金 融 研 究

2025 年 1 月 / 第 44 巻 第 1 号

第 24 回情報セキュリティ・シンポジウム
「データ活用とプライバシー保護の両立」の模様

オープンAPI のセキュリティ：
認可処理における脆弱性と対策の高度化 …… 宇根正志

電子決済手段の法形式とその移転 …… 神作裕之

前払式支払手段をクレジットカードにより購入（チャージ）した場合の法律関係の整理 …… 内山理映子 石岡佑太

日本銀行金融研究所

金 融 研 究

2025 年 1 月 / 第 44 巻 第 1 号

目　次

1	第 24 回情報セキュリティ・シンポジウム 「データ活用とプライバシー保護の両立」の模様	
19	オープン API のセキュリティ： 認可処理における脆弱性と対策の高度化	宇根正志
49	電子決済手段の法形式とその移転	神作裕之
89	前払式支払手段をクレジットカードにより購入（チャージ） した場合の法律関係の整理	内山理映子 石岡佑太
115	金融研究所の概要等	

日本銀行金融研究所

第 24 回
情報セキュリティ・シンポジウム「データ活用とプライバシー保護の両立」の模様

1. はじめに

日本銀行金融研究所・情報技術研究センター（Center for Information Technology Studies: CITECS）は、2024 年 2 月 15 日、「データ活用とプライバシー保護の両立～プライバシー保護技術を正しく理解する～」をテーマとして、第 24 回情報セキュリティ・シンポジウムを開催した。

近年、多くの組織が、戦略的にデータ活用を推進しながら、デジタル・トランスフォーメーション（DX）や新たな価値創造に向けた取組みを強化している。また、複数の組織がデータを持ち寄ることによって、高度な統合分析を目指す動きへの関心も高まっている。このように各組織においてデータを取り扱う際、そうしたデータに「個人に関する情報」が含まれている場合には、プライバシーへの配慮が必要となる。

こうした観点から、本シンポジウムでは、専門家の方々から、さまざまなプライバシー保護技術の特徴や技術を組み合わせた場合の効果について、技術と法制度の両面から解説いただくとともに、プライバシー保護技術の利用に当たっての留意点などについてパネル・ディスカッションを行った。当日は、金融機関やフィンテック企業などの実務家、システム開発・運用に携わる技術者、研究者など約 200 名がオンラインで参加した。本稿では、以下に示したプログラムに沿って、3 つの講演とパネル・ディスカッションにおける議論の概要を紹介する（以下、敬称略、文責：日本銀行金融研究所）[1]。

1 文中の講演者やパネリストの所属および肩書きは、シンポジウム開催時点のものである。また、本稿において示された意見はすべて発言者個人に属し、その所属する組織の公式見解を示すものではない。また、本シンポジウムでの講演の資料等については、日本銀行金融研究所のサイト（https://www.imes.boj.or.jp/jp/conference/citecs/24sympo/24sec_sympo.html）を参照されたい。

【第 24 回情報セキュリティ・シンポジウムのプログラム】

- 講演 1「プライバシー保護技術の動向～主要技術の概要と組み合わせ事例の紹介～」
  LINE ヤフー株式会社 プライバシー&トラストチーム リーダー　竹之内隆夫
- 講演 2「プライバシー保護技術の国内法制度における位置づけ」
  ひかり総合法律事務所 パートナー弁護士　板倉陽一郎
- 講演 3「業界横断の安全なデータ活用に基づく社会課題解決の試み」
  株式会社 NTTドコモ クロステック開発部 担当部長 セキュリティプリンシパル
  寺田雅之
- パネル・ディスカッション
  パネリスト：竹之内隆夫、板倉陽一郎、寺田雅之、
  日本銀行金融研究所 企画役　菅　和聖
  モデレータ：日本銀行金融研究所 企画役　田村裕子

2. 講演 1「プライバシー保護技術の動向～主要技術の概要と組み合わせ事例の紹介～」

竹之内は、企業におけるプライバシー保護への取組状況、および、主要なプライバシー保護技術の概要と最近の活用トレンドについて、次のとおり講演した。

(1) プライバシー保護は経営戦略の一部に

プライバシー保護においては技術面の対応を要するが、それだけですべて対応できるものでもなく、技術者と非技術者の連携が極めて重要となる。こうした連携に当たっては、相手方の専門分野に関する知識がある程度必要になり、例えば非技術者においても、プライバシー保護技術について一定の知識を備えておくことが望ましい。

海外では、ユーザのプライバシーに対する意識の高まりを受けて、プライバシー保護を経営戦略として位置づけるとともに、プライバシーへ配慮する姿勢をブランド化する動きが増えてきている。こうしたブランド化によって、ユーザから個人データ[2]を収集しやすくなる効果も見込めるようである。個人データはデジタル化

2 本講演では、「個人データ」を、個人に関するデータという意味で用いる。法令上の用語・定義ではない点には注意されたい。

社会において重要であり、企業活動において個人データの安全な収集・活用は不可欠となっている。国内企業がこうしたグローバル企業と伍していくうえでは、企業間でのデータ連携もありうべき戦略の 1 つであろう。そのためにも、プライバシー保護技術は今後より一層重要になっていくと考えられる。

(2) プライバシー保護技術とその組み合わせ

プライバシー保護技術にはさまざまな種類がある。近年の主流は、①差分プライバシーを満たす手法、②連合学習、③秘密計算[3] の 3 つであり、これらは概念の異なるプライバシー保護技術である。やや抽象的に表現すると、①差分プライバシーを満たす手法はデータを「ぼかす」、②連合学習はデータを「減らす」、③秘密計算はデータを「隔離する」ことを通じて、それぞれユーザのプライバシーを保護する。

より具体的に表現するために、ユーザのデバイスからサーバに個人データを送信して個人データベースに蓄積し、当該サーバで個人データを集計・加工したのち、分析結果を分析者に送信する、という典型的なデータ処理のフローを想定してみる。このとき、①差分プライバシーを満たす手法は、ユーザのデバイスからサーバに送信される個人データ、または、サーバから分析者に送信される集計結果のデータに確率的なノイズを付与するなどしてデータを「ぼかす」ものである[4]。②連合学習は、ユーザのデバイス内で個人データを用いた機械学習モデルの更新を行い、更新情報だけをサーバに送信することで、共有される個人データの範囲を「減らす」ものである。③秘密計算（TEE〈Trusted Execution Environment〉を用いる場合）は、個人データをサーバの安全な領域に「隔離」してから処理するものであり、処理中のデータも保護できる。このように、これらのプライバシー保護技術は、データ保護の様態や安全性の性質が異なるため、それぞれ単体で用いられる場合もあるが、近年では、複数の技術を組み合わせることでプライバシー保護を強化する事例が増えてきている。

イ. 差分プライバシー

差分プライバシーとは、個人データまたは個人データベースの集計結果にノイズを加えるなどしてデータを確率変数化する手法について、その安全性を統計的に評価する尺度である。例えば、あるユーザ A の個人データを含まない個人データ

3 本講演では、秘密計算を、データを暗号化したまま計算する技術の総称として用いている。

4 差分プライバシーには、セントラル差分プライバシーとローカル差分プライバシーの 2 種類がある。前者は、個人データベースを集計加工した結果を分析者などに提供する際に、サーバ側で集計加工結果にノイズを付加するものである。後者は、ユーザのデバイスから個人データをサーバに提供する際に、デバイス側で個人データにノイズを付加するものである。

ベースと、これを含む個人データベースを用意し、それぞれのデータベースから得られる集計結果にノイズを加えることを考える。このとき、両者の集計結果を区別できる確率が無視できるほど小さければ、集計結果からユーザ A に関する情報が漏れていないとみなすことができる。こうした性質がユーザ A だけでなくすべてのユーザに対して成り立つのであれば、当該手法は差分プライバシーを満たすといえる。差分プライバシーの特長は、個人データベースの情報を除くいかなる知識（背景知識）を持つ攻撃者に対しても安全性を保証できる点にある。

ロ．連合学習

一般的な機械学習では、各ユーザのデバイスから個人データを集め、それらを訓練データとして集約したものを機械学習モデルの訓練に用いる。この場合、各ユーザの個人データは、機械学習モデルの訓練を実施する主体に送信・開示されることとなる。これに対し、連合学習では、個人データをユーザのデバイスから外部に送信することなく、機械学習モデルの訓練が行われる。具体的には、ユーザのデバイス内で機械学習モデルが更新され、その更新情報を受け取ったサーバが機械学習モデルを生成する。ただし、近年の研究において、機械学習モデルの更新情報から個人データを復元できる可能性が指摘されていることを受けて、更新情報に差分プライバシーを満たす手法を適用するケースが増えてきている。

ハ．秘密計算

秘密計算とは、処理中のデータに機密性を持たせることを目的とする暗号技術の一種である。秘密計算を実現する方法には、暗号アルゴリズムの安全性に依拠する MPC（Multi-Party Computation）と、ハードウェアの安全性に依拠する TEE がある。TEE では、処理するプログラムが不正に改竄されていないことを確認する機能もあわせて提供する。なお、ユーザのデバイスから個人データをサーバに送信して集計するタスクに秘密計算を適用すれば、ローカル差分プライバシー[5] を適用する際に個人データに付加するノイズを小さくできるとの研究結果が報告されており、こうした組み合わせは、個人データの有用性とプライバシー保護のトレードオフの改善に有効であることがわかっている。

5 脚注 4 参照。

(3) プライバシー保護技術の組み合わせ事例

イ. LINE ヤフー社によるスタンプの自動推薦

モバイル・メッセージ・アプリ「LINE」[6] で提供するスタンプ[7] には、ダウンロードして使用するタイプ以外に、「LINE スタンププレミアム」[8] というダウンロードしなくても使用できるサービスもある。このサービスでは 1,200 万以上のスタンプを利用可能であるため、ユーザへの推薦機能が重要となる。推薦に当たっては、まず、スタンプの入手履歴データを訓練データとした機械学習の手法により、推薦するスタンプの候補を絞りこむ。次に、各ユーザのスタンプの閲覧・送信履歴データをもとに機械学習を行い、推薦候補を並び替える。これら 2 つのタスクのうち推薦候補を並び替える処理において、サーバ（LINE ヤフー社）に送信するプライバシーに関する情報を「減らす」観点から連合学習を採用したうえで、さらに機械学習モデルの更新情報を差分プライバシーにより保護している[9]。

スタンプ推薦機能におけるプライバシー保護については、エンジニアや開発者向けに詳細な技術仕様を記載したホワイトペーパーを公表している[10]。これは、プライバシー保護に関する取組みは外部からみえにくいため、積極的な情報発信が必要との考えからである。また、公表に際しては、技術者と非技術者に対して、それぞれの立場の違いを意識して理解しやすい情報発信を心がけている。

ロ. 他社の事例

Google 社では、多言語キーボード・アプリにおいて、連合学習と差分プライバシー、および秘密計算を組み合わせて適用することで、ユーザのキーボード利用に関するプライバシー保護を図っている[11]。具体的には、連合学習においてユーザ端末がサーバに送信するモデル更新情報は差分プライバシーで保護されるほか、サーバにおけるデータ処理には秘密計算が適用されている。

また、Apple 社と Google 社による企業間連携の事例として、新型コロナウイルス

6 LINE は LINE ヤフー株式会社の登録商標である。

7 スタンプとは、テキスト・メッセージに挿入できるイラストをいう。通常は、アプリにダウンロードしたスタンプ一覧から、ユーザが送信したいスタンプを選択する。推薦機能を利用する場合には、ユーザがテキストで「ありがとう」と入力すると、「ありがとう」とタグづけされたスタンプが候補として表示される。

8 https://store.line.me/stickers-premium/landing/ja。LINE スタンプは LINE ヤフー株式会社の登録商標である。

9 https://privacy.lycorp.co.jp/ja/acquisition/privacy_techs.html

10 https://s.yimg.jp/images/cdo/privacycenter/2023renewal/pdf/ja/line-differential-privacy-whitepaper-ver1.0.pdf

11 https://research.google/blog/federated-learning-collaborative-machine-learning-without-centralized-training-data/

感染症に関するデータ集計において、秘密計算と差分プライバシーの組み合わせが使用された[12]。具体的には、ユーザのデバイスからサーバに送信される個人データは差分プライバシーで保護されるほか、iPhone[13] ユーザと Android[14] ユーザの個人データを集計する際には、秘密計算が応用される。これにより、Apple 社と Google 社は、互いにユーザ端末の特定や位置情報の取得などができない仕組みとなっている。

国内では、複数の金融機関が取引データを持ち寄り、連合学習と秘密計算を応用して、顧客のプライバシーに配慮しながら不正送金検知の精度を向上させる実証実験の事例がある[15]。

3. 講演２「プライバシー保護技術の国内法制度における位置づけ」

板倉は、プライバシー保護技術の 1 つである秘密計算のうち暗号処理を伴う方式に関し、個人情報保護法における取扱いの現状について、次のとおり講演した。

(1) プライバシー・バイ・デザイン

1990 年代に提唱された「プライバシー・バイ・デザイン」は、システムの企画・設計の段階からプライバシーを保護する施策を組み込む考え方である。この考え方は、プライバシー保護技術を事後的に適用するアプローチのみではプライバシー保護を達成できないのではないか、との問題意識から生まれた。近年、プライバシー保護技術の利用事例が増えてきたことから、技術で解決できる課題とそうでない課題が明確になりつつある。本講演では、プライバシー保護技術のうち近年注目を集めている秘密計算について、日本の個人情報保護法上の位置づけを整理したい。

12 https://www.google.com/covid19/exposurenotifications/
13 iPhone は Apple inc. の登録商標である。iPhone 商標はアイホン株式会社のライセンスに基づき使用されている。
14 Android は Google LLC の登録商標である。
15 https://www2.nict.go.jp/oihq/seeds/detail/0024.html

(2) 個人情報該当性

個人情報保護法が対象としているのは、「個人に関する情報」であることが前提となっている「個人情報」である。そのため、個人に関する情報に該当しなければ、個人情報保護法の規制下にはおかれない。秘密計算とは、データを秘匿したまま演算処理する技術のことであり、直感的には、秘密計算において処理中のデータは、個人に関する情報ではないようにも思われる。しかしながら、個人情報保護委員会において、個人に関する情報に該当するかは、暗号化等によって内容が秘匿されているか否かを問わない、という見解が示されていることを踏まえると、秘密計算における処理中のデータであっても、個人情報該当性は失われないという前提で議論せざるをえない。

(3) 安全管理措置

個人情報保護法第 23 条では、個人情報取扱業者に対して、個人情報を含むデータ（個人データ）に、適切に安全管理措置を施す義務を課している。この安全管理措置の一環として、情報の漏えい等を防止する手法がガイドラインで例示されているが、秘密計算は例示された手法には含まれていない。もっとも、秘密計算が、情報の漏えい等を防止し、または、情報が漏えいした場合の影響を最小限に抑制する技術であることに疑いの余地はない。実際、政府が公表する資料などからは、安全管理措置として秘密計算を推奨する姿勢を読み取ることができる。このため、適切に実装されていることを前提とすれば、秘密計算は技術的安全管理措置の一部を構成すると考えてよい。

(4) 監督官庁への通知義務の免除

個人情報保護法第 26 条（民間事業者の義務）および同 68 条（行政機関等の義務）では、個人情報取扱事業者に対して、取り扱う個人データが漏えいなどした場合に、個人情報保護委員会に報告し、本人に通知する義務が規定されている。ただし、同法の施行規則第 8 条では、情報の漏えい等が発生した場合であっても、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている個人データの場合については報告を要しない、とされている。秘密計算がこうした措置に該当するか否かについて、ガイドライン等に特段の記述は見当たらない。また、秘密計算は電子政府推奨暗号ではない。しかし、秘密計算は、CRYPTREC

暗号技術ガイドライン（高機能暗号）において取り上げられていることから、暗号化等の技術的措置に該当する場面があると整理する方向で検討が進んでいるともいえる。

(5) 利用目的規制・第三者提供規制との関係

個人情報保護法上、個人情報取扱事業者には、個人情報の利用目的をできる限り特定する義務が定められているほか（第 17 条 1 項）、利用目的を公表していない場合には、速やかに利用目的を本人に通知する義務が定められている（第 21 条 1 項）。データを開示せずに計算結果だけが導き出されるという秘密計算の性質に着目すれば、秘密計算による計算結果の導出が利用目的規制の対象となるか否かについては、一考の余地があると考えられる。個人情報保護委員会が公表している Q&A では、個人情報に該当しない統計データは利用目的規制の対象とはならないほか、統計データの加工自体を利用目的とする必要はないとされている。そのため、単独の事業者によって行われる、秘密計算による計算結果の導出に当たっては、利用目的の特定は不要と理解することができる。

次に、個人データの第三者提供について考察する。個人情報保護法上、個人データの第三者提供には、あらかじめ本人の同意が必要とされている。秘密計算により秘匿化されたデータが組織の垣根を越えて交換されるケースでは、こうしたデータ交換が個人データの第三者提供に当たるか、という論点がある。この点、個人情報保護委員会は、準同型暗号を用いた秘密計算について、暗号化は安全管理措置の 1 つとして考慮されるべき要素ではあるが、個人情報該当性に影響するものではないとの見解を示している。当該見解は、秘密計算の過程で暗号化された個人データの個人情報該当性を示すものではあるが、秘密計算の過程における個人データの交換が第三者提供に該当するか否かについて正面から回答していない。このように、現時点では、秘密計算において行われる、暗号化された個人データの組織を越えた交換については、第三者提供に該当しないとはいいきれないことには留意が必要である。

対照的に、仮名加工情報については、利用目的の柔軟な変更が許容されている。例えば、仮名加工情報については、共同利用が認められているほか、名寄せを伴う共同利用も排除されていない。もっとも、仮名加工情報を作成する前に仮 ID の作成方法に関する情報を他の事業者と共有する場合には、作成後、直ちに削除しなければならないとされている。いずれにせよ、秘密計算を利用する際には、仮名加工情報を対象とすることも一案であろう。

(6) 海外の事例

2014 年、エストニアにおいて、政府機関等が保有する税情報と教育情報を結合し、大学生の留年と仕事量（アルバイト等）の相関関係を導出するのに秘密計算が用いられた事例がある。一般データ保護規則（GDPR: General Data Protection Regulation）施行前のエストニアの法律では、個人データの処理にはデータ保護機関による事前の許諾が必要であったが、秘密計算を用いた処理は個人データの「処理」に該当しないとして事前許諾は不要と判断された。

米国には連邦レベルでの包括的なデータ保護法は存在しないが、欧米間のデータ移動については、欧米間で合意されたデータ保護の枠組みである欧米プライバシー・シールドが適用されてきた。その後、米国に移転された個人データの米国国内法による保護が不十分であるとして、欧州司法裁判所は、欧米プライバシー・シールドについての十分性決定を無効とする決定を下したが、追加的措置が必要な場合があることを前提に、データ移転をすべて無効とはしなかった。この追加的措置の有効な手法の 1 つとして秘密計算が挙げられており、秘密計算が個人データの保護に資する技術として認められている。

日本と欧州は相互にデータ保護制度を認証している（欧州からの十分性認定、日本からの同等性の決定）ことから、海外の事例における GDPR の解釈は、日本法の解釈に当たっても参考になると思われる。

4. 講演 3「業界横断の安全なデータ活用に基づく社会課題解決の試み」

寺田は、複数の企業が持つデータの秘匿性を維持し、プライバシーが保護された安全な統計情報の作成に関する実証実験の内容について、次のとおり講演した。

(1) 統計データを「つくる」技術と「つかう」技術

NTT ドコモ社では、携帯電話ネットワークの運用データに基づき、日本全国を対象にエリアごとの人流を継続的に把握できる「モバイル空間統計」[16] と呼ばれる統計データを提供している。降雨の状況から、川の水位上昇や堤防の越水可能性を予

16 モバイル空間統計は株式会社 NTT ドコモの登録商標である。

測できるように、モバイル空間統計を使えば、交通渋滞の発生や店舗売上の変動、感染症の拡大など、数時間先の社会の未来を予測できる可能性がある。

その一例に「AI 渋滞予知」[17] がある。モバイル空間統計と AI 技術を組み合わせて数時間先の渋滞予測データを提供することにより、人々は渋滞を回避しやすくなる。その結果、渋滞そのものの消失または緩和が期待される。

(2) 統計データを「まもる」技術

健全なデータ活用には適切なプライバシー保護が必須であり、統計データを「まもる」技術は、データを「つくる」・「つかう」ための基盤となる。モバイル空間統計は、プライバシーが保護された安全な統計データに変換されていればこそ、多くの企業に提供して広く利用してもらうことができる。また、異なる組織がそれぞれ保有するデータを、プライバシーを保護したまま掛け合わせて安全な統計データに変換する技術が確立できれば、さらに有益な応用事例へと発展していくことも展望できる。そうした観点から開発した技術が「秘匿クロス統計技術」[18] である。

(3) 秘匿クロス統計技術

NTT ドコモ社では、2022 年 10 月、他社と共同で、差分プライバシーと秘密計算を組み合わせた「秘匿クロス統計技術」による企業横断データ活用の実証実験を開始した。秘匿クロス統計技術とは、複数の企業が、それぞれのデータの秘匿性を保ったまま、プライバシーが保護された安全な統計情報（クロス集計表）を出力する技術である。秘匿クロス統計の安全性要件は、(1) 出力されるデータが、適切にプライバシーが保護された統計情報であること、および、(2) それぞれの組織にとって、自らの不正がない限り、出力される統計情報以外に、自らのデータに関する情報が漏えいしないことである。

秘匿クロス統計技術は、①入力データの個人識別性を除去する「非識別化処理」、②秘匿共通集合濃度計算を用いて（暗号化された）クロス集計表を作成する「集計処理」、③暗号化された集計表に差分プライバシーを適用したうえで復号する「秘匿処理」の 3 つの処理で構成される。

複数企業が互いの情報を持ち寄ってクロス集計表を作る場合、共有 ID（仮名）を

17 東京湾アクアライン上り線と、関越自動車道上り線（練馬～沼田間）の渋滞予測情報が、NEXCO 東日本の道路情報サイト「ドラぷら」から配信されている。ドラぷらは東日本高速道路株式会社の登録商標である。

18 秘匿クロス統計技術は株式会社 NTT ドコモの登録商標である。

持たせたデータを平文のまま他社に渡してしまうと、特定の個人が識別されたり、プライバシーが暴露されたりする可能性が生じる。そこで、秘匿共通集合濃度計算を使用することによって、互いのデータを知られることなく計算の結果だけを得られるようにする。ここで、秘匿共通集合濃度計算は、集合 A と集合 B がそれぞれ異なる組織により保持されているときに、互いに集合の内容を明かさずに、共通集合の要素数 |A∩B| のみを計算する技術である。これは、準同型暗号を利用した秘密計算の一種であり、安全性要件（2）を満たすうえで重要な役割を果たす[19]。

次の課題は、最終成果物であるクロス統計表そのものの安全性である。秘匿共通集合濃度計算は、クロス集計表を作成する過程の安全性を保証するが、作成されたクロス集計表そのものの安全性を保証するものではない。実際、公表された複数のクロス統計表を手掛かりに、データベース再構築攻撃と呼ばれる攻撃によってプライバシー情報が漏えいする可能性がある。これは、あるデータベースから作成された複数の集計表を組み合わせることによって、元のデータベースの一部または全部を復元し、個人のプライバシーを暴露する攻撃である[20]。データベース再構築攻撃への対策には、差分プライバシーの枠組みが有効である。

秘匿クロス統計技術では、暗号化された状態のクロス集計表に対して差分プライバシーに基づくノイズ付与を行い、そのあと復号することとしている。これにより、安全なクロス集計表のみが平文で出力される。

(4) データベース再構築攻撃への対応

米国では、従前より、国勢調査における国民のプライバシー保護のあり方について議論が行われていた。そうしたなか、2010 年の国勢調査結果に対してデータベース再構築攻撃を適用したところ、46％の国民について、移住ブロック、性別、年代、人種、民族が復元されてしまうことが判明した。また、1 歳の年齢誤差を許容した場合には、71％の国民についての情報が復元可能であったとの結果が報告された。復元されたデータは、個人を特定できるものではなかったが、その後、一般に入手可能な市販データと照合するによって、約 5,200 万人分（米国民の約 17％）の個人を特定できることが判明した。

米国センサス局では、データベース再構築攻撃のリスクは、理論上のリスクから

19 この方式以外にも、秘密分散に基づく方式がある。秘密分散とは、秘密情報を n 個のシェアと呼ばれるデータに分割し、そのうちの k 個以上を集めれば秘密情報を復元することができるというデータの分散保管技術である。秘密分散では、その性質上、自分以外の組織が結託した場合には秘密情報が復元されうる（$n > k$ の場合）。秘密分散に基づく方式は安全性要件（2）を満たさないため、実証実験での利用は見送られた。

20 直感的には、複数の統計表を組み合わせて、虫食い算のような制約充足問題を作り、これを解くことで元データを復元する攻撃が挙げられる。

対策が求められる課題へと変質したとして、2020年の国勢調査から差分プライバシーの導入を決定した。差分プライバシーは、さまざまなプライバシー保護技術に対する統一的な安全性の尺度である。この尺度は、データベースから出力される情報から、データベースに含まれる特定個人に関するプライバシー情報の流出量の最大値を測るものである。

(5) まとめ

秘匿クロス統計を用いて2022年から2023年にかけて実施した実証実験では、異業種間でのデータ連携において、プライバシーを技術的に安全に保護しながら有益な社会価値を創出できることを確認できた。今後、さらに実績を重ねることにより、新たなデータ分析の方法論を確立し、得られた知見を広く社会に還元していきたい。安全な統計データの作成方法を確立することは容易ではないが、これを実現することで、有益な社会価値の創出が進んでいくと期待している。

5. パネル・ディスカッション

(1) 関係者間におけるコミュニケーションの重要性

プライバシー保護技術は、安全性の基準やデータ処理プロセスの異なるフェーズで適用されるものが混在しているため、ユースケースに照らした技術の選択やそれらの組み合わせが難しい。こうした観点から、田村（モデレータ）は、各組織が顧客のプライバシー保護の取組みを行う際の留意点について、パネリストに意見を求めた。

竹之内は、関係者間のコミュニケーションの重要性を指摘した。具体的には、顧客のプライバシー保護に当たっては、ビジネス側と技術者側のコミュニケーションが必須であるとしたうえで、顧客に価値を提供するためにはどのようなデータが必要かを明確にし、ユーザのプライバシーを保護する方法について話し合うことが重要である、との見解を示した。

寺田は、収集するデータの粒度に関する留意点について意見を述べた。そもそも細かすぎるデータを安全にすることは極めて難しいとしたうえで、ビジネス側には技術的な制約への理解が必要であるほか、ビジネス側から細かいデータの出力を求めた場合であっても、実際には、そこまでの細かいデータが不要であるケースや、

むしろ粗いデータの方がサンプル数を増やせることで品質のよい結果が得られるケースもあることを紹介した。また、プライバシー保護の観点からは、まずは粗いデータで分析を行い、徐々にブレークダウンしていくというアプローチが有用ではないか、との見方を示した。

板倉は、データの取扱いにおいては、個人情報保護法を遵守するための対応と、技術的なリスクを想定した対応の両方が必要であると指摘した。そのうえで、両者は観点が異なるため、両方に対応するためには、関係者に広く相談する必要があるとして、関係者間でのコミュニケーションの重要性を指摘した。

菅は、プライバシー保護技術にはさまざまな方式があり、安全性の概念と強度、保護の範囲がそれぞれ異なると指摘した。そのうえで、プライバシー保護に当たっては、データのライフサイクルでの安全性評価が必要であり、残余リスクを洗い出して関係者間で共有し、リスクを受容することも含めて対応方法を検討することが重要である、との見解を示した。

(2) プライバシー保護に関する取組みを公表することの重要性

田村は、国内においても、プライバシー保護技術の活用事例が増えてきていることについて、今後、同技術をより一層普及させていくには、どういったことに留意すべきか、各パネリストに問うた。

竹之内は、プライバシー保護技術の効果は社外からは見えにくいため、プライバシー保護技術を実際には適用していないのに、適用しているように偽装することができてしまうことの問題点を指摘した。そのうえで、今のところこうした偽装への有効な対策はなく、コミュニティー間での情報連携によって対応するほかないとの見解を示した。また、プライバシー保護に関する情報収集には、専門家が多く集まる学会の場を積極的に利用していくことも有用であり、そうなっていくことが望まれる、と述べた。

寺田は、竹之内と同様、プライバシー保護に関しては、実際には安全でなくても安全であると主張できてしまう点に留意が必要である、と述べた。実際、プライバシー保護のために相応のコストをかけて対応している企業と、単に偽装しているだけの企業の見分けがつきにくいことを指摘したうえで、第三者による検証制度の構築が課題であるとの見解を示した。この点、「IT セキュリティ評価及び認証制度」といった第三者による評価・認定制度を利用するといったアイデアもあるが、プライバシー保護分野についての活用事例はなく、コストの面でも課題があるだろうと述べた。

