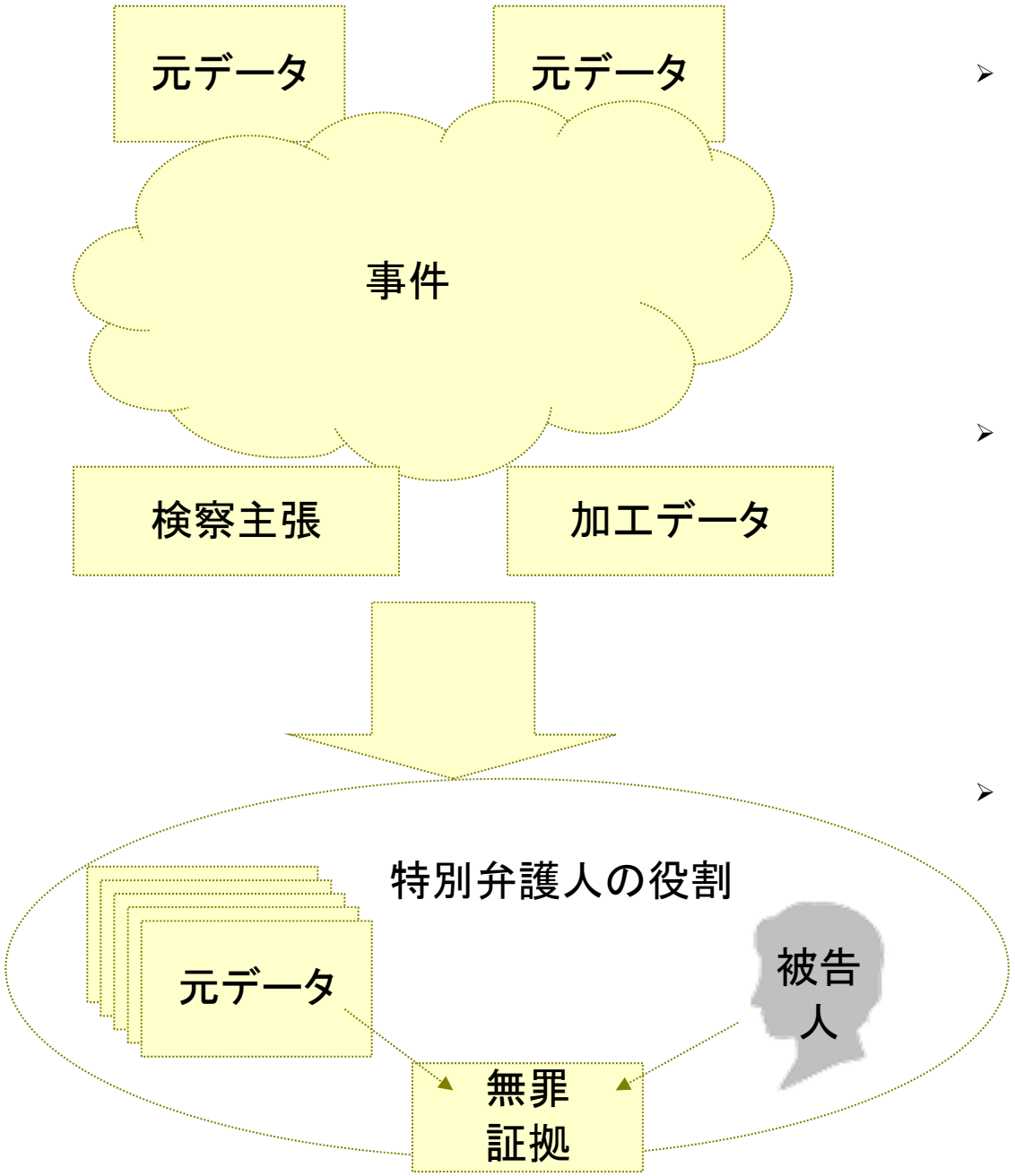
特別弁護人から見た PC遠隔操作事件

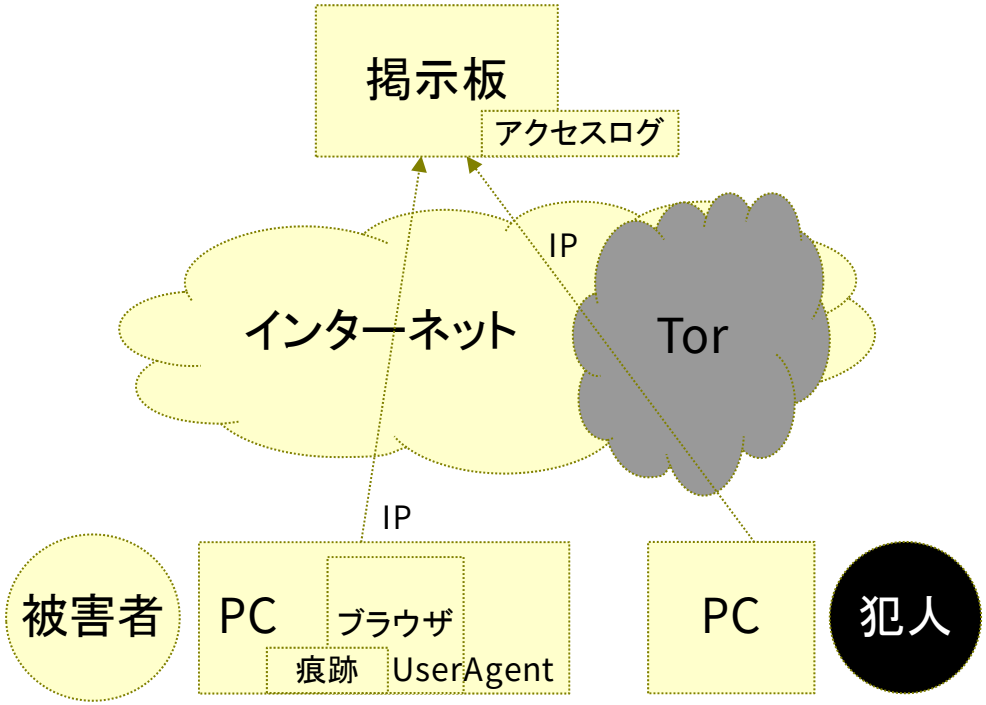
2014-09-29

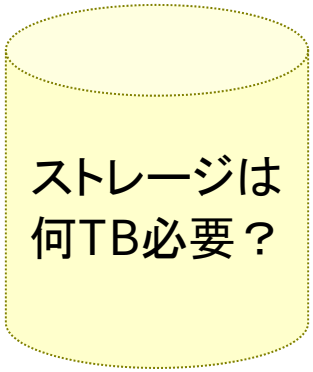
デジタル・フォレンジック研究会

ロジトーイ
野間　英樹
noma@logitoy.jp



- データ開示手続き
  - 何を開示請求するか？
  - どう取り扱うか？
- 分析と立証
  - 分析の方針
  - 必要な知識、経験
- 被告人との対話
  - 基本方針
  - 弁護側特有の注意点





- 存在するデータは何か？
  - ネットワーク図描けますか？
