部内用

暗号資産分析ハンドブック

Chainalysis Japan株式会社
Principal Solutions Architect

愛知県警察サイバー事案対策アドバイザー

重川 隼飛 著

2025年3月

※この書籍は部内用です。
お取扱いには御注意ください。

立花書房

本書は、時々・情勢の必要に応じ、内容を変更・追加する場合があります。

推薦のことば

2008年に発明されたビットコインを始めとする暗号資産は、今や全世界で広範に活用され、決済手段のみならず投資の対象としても注目されている。一方で暗号資産は高い匿名性、容易に国境を越えて決済できる越境性といった特徴から、多くの犯罪に用いられている現状がある。この状況は今後ますます加速すると考えられる。

暗号資産が関わる犯罪を捜査するには、暗号資産への深い知識は言うに及ばず、司法当局に対してそれらを平易簡潔に説明する能力も求められる。しかし学習しようにも暗号資産の基礎をなす分散台帳、電子署名といった技術はその概念自体が難解である上、匿名性が一段高いモバイルウォレットの仕組みや、新たに出現した分散型取引所の提供するサービスなど得るべき知識は広範にわたる。また、インターネット上に決済利用目的、投資目的の解説はあるが、捜査に必要な知識をまとめたものはなく、捜査員の苦労は並々ならぬものがあった。

こうした現状を憂慮したChainalysis社の重川隼飛氏の御厚意により、この度、犯罪捜査のための暗号資産の解説書を上梓する運びとなった。氏は暗号資産追跡の第一人者であり、その高い分析力により数々のマネー・ローンダリングの摘発に寄与されてきた。氏の解説は微に入り細に入り、およそ犯罪捜査上要求される知見は網羅されている。また、付録として愛知県警察における検挙事例の解説を付加したことで、検挙の流れをより仔細にイメージいただけるものと考えている。

本書を座右に置くことで全国の捜査員が知見を深め、暗号資産を用いた犯罪を多数検挙し、同種犯罪を撲滅することを願ってやまない。

令和７年４月

愛知県警察本部生活安全部
サイバー局サイバー犯罪対策課長
松本　淳平

はじめに

私は、Chainalysis（チェイナリシス）という暗号資産の捜査上の分析を専門とする会社に、2020年2月に入社しました。私の以前の職歴は、エンタープライズITやサイバーセキュリティに関するものであって、実はChainalysisに入るまでは、暗号資産には一切触れたこともなければ、特段の関心があったわけでもありませんでした。また、入社当時、日本を含むアジア地域のメンバーは私ともう一人の営業担当者の2名だけでしたし、直後にコロナウイルスのパンデミックが世界的に発生したこともあり、オフィスに行けば他の専門家が手取り足取り教えてくれるといった環境ではありませんでした。したがって、暗号資産の広範なトピックについては、根本的な仕組みを含め、大部分を一から独習する必要に迫られました。

暗号資産の仕組みを理解するに当たっては、まず手始めに複数の関連書籍を当たりました。ビットコインの技術書の代表格である「Mastering Bitcoin[1)]」や、暗号資産を論ずる諸々の書籍に一通り目を通しましたが、その過程で気づいたことは、一つの本や参考資料だけで、都合よく良いところ取りをしてくれるようなものはないということでした。つまり、技術書だと開発者向けの抽象度の低い詳細な説明が多くて全体像をつかむのが難しく、広い読者層に向けた本だと肝心な技術的要点が抽象化されていたり端折られていたりして、要領を得づらいということです。そのため、自身の総合的な理解度を高めるために、記述の詳細度や切り口が異なる書籍やオンライン上の参考資料等を行ったり来たりして、内容を咀嚼（そしゃく）するというプロセスが必要でした。

さらに、暗号資産の業界や分野の発展のスピードは、一般的なITやサイバーセキュリティの分野と比べても、圧倒的に速いです。そのため、2〜3年前の情報がことごとく時代遅れになってしまったり、先進的なトピックはそもそも書籍のようなまとまった形にならなかったりすることがあります。最新の情報を得るには、（特に英語圏の）様々なWebページやオンライン上のリソースを拾い上げていかなければなりません。

幸いにして、私は暗号資産分析を専門とする会社にいますし、特に入社当初は基礎学習に充てる時間的猶予もあったため、ある意味で有利な状況にいます。しかしながら、多くの方々は暗号資産分析に限らない様々な業務を抱えており、専門的な事柄の学習に充てられる時間は一層限られているはずです。暗号資産事案捜査のニーズとともに徐々に理解者も増えているとはいえ、まだまだ暗号資産分析は歴史が浅い分野です。それを必ずしも専業としない組織における全体的な知識・スキルの向上、ノウハウの蓄積は非常に大きな課題であるとみています。

