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～

倉持 俊宏 編集代表

吉田　正宏
宮　友一
河原塚 泰　著
原島　一郎
冨士﨑 真治

立花書房

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～

倉持 俊宏 編集代表

吉田　正宏
宮　友一
河原塚 泰　著
原島　一郎
冨士﨑 真治

立花書房

本書は、時々・情勢の必要に応じ、内容を変更・追加等する場合があります。

推薦のことば

昨今におけるデジタル技術、情報通信技術の加速度的な発展に伴って、これらを悪用した犯罪も頻発し、犯罪の匿名化・広域化が顕著なものとなっています。

このような社会情勢の変化に伴い、サイバー捜査やデジタルフォレンジックも一部の専門家のみが対応すればよいものではなくなり、捜査官一般において一定程度の知見を有することが求められるに至っています。

検察庁においても、同様の問題意識等から、本年４月、サイバー犯罪やデジタルフォレンジックを用いた事案等を収集し、全国的に共有すべき情報を管理・提供することなどを通じて各庁の捜査・公判を支援するため先端犯罪検察ユニット（略称 JPEC）を設立したところです。

今般、倉持俊宏検事の編著により「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」が発刊されることとなり、その執筆作業等は JPEC 設立の相当以前から JPEC とは独立して行われてきたものですが、平易な言葉を用い、Ｑ＆Ａ形式やケーススタディ方式を活用するなど、一般の捜査官にとっても親しみやすい内容となっております。

社会のデジタル化等が推し進められる状況において、サイバー捜査やデジタルフォレンジックを的確に行うことの重要性は益々高まるものと思われますが、本書がその一助となることを祈念しております。

令和４年２月

先端犯罪検察ユニット（JPEC）班長検事　　内藤　惣一郎

はしがき

皆さんは、サイバー犯罪と聞いてどのような印象を持たれるでしょうか？

難しい横文字が飛び交い、意味不明だ、と毛嫌いしていませんか？

通常の犯罪とは異なる捜査手法が必要になりそうで難しそう、あるいは、コンピュータなどに詳しい一部の人が捜査を担当すればいいから、自分には関係ない、などと思ったりしていませんか？

しかし、現代社会では、日常生活にコンピュータ、そしてインターネットをはじめとするネットワークが広く浸透しています。たとえば、街のあちこちに設置されている ATM も、コンピュータネットワークを利用したシステムの一部であり、利用者は ATM の画面越しに、金融機関のオンラインシステムにアクセスし、タッチパネルから情報を入力することで、現金を引き出したり送金したりしているのです。

このように、コンピュータネットワークは人の生活に溶け込んでいますし、一口に「コンピュータ」と言っても、そこには、一般的なイメージとしてよくあるデスクトップ型やノート型の PC のみならず、タブレット端末やスマートフォンも含まれるのです。

そして、このような機器を利用した犯罪が数多く発生し、コンピュータやそのネットワークに関する証拠収集に始まり、犯人の特定・検挙、事件の起訴と公判遂行は、もはや特別な犯罪類型特有のものではない、といっても過言ではありません。

本書は、犯罪の手段としてコンピュータやインターネットが利用されている事件や、コンピュータシステムで処理される情報を毀損するなど、直接的にコンピュータ等が犯罪の目的となっている事件などに関し、捜査計画を立案し、捜査活動を進めようとするときや、事件関係者の説明でコンピュータやインターネットに関する専門用語が出てきたときなどに、サイバー犯罪捜査に関する特別な指導・教養を受けたことのない捜査官でも一定の理解をすることができるよう、サイバー犯罪捜査に知見のある検察官及び検察庁でデジタルフォレンジックを担当する情報解析官が、Q＆A編では、具体的な犯罪類型ごとの捜査のポイントや、デジタル証拠の収集や分析について解説しており、ケーススタディ編では、具体的に想定される架空の事件を題材として、捜査上の問題点やその解決策をより具体的に紹介しています。

ただし、本書の内容は各執筆者の見解であり、検察庁としての公式見解ではないことをあらかじめお断りしておきます。

本書が現場における捜査活動の助けになれば幸いです。

なお、本書の発刊に当たり、馬場野武部長や本山進也参与、下村大志係長や中埜誠也係長等、立花書房出版部関係各位には、企画・編集段階から完成に至るまで、貴重な示唆、助言等を頂戴しました。ここに記して、特に感謝を申し上げます。

令和４年２月

編集代表　　倉持　俊宏

凡　　例

〈判例表記〉

判例の表記には、次の略号を用いた。

大審院判決明治 40 年 10 月 25 日大審院刑事判決録 13 巻 1194 頁
＝大判明 40・10・25 刑録 13・1194
最高裁判所判決昭和 50 年 7 月 1 日最高裁判所刑事判例集 29 巻 7 号 355 頁
＝最判昭 50・7・1 刑集 29・7・355
最高裁判所決定昭和 53 年 2 月 13 日最高裁判所刑事判例集 32 巻 2 号 295 頁
＝最決昭 53・2・13 刑集 32・2・295

なお、公刊物未登載のものは〈未〉と表示した。

〈法令表記〉（本文内にことわり書きがない場合は、下記表記を使用しています）

刑訴法	刑事訴訟法
不正アクセス禁止法	不正アクセス行為の禁止等に関する法律
児童ポルノ防止法	児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律
資金決済法	資金決済に関する法律
組織的犯罪処罰法	組織的な犯罪の処罰及び犯罪収益の規制等に関する法律

〈判例集・雑誌等略語表記〉

刑　録	大審院刑事判決録
刑　集	最高裁判所刑事判例集
民　集	最高裁判所民事判例集
高刑集	高等裁判所刑事判例集
東高時報	東京高等裁判所刑事判決時報
判　時	判例時報
判　タ	判例タイムズ
裁判所ウェブ	裁判所ウェブサイト
LEX/DB	LEX/DB インターネット