  - どのようなログ・痕跡があるか？
- 開示手続きという難関
  - 開示請求の困難さ
  - データの謄写に掛かる時間・手間
- どうやって取り扱う？
  - 大量のデータを扱えますか？
  - データの同一性担保はできますか？

Point!

断片的情報から現実に
起きたことを再現・イメージする

Point!

ツールはツール
Rawデータを見て分かることが多い

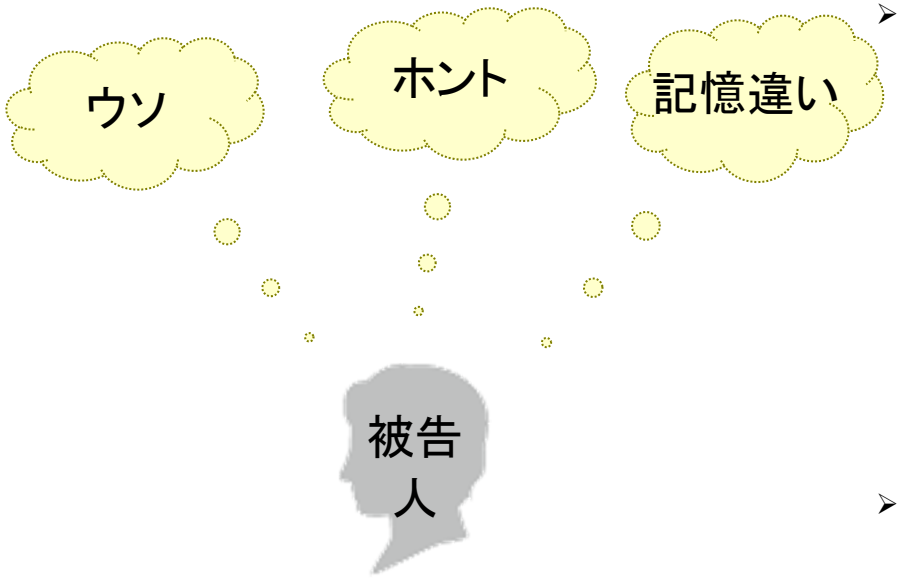
必要な知識・経験
インターネット上の各種プロトコル
Webサーバ・メールサーバ
プロキシサーバ
日本のプロバイダの業務
エンタープライズ系のセキュリティー保守業務
各種プログラミング言語
ソフトウェア開発ツール
Windowsの内部動作
ファイルシステム