板倉は、情報開示の重要性について指摘した。すなわち、個人情報保護法では、

安全管理のために講じた措置の公表等が義務化されており、こうした公表物は、企業の安全管理措置に対する姿勢の評価にも活用されている実情を紹介した。そのうえで、プライバシー保護への対応についても同様であり、外から見えにくいからこそ、企業の取組み姿勢を積極的に公表していくことが重要である、との見解を示した。また、一般向けのプレスリリースでは、技術的な内容まで説明することは難しく、それにより誤解が生じるリスクがあるとしたうえで、技術的な内容については別途詳細版を公表することが望ましい、と述べた。

(3) セキュリティ・パラメータの設定

プライバシー保護技術には、それぞれにプライバシー保護の程度を評価するためのパラメータが存在する。田村は、こうしたパラメータについて、どの程度の数値であれば十分に安全であるといった何らかの目安はあるのか、と各パネリストに質問した。

竹之内は、プライバシー保護におけるデータの安全性は、有用性とのトレードオフの関係にあるため、どの程度の安全性を確保すれば十分といった数値基準を提示するのは難しい、との見解を示した。そのうえで、LINE スタンプのオンライン・サービスを例に挙げ、まだユーザ数が少なかった当初は、データの有用性確保の観点から、差分プライバシーのノイズを少なくせざるをえなかったと述べた。それと同時に、同取組みが「ただちにプライバシーの向上にはつながるものではありません」と公表したことを紹介した。そして、現在も、データの有用性とプライバシー保護の両立のあり方に向けて検討を進めている段階であり、望ましいセキュリティ・パラメータはどの程度かといった数字を提供できる段階にはない、と述べた。

寺田は、*k*-匿名化[21] を例に取り上げ、データベース再構築攻撃に対して安全な方式ではないため、十分な安全性を確保できる *k* は一般には存在しないとの見解を示した。また、差分プライバシーのセキュリティ・パラメータ ε[22] については、例えば ε が 1 より小さければ十分にプライバシーを保護できているだろうとの相場観はあるものの、社会的なコンセンサスが形成されているわけではないため、今後、関係者間での議論が深まることが期待される、と述べた。

菅は、研究分野では、差分プライバシーがプライバシー保護技術の安全性を示すスタンダードになりつつあることを紹介した。そのうえで、寺田と同様、*k*-匿名化といったプライバシー保護技術は、外部の情報と突合したときの安全性を十分に考

21 *k*-匿名化とは、同じ属性を持つ値が *k* 個以上になるようにデータを加工することで、*k* 人未満へのデータの絞込みを困難にする方法である。

22 ε は、2 つのデータベースから得られる集計結果にノイズを加えたとき、これらを区別することができる程度を表すパラメータであり、ε の値が小さいほど安全性が高いとされる。

慮したものではないことから、現実的な脅威への対策とはなりにくい点には留意が必要である、との見解を示した。

板倉は、匿名加工情報は第三者への提供が認められていることから、第三者に提供しても問題がないような加工処理が求められると指摘した。そのうえで、多くの企業は、個人情報委員会が提示している例を参考に対応しているが、事例集に掲載されている手法を単純に適用しただけでは、実際のリスクに照らして安全なデータになっているとはいい切れないことに留意が必要である、と述べた。

(4) 差分プライバシー

差分プライバシーについては、外部にある情報と突合した場合にもプライバシー保護が可能という点で相対的に安全性が高いことから、今後利用が増えていくことが想定されている。そうしたもとで、田村は、差分プライバシーを利用するうえでの留意点について、各パネリストに意見を求めた。

竹之内は、データにノイズを付加さえすれば、一定の差分プライバシーは確保されるが、データの有用性を維持しつつプライバシーを保護するには、高いスキルが必要であると指摘した。

菅は、感染症アプリの例に照らすと、高機能なプライバシー保護の実現には、差分プライバシーを他の技術と組み合わせて使用することが必要である、との見解を示した。また、金融機関における不正検知の例では、監査可能性とプライバシー保護という相反する性質の両立が求められるほか、医療分野の例では、データにノイズを加えてしまうとデータに価値がなくなることがあると指摘したうえで、ユースケースに応じたプライバシー保護技術が必要であり、差分プライバシーさえあれば十分ということではない、と述べた。

寺田は、差分プライバシー等のプライバシー保護技術は、データに含まれるプライバシー情報の秘匿性を保つ技術であることから、情報セキュリティ技術の一部と位置づけることもできる、と説明した。そのうえで、差分プライバシーの場合、プライバシー情報は秘匿するが、それ以外の情報は開示できるという性質を持つことが求められるため、既存の暗号技術とは安全性の定義が異なるものの、これまでセキュリティ分野で蓄積されてきた知見がプライバシー保護技術の分野でも活用されていくことが期待される、と述べた。

(5) 個人情報保護法とプライバシー保護技術

個人情報保護法では、特定の個人を識別することができないように個人情報を加

工したものであれば、本人の同意を得ずに第三者に提供することが可能とされている。また、個人との対応関係が排斥された統計データは個人情報でなくなることから、個人情報保護法の規制下にはおかれない。こうしたもとで、田村は、個人情報保護法を踏まえたデータの加工技術とプライバシー保護技術の関係について、各パネリストに見解を問うた。

菅は、差分プライバシーの発想は、個人に関する情報の流出量を制限することで確定的な暴露を回避するというものであり、個人情報保護法におけるプライバシー保護とはコンセプトが大きく異なるのではないか、と述べた。

板倉は、個人情報保護法では、k-匿名性（k は 2 以上）を満たすように加工された個人データは、匿名加工情報に該当する、と説明した。それは、個人情報保護法上、仮名加工情報や匿名加工情報については、元の個人データと照合してはいけないとの義務が課せられているうえに、k-匿名性を有するデータであれば、個人の特定が難しいと考えられるためである、と述べた。そのうえで、個人データを集計加工して得られる統計データは、個人に関する情報ではなく、匿名加工情報でもないとすると、もはや個人情報保護法の範囲外であって法的制約はないが、技術的には、他の個人データとの照合などによって個人が特定される可能性は排除できないことから、今後の法改正によって見直しが行われる可能性はある、との見解を示した。

寺田は、特定の個人との対応関係が排斥された統計データは「個人情報」ではなくなることに関連して、差分プライバシーは、統計データなどから個人に関する情報が確定的に暴露されるのを防止する枠組みであり、個人情報ではない形に加工する技術として有益である、と説明した。

さらに、板倉は、現在の個人情報保護法では、差分プライバシーが適用されていたとしても、個人データの一部が少しでも外部に出てしまえば、仮にそれが当たり障りのないものであっても個人情報の漏えいに該当するが、今後の検討次第で、規制を緩和することも考えられるのではないか、との見解を示した。

(6) 人材育成

シンポジウム参加者から、企業における人材育成のあり方について質問がよせられた。

寺田は、人材育成には教師となる専門家が必要であるが、国内においてプライバシー保護技術の専門家はまだ少ないこともあって、現時点において企業内での育成は難しいのではないか、との見解を示した。そのうえで、まずは大学等でプライバシー保護技術の基礎を学べるようになることが望ましいが、そうしたカリキュラム

を持つ大学は多くないことから、企業のニーズにあわせたカリキュラム構成を大学側に働きかけることは一案となりうる、と述べた。

これに対して、菅は、データ・アナリストやデータベースのスペシャリストらがプライバシー保護についても勉強していく、というのが人材育成の近道ではないか、との見解を示した。また、大学での座学と、実社会において実際にユーザのプライバシーを保護することとの間には大きなギャップがあると想像されるため、企業で実戦経験を積むことが重要である、と述べた。

オープン API のセキュリティ：認可処理における脆弱性と対策の高度化

宇根正志（うねまさし）

要　旨

オープン API は、API の提供者が外部の組織への使用に供するために公開した API を指す。金融分野では、金融機関が電子決済等代行業者などのフィンテック事業者に対して顧客の口座情報を提供するケースなどで活用されている。金融機関は、顧客がフィンテック事業者に対して口座情報の提供を認可したことを確認し、フィンテック事業者と連携して口座情報を安全に提供することが求められる。

こうした認可の処理に関するプロトコルの標準仕様として OAuth 2.0 が広く採用されている。もっとも、OAuth 2.0 の要求事項を十分に満たしていない実装例が少なからず存在していることが、学術研究の成果として最近発表されている。このようなサービスには脆弱性が存在し、それが悪用されると情報漏洩などのリスクにつながる可能性があるため、OAuth 2.0 を実装する際に脆弱性を極力排除する必要がある。

脆弱性を排除するうえで、OAuth 2.0 のセキュリティ・プロファイルである FAPI 2.0 を活用することが有効である。ただし、実装環境や想定される攻撃方法によっては、FAPI 2.0 の要求事項を満たすだけではリスクを十分に軽減できない場合がある。そのため、自社のサービスで想定される実装環境や攻撃方法を考慮したうえで、FAPI 2.0 の要求事項を適用しつつ、追加的な対応の必要性を検討することが重要である。

キーワード：　オープン API、脆弱性、セキュリティ、フィンテック、リスク、FAPI 2.0、OAuth 2.0

本稿は 2024 年 5 月 31 日時点の情報に基づいて作成した。本稿の作成に当たっては、小岩井航介氏（KDDI 株式会社）から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

宇根正志　日本銀行金融研究所参事役（E-mail: masashi.une@boj.or.jp）

1. はじめに

オープン API（application programming interface）は、API の提供者が外部の組織に使用させるために公開した API を指す。オープン API を活用した金融サービスの代表的な例としては、金融機関が電子決済等代行業者などのフィンテック事業者に対して顧客の口座情報や金融取引にかかる処理を API によって提供するケースが挙げられる。個人の顧客が複数の金融機関に開設している預金口座の情報をフィンテック事業者のアプリによって一元的に収集・管理するなど、使い勝手のよいサービスが既に提供されている。フィンテック事業者がこうしたサービスを複数の金融機関と連携して円滑に実現するうえで、オープン API は不可欠な技術である（Alam, Azad, and Ali [2022]、Basel Committee on Banking Supervision [2024]）。

オープン API を用いた安全な金融サービスを実現するうえで、認可に関する処理（認可処理）が重要である。金融機関は、顧客がフィンテック事業者に対して何らかの処理の実行を認可したことを適切に確認するなど、認可処理を適切に実行する必要がある。金融サービスにおける認可処理の実装では、OAuth 2.0 に準拠するケースが多い（中村［2018］）。OAuth 2.0 は、認可処理を実現するプロトコル（認可プロトコル）のフレームワークを定める標準仕様 RFC 6749（Hardt [2012]）とそれに付随する各種機能を実現するための多数の標準仕様から構成されている。適用するサービスの機能や特性に応じて採用する標準仕様を選択し、フレームワークと組み合わせて実装するというアプローチとなっている。そのため、セキュリティの観点からは、オープン API を用いるサービスのリスク[1] を評価したうえで、リスク軽減策として適切なセキュリティ機能を選択し、それを実現するための標準仕様の要求事項を選択して実装することが求められる。

もっとも、OAuth 2.0 に関連する標準仕様にはさまざまな要求事項が存在することから、認可プロトコルの処理フローをなるべく効率化しつつ、選択したセキュリティ機能に必要な要求事項を適切に抽出して認可プロトコルの設計に反映することは必ずしも容易でない。OAuth 2.0 に準拠したオープン API の実装において、必須とされる要求事項が満たされていない事例が少なからず存在することが学術研究の成果として最近発表されている（Philippaerts, Preuveneers, and Joosen [2022, 2023]）。この研究では、OAuth 2.0 に準拠したサービス（約 100 件）を対象に、標準仕様やベスト・プラクティスにおいて必須とされる要求事項が満たされているか否か、満

1 オープン API を用いるサービスのリスクを評価する際には、本稿で焦点を当てる認可に関連するリスクに加えて、API に関連する業務フローやシステム・リソースのリスク、API の接続先のリスクなど、他のリスクについても評価し対応する必要がある。API に関連する各種リスクについては補論 1. を参照されたい。

たされていない場合にはどのような脆弱性が存在しうるかが調査・分析された。その結果、OAuth 2.0 のフレームワークの技術仕様において必須とされる要求事項の約 2 割が満たされていなかったことが判明した。また、要求事項が満たされていないことによって脆弱性が存在し、それが悪用された場合、顧客に関する情報が漏洩するなどの問題が生じうることが示された。

OAuth 2.0 の標準仕様における要求事項を適切に選択するうえで、セキュリティの観点から選択すべき要求事項を定めている FAPI 2.0 を活用することが有用である（Fett [2022b]）。FAPI 2.0 は、比較的価値が高い情報を取得したり取引を実行したりするケース（high-value scenario）を想定しており、FAPI 2.0 の要求事項に沿って認可プロトコルを設計・実装することによって比較的高いセキュリティを達成することが期待できる。また、一定の条件のもとでは特定のセキュリティ目標の達成を数学的に証明することができるという望ましい面もある（Hosseyni, Küsters, and Würtele [2024]）。

ただし、証明の前提となる条件が実装環境と合致しないケースでは、セキュリティ目標の達成可否が定かでないため、相応のリスクが存在する可能性がある。FAPI 2.0 の要求事項を採用する際には、適用対象のサービスや実装環境が FAPI 2.0 における想定と整合的か否かを確認し、整合的でない部分がある場合、それに関連するリスクを軽減するための対策を追加するなどの対応が求められる。こうした留意点を考慮しつつ FAPI 2.0 を適切に活用することが重要である。

2 節では、オープン API における認可処理の全体像と、それを具体化した OAuth 2.0 のフレームワークを説明する。3 節では、OAuth 2.0 の認可プロトコルに対する主な脅威や攻撃方法を中村［2018］をベースに説明するほか、Philippaerts, Preuveneers, and Joosen [2022, 2023] を引用し、標準仕様などの要求事項の充足度合いや脆弱性に関する研究結果を紹介する。4 節では、FAPI 2.0 の主な要求事項を説明するほか、3 節の攻撃方法への有効性を考察する。

2. オープン API における認可処理

本節では、認可処理の全体像と OAuth 2.0 の認可プロトコルのフレームワークを説明する。

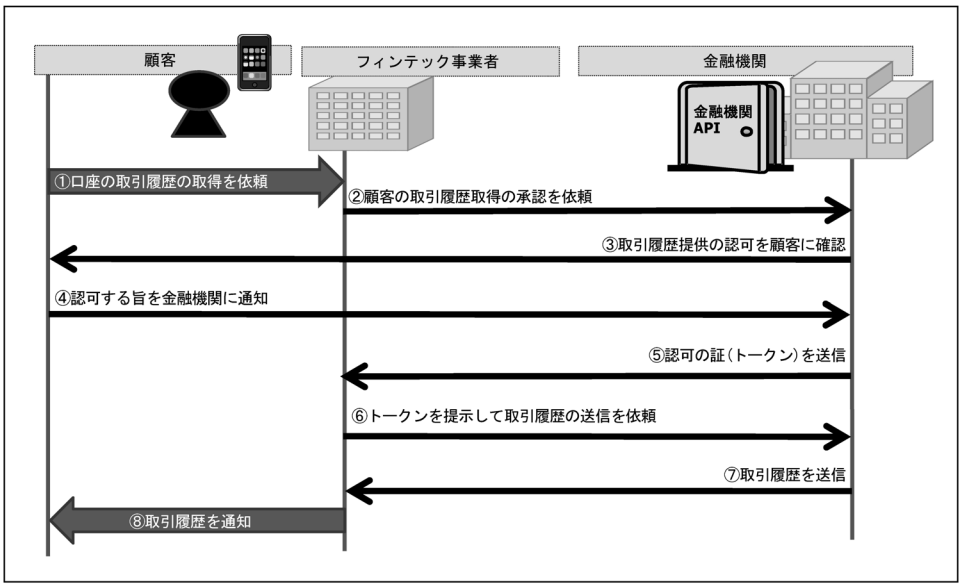
(1) 認可処理の全体像

理解しやすいように、ここでは、フィンテック事業者が金融機関にオープン API

を介してアクセスし、顧客の口座の取引履歴を取得するケースを考える。顧客の依頼を受けたフィンテック事業者は、取引履歴を顧客に代わって取得することを金融機関に認めてもらう必要がある。金融機関は、フィンテック事業者に取引履歴を提供することを顧客に確認する必要がある。こうした処理の流れは次のように整理することができる（図 1 を参照）[2]。

① 顧客は、自分の口座の取引履歴の取得をフィンテック事業者に依頼する。
② フィンテック事業者は、金融機関のオープン API を用いて、顧客の口座の取引履歴の取得に対する承認を金融機関に依頼する。
③ 金融機関は、フィンテック事業者に取引履歴を提供することを顧客に確認する。
④ 顧客は提供を認可する旨を返信する。
⑤ 金融機関は、認可の証となるデータ（トークン）をフィンテック事業者に送信する。
⑥ フィンテック事業者はトークンを金融機関に提示して取引履歴の送信を依頼する。
⑦ 金融機関は取引履歴をフィンテック事業者に送信する。
⑧ フィンテック事業者は顧客に取引履歴を通知する。

図 1　オープン API における認可処理の全体像（イメージ）



2 ここでは、認可処理に注目するために、通信相手の確認や通信メッセージの一貫性の確認の処理を明記していないが、通常、これらの処理（認証）も実行される。

(2) OAuth 2.0 の認可プロトコルのフレームワーク

イ. エンティティ

OAuth 2.0 の認可プロトコルのフレームワークでは、リソース・オーナー、ユーザ・エージェント、クライアント、リソース・サーバ、認可サーバが登場する。

●リソース・オーナー

リソース・オーナーは、金融機関の顧客であり、フィンテック事業者の顧客でもある。ここでのリソースとは、フィンテック事業者が顧客の認可によって取得する情報（金融機関に顧客が開設している口座の取引履歴など）や実行する取引（送金など）を意味している。以下では、理解しやすくするために、リソース・オーナーを顧客と呼ぶ。

●ユーザ・エージェント

ユーザ・エージェントは、顧客がフィンテック事業者や金融機関とやり取りするためのソフトウェアである。主に、顧客の端末のブラウザを想定している。以下ではユーザ・エージェントをブラウザと呼ぶ。

●クライアント

クライアントは、フィンテック事業者が顧客にサービスを提供するためのアプリケーション・ソフトウェアである。

クライアントは、顧客の端末内で動作するもの（ネイティブ・アプリ）[3] と、フィンテック事業者のサーバで動作するもの（サーバ・アプリ）がある。OAuth 2.0 では、ネイティブ・アプリに関して、各アプリが固有の秘密情報（暗号鍵など）[4] を安全に使用することができないケース（パブリック・クライアント）を対象としている。サーバ・アプリに関しては、固有の秘密情報を安全に使用することができるケース（コンフィデンシャル・クライアント[5]）を想定している。

●リソース・サーバ

リソース・サーバは、金融機関のサーバであり、顧客の口座を管理して口座の取引履歴を提供したり送金を実行したりする。

●認可サーバ

認可サーバは、金融機関のサーバであり、顧客の認可を確認したうえでフィン

3 ネイティブ・アプリは、インターネット上のアプリ配信サイトなどから端末にダウンロード・インストールされて動作するケースや、顧客の端末のブラウザ上でウェブ・アプリケーションとして動作するケースがある。

4 秘密情報は、クライアントが他のエンティティに対して認証を実施する際などに用いられる。

5 コンフィデンシャル・クライアントには、各クライアントに固有の秘密情報がそのクライアント自身によって安全に管理されるケースに加えて、端末や OS の機能によって安全に管理されるケースも含まれる。

テック事業者に顧客のリソースへのアクセスを許可する。

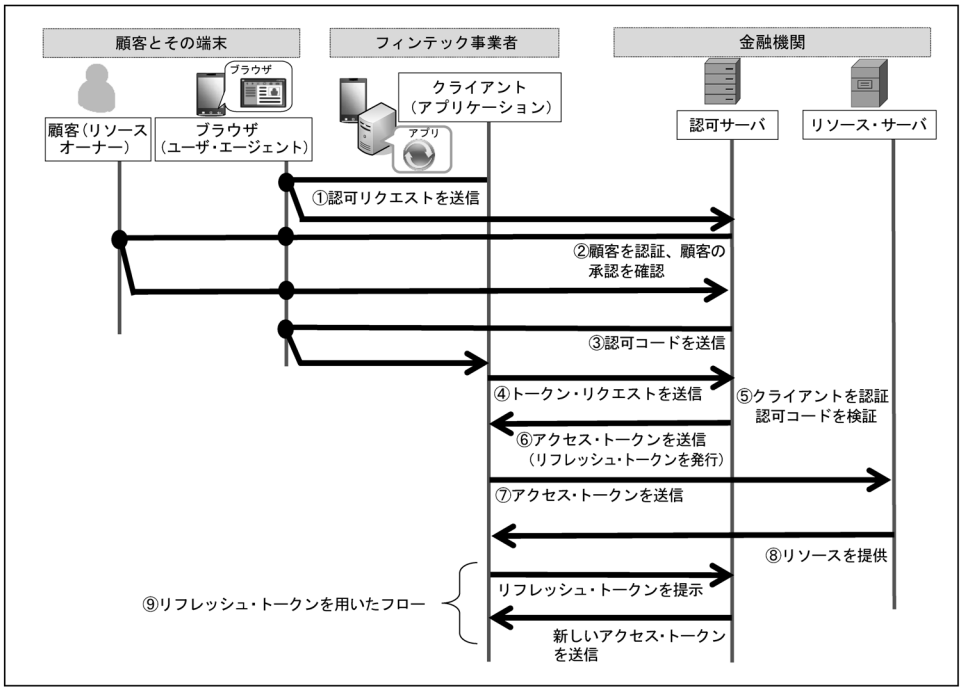
ロ．認可プロトコルの処理フロー

OAuth 2.0 では、認可プロトコルの処理フローとして、認可コード・フロー[6]、インプリシット・フロー、リソース・オーナー・パスワード・クレデンシャル・フロー、クライアント・クレデンシャル・フローの 4 種類[7] が想定されている[8]。以下では、代表的なフローである認可コード・フローを取り上げて説明する。概要は以下のとおりである（図 2 を参照）。

① クライアントは、顧客の口座の取引履歴へのアクセスを求めるメッセージ（認可リクエスト）を認可サーバに送信する。認可リクエストは顧客のブラウザを経由して認可サーバに送られる。
② 認可サーバは、顧客を認証し、クライアントへの認可を確認する。顧客の認証では、例えば、認可サーバはインターネット・バンキングのログイン ID・パスワードの入力を顧客に求める。
③ 顧客から認可を確認した後、認可サーバは、その証として認可コードを発行し、それを含むメッセージ（認可レスポンス）をクライアントに送信する。認可レスポンスは、ブラウザを経由してクライアントに送信される。
④ クライアントは、認可サーバを認証した後、認可コードなどを認可サーバに送信し、アクセス・トークンの送信を依頼する（トークン・リクエスト）。
⑤ 認可サーバは、クライアントを認証した後、認可コードを検証する。具体的には、認可コードが有効であること、アクセス・トークンの送信先が認可コードの送信先と一致していることなどを検証する。
⑥ 認可サーバは、認可コードの検証が成功した場合、アクセス・トークンを発

6 認可コードは、認可サーバが顧客による認可を確認した証としてクライアントに対して発行するトークンである。
7 インプリシット・フローは、認可サーバがクライアントに認可コードを発行せずに直接アクセス・トークン（クライアントがリソースにアクセスする際に用いられるトークン）を発行する方式である。リソース・オーナー・パスワード・クレデンシャル・フローは、クライアントが認可サーバから認可コードを受け取る代わりに顧客からログイン ID とパスワードを受け取り、それを認可サーバに送信することによってアクセス・トークンを得る方式である。クライアント・クレデンシャル・フローは、クライアントが認可コードの代わりに自分のクレデンシャルを認可サーバに送信してアクセス・トークンを得る方式である。
8 これらに加えて、OAuth 2.0 の拡張として、デバイス認可フロー（Denniss *et al.* [2019]）とクライアント・イニシエイティッド・バックチャネル認証フロー（Fernández *et al.* [2021]）が存在する。デバイス認可フローは、顧客の端末がブラウザを搭載していない、または、顧客とのインタフェースに制限があるなどの場合を想定した方式である。クライアント・イニシエイティッド・バックチャネル認証フローは、クライアントと（顧客の）ブラウザ間の通信が行われることなく、認可サーバが顧客の認証や認可の確認を（顧客の）端末との間で直接行う場合を想定した方式である。

図 2　OAuth 2.0 における認可コード・フロー



資料：中村［2018］図表 2

行してクライアントに送信する。認可サーバは、アクセス・トークンが有効期限切れとなった際に新しいアクセス・トークンを得るためのリフレッシュ・トークンを発行してクライアントに送信する場合がある。

⑦ クライアントは、アクセス・トークンをリソース・サーバに送信する。

⑧ リソース・サーバはアクセス・トークンを検証し、それが成功すればクライアントにリソース（ここでは口座の取引履歴）を提供する。

⑨ クライアントは、アクセス・トークンの有効期限が切れた際に、リフレッシュ・トークンを認可サーバに提示して新しいアクセス・トークンを取得する場合がある。リフレッシュ・トークンを取得しておくことによって、クライアントは、認可処理を再度実施することなく、新しいアクセス・トークンを得ることができる。

3. 認可処理における主な脅威

(1) 攻撃者の想定と主な脅威

攻撃者が、2 節で紹介した一連の処理における脆弱性を悪用して被攻撃者（顧客）の口座の取引履歴の入手を試みるケースを考える。金融機関、フィンテック事業者、攻撃者に関して以下の想定を置く。これは中村［2018］の想定と同一である。

・ 金融機関が管理するサーバの特権は攻撃者に奪取されない。
・ 金融機関とフィンテック事業者の内部者は不正行為を行わない。
・ 攻撃者は、クライアント、それが稼働する端末・サーバ、顧客の端末、ブラウザに関して、管理者権限を奪取することがある。
・ 攻撃者は、暗号化・署名に関する処理、および、認証に関する処理を不正に実行することができない。

(2) 主な脅威の類型

本節（1）の想定のもとで主な脅威を整理すると以下の 4 つが挙げられる（表 1 を参照）[9]。これらのうち、I〜III の脅威に対応する攻撃方法は中村［2018］を引用し、IV の脅威に対応する攻撃方法は OAuth 2.0 のセキュリティ・ベスト・カレント・プラクティス（Lodderstedt *et al.* [2024]）[10] において紹介されているものを引用した。各攻撃方法の概要は補論 2. を参照されたい。

I. アクセス・トークンを奪取する。
II. クライアントとリソース・サーバとの間のセッションを奪取する。
III. 自分の口座の取引履歴を攻撃者の口座の取引履歴として入力するように顧客を誘導する。
IV. ブラウザを不正なサイトにアクセスさせ、クレデンシャルを入力するように顧客を誘導して奪取する。その後、顧客のクレデンシャルを用いて顧客になりすまし、認可プロセスを実行する。

9 脅威や攻撃方法の名称については、内容を理解しやすくするために、中村［2018］のものを一部変更している。
10 このベスト・プラクティスは OAuth 2.0 において想定すべき脅威とそれへの対策例を記載している。

表 1　主な脅威と攻撃方法

主な脅威	攻撃方法
Ⅰ．アクセス・トークンの奪取	① アクセス・トークンの推測
	② 通信経路上での盗聴
	③ クライアントからの奪取
	④ 転送機能の悪用
	⑤ 中継サーバの自動接続機能の悪用
	⑥ 認可リクエストの改変
Ⅱ．セッションの奪取	⑦ 不正なアプリの使用
	⑧ セッション管理用パラメータの奪取
Ⅲ．顧客の誘導	⑨ 攻撃者のリソースの偽装
	⑩ セッション管理用パラメータの悪用
Ⅳ．顧客のクレデンシャルの奪取	⑪ 不正なサイトへのリダイレクト

備考：中村［2018］と Lodderstedt *et al.* [2024] をベースに作成した。

(3)　認可プロトコルの実装における脆弱性と脅威の調査・分析の事例

本節（2）で示した脅威や攻撃方法は広く知られている。したがって、OAuth 2.0 の各種標準仕様の要求事項などを参照しつつ、各脅威によるリスクを軽減するための対応が相応に実施されているとみることができる。この点について、標準仕様などの要求事項が実装においてどの程度満たされているか、また、どのような脆弱性が残存しているかを調査・分析した研究事例（Philippaerts, Preuveneers, and Joosen [2022, 2023]）が最近発表されている。

この研究は個人の ID 情報を第三者に提供するサービスを対象としている。このサービスは、ある組織が保持している ID 情報を、それに紐づく個人による認可に基づいて他の組織に提供するというものであり、広く提供されている。この研究は、一般的な認可プロトコルの実装におけるセキュリティの現状を把握して金融分野での検討に活用するという観点で有益である。