目　　次

第1編　Q & A 編

第1章　サイバー犯罪捜査総論

第２章　サイバー犯罪捜査各論

第１節　電子データの捜索押収

第２節　通信端末に関する捜査

スマートフォンには、どのような犯罪に関する痕跡が残っていますか？また、そのような痕跡は具体的にどのように発見・証拠化しますか？

第３節　メッセージ送受信に関する捜査

コンピュータは、文字や音声によるメッセージの送受信にも使われますが、それにはどのようなものがあるのでしょうか？　また、それらの履歴を捜査する際にはどのような部分に注意すべきでしょうか？

スマートフォンは、自らの位置をどのように特定するのでしょうか？　また、スマートフォンの過去の位置情報をどのように収集することができるでしょうか？

第４節　暗号資産（仮想通貨）に関する捜査

暗号資産（仮想通貨）に関する犯罪にはどのようなものがありますか？また、その捜査はどのように行われますか？

第３章　各種サイバー犯罪に対する捜査

第１節　ファイル共有ソフト関連犯罪

　ファイル共有ソフトにはどんな種類のものがありますか？　また、それらにはどのような違いがありますか？

　ファイル共有ソフトを用いた犯罪に対する捜査はどのように進めますか？

第２節　インターネット通信関連犯罪

　通信関係の犯罪にはどのような事例がありますか？　また、どのように捜査を進めていきますか？

　インターネット通信に関する事件の捜査を行うためには、どのような前提知識が必要になりますか？

第３節　インターネット利用犯罪

第４節　ウェブサイト関連犯罪

ウェブサイトに関連する犯罪にはどのようなものがありますか？　また、このような事案の捜査ではどのような点に留意する必要がありますか？

ウェブサイトへの投稿等が犯罪を構成する事案にはどのようなものがありますか？　また、その捜査上の留意点は何ですか？

ウェブ上における取引に関連する犯罪にはどのようなケースが想定され、どの罪名が適用されますか？

第５節　情報漏洩関係犯罪

情報を漏洩した場合、どのような犯罪が成立し得るでしょうか？　また、情報漏洩関係の捜査では、どのような点を解明することが重要でしょうか？

第4章　デジタルフォレンジック

第２編　ケーススタディ編

第１章　プロキシサーバを利用して行動を隠蔽した犯人による不正指令電磁的記録供用事案

第２章　特殊なソフトウェアを利用した威力業務妨害・脅迫等事案

第３章　Tor を利用して行動を隠蔽した犯人による不正アクセス禁止法違反、不正指令電磁的記録供用等事案

第４章　他人のインターネットバンキングに不正アクセスして不正送金し、ATM から現金を引き出した後、中国で主に用いられる電子マネー「AP」にマネー・ローンダリングして地下銀行を営んだ国際的なサイバー犯罪事案

第５章　キャッシュレス決済に関連する犯罪の擬律判断

第６章　不正なアカウント、決済用カード情報等を利用したインターネット上の電子商取引の犯罪捜査における財産犯の擬律判断、犯意の認定等が問題となった事案

第７章　暗号資産の不正流出にかかる捜査の留意点

第８章　電子マネーアカウントに、他人の金融機関口座を不正に紐づけて同アカウントに資金を移転し、コンビニエンスストアで出金するなどして不正利用した事案

第１編

Ｑ＆Ａ編

第１章　サイバー犯罪捜査総論

01　サイバー犯罪捜査とは

サイバー犯罪とはどのようなものを指しますか？　また、サイバー犯罪捜査とはどのようなものですか？

〔関係条文〕不正アクセス禁止法３条、刑法 168 条の２、168 条の３、著作権法 21 条、児童ポルノ防止法７条

１　サイバー犯罪とは

サイバー犯罪捜査についてお話しする前に、まず「サイバー犯罪とは何か？」について簡単に説明しましょう。

サイバー犯罪とは、不正アクセス禁止法違反、刑法のコンピュータや電磁的記録に関する罪、すなわち不正指令電磁的記録に関する罪や電子計算機使用詐欺、電子計算機損壊等業務妨害、電磁的記録不正作出の罪、及びコンピュータネットワークが利用された犯罪の総称とするのが一般的です。

一般に不正アクセス行為や不正指令電磁的記録（いわゆるコンピュータウィルス）関連の犯罪やコンピュータがダイレクトに連想される電子計算機使用詐欺等は、典型的なサイバー犯罪と感じられるでしょうし、それ故に何か難しそうだなあと思われるかもしれません。ただ、「コンピュータネットワークが利用された犯罪（以下「ネットワーク利用犯罪」と言います）」は、たとえば詐欺の手段としてネットワークが利用されるような場合ですから、SNS を通じて知り合った者同士が、その後ダイレクトメッセージのやりとりをし

て相手をだまし、現金を送らせてだまし取ったら、サイバー犯罪なのです。そうだとすると、日常生起する犯罪でも、サイバー犯罪に該当する類型のものが多いことは感じられるかと思います。

2　サイバー犯罪捜査とは

そこで、「サイバー犯罪捜査とはなんぞや」と改めて大上段に振りかぶって考えてみましょう。

……どうですか？　やはりよくわからないでしょうか？　しかし、典型的な、知人に嘘の話をして現金をだまし取る詐欺、コピー商品の販売等の著作権法違反、あるいは児童のわいせつ画像の作成・配布といった児童ポルノ防止法違反などであれば、どのような証拠を収集してどのような事実を立証すべきなのかは、イメージしやすいでしょう。