1）日本語訳版も含め書籍が出版されているが、Githubでも内容が無償公開されている。
https://github.com/bitcoinbook/bitcoinbook

特にここ数年で、暗号資産が関係する事案の認知は全国的に急増しています。なお、暗号資産は資金洗浄の手段として用いられることから、必ずしもサイバー事案の範疇（はんちゅう）にとどまらず、むしろ金融犯罪や組織犯罪の中で多く扱われるようになってきています。それを踏まえると、今日では暗号資産は、サイバー犯罪対策課など技術に特化した部署のみが知っておくべき、ニッチなトピックではもはやなく、より広範な捜査員が理解するべきものといえます。

このような情勢にもかかわらず、未だに暗号資産分析について実践的に深く解説したような資料は極めて少なく、ましてや日本語で書かれたものは事実上ほぼ皆無と思われます。この空白状態に手を打つことが、まさに本書の目的です。本書が現場における捜査活動の一助になれば幸いです。

ただし、本書は私個人が企画・執筆したものであり、Chainalysis社としての公式な出版物ではないことをあらかじめお断りいたします。

なお、本書の想定読者である全国の警察や検察の関係職員等に、円滑に周知・配布できるよう、この度は、私をサイバー事案対策アドバイザーとして2024年から選任いただいている愛知県警に御協力をお願いし、出版の手配や、実際の検挙事例の解説を追記いただけることとなりました。この場を借りて改めて感謝申し上げます。

令和７年３月

Chainalysis Japan株式会社　Principal Solutions Architect
愛知県警察サイバー事案対策アドバイザー
重川　隼飛

本書の使い方

本書は、付録を除けば、「暗号資産の基本」、「暗号資産の追跡の要点」、「暗号資産の分析手法」の3つの章で構成されています。

「暗号資産の基本」や「暗号資産の追跡の要点」の章では、暗号資産の仕組みやそのエコシステムの基本や、暗号資産追跡の概要を扱います。これらの章の大部分は、分析を専門としない方、必ずしも暗号資産について詳しくない方も含めて幅広い読者層にも読んでいただけるものと思います。

特に分析を専門としない初心者が本書のどの部分を読んだら良いのかを示すために、重要なセクションの見出しには「(★)」をつけています。暗号資産についてある程度知りたいものの、技術的に深追いしなくて良いという立場の方は、まずは目次のうち「(★)」がついている箇所を優先して目を通していただくのが良いでしょう。

「暗号資産の分析手法」の章では、暗号資産追跡を行うための実務的な手法や知識についてまとめています。この内容は、暗号資産の分析で必要となるであろう具体的な技術的知識やノウハウについてのものなので、特に暗号資産の分析業務を技術的に行う担当者が参照することを想定しています。

まだ暗号資産や分析の知識がない方であれば、目次通り、順番に読んでいただくのが良いですが、ある程度知識のある方であれば、辞書のような形で、自身が知りたい事柄のセクションを適宜拾い読みしていただくことでも結構です。

なお、暗号資産の分析に当たっては、現実的にはChainalysis Reactorなどの分析専門ツールを使うことがほとんどと思われますが、本書ではあえて操作方法や機能に触れるなど、特定のツールに特化したような説明はほとんどしていません。

多くは無償公開されている各種ツールやエクスプローラを参照しながら、説明を極力一般化していますが、場合によっては、Reactorなどの分析ツールで行えば、幾分効率的にできる作業や分析もあろうかと思います。