イ．調査の概要

調査の対象や実施時期など、概要は以下のとおりである。

- 調査対象：オープン API による個人 ID 提供事業者（individual identity

provider）。全体で 100 件（初回の調査）[11]。このうち 20 件は OpenID Connect もサポートしている[12]。また、海外の金融機関 2 件が含まれている。

- 調査実施時期（2 回）：2020 年 11 月（初回）と 2023 年 3 月（フォローアップ）であり、フォローアップでの調査対象は 100 件（初回）のうち 92 件。
- 調査の内容：主な標準仕様やベスト・プラクティスにおいて必須（must）や推奨（should）とされている要求事項が満たされているか否かを明らかにする。ただし、調査者は、クライアントおよび顧客として調査対象先にアクセスすることから、要求事項のうち、認可サーバやリソース・サーバに関するもののみを調査する。対象とする主な標準仕様やベスト・プラクティスは以下のとおりである[13]。
  - RFC 6749: The OAuth 2.0 Authorization Framework
  - RFC 6750: The OAuth 2.0 Authorization Framework: Bearer Token Usage[14]
  - RFC 6819: OAuth 2.0 Threat Model and Security Considerations[15]
  - RFC 7009: OAuth 2.0 Token Revocation[16]
  - RFC 7523: JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants[17]
  - RFC 7636: Proof Key for Code Exchange by OAuth Public Clients (PKCE)[18]

11 調査対象先は Philippaerts, Preuveneers, and Joosen [2022] に明記されている。この論文の筆者らは論文発表前に調査対象先に対して内容を連絡し発表の許諾を得ている（coordinated disclosure）。

12 OpenID Connect は、OAuth 2.0 において、認可サーバの認証結果に基づいてクライアントがリソース・オーナーの属性を検証するとともに、クライアントがリソース・オーナーの属性情報を認可サーバなどから取得するプロトコルである（Sakimura *et al.* [2014]）。

13 いずれも 2021 年 5 月 20 日時点のものが参照されている。

14 この標準仕様は、保持者と紐づけされていないアクセス・トークン（bearer token）を使用するケースにおいて、クライアントがアクセス・トークンをリソース・サーバに送信する手順やメッセージ形式を定めている（Jones and Hardt [2012]）。

15 この標準文書は、OAuth 2.0 におけるセキュリティの特性、プロトコルを実装・運用する際に想定すべき脅威、各脅威への対策方針などを記載している（Lodderstedt, McGloin, and Hunt [2013]）。

16 この標準仕様は、アクセス・トークンなどを失効させる際に、クライアントと認可サーバの通信されるメッセージの形式、セキュリティ上の留意点などを定めている（Lodderstedt, Dronia, and Scurtescu [2013]）。

17 この標準仕様は、JavaScript ベースのトークン JWT（JSON〈JavaScript Object Notation〉Web Token）によってアクセス・トークンを実装するケースにおいて、トークンの形式や処理方法、使用上の留意点などを定めている（Jones, Campbell, and Mortimore [2015]）。

18 この標準仕様は、認可サーバが認可コードの正当な保持者を確認する手法 PKCE を定めている（Sakimura, Bradley, and Agarwal [2015]）。クライアントは、乱数 R とそのハッシュ値（コード・チャレンジ）を生成したうえで、認可リクエストにコード・チャレンジと（それを生成した）ハッシュ関数の情報を加えて認可サーバに送信する。認可サーバは、認可コード発行時に、それと紐づけてコード・チャレンジとハッシュ関数を登録する。トークン・リクエストにおいて、クライアントは R を認可コードとともに認可サーバに送信し、認可サーバは R からコード・チャレンジを生成して認可コードとの対応関係を確認する。確認できた場合、認可サーバは通信相手のクライアントが認可

  - OAuth 2.0 Security Best Current Practice
  - OpenID Connect
- 調査の手法：以下の手順で調査が実施された。
  ① 標準仕様などからセキュリティに関する要求事項を抽出する。
  ② 抽出した各要求事項が調査対象先において満たされているか否かを明確にするためのテスト・ケース[19]をそれぞれ作成する。
  ③ 調査者の端末に（各調査対象先の）クライアントをインストールし、調査対象先にアクセスしてテスト・ケースを実行する。
  ④ テスト・ケースの結果から、調査対象先における各要求事項の達成状況を明らかにするほか、要求事項が満たされていないことによって生じうる脆弱性やそれを悪用する脅威を分析する。

ロ. 主な調査・分析結果

上記の調査・分析が 2020 年 11 月と 2023 年 3 月にそれぞれ実施された。主な結果を紹介すると以下のとおりである。

・調査対象先がサポートしていた認可プロトコルの処理フローに関しては、2020 年 11 月の調査において、認可コード・フローをサポートしていた調査対象先が全体の約 94%であった。インプリシット・フロー、リソース・オーナー・パスワード・クレデンシャル・フローをサポートしていた先はそれぞれ全体の約 37%、約 3%であった。
・標準仕様などにおける要求事項の充足度合いを表す指標として、失敗したテスト・ケースがテスト・ケース全体に占める割合（失敗率〈failure rate〉）[20]を算出した。失敗率が低いほど要求事項の充足度合いが高いと判断できる。2023 年 3 月の調査では、OAuth 2.0 のフレームワークの標準仕様 RFC 6749 において、必須および推奨の要求事項に対応するテスト・ケースの失敗率がそれぞれ約 19%、約 37%であった（表 2 を参照）。セキュリティ・ベスト・カレント・プラクティスでは、必須および推奨の要求事項に対応するテスト・ケースの失敗率がそれぞ

コードの正当な保持者と判断する。

19 テスト・ケースは、それが失敗した場合、対応する要求事項が満たされていないと判断できるように作成される。例えば、要求事項が「コンフィデンシャル・クライアントは認可サーバに対して認証を実施しなければならない（必須である）」というものの場合、これに対応するテスト・ケースとして、「クライアントは、クライアント認証を実施することなく、認可サーバからアクセス・トークンを取得することができない」と設定する。仮に、ある個人 ID 提供事業者においてこのテスト・ケースが失敗した場合（クライアント認証なしでアクセス・トークンの取得が可能な場合）、対応する要求事項が満たされていないと判断することができる。

20 調査対象先（全体で 92 件）に対してそれぞれテスト・ケースを実施し、失敗したケースがテスト・ケース全体に占める割合を調査対象先ごとに算出する。そのうえで、失敗したケースの割合を調査対象先に関して平均し、それをテスト・ケースの失敗率とする。

表２　各標準仕様などにおけるテスト・ケースの失敗率（2023 年 3 月時点）

標準仕様やベスト･プラクティス	テスト・ケースの失敗率	
	必須の要求事項	推奨の要求事項
RFC 6749（Authorization Framework）	19.1	36.9
RFC 6750（Bearer Token Usage）	0.4	62.2
RFC 6819（Threat Model and Security Considerations）	1.8	21.6
RFC 7009（Token Revocation）	4.3	12.5
RFC 7523（JWT Profile）	12.5	---
RFC 7636（PKCE）	8.4	---
Security Best Current Practice	31.7	65.6
OpenID Connect	16.2	5.3

備考：表中の数字の単位はパーセント。値が小さいほど要求事項の充足度合いが高い。

れ約 32％、約 66％であった。

・テスト・ケースの結果から判明した主な脆弱性・脅威は以下のとおりである。

① リフレッシュ・トークンの奪取・悪用：約 44％の調査対象先（2020 年 11 月時点）において、認可サーバによるリフレッシュ・トークンの取扱いが不適切な場合[21]があった。リフレッシュ・トークンを奪取した攻撃者は、この取扱いによってアクセス・トークンを入手する。この脆弱性は、表 1 におけるクライアントからの奪取に対応する攻撃で悪用される可能性がある。

② 認可コードの悪用：約 43％の調査対象先において、認可サーバが PKCE を適切に実施していない場合[22]があったほか、約 14％の調査先において、使用済みの認可コードが再度提示された際にアクセス・トークンを誤って発行する場合があった。このような場合、認可コードを奪取した攻撃者はアクセス・トークンを入手することができる。この脆弱性は、表 1 における中継サーバの自動接続機能の悪用やセッション管理用パラメータの奪取に対応する攻撃で悪用される可能性がある。

21 例えば、クライアント認証によってリフレッシュ・トークンの使用を制限していないケースや、認可サーバが使用済みのリフレッシュ・トークンを無効化していないケースである。

22 例えば、認可サーバが、コード・チャレンジの値を含まない認可リクエストを受信したにもかかわらず認可プロトコルをそのまま継続する（エラー・メッセージを返信したり認可プロトコルを中止したりしない）ケースが紹介されている。このようなケースにおいて、攻撃者は、認可リクエストのコード・チャレンジのみを削除することによって PKCE を無効化することができる場合がある（PKCE ダウングレード攻撃）。

③ クライアントへのなりすまし：約 24％の調査対象先において、クライアントが認証用に秘密情報を保持しているにもかかわらず、認可サーバがトークン・リクエストの際などにクライアント認証を適切に実行しない場合があった。このような場合、攻撃者は認可サーバに対してクライアントになりすますことができる。この脆弱性は、表 1 におけるクライアントからの奪取、中継サーバの自動接続機能の悪用、認可リクエストの改変、不正なアプリの使用、セッション管理用パラメータの奪取に対応する攻撃で悪用される可能性がある。

④ ログ・ファイルなどからのアクセス・トークンの奪取：約 40％の調査対象先において、リソース・サーバがクライアントからリソース・リクエストを受信した際に、それに含まれるアクセス・トークンをログ・ファイルなどに意図せず格納しうる場合があった[23]。このような場合、ログ・ファイルへのアクセスが可能な攻撃者はアクセス・トークンを奪取することができる。この脆弱性は、表 1 におけるクライアントからの奪取に対応する攻撃で悪用される可能性がある。

ハ．小括と留意点

標準仕様などにおける必須の要求事項が少なからず満たされていないケースがあることが示された。また、リフレッシュ・トークンやアクセス・トークンの奪取などに悪用されうる脆弱性が相応の割合の調査対象先で存在することも明らかとなった。

ただし、この調査は認可プロトコルにのみ焦点を当てたものであり、調査対象先のサービスのリスクを検討しているわけではない。例えば、認可プロトコルに脆弱性があったとしても、保護対象となる情報（この場合は個人 ID）が漏洩するなどのリスクを運用によって軽減しているケース（例えば、認可コードやアクセス・トークンの有効期間を短く設定する）が考えられる。今回の脆弱性がサービスのリスクの増加につながるとは必ずしもいえない点に留意が必要である。

今回の調査は個人 ID を提供するサービスを対象としたものであり、金融分野の状況を示すものではないが、金融機関やフィンテック事業者は、認可プロトコルの実装における脆弱性の実例として捉え、自社のサービスにおける脆弱性の洗出しやリスク評価を実施する際に参考にすることができる。

23 クライアントがリソース・リクエストにおいてアクセス・トークンを URL の一部（クエリ・パラメータ）として埋め込んでリソース・サーバに送信する場合、これを受信したリソース・サーバがログ・ファイルにアクセス・トークンを格納するほか、過去の通信相手の URL を外部に送信する際にアクセス・トークンも一緒に送信する可能性がある。リソース・サーバには、アクセス・トークンをログ・ファイルに格納しないようにする、または、ログ・ファイルからの情報漏洩を防止することが求められる。

4. 認可プロトコルにおける FAPI 2.0 の適用

3 節（3）の研究成果は、OAuth 2.0 の認可プロトコルの実装にさまざまな脆弱性が潜んでいる可能性を示唆している。こうした脆弱性を作り込まないように認可プロトコルを設計・実装することが望ましい。その方法の 1 つとして、FAPI 2.0 を活用することが考えられる。

(1) FAPI 2.0 の概要

FAPI 2.0 の旧バージョンである FAPI セキュリティ・プロファイル 1.0（FAPI 1.0）は、2016 年 6 月に OpenID Foundation の FAPI ワーキング・グループによって策定が開始され、2021 年 3 月に公開された。その後、FAPI 1.0 の改訂が始まり、2022 年 12 月に FAPI 2.0 セキュリティ・プロファイルのインプリメンテーション・ドラフト（Fett [2022b]）が公開された[24]。

FAPI という名称は、金融サービスを対象として策定された経緯から、当初は「Financial-grade API」の略称として呼ばれていた。その後、金融分野に限らず医療分野や公的分野などでも幅広く活用されるようになったことから、現在では「FAPI」が（略称ではなく）正式名称となっている。

FAPI 2.0 のセキュリティ目標は、以下のそれぞれの状態を達成することである（Fett [2022a]）。

・攻撃者が他者の（保護された）リソースにアクセスできない。
・攻撃者が他者の ID のもとでクライアントにログインできない。
・攻撃者が自分の ID のもとで他者をクライアントにログインさせることができない。
・攻撃者が自分のリソースに他者を誘導し使用させることができない。

FAPI 2.0 の要求事項を満たす認可プロトコルが一定の条件のもとでセキュリティ目標を達成することは、形式検証の手法（formal verification）によって証明されている（Hosseyni, Küsters, and Würtele [2024]）。また、FAPI 2.0 を適用した認可プロトコルが実際に要求事項を満たしていることを確認するためのツールが提供されてい

24 以下の FAPI 2.0 に関する説明は 2022 年 12 月のインプリメンテーション・ドラフトに基づく。ただし、本稿の執筆時点において FAPI 2.0 の標準化が継続しており、本節の説明と異なる内容で今後標準化が進められる可能性がある点に留意されたい。

るほか、ツールによる確認が実施された事例も知られている[25]。

(2) FAPI 2.0 における想定環境や攻撃者

イ. 想定環境とスコープ

主な想定環境とスコープは以下のとおりである。

・暗号化やデジタル署名に用いられる鍵の配送は、期待通り安全に行われる。
・顧客の端末やブラウザは安全に動作する。
・攻撃者に悪用されていないエンティティは期待通りに動作する。
・暗号鍵などの秘密情報はランダムで安全に生成される。攻撃者が秘密情報を効率的に推定することは困難である。
・クレデンシャルの漏洩につながるデータベースの設定ミス、OS やブラウザの設定ミスは、スコープ外とする。
・認可サーバ上でマルウェアなどを実行させる攻撃（remote code execution）はスコープ外とする。
・フィッシングへの対策はスコープ外とする。
・クライアントや認可サーバによる顧客の登録・本人確認、当人確認、ID・アクセス管理は、スコープ外とする。

ロ. 攻撃者の類型

攻撃者の類型は主に表 3 の 5 つである。特に、表 3 の A3a と A7 の攻撃者は、認可サーバとリソース・サーバにそれぞれアクセス可能であり、相当高度なスキルを有していることを想定している。もっとも、アクセス対象は認可リクエストとリソース・サーバへのリクエストであり、攻撃者が入手できる情報が限定されている。

(3) FAPI 2.0 の要求事項を適用した認可プロトコル

FAPI 2.0 の主な要求事項は以下のとおりである（図 3 参照）[26]。

25 イギリスやブラジルのオープン・バンキング（Open Banking）においては、FAPI 1.0 に基づくものではあるが、こうしたツールによる認証の取得が必須とされている（OpenID Foundation [2022]）。適合性を確認するツールに関する情報は https://openid.net/certification/に掲載されている（アクセス日：2024 年 5 月 27 日）。確認済みの事例は https://openid.net/developers/certified-openid-connect-implementations/ に掲載されている（アクセス日：2024 年 5 月 27 日）。

26 FAPI 2.0 では、認可サーバがインプリシット・フローとリソース・オーナー・パスワード・クレデンシャル・フローによるリクエストを拒否することが定められている。したがって、FAPI 2.0 を適用した認可プロトコルでは、これら以外のフローが使用されることとなる。

表 3　攻撃者の類型

類型	攻撃者の行動の概要
A1	・顧客を不正なサイトに誘導し、任意の認可リクエストを開始させる。 ・他のエンティティ間のメッセージを横取りしたりブロックしたりすることは不可能。認可サーバとして振る舞うこともできない。
A1a	・A1 の行動に加えて、認可サーバとして振る舞う。 ・他の認可サーバから取得したメッセージを悪用したり、顧客を不正なサイトに誘導したりすることができる。
A2	・無線アクセス・ポイントを悪用したり、脆弱なネットワーク・ノードを操作したりして、顧客が使用するネットワークを悪用可能。 ・メッセージの横取り・ブロック・改変が可能。
A3a	・A1 の行動に加えて、認可サーバにアクセス可能。 ・認可リクエストを入手可能。
A7	・A1 の行動に加えて、リソース・サーバにアクセス可能。 ・リソース・サーバへのリクエストを入手可能。

・エンティティ間における暗号通信や認証は、暗号通信プロトコル TLS（Transport Layer Security）のバージョン 1.3、または、一定の条件を満たすバージョン 1.2 を使用して行う[27]。
・クライアントはコンフィデンシャル・クライアントのみとする。
・クライアントへのメタデータの提供は、RFC 8414（OAuth 2.0 Authorization Server Metadata）や OpenID Connect Discovery によって適切に行う[28]。
・認可サーバによるクライアント認証の方式は、MTLS（Mutual TLS）[29] または private_key_jwt[30] とする。

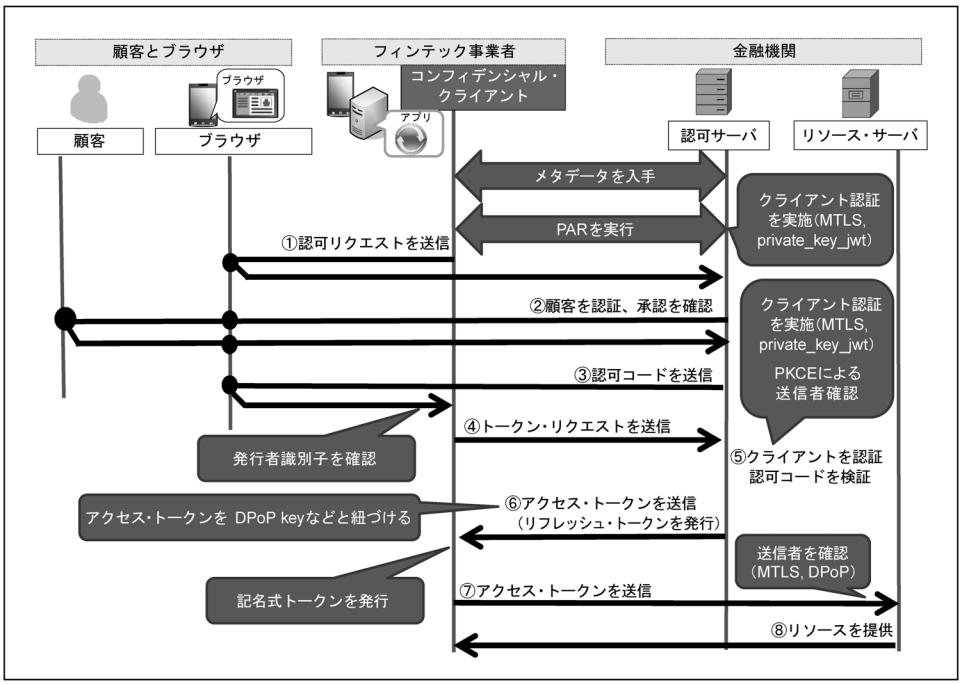
27 TLS 1.2 によって接続する場合には、条件として、TLS の安全な使用のための推奨事項（Sheffer, Holz, and Saint-Andre [2015]）に従うこと、特定の暗号アルゴリズムの組合せを使用することなどが定められている。

28 RFC 8414 は、認可サーバに関するメタデータ（認可サーバの識別子、認可リクエストやトークン・リクエストの送信先アドレス、認可プロトコルの処理フロー、サービス内容など）、メタデータのリクエストやレスポンスのメッセージ形式などを定めている（Jones, Sakimura, and Bradley [2018]）。OpenID Connect Discovery は、クライアントが OpenID Connect に基づく処理を実行する際に、認可サーバのメタデータを取得する方法を定めている（Sakimura *et al.* [2023]）。

29 MTLS（RFC 8705）は、サーバ認証に加えてクライアント認証も実行する TLS を指す（Campbell *et al.* [2020]）。クライアントが自分の電子証明書とデジタル署名を認可サーバに送信し、認可サーバが署名検証や電子証明書の有効性検証などを実施する。

30 private_key_jwt は、クライアントがデジタル署名を JWT に埋め込んで認可サーバに送信し、認可サーバは署名検証によってクライアントを認証する手法である（Sakimura *et al.* [2014]）。

図 3　FAPI 2.0 の主な要求事項を適用した認可コード・フロー



資料：Hosseyni, Küsters, and Würtele [2024] Figure 1

- クライアントが認可リクエストの内容を事前に認可サーバに登録する仕組み PAR（Pushed Authorization Request）[31] を用いる。認可サーバは登録時にクライアント認証を実施する。
- クライアントは認可レスポンス内の発行者識別子を用いて認可サーバを特定・検証する。
- 認可サーバは認可コードの送信者確認を PKCE（ハッシュ関数 SHA256 によるコード・チャレンジを使用）によって行う。
- 認可サーバは記名式トークン（持ち主が特定されているトークン）のみ発行する。
- リソース・サーバはアクセス・トークンの送信者確認を行う。その方法として、MTLS または DPoP（Demonstrating Proof of Possession）[32] を用いる。DPoP を使

31 PAR（RFC 9126）は、クライアントが認可リクエスト送信前にリクエスト内容など（PKCE のコード・チャレンジなども含まれる）を認可サーバに直接送信・登録する手法である（Lodderstedt *et al.* [2021]）。認可リクエスト時には、リクエスト内容などの情報の格納先を示す情報（Uniform Resource Identifier）とクライアントの識別子のみを送信する。これによって、リクエスト内容がブラウザなどから漏洩したり改変されたりするリスクを低くすることができる。

32 DPoP（RFC 9449）は、クライアントの署名検証鍵（DPoP key）を用いてアクセス・トークンの送信

用する場合、認可サーバは認可コードも DPoP key と紐づけする。
・認可サーバは顧客が認可の内容を正しく認識して認可処理を開始するように情報を適切に提供する。

(4) 各攻撃方法によるリスク軽減に寄与する主な要求事項

FAPI 2.0 の要求事項を満たすように OAuth 2.0 の認可コード・フローを実装したとする。その場合、3 節（2）の表 1 に示した各攻撃方法によるリスクの軽減に寄与するか否かを検討すると、表 4 に示すように、大半の攻撃方法によるリスクの軽減に寄与する。表 4 の「リスク軽減に寄与する FAPI 2.0 の主な要求事項」の列に記載されている要求事項（群）は、それぞれ対応する攻撃方法への対策となりうる要求事項を示しており、攻撃方法を防止するための十分条件ではない点に留意されたい。また、これらの要求事項を適用した際のリスク軽減の効果が十分か否かは、各サービスのビジネス要件に依存するため、一概にはいえない。

一部の攻撃方法については、リスクを軽減できない場合やその効果が状況に依存する場合がある。具体的には、不正なアプリの使用、セッション管理用パラメータの奪取、攻撃者のリソースの偽装、セッション管理用パラメータの悪用が挙げられる。これらについてそれぞれ以下で説明する。

イ. 不正なアプリの使用

これは、攻撃者が不正なアプリを顧客の端末にインストールさせ、そのアプリを用いて認可コードや顧客のリソースを奪取する攻撃である。FAPI 2.0 には不正なアプリを排除する機構が準備されておらず、FAPI 2.0 の要求事項を適用するだけではリスクを十分に軽減することが困難である。

対策としては、フィンテック事業者がアプリ配信サイトを限定する、アプリ配信サイトにおける不審なアプリを探索・排除する、正しいアプリの入手方法を顧客に説明して理解を得るといった対応が挙げられる[33]。

ロ. セッション管理用パラメータの奪取

これは、攻撃者がクライアントやそれが動作する端末の管理者権限を用いてセッ

者を確認する手法である（Fett *et al.* [2023]）。アクセス・トークンは DPoP key と紐づけされて発行される。リソース・サーバは、クライアントから、アクセス・トークンとともにクライアントのデジタル署名（DPoP Proof）と署名検証鍵を受信した後、署名検証、および、署名検証鍵とアクセス・トークンの対応関係を認可サーバへの問合せなどにより検証する。

33 これらに加えて、例えば、顧客の端末の OS による不正なアプリの使用を防止する機構（アプリのインストールの状態、通信内容、既知の不正なコードの有無などから不正なアプリか否かを分析・判断するなど）を活用するといった対応も考えられる。

表 4　各攻撃方法によるリスク軽減に寄与する FAPI 2.0 の主な要求事項

攻撃方法	リスク軽減に寄与する FAPI 2.0 の主な要求事項 （【 】：要求事項の効果）
① アクセス・トークンの推測	128 ビット以上のエントロピーをもつクレデンシャルの使用
② 通信経路上での盗聴	TLS（バージョンが 1.3 または条件付きで 1.2）の採用
③ クライアントからの奪取	・トークン送信者の確認 【アクセス・トークンの不正使用の検知】 ・クライアント認証 【リフレッシュ・トークンの不正使用の検知】
④ 転送機能の悪用	・オープン・リダイレクト（自動転送）の禁止 ・PAR【リダイレクト先の情報の事前登録と改変の検知】 ・トークン送信者の確認 【アクセス・トークンの不正使用の検知】
⑤ 中継サーバの自動接続機能の悪用	・PKCE【認可コードの不正使用の検知】 ・PAR【PKCE のコード・チャレンジの事前登録】 ・クライアント認証【認可コードの送信者の検証】 ・トークン送信者の確認 【アクセス・トークンの不正使用の検知】
⑥ 認可リクエストの改変	・メタデータの安全な提供 【正しいリソース・サーバなどの特定】 ・PAR【リダイレクト先の情報の事前登録と改変の検知】 ・発行者識別子の検証【認可コードの発行者の検証】 ・クライアント認証【認可コードの送信者の検証】 ・トークン送信者の確認 【アクセス・トークンの不正使用の検知】
⑦ 不正なアプリの使用	（不正なアプリの排除機構が準備されていない）
⑧ セッション管理用パラメータの奪取 （奪取した認可コードなどを用いてクライアントになりすますケース）	・PKCE【認可コードの不正使用の検知】 ・PAR【PKCE のコード・チャレンジの事前登録】 ・クライアント認証【認可コードの送信者の検証】 ・トークン送信者の確認 【アクセス・トークンの不正使用の検知】
⑨ 攻撃者のリソースの偽装 ⑩ セッション管理用パラメータの悪用	認可内容の情報の顧客への十分な提供 （効果は顧客による認可内容の理解度合いに依存）
⑪ 不正なサイトへのリダイレクト	・オープン・リダイレクト（自動転送）の禁止 ・PAR【リダイレクト先の情報の事前登録と改変の検知】

ション管理用のパラメータを奪取し、それを悪用して正規のセッションを乗っ取るというものである。最終的には、攻撃者は顧客のリソースを不正に入手する。

このタイプの攻撃のうち、攻撃者がセッションの乗っ取りによって認可コードやアクセス・トークンを入手したうえで認可サーバやリソース・サーバにそれらを提示するケースに関しては、FAPI 2.0 の要求事項（クライアント認証、PKCE、PAR、トークン送信者の確認）によって、攻撃者によるクライアントへのなりすましを検知することができる。ただし、攻撃者が、クライアントやそれが動作する端末の管理者権限を悪用し、セッション管理用パラメータの奪取とともに、他の処理（例えば、攻撃者への通信の実施）を実行するケースも想定される。このようなケースに対しては、上記の要求事項による対応だけではリスクを軽減できない可能性がある[34]。

対策としては、FAPI 2.0 の要求事項を満たすことに加えて、クライアントやそれが動作する端末において権限昇格につながる脆弱性を極力排除することが挙げられる。

ハ．攻撃者のリソースの偽装

これは、攻撃者が、攻撃者の口座の取引履歴（金融機関が保持しているもの）のアクセス先に顧客をフィッシングなどによって誘導し、顧客に自分の口座の取引履歴を入力させるなどして奪取するものである。複数の口座の取引履歴を同期させることができるケースでは、攻撃者は、自分の口座の取引履歴と顧客の口座の取引履歴を同期させるように顧客を誘導し、同期させた後で顧客の口座の取引履歴を入手することも想定される。

この攻撃では、正規の認可プロトコルが実行されるため、顧客が攻撃を検知しづらい。FAPI 2.0 では、認可の内容を顧客が正しく理解したうえで認可処理を実施するように、認可サーバが認可内容に関する情報を顧客に十分に提供することとしている。これに基づく対応によって、顧客が認可内容を正確に理解し、攻撃者による誘導に気づくことができたならば、リスク軽減に寄与する。

また、金融機関が複数の口座の取引履歴の同期を禁止する、フィンテック事業者が口座の取引履歴へのアクセス先に関する情報を顧客に対して適切に提供するといった対応もリスク軽減につながる。この攻撃方法によるリスクが高いと判断した場合には、上記の対応を組み合わせて実施することが有用である。

ニ．セッション管理用パラメータの悪用

これは、攻撃者が、クライアントやそれが動作する端末の管理者権限を用いて顧客のセッション管理用のパラメータを攻撃者のものに改変し、顧客を攻撃者の口座の取引履歴のアクセス先に誘導するというものである。この攻撃に関する FAPI

34 例えば、攻撃者が、リソース・サーバから顧客の口座の取引履歴を入手した際にそれを攻撃者のサーバに送信するようにクライアントの機能を改変するというシナリオが考えられる。この場合、クライアント認証やトークン送信者の確認などではリスク軽減が難しい。

2.0 の要求事項の効果や対応に関しては、攻撃者のリソースの偽装の場合と同様である。

5. おわりに

本稿では、オープン API における認可プロトコル OAuth 2.0 について、脅威や攻撃方法を既存研究に基づいて整理したほか、標準仕様などの要求事項が満たされておらず脆弱な実装が少なからず存在している状況を最近の研究成果を引用しつつ紹介した。また、脆弱性を排除する方法として、FAPI 2.0 の要求事項を認可プロトコルに適用した場合、大半の攻撃方法によるリスクの軽減に寄与することを示した。ただし、一部の攻撃方法に関しては、リスクを軽減できない場合やその効果が状況に依存する場合があり、追加的な対応が必要になることも説明した。

サイバーセキュリティの脅威は日々高度化しており、オープン API を標的とした攻撃も今後増える可能性がある[35]。そうしたなか、OAuth 2.0 に関連する標準仕様などの改訂が随時行われているほか、脆弱性や脅威に関する学術研究も進められている。オープン API のシステムのセキュリティを維持・向上させるためには、脅威の状況や標準仕様の動向を常に把握し、脆弱性を生じさせないように認可プロトコルを実装することが必要である。また、リスク評価を適宜実施し、許容できないレベルのリスクが生じている場合にはリスク軽減策を検討することも求められる。こうした対応を実施するうえで、FAPI 2.0 を活用することが有効である。今後、オープン API による安全なサービスが継続的に提供されることを期待したい。

35 Akamai Technologies, Inc. は、2023 年中に発生したインターネット上での攻撃全体の約 3 割が API を標的にしていた旨の調査結果を発表するとともに、攻撃が今後増加する可能性があるとの見方を示している（https://www.akamai.com/lp/soti/lurking-in-the-shadows、アクセス日：2024 年 5 月 27 日）。

参考文献

中村啓佑、「OAuth 2.0 に対する脅威と対策：金融オープン API の一段の有効活用に向けて」、『金融研究』第 37 巻第 3 号、日本銀行金融研究所、2018 年、111～141 頁

Alam, Mahbub Ul, Muhammad Abul Kalam Azad, and Md. Showkat Ali, "Best Practices to Secure API Implementations in Core Banking System (CBS) in Banks," *Proceedings of 2022 IEEE 12th Annual Computing and Communication Workshop and Conference*, IEEE, 2022, pp. 730–735.