たとえば、対面で実行された知人間の詐欺であれば、まずは被害者からだまされた状況、現金を準備した状況や、それを相手に渡したときの状況を聴取して、調書化して、被害者の説明を元にして、二人が会って話をした日時や場所、取られたお金の出所、交付した日時場所といった、被害者の説明を裏付ける事実の確認といった捜査をしよう、と思い浮かぶはずです。このとき、犯人と被害者が同じアイドルを応援する人が参加するSNSで知り合い、遠方に居住していたことから、いつもSNSのダイレクトメッセージで会話をしていたところ、入手困難なライブのチケットが余っているから買わないかと持ちかけ、それを本当だと信じた被害者が、指定された口座に10万円を振り込んだが、犯人はチケットを持っていなかった…という詐欺だったらどうしますか？

サイバー犯罪捜査であっても、ネットワーク利用犯罪の類型であれば、通常の事件の捜査とやるべきことは変わらないのです。ただ、収集すべき証拠の全てもしくは大半が、コンピュータネットワークに存在するのがサイバー犯罪の特徴です。

第２章　サイバー犯罪捜査各論

第１節　電子データの捜索押収

07　電子データの押収～押収総論

電子データの押収はどのように進めますか？　また、その際の留意点は何ですか？

〔関係条文〕刑訴法 218 条、110 条の２、123 条３項、220 条２項、111 条の２、111 条１項、99 条の２、219 条１項、106 条

１　捜査において電子データの押収はどのようにするのですか

刑事訴訟法において、押収方法として任意捜査と強制捜査がありますが、電子データに関してもこの点は変わりません。

任意捜査による場合は、どのように証拠化するか、これといった決まりはありませんが、強制捜査、この場合であれば刑訴法に基づく捜索・差押え（刑訴法 218 条、電子データであれば同条２項）や検証の結果に基づいて証拠化していくことになります。

まず、捜索・差押えについては、刑訴法は有体物を想定しているので、原則は電子データが記録された記録媒体やそれと一体となっているコンピュータ等の有体物を差し押さえることになります。

差押状の執行の際には、執行者すなわち捜査機関は、「電磁的記録に係る記録媒体」として、記録媒体そのもの（ハードディスクなど）やその記録媒

体を内部に有するコンピュータ自体を差し押さえることもできますが、状況に応じて、執行者側の判断で、必要な電子データを、複写（単なるコピーや暗号化されたデータを復号して記録することも同一性が認められるので含まれる。）、移転（コピーではなく、元データを複写するとともに元データを消去するいわゆる「移動」）した記録媒体や印刷した紙等の媒体を差し押さえることもできます（刑訴法 110 条の２）。

この場合、複写元の電子データを複写して記録するための複写先の記録媒体については、差押えを受ける側が用意する場合もあれば、差押えをする側が用意するのでもかまいません。

なお、「移転」の場合には、電子データを移転した記録媒体について、刑訴法 123 条３項、同法 220 条２項に留意する必要があります。

2　差押許可状の執行の際に電子データの複写、移転、印刷は誰がするのですか

刑訴法 110 条の２第１項では、差押許可状の執行は捜査機関において行うことが前提となっています。

しかし、捜査機関において必要とする電子データを探しだしたり、セキュリティを解除したり、これを適切に記録等したりするのに困難が伴うことも多くあります。そこで、刑訴法 110 条の２第２項では、「差押えを受ける者」に電子データを他の記録媒体に複写、移転させ、あるいは紙媒体等に印刷させることができるとしています。

また、記録、移転や印刷を被処分者にさせる場合に限らず、捜査機関においてする場合にも、被処分者に対しては、「電子計算機の操作そのほかの必要な協力を求めることができる。」（刑訴法 111 条の２）として、その差押え等の目的を達成するために必要な協力を求めることができます（協力要請）。

求めることができる協力の具体的な内容は、事案に応じていろいろですが、「電子計算機の操作」のみならず、システム構成やファイルの存在場所の指示、暗号化されたファイルの復号なども含まれます。

この協力要請は、要請を受けた相手方に対して、協力を法的に義務づける

第３章　各種サイバー犯罪に対する捜査

第１節　ファイル共有ソフト関連犯罪

15　ファイル共有ソフト関連犯罪捜査～総論

ファイル共有ソフトにはどんな種類のものがありますか？　また、それらにはどのような違いがありますか？

〔関係条文〕著作権法 23 条、119 条１項

１　ファイル共有ソフトとはどのようなものですか

ファイル共有ソフトとは、インターネットを利用して不特定多数の利用者とファイルをやりとりするためのソフトウェアです。

ファイルをインターネット上でやり取りし、共有するだけであれば、それを実現するためのソフトウェアやインターネットサイトは無数にあります。

その中でも、その手軽さから、以前から多くの犯罪等に利用されてきたのが、P2P 接続（Peer-to-Peer 接続）によるファイル共有ソフトです。以下では、このような P2P 接続を利用したファイル共有ソフトについて「P2P 型ファイル共有ソフト」と言って説明していきます。

まず、「Peer」とは「同等の立場」を意味するもので、ファイル共有ソフトの中でも、「Winny」や「Share」などは「ピュア P2P 型」のファイル共有ソフトに該当します。この「ピュア P2P 型」のファイル共有ソフトは、ネットワークに参加しているコンピュータ同士で、ファイルのデータをやり

取りし、そのファイルの検索に関する情報についても、参加しているそれぞれのコンピュータの接続先を伝言ゲームのようにたどって発見しフィードバックを得る仕組みになっており、固定されたサーバの存在を全く必要としないものです。

これに対して、「BitTorrent」等の一部のファイル共有ソフトについては、共有するデータの情報をサーバ（＝インデックス・サーバ）が管理するものもあり、「ピュア P2P 型」と区別して、その接続形態や接続するコンピュータの役割分担の携帯に応じて「ハイブリッド P2P 型」、「スーパーノード P2P 型」などと呼ばれます。

ただ、いずれにしても、捜査において利用できる情報の痕跡は、基本的にはファイル共有ソフト利用者が、実際に使用した端末以外には残らないと考えるべきです。

2　P2P 型のファイル共有ソフトにはどのようなものがありますか

話題になった中で、古いものでは「WinMX」「Napster」といったものがあります。中でも、P2P 型のファイル共有ソフトの草分け的存在として、Winny（ウィニー）が 2002 年に登場してから脚光を浴びるようになりました。

