

警察官のための

デジタル・ フォレンジック 捜査入門

富士崎 真治 著



立花書房

はしがき

インターネットが普及した現在では、人間の社会的な活動領域として、従前は現実世界の全てであると思われていた「フィジカル（物質的）空間」だけではなく、「サイバー空間」というデジタルデータで構築される仮想的な世界が観念されるようになっていきます。

そして、犯罪という社会現象もまた、サイバー空間にまで広がりを見せ、飛躍的に利便性が高まった情報通信技術等は、犯罪の手段としても悪用されるようになりました。

つまり、現在においては、フィジカル空間だけではなく、サイバー空間にも犯罪の痕跡が残されることから、デジタルないし情報通信技術を利用した犯罪捜査手法の習得が必要となっており、その代表的なものとして、「デジタル・フォレンジック」と呼ばれる捜査手法ないし捜査技術があります。

ただ、多くの捜査官にとって、デジタルとか情報通信技術という話は、近寄り難く、敬遠してしまいがちなもののように受け止められていたと感じていますし、我が国における文系・理系の区別や、理系の学問領域に固有のとっつきにくさなどが、そういった苦手意識の原因となっているようにも思っていました。

そのような中で、完全文系人間（!?）を自負される方にとっても、楽しみながら、デジタル・フォレンジック捜査技術の基本的な考え方を理解していただけるようなコンテンツが提供できないものかと考え、架空の事例を題材にして、コミカルな登場人物と一緒に事件捜査を追体験していただけるような物語調で、「警察官のためのデジタル・フォレンジック捜査入門」を作成しました。

ですので、読者の皆さまには、どうか、漫画でも読むような気楽な雰囲気、このコンテンツを楽しんでいただければと思っていますところであり、登場人物の台詞などが、実際の捜査活動のヒントとなれば、望外の幸せです。

なお、このコンテンツの内容は、元技術屋でもある筆者が個人的な立場で書いた個人的な見解であることを、あらかじめ御理解の上で、お楽しみいただければと思います。

また、このコンテンツは、「警察公論」での連載から始まりましたが、連載に当たり、様々な貴重な御意見や御示唆等を関係各位から賜っており、深く感謝を申し上げます。

特に、馬場野武部長や伊地山恒彦編集長、立花書房編集部関係者各位には、校正、編集そして親しみやすいキャラクターの作画等に至るまで、貴重な御示唆、御助言と御助力を頂きましたので、この場をお借りして、心からのお礼を申し上げます。

令和6年10月

富士崎 真治

◆ 目 次

第 1 回	路上強盗事案 ～バックアップデータからの復元	1
第 2 回	爆破予告事案 ～パソコンの基本構成要素	21
第 3 回	偽札事案 ～ソフトウェア編(上)【OS、アプリ】	44
第 4 回	昏酔強盗事案 ～ソフトウェア編(下)【データベース】	66
第 5 回	強盗傷人事案 ～Exif情報からの事実特定	83
第 6 回	銀行強盗事案 ～Webサービス情報の捜査利用	102
第 7 回	名誉毀損事案【インターネット/IPアドレス等】	116
第 8 回	脅迫、ストーカー事案【SNS】	136
第 9 回	脅迫事件の余罪(電子計算機使用詐欺罪) 【続SNS、暗号化メッセージアプリ】	152
第10回	傷害致死・死体遺棄と思いきや強盗殺人 ～デジタル・フォレンジック捜査の総決算【暗号資産】	168

完 結

※ 本電子書籍は、『警察公論2024年2月号(第79巻第2号)』から
『警察公論2024年11月号(第79巻第11号)』掲載分と同じ内容です。

警察官のための

デジタル・フォレンジック 捜査入門

第1回 路上強盗事案

～バックアップデータからの復元

神戸地方検察庁総務部検事

ふじさき
富士崎

しんじ
真治

今回の登場人物



【池大路 圭治】

N警察署刑事課の警部補。捜査一筋のバツイチ。従前の事件捜査に関する能力は高いが、デジタル・フォレンジック捜査に関してはサッパリ。出会って早々、白帽子からは「イケオジ」と呼ばれることに？



【課長】

N警察署刑事課の警部。部下からの信頼が厚く、周りからは親しみを込めて「カチョー」と呼ばれている。社会情勢の変化にも敏感で、デジタル・フォレンジック捜査に対して強い関心を抱いている。



【白帽子 桃】

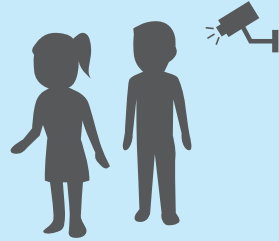
A県警察本部サイバー犯罪対策課（通称：サイ対策）のデジタル・フォレンジック担当技官。民間企業でホワイトハッカーとして従事後、いわゆるブラックハットと対峙すべく、警察へと転職した異色の存在。

◆事案（あらすじ）◆

N警察署刑事課の新任係長である池大路警部補は、強盗致傷事件を担当している。

この事件は、令和5年10月14日午後10時7分頃、N市内の路上で発生し、被害者の女性は、犯人の男から、ボールのような物で脅され、運転免許証やキャッシュカード等が入った財布を奪われた上、キャッシュカードの暗証番号も聞き出されていた。

被害者が襲われる直前、犯行現場付近の防犯カメラに、被害者の後ろをついて歩く犯人が映っており、その犯人が被疑者と似ていること、事件発生から約25分後、被害者のキャッシュカードがコンビニで使用されていたが、その際にも、被疑者と似た男




が防犯カメラ等に映っていたこと、また、この男がコンビニに乗ってきた車のナンバーの一部が分かり、条件に合致する24台の車両が割り出されたところ、被疑者がその車両所有者のうちの一人であったことなどから、被疑者の逮捕へと至った。