Basel Committee on Banking Supervision, "Digitalisation of Finance," Bank for International Settlement, 2024 (available at https://www.bis.org/bcbs/publ/d575.pdf、2024 年 5 月 27 日).

Campbell, Brian, John Bradley, Nat Sakimura, and Torsten Lodderstedt, "OAuth 2.0 Mutual-TLS Client Authentication and Certificate-Bound Access Tokens," RFC 8705, IETF, 2020 (available at https://www.rfc-editor.org/rfc/rfc8705.pdf、2024 年 5 月 27 日).

Denniss, William, John Bradley, Michael B. Jones, and Hannes Tschofenig, "OAuth 2.0 Device Authorization Grant," RFC 8628, IETF, 2019 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc8628.txt.pdf、2024 年 5 月 27 日).

Fernández, Gonzalo, Florian Walter, Axel Nennker, Dave Tonge, and Brian Campbell, "OpenID Connect Client-Initiated Backchannel Authentication Flow—Core 1.0," OpenID Foundation, 2021 (available at https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0.html、2024 年 5 月 27 日).

Fett, Daniel, "FAPI 2.0 Attacker Model," fapi-2_0-attacker-model-03, OpenID Foundation, 2022a (available at https://openid.net/specs/fapi-2_0-attacker-model.html、2024 年 5 月 27 日).

———, "FAPI 2.0 Security Profile," fapi-2_0-security-profile-03, OpenID Foundation, 2022b (available at https://openid.net/specs/fapi-2_0-security-profile.html、2024 年 5 月 27 日).

———, Brian Campbell, John Bradley, Torsten Lodderstedt, Michael B. Jones, and David Waite, "OAuth 2.0 Demonstrating Proof of Possession (DPoP)," RFC 9449, IETF, 2023 (available at https://www.rfc-editor.org/rfc/rfc9449.pdf、2024 年 5 月 27 日).

Hardt, Dick, "The OAuth 2.0 Authorization Framework," RFC 6749, IETF, 2012 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc6749.txt.pdf、2024 年 5 月 27 日).

Hosseyni, Pedram, Ralf Küsters, and Tim Würtele, "Formal Security Analysis of the OpenID FAPI 2.0: Accompanying a Standardization Process," Cryptology ePrint Archive, Paper 2024/078, International Association for Cryptologic Research, 2024 (available at https://eprint.iacr.org/2024/078.pdf、2024 年 5 月 27 日).

Jones, Michael B., Brian Campbell, and Chuck Mortimore, “JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants,” RFC 7523, IETF, 2015 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc7523.txt.pdf、2024 年 5 月 27 日).

———, and Dick Hardt, “The OAuth 2.0 Authorization Framework: Bearer Token Usage,” RFC 6750, IETF, 2012 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc6750.txt.pdf、2024 年 5 月 27 日).

———, Nat Sakimura, and John Bradley, “OAuth 2.0 Authorization Server Metadata,” RFC 8414, IETF, 2018 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc8414.txt.pdf、2024 年 5 月 27 日).

Lodderstedt, Torsten, John Bradley, Andrey Labunets, and Daniel Fett, “OAuth 2.0 Security Best Current Practice,” Internet Draft, draft-ietf-oauth-security-topics-27, IETF, 2024 (available at https://www.ietf.org/archive/id/draft-ietf-oauth-security-topics-27.html、2024 年 5 月 27 日).

———, Brian Campbell, Nat Sakimura, Dave Tonge, and Filip Skokan, “OAuth 2.0 Pushed Authorization Requests,” RFC 9126, IETF, 2021 (available at https://www.rfc-editor.org/rfc/rfc9126.pdf、2024 年 5 月 27 日).

———, Stefanie Dronia, and Marius Scurtescu, “OAuth 2.0 Token Revocation,” RFC 7009, IETF, 2013 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc7009.txt.pdf、2024 年 5 月 27 日).

———, Mark McGloin, and Phil Hunt, “OAuth 2.0 Threat Model and Security Considerations,” RFC 6819, IETF, 2013 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc6819.txt.pdf、2024 年 5 月 27 日).

OpenID Foundation, “Open Banking, Open Data and Financial-Grade APIs: A Whitepaper for Open Banking and Open Data Ecosystem Participants Globally,” Version: Final 1.0, OpenID Foundation, 2022 (available at https://openid.net/wordpress-content/uploads/2022/03/OIDF-Whitepaper_Open-Banking-Open-Data-and-Financial-Grade-APIs_2022-03-16.pdf、2024 年 5 月 27 日).

Philippaerts, Pieter, Davy Preuveneers, and Wouter Joosen, “OAuch: Exploring Security Compliance in the OAuth 2.0 Ecosystem,” *Proceedings of the 25th International Symposium on Research in Attacks, Intrusions and Defenses*, Association for Computing Machinery, 2022, pp. 460–481.

———, ———, and ———, “Revisiting OAuth 2.0 Compliance: A Two-Year Follow-Up Study,” *Proceedings of 2023 IEEE European Symposium on Security and Privacy Workshops*, IEEE, 2023, pp. 521–525.

Sakimura, Nat, John Bradley, and Naveen Agarwal, “Proof Key for Code Exchange by

OAuth Public Clients," RFC 7636, IETF, 2015 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc7636.txt.pdf、2024 年 5 月 27 日).

———, ———, Michael B. Jones, and Edmund Jay, "OpenID Connect Discovery 1.0 Incorporating Errata Set 2," OpenID Foundation, 2023 (available at https://openid.net/specs/openid-connect-discovery-1_0.html、2024 年 5 月 27 日).

———, ———, ———, Breno de Medeiros, and Chuck Mortimore, "OpenID Connect Core 1.0 Incorporating Errata Set 1," OpenID Foundation, 2014 (available at https://openid.net/specs/openid-connect-core-1_0-errata1.html、2024 年 5 月 27 日).

Sheffer, Yaron, Ralph Holz, and Peter Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)," RFC 7525, IETF, 2015 (available at https://www.rfc-editor.org/rfc/pdfrfc/rfc7525.txt.pdf、2024 年 5 月 27 日).

補論 1. API に関するセキュリティ・リスク

The OWASP Foundation Inc.[36] は、API の開発主体やサービス提供主体が認識しておくべき主なセキュリティ・リスク 10 件を「Top 10 API Security Risks」として 2023 年に公表している[37]。リスクをその所在（リスクにつながる脆弱性が存在しうる箇所）に基づいて類型化すると表 A-1 のとおりである。認可プロトコルに関するリスクは、オブジェクトそのもの、オブジェクトのプロパティ、機能の 3 つのレベルに分けられている。

認証プロトコルのリスクについては、従来から金融機関が各種サービスのリスク

表 A-1　OWASP Top 10 API Security Risk (2023) で挙げられているリスク

リスクの所在		主なリスク
認可プロトコル	オブジェクト・レベル	オブジェクトそのものやその識別子の漏洩などによって、リソースへの不正アクセスが発生する。
	オブジェクト・プロパティ・レベル	API の応答からオブジェクトの属性情報が漏洩し、その悪用によってリソースへの不正アクセスが発生する。
	機能レベル	アクセス制御ポリシーの脆弱性（権限を確認しないなど）が悪用され、他のユーザによる API リクエストが横取りされたり改変されたりする。
認証プロトコル		認証プロトコルの脆弱性が悪用され、他のユーザになりすましされる。
API リソース管理		API へのリクエストの制御に不備があり、大量のデータを短時間で送信するなどの攻撃によって、API の処理能力が枯渇する。
業務フロー管理		API へのリクエストの制御に不備があり、短時間でサービス要求を繰り返し行うなどの攻撃によって、業務遂行に問題が発生する。
API のアクセス先管理		API の処理において不適切なサイトへのアクセスが実行され、アクセス先のサイトに関する情報が漏洩する。
API 構成管理		API の設定が不適切であり、他のユーザのリソースやシステムの重要な情報が漏洩する。
API インベントリ管理		API のインベントリ管理が不適切（API の属性情報が更新されないなど）であり、API 構成管理を適切に実施できない。
外部の API の管理		セキュリティ・レベルが低い外部の API にアクセスすることにより、API に関する重要な情報の漏洩、不正な処理、サービス妨害が発生する。

36 The OWASP Foundation Inc. は、ソフトウェアのセキュリティ向上を目的とするグローバルな非営利団体であり、セキュリティ向上に資する各種プロジェクトの支援、イベント開催などを通じた人材交流・コミュニティ形成の支援、セキュリティに関する啓発資料や情報の提供などを行っている。OWASP は Open Worldwide Application Security Project の略称であり、The OWASP Foundation Inc. の登録商標である。

37 これらのリスクは、https://owasp.org/API-Security/editions/2023/en/0x11-t10/（アクセス日：2024 年 5 月 27 日）において公表されている。

のレベルに応じた適切な認証手段を選択・実装してきた。API における処理フローにおいて、顧客やフィンテック事業者をどのように認証するかについても、これまでの延長線上で検討することができる。

API リソース管理や業務フロー管理のリスクについても、従来の業務継続に関する取組みを、API の計算資源の確保や関連業務の継続に拡張してリスク軽減策を検討することになる。

API 構成管理のリスクに関しては、API 開発プロセスにおけるコード・レビューや各種テストの実施を通じて、不適切な設定を検知・修正する対応が考えられる。ソフトウェア開発一般で実施されているものであり、API 開発においても同様に対応することとなる。また、API を FAPI 2.0 ベースで実装する場合、OpenID Foundation による適合性テストや認証スキームを活用することもできる。

API インベントリ管理のリスクについては、金融機関が API のインベントリを適切に構築・管理していない場合、それらのシステムの構成管理に支障が生じ脆弱性への対応などが適切に行われない可能性がある。システムの構成要素やそのバージョン、API を通じて提供される情報とその重要度、リスク軽減策の実施状況など、通常のシステムにおけるインベントリと同様の管理が必要となる。

外部の API の管理のリスクについては、金融機関による API 接続先管理の一環として対応することが想定される。

補論 2. 主な脅威の概要

(1) アクセス・トークンの奪取

① アクセス・トークンの推測

攻撃者が、自分のリソースにアクセスするためのアクセス・トークンを自分の端末などから入手したうえで、それを分析して顧客のリソースにアクセスするためのアクセス・トークンを推定する。サーバ・アプリの場合には、クライアントのサーバ（アクセス・トークンを格納）などから不正に入手する。

② 通信経路上での盗聴

攻撃者が、クライアントと認可サーバとの間の通信、または、クライアントとリソース・サーバとの間の通信を盗聴・解析してアクセス・トークンを入手する。

③ クライアントからの奪取

攻撃者が、クライアントや端末・サーバの脆弱性を悪用してそれらの管理者権限を入手し、それを用いてアクセス・トークンやリフレッシュ・トークンをクライアントから奪取する。

④ 転送機能の悪用

クライアントが特定の URL にアクセス・トークンを自動的に転送する機能（オープン・リダイレクト）を有効化しているケースにおいて、攻撃者が、リダイレクト先の URL を自分のサーバのものに改変し、アクセス・トークンを自分のサーバに転送させる。

⑤ 中継サーバの自動接続機能の悪用

顧客の端末が認可サーバなどとの通信に中継サーバ（プロキシ）を使用しているケースにおいて、攻撃者が、プロキシの自動設定ファイルを悪用して認可コードやアクセス・トークンをプロキシから自分のサーバに送信させる。

⑥ 認可リクエストの改変

攻撃者が、認可リクエストにおいて、認可サーバやリソース・サーバの IP アドレスを自分のサーバのものに変更し、認可コードやアクセス・トークンをクライアントから攻撃者のサーバに送信させる。

(2) セッションの奪取

⑦ 不正なアプリの使用

攻撃者が、不正なネイティブ・アプリを顧客の端末にインストールさせ、ブラウザとクライアントの間のセッションに中間者として侵入し、認可コードや顧客の口座の取引履歴を奪取する。

⑧ セッション管理用パラメータの奪取

攻撃者が、クライアントやそれが動作する端末の管理者権限を奪取し、それを用いてセッション管理用のパラメータを入手する。入手したパラメータによって正規のセッションを引き継ぎ、顧客の口座の取引履歴を奪取する。

(3) 顧客の誘導

⑨ 攻撃者のリソースの偽装

攻撃者が、フィッシングなどによって、攻撃者の口座の取引履歴へのアクセス先に顧客を誘導し、顧客の口座の取引履歴を入力させる。また、複数の口座の取引履歴を同期させることができる場合には、顧客の口座の取引履歴と攻撃者の口座の取引履歴を同期させるように顧客を誘導し、攻撃者は同期後に顧客の口座の取引履歴を入手する。

⑩ セッション管理用パラメータの悪用

攻撃者が、クライアントやそれが動作する端末の管理者権限を奪取してセッション管理用のパラメータを改変し、攻撃者の口座の取引履歴のアクセス先に顧客を誘導する。そのうえで、顧客に自分の口座の取引履歴を入力させる。顧客が口座の取引履歴を入力したら、攻撃者はそれにアクセスする。また、複数の口座の取引履歴を同期させることができる場合には、顧客の口座の取引履歴と攻撃者の口座の取引履歴を同期させるように顧客を誘導し、同期後に顧客の口座の取引履歴を入手する。

(4) 顧客のクレデンシャルの奪取

⑪ 不正なサイトへのリダイレクト

攻撃者が、フィッシング・サイトの URL をクライアントのアクセス先として認可サーバに登録し、フィッシング・メールなどによって不正な認可リクエストを顧客に開始させる。それを受信した認可サーバは、エラー・

メッセージなどをブラウザに返信するとともに、ブラウザを登録済の URL（フィッシング・サイト）にリダイレクトさせる。顧客がそのサイト上で ID やパスワードを入力すると、攻撃者がそれらを用いて顧客になりすまし、正規の認可プロトコルを経て顧客の口座の取引履歴を入手する。

電子決済手段の法形式とその移転

神作裕之（かんさくひろゆき）

要　旨

本稿では、2022 年「資金決済に関する法律」の改正により創設された電子決済手段（いわゆるステーブルコイン）の法形式と移転について検討する。電子決済手段は、実際には、資金移動業者を発行者とする P2P（Peer-to-Peer）型の 1 号電子決済手段、または信託銀行・信託会社を発行者とする P2P 型もしくは非 P2P 型の 3 号電子決済手段として利用される可能性が高い。これらの電子決済手段が、決済手段として十全に機能するには、その移転が法的に確実・安全かつ簡易迅速になされるべきことから、要求払預金を決済手段とする振込等につき判例・有力説の採用する、いわゆる消滅・発生構成を適用することの妥当性を検討する。当該構成では、資金移動の指図の効力がその原因となる法律関係の影響を受けない点は妥当であるが、意思表示に瑕疵のある指図や無権限者による指図に基づく資金移動が有効とされる理由は明らかでない。P2P 型の電子決済手段について、決済システムにおける指図行為自体の無因性・抽象性・文言性の範囲を検討する必要があり、類似点を有する支払委託有価証券に関する議論を参考に、消滅・発生構成の射程を限定することが考えられる。電子決済手段は、発行者を中心とした利害関係者によりコントロールされる可能性があり、将来的には、支配（コントロール）概念を中核とする権利の発生・移転・消滅・善意取得・抗弁の制限等に係る民事法上の規律を、立法により整備することが期待される。

キーワード：　電子決済手段、預金、資金移動業、電子マネー、ステーブルコイン、暗号資産、有価証券

本稿は、筆者が日本銀行金融研究所客員研究員の期間に行った研究をまとめたものである。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者個人に属する。

神作裕之　学習院大学法学部教授（E-mail: hiroyuki.kansaku@gakushuin.ac.jp）

1. はじめに

2022年の「安定的かつ効率的な資金決済制度の構築を図るための資金決済に関する法律等の一部を改正する法律」（令和4年法律第61号）に基づく資金決済に関する法律（以下、「資金決済法」という。）の改正によって、主としてパーミッションレス型ブロックチェーン技術等のトークン化技術の利用を前提にしたP2P（Peer-to-Peer）型を念頭に置いた電子決済手段について、新たな規制が導入された。2022年改正資金決済法は、ステーブルコインと呼ばれるものの一部を電子決済手段として4類型に分けて定義し、その発行・償還業務を為替取引と把握する。そのうえで、電子決済手段の発行・償還および仲介業務を軸に据えて新たな規制を導入し、電子決済手段の仲介を業とする電子決済手段等取引業者（第1号取引業務～第3号取引業務）に業規制を適用することとした。他方、従来、特段の法規制が存在しなかった、銀行預金または資金移動業マネーを用いた電子マネーの仲介を業とする者を、前者すなわち銀行預金電子マネーについては銀行法改正により電子決済等取扱業者として、後者すなわち資金移動業電子マネーについては資金決済法改正により電子決済手段等取引業者（第4号取引業務）として、新たに規制することにした。

本稿では、電子決済手段の定義と発行者に係る監督法上の規制について概観したうえで、現実的に利用される可能性が高いと考えられるタイプの電子決済手段、すなわち資金移動業者による1号電子決済手段と信託銀行・信託会社による3号電子決済手段（特定信託受益権）を中心に、その民事法上の性質について、既存の決済手段との比較等により若干の検討を行う。どのような発行者がどのような法形式によって電子決済手段を発行するかによって、その発生や移転等をめぐる法律構成が異なりうるからである。

2. 要求払銀行預金を用いた決済システム

(1) 日銀ネット・全銀システムによる複層的な決済システム

決済手段に求められる要素は、さまざまであるが、決済機能は、通貨（マネー）の機能である①価値尺度機能、②価値保蔵機能と並ぶ重要な機能である。決済とは金銭債務を消滅させる行為である。金銭債務の弁済により、その債務に係る債権は

消滅し（民法 473 条）、決済がなされることになる。金銭債務は、通貨で弁済することができるほか（民法 402 条）、相殺、更改や混同等により消滅する。

資金決済の多くの部分は、銀行に対する要求払預金の移動すなわち電子資金移動によってなされている[1]。平成 29 年民法改正により、債権者の預金の口座に対する払込みによって弁済する場合には、債権者が当該預金に係る債権の債務者に対しその払込みに係る金額の払戻請求権を取得した時に、弁済の効力が生じるものとされた（民法 477 条）。振込による金銭債務の消滅が弁済か代物弁済かについては争いがあったが、平成 29 年民法改正は、弁済として整理[2] するとともに[3]、債務の消滅時期が、払い込まれた金額について「払戻しを請求する権利を取得した時」であることを明確化した[4]。振込による弁済という現代社会における重要な仕組みついて、その法的性質と債務消滅時期を明確化し、振込に関する基本的な規律を示したものと説明される[5]。振込により受取人が自己の預金口座に払い込まれた金額の払戻請求権を取得した時点で弁済の効力が生じるものとして、いわゆる決済のファイナリティーが確保された。

要求払預金が決済手段として決済機能を営むのは、銀行間の為替取引が最終的には日銀マネーといった法貨の引渡請求権に結び付いた全銀システムと日本銀行金融ネットワークシステム（以下、「日銀ネット」という。）の二重の決済システムを通じて、安全、確実、かつ効率的に資金決済がなされていることに裏付けられているためであると解される。

送金人 A が受取人 B に振込により金銭債務 100 万円を弁済しようとしているとする。A と B の預金口座が同一の銀行である甲銀行に開設されている場合には、甲銀行が、A の口座残高を 100 万円減少させ、B の口座残高を 100 万円増加させることによって、資金移動が完了する。口座における記帳の書換えによって資金移動がきわめて効率的かつ迅速に実行される。決済システムが甲銀行内部で完結されているためである。

これに対し、送金人と受取人の銀行口座が異なる銀行に開設されている場合には、仕組みは複雑になり、関係当事者が増加する。甲銀行に預金口座をもつ X が乙銀行に口座をもつ受取人 Y に対して 100 万円の振込を行う場合、X から振込委

1 岩原［2003］30〜37、605 頁参照。

2 大村ほか［2018］314 頁〔加毛明〕。代物弁済の場合と異なり、弁済については、債権者の承諾を要しない（民法 482 条）。

3 銀行振出の自己宛小切手（預手）の交付の提供について、最判昭和 37 年 9 月 21 日民集 16 巻 9 号 2041 頁は、金銭債務の弁済の提供を認めた。その理由として、同最判は、預手は取引界において通常その支払が確実なものとして現金と同様に取り扱われているものであり、特段の事情がない限り、その提供をもって債務の本旨に従ってなされた履行の提供と認めるのが相当であると述べる。

4 なお、他行間振込を例にとると、受取人の被仕向銀行に対する預金債権の成立時がいつかについて、民法は規定を置いておらず、解釈論に委ねられている。被仕向銀行が受取人に入金記帳をした時点とする見解が有力であるが、それ以前に成立することもありうるとする見解もある。

5 中田［2020］374 頁。

託を受けた仕向銀行である甲銀行は被仕向銀行である乙銀行に対して 100 万円の債務を負い、甲乙銀行間における資金決済は、為替決済（資金清算）の仕組みを用いて、1 日 1 回、銀行が日本銀行に開設している日銀当座預金口座の残高を増減させることによって決済される[6]。実際には、多数の銀行相互間で網の目のように為替決済が行われるが、決済リスクを削減し決済を効率化するために、全国銀行資金決済ネットワーク（以下、「全銀ネット」という。）が資金清算機関（セントラル・カウンターパーティ）として[7]、為替取引ごとに送金人 X が口座を開設している全銀システムの参加銀行である甲銀行の債務を引き受ける一方、受取人 Y が口座を開設している全銀システムの参加銀行である乙銀行が有する債権を取得することにより[8]、全銀ネットと各参加銀行の間における決済関係に置きなおし、差引計算を行ったうえで残高だけを日銀ネットを通じて決済する[9]。

日銀ネットの 1 つである日銀ネット当預系により、金融機関等が日本銀行に開設している日本銀行当座預金の間の資金の振替によって、全国銀行内国為替制度を含む各種の民間資金決済システム等にかかわる資金決済が行われる[10]。日本銀行と日

6 1 億円以上の為替取引は、それぞれの為替通知ごとに、仕向金融機関と被仕向金融機関の間で資金決済を行い、被仕向金融機関に為替通知が送信される。各取引の資金決済が完了するまでの間、為替通知は、全銀センターに保留され、為替通知ごとに、日銀ネットの流動性節約機能付 RTGS（即時グロス決済）によって決済される。

7 全銀ネットは、資金決済法に基づき資金清算業を営む一般社団法人である。

8 全銀システムには、清算参加者としての参加と、代行決済委託金融機関としての参加の 2 つの参加類型がある。清算参加者は、日本銀行に有する自身の当座勘定により決済するのに対し、代行決済委託金融機関は、日本銀行に当座預金を保有せず、決済尻の資金清算を他の清算参加者に委託することにより全銀システムに参加する。日本銀行における代行決済受託金融機関の当座勘定により決済し、代行決済委託金融機関間で別途清算がなされる。清算参加者になるためには、清算資格の取得が必要であり、為替決済を行う店舗における日本銀行との当座勘定取引の承認等が要件になる。また、全銀システムへの接続に当たって必要な条件を満たさなければならない。他方、代行決済委託金融機関として参加するためには、清算参加者 1 行だけを代行決済受託金融機関として指定しなければならない。全銀システムへの接続に当たって必要な条件（金融機関コードの付与、取扱店の登録等）を満たす必要があることは、清算参加者の場合と異ならない。

9 2020 年 10 月、全銀ネットは、全銀システムへの参加資格を従来の預金取扱金融機関だけでなく新たに資金移動業者に開放した。一般社団法人全国銀行資金決済ネットワーク［2022］参照。全銀システムに参加する資金移動業者の監督に際する留意事項については、金融庁「事務ガイドライン第三分冊：金融会社関係 14 資金移動業者関係」II-2-3-4 参照。

10 日本銀行は、日本銀行法 33 条 1 項に定める通常業務の 1 つとして、金融機関等から当座預金を受け入れ、その当座預金の振替や入金・引落しによって資金の決済を行う仕組みを運営している。日本銀行は、日本銀行法 39 条 1 項に従い、内閣総理大臣（金融庁長官に権限委任）および財務大臣から認可を得てその支払指図を電子的に送信する日銀ネットを提供している。この業務は、「銀行その他の金融機関の間で行われる資金決済の円滑の確保を図り、もって信用秩序の維持に資する」（同法 1 条 2 項）ためのものである。日銀ネットの参加者は、資金決済の主要な担い手である金融機関等（銀行、協同組織金融機関の中央機関、信用金庫、資金清算機関等）のうち「日本銀行の当座預金取引または貸出取引の相手方に関する選定基準」に合致した者であって、日本銀行と日銀当座預金締結を締結した者である。日本銀行と参加者の法律関係は、当座勘定規定や、日銀ネット当預系の利用に関する規則類で規定している各種規定によって規律されている。2023 年 3 月末現在、取引先金融機関等は 484 機関である。なお、日本銀行は、日銀ネットを通じた資金決済を円滑に処理するため、取引先金

銀ネットに参加する金融機関等との間、および、全銀ネットと全銀システムに参加する金融機関等との間は、いずれも通信回線によって接続されており、入力されたデータはオンライン処理される。

このように、送金人と受取人の間では、銀行預金債権をもって、また、銀行間の内国為替決済は、日本銀行マネーをもって決済され、最終的には法貨の引渡請求権が裏付けになっているという強固で複層的な決済システムから構築されている。そして、日本銀行が定める当座勘定規定において、入金の時期は、日本銀行がその決済を確認し、当座勘定元帳に記帳をした時と規定されており（日本銀行当座勘定規定3条）、日銀ネットを通じた資金決済のファイナリティ（債務の履行）が確保されている。

(2) 決済システムが機能するための条件

ある決済手段が決済手段としての機能を発揮するためには、当該決済システムの内部において、そしてそれが上位の決済システムに接続している場合にはその上位の決済システムとの関係において、決済手段が価値尺度としての安定性と決済手段としての規格性・等価性を有していることが求められる。送金人と受取人のそれぞれの取引銀行が異なっていても、預金債権は規格性・等価性を有している必要があり、かつ、当該決済手段が預金債権のような無体物である場合には、システム内での流動性を確保する一方で、システム外での移転を防止し、システムとしての完全性・完結性を維持する必要がある。銀行預金と全銀システムおよび日銀ネットは、それらの要件を十分に満たしており、それが前述した平成29年民法改正の法的評価すなわち銀行預金の決済手段としての法的承認の背景になったと考えられる。銀行当座預金も日銀当座預金も日銀マネーによる決済システムであり、預金者には法貨の引渡請求権が認められる。銀行預金の価値の安定性やその等価性・均一性の確保のために、銀行法をはじめとする各種の規制監督のほか、資金決済システムの複層的なレベルのそれぞれにおいて参加者の資格を制限していることに加え、参加金融機関等に係るリスクについてさまざまな自律的なコントロールがなされている[11]。さらに、銀行破綻の場合における決済性預金についての全額保護といったセ