分析方針

- アリバイ探し
  - 時系列にすべてのデータを整理
  - 犯人の痕跡と被疑者の行動の照合
- 検察官立証崩し
  - 立証内容の根拠となる元データの検証
    1. 元データは信頼できるのか？
    2. 別の解釈は可能か？

立証

- 今回は結果的に書証レベルでは立証はせず



特別弁護人から見て
どうだったのか？

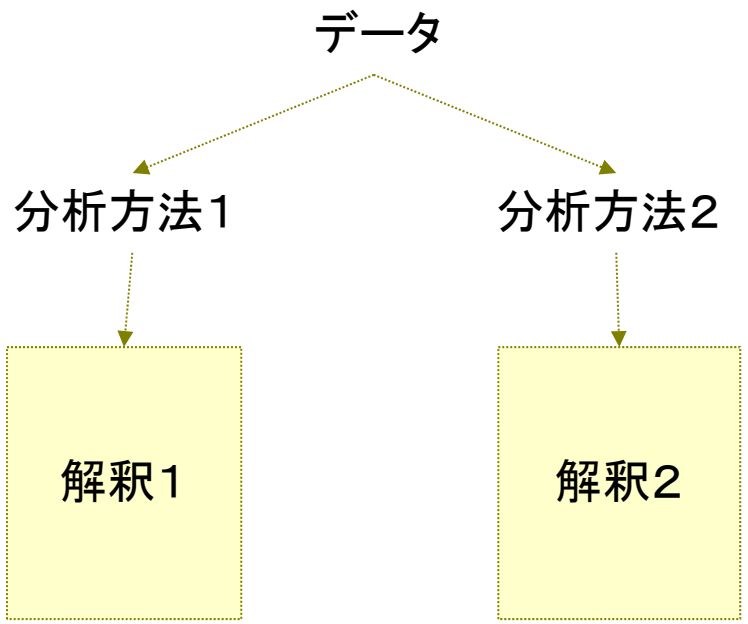
対話の目的

- データとの照合を通じた真実の見極め
  - → 真犯人の場合、必ず矛盾が生じる
  - → 冤罪の場合、本人以外の痕跡が見つかる可能性が高い

対話の方針

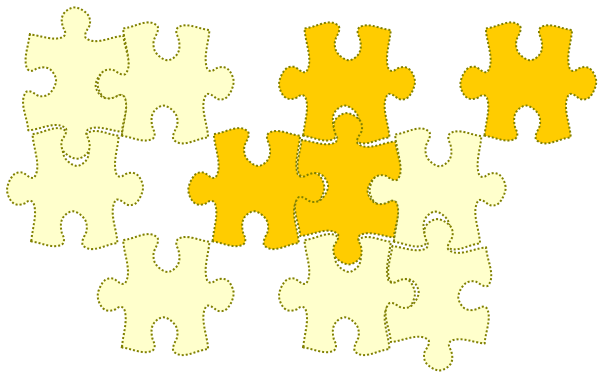
- 全ての主張は「事実」という前提で聞き入れ記録する
- データ上の真実との照合、矛盾点についての可能性の検討
- 不用意にデータを開示しない

同一のデータに基づいた
「解釈」
を裁判の土俵にするべきでは？



例）
遠隔操作されていないってどう立証するのか？

- デジタルデータ取扱い上の課題
  - 入手できていないデータがある
  - 改竄防止措置は努力中
  - 同一性担保は不十分
- デジタルデータ分析の課題
  - 分析結果の再現性が不完全
  - 担当領域以外は関知しない
    - → 分析ミスが一カ所で発生するとそれ以降もミスしたままになるリスク大
  - 機械的な分析中心
    - → 見落とし、誤認識リスク
  - 尋問と組み合わせれば・・・



パズルのピースが抜けたまま
弁護側は強制力が無い
スタートが遅いのでログなどは入手困難

向き合う対話

技術的なトピックに
踏み込む

データ
過去の発言

- データの入手について
  - そもそも圧倒的に不利
  - 入手できるデータが少ない
  - 時間が掛かりすぎる
- データに基づく検証
  - データの解釈が出来る人が少ない
  - 特別弁護人という立場では十分な接見がしにくい
  - 保釈後、被告人との対話姿勢が変わってしまった

これから同じ立場で仕事をする人へ

地道で大変な仕事です
周りの人は、データ・数字に疎いです

おそらく
サーバ運用経験者に向いてます
でも広範な知識も必要です

- データはウソをつかない
  - 人は真実を語らない
  - データを解釈するのは人
- 生の情報が大事
  - 目でデータを確認する
  - 仕組みを理解する
  - 自分で確かめる
- 弁護サイドで仕事を出来る人はもっともっと必要