しかし、逮捕後、被疑者は黙秘しており、裏付け捜査も進まない状況で、池大路は、担当の才羽^{さいば}検事との事件協議に出掛けたものの、仏頂面で帰ってきた。

N警察署刑事課にて




カチョー、戻りました！



お疲れさん。で、才羽検事との事件協議はどうだった？




うーん……。可もなく、不可だけですね……。



それって、全然ダメってことじゃないか。でも、才羽検事のことだから、全くのゼロ回答じゃなかったんだろ？



まあ、そうなんですが、「顔貌鑑定に必要な特徴点が十分とれず、鑑定もできなかった防犯カメラ映像だけでは起訴するのが厳しいから、被疑者が犯行直後に被害品等を持っていたことなどを示す証拠は見当たらないの？」と言うんですよ……。そんな簡単に見つかれば、こっちも苦労しませんよ……。被疑者方のガサでも、被害品は出てきませんでしたし……。「言うは易く行うは難し」ですよ……。



盗品の近接所持か……。才羽検事は、そのあたりのヒントも言ってなかったのかい？





コンビニの防犯カメラに映った犯人と思われる男が、被害者のキャッシュカードを使ってATMを操作する前に、スマホをチラチラ見ている様子だったので、そのあたりに手掛かりがあるのではないかと行ってましたね……。

被疑者のスマホに、何か証拠になる情報はなかったのかい？



ダメですね。被疑者がパスコードを言わないので、スマホの中身が確認できないんですよ。

それなら、「サイ対課」に相談してみたいかい？



へ？

サイバー犯罪対策課の解析班だよ。スマホとかの解析をしてくれる所。





ああ、例の解析班ですか……。以前、「パスワードが分からないなら無理！」って言われたことがあったんで、今回も、無理かなと……。

最近、ハッキングが得意だという民間出身の解析官が解析班に着任して、活躍しているらしいぞ。難しい否認事件でも、彼女に相談したら、いい証拠を見つけてくれるらしい。



へえー、そうなんですか……。

ん？ なんだ？ あんまり乗り気じゃないみたいだな？



どうせ、また同じことを言われるだけですよ。「パスワードが分からないと無理！」ってね。

なら、被疑者は釈放で、被害者は泣き寝入りってわけか……。





いや、それは……。

じゃあ、何か打開策でもあるのかね、
係長殿？



えーっと……。さっそく、行ってまいります！

サイ対課デジタル・フォレンジックラボにて



すみませーん。最近、何でもハッキングして解決してくれる民間出身の解析官がやってきたって聞いたんで、ここに来てみたんですけど……。

はあ？





いやさ、ちょっと被疑者のスマホの解析をお願いしたいんだよね。

パスワードは？



分かりません……。

機種は？



たしかiPhoneだったと……。

バージョンは？



さあ？

パスワードは何桁？





忘れたよ……。

電源は？



押収時、電源オフは基本だろ？

そう……。なら、無理なんじゃない？



ほら見る。やっぱり無理じゃないか。

当たり前でしょ！ 署に来た人が、「財布を落としたんですけど、届いていませんか？ どこで落としたかも、どんな財布だったかも分かりません。手掛かりになることは、全部忘れまして。」って言ってきたら、あなたは一体どうするの？





とても丁寧な口調で、「俺をおちよくっているのなら、とっとと帰れ。」って言うんだろうね。

さっきのあなたの答え、それと同じレベルなんだけど……。さっき聞いたことが分からないなら、こっちも答えようがないわ。



なんだよ……。前の担当者は、そんな細かいこと言わなかったぞ、クソッ……。

クソッ？



いやっ……。それは聞き間違いだな……。仕方ない、被疑者を逮捕した若い衆に、そのへんのことを聞いてくるんで、ちょっと待っててくれ。

池大路は、いったん署の刑事課に戻り、被疑者を逮捕した後輩に事情を確認した後、再びサイ対課へと駆け込んだ。



確認したけど、最新のiPhoneで、パスコードは8桁の英数字だったと言ってたよ。これで、パスコードをチョチョイのチョイでハッキングしてくれるんだろ？

あなた、ガラケー時代の感覚でお願いしてきてない？



同じ携帯電話だろ？ 同じようにやってくれないの？

あのねえ。ガラケーのときは、パスコードも4桁の数字とかだったでしょ？今回は、その倍の8桁で、しかも、英数字のパスコードなのよ。何とおりのパスコードになるか、分かってるの？



いや……。なんとなくだけど、100万とおりにくらい？

〈著者紹介〉

ふじしんじ
富士崎 真治

大阪地方検察庁刑事部兼総務部検事
最高検察庁検察官事務取扱検事
前神戸地方検察庁総務部

〈主要著書〉

『サイバー捜査・デジタルフォレンジック実務ハンドブック
～実務家の分かりやすい解説とQ&A形式、
ケーススタディ形式で学べる捜査・実務の要点～』
(立花書房、2022年)

★本電子書籍は、『警察公論2024年2月号（第79巻第2号）』から『警察公論
2024年11月号（第79巻第11号）』掲載分を基に制作しました。

本電子書籍の全部または一部を無断で複写複製（コピー）することは著作権法
上での例外を除き、禁じられています。

警察官のためのデジタル・フォレンジック捜査入門【電子限定版】

令和6年11月15日 電子書籍発行

著 者 富士崎 真治

発 行 者 橘 茂 雄

発 行 所 立 花 書 房

東京都千代田区神田小川町3-28-2

電 話 03(3291)1561(代表)

FAX 03-3233-2871

<https://tachibanashobo.co.jp>