融機関等に対して、当日の終業時を返済期限とする当座貸越（日中当座貸越）の形態で日中流動性を供与しており、取引先金融機関等は、予め差し入れられた担保の評価額の範囲内で、日本銀行から、無利息で当座貸越の形態による資金借入を行うことができる。以上につき、日本銀行［2023］6頁。

11 例えば、日本銀行は、取引先金融機関等に係るリスク（信用リスク、資金流動性リスクおよびオペレーショナルリスク等）を管理・抑制するため、取引先金融機関等の選定基準を公表しているほか、取引先金融機関等選定時の審査、取引先金融機関等に対する考査・モニタリング等、取引先金融機関等であるFMIに対するオーバーサイトの実施、決済システムレポートの公表を通じて、取引先金融機関等に係るリスクとそれへの対応策に関する情報提供を行っている。日本銀行［2023］24頁。

イフティ・ネットが整備されている。日本銀行は日本銀行法に基づく規制監督を受けるほか、株式会社である銀行が作成する銀行口座の帳簿は商業帳簿に該当し、商法上の規制に服するほか、監督法上の規制にも服し、帳簿の記載の正確性や正当性が保持されている。

民間銀行の発行する銀行券が次第に駆逐され、銀行預金による決済に収れん・一元化してきたという歴史的経過の中で、P2P 型の電子決済手段について、最終的には預金制度に結び付くように制度が構築されたことは（3 節（3）ないし（7）参照）、慎重かつ適切な立法態度であったと思われる。さらに、決済手段として用いられるためには、決済手段が法的に確実に移転するとともに、基本的に無効・取消の主張や抗弁が決済手段としての機能を保持するのに必要な範囲で制限されていることが望ましい。後述するように、銀行預金については消滅・発生構成がとられている。その法的効果は、いわゆる「占有＝所有」の理論[12] が適用される金銭を決済手段として用いる場合にかなり接近するものになっている。銀行預金による資金決済の動的安全への配慮は、有価証券としての決済手段である小切手や為替手形よりも強固であるといえる。

電子決済手段について、業法・監督法上は、2022 年資金決済法改正により、3 節に述べるような緻密な規制が整備されたといえるのに対し、とくに P2P 型の電子決済手段の民事法上の規律については、解釈論・立法論とも一部の例外を除き、議論が低調であると思われる。諸外国では、立法論を中心に、P2P 型のステーブルコインやより一般的にデジタル資産またはコントロール可能な電子記録（controllable electronic record）について民事立法の動きが顕著であることに比べると、日本における業法・監督法と民事法の格差はひときわ目立つ。

3. 電子決済手段

(1) 類型

資金決済法は、1 号電子決済手段から 4 号電子決済手段まで、4 類型の電子決済手段を認めている（同法 2 条 5 項 1〜4 号）。基本的に、電子決済手段は、パーミッションレス型のブロックチェーン技術等を用いて移転され、中央管理者が当該移転

12 判例によれば、金銭は通常物としての個性を有せず、単なる価値そのものと考えるべきであり、価値は金銭の所在に随伴するものであるから、金銭の所有権は特段の事情のないかぎり金銭の占有の移転と共に移転するものとされる（最判昭和 29 年 11 月 5 日刑集 8 巻 11 号 1675 頁）。金銭は、通貨媒体としての有体物それ自体が価値的権能すなわち金銭債務を弁済により消滅させる権能を有しており、財産的価値が有体物に表章されている有価証券とは異なる。

に関与しない P2P 型を想定している。もっとも、例外もあり、3 号電子決済手段すなわち特定信託受益権を受益証券発行信託として発行し、受益権原簿制度を利用する場合には、電子決済手段の発行者である受託者が受益権原簿を作成・管理する非 P2P 型の存在が想定されている。もっとも、P2P 型といっても、自らブロックチェーンに参加して電子決済手段を決済や移転に用いる場合のほか、現実的には、管理業務を行う電子決済手段等取引業者を介してそれを使用・処分する場合が多いと推測される。電子決済手段については、その導入にあわせて電子決済手段の交換等または電子決済手段の管理を業として行うことを電子決済手段等取引業と定義したうえで（同条 10 項）、管理も含めて電子決済手段の仲介に関する業規制が整備された。

以下では、1 号電子決済手段から 4 号電子決済手段の 4 類型の発行者になりうる者は誰であるかを明確にしたうえで、実際に発行される可能性が高い電子決済手段に重点を置いて、その定義および法形式について、検討することにする。

(2) 発行者

イ. 銀行

（イ） 1 号電子決済手段の発行

銀行は、その固有業務として為替取引を営むことができる（銀行法 10 条 1 項 3 号）。そのため、銀行が為替取引と整理されている 1 号電子決済手段の発行・償還を行うことは、本来的には可能である。しかし、当面、銀行が 1 号電子決済手段を発行することは想定されていない。監督指針においても、銀行が電子決済手段を発行することを想定した記載は一切ない。

銀行が 1 号電子決済手段を発行することが想定されていない理由は、次のような懸念ないし問題点が指摘されているからである。第 1 に、銀行の業務の健全かつ適切な運営の観点から、銀行がステーブルコインに関与することに懸念がしめされている[13]。むしろ銀行には、不適切な電子決済手段を発行しないための体制整備を行う組織上の義務が課されている（銀行法施行規則 13 条の 6 の 9）。第 2 に、銀行による 1 号電子決済手段の発行が、預金債務であるのか、為替取引に用いるために受け入れた資金であって利用者が 1 号電子決済手段の発行見合金を預託し、同額の電子決済手段が発行された時点で、利用者に対し当該為替取引に関する債務（未達債務）を負担するものであるのか、基準が不明確であり、どちらに当たるかによって

13 金融庁「令和 4 年資金決済法等改正に係る政令・内閣府令案等に関するパブリックコメントの結果等について」（2023 年 5 月 26 日）（別紙 1）2〜3 頁（No.8）参照（https://www.fsa.go.jp/news/r4/sonota/20230526/01.pdf）。

預金保険法上の取扱いに差異が生じる可能性がある[14]。すなわち、仮に預金債務であるとすると預金保険の対象になるものの、実務的に名寄せを行うことが困難であり実効性を欠く。これに対し、仮に未達債務であるとすると、預金保険のカバーする対象である「特定決済債務」に該当するかどうかが問題になるが、結論が不明である。なお、銀行には資金移動業者のような資産保全義務は課されていない。第3に、P2P型電子決済手段については、マネー・ロンダリングおよびテロ資金供与に用いられるリスクが高く[15]、それにより銀行のレピュテーショナル・リスクが発現するおそれが大きい。

（ロ） 非P2P型の電子マネーの発行と電子決済等取扱業

もっとも、銀行が非P2P型の電子マネーを発行することは可能であり、すでにそのような電子マネーは実際に利用されている。2022年銀行法改正により、そのような非P2P型の電子マネーの仲介等を業とする者について新たに電子決済等取扱業規制が導入された。暗号資産や電子決済手段と同様、非P2P型の電子マネーを銀行が預金により発行する場合にも、仲介機能を別の業者が営むいわゆる発行と仲介の分離が進展することが想定され、仲介業規制の必要性が認識されたためである[16]。

電子決済等取扱業とは、次の2つの行為から構成される。第1は、銀行の委託を受けて、当該銀行に代わってその銀行に預金口座を開設している預金者との間で次の①または②のいずれかを電子情報処理組織を使用する方法により行うことを合意し、かつ、その合意に基づいて預金債権の額を増加または減少させるという行為である。①当該預金口座に係る資金を移動させ、当該資金の額に相当する預金債権の額を減少させる。②為替取引により受け取った資金の額に相当する預金債権の額を増加させる。以上の①または②は、後述する消滅・発生構成に親和的な法律構成である。電子決済等取扱業者は、送金人からの支払指図を承諾する権限を銀行から付与されて上記①または②の行為を行い、電子マネーを移転させるものと整理されている[17]。電子決済等取扱業者が銀行の代理人として送金人からの支払指図を受け、それに対し承諾をしたうえで、帳簿の記帳を行う場合には、利用者の電子決済等取扱業者に対する権利の内容は、発行者に対して有する権利と同一になり、権利

14 市古［2024］266～267頁。
15 FATF [2020] pp. 7–9.
16 金融審議会［2022］16頁。
17 金融審議会［2022］23頁において、「銀行から代理権を付与された仲介者が、個々の利用者の持分を管理し、振り替える仕組み（発行者である銀行は総額のみを管理）」として電子決済等取扱業に相当する業務の規制が構想されていた。電子決済等取扱業者は、銀行に代わって、利用者との合意に基づき利用者からなされた指図を承諾し、それを自らが管理する口座帳簿に反映させる権限を有するものと整理されていると考えられる。

内容の同一性が確保される[18]。決済手段としての等価性・均一性が確保されることになろう。電子決済等取扱業の第 2 の行為は、第 1 の行為に関して、委託銀行のために預金の受入れを内容とする契約の締結の媒介を行うことである（銀行法 2 条 17 項）。

上述した電子決済等取扱業の定義から明らかなように、銀行による電子マネーは、銀行預金口座の存在を前提にし、銀行（正確には、銀行から委託を受けた電子決済等取扱業者）が当該口座の預金債権の額を減少または増加させることによってその移動を行うものであり、非 P2P 型である。

ロ．前払式支払手段発行者

次に、前払式支払手段発行者は、1 号電子決済手段を発行できるのであろうか。前払式支払手段発行者は P2P 型の前払式支払手段を発行することができ、現に利用されているが、そのような前払式支払手段は電子決済手段に該当するものとされる（資金決済法 2 条 5 項 1 号、取引業府令 2 条 2 項）[19]。ところが、2022 年資金決済法改正により、前払式支払手段発行者に対し、P2P 型のプリペイド・カードの発行をしないための措置を講じるべき組織上の義務が課されることになった（前払式府令 23 条の 3 第 3 号）。同様に、仲介者にも電子決済手段に該当する前払式支払手段を取り扱わないための措置を講じるべき組織上の義務が課されている[20]。他方、電子移転可能型の前払式支払手段については[21]、発行者の関与を必須にして非 P2P 型のものに限定する一方、そのような前払式支払手段は電子決済手段には該当しないものとされた（本節（3）ニ．参照）。

P2P 型の電子移転可能型の前払式支払手段は電子決済手段には該当しないこととされた。その理由は、第 1 に、前払式支払手段については払戻しが原則として禁止されており（資金決済法 20 条 5 項）、利用者の償還請求権が確保されていないため、発行者が額面額での償還する義務を負う 1 号電子決済手段には該当しないからである。なお、前払式支払手段には、円で表示される金額表示型と特定の物品等の

18 デジタルマネーの私法上の性質を巡る法律問題研究会［2024］23 頁。

19 前払式支払手段のうち、電子移転可能型のものについては、電子データであり、かつ P2P 型の移転が可能であるが、1 号電子決済手段から除外されている。後掲脚注 21 およびそれに対応する本文参照。

20 金融庁「事務ガイドライン第三分冊：金融会社関係 17 電子決済手段等取引業者関係」I-1-2-3 ④（注）参照。

21 電子移転可能型の前払式支払手段とは、前払式支払手段ごとにその内容の記録を行う口座であって、当該口座に前払式支払手段の内容が記録されることにより、当該前払式支払手段を代価の弁済のために使用することまたは物品等の給付・役務の提供を請求することが可能になる口座に未使用残高が記録されるものである（前払式府令 1 条 3 項 6 号・5 条の 3 第 2 項）。このように、電子移転可能型支払手段は、口座とその口座に未使用残高を記録することが求められており、非 P2P 型に限定されている。なお、電子移転可能型前払式支払手段は、①残高譲渡型前払式支払手段、②番号通知型前払式支払手段、および、③国際ブランド・プリペイド・カードの 3 種類に分かれる（前払式府令 1 条 3 項 4、5 号、23 条の 3 第 2 号ロ）。

購入に使用できる数量表示型とがあるが、数量表示型の場合には原則として通貨建資産には該当せず、そのような前払式支払手段は電子的移転が可能であっても通貨建資産であることを要件とする 1 号電子決済手段には該当しえない。第 2 に、実質的にも、前払式支払手段の発行者は、基準日未使用残高の半額保全しか義務付けられておらず（資金決済法 14 条 1 項）、前払式支払手段発行者が破綻した場合における利用者保護が十分でないからである[22]。

ハ. 資金移動業者

（イ） 1 号電子決済手段の発行

1 号電子決済手段として、当面、想定されているのは、為替取引を業とする資金移動業者が、利用者との間に締結した契約に基づく為替取引に係る債務（未達債務）をもって、P2P 型の電子決済手段を発行する場合である。さらに、事実上は、第二種資金移動業者（送金上限額 100 万円）によって取り扱われることになると推察される。というのは、第一種資金移動業者は、厳格な滞留規制の適用を受け（資金決済法 51 条の 2）、具体的な送金指図なく利用者資金を受け入れることができず（同条 1 項）、また、第三種資金移動業者は、送金上限が 5 万円であるうえ、利用者資金の厳格な受入上限（1 人当たり 5 万円以下）の適用を受け、第二種資金移動業者に比較して事業の自由度が低いためである[23]。これに対し、第二種資金移動業者は、前述したように送金上限額 100 万円の制約を受けるものの、第一種資金移動業者に比べると緩やかな滞留規制等が適用されるに過ぎない。

そもそも、委任契約に基づく為替取引に係る未達債務が、預金債務と同様に決済手段になりうるのはなぜであろうか。それは、未達債務が、預金と同様にその安全性と等価性・均一性が確保されているためであると考えられる。すなわち第 1 に、資金移動業者は「未達債務の額」について資産保全義務を負う（資金決済法 43 条 1、2 項）。これにより、為替取引に係る債務の全額について保全が図られることになる。第 2 に、仮に資金移動業者が破綻しても、未達債務に係る債権者は、保全資産（履行保証金）を引き当てとして他の債権者に先だって優先的に弁済を受ける権利を有する（同法 59 条 1 項）[24]。このように、前述した預金債務とは異なる方法に

22 もっとも、P2P 型の電子移転が可能な前払式支払手段については、電子決済手段に該当する旨の規定（取引業府令 2 条 2 項）は、改正法施行日である 2023 年 6 月 1 日から起算して 2 年を経過するまでの間は適用されないとする経過規定が設けられている（取引業府令附則 2 条）。

23 市古［2024］255 頁。

24 この優先弁済権は、保全資産である履行保証金を引当てとして実現される。その法的性質については、特別の先取特権とする説と利用者の履行保証金に対する還付請求権とする説がある。特別先取特権であるとする説として、高橋［2023］190～191 頁、還付請求権とする説として丸橋・松嶋［2019］126 頁、市古［2024］85 頁。なお、資金移動業者の未達債務に係る債権者と同様の優先的弁済を受ける権利は、暗号資産交換業者に対して預託者が有する預託暗号資産の移転を目的とする債権についても認められている（資金決済法 63 条の 19 の 2 第 1 項）。この権利については、動産先取特権の第三取得者に対する追求効を否定する民法 333 条が準用されているほか（資金決済法 63 条の 19 の

よって、資金移動業者の未達債務の安全性が確保され、単純な金銭債権である未達債務であることからその等価性・均一性が確保されているといえる。

さらに、異なる資金移動業者のもとで口座を開設している者の間で資金移動業電子マネーの送金が行われる場合には、資金移動業者は、清算参加者または代行決済委託金融機関として全銀システムに参加し、清算参加者は、日本銀行に有する自身の当座勘定により、代行決済委託金融機関は他の清算参加者に委託することにより日銀ネットを通じた資金決済がなされる。この場合には、前述したように、最終的には法貨を発行している日本銀行の内部で決済される日銀ネットに連結した全銀システムという複層的な決済システムに資金移動業者が直接または間接に参加することにより、資金移動業電子マネーが決済手段として効率的かつ安全に機能するような各種手当が講じられている。

（ロ） 電子決済手段等取引業

P2P 型であり電子移転可能型の 1 号電子決済手段については、発行者と仲介者が分離し、発行・償還機能と仲介・媒介・保管機能がそれぞれ別の業者によって担われることが想定される。電子決済手段の決済機能が確実に履行されるようにするとともに、仲介業者の破綻リスクから利用者を保護する必要性が高い。そこで、2022 年資金決済法改正により、電子決済手段の仲介業規制が導入されることになった。

1 号電子決済手段に係る電子決済手段等取引業については、第 1 号取引業務から第 3 号取引業務に係る規定が適用される可能性があるが、これらは 2 つに類型化することができる。第 1 は、電子決済手段の交換等を業とすることであり、具体的には、①電子決済手段の売買または他の電子決済手段との交換（資金決済法 2 条 10 項 1 号）、または、②①の媒介・取次ぎ・代理（同項 2 号）を業とする。第 2 は、電子決済手段の管理であり、他人のために電子決済手段を管理することである（同項 3 号）。

（ハ） 業規制の概要

電子決済手段の定義は、通貨建資産かどうかという点を除いて、暗号資産の定義に類似しており、電子決済手段等取引業者に対する規制も、暗号資産交換業者に対する規制と類似している。その概要については本稿では省略するが、預託金銭および預託電子決済手段の分別管理義務、情報の安全管理および委託先管理、説明義務、情報提供義務、利用者保護を図るための措置、電子決済手段の発行者との契約締結義務、苦情処理措置、紛争解決措置、帳簿書類の作成および保存、事業報告書および利用者財産の管理に関する報告書の作成義務、ならびに信用取引を行う場合

2 第 2 項）、前払式支払手段発行者や資金移動業者については、優先弁済権の引当てとなる保全資産について当局が主導して債権者に対する配当表の作成等が行われるものとされているのに対し、暗号資産の場合にはどのように優先弁済権を実行するかについて、法令に定めがない等の違いがある。

のレバレッジ規制およびロスカット・ルール等が課されているほか、犯罪による収益の移転防止に関する法律（平成 19 年法律第 22 号）における特定事業者とされており、取引時確認義務やトラベル・ルールの適用等、同法に基づく規制に服する。

現実に発行が想定される第二種資金移動業者による 1 号電子決済手段および資金移動業者による非 P2P 型の電子マネー（本節（2）ハ.（ニ）参照）を電子決済手段等取引業者に取り扱わせる場合には、それらを発行または仲介する資金移動業者に対し、送金上限規制および滞留規制等が課されている。資金移動業者が自らそれらの移転・管理等の仲介を行わず、電子決済手段等取引業者に委託する場合には、発行者に課される送金上限規制および滞留規制等を電子決済手段等取引業者が遵守できるように態勢を整備させる義務を負うものとされている。

（ニ） 資金移動業者による非 P2P 型の電子マネーの発行

a. 非 P2P 型の電子マネー

資金移動業者が非 P2P 型の電子マネーを発行することは可能であり、すでにそのような電子マネーは実際に利用されている。本節（2）ハ.（イ）に述べたように、資金移動業者が利用者に対して負っている為替取引に係る債務すなわち未達債務は、預金と同様にその安全性と等価性・均一性が確保されているため、決済手段としての適格性を有している。

資金移動業者の発行する 1 号電子決済手段と非 P2P 型の資金移動業電子マネーとは、いずれも資金移動業者が発行するものであって、利用者との間の契約に基づいて利用者から出捐された為替取引に関する債務に係る債権の移転により資金決済を行うものである点で、共通している。しかし、両者には以下の相違点があると指摘される。すなわち、非 P2P 型の資金移動業電子マネーの場合には、委任事務の遂行を求める委託者の権利すなわち資金移動業電子マネーの残高を他の利用者に移転し、移転を受けた者が当該保有残高に相当する額の金銭の払戻請求権を取得する。そのためには送金人から移転指図を受けた資金移動業者がその指図を承諾し帳簿に記帳することが要件になる。これに対し、P2P 型の 1 号電子決済手段については、発行者が関与しないで電子決済手段が移転される[25]。1 号電子決済手段の法形式については、節を改めて検討するが、資金移動業者の未達債務については、預金債務と同様に消滅・発生構成をとる余地があると解されている[26]。その場合には、冒頭に述べたように、実質的には、抗弁事由や意思表示の瑕疵からの独立性が認められ

25 市古［2024］219～220 頁。

26 加毛教授は、資金移動業マネーについて、預金債権の譲渡制限に係る民法 466 条の 5 の類推適用を認めたうえで、銀行振込の場合と同様に、支払人、受取人、資金移動業者の三者合意を要しないから更改ではなく、決済手段としての機能等から資金移動業者の管理する口座を基準にして第三者との関係を規律することの合理性が認められるとして、一定の留保を付しながらも消滅・発生構成を肯定する。加毛［2023］261～263、266、270～271 頁、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］16～17 頁。

たり、善意か悪意かを問わず受取人が保護されたりする等、債権譲渡や更改の場合には認められない、あるいは認めることのむずかしい法的効果が認められることになり、決済手段としての高い適格性をもつに至る。

b. 第 4 号取引業務

資金移動業者が、従前から行われてきた資金移動業マネーを用いた非 P2P 型の電子マネーを発行した場合についても、前述した預金を用いた電子マネーについてと同様、消滅・発生構成に整合的な第 4 号取引業務に係る仲介業規制が新設された。

第 4 号取引業務とは、資金移動業者の委託を受けて、その資金移動業者に代わって利用者との間で次の①または②のいずれかを電子情報処理組織を使用する方法により行うことに合意し、かつ、その合意に基づいて為替取引に関する債務（未達債務）に係る債権の額を増加または減少させることである。①当該契約に基づき資金を移動させ、当該資金の額に相当する為替取引に関する債務に係る債権の額を減少させる。②為替取引により受け取った資金の額に相当する為替取引に関する債務に係る債権の額を増加させる（資金決済法 2 条 10 項 4 号）。上記の①または②は、後述する消滅・発生構成に親和的である。第 4 号取引業務を行う電子決済手段等取引業者は、送金人からの支払指図を承諾する権限を資金移動業者から付与されて上記①または②の行為を行い、電子マネーを移転させるものと整理されている[27]。なお、ここにいう利用者とは、資金移動業者との間で為替取引を継続的にまたは反復的に行うことを内容とする契約を締結している者と定義されており（同条同項同号かっこ書き）、資金移動業者のもとで資金移動業マネーの為替取引に係る口座を開設していることを前提にしていると解される。資金移動業者による電子マネーの移動は、当該口座の残高の減少または増加によって行われ、非 P2P 型であるといえる。

(3) 1 号電子決済手段

イ. 定義

資金決済法 2 条 5 項 1 号は、1 号電子決済手段を、「物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されている通貨建資産に限り、有価証券、電子記録債権法第 2 条第 1 項に規定する電子記録債権、第 3 条第 1 項に規定する前払式支払手段その他これらに類するものとして

27 前掲脚注 17 に対応する本文参照。

内閣府令で定めるもの（流通性その他の事情を勘案して内閣府令で定めるものを除く。）を除く。）であって、 電子情報処理組織を用いて移転することができるもの」（特定信託受益権を除く。）と定義する。

ロ. 通貨建資産

この定義規定は、1 号暗号資産の定義（資金決済法 2 条 14 項 1 号）と非常によく似ている。暗号資産と異なるのは「通貨建資産」に限られている点である。暗号資産は、反対に、その定義から、本邦通貨や外国通貨とともに通貨建資産と電子決済手段を除外する。通貨建資産とは、「本邦通貨若しくは外国通貨をもって表示され、またはそれらをもって債務の履行、払戻しその他これらに準ずるものが行われることとされている資産」である（同条 7 項）。通貨建資産をもって債務の履行等が行われることとされている資産は、通貨建資産とみなされる（同条同項後段）。

通貨建資産に該当するかどうかの判断に当たり、「発行者及びその関係者と利用者との間の契約等により、発行者及びその関係者が当該利用者に対してその券面額と同額の法定通貨をもって払い戻す等の義務を負っているか」どうかがポイントになる[28]。具体的には、1 号電子決済手段から 3 号電子決済手段、預金債権、未達債務に係る債権、金額表示型の前払式支払手段、数量表示型の前払式支払手段のうち発行者または加盟店に対し通貨建資産を請求できるもの、および国債や社債等の額面での償還が約されている有価証券が、「通貨建資産」に該当するとされる[29]。

ハ. 対価性

次に、「対価を得ないで発行される財産的価値であって、当該財産的価値を発行する者又は当該発行する者が指定する者から物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために提示、交付、通知その他の方法により使用することができるもの」は電子決済手段から除外される（資金決済法 2 条 5 項 1 号、取引業府令 2 条 1 項）。無償ポイント等は、券面額と同額の法定通貨での債務の履行が約されているため、本節（3）ロ. に述べた通貨建資産には該当するものの、対価を得ないで発行されるため、電子決済手段には該当しない。対価を得ないで発行される財産的価値が電子決済手段の定義から除外されているのは、積極的な信用創造機能を否定し、その機能を決済機能に限定するためであると考えられる。

ニ. 電子移転可能型の前払式支払手段

前払式支払手段のうち、残高譲渡型や番号通知型は、電子的に移転することができるが、1 号電子決済手段から除外されている（取引業府令 2 条 2 項）。残高譲渡

28 金融庁「事務ガイドライン第三分冊：金融会社関係 17 電子決済手段等取引業者関係」I-1-1 ⑤参照。
29 市古［2024］166～167 頁。

型前払式支払手段とは、前払式支払手段のうち、利用者の指図に基づき、発行者が電子情報処理組織を用いて一般前払式支払手段記録口座[30]における未使用残高の減少・増加の記録をする方法その他の方法により、発行者が管理する仕組みに係る電子情報処理組織を用いて移転をすることができるものをいう（前払式支払手段に関する内閣府令1条3項4号）。番号通知型前払式支払手段とは、前払式支払手段のうち、電子情報処理組織を用いて第三者に通知することができる番号等であって、当該番号等の通知を受けた発行者が当該通知をした者をその保有者としてその未使用残高を一般前払式支払手段記録口座に記録するものをいう（同項5号）。

残高譲渡型や番号通知型の前払式支払手段は、いずれも一般前払式支払手段記録口座において未使用残高が記帳されるものであり、発行者の承諾その他の関与が必要である。すなわち、いずれも、電子的移転は可能であるものの、非P2P型であるという点において、電子決済手段に求められる流通性の要件を満たさないものとされた。さらに、前払式支払手段については払戻しが原則として禁止されているため通貨建資産性の要件を満たさず、基準日未使用残高の半額保全しか義務付けられていないため（資金決済法14条1項）、利用者保護が万全でないことから、発行者に係る債務の安全性や等価性・均一性に疑問があり、決済手段としての適格性に欠けることは、前述したとおりである（本節（2）ロ．参照）。

ホ．P2P型：「不特定の者」に対する使用等

1号電子決済手段は、「不特定の者」に対し使用できるP2P型であることが重要な要件の1つであると解される。事務ガイドラインにおいては、「代価の弁済のために不特定の者に対して使用することができる」かどうかを判断するに当たり、「ブロックチェーン等のネットワークを通じて不特定の者の間で移転可能な仕組みを有しているか」、「発行者と店舗等との間の契約等により、代価の弁済のために電子決済手段を使用可能な店舗等が限定されていないか」、「発行者が使用可能な店舗等を管理していないか」等をチェックするものとされている[31]。また、「不特定の者を相手方として購入及び売却を行うことができる」かどうかを判断するに当たっては、「ブロックチェーン等のネットワークを通じて不特定の者の間で移転可能な仕組みを有しているか」、「発行者による制限なく、本邦通貨又は外国通貨との交換を行うことができるか」、「本邦通貨又は外国通貨との交換市場が存在するか」等をチェックするものとされている[32]。1号電子決済手段に該当するためには、発行者が関与することなく、ブロックチェーン等の情報技術を用いてP2P型で移転できる

30 一般前払式支払手段記録口座とは、前払式支払手段記録口座その他の前払式支払手段発行者が自ら発行した前払式支払手段ごとにその内容の記録を行う口座を指す（前払式支払手段に関する内閣府令1条3項6号）。