現在よく利用されている P2P 型のファイル共有ソフトの代表的なものは

Share（シェアー）
PerfectDark（パーフェクトダーク）
Cabos（カボス）

といったものがあります。

他に、犯罪に利用され、検挙例があるものとしては

Shareaza（シェアーザ）
LemonWire（レモンワイアー）
Vuze（ヴューズ）

といったものがあります。

第４章　デジタルフォレンジック

31　デジタルフォレンジックとは

デジタルフォレンジックとはどのようなものですか？

〔関係条文〕刑法 168 条の２第１項、刑訴法 218 条２項

１　はじめに

サイバー空間と呼ばれるコンピュータネットワークの中で行われるサイバー犯罪に対する捜査では、ネットワークへの入り口であるパーソナルコンピュータやスマートフォンなどの利用者が通信に使用した機器やネットワークの途中にあるサーバコンピュータやネットワークスイッチ等の通信を中継している機器などから操作や通信のログを取得するほか、ネットワーク上の公開されている通信を監視することによって捜査の端緒となるデータを収集することも行われます。

一方で、一般的な刑事事件に対する捜査においても、様々な分野での電子機器の普及にともない犯罪の証拠がデジタルデータとして存在することから、電子機器とそこに保存されているデジタルデータに対する捜査が必要となる場面が増えています。

例えば、駅や繁華街の街角やコンビニなどの店内などに設置されている防犯ビデオカメラ[1)]、今や多くの車両に取り付けられているドライブレーダー[2)]、ほとんどの人が持っている小型の通信用コンピュータであるスマートフォン[3)]、事業所において事務機器として必須であるパーソナルコン

ピュータなど、ざっと周りを見渡しても様々な電子機器が普及し、これらの機器は画像や文書、ログなどの様々な情報をデジタルデータとして保存しています。ですから、それらの中には事件の証拠データと言える「犯行状況が撮影されている画像」や「謀議を行った電子メールやメッセージ」などといった証拠がデジタルデータとして記録されている訳です。

このような犯罪の証拠であるデジタルデータとそれを保存している証拠物である電磁的記録媒体を、事件捜査や公判遂行のために法的、技術的に適切に取り扱う手法や技術のことをデジタルフォレンジックと呼んでいます。

デジタルフォレンジックという言葉を知っている人は、パソコンなどのコンピュータを解析するイメージが強いと思いますが、コンピュータ以外でも、例えば、外付けハードディスクやUSBメモリといったストレージ[4)]やデジタルカメラやICレコーダーなどに内蔵されている記憶領域なども対象になりますし、例えばJPEG[5)]などの写真1枚だけのデータのみであっても対象になります。

デジタルフォレンジックは民間における不正調査等でも使われる手法でもあるので、その定義はいくつかありますが、警察白書[6)]では「犯罪の立証のための電磁的記録の解析技術及びその手続」とされていますし、特定非営利活動法人デジタル・フォレンジック研究会[7)]では「インシデントレスポンス（コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を言う。）や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」としています。

また、デジタルフォレンジックは「デジタル鑑識」と呼ばれることもありますが、犯罪捜査に限れば当を得ていますし、鑑識において重要である「証拠の収集および保全」はデジタルフォレンジックでも重要なパートですから、デジタルフォレンジックの定義は「証拠である電磁的記録を押収、保全、解析するための手法および技術」と表現しても良いのではないでしょうか。

第２編

ケーススタディ編

第１章　プロキシサーバを利用して行動を隠蔽した犯人による不正指令電磁的記録供用事案

１　はじめに

⑴　不正指令電磁的記録に関する罪

不正指令電磁的記録に関する罪に関しては、近時、検挙件数も増加しているところであり、特に供用罪、保管罪に関しては、立件・捜査のノウハウに関しても比較的、蓄積されているところです。本題に入る前に、念のため、不正指令電磁的記録の定義や構成要件の概要について確認しておきます。

不正指令電磁的記録とは、①人が電子計算機を使用するに際して、②その意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき③不正な指令を与える電磁的記録（刑法168条の２第１項１号）と、④不正な指令を記述した電磁的記録その他の記録（同項２号）です。

そして、正当な理由がないのに、人の電子計算機における実行の用に供する目的でこれら電磁的記録その他の記録を作成・提供すること（同項）や、取得・保管すること（168条の３）、そして、不正指令電磁的記録（168条の２第１項１号）を正当な理由がないのに人の電子計算機に供用する行為（168条の２第２項）を犯罪としています。

１号の「電磁的記録」というのは、コンピュータ上でそのまま実行することができるプログラムのことです。

２号の「不正な指令を記述した電磁的記録その他の記録」というのは、そのままではコンピュータ上で実行することはできませんが、不正プロ

グラムを作り出すことができるような指令（コード）が記録されているもの（例を挙げれば、マルウェアのソースコードのデータやそれが印字された紙）です。

あるプログラムが不正指令電磁的記録に該当するか否かは、前記②の要件、つまり人が電子計算機を使用するに当たり、使用者の意図に沿うべき動作をさせない、あるいは意図に反する動作をさせるようなプログラムかどうか、ということが検討されることになります。

⑵　不正指令電磁的記録における供用罪

一般的に、ユーザが想定していない動作をする場合、たとえば普通の表計算ソフトだと認識してインストールしたところ、表向きは通常のアプリケーションの動作をしていますが、バックグラウンドで攻撃者が準備したウェブサイトに定期的にアクセスし、同サイトからの命令を受信するとインストールされているPCの操作権限を乗っ取り、bot化（他人のPCを遠隔地から自己の支配下に置いてコントロール可能な状態にすること）するプログラムだったようなケースは、そのようなサイトへのアクセスをユーザが許可しておらず、また操作が乗っ取られて制御不能になるようなことを意図しているはずもありませんので、これが不正指令電磁的記録であると容易に判明します。

