



# 我が国の刑事訴訟における デジタル・フォレンジック

---

企業の情報漏えい犯罪(事故)におけるデジタル・フォレンジックの手法は, 専門部署の法執行機関から, 一般セキュリティ業界へ普及した。

民間部門でのデジタル・フォレンジックでも, **刑事訴訟を見据えた調査**の必要性が痛感される「事故対応社会」という時代へ突入した。

そのポイントを説明する。

なお, **意見にわたる内容は私見(試見)である。**

---

(C)ハッカー検事



## 刑事手続に準拠する(パクろう)

---

★★常に念頭に置くべき**5つのポイント**★★

- 適法な**調査**→的確な**証拠化**→**証拠保全**
- ① この証拠で ② 何を立証(する)できるか
- (1) 現場保全, (2) 端末保全, (3) ログ保全
- 調査過程は全部記録をとる(5W1H)
- デジタルデータの証拠保全を習得する

---

(C)ハッカー検事

## 【実務上の現実問題】

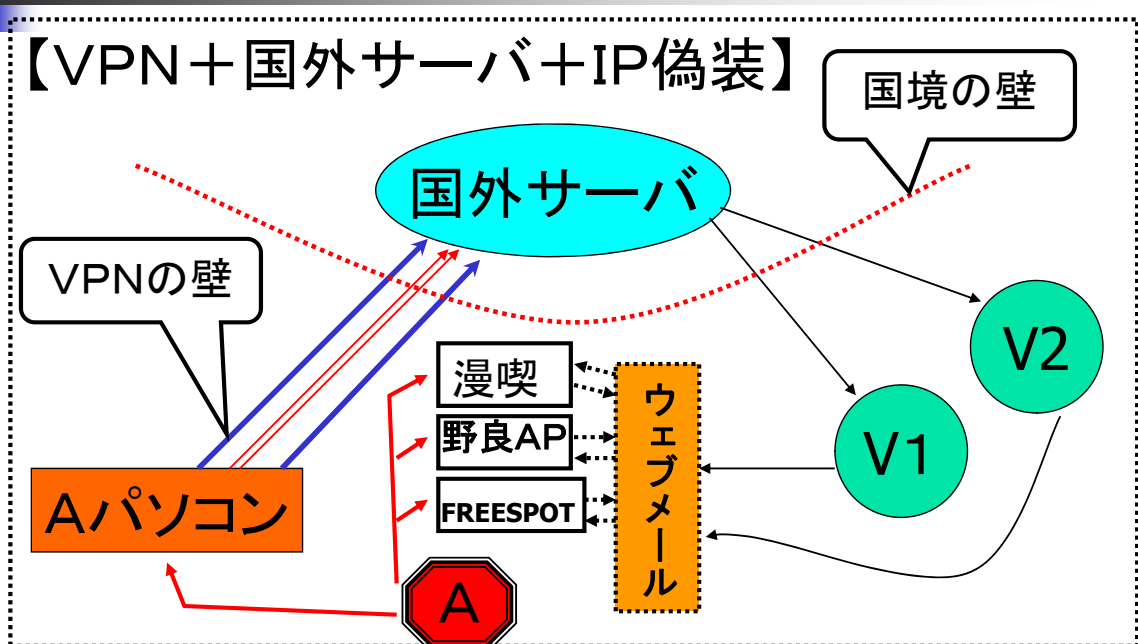
# デジタル・フォレンジックの限界

- DF手法の分析(法曹ヲイ易ク「DF成り」難し)
  - 商品知識や最新技術も平易に説明する。
- 旧来手法の分析も大事
  - 聞き込みや質問回答で供述調査。
  - 関係証拠を精査する裏付け調査。
- 正常態様ノーマルとの比較・偏差(調査初歩)
  - 「普段はどうよ？」という発想が基本のキ！

(C)ハッカー検事

## 【最新検挙事例】

# 発信元偽装手口の実態



(C)ハッカー検事

# 適法な調査→的確な証拠化 →→→証拠保全

- 適法な調査(全て任意ですw)
  - ◆ 対人:業務命令権
  - ◆ 対物:施設管理権と備品管理権
- 的確な証拠化(法廷に提出できる証拠)
  - ◆ 可視化(書類化「ドキュメント化」と「写真化」)
  - ◆ 記録可(①誰が②いつ③何処で④何を⑤どのように、証拠化したか)
- 証拠保全(不適切な調査・証拠化の逆効果に注意)
  - ◆ 違法収集証拠排除法則(証拠排除)

(C)ハッカー検事

## ① この証拠で

## ② 何を立証(する)できるか

- 立証趣旨(実力・技能がバレバレになる)
  - ◆ この証拠で何を立証するかの明示が必要
- 激しい論理的飛躍は却下(論理法則違背)
  - ◆ ×アリバイがない→あいつが犯人だ
  - ◆ ×アンケートの多数決→君が犯人だ
- 非常識は問題外(経験則違背)
  - ◆ ×社長の決定→外部の犯行だ
  - ◆ ×ヲタクの風貌→君が犯人だ