31 金融庁「事務ガイドライン第三分冊：金融会社関係17電子決済手段等取引業者関係」I-1-1 ①。

32 金融庁「事務ガイドライン第三分冊：金融会社関係17電子決済手段等取引業者関係」I-1-1 ②。

仕組みであることが必要とされており、それが「不特定の者」に対する使用や「不特定の者」を相手方とする購入・売却が可能であることの意味するところであると解される。

(4) 1号電子決済手段の移転の仕組み

イ. 移転の仕組み

1号電子決済手段がP2P型であることから、発行者の関与なくそれが移転され決済に用いられることになる。その時、民事法上確実かつ明確に1号電子決済手段が移転して弁済の効力が生じるとともに、二重使用の問題等を回避するために当該システム外での移転を封じP2P型でありながらシステム内部の閉じた世界であることが要請される。そこで、各種ガイドラインでは、電子決済手段はブロックチェーン上の移転記録の完了時点に移転すること、および、ブロックチェーン外で電子決済手段を移転させることができないことを確保することが重視されている。例えば、これらについて、発行者がホワイトペーパー等で周知することを要するとともに、電子決済手段等取引業者は利用約款においてホワイトペーパー等の内容を自身の利用者に説明することが求められる[33]。

ロ. 法律構成

1号電子決済手段について、ブロックチェーン上の移転記録の完了時点で移転の効力が生じること、および、ブロックチェーン外で電子決済手段を移転させることができないことを、どのような法律構成によって民事法上確保することができるかが問題になる。

これまでになされている議論や実務は、次のようなものである。第1は、一定の記録によって権利者やその残高を把握・確定できるファンジブルな権利である場合には、ブロックチェーン上の記録をその効力発生要件および対抗要件と解する[34]。第2は、ブロックチェーン上の記録について、有価証券法理を適用し、トークンの移転記録を証券の交付と同視し、それによりトークン表示権利の移転の効力が発生すると解する[35]。第3は、資金移動業電子マネーの法律構成と同様に、資金移動業者の未達債務であって、債権譲渡、更改（債権者の交替）、帳簿の記載に基づく消滅・発生構成が考えられるとする[36]。第3の見解は、発行者の関与なく移転される

33 金融庁「事務ガイドライン第三分冊：金融会社関係14資金移動業者関係」II-2-2-1(9)①、金融庁「事務ガイドライン第三分冊：金融会社関係17電子決済手段等取引業者関係」I-1-2-3(1)①。
34 金融法委員会［2022］12～13頁。
35 大越［2019］106頁。
36 デジタルマネーの私法上の性質を巡る法律問題研究会［2024］12～14頁。

P2P 型の電子決済手段についても、預金や未達債務の場合と同様に、消滅・発生構成を採用する余地を否定していない点が注目される。1 号電子決済手段の移転の法律構成については、節を改めて検討する（4 節（2）参照）。

(5) 2 号電子決済手段

2 号電子決済手段とは、「不特定の者を相手方として 1 号電子決済手段と相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの」（特定信託受益権を除く。）である（資金決済法 2 条 5 項 2 号）。

2 号電子決済手段に該当するかどうか、すなわち、不特定の者を相手方として 1 号電子決済手段と相互に交換できるかどうかを判断するに当たり、「ブロックチェーン等のネットワークを通じて不特定の者の間で移転可能な仕組みを有しているか」、「発行者による制限なく、1 号電子決済手段との交換を行うことができるか」、「1 号電子決済手段との交換市場が存在するか」、「1 号電子決済手段を用いて購入又は売却できる商品・権利等にとどまらず、当該電子決済手段と同等の経済的機能を有するか」等をチェックするものとされる[37]。2 号電子決済手段は、1 号電子決済手段の要件を欠きながらも、不特定の者を相手方としてそれと交換することによって、事実上、1 号電子決済手段の規制を潜脱することを防止するために定められた類型である[38]。

(6) 3 号電子決済手段（特定信託受益権）

イ. 定義

3 号電子決済手段、すなわち特定信託受益権とは、電子情報処理組織を用いて移転することができる財産的価値に表示された金銭信託の受益権であって、受託者が信託契約により受け入れた金銭の全額を預貯金により管理するものであることその他内閣府令で定める要件を満たすものである（資金決済法 2 条 9 項）。

金銭信託であるから、受託者は、当初信託財産である金銭の拠出を受け、資金決済法に基づきその全額を預貯金により管理することが求められる。特定信託受益権は、利用者から対価としての金銭の拠出を受けたうえで、その全部を預貯金により運用する点で、未使用残高全額について預託等の義務が生じる資金移動業者により発行される 1 号電子決済手段とその経済的実質は類似しているが、1 号電子決済手

37 金融庁「事務ガイドライン第三分冊：金融会社関係 17 電子決済手段等取引業者関係」I-1-1 ③。
38 市古［2024］230 頁。

段と異なり、「不特定の者を相手方として購入および売却を行うことができる」こととという要件が規定されていない点に大きな特徴がある。不特定性の要件が規定されていないことから、特定受益権については、P2P 型のほか、中央管理者としての受託者が存在しその移転に関与する非 P2P 型の発行者原簿型の受益権も 3 号電子決済手段に該当しうることになる。

ロ. 信託財産

特定信託受益権が円建てで発行される場合には、「信託財産の全部が預金又は貯金により管理されるものであること」（特定信託受益権電子決済手段等取引業者に関する内閣府令 3 条 1 項）、外貨建てで発行される場合には、「信託財産の全部がその外国通貨に係る外貨預金又は外貨貯金により管理されるものであること」とされている（同条 2 項）。特定信託受益権は、預貯金債権を信託財産とする受益権であるという点において、預貯金債権とリンクしている。発行者または仲介者の固有財産からの分離が図られることによって信託財産の独立財産性が確保されるとともに、信託財産の内容はきわめて安全性および等価性・均一性の高い預貯金債権から構成されることになり（2 節（2）参照）、安全性・規格性・等価性を有するため、決済手段としての適格性が担保されている。

ハ. 発行者

3 号電子決済手段の発行および償還は、為替取引に該当するという前提で、資金決済法において規制されている。特定信託受益権については、信託銀行が発行する場合には、銀行業務の本来業務に為替取引が含まれるため、銀行規制によってカバーされる。それに対し、信託銀行ではない信託会社が特定信託受益権を発行する場合には、特定信託為替取引とされ、それを業として営むことは、特定資金移動業として資金移動業の一種と整理されている（資金決済法 36 条の 2 第 4 項）。特定信託会社が特定資金移動業を営む場合には、特定資金移動業を資金移動業と、当該特定信託会社を資金移動業者とみなして、資金決済法の規定が適用される（同法 37 条の 2 第 2 項）。

(7) 4 号電子決済手段

イ. 意義

4 号電子決済手段とは、1 号電子決済手段から 3 号電子決済手段に準じるものとして内閣府令で定めるものである。内閣府令は、「…物品等を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行

うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限る。）であって、電子情報処理組織を用いて移転することができるもののうち、当該代価の弁済のために使用することができる範囲、利用状況その他の事情を勘案して金融庁長官が定めるもの」と規定する（電子決済手段等取引業者に関する内閣府令 2 条 3 項）。4 号電子決済手段の大きな特徴は、通貨建資産に限られない点にあり、そのためいわゆる暗号資産型ステーブルコインがこれに該当する可能性がある。

ロ．特徴

4 号電子決済手段の大きな特徴は、第 1 に、通貨建資産の要件が課されていない点にある。対象になる財産的価値も通貨建資産に限定されない。非通貨建資産も 4 号電子決済手段に該当しうるのであって、発行者による発行や償還が必ずしも想定されない。他の類型の電子決済手段と異なり、発行や償還が観念されないのであるから、4 号電子決済手段の発行等は、為替取引には該当しないことになると考えられる。第 2 に、他の類型の電子決済手段と異なり、金融庁長官の指定を要する。

もっとも、4 号電子決済手段に係る金融庁長官の指定は、当面、なされない見込みである。そこで、本稿では、4 号電子決済手段については、捨象する。

4. 電子決済手段の民事法上の規律

(1) 電子決済等取扱業の対象である電子マネーの移転

電子決済手段の法形式について述べる前に、銀行預金を用いた非 P2P 型の電子マネーの仲介業すなわち電子決済等取扱業の対象である預金債権が、どのように移転して決済に用いられるかを概観する。要求払預金を用いた非 P2P 型の電子マネーの移転・処分に関する議論をみると、債権譲渡構成、更改構成、消滅・発生構成、債務引受構成等が考えられる。このうち、消滅・発生構成とは、口座の存在を前提とし、口座の記帳を通じて権利義務の変動が生じるとする構成であり、判例・多数説の立場であるが、その法的根拠は、不明であると指摘されている[39]。

債権譲渡構成には、対抗要件の具備、および、意思表示の瑕疵や抗弁の接続といった決済手段に求められる性質にふさわしくない法的効果が生じる。また、更改構成は、抗弁の制限という法的効果を実現しうるものの、債権者の交替による更改は、対抗要件の具備の問題が残る（民法 515 条 2 項）。いずれの構成も、現行の実

39 デジタルマネーの私法上の性質を巡る法律問題研究会［2024］11 頁。

務の取扱いと合致しない。すなわち、実務において、電子決済等取扱業の対象である電子マネーの移転について対抗要件を具備することはなされていないし、それを要求することは決済の効率性・迅速性を大きく阻害するものと考えられる[40]。

イ．消滅・発生構成

判例・多数説は、消滅・発生構成を採用する[41]。消滅・発生構成によれば、第1に、決済手段である銀行預金の移転に対抗要件を要求することの不適切性、および抗弁の接続を認めることの不適切性を回避することができる。第2に、預金債権の譲渡禁止により銀行の予定している決済方法以外での預金債権の移転が禁止されているが、預金債権についての譲渡制限の意思表示は、その意思を知りまたは重過失によって知らなかった譲受人その他の第三者に対抗することができる（民法466条の5第1項）。要求払預金債権の譲渡が制限されていることは広く周知されているので、決済システム内部において完結したシステムを創設することができる。第3に、社会的信頼のある銀行による預金口座簿の記帳によってのみ第三者との関係を規律できる。第4に、日本銀行を頂点とする複層的な決済システムにおいて規格性・等価性・安定性を有する決済手段であるという（2節（1）参照）実態と現実に整合的であり、また、預金口座における銀行による記帳に対する規制と信頼性等がそれを支えている。消滅・発生構成を採用した場合には、決済の取消不能性や確実性・明確性という観点から、決済手段や決済システムに適用される法律構成として、「占有＝所有」の理論が適用される金銭による決済の場合とかなり接近した法的効果が導かれる。他方、その法的根拠や法的性質については、必ずしも解明されていない点があるほか、後述するように具体的妥当性を欠くと思われる結論が導かれる可能性も否定できないと思われる（本節（2）ロ．および5節参照）。

消滅・発生構成の前提として、そもそも、決済性預金については、口座に入金された個々の預入金ごとに預金債権が個別に成立するのではなく、入金記帳がなされる都度債権は消滅するとともに、入金記帳された時点において、すべての個別の入金と支払を差引計算した残高として1つの残高債権が発生するものとされる（最判平成8年4月26日民集50巻5号1267頁）。消滅・発生構成が最もわかりやすいのは、同一の銀行のもとで送金人と受取人の双方の預金口座が開設されている場合である。送金人の預金口座の減額記帳とともに受取人の預金口座の増額記帳により送金人から受取人に対する預金債権の移転がなされる。しかし、異なる銀行間の振込のように異なる銀行のもとで決済当事者の口座が開設されている場合であっても、消滅・発生構成を採用することができる。すなわち、送金人の甲銀行における預金

40 電子マネー及び電子決済に関する懇談会［1997］。

41 森田［1997a］49頁、加毛［2023］260～261頁、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］10～12頁、市古［2024］15～18頁等。一定の限定を加えつつ、消滅・発生構成により説明する文献として、岩原［2003］78頁。

口座の減額記帳により送金人の甲銀行に対する預金債権が減少し、それに続く受取人の乙銀行における預金口座の増額記帳により受取人の乙銀行に対する預金債権が増額することになる。もっとも、その場合には、甲銀行と乙銀行が全銀システムとさらにはその上位に位置する日銀ネットという複層的な決済システムに組み込まれており、完結した決済システムの内部において甲銀行と乙銀行との資金決済が確実・安全・効率的になされ、上記のような記帳の変更が生じるのである。

判例も、消滅・発生構成に依拠する。すなわち、上記平成 8 年最高裁判決は、「振込依頼人から受取人の銀行の普通預金口座に振込みがあったときは、振込依頼人と受取人との間に振込みの原因となる法律関係が存在するか否かにかかわらず、受取人と銀行との間に振込金額相当の普通預金契約が成立し、受取人が銀行に対して右金額相当の普通預金債権を取得するものと解するのが相当である」と判示する。その理由として、同判決は次の 2 点を挙げる。第 1 に、前記普通預金規定には、振込があった場合にはこれを預金口座に受け入れるという趣旨の定めがあるだけで、受取人と銀行との間の普通預金契約の成否を振込依頼人と受取人との間の振込の原因となる法律関係の有無に係らせていることをうかがわせる定めは置かれていない。第 2 に、振込は、銀行間および銀行店舗間の送金手続を通して安全、安価、迅速に資金を移動する手段であって、多数かつ多額の資金移動を円滑に処理するため、その仲介に当たる銀行が各資金移動の原因となる法律関係の存否、内容等を関知することなくこれを遂行する仕組みがとられている。

前述したように、判例・通説ともに、振込指図により預金口座の帳簿に入金時に存在した残高と合算して新たな 1 本の預金債権になると解する。その法律構成については、段階的交互計算説が有力である。しかし、判例・通説が思い描く消滅・発生構成は、少なくとも典型契約である交互計算契約（商法 529 条）とは異なる。第 1 に、交互計算は、交互計算期間があり、交互計算に係る計算書の承認により交互計算期間中に交互計算に組み入れられた債権債務の総額について差引計算がなされ、それにより 1 本の債権債務関係が発生する（同法 529 条・532 条）。商法上の交互計算は、古典的交互計算であるというのが、判例（大判昭和 11 年 3 月 11 日民集 15 巻 320 頁）および通説である。しかし、預金口座についてはそのような計算書の承認手続は存在しない。もっとも、民法上の交互計算契約が非典型契約として認められるとすれば、商法上の交互計算契約に該当しなくても問題ないであろう。第 2 に、交互計算に組み入れられる債権債務は、有因であり、組み入れられた債権債務が無効であれば、交互計算の結果にも瑕疵が生じる（商法 532 条但書参照）。この点は、消滅・発生構成の法的効果と異なるように思われる。

消滅・発生構成のもとでは、二重の無因性が前提にされていると考えられる。すなわち、上記平成 8 年最高裁判決が指摘するように、指図に基づく入出金は、指図の抽象性（無因性）に基づいて、その原因関係から遮断されるという第 1 段階の無

因性に加え、そのようにして新たに成立した預金債権は、それ以前の残高債権に係る瑕疵等から遮断されるうえに、当該指図行為自身が無因的（抽象的）な行為と解されているという第2段階での無因性の双方が判例・通説の前提になっていると考えられる。最決平成28年12月19日民集70巻8号2121頁は、「普通預金契約及び通常貯金契約は、一旦契約を締結して口座を開設すると、以後預金者がいつでも自由に預入れや払戻しをすることができる継続的取引契約であり、口座に入金が行われるたびにその額についての消費寄託契約が成立するが、その結果発生した預貯金債権は、口座の既存の預貯金債権と合算され、1個の預貯金債権として扱われるものである」と判示する。上記平成28年最高裁決定のこの判示と、振込依頼人から受取人の銀行の普通預金口座に振込があった時は、振込依頼人と受取人との間に振込の原因となる法律関係が存在するか否かにかかわらず、かつ、誤振込であったのに受取人の普通預金債権が成立するとした上記平成8年最高裁判決を併せ読むならば、消滅・発生構成によれば、物と同様の法的効果、さらには物を超えて金銭に関する法理すなわち「占有＝所有」の理論を適用する場合にかなり接近した法的効果が導かれる。もっとも、消滅・発生構成の前提になっていると考えられる二重の無因性について、十分な解明がなされていない点があるように思われる。

ロ．二重の無因性

誤振込による記帳であっても、誤振込を受けた受取人の被仕向銀行に対する預金債権の成立を認めた上記平成8年最高裁判決は、振込の原因になる法律関係に基づく振込指図かどうかは問題にならないとし、振込の原因になる法律関係と振込指図との間には有因の関係がないこと、すなわち無因の関係にあると判示した。さらに同判決は、明示的には論じていないものの、本件でなされた振込指図という法律行為自身に、錯誤という意思表示の瑕疵があり、取消しの対象になるとも考えうるところ（民法95条1項）、意思表示に瑕疵のある振込指図に基づく預金口座簿への記帳の有効性を、何ら理由を示すことなく認めているものと考えられる。日本の判例・通説は、第1段階において振込指図の原因になる法律関係と振込指図の無因性（抽象性）を、第2段階においては振込指図という法律行為について手形行為・小切手行為に認められているのと同様の無因性（抽象性）もしくは文言性を認めているものと考えられる[42]。

42 判例は、手形行為につき、「手形の裏書は、裏書人が手形であることを認識してその裏書人欄に署名又は記名捺印した以上、裏書としては有効に成立するのであつて、裏書人は、錯誤その他の事情によって手形債務負担の具体的な意思がなかつた場合でも、手形の記載内容に応じた償還義務の負担を免れることはできない」と判示し、「手形債務負担の意思がないことを知つて手形を取得した悪意の取得者に対する関係においては、裏書人は人的抗弁として償還義務の履行を拒むことができるものと解するのが相当であ」ると述べ、手形行為の瑕疵を人的抗弁の問題として対処する（最判昭和54年9月6日民集33巻5号630頁）。

上記平成8年最高裁判決は、錯誤に基づく振込指図による預金口座簿への記帳の有効性を認めた。

ハ．支払委託証券との比較

支払委託証券である小切手や為替手形が利用された場合には、振出や裏書等の各種の手形・小切手行為について、その無因性・文言性から有価証券法理に固有の理論が適用される。支払委託証券である小切手や為替手形といった有価証券には、振出人の指図に基づく支払権限が証券上に表章されていると解されている。とりわけ、本稿の対象である P2P 型の電子決済手段の機能は、銀行が振り出す自己宛小切手である預手に類似していると考えられる。そこで、以下では、指図の無因性・文言性という観点から、小切手や為替手形を用いて決済する場合と振込とを比較する。

支払委託証券による決済と振込による決済には、次の違いがある[43]。すなわち、第 1 に、支払指図の伝達経路が、振込の場合には、送金人の支払指図が直接送金銀行に伝達されて受取人に対する支払指図が行われるのに対し、小切手の場合には、振出人の支払指図は、受取人を介して送金銀行に伝達される。第 2 に、支払指図の伝達手段が、振込の場合には電子的信号であるのに対し、小切手の場合には証券という物であるという物理的な違いがある。しかし、送金人または振出人からの支払指図に基づいて資金移動がなされる点では共通している。

ところが日本においては、指図の民事法上の位置付けや性質が不明確である[44]。指図概念の不明確性と規律の必要性は、平成 29 年民法改正の際にも俎上に上った。すなわち、「(振込や資金移動取引) の法律関係は、指図という法律行為を基礎とするものと解されることから、…民法に指図に関する明文の規定を設けるべきであるとの考え方」が示され、その当否について検討することが論点に挙げられた[45]。しかし、平成 29 年民法改正において指図について規律が置かれることはなかった。もっとも、支払委託証券であり法律上の指図証券である為替手形や小切手については、指図にかかわる判例や学説が豊富に存在しており、P2P 型の電子決済手段にとってかなり参考になると考えられるため、具体的な論点に即して後述する（本節 (2) ロ．参照)。

しかし、比較法的には、例えばドイツ法のように、第 1 段階については日本の判例・通説と同様に解するが、第 2 段階については、預金契約の条項と合わせて権利外観法理を適用することによってある程度動的安全の保護を確保するものの、ドイツ法のもとでも、指図行為について有価証券行為と同様の無因性もしくは文言性が肯定されているわけではないと理解される。

43 岩原［2003］33〜34 頁。

44 銀行振込における支払指図について、委任契約と消費寄託契約という 2 つの側面に基礎を置くものであり、委任契約に基づき銀行は支払人の指図した受取人に一定の金額を支払う義務を負い、その支払は受取人と銀行との預金契約に基づくものであるとし、指図は上記 2 つの契約に基づく義務として説明される。森田［1997b］49〜53 頁。そこでは、指図自体の法的性質についてはとくに触れられていない。

45 法務省民事局参事官室［2011］170 頁。

ニ. 債務引受構成

銀行預金の移転・処分について考えられる4つ目の法律構成として、債務引受構成がある。例えば、銀行間の決済については、他行間の振込が全銀システムにより清算される場合には、全銀ネットが参加銀行からの振込通知に基づく為替取引に係る債務を引き受けており、中央対当当事者（セントラル・カウンターパーティ）を設置することによって多数当事者間の複雑な決済関係を単純化するとともに決済金額を圧縮する等して、決済の効率化・安定化を図っている。この構成のもとでは、契約の定め方によっては、対抗要件具備、抗弁の接続、および意思表示の瑕疵等の問題をクリアできる可能性がある。しかし、リテールの分野において送金人の取引銀行が振込に際して、送金人の債務を引き受ける意思は通常はなく、振込指図は送金事務の委託であると解される。

(2) 1号電子決済手段

イ. 移転の法律構成

現実に利用される可能性がある1号電子決済手段は、資金移動業者により発行されることになろう（3節（2）参照）。発行者である資金移動業者は、1号電子決済手段の保有者に対し、約定に従って送金・決済サービスを提供する義務を負い、資金決済法の規定にしたがって保有者に対し額面額の通貨で償還する義務を負っている。口座型すなわち非P2P型の資金移動業電子マネーについては、前述した銀行預金を用いた非P2P型の電子マネーの法律構成と基本的に同様に考えることができると思われる。資金移動業電子マネーは、保有者にはその残高に応じた払戻請求権があり、口座の記帳を通じて移転が行われる等、銀行預金との類似性が大きいからである[46]。すなわち、債権譲渡構成[47]、更改構成[48]、消滅・発生構成[49]、債務引受構成が考えられる。

ところが、P2P型の1号電子決済手段の場合には、保有者は、口座とは独立して資金移動業者に対する債権を保有していることが想定される。すなわち、資金移動業マネーの場合には、口座を通じた発行者と債権者の連結を必ずしも前提にしてい

46 デジタルマネーの私法上の性質を巡る法律問題研究会［2024］6〜7、9頁、市古［2024］29頁。
47 電子マネー一般につき、電子マネーに関する勉強会［1997］11頁、小沢［1997］11〜12頁等。
48 電子マネーに関する勉強会［1997］12頁。
49 市古［2024］337頁。P2P型の1号電子決済手段の移転には、移転の都度、債権の消滅・発生の承諾行為はないとしても、パーミッションレス型ブロックチェーンで発行する以上、P2P取引によりブロックチェーン参加者の債権額が増減することを発行者が予め包括的に承諾していると評価する余地があると指摘される。市古［2024］338頁注183。また、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］31〜32頁は、債権譲渡構成、更改構成、または消滅・発生構成のいずれも採用する余地があるとする。

ない点が、銀行預金に基づく電子マネーと異なり、それゆえ資金移動業者は P2P 型の資金移動業電子マネーである 1 号電子決済手段を発行することができるのである。P2P 型の電子決済手段については、非 P2P 型の電子マネー等を念頭においた上記 4 つの法律構成に加えて、有価証券とりわけ支払委託証券、金銭、さらにはデジタル資産ないし金券と対比することによって、1 号電子決済手段の法的位置づけを明らかにすることができるように思われる。

検討に先立ち、資金移動業者が発行する 1 号電子決済手段により権利者もしくは保有者が発行者に対し求めることができる権利の内容を確認する必要があろう。資金移動業者は、為替取引に用いられることがないと認められる資金の受入れを禁じられており（資金決済法 51 条）、この点で銀行預金における預金者の銀行に対する消費寄託に基づく返還請求権とは法的性格が異なる。1 号電子決済手段の権利者ないし保有者は、その発行者である資金移動業者に対し約定に則った指図を通じて資金移動による決済サービスを求める権利および 1 号電子決済手段の対価として出捐された当該決済サービスの提供のための送金資金の償還を請求する権利を有すると考えられる[50]。

以下では、P2P 型の電子決済手段の移転に発行者の関与が不要であることに着目した法律構成について検討する。まず、有価証券的構成、すなわち、電子決済手段を、上記の保有者が有する債権が有価証券に化体されて有価証券法理に基づいて移転する場合と同様に考えてみる。この場合には、さらに、支払委託証券とりわけ預手とのアナロジーによる見解と、無記名証券と同様に考える見解とがありうる。しかし、物理的な証券等の存在を前提にする有価証券についての法理を物ではなく電子データにすぎない電子マネーに適用することに対しては強い批判がある[51]。そこで、デジタル資産的構成、すなわち、トークンの移転によりデータに基づく権利が移転し、電子的データそのものに法的価値を承認する、いわば電子データを物と同視または物として扱うという考え方が登場しうる。デジタル資産については、後述するが（本節（2）ハ．参照）、電子決済手段自体を金券[52] と同様に価値と媒体を不可分のものとし、物の移転の場合と同様の法的効果を導く考え方も、デジタル資産的構成に含まれると考えられる。有価証券的構成およびデジタル資産的構成によれば、善意取得の類推適用等、物権的法理を電子決済手段に適用する余地が生じる。

債権譲渡構成、更改構成、消滅・発生構成、債務引受構成については、銀行預金

50 デジタルマネーの私法上の性質を巡る法律問題研究会［2024］8 頁。

51 森田［1999］60 頁。

52 金券または金銭代用証券とは、郵便切手や収入印紙等、それ自体が表示された金額に相当する 1 個の価値体としての価値を有するものであり、金銭の支払と同様の効力を有する証券である。金券は、証書（紙）と権利を分離することができない点において、両者を観念的に分離できる有価証券とは異なるとされる。法的には、金券には有体物についての規律が適用される。

なお、物を超えて金銭の法理すなわち「占有＝所有」の理論の適用を肯定するという考え方もありうるが、同様の法的効果は、消滅・発生構成により実質的にほぼ達成しうることは、すでに述べた。

を用いた電子マネーの箇所で言及したので（本節（1）参照）、以下では、有価証券的構成およびデジタル資産的構成について扱う。

ロ．有価証券的構成

（イ） 支払委託証券―為替手形・小切手

a. 1号電子決済手段との異同

1号電子決済手段を有価証券的に構成する場合には、その機能に着目し、支払委託証券と比較することが適切であろう。支払委託証券であり支払手段として用いられる為替手形や小切手は、有価証券の代表である。有価証券法理に基づく動的安全の保護を目的にする規律や法理、すなわち、有価証券行為の抽象性（無因性）、善意取得、抗弁の制限、支払免責（ただし、小切手の場合は手形法の規定の類推適用による）等が適用される。支払委託証券は、単純な金銭債権を表章するものであるが、支払の委託を内容にするものであり、法律上の指図証券である。

支払委託証券である小切手における指図の法的効果についていえば、小切手の所持人は直接支払銀行に対して小切手金支払請求権をもつわけではなく、支払銀行から支払を受ければ、それを受領する権限のみを有しているにすぎない。小切手の振出人が支払銀行に対し支払指図をすると、支払銀行に対し支払権限が授与されるとともに、所持人に対する関係では当該支払権限に対応する受領権限が授与されるという二重授権説が通説である[53]。この点において、小切手の所持人は電子決済手段の権利者・保有者とは異なる法的地位にあり、1号電子決済手段は支払委託証券のうち預手に類似しているといえよう。これに対し、為替手形の場合には、支払人が引受けをするまでは手形所持人の支払人に対する法的請求権は生じない。1号電子決済手段が保有者の発行者に対する償還請求権をも表章していることにかんがみるならば、支払人による引受けがなされた為替手形に類似していると考えられる。

指図は、欧州では、更改に近い淵源をもつとされたが、次第に更改制度から独立し、民法上独自の制度として確立してきたという経緯がある[54]。なお、かつては、指図は更改の一種であり、指図人と被指図人との資金関係または指図人と受取人の対価関係のいずれかまたは双方の債務が消滅し、被指図人の受取人に対する債務が発生するものと理解されていた。ところが、欧州において既存債務を必ずしも前提

53 石井・鴻［1976］300～301頁、鈴木［1992］355頁等。為替手形・小切手の所持人に対する引受人・支払人による支払が非債弁済にならず、所持人に対して引受人・支払人が支払ったものの返還を請求できないというためには、所持人には受領権限があると解するほかなく、そのような権限が支払委託証券に表章されているとされる。さらに、為替手形および小切手の振出における支払委託の場合には、所持人が支払人から支払を受けられなかった場合には支払委託をした振出人が担保責任を負うことがあるが（手形法9条、小切手法12条）、この責任は振出人が所持人に対し受領権限を付与したことが基礎になっていると説明される。前田［1999］670～674頁。

54 指図に関する研究として、古くは伊澤［1930, 1931, 1935, 1936a, 1936b］、最近では隅谷［2016］がある。本文の記述は、これらの文献による。

