

平成21年12月15日  
デジタル・フォレンジック・  
コミュニティ2009

# 警察における デジタルフォレンジックと今後の課題

警察庁情報通信局  
情報技術解析課長  
高橋 守

## 1 警察とデジタル・フォレンジック

## 1-1 経緯

- 警察でデジタル・フォレンジック(ITフォレンジック)に取り組んだのは昭和の時代から
- 電話が犯罪に用いられるようになって、電話に対する捜査が必要となった
- 犯罪にコンピュータが関係するようになって、デジタルフォレンジックが必要となった
- 従来から電気通信や情報処理に知識のあった警察の情報通信部門がこれを担当することとなった

### 1-1-1 宗教団体によるテロ事件

- 平成7年3月
  - 宗教団体によるテロ事件の捜査の過程で、大量の電磁的記録が押収され、その解析が必要となった
  - 高度な技術を背景とし、独自の暗号システムを使用するなどしていたため、これの解析は困難を極めた

## 1-1-2 不正アクセス行為の禁止等に関する法律の施行

- 平成11年8月13日公布
- 平成12年2月13日施行
  - 不正アクセスを立証するためには、デジタル・フォレンジックが必要である
  - 技術的に高度な知識を必要とする

## 1-1-3 技術対策課の発足

- 平成11年4月
  - 「電磁的記録の解析その他情報通信の技術を利用する犯罪の取締りのための情報通信の技術に関すること。」を担当する「技術対策課」を警察庁情報通信局に設置

## 1-1-4 情報技術解析課の設置

- 平成13年4月
  - 技術対策課にサイバーテロ対策技術室を設置
- 平成16年4月
  - 技術対策課を情報技術解析課と改称
  - 全国の都道府県情報通信部にも情報技術解析課を設置

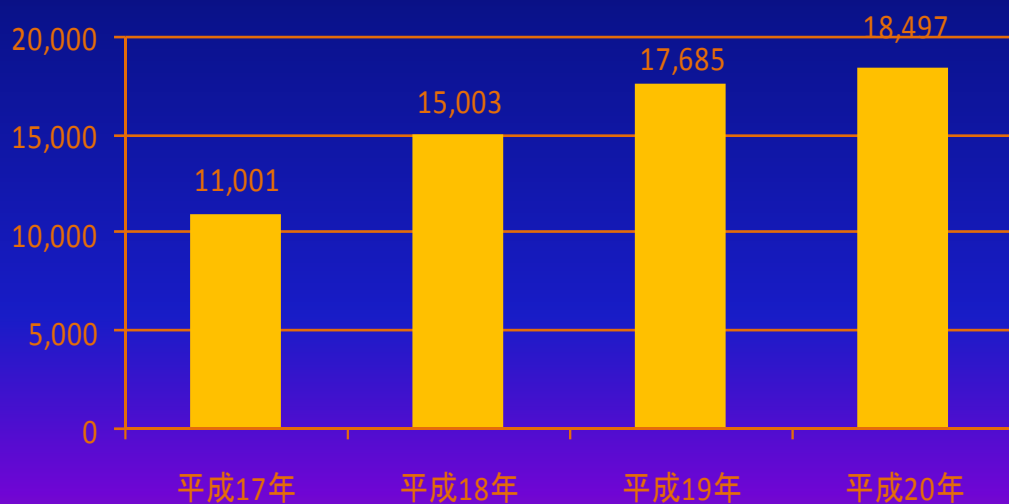
## 2 デジタル・フォレンジックの現状

## 2-1 体制

- 警察庁
  - 情報技術解析課
    - 技術センター(DFC)
    - サイバーテロ対策技術室(CFC)
- 管区警察局
  - 情報技術解析課
- 都道府県警察情報通信部
  - 情報技術解析課

## 2-2 解析の状況

- 電磁的記録の解析等の実施件数  
(件)



## 2-3 解析の事例(1)

- 平成20年北海道の殺人事件
  - 殺人を犯し、他人がそれを実行したように偽装し、その者をも自殺を偽装して殺害しようとした事件
  - パソコン、携帯電話を解析
  - 解析された情報から、供述の矛盾点や計画性を裏付ける情報が判明し、犯行の全容解明に貢献

## 2-4 解析の事例(2)

- 平成20年京都の著作権法違反事件
  - 著作権者に無断でテレビアニメの画像を用いたコンピュータ・ウイルスを作成し、動画を装いファイル共有ソフトWinnyを利用して公衆送信した事件
  - パソコン、コンピュータ・ウイルスを解析
  - 解析された情報から、犯行の全容解明に貢献

## 3 情報技術解析の基本

### 3-1 情報技術解析に必要な要件

- 同一性
  - 証拠に対して、一切の改変が行われていないこと
- 再現性
  - 同一の手順で作業を行えば、誰でも同じ結果が出せること
- 検証性
  - 適正な手順で行われていることが検証できること

## 3-2 職員に求められる能力

- コンピュータ等に関するソフトウェアの知識
- デバイス等に関するハードウェアの知識
- ネットワークに関する知識
- 法令等に基づく手続きに関する知識
  
- 時には自分で簡単な回路設計を行ったり、はんだごてを握ることも

## 3-3 作業環境等の要件

- 第三者が容易に立ち入りできないよう、一般の事務室等から仕切られていること
- 入退室が管理されていること
- 証拠品はその出し入れも含め、厳重に保管されていること
  
- これらは責任ある立場の者が管理する

## 4 今後の課題

### 4-1 環境の変化

- 解析の対象の変化
  - 容量の飛躍的増大
  - 対象の多種多様化
- 技術的高度化
  - さらに広範な知識の必要性
- 解析対策技術 (Anti-forensic)
  - 暗号化
  - パスワード保護

## 4-2 人材の育成

- 人材育成に要する長い期間
  - 単独で解析ができるようになるまでに、教育カリキュラムを通じ、概ね3、4年を要する
- 技術のフォローアップ
  - 新技術に対応するため、常にフォローアップのための教育が必要

## 4-3 連携の必要性

- 警察単独では技術的にも限界
  - 企業等との連携による技術情報の収集
    - 技術情報の開示は企業にとって死活問題
- 海外の法執行機関との連携
  - 文化、環境の違いによる壁

平成21年12月15日  
デジタル・フォレンジック・  
コミュニティ2009

おわり

警察庁情報通信局  
情報技術解析課長  
高橋 守