【目次】

＜暗号資産分析ハンドブック　目次＞

第１章　暗号資産の基本

第２章　暗号資産の追跡の要点

【目次】

第３章　暗号資産の分析手法

【目次】

付録　愛知県警察による事例集

#1. 暗号資産41BTC不正送信事件

#2. 暗号資産交換業者における口座の不正開設事件

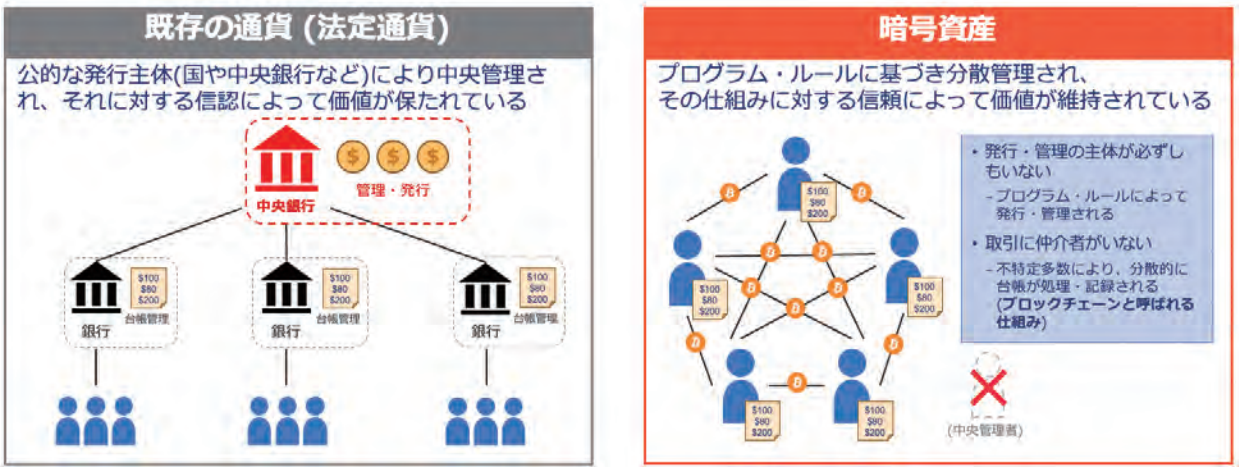
第1章 暗号資産の基本

この章では、暗号資産の技術的な性質や関連する法令の概要をまとめます。

1　暗号資産とは（★）

暗号資産とは、国や銀行などといった中央管理体制をとらずして、インターネット上で不特定の者に対してやりとりできる財産的価値（電子的な「お金」のようなもの）です。

既存の法定通貨は、国や中央銀行などの公的な発行主体によって中央管理され、それに対する信認によってその価値は保たれています。また、資金の流通には銀行などの金融機関が介在し、それらが厳格な取引や台帳の管理を行っています。あるいは、キャッシュレス決済を実現している電子マネーといった支払手段についても、法定通貨建てであり、取引には必ず決済業者を介することから、根本的な運営モデルに差はありません。一方で、暗号資産は、裏付け資産を必ずしも持たず、銀行などの第三者を介することなく、インターネット上で任意の取引相手に対して送金ができるという点で、既存の通貨や電子マネーとは一線を画します。



＜既存の通貨と暗号資産の比較イメージ＞

暗号資産の元祖であるビットコインは、「サトシ・ナカモト」と名乗る人物[2]によって、2008年

2）　2025年3月現在、未だに正体が知られていない。

第2章 暗号資産の追跡の要点

この章では、暗号資産を追跡する上で前提としておさえるべき事項と、全体的なワークフローの概要を説明します。

1　暗号資産の特性（★）

暗号資産がなぜ違法な活動に使われるのかといえば、主に以下３つの特性が好都合であるからと言えます。

①　利便性

決済業者や銀行などの仲介者を介さず、インターネット上で容易かつ安価に送金ができる上、物理的な貨幣などと違い可搬性の問題が生じないこと

②　高価値 / 流動性

それ自体に金銭的な価値がつけられており、取引を行う市場が出来上がっていること

③　匿名性

取引記録を一見するだけでは、誰が取引に介在したのか必ずしも分からないこと

暗号資産を追跡する上で特に問題となるのは、匿名性です。顧客情報に紐づく口座を介して行われる従来の銀行送金とは異なり、暗号資産では当事者自身のノンカストディアルウォレットのみを使えば、誰にも身元を明かすことなく誰からの関与も受けることなく、送金が可能です。

第3章

暗号資産の分析手法

この章では、主要なブロックチェーンの大分類ごとに、暗号資産追跡を行うための技術的な手法や関連する事項について説明します。またそれらに加え、複数の異なるブロックチェーンをまたぐクロスチェーンブリッジを介する暗号資産追跡の分析手法についても解説します。

1　ブロックチェーンの分類

暗号資産のブロックチェーンはビットコインから始まり、その後スマートコントラクトという仕組みを導入したEthereumが作られ、以降も様々な種類のブロックチェーンが作られています。そこで、ブロックチェーン分析を行う者としては、一体どれだけのブロックチェーンについて学べばいいのかという疑問が湧くかもしれません。確かにブロックチェーンには様々な種類があり、それら全ての仕様を覚えるのは非常に難しいですが、ブロックチェーンや暗号資産の普及度合いは一様ではなく、「パレートの法則（2：8の法則）」のように少数に偏っているため、捜査事案でよく目にするブロックチェーンの種類はある程度絞られるでしょう。また、後発のブロックチェーンには、他のブロックチェーンの派生系であるものも多く、同系統のブロックチェーンでは概ね同じ分析手法や観点が適用できます。よって、主要な系統のブロックチェーンの類型を押さえておけば、大部分の捜査に通用するはずです。それを踏まえ、本書では、UTXO系ブロックチェーンとEVM互換ブロックチェーンの2大類型ごとに分析の観点をまとめます。