としない無因的（抽象的）な指図がそもそもローマ法において認められていたという認識が広まり、更改を生じない指図もあるとして、指図と更改とは別制度であると認識されるようになった。ローマ法のもとでは、被指図人の受取人に対する義務の発生を伴わない支払指図と義務が発生する義務設定指図の 2 種類があったとされ、前者がドイツ法の指図の淵源となっており、それが支払委託証券における指図に係る日本法の理解や学説に影響を与えているものと推測される。日本法において指図に関する民商法上の規律が存在しないこと、ジュネーブ手形法・小切手法統一条約によりその内容はそれを批准している日本とドイツの間ではほぼ一致していること等から、ドイツ法の理論が下敷きになってきたものと推測される。

b. 指図に瑕疵等がある場合

以下では、指図に瑕疵や欠缺がある場合を類型化して、支払委託証券に係るリスクが関係者の間でどのように分配されているかを概観する。

（a）振出人の行為無能力

振出人が行為無能力であった時は、当該支払委託証券の振出は取り消され、善意の第三者にも対抗できると解されている[55]。

（b）意思表示の欠缺・瑕疵

判例・通説は、手形・小切手の振出に係る意思表示の瑕疵はその効力には影響を与えず、人的抗弁としてしか悪意の所持人に対抗できないとする[56]。なお、債務者の支払の局面においては、手形法では債務者に悪意・重過失がない限り免責が認められるが（手形法 40 条 3 項）、小切手法にはこれに相当する規定が置かれていない。しかしながら、支払銀行による小切手に対する支払については、同条同項を類推適用する説が有力である。

（c）無権限の支払委託

偽造小切手等を作成した無権限者に対し、債務者・支払人が行った支払は無効であるが、判例・多数説は、偽造小切手等による支払による損害を振出人に負担させる傾向が強い。その場合の法律構成については、見解が分かれている[57]。第 1 は、民法 478 条により取引上の社会通念に照らして受領権者としての外観を有する者に対する弁済をした支払銀行の免責を認めるものであるが、支払銀行の無過失を要件にする一方、過失なく弁済した支払銀行はすべて免責されるとする。判例は、この立場を採用する[58]。第 2 は、商慣習により振出人が責任を負担するとする。第 3 は、偽造小切手の支払も委任事務処理費用の支払として振出人に負担させることができると解する。ただし、支払銀行は偽造小切手等の支払に際し相当の注意を払わ

55 石井・鴻［1976］91 頁、大隅・河本［1977］91 頁、岩原［2003］203 頁等。
56 判例として、最判昭和 54 年 9 月 6 日民集 33 巻 5 号 630 頁【錯誤の事案】等。
57 学説の分類を含め詳細は、岩原［2003］136〜144 頁。
58 最判昭和 46 年 6 月 10 日民集 25 巻 4 号 492 頁。

なければ被偽造者等に対し損害賠償責任を負うとする。

c. 資金関係の不在

通説によれば、支払委託証券上、支払委託により振出人から支払人に対し、支払権限の授与がなされるが、この支払権限は手形・小切手の支払委託関係という支払委託証券外の契約関係に基づいて生じるのが通常であろう。振出人から支払銀行に付与された支払権限は、受領権限とは異なり、小切手外の資金関係に基づくものである。小切手法は、支払人を銀行に限るとともに（同法 3 条）、振出人が支払銀行に対し処分可能な資金を有し、かつ、振出人と支払人との間にその資金を小切手により処分できる旨の契約の存在を必要としている（同条）。支払手段としての小切手の信用証券化を防止する趣旨である。しかし、資金関係が存在しない場合であっても、無因（抽象）行為である指図、ここでは振出人から支払人に対する支払権限の授与の効力には影響を与えない（同条但書）。

d. 支払銀行による誤払い

支払銀行が当座勘定口座の資金不足や当座勘定契約の解約等の場合に誤払いをしても、支払委託証券上になされた指図によって所持人に付与された受領権限に基づいて、所持人は支払銀行に対し不当利得返還義務を負わないと解されている。ただし、支払銀行が要素の錯誤により支払った場合には、支払自体が無効であり、所持人は支払銀行に不当利得返還義務を負うと解されている[59]。

（ロ） 投資証券―振替証券

次に、電子化された有価証券であり、ステーブルコインと同様に高度の流動性をもつ上場投資証券の移転に係る規律をみる。これらは支払手段としてではなく投資対象であり、経済的機能は 1 号電子決済手段と大きく異なるが、高度の流動性を有するペーパーレス化された投資証券の移転に関するルールは、電子決済手段の規律についても参考になる。「社債、株式等の振替に関する法律」（平成 13 年法律第 75 号）による振替制度に基づく振替証券の移転は、振替機関における振替口座の存在を前提とし、口座の記帳を通じて権利義務の変動が生じるものとされる。

電子決済手段について、社債、株式等の振替に関する法律の適用により中央管理機関および口座管理機関の帳簿の記載に基づき権利が移転するものと解釈するために、同法の規定を類推適用する余地がある。しかし、この構成を採用する場合には、口座の存在が類推適用の基礎になるため、P2P 型の 1 号電子決済手段には適合しないと考えられる。

59 鈴木［1992］114 頁、神作［1992］96～97 頁、岩原［2003］312～313 頁等。

ハ. デジタル資産的構成

支配（コントロール）[60] や排他性に着目し、デジタル資産や支配可能な電子データに物権法的な規律を適用しようとする動向がグローバルに認められる。解釈論によることには限界が大きく、立法的な解決が目指されている[61]。

日本でも、P2P 型の電子マネーについて民事法上の規律を整備し、①電子データが受取人に受信され排他的に支配されるに至ったことにより譲渡の成立を認めること、②偽造や二重譲渡がなされた場合には正規のものと偽造のものとの判別が困難であること等から過失がない保有者についてはいずれも有効なものとして扱うものとすること、③無権限者による移転等の処分の場合には非 P2P 型の電子マネーの場合と共通のルールを、過失責任原則や支配領域責任の考え方等を踏まえて立法によって明らかにすること、その一方で、④すでに引き出されて顧客のデバイスに蓄えられていた電子マネーを無権限者が処分した場合には、基本的に無効であり、無権限者から電子マネーを譲り受けた者は善意取得制度によって保護すべきであること、⑤移転行為やその原因関係に瑕疵がある場合には、悪意や重過失がある者については抗弁の提出を認める余地があること、⑥弁済の効力発生時期を電子マネーの交付時とすべきこと等が主張されている[62]。

なお、法制審議会商法（船荷証券関係）部会が決定した「商法（船荷証券等関係）等の改正に関する要綱案」において、電子船荷証券に係る規律が提案されている（法制審議会商法（船荷証券関係）部会［2024］）。そこでは、電子船荷証券記録とは、「船荷証券に記載すべき事項を記録した電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）のうち、特定情報処理システムにおいて作成され、及び管理されたものであって、当該電磁的記

60 例えば、UNIDROIT（International Institute for the Unification of Private Law）のデジタル資産私法原則 6（UNIDROIT [2023] pp. 51–52, Principle 6）は、デジタル資産または関連するプロトコル・システムが、①他者がデジタル資産から生じる実質的にすべての便益を享受することを妨げる排他的な権限、②デジタル資産から生じる実質的にすべての便益を享受することができる権限、および③他者に対して上記①②および③の権限を移転する排他的な権限を付与された者が、当該デジタル資産の支配（コントロール）を有すると定める。

61 UNCITRAL（The United Nations Commission on International Trade Law）の電子的移転可能記録に関するモデル法（UNCITRAL [2017]）や前掲脚注 60 に述べた UNIDROIT のデジタル資産私法原則のほか、米国では 2022 年に統一商事法典 12 章を新設しコントロール可能な電子的記録（controllable electronic record）についての規律が整備された。英国では、2022 年に公表された法律委員会のデジタル資産に関するコンサルテーション・ペーパー（Law Commission [2022]）および 2023 年公表の最終報告書（Law Commission [2023]）に基づき、2024 年 2 月に立法提案と最終的な市中協議がなされている。Law Commission [2024]. ドイツでは、デジタル資産やコントロール可能な電子的記録についての一般的規律ではないが、商法上の物品証券と投資証券を電子データ化したものについて 2013 年商法改正と 2021 年電子有価証券法制定によりそれぞれ立法的手当を行った。UNCITRAL のモデル法については、小出［2013］。

62 岩原［2003］466〜506 頁。

録が改変されているかどうかを確認することができる措置その他の当該電磁的記録が運送人又は船長の作成に係るものであることを確実に示すことができる措置がとられているものいう」と定義されている[63]。そのうえで、船荷証券の占有または所持に代わる概念として「電子船荷証券記録の支配」を設け、電子船荷証券記録の支配とは、特定情報処理システムにおいて、特定の者のみが電子船荷証券記録に記録されている運送品に係る権利を有する者として当該電子船荷証券記録を利用することができる状態にあることであり[64]、船荷証券の交付または引渡しに代わる概念として「電子船荷証券記録の提供」を設け、電子船荷証券記録の提供とは、特定情報処理システムにおいて、運送人もしくは船長または電子船荷証券記録の支配に係る権限を有する者が、その指定する者が当該電子船荷証券記録の支配に係る権限を有する者となるようにするための措置をとることであると定義する[65]。

(3) 3号電子決済手段（特定信託受益権）

イ. 非P2P型

3号電子決済手段すなわち特定信託受益権の移転・処分については、P2P型と非P2P型に分けて検討する必要がある。特定信託受益権の大きな特徴は、1号電子決済手段と異なり、P2P型のほかに、非P2P型の中央管理者が存在する発行者原簿型の特定信託受益権が認められている点にある。

非P2P型の場合には、決済手段としての適格性を満たすためには、口座の記録と移転の効力発生を一致させ、かつ、システム外での移転・処分を封じることが求められる。そのためには、第1に、受益証券発行信託としたうえで、受益証券を発行しない受益権を発行し、受益権原簿制度を利用することが考えられる（信託法185条1、2項）。受益証券発行信託において受益証券を発行しないものと信託行為において定められた信託受益権（同法185条2項）は、当事者の合意のみによって譲渡することができる（同法194条かっこ書き）。そして、受益証券発行信託につ

63 法制審議会商法（船荷証券等関係）部会［2024］第1部第1の1。

64 法制審議会商法（船荷証券等関係）部会［2024］第1部第1の3。

65 法制審議会商法（船荷証券等関係）部会［2024］第1部第1の4。中間試案の公表、パブリックコメント手続の実施後に開催された法制審議会商法（船荷証券等関係）部会において、電磁的記録は「占有」や「所持」の対象にはならず、電磁的記録に対する「支配」という用例もないため、「支配」という概念を法律上の定義なく用いると、法規範としての具体性を欠くことになることは否定できず、「電子船荷証券記録を〔排他的に〕利用することができる状態」といった定義を置いたとしても、抽象的に過ぎ、その具体的な当てはめは容易ではないという批判について議論された。電子船荷証券記録の利用実態等も踏まえつつ、「占有」または「所持」に代わる概念について、より具体的な定義を設けること、あるいは既存の概念を用いることは考えられないかとして、たとえば「帰属」という概念が取り上げられていた。法制審議会商法（船荷証券等関係）部会資料11（第11回会議（令和5年8月30日開催）3〜4頁（https://www.moj.go.jp/content/001402989.pdf）。

いては受益権原簿制度が採用されており、受益券を発行しない受益権の譲渡の受託者その他の第三者に対する対抗要件は、受益権原簿への記載または記録による（同法 195 条 2 項）。受託者であるとともに受益権原簿管理人になる者が、サーバ上に記録されているブロックチェーン上の記録を管理し、当該記録を受益権原簿と取り扱うことによって、システム内で譲渡手続を完結させることが可能になる。そのために、譲渡制限の定め（同法 93 条 2 項）として、譲渡の効力発生には受託者の承諾を要する旨の定めを置き、受託者・第三者対抗要件の具備は、デジタル化した受益権原簿の記載・記録によることになるため（同法 195 条 2 項）、受託者が受益権原簿の書換えに応じた場合には、受託者は譲渡を承諾したものとみなすこと等が考えられる。受益権の譲渡制限については、銀行預金の譲渡制限に関する規律と同様の規律が置かれており（同法 93 条 2 項）、悪意・重過失のある者に譲渡制限を対抗できるものとされている。そのため、悪意・重過失のある者に対しては、譲渡制限受益権の譲渡の効力は合意のみでは生じず、譲渡がなされ、受益権原簿の名義書換がなされた時に譲渡の効力が発生することになる。この場合には、権利の移転とデジタル化された受益権原簿の書換えが一体としてなされているものと評価できる。

もっとも、上述した特定信託受益権のスキームには、いくつかの解釈上の論点が残されている。受益証券発行信託でありながら、すべての受益権について受益証券を発行しないことができるかどうかが議論されている。受益権原簿制度について記載事項やその法的効果について厳格な規律が置かれており、その違反に対し過料の制裁等があることから、受益証券発行信託でありながら、すべての受益権について受益証券を発行することも可能であると解しうるのではないか。他にも受益権原簿の法定記載要件である氏名や住所を特定し記録できるかという問題がある（信託法 186 条 3 号）。この点も、非 P2P 型の特定信託受益権であれば、実務的に解決が困難ではないように思われる。

P2P 型ではなく、したがって中央管理者が存在する発行者原簿型の特定信託受益権は、受益証券発行信託として組成することができ、その場合には、上述したことが当てはまる（信託法 194 条かっこ書き）。

第 2 に、受益権が記録によって権利者やその残高を把握・確定できるファンジブルな権利であることに着目し、解釈論として、ブロックチェーン上の記録をもってその効力発生要件・対抗要件と解することが考えられる[66]。この議論は、信託受益権は、分割し割合的単位を創設することが可能であり、均一化・単位化されたファンジブル（代替可能）な権利は、口座上の記録を離れて譲渡の対象を特定することが困難である点にその法的な特性を認めるものである。代替性のある動産（種類物）については、物理的な分離によって譲渡の対象を特定することが可能であるが（民法 401 条 2 項）、無体物である権利は観念的な存在にすぎず物理的な分離によっ

66 前掲脚注 34 およびそれに対応する本文参照。

て特定することはできないからである。そのような権利を口座上に記録し、その数量または単位数として把握することは、観念的な存在であるファンジブルな権利に特定性ないし個別性を付与する法技術としての機能を有するものと捉えることができ、権利者が有する他の権利から移転対象の権利を分離し特定するためには、権利を移転しようとする者も権利を取得しようとする者も口座保有者であることとともに、権利者の口座の減額および取得者の口座の増額の記録によって裏付けられる必要があることから、口座の記録が権利移転の効力要件になることが導かれるとする。この考え方は、消滅・発生構成の理論的根拠を提示する可能性を秘めている。

ロ. P2P 型

特定信託受益権の第 2 類型は、P2P 型の中央管理者が存在しないタイプの受益権である。電子マネートークンとそれに表章された債権との分離を防止するための法律構成を考える必要があり、1 号電子決済手段に関する議論とパラレルな議論がなされている（3 節（4）参照）。以下では、信託受益権に固有の議論について概観する。

それは、信託法 88 条 1 項に基づく消滅・発生構成である。消滅・発生構成の法的根拠が不明であることは前述のとおりであるが、信託受益権を用いる場合にはそれに法的根拠が与えられている点が注目される。同条同項は、信託行為の定めにより受益者となるべき者として指定された者は、当然に受益権を取得する旨を規定する。この規定に基づいて、特定信託受益権の受益者は「信託契約の期間中のその時々におけるトークンの保有者である」旨を信託契約に定めることにより、常にトークンの保有者と特定信託受益権の受益者を法的に一致させることが検討されている[67]。

具体的には、信託契約において、異なるブロックチェーン・アドレスにトークンの移転記録がなされた時点で、旧トークン保有者である旧受益者の受益権は消滅し、送信先の新トークン保有者の元で新たに受益権が発生する旨を定めることによって、受益権の二重譲渡によってトークンの保有者と受益者が分離する事態を回避しようとするものである。

信託法 88 条 1 項は、第一受益権とその受益者の死亡等に基づく第二受益権の発生等、典型的には民事信託とりわけ世代超越機能の実現を念頭に置いた規定であり、この規定を根拠に消滅・発生構成に法的基礎を付与することは、たまたま信託法にはそのような規定があるから問題ないものの、その他の法形式を採用した場合にも妥当する、より一般的な法理を検討する必要があると思われる。

67 デジタルアセット共創コンソーシアム［2022］参照。

5. おわりに―今後の検討の方向性

電子決済手段は、当面は、資金移動業者がP2P型の1号電子決済手段として、あるいは、信託会社・信託銀行がP2P型または非P2P型の3号電子決済手段すなわち特定信託受益権として発行することが想定される。これらの電子決済手段の民事法上の性質や移転の法律構成については、議論が始まったばかりであるが、預金の振込について判例が採用しており、非P2P型の預金または資金移動業マネーを用いた電子マネーの移転の法律構成についても妥当すると解される消滅・発生構成が、金銭による決済に近い法的効果をもたらすために、電子決済手段の移転についても有力な法律構成の候補になると考えられる[68]。消滅・発生構成は、口座帳簿における記帳を基準にするものであり、債権譲渡や更改と法律構成した場合の対抗要件や抗弁の接続等の問題を克服した優れた法律構成であるからである。

しかし、口座帳簿の記帳を基準にした消滅・発生構成には、必ずしも理論的に十分に解明されていない点があるうえに、支払委託証券を用いる場合よりも金銭に近い法的効果を付与するものであって、とくに消費者が利用者に含まれる場合には必ずしも適切でないと思われる結論が導かれる可能性がある。口座帳簿の記帳に基づく消滅・発生構成は、日銀ネットや全銀システムのようにプロの金融機関等のみが参加し、膨大かつ多額の決済を効率的かつ安定的に処理することを法的に支える適切な法律構成であると思われる。しかし、リテールの決済を含む銀行預金や資金移動業マネーによる資金決済については、振込や移転の指図に意思表示の瑕疵がある場合や無権限移動といった適法な指示がなかったと解しうるような場合であっても、口座帳簿の記帳に基づく消滅・発生構成によれば、記帳によってつねに移転の効力が認められることになりかねない。こうした実質論あるいは利益衡量論からしても、また、比較法的検討からしても、消滅・発生構成の帰結は、動的安全の保護にやや傾きすぎているとも考えられる。有価証券法理が適用される支払委託証券である為替手形や小切手についても、そこまでの法的効果は認められていない。口座帳簿の記帳に基づく消滅・発生構成は、実質的に金銭による決済に非常に近い法的効果を導くものとなっており、支払委託証券と同様に発行者の関与なく移転するP2P型の電子決済手段の場合には、非P2P型の電子マネーに適用する場合よりも一層ふさわしい法律構成であるとも考えられる。しかし、他方で、電子データについてはその設計によっては金銭にはない精度の高い管理を実現できる可能性があり、そのようなメリットを活かした法律構成を検討する余地があるように思われる。

口座帳簿の記帳を基準にする消滅・発生構成は、債権譲渡や更改と法律構成した

68 前掲脚注49参照。

場合の対抗要件や抗弁の接続等の難点を克服する優れた構成であるが、理論的には、二重の無因性が暗黙裡に前提にされている点に問題があると思われる。支払指図とその原因関係が無因の関係にあることは、比較法的にも広く承認されており適切であるが、指図という法律行為について、必ずしも十分な検討がなされないまま、支払委託証券である為替手形・小切手の振出や裏書等の有価証券行為と同様に、その無因性・抽象性・文言性が認められているものと思われる。この点については、検討の余地があろう。紙幣や硬貨のような物理的な金銭と異なり、精度の高い支配可能な電子データとして電子決済手段を組成することが可能であるならば、実質的な利益衡量を反映した木目の細かい処理をすることが技術的に不可能とはいえないのではないか。少なくともリテールの資金決済において、指図の意思表示に重大な瑕疵がある場合や無権限者により指図がなされた場合には、そのような事情を知って取得した悪意者に権利の発生を認める必要はないと思われる。むしろ、支払委託証券に係る有価証券法理をベースとしつつ（4節（2）ロ.（イ）参照）、管理可能な電子データにふさわしい規律を構想することが考えられる。

資金移動業者が発行するP2P型の1号電子決済手段であれ、非P2P型とP2P型の両類型を含む3号電子決済手段（特定信託受益権）であれ、口座帳簿の記帳を基準にした消滅・発生構成以外にも、送金人の指図と当該電子決済手段の移転の方式に基づいて、送金人から受取人に対し電子決済手段が承継取得以外の方法で移転するものと法律構成する可能性は、検討に値するであろう。しかし、そのような検討の結果、やはり口座帳簿の記帳のみを基準にした消滅・発生構成によるほかないとしたら、特段の事情や原則に対する例外を認めることによっても、適切な法的効果を導くことは可能であり、特段の事情や例外について検討していくという方向性が考えられる。

従来の消滅・発生構成は、預金口座簿への記帳を基準にするものであるが、資金移動は、支払人の指図に基づいてなされるものであり、有効な指図と口座帳簿への記帳をもって消滅・発生構成を採用することができないか。換言すれば、指図の法的性質について検討を深め、有効な指図と記帳に基づく消滅・発生構成を採用する余地はないであろうか。仮に、有効な指図がなされることによって、送金人に対する未達債務が消滅し、受取人のもとで指図の内容に応じた発行者の未達債務が発生すると解するならば、指図の効力や抗弁の性質、および抗弁を第三者に対抗できる範囲等を検討することによって、従来の消滅・発生構成よりも柔軟で適切な法的効果を導くことができるように思われる。指図権の行使により指図が有効になされる場合とはどのような場合か、意思表示に瑕疵がある指図や無権限者による指図について、静的安全の保護と動的安全の保護のバランスをどのように図るか、無権限者と法的に評価された者の行った指図による移転に基づいて償還を行った発行者は、どのような要件のもとで支払免責をえることができるのか等について、類型化した

うえで、個別具体的に検討する必要がある。

電子決済手段の移転は、保有者による指図と当該電子決済手段の定める移転の方式に従ったうえで口座帳簿に記載されることによって、前保有者に対する発行者の債務が消滅し、新保有者に対する発行者の債務が発生するものと解することはできないであろうか。電子決済手段が決済のために用いられる支払手段である以上、電子決済手段の発行者と利用者との間に締結される契約には、発行者における電子決済手段の額面相当額での償還債務と、それを用いた決済サービスの提供に係る条項が定められることになろう。そのような契約に基づいて、電子決済手段の発行を受けた者は、自己の電子決済手段を誰に対しいくら移転するかを指図する権利を有しているものと考えられる。資金移動業者が1号電子決済手段の発行者である場合には、資金移動業者は利用者の指図に基づき資金の移動を実現するという事務を委託され、それに必要な送金資金の前払いを受けているものと解される[69]。受託者が特定信託受益権を発行する場合についても同様に、受託者は利用者の指図に基づき資金の移動を実現するという信託事務を委託され、それに必要な送金資金を信託財産として受け入れていると解される。いずれの電子決済手段についても、保有者には発行者に対する額面相当額の償還請求権が認められる。

発行者と電子決済手段の発行を受ける保有者との間には、保有者が発行者に対し為替取引に係る役務の提供を請求する権利を有することが約定されており、その中には移転の方式や、移転先や移転する金額に係る保有者の指図権が定められることになると解される。電子データである電子決済手段には、保有者が有する契約上の権利のうち、資金移動について送金先および金額を指図する権利が表章されていると解することはできないであろうか。そのように解する場合には、口座の存在を前提としないP2P型の電子決済手段については、電子決済手段の保有者から、当該電子決済手段の移転の方式に従ってそれを取得した者は、前の保有者が有している指図権を発行契約に則った適法な指図に基づいて取得した場合には、指図された受取人はその電子決済手段を取得し、約定に従って決済サービスの履行を求める権利と償還請求権、および指図権を取得するものと解される。電子決済手段には、その決済手段としての性質上、保有者の発行者に対する指図権が表章されており、有効な指図を受けるとともに電子決済手段をその移転の手続に従って取得した者は、権利者となり、あわせて指図権を取得すると考えることができると思われる。適法な指図と電子決済手段の移転の形式の具備によって、前の権利者の当該電子決済手段に係る権利は消滅し、新たな権利者のもとで権利が発生すると解するわけである。非P2P型の特定信託受益権を受益権発行信託により発行する場合には、それに加え、受益権原簿における記載が受託者および第三者に対する対抗要件になる。

電子決済手段における指図は、指図の原因となる法律関係の影響を受けない無因

69 デジタルマネーの私法上の性質を巡る法律問題研究会［2024］8頁。

の法律行為であるけれども、少なくともリテール決済の分野における指図自体については、意思表示の瑕疵や欠缺に係る民法の規律の適用を受け、場合によっては若干の修正を施したうえで民法の規定の適用を受け、瑕疵の程度や性質等に応じて一定の場合には指図の効力を否定し、一定の場合には指図は有効ではあるが悪意者に対しては対抗できる抗弁事由と解すること等が検討されるべきであろう。無権限者による指図は、基本的に無効であると解したい。電子決済手段について、保有者からその移転を受けた者が、発行者に対して自らの権利を主張するためには、その前提として、前の保有者から適法な指図を受けたこと、かつ、予め定められた当該電子決済手段の移転の手続によってその移転を受けたことが必要である。前の保有者の指図に瑕疵があった場合、例えば指図が行為無能力者によってなされたものであったり、無権限者による指図がなされたりした場合には、有効な指図がなされていないと評価し、権利の移転が生じていないとして静的安全を保護することが考えられる。指図の意思表示の瑕疵や不存在を、例えば移転を受けた者が悪意である場合には移転の効力を否定し、あるいは抗弁として権利の主張を制限する等、より柔軟で適切な法的効果を導くことができるように思われる。無権利者からさらに当該電子決済手段を取得した者は、善意取得制度により保護する必要があり、善意取得を認めることが解釈論上困難な場合には、権利外観法理を用いる等、可能な限り解釈論上の努力をすべきである。

しかし、電子決済手段の民事法上の規律については、支配可能な電子データであることに着目した立法による整備が望ましい。日本においても、排他的な支配の取得をもって電子マネーの移転が生じること等を規定すべきであること等、私法上の論点を網羅した立法論が公表されている[70]。「支配」の意義についても、UNIDROITデジタル資産私法原則では、具体的な定義が置かれており[71]、諸外国や国際レベルで近年急速に発展している立法や立法論を参考に[72]、「支配」概念を中核とした電子決済手段あるいは、より一般化すべきであるとしたら支配可能な電子移転記録、さらにはデジタル資産一般についての民事法上の規律を整備することが望ましいと思われる。

電子決済手段の民事法上の規律について立法化する場合には、電子データ自体を価値と捉えるアプローチと、電子データにはデータ自体とは別に存在する権利が結合しているとするアプローチがありうる。前述したように、電子データそのものとは別にそれに表章された実体法上の権利もしくは法的地位があると理解する場合には、電子データとそれに表章されている権利は法的には独立していることを前提に検討を進めることが、柔軟で妥当な結論を可能にする所以であると考えられる。す

70 前掲脚注 62 および前掲脚注 63 とそれらに対応する本文参照。
71 前掲脚注 60 参照。
72 前掲脚注 61 参照。

なわち、有価証券的な規律すなわち電子データとそれに結び付いた権利とが法的には分離されているという前提のもとで、立法論を検討すべきであろう。指図と予め約定された方式による移転に基づいて、送金人から受取人に電子決済手段が消滅・発生構成によって移転すると考える場合には、善意取得制度や適切な抗弁制限制度の創設が必要になるであろう。

立法論に当たり、基本的には、岩原教授を中心とするこれまでの提言と UNIDROIT のデジタル資産私法原則を基礎に、電子決済手段の民事法上の規律のあり方について考察することが出発点になろう。なお、UNIDROIT の上記原則では、「支配」概念は法的概念ではなく事実上の概念であるとされるが、カストディアンによる電子決済手段の管理や担保化のこと等を考慮すると、間接占有に対応する「間接支配」の概念を導入する等、法的概念として構築する方向性も検討すべきであると思われる。電子データの支配可能性に着目し、電子決済手段の発行者の関与や管理がない状態で移転可能な P2P 型の電子決済手段について、その発生、移転、消滅、善意取得および抗弁の制限、支払免責等について、民事法上の規律のあり方を検討することになろう。立法論の具体的な展開は、他日を期したい。

参考文献

伊澤孝平、「指図（Anweisung）の本質（一）」、『法学協会雑誌』48 巻 11 号、1930 年、1〜50 頁

————、「指図（Anweisung）の本質（二・完）」、『法学協会雑誌』49 巻 6 号、1931 年、32〜72 頁

————、「指図の観念」、『法学』4 巻 4 号、1935 年、367〜393 頁

————、「指図の効果（1）」、『法学』5 巻 1 号、1936 年 a、1〜37 頁

————、「指図の効果（2・完）」、『法学』5 巻 2 号、1936 年 b、166〜201 頁

石井照久・鴻　常夫、『手形法・小切手法〔増補版〕』、勁草書房、1976 年

市古裕太、『デジタルマネービジネスの法務』、商事法務、2024 年

岩原紳作、『電子決済と法』、有斐閣、2003 年

大越有人、「電子記録移転権利（トークン表示権利）の第一項有価証券該当性について」、『商事法務』2206 号、2019 年、106〜112 頁

大隅健一郎・河本一郎、『注釈手形法・小切手法』、有斐閣、1977 年

大村敦志・道垣内弘人編著・石川博康・大澤　彩・加毛　明・角田美穂子・筒井健夫・幡野弘樹・吉政友広、『解説　民法（債権法）改正のポイント』、有斐閣、2018 年

小沢徹夫、「電子マネーの取引当事者間の法律関係と損失の配分（1）」、『NBL』623 号、1997 年、6〜12 頁

加毛　明、「決済手段の移転に関する私法上の法律問題―資金移動業電子マネーを中心として」、沖野眞已・丸山絵美子・水野紀子・森田宏樹・森永淑子編『これからの民法・消費者法（I）河上正二先生古稀記念』、信山社、2023 年、245〜271 頁