しかし、ユーザの意図に反するか否か、については線引きが難しい問題もありますので、慎重な検討を要するケースもあるでしょう。そこで、不正指令電磁的記録の供用罪の立件を目指した事件において、犯人にたどり着くまでの流れを紹介します。

第２章　特殊なソフトウェアを利用した威力業務妨害・脅迫等事案

１　はじめに

以前は、「２ちゃんねる」（現在の「５ちゃんねる」、以下同じ）等インターネット上の掲示板や、ブログのコメント欄やSNS上のコミュニケーションスペース等への犯罪予告の書き込みについては、言ってしまえば「ありふれた」というか言わば「カジュアル」に、一部のインターネットユーザに受け入れられていたような風潮がありました。

しかしながら、それによって迷惑を受けた被害者が次第に声を上げるようになり、加えて、警察がそれらの事案について着々と捜査を進め、実績を出してきたため、現在では、そのような犯罪予告の情報については収集されて、即座に警察へ通報・報告され、その捜査の結果、脅迫や業務妨害事件として立件・処理される、というのが現在の通常の流れであるとインターネットユーザの間では認識されるようになっています。

そのような中、当初はそのように粛々と犯人が検挙され、手続が進められているものと思われていたのに、実は真犯人が別に存在することが後に判明し、社会・そして捜査機関に衝撃を与える事件が発生しました。いわゆる「遠隔操作ウィルス事件」です。

なお、本項は、上記事件から着想を得た架空のケーススタディであることをお断りしておきます。

2　事案の概要

被疑者は

① 掲示板に自分が作成したPHPプログラムへのリンクを書き込み、某日、それを知らずにリンクをクリックした甲のPCのブラウザから、前記プログラムを実行させ、A市役所の「市民の声」ページから、市内の小学校を襲撃する旨の内容が記載されたメールをA市役所のメールサーバに送信させて、これを市役所職員に閲読させ、小学校の通常業務を妨害した

② 情を知らない乙が使用するPC上で実行中のプログラム（Sとします）に対し、ある掲示板を介して命令を送信し、これを受信したSを用いて、乙のPCから某掲示板に、Bを殺害する旨を書き込ませ、これを閲読したBを脅迫した

というものです。

脅迫文を受信ないし書き込まれたサーバコンピュータからたどると、それを送信したのは甲のPCであり、乙のPCです。結果的に、それらを実際に送信したのも甲のPCであり、乙のPCでした。

第1章の解説で説明したとおりですが、サーバコンピュータが記録する接続元のPCについては、直接サーバにアクセスしてきたPCに関する情報ですから、サーバコンピュータのログを確認すれば、犯罪予告文を送信したのは、それぞれ甲のPCと乙のPCだと容易に判明することとなります。ただ、第1章の事件と異なり、海外の匿名プロキシサーバ（プロキシとは、「代理」という意味であり、「プロキシサーバ」とは、その名の通り他のコンピュータの「代理」として他のサーバと通信するサーバのこと）が利用されていない本件では、捜査は比較的容易だと思われました。

しかし、実際は、甲も乙も、自分のPCがいわば「踏み台」として真犯人に利用されただけでした。

「賢い」犯罪者は、たとえそれがサイバー空間内での犯行だとしても、自分には容易にたどり着けないように、様々な策を講じるものです。

インターネット上で何らかの行動をすれば、サーバコンピュータにもクライアントコンピュータにも何らかの痕跡が残されます。

第３章　Tor を利用して行動を隠蔽した犯人による不正アクセス禁止法違反、不正指令電磁的記録供用等事案

１　はじめに

本編で紹介するケースは、相応に知識のある人物がサイバー犯罪を実行した事案です。いかにして、捜査機関が犯人を捜し出したのかを説明していきます。

さらに、サイバー犯罪の典型として不正アクセス行為と同様に挙げることができる、コンピュータウィルス（不正指令電磁的記録）に関する罪の適用の是非についても触れてみたいと思います。

２　事案の概要

被疑者は

① 甲社の管理するサーバに不正アクセスし、管理者権限を有する ID に対応するパスワードを変更するなどした上、同サーバの OS を再インストールしてサーバのデータを削除した

② 乙社の運営するオンラインショッピングサイトにおいて、他人のクレジットカード情報を入力することで、同サイトで販売しているユーティリティソフトを購入する手続をし、その情報に従い、サイト上でソフトをダウンロードできる状態にした

③ ランサムウェアを作成するためのツールを入手した上で、これを使ってランサムウェアを作成し、第三者の PC で実行させた

というものです。

3　捜査の開始

本件は、サイバーパトロールにおいて、「ランサムウェアに感染させた」という内容のSNS上の書込を捜査員が発見したことが始まりです。

ランサムウェアとは、マルウェア（スパイウェア等、不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェア）の一種であり、これに感染し、ソフトウェアが実行される状態になると、そのPCユーザの意に反する動作をすることになり、「不正指令電磁的記録」に該当することとなります。

そこで、コンピュータウィルスに関する罪の被疑者と思料されるSNSユーザについて、調査が進められることになりました。そのユーザのSNSアカウントは明らかですが、そのアカウントの接続履歴を照会したところ、ログインには全てTor（IPアドレスを相手に知られることなく、インターネットに接続したり、メールを送信したりできる匿名の通信システム）が用いられていました。

そのことから、Torにおけるノード（ネットワークの節点のことで、コンピュータネットワークではサーバ、ハブ、ルータ、アクセスポイント等）のIPアドレスは分かるものの、どこからTorを経由して、SNSにログインしたものなのかについては、全く分からない状況でした。