2　UTXO系ブロックチェーンの分析

ビットコイン（BTC）、その派生系であるビットコインキャッシュ（BCH）、ライトコイン（LTC）は、UTXOと呼ばれる残高管理方式を採用しています。この方式は、現金の取り扱いに似ておつりが発生する仕組みとなっていて、そのおつりが出るたびに多くのウォレットでは新しいアドレスが払い出されます。そのため、同じウォレットのアドレスが増えたり、ばらけたりしやすいのが特徴であり、異なるアドレスのうちどれが同じ所有者に紐づくのか、どこから資金が他者の手に渡ったのかを評価することが重要です。

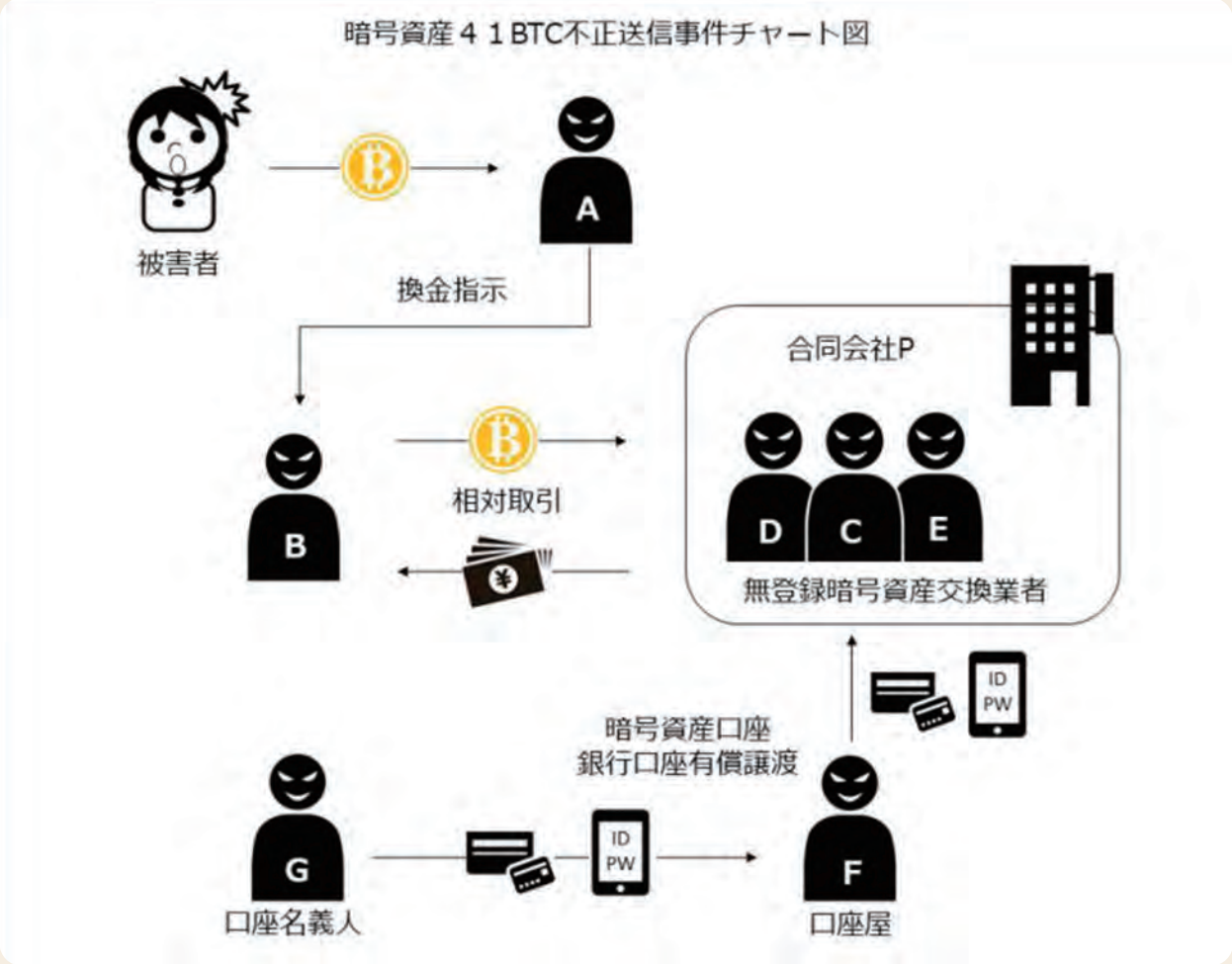
付録

愛知県警察による検挙事例

#1 暗号資産41BTC不正送信事件

(1) 事件概要

本件は、被疑者らが、知人の暗号資産（41BTC）を自己が管理するコインアドレスに不正送信した上、同暗号資産を無登録暗号資産交換業者に依頼して現金化した、電子計算機使用詐欺及び組織的犯罪処罰法違反等事件である。



部内用

暗号資産分析ハンドブック

令和７年５月30日　第１刷発行

著　者　重　川　隼　飛
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・製本　星野精版印刷