神作裕之、「判批〔商事判例研究〕資金不足を看過してなされた手形支払の効力」、『ジュリスト』1005 号、1992 年、96〜98 頁

金融審議会、「資金決済ワーキング・グループ報告」、金融庁、2022 年（https://www.fsa.go.jp/singi/singi_kinyu/tosin/20220111/houkoku.pdf、2024 年 10 月 31 日）

金融法委員会、「セキュリティ・トークンの譲渡に関する効力発生要件及び対抗要件について（特に匿名組合持分及び信託受益権の譲渡に関して）」、金融法委員会、2022 年（http://www.flb.gr.jp/jdoc/publication60-j.pdf、2024 年 10 月 31 日）

小出　篤、「『手形の電子化』と電子記録債権―UNCITRAL における『電子的移転可能記録』の検討から」、小出　篤・小塚荘一郎・後藤　元・潘　阿憲編『企業法・金融法の新潮流：前田重行先生古稀記念』、商事法務、2013 年、537〜570 頁

鈴木竹雄、『手形法・小切手法〔新版・前田　庸補訂〕』、有斐閣、1992 年

隅谷史人、『独仏指図の法理論』、慶應義塾大学出版会、2016 年

全国銀行資金決済ネットワーク、「全銀システム参加資格拡大の実現について」、全国銀行資金決済ネットワーク、2022 年（https://www.zengin-net.jp/announcement/

pdf/announcement_20221007.pdf、2024 年 10 月 31 日）
高橋康文編著、『新・逐条解説　資金決済法〔第 2 版〕』、金融財政事情研究会、2023 年
デジタルアセット共創コンソーシアム、「パーミッションレス型ステーブルコインの健全な導入・普及に向けた整理」、三菱 UFJ フィナンシャル・グループ、2022 年（https://www.tr.mufg.jp/ippan/pdf/permissionlesssc_rpt.pdf、2024 年 10 月 31 日）
デジタルマネーの私法上の性質を巡る法律問題研究会、「デジタルマネーの権利と移転」、『金融研究』 第 43 巻第 1 号、日本銀行金融研究所、2024 年、1〜48 頁
電子マネー及び電子決済に関する懇談会、「報告書」、金融庁、1997 年（https://www.fsa.go.jp/p_mof/singikai/kinyusei/tosin/1a1201.htm、2024 年 10 月 31 日）
電子マネーに関する勉強会、「電子マネーの私法的側面に関する一考察『電子マネーに関する勉強会』報告書」、『金融研究』 第 16 巻第 2 号、日本銀行金融研究所、1997 年、1〜45 頁
中田裕康、『債権総論（第 4 版）』、岩波書店、2020 年
日本銀行、「日本銀行が運営する資金決済システムに関する情報開示」、日本銀行、2023 年（https://www.boj.or.jp/paym/outline/pay_boj/pboj230731a.pdf、2024 年 10 月 31 日）
法制審議会商法（船荷証券等関係）部会、「商法（船荷証券等関係）等の改正に関する要綱案（令和 6 年 8 月 21 日）」、法務省、2024 年（https://www.moj.go.jp/content/001423391.pdf、2024 年 10 月 31 日）
法務省民事局参事官室、「民法（債権関係）の改正に関する中間的な論点整理（平成 23 年 4 月 12 日決定）」、法務省、2011 年（https://www.moj.go.jp/content/000074384.pdf、2024 年 10 月 31 日）
前田　庸、『手形法・小切手法』、有斐閣、1999 年
丸橋　透・松嶋隆弘編著、『資金決済法の理論と実務』、勁草書房、2019 年
森田宏樹、「電子マネーの法的構成（3）」、『NBL』 619 号、1997 年 a、30〜37 頁
————、「電子マネーの法的構成（5）」、『NBL』 626 号、1997 年 b、48〜56 頁
————、「（報告）電子マネーをめぐる私法上の諸問題」、『金融法研究』 15 号、金融法学会、1999 年、51〜90 頁
Law Commission, “Digital Assets: Consultation Paper,” Law Com No 256, Law Commission, 2022 (available at https://www.lawcom.gov.uk/project/digital-assets/、2024 年 10 月 31 日).
————, “Digital Assets: Final Report,” Law Com No 412, Law Commission, 2023 (available at https://www.lawcom.gov.uk/project/digital-assets/、2024 年 10 月 31 日).
————, “Digital Assets as Personal Property: Short Consultation on Draft Clauses,” Law Commission, 2024 (available at https://www.lawcom.gov.uk/project/digital-assets/、

2024 年 10 月 31 日).
FATF (The Financial Action Task Force), “FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins,” FATF, 2020 (available at https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf.coredownload.pdf、2024 年 10 月 31 日).
UNCITRAL (The United Nations Commission on International Trade Law), “Model Law on Electronic Transferable Records,” UNCITRAL, 2017 (available at https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/mletr_ebook_e.pdf、2024 年 10 月 31 日).
UNIDROIT (International Institute for the Unification of Private Law), “Principles on Digital Assets and Private Law,” UNIDROIT, 2023 (available at https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf、2024 年 10 月 31 日).

前払式支払手段をクレジットカードにより購入（チャージ）した場合の法律関係の整理

内山理映子（うちやまりえこ）／石岡佑太（いしおかゆうた）

要　旨

キャッシュレス決済サービスの利用が進展する中、日本では、後払いであるクレジットカードを利用して前払式支払手段を購入（チャージ）する決済サービスが広く利用されている。前払式支払手段とクレジットカードの取引は、いずれも、サービスの提供者、利用者、加盟店の三者による決済サービスであるが、利用者があらかじめ資金を支払う前払式支払手段と、利用者が与信を受けて資金を後払いするクレジットカードでは、規律する法律が異なるほか、それぞれの取引の法律構成についてもさまざまな考え方があり1つには定まっていない。こうした状況のもとで、各決済サービスの提供者が破綻した場合、利用者、加盟店のいずれが損失を負担することになるか、利用者が不利益を被る可能性はないかといった点を検討すると、法律構成によっては、必ずしも利用者が保護されない可能性があることがわかった。利用者が不測の損害を負うことなく、安定して決済サービスを利用できるようにするためには、サービスの提供者・利用者・加盟店間の法律関係をあらかじめ明確にしておくことが肝要である。

キーワード：前払式支払手段、クレジットカード、抗弁の接続、キャッシュレス決済、資金決済法、割賦販売法、破産法

本稿の作成に当たっては、片岡義広弁護士（片岡総合法律事務所）、神作裕之教授（学習院大学）、神田秀樹名誉教授（東京大学）、丸山絵美子教授（慶應義塾大学）（五十音順）の各氏および金融研究所スタッフから有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

内山理映子　日本銀行金融研究所企画役（現総務人事局企画役、E-mail: rieko.uchiyama@boj.or.jp）
石岡佑太　日本銀行金融研究所（E-mail: yuuta.ishioka@boj.or.jp）

1. はじめに

さまざまなキャッシュレス決済サービスの利用が進展する中、複数のサービスを組み合わせる場面がみられる。決済サービスのうち、利用者から決済サービスの提供者へ資金が移動するタイミングに着目すると、前払い・後払い・即時払いがあり、前払いの代表的なサービスとして前払式支払手段、後払いの代表的なものとしてクレジットカードがある。日本では、これらを組み合わせて、前払式支払手段をクレジットカードで購入（チャージ）するというサービスが広く利用されるようになっている。もっとも、それぞれのサービスにおいて適用される法律関係は異なる[1]。

「デジタルマネーの私法上の性質を巡る法律問題研究会」［2024］では、銀行、資金移動業者、前払式支払手段発行者などが提供するデジタルマネーを対象に、利用者が発行者に対して有する権利の性質や、デジタルマネーを移転する場合の法律構成、発行者や仲介者が破綻した場合の利用者の権利の処遇などについて検討が行われた。本稿では、同研究会では検討の対象外とされた、前払式支払手段を後払いであるクレジットカードでチャージする場合に、法律構成によって損失負担のあり方が異なりうるのではないかという点について、特に、決済サービスの提供者（クレジットカード発行会社（以下「カード会社」という）および前払式支払手段発行者（以下「前払式発行者」という）が破産した場合を取り上げて検討を行った。

安定的な決済サービスの利用に向けて検討すべき論点は複数あるが、本稿の具体的なリサーチ・クエスチョンは、それぞれの決済サービスについて複数の法律構成が考えられるもとで、法律構成によって損失負担の帰趨は異なるのか、仮に異なるとした場合、利用者が不利益を被る可能性などはないのかである。決済サービスの提供者の破綻のうち、再建型倒産手続による場合には決済サービスの事業の継続を前提に利用者の権利を検討することとなるが[2]、ここでは、損失負担の帰趨を考えるに当たり、破綻のうち破産に絞って事例を想定する[3]。日本では、前払式支払手段をクレジットカードで購入（チャージ）するサービスが広く利用されているところ、各決済サービスの提供者が破産した場合の損失負担の帰趨については必ずしも

1 銀行の口座振込、クレジットカード決済、電子マネー決済に共通性があること、他方、リテール決済の発展過程から、法規整が銀行法・資金決済に関する法律（以下「資金決済法」という）と割賦販売法に分断されている現状および各種決済サービスの横断的な分析の必要性を指摘したものとして、千葉［2019］9～17頁。

2 デジタルマネーの発行者が破綻した場合の利用者の権利について検討したものとして、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］37～38頁。

3 カード会社の破産事例は必ずしも多くはないとみられるが、前払式発行者について破産手続開始の申立て等が行われた場合に発行保証金の還付手続（資金決済法31条2項）が実施されたのは、前身となる「前払式証票の規制等に関する法律」施行日（1990年10月1日）から2023年6月末までに56件（金融庁［2023］534頁）。

明らかではない。そこで本稿では、こうしたサービスを利用する事例をベースに、前払い、後払いそれぞれの決済サービスの提供者が破産した場合の法律関係について比較検討を試みる。

2. クレジットカードと前払式支払手段をめぐる取引の概要

(1) 検討対象とするクレジットカード取引

クレジットカード取引は、割賦販売法の包括信用購入あっせん（割賦販売法 2 条 3 項）として規律される。もっとも、二月払購入あっせん（いわゆるマンスリークリア＜翌月一括払い＞）（同法 35 条の 16 第 2 項）は、一時的にカード会社から利用者への与信は発生するが、事務処理に伴う一時的な時間差と考えられるため[4]、包括信用購入あっせんの定義から除かれており（同法 2 条 3 項 1 号括弧書き）、割賦販売法の一部の規定のみが適用される[5]。

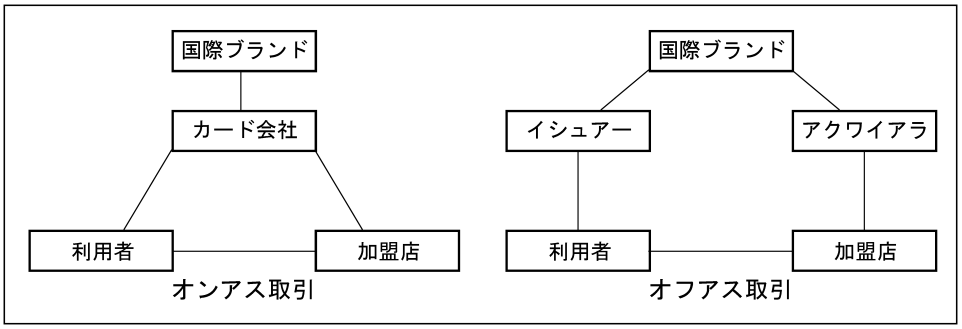
日本におけるクレジットカード取引では、利用の対価をマンスリークリアとする取引が、通常は手数料もかからず、広く決済手段として利用されている[6]。当初は、カード会社自身がクレジットカード加盟店（以下「カード加盟店」という）と契約する取引（オンアス取引）を前提として取引が始まったが、図 1 に示すように、近年、国際ブランドを通じてカード会社と加盟店契約会社（アクワイアラ）が異なる取引（オフアス取引）が一般化しているほか、決済代行業者が加盟店と加盟店契約会社の間に入る契約も増加してきているなど、複雑化している[7]。本稿では、議論を単純化することを優先して、カード会社、カード加盟店、利用者の三者によるマンスリークリアのオンアス取引について整理を試みる[8]。

(2) 検討対象とする前払式支払手段にかかる取引

前払式支払手段は、対価を得て発行される証票等であって、発行者等から物品の

4 小塚・森田［2018］184 頁。
5 犯罪による収益の移転防止に関する法律に基づく規制やクレジットカード番号等取扱業者としての規制には服する。
6 例えば、前払式支払手段の約款において、クレジットカードでチャージする場合の支払方法は 1 回払いとすることが定められているものがある。
7 小塚・森田［2018］182〜183 頁。
8 三者型（オンアス取引）の法律構成の議論は、基本的にはオフアス取引についても妥当する（経済産業省［2021］48 頁）。

図１　クレジットカード取引における当事者



資料：千葉［2019］7 頁を参考に筆者作成。

購入や役務の提供を受ける場合等に、これらの代価の弁済のために使用することができるもの（資金決済法 3 条 1 項）である。前払式支払手段には、発行者から物品の購入を行った場合等における弁済に使用できる自家型（同法 3 条 4 項）と、発行者以外の加盟店（以下「前払式加盟店」という）からの物品の購入等に使用できる第三者型（同法 3 条 5 項）がある。

本稿では、幅広い相手に対して利用できる決済サービスであり、クレジットカードによるチャージが可能なサービスも広くみられる第三者型前払式支払手段を検討の対象とする。

なお、前払式発行者には、利用者資金保護の観点から、資金決済法により資産保全義務（未使用残高の 2 分の 1 以上の額を保全。同法 14〜16 条）が課されており、利用者は発行保証金に対して優先弁済権を有する（同法 31 条 1 項）。

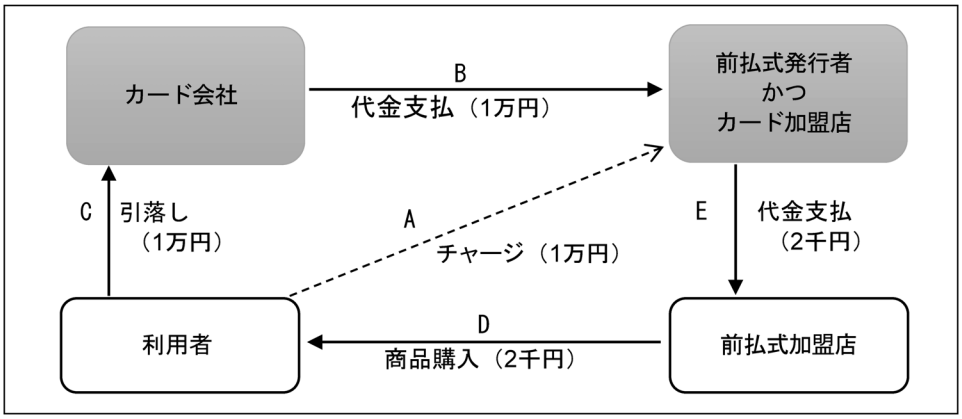
3.　設例の検討

(1)　想定する取引の流れ

前払式支払手段の購入（チャージ）をクレジットカードで行った場合について、次のようなケースを想定する。

クレジットカード取引については、利用者・カード会社・カード加盟店の三者が、前払式支払手段の取引については、利用者・前払式発行者・前払式加盟店の三者が登場する。前払式支払手段のチャージをクレジットカードにより行う場合、前払式

図２　前払式支払手段をクレジットカードによりチャージする取引の流れ



発行者は、クレジットカード取引においてはカード加盟店となる[9]。具体的な取引の流れは、図２のとおりとなる。

A：利用者が、クレジットカードを利用して前払式支払手段として１万円をチャージし、前払式支払手段の発行を受ける。
B：カード会社は、カード加盟店（前払式発行者）に対して、カード利用代金（１万円）を支払う。
C：カード会社は、利用者に利用代金の支払を請求し、利用者の銀行口座から代金（１万円）を引き落とす。
D：利用者が、前払式加盟店において商品（２千円）を購入する。
E：前払式加盟店は、前払式発行者に２千円の支払を請求し、前払式発行者から支払を受ける。

取引の時系列としてはさまざまなパターンがありうるが、基本的にはクレジットカードでのチャージに関する取引（ABC）と、前払式支払手段での商品購入に関する取引（ADE）の組合せとなる[10]。

9　以下では、前払式支払手段の発行者を、文脈に応じて、「前払式発行者（カード加盟店）」または「カード加盟店（前払式発行者）」と表記する。

10　チャージ（A）から、カード加盟店への支払（B）と利用者からの代金引落（C）までにタイムラグがあるため、実際にはまだ前払いされていない段階で、利用者が前払式支払手段を利用した商品の購入（D）とその代価の前払式加盟店への支払（E）を行うケースもある。なお、カード加盟店への代金支払（B）のタイミングは、取決めによってさまざまではあるが、一例を挙げると、月２回の支払（月初から15日までの請求分を月末に入金。16日から月末までの請求分を翌月15日に入金。）などがある。前払式加盟店への代金支払（E）も同様である。利用者からの代金引落についても取決め次第だが、前月16日から当月15日までの利用代金を、翌月10日に口座から引き落すといった例がある。

(2) 取り上げる設例

本稿では、決済サービスの提供者たるカード会社または前払式発行者が破産したケースとして、カード加盟店への支払（B）を履行する前にカード会社が破産した場合と、前払式加盟店への支払（E）を履行する前に前払式発行者が破産した場合を設例として取り上げる[11]。

（設例 1）利用者がクレジットカードを利用して前払式支払手段として 1 万円をチャージした（A）後、カード会社がカード加盟店（前払式発行者）にカード利用代金（1 万円）を支払う（B）前に破産。

（設例 2）利用者がクレジットカードを利用して前払式支払手段として 1 万円をチャージし（A）、前払式加盟店で 2 千円の商品を購入した（D）後に、前払式発行者が破産。この際、カード会社からカード加盟店（前払式発行者）へのカード利用代金（1 万円）の支払（B）、カード会社による利用者口座からのカード利用代金（1 万円）の引落し（C）、および前払式発行者から前払式加盟店への商品代金（2 千円）の支払（E）のいずれも未了であった[12]。

4. 設例 1：カード会社の破産

(1) カード加盟店（前払式発行者）の請求

カード加盟店（前払式発行者）は、カード会社が破産し、チャージの代価である 1 万円が入金されていない場合、カード会社の代わりに利用者に対して直接 1 万円の請求（直接請求）を行うことは可能であろうか。

11 なお、利用者が破産した場合、通常はカード会社が利用者のカード利用代金相当額の損失を負担することとなる。また、前払式加盟店が破産した場合には、前払式支払手段で商品等を購入した時点（D）以降が問題となるが、前払式発行者は前払式加盟店の破産管財人に商品等の代金を支払う（E）ことが見込まれる。

12 前払式発行者破産時に、前払式発行者・前払式加盟店・利用者の三者間において、前払式加盟店と利用者のいずれが損失を負担することとなるかを検討するため、前払式加盟店に 2 千円の支払が行われる（E）前の時点としている。また、クレジットカードによる後払いでチャージを行っていることで、即時払いとどのような違いが生じるかを検討するため、クレジットカードの取引における利用者からカード会社、カード会社からカード加盟店への資金の移転（B・C）が完了する前の時点を取り上げる。

クレジットカード取引の法律構成については、割賦販売法は特定の法律構成を前提とした定めとはなっておらず、これまでさまざまな考え方が議論されてきた[13]。経済産業省［2021］48頁によれば、現行の契約実務上は、大別して債権譲渡構成と立替払構成の2つが存在するとされており、実際の約款でも、これら2つのいずれかまたは両方に言及しているものが多い。このため、これら2つの法律構成を前提に、現在確認できる各社の約款等を踏まえつつ、法律構成によって直接請求の可否が異なるか、検討を行う。

イ．クレジットカード取引の法律構成

（イ） 債権譲渡構成

債権譲渡構成とは、カード会社とカード加盟店との間において、カード加盟店が利用者に対して有する代金債権の有償譲渡が行われ、カード会社が事後的に利用者に対してこの代金債権を行使して代金を回収するという構成である。この構成をとる場合、債権譲渡の当事者であるカード会社とカード加盟店との間の加盟店規約において、債権譲渡の規定が設けられる。実際には、カード会社からカード加盟店に対して債権譲渡の対価が一括で支払われ、その後、利用者がカード会社に対して代金債務を支払う[14]。

利用者がカード加盟店においてクレジットカードを提示して商品を購入する取引は、①カード加盟店が利用者から提示されたカードの利用について、専用の決済端末を通じてカード会社から承認（オーソリゼーション）を得て[15]、②カード加盟店がカードの利用により発生した売上代金について、カード会社に売上データを送信する（クリアリング）[16]という流れとなる。この場合、カード加盟店が、カード会社から承認（オーソリゼーション）を得たことを前提に利用者のカード利用を承認した時点で、カードにより支払をすることが認められる。このことを踏まえ、以下では、債権譲渡の効力発生時期は、カード加盟店が利用者にカード利用を承認した時点であるとして、検討を進める[17]。

債権譲渡構成の場合、カード利用が承認された時点でカード会社が債権者となる

13 割賦販売法上の「包括信用購入あっせん」は、取引形態に着目して定義されており、契約形態には触れられていない。これは契約形態のいずれかに偏して定義付けを行うと容易に脱法が可能となることから、法律構成に依存せず、実質的に同様の経済的効果をもたらす取引行為自体に着目したものであるとされる。経済産業省［2021］46〜48頁。

14 経済産業省［2021］48頁。

15 ①オーソリゼーションと、②売上決済にかかる電文が分かれる方式が一般的であるが、これらが同時に伝送される場合もある。山本［2012］89頁、122〜125頁。

16 山本［2012］89〜90頁、129〜131頁。

17 本稿はオンアス取引を前提とした検討にとどまるが、オフアス取引を前提にした場合、オーソリゼーションによってイシュアーにより免責的債務引受がされ、クリアリングによりアクワイアラが加盟店のイシュアーに対する債権の買取りをしている（債権譲渡がされる）との指摘がある。玉垣［2017］52頁。

ことから、カード加盟店は債務者である利用者に対して代金を請求することはできない。

（ロ） 立替払構成

カード会社各社の約款等では、「立替払」という用語が定着している[18]が、立替払の概念は一義的には明確でなく[19]、その法律構成をどのように解するかについてもさまざまな考え方がありうる。ここでは、経済産業省[20]で取り上げられているところをもとに、①第三者弁済構成および②債務引受構成のほか、③更改構成について検討を行う。

①第三者弁済構成は、カード会員規約に基づいて、カード会社が利用者のクレジットカード利用代金をカード加盟店に支払うことにより、利用者の代金債務を第三者弁済する（民法474条）という法律構成である。カード会社は立替金の支払により、利用者に対し、カード会員規約に基づく立替金支払にかかる求償権を取得し、利用者は、立替金相当額の金銭をカード会社に支払うこととなる。この構成によれば、第三者弁済を行う約定はあくまで利用者とカード会社間の契約関係に過ぎないことから、カード加盟店は売買代金の支払が未了の場合には、債務者たる利用者にチャージ代金を請求することが可能である[21]。

②債務引受構成には、(i) 免責的債務引受構成（民法472条）と (ii) 併存的債務引受構成（民法470条）があり、いずれの構成であるかは当事者の合理的意思解釈によって決せられるとされる[22]。また、いずれの場合であっても、債務の引受人は原債務と同一の債務を負担する（すなわち、カード加盟店は、債務の引受人たるカード会社に直接の請求権を有する）[23]。

債務引受の効力は、(i) 免責的債務引受構成については、(a) 債権者と引受人となる者との契約によってするときは、債権者が債務者に通知することによって発生するが（民法472条2項）、(b) 債務者と引受人となる者が契約し、債権者が引受人となる者に対して承諾することによっても発生する（民法472条3項）。クレジットカード取引における債務引受の効力が (a)、(b) のどちらによって発生するかは、個別の加盟店規約や会員規約の定めによる。すなわち、(a) については、カード加盟店（債権者）とカード会社（引受人となる者）との契約（加盟店規約）において、カード利用によってカード会社が利用者の債務を引き受ける旨を定めていることを前提に、具体的な商品等の購入に際し、カード加盟店（債権者）が利用

18 経済産業省［2021］48頁。
19 清水［1974］300頁。
20 経済産業省［2021］48頁。
21 ただし、カード会社・利用者間およびカード会社・カード加盟店間の規約によって、平時においては、まずカード会社に請求するものとされていると考えられる。
22 経済産業省［2021］49頁。
23 経済産業省［2021］49頁。

者（債務者）にカード利用を承認することをもって、債務者に対する通知があったと考えられる[24]。一方、(b) については、利用者（債務者）とカード会社（引受人となる者）間の契約（会員規約）において、利用者がカードを利用して購入した商品の代金債務をカード会社が引き受ける旨の契約（立替払）が締結されていることを前提に、具体的な商品等の購入に際して、カード加盟店（債権者）がカード会社（引受人となる者）に売上データを送信することをもって、債務引受の効力が生じると考えられる。そうだとすれば、(a)、(b) のいずれの場合であっても、債務引受の効力はカード利用時に発生することとなる。

(ii) 併存的債務引受構成については、(c) 債権者と引受人となる者との契約によって発生し（民法 470 条 2 項）、または (d) 債務者と引受人となる者が契約し、債権者が引受人となる者に対して承諾することによっても発生する（民法 470 条 3 項）。(c) については、カード加盟店（債権者）とカード会社（引受人となる者）との契約（加盟店規約）において、カード利用によってカード会社が利用者の債務を引き受ける旨を定めていることを前提とすると、カード加盟店（債権者）によるカード利用の承認時に債務が引き受けられると考えられる。(d) については、(b) と同様に考えられる。(c)、(d) のいずれの場合であっても、債務引受の効力はカード利用時に発生することとなる。

以上を踏まえると、(i) 免責的債務引受構成、(ii) 併存的債務引受構成による具体的な帰結は次のとおりとなる。

まず、(i) 免責的債務引受構成では、利用者は、カード会社が債務引受を行ったことにより、カード加盟店に対する代金債務について免責される。カード加盟店は、カード会社が引き受けた代金債務にかかる債権を取得し、カード会社は、利用者に対し、カード会員規約に基づく立替金支払にかかる求償権を取得する。これにより、利用者は立替金相当額の金銭をカード会社に支払うこととなる[25]。なお、免責的債務引受の効力が発生して以降は、利用者はカード加盟店に対する代金債務について免責されることから、カード加盟店は利用者に対して代金を請求することはできない。

これに対して、(ii) 併存的債務引受構成では、利用者のカード加盟店に対する代金債務について、利用者とカード会社が併存的に債務者となることから、利用者とカード会社は同一の債務を負担することとなる。この場合、利用者はカード加盟店に対する代金債務について免責されず、カード加盟店は、利用者に対して代金を請求することが可能である[26]。

24 片岡［2021］80 頁では、カード加盟店がカード会社のオーソリゼーションを得て、クレジットカードによる支払を利用者に承諾したときに、免責的債務引受の効力として利用者の加盟店に対する債務が消滅すると考えられることを指摘している。

25 経済産業省［2021］49 頁。

26 第三者弁済構成と同様、カード会社・利用者間およびカード会社・カード加盟店間の規約によって、

最後に、③更改構成について考察する。具体的には、(i) 債権者の交代（債権者がカード加盟店からカード会社に交代）による更改（民法 515 条 1 項）と、(ii) 債務者の交代（債務者が利用者からカード会社に交代）による更改（民法 514 条 1 項前段）が存在する[27]。

更改の効力が発生する時期については、カード会社とカード加盟店間の契約（加盟店規約）とカード会社と利用者間の契約（会員規約）がともに締結されていることを前提とすると、(i) 債権者の交代の場合は、カード会社がカード利用を承認（オーソリゼーション）し、カード加盟店が利用者にカード利用を承認した時点で、カード会社・カード加盟店・利用者の三当事者間の合意が成立（民法 515 条 1 項）したと解することができるのではないか。また、(ii) 債務者の交代による更改の場合は、カード加盟店とカード会社間の契約（加盟店規約）においてカード会社がカードの利用代