捜査員は、SNSアカウントの接続ログによらずに、このSNSアカウントの利用者を割り出さなければならないこととなりました。

4　採用した捜査手法

⑴　SNSのモニタリング

被疑者ではないかと考えられたSNSアカウント（ここでは仮に「A」としておきます）のユーザにつき、その属性（性別、年齢、職業、行動パター

第4章　他人のインターネットバンキングに不正アクセスして不正送金し、ATMから現金を引き出した後、中国で主に用いられる電子マネー「AP」にマネー・ローンダリングして地下銀行を営んだ国際的なサイバー犯罪事案

1　意　　義

これから紹介するケースは、平成25年以降毎年数十億円の被害が生じているインターネットバンキングを利用した不正送金に関連し、国外及び国内の犯罪グループのメンバーが連絡を取り合いながら、送金後の犯罪収益のマネー・ローンダリング及びその運用が行われた国際的なサイバー犯罪の事案です。

不正送金は、金融機関の対策によって一時期より減少傾向にあるものの、依然として多額の被害が生じており、犯罪グループの狙いはメガバンク等の都市銀行にとどまらず、地方銀行、信用金庫等をも対象としており、全国の捜査機関において捜査を行っています。

また、本件は、サイバー犯罪であるインターネットバンキングの不正送金の捜査から始まるものの、その後のマネー・ローンダリングは、サイバー犯罪のみを前提とする犯罪ではなく、その問題点に関する検討や捜査手法は、この種マネー・ローンダリングの捜査に従事する捜査官においても一般に参考となると考えられることから、ここで紹介する次第です。

2　事案の概要

⑴　A１（出し子）関連の事件

ア　不正送金

まず、前提となる不正送金の犯行状況について、紹介したいと思います。

本件の犯人グループ（国外に拠点を有するとみられます。）は、何らかの方法で、日本の金融機関のインターネットバンキング利用者のID及びパスワードを不正に入手しました（ID等を不正に入手する手法は、対象のPCをマルウェアに感染させてログイン情報を抜き取るケース、フィッシングサイトと呼ばれる偽サイトにアクセスさせて情報を入手するケースなど多数の手法が確認されています。）。

次に、この犯人グループは、当該ID等を用いて、当該インターネットバンキング利用者のアカウントに対して、不正にログインをしました。

これは、不正アクセス行為等の禁止等に関する法律（以下「不正アクセス禁止法」といいます。）、２条４項１号に規定される不正アクセス行為に該当し、同法４条違反を構成します。

そして、犯人グループは、不正なログイン状態を利用して当該インターネットバンキング利用者の預金から犯人グループが第三者から不正に入手した預金口座に送金する操作を行いました。

この操作は、電子計算機使用詐欺（刑法246条の２）に該当するとともに、犯人グループに属しない第三者の口座に送金することで犯罪者が得た犯罪収益等の帰属を仮装する行為といえるため、犯罪収益等仮装（組織的な犯罪の処罰及び犯罪収益等の規制等に関する法律10条（以下「組織犯罪処罰法」といいます。））も構成します。

第５章　キャッシュレス決済に関連する犯罪の擬律判断

１　意　　義

令和元年 10 月１日から消費税率が 10 パーセントとなりました。

この増税に伴い、政府は、いわゆるキャッシュレス決済の普及に努め、当時は軽減税率も導入していました。

これに対応し、従前から存在したデビットカード、クレジットカード等にとどまらず、事前にアカウント等にいわゆる電子マネーをチャージした上、スマートフォンを用いて QR コードを読み取らせる形式、スマートフォンに内蔵された非接触式チップを店舗の端末に読み取らせる形式等種々の手法を組み合わせた決済手段が定着しつつあります。

そして、これらの新たな決済手段を悪用した犯罪も急増しています。

近年、コンビニエンスストアチェーンが提供を開始した QR コード決済につき、利用開始から数日の間に多額の不正利用が行われ、最終的に同決済は利用廃止となりました。これらの犯罪に対しては、犯罪を防止するための事前のセキュリティ構築が重要です。

他方、厳重なセキュリティは、ユーザーの利便性と相反し得るため、民間事業者のセキュリティ構築のみによって問題解決を図ることは困難です。

よって、不正利用が発覚した際、捜査機関がこれに的確に対応する必要があります。

これらのキャッシュレス決済を悪用した犯罪は、前提として不正アクセス等のサイバー犯罪を伴うものが多いものの、店頭における詐欺罪等に該当する知能犯としての側面、商品を購入する際の帰属の仮装、犯罪収益である購

入商品等の処分に関するマネー・ローンダリング罪としての側面、海外の犯罪集団があらかじめアカウント情報を不正に入手し、国内所在の者と連携して犯行に及ぶ外事犯罪、組織犯罪としての側面もあります。

各警察によって、キャッシュレス決済の不正利用をいかなる部署が扱うかは異なると思われますが、これらの複合的な側面が含まれる犯罪であることを把握して的確に対応する必要があるため、ここに取り上げる次第です。

2　事案の概要

⑴　ポイント利用の仕組み

本章で取り上げるのは、通信販売業者が展開するポイントの不正利用の事案です。

まず、そのポイントの発生及び利用の仕組みを簡単に説明します。

本件では、前記業者はインターネット上の通信販売サイトを運営していたところ、当該業者が発行するポイントを得るには、当該ウェブサイトにおいて、事前に電話番号等の一定の情報を登録してアカウントを作成する必要がありました。

そして、そのアカウントにログインして商品を購入することで、購入額等に応じて当該アカウントにポイント等が付与されました。

付与されたポイントは、当該ウェブサイトで更に商品を購入する際に利用することもできますが、これ以外にも提携する実店舗等で商品を購入することが可能となっていました。

そして、店舗でポイントを使用するには、スマートフォンで当該通信販売業者のアプリをダウンロードし、当該アカウントでログインした上、QR コードを表示させて読み取らせたり、ポイントを利用できるよう紐付けた提携店舗のカードを呈示したりする必要がありました。

