング→調査項目を立てる→保全→解析→報告)
  - ✓ 1人でできる情報収集の仕方
  - ✓ その他具体的なアーティファクトを体系的に

- **自分がこう教えてもらえて良かったということを形にする**
  - ✓ フォレンジッカーとして仕事をする上で気をつけることや、心構え
    (職人の暗黙知的な部分：明示的に教わらないが、仕事上特に注意している点)

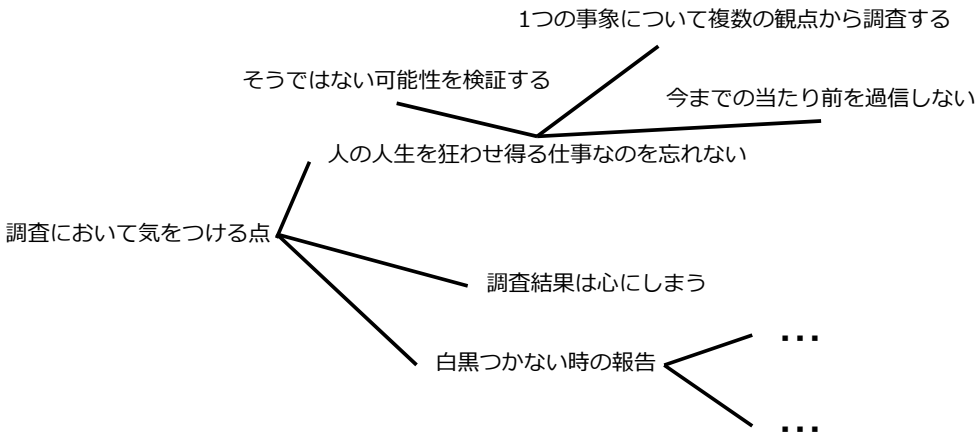
コース作成時に重要視したこと

- **証拠保全の説明例**
  ✓自分がこう教えて欲しかったという形で体系化して掘り下げていく



コース作成時に重要視したこと

- **あまり文書としては残っていない心構え等**
  ✓自分がこう教えてもらって良かったと思う暗黙知を言語化する



まとめ

- **案件全体の流れを通して、自分のしている作業の目的や意味をしっかり わからせる**
- **暗黙知的な「調査上大切なこと」「考え方」のようなものを洗い出して 明示的に伝える方法を考える**

といった点もデジタル・フォレンジックの教育において価値があるかもしれない

CySec Proのホームページ

- https://cysec-pro.org/