(C)ハッカー検事



# 現場保全, 端末保全, ログ保全

---

## 1. 現場保全

1. 被害現場や犯行現場は, 清掃立入制限
2. 入退室記録(出勤簿や防犯カメラ)のロック

## 2. 端末記録保全

1. 下手に現場にいじらせない
2. HDはイメージコピーをとる

## 3. ログ保全(重ね書きタイプに注意)

---

(C)ハッカー検事



# 調査過程は全部記録をとる (5W1H履歴)

---

## ■ 調査報告書 : 5W1Hが基本

「本職は, 平成XX年X月X日, OO研究所において, 被害に遭ったHDをHDアナライザーでセクタダンプしたところ, 犯行直後に改ざんされたと判明したので報告する。」

## ■ 調査履歴書 : 5W1Hで犯人が割り出せる

- 犯罪とは, ①ヒト②モノ③カネ④情報, が動く
- 通信解析 : 時系列①~④の動きで態様を割出す
- 調査妨害 : 内部犯人は調査進展に連動して動く

---

(C)ハッカー検事



## デジタルデータの証拠化の習得

- A) 不可逆的記録メディアでデータの証拠化
  - ◆ 改ざんされた！との言いがかりを防ぐために
- B) メディア筐体への作成者の署名押印
  - ◆ 出所不明の証拠は信用性が乏しい(信用されず)
- C) 原本との同一性証明
  - a. ハッシュ値やファイルコンペアで確定
  - b. 写しは2本作る（1本はそのまま保管）
- D) 機械的正確な写しは信用性も証明力も共に高い

---

(C)ハッカー検事

### 【証拠能力の次は】



## 証拠の信用性と証明力

- 信用性(個々の証拠をどこまで信用できるか)
  - 出典の信用性→出所属性,技術的信用性,非人為性
  - 内容の信用性→自然かつ合理的で他の証拠と整合性
- 信用性ある証拠が集まって>証明力生成
- 証明力(直接証明or間接証明;間接証拠で推認)
  - 自白:裏付け証拠と秘密の暴露で真実性を判断する
  - 否認:①動機,②凶器,③結果,④手口,⑤直後の言動,  
⑥前足&後足,⑦遺留物DNA,etc.の総合判断

---

(C)ハッカー検事

## 証拠の信用性

(その証拠をどこまで信用できるか)

- ソース(出典)の信用性
  - 出所属性(人的信用,専門性,多数利用)
  - 技術的信用性, 非人為性(非供述証拠)
- 内容の信用性→自然かつ合理的
  - 自然性合理性: 経験則や論理法則と合致
  - 供述証拠: 臨場感・迫真性・秘密の暴露
  - ウラツケ証拠との符合性

---

(C)ハッカー検事

【実務での攻防: 否認弁解との闘い】

## 否認事件の弁解に学ぶ調査

- 犯人性(♪私はやってない～潔白だ～)
  - 現場に行っていない(ネットに接続していない)
  - 見ていただけ(真犯人は第三者)
- 犯意(♪それでも～故意は～故意～)
  - 間違えた(過失の抗弁)
  - 冗談です(冗談の抗弁)
  - 知らなかった(不知の抗弁)
- 犯罪事実(事実自体が不存在)
  - 被害者のねつ造(自作自演とかw)
  - 警察のデッチ上げ(国策捜査?)

---

(C)ハッカー検事

【独り言】

## 今一度振り返ると(補論)

- デジタル・フォレンジックは**技術と法律の融合**
- 調査→証拠化→公判立証→**裁判官の納得**
- ①どんな証拠で②何を立証するか
- 信用性と証明力を念頭に証拠化しよう
- 調査は、**常識と論理的整合性が前提**
- **事実認定は価値判断に先行する**
- **意見は証拠にならない(意見法則)**

---

(C)ハッカー検事

【エクスキューズ<(\_ \_)>】

## 終わりに

- **本講演は研究者としての個人的な見解です**
- **ハッカー**という言葉は、ハイテク犯罪等を行う者という意味でも使われるが、本来の語源は「コンピュータ技術に精通した者」という意味での尊称である（JIS-X-0001-1994 01.07.03～04参照）。
- 「**ハッカー検事**」の語源はこれと異なり、「**検事のくせにコンピュータや機械が好きな変な奴・変わった奴**」（命名明した先輩検事の定義）という「**変人の愛称(笑)**」に過ぎないものです。(^^ゞポリポリ
- **ご清聴ありがとうございました。m(\_ \_)\*)mぺコッ**  
本講演が皆さんの調査能力向上の一助になれば幸いです。

---

(C)ハッカー検事