このようにスマートフォンでアカウントにログインして QR コード等を表示させる決済の態様は、事前にアカウントを作成し、電子マネーを当該アカウントにチャージし、スマートフォンのアプリで QR コード等を表示させて商品を購入するキャッシュレス決済と態様が符合します。

第６章　不正なアカウント、決済用カード情報等を利用したインターネット上の電子商取引の犯罪捜査における財産犯の擬律判断、犯意の認定等が問題となった事案

１　意　　義

現在の電子商取引においては、市民のほとんどが所持しているスマートフォンさえあれば、インターネット上のいわゆる通信販売サイトにアクセスし、商品やサービスを購入し、商品であれば指定された場所に送付させて受領できます。

このような利便性から、非対面による電子商取引、すなわちインターネット等を利用した通信販売等の市場規模は拡大しています。

経済産業省による電子商取引に関する市場調査の結果によれば、電子商取引の規模は年々増加し、平成 30 年における消費者向け電子商取引の市場規模は、年間 18 兆円（前年 16.5 兆円、前年比 8.96％増）に達しているとされます（経済産業省ウェブサイト https://www.meti.go.jp/press/2019/05/20190516002/20190516002.html より引用）。

かかる電子商取引の拡大に伴い、犯罪の手段としての電子商取引の不正利用も散見されるようになりました。

これらの電子商取引を用いた犯罪は、従前の対面における商品等の不正取得に関する擬律判断、捜査手法を当てはめることができるケースもあるものの、電子商取引の特性に応じ、擬律判断や捜査手法を再検討すべきケースが存在します。

すなわち、擬律判断としては、電子商取引の場合、対象となる商品の送付手続等により、窃盗罪、詐欺罪、電子計算機使用詐欺罪等の財産犯のうちいかなる罪が適用されるか異なります。

また、対面で即時に商品が交付されれば占有の移転時期は明確ですが、電子商取引における送付型の犯罪においてはいかなる時点で占有が移転したのかも検討の必要があります。

さらに、この種の犯罪は、インターネットで商品を注文する者と、コンビニエンスストア等で商品を受領する者等複数名がそれぞれ役割を分担して犯行に関与するケースも存在し、特に商品を受領する者における犯意の認定も重要な問題点となり得ます。

本章では、これらの電子商取引を利用した商品の不正取得等の犯罪類型の捜査における留意点につき、具体的なケースを紹介しながら論じたいと思います。

2　事案の概要

本稿では、以下に紹介する二つのケースを検討の題材として取り上げます。

⑴　アカウント不正利用によるスマートフォンの不正入手（事案1）

一つ目の事案は、携帯電話事業者のアカウントを不正利用し、最新のスマートフォンを不正に取得した事案です。

犯人グループは、何らかの方法で入手したIDとパスワードを利用し、いわゆるリスト型攻撃を行い、多数の携帯電話事業者のアカウントにログインできる状況を作出しました。

次に、犯人グループは、携帯電話事業者のオンラインショップに、前記のリスト型攻撃で得た多数のアカウントでログインし、各アカウントの正規利用権者が登録した支払方法に基づき、当時の最新機種のスマートフォンを購入する手続を行いました。

第７章　暗号資産の不正流出にかかる捜査の留意点

１　はじめに

本章では、近年その存在が着目される暗号資産（いわゆる仮想通貨一般を指します。資金決済に関する法律（以下「資金決済法」といいます。）の改正によって「仮想通貨」が「暗号資産」と呼称変更されたことを踏まえ、暗号資産と呼称したいと思います。）の不正流出事例を紹介します。

⑴　暗号資産について

暗号資産は、ブロックチェーン（分散型台帳とも呼ばれます。）に基づき、その取引履歴がネットワークに接続するコンピュータ機器等に分散して保存され、特定のサーバー等に依存せずにデータが保管されるため、故障やサイバー攻撃によって特定の機器が稼働しない状態が作出されても、取引等が阻害されるリスクが少ないとされています。

また、ブロック単位でデータが保管されるため、特定のブロックのデータを改ざんしても、前後のブロックとの整合性が取れなくなるため、履歴の改ざんが困難であることも特徴と評価されています。

これらの特徴から、暗号資産は、決済方法、国境をまたいだ迅速な送金手段、金融商品などとしてその存在が注目され、その基幹技術であるブロックチェーンについては、他の分野における技術の利用も期待されています。

国外においては、新たな暗号資産が次々に生み出され、これらを取引の対象とする暗号資産交換所も多数開設されているほか、米国においては、SNS を運営する IT 企業を中心とした団体が次世代の決済手段としての暗号資産を開発しているとされ、様々な議論を巻き起こしています。

国内に目を向けると、同様に暗号資産交換所が増加し、暗号資産が金融商品として活発な取引の対象となっており、代表的な暗号資産ビットコインが国内の小売店で決済手段として利用できるようになったことなどから、市民にも一定程度認知されているようにみえます。

⑵　負の側面とは

他方、暗号資産の負の側面として、その性質上、インターネットを通じて容易にデータの移動が可能であるため、国境をまたいだマネー・ローンダリングに用いられやすいという大きな問題が存在します。

また、マネー・ローンダリングが容易に行えることを前提に、いわゆるダークウェブと呼称される、一部のウェブサイト群における禁制品等の取引の決済手段として、暗号資産が定着しつつある現状も看過することはできません。

国内における暗号資産を巡る犯罪としては、いわゆるマウントゴックス事件を皮切りに、平成 30 年 1 月に甲社が運営する暗号資産交換所から顧客財産を含む 580 億円相当の巨額の暗号資産が不正に流出し、同年 9 月にも、乙社が運営する暗号資産交換所から多額の暗号資産が不正に流出するなど、不正流出事件が目立っています。

しかし、以上に述べたマネー・ローンダリング、不正流出にかかる諸犯罪以外にも、金融商品としての暗号資産の規制にかかる金融商品取引法違反等の経済犯罪、決済で用いられる場面における詐欺等の財産犯罪など多様な犯罪類型が想定され、これらは当然にサイバー空間で行われサイバー犯罪のカテゴリーにも属するもので、その捜査における犯人特定の捜査における着眼点、法律適用に関する問題点等を把握しておくことは有用であると考え、本章で取り上げた次第です。

第８章　電子マネーアカウントに、他人の金融機関口座を不正に紐づけて同アカウントに資金を移転し、コンビニエンスストアで出金するなどして不正利用した事案

１　はじめに

近年、キャッシュレス決済が普及している状況は従前に述べましたが、これらのキャッシュレス決済で用いられる各電子マネーアカウントはそれ単体ではなく、金融資産等に紐づけて用いられることが通常です。すなわち、何らかの金融資産等とキャッシュレス決済のアカウントを紐づけることで、電子マネーを手軽にチャージし、様々な場面で電子マネーを用いることができるというものです。

その手段としては、各人が契約する携帯電話事業者の月毎の利用料金に紐づけるケースなどに加え、各人が保有する金融機関の預貯金口座に紐づけるケースが多くみられます。

金融機関の預貯金口座の資金を電子マネーに移転することは、各国政府が推進を図るいわゆる FinTech の一部と考えられており、保有資産を流動的に用いることが可能となるため、電子マネーの利用を活性化するのみならず、資金の流動化が進むことによって経済を活性化させ、好影響を与える効果も期待されます。

他方、預貯金口座等を電子マネーと紐づけることは、多額の預貯金を電子マネーとして不正利用されるリスクもはらんでいます。

本件は、犯人たちが不正に作成した電子マネーアカウントに、他人の銀行口座情報を不正に紐づけ、同アカウントと提携しているコンビニエンスト

アの現金自動預払機（以下「ATM」といいます。）から多額の現金を引き出した事案であって、まさにFinTechによる金融資産の流動化の一場面においてリスクが顕在したものと言えます。

このような資金移動が悪用された場合、いかなる犯罪が成立し得るのかという観点は、捜査機関として留意すべき視座を多く含んでおり、FinTechの普及が予想される今後も同種事案を取り扱う可能性が高いことから本稿で取り上げた次第です。

２　事案の概要

①　犯行の流れは以下のとおりですが、主犯格のＡ１以外に、実行犯として一部犯行に関与するＡ２及びＡ３が登場します。主犯格であるＡ１は、かねて財産犯等を繰り返していたところ、被害者Ｖを含む多数の預貯金口座情報（口座名義人氏名、暗証番号等）を不正な手段によって入手しました（その手法については模倣犯を防止する観点から記載を控えます）。

②　多数の口座情報を得たＡ１は、これを用いて多額の利得を得ようと考え、近時、預貯金を電子マネーに移転させることが可能となったことに着目しました。そして、電子マネーＤのアカウントを得るためには携帯電話回線が必須であったところ、Ａ１は、自己の犯罪への関与を隠匿するため、知人のＡ２に報酬を約束し、Ａ２名義でＡ１が使用するための携帯電話回線の契約を行わせ、同時に当該電話回線を利用できるスマートフォン１台を購入させました。

③　その上で、Ａ１は、かねて金銭トラブルによって身分証等を取り上げるなどして自己の手駒として利用していたＡ３につき、後の電子マネーの現金化の作業に従事するために呼び出した上、Ａ２が入手したスマートフォンを使用して電子マネーサービス「Ｄ」のアプリをインストールし、Ａ２が契約した携帯電話番号を用いて電子マネーＤのアカウントを作成しました。

用語索引

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／著者等紹介

（令和４年２月現在）

【編集代表・著者】

倉持 俊宏（くらもち　としひろ）　東京高等検察庁刑事部検事、前札幌高等検察庁検事、元横浜地方検察庁刑事部副部長、元福島地方検察庁次席検事、元東京地方検察庁刑事部検事、元宇都宮地方検察庁栃木支部長、元東京地方検察庁刑事部サイバー係検事等

【著　　者】

吉田 正宏（よしだ　まさひろ）　東京地方検察庁総務部 DF センター情報解析官、前東京地方検察庁特別捜査部 DF 班統括捜査官、元最高検察庁総務部情報システム管理室主任捜査官等

宮　友一（みや　ともかず）　札幌地方検察庁特別刑事部検事、前神戸地方検察庁姫路支部検事、元東京地方検察庁刑事部サイバー係検事等

河原塚 泰（かわはらつか　ゆたか）　千葉地方検察庁特別刑事部兼先端犯罪検察ユニット（JPEC）ユニットサポーター検事、前一般財団法人日本サイバー犯罪対策センター（JC3）派遣、元法務研究員「サイバー犯罪をめぐる諸問題」等

原島 一郎（はらしま　いちろう）　大阪地方検察庁刑事部サイバー係兼総務部 DF センター担当兼特別捜査部兼先端犯罪検察ユニット（JPEC）最高検指名検事、前東京地方検察庁刑事部サイバー係検事兼最高検察庁刑事部検察官事務取扱（サイバー・DF 担当）、元一般財団法人日本サイバー犯罪対策センター（JC3）派遣等

冨士﨑 真治（ふじさき　しんじ）　名古屋地方検察庁刑事部サイバー係兼先端犯罪検察ユニット（JPEC）サポーター検事、前大阪地方検察庁刑事部サイバー係検事兼総務部 DF センター担当検事、元国立研究開発法人情報通信研究機構（NICT）派遣、元民間企業のシステムエンジニア等

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～

令和４年４月20日　第１刷発行

編集代表　倉持俊宏

著者　吉田正宏
宮友一
河原塚泰
原島一郎
冨士﨑真治

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

（印刷）倉敷印刷　（製本）牧製本印刷
乱丁・落丁の際は本社でお取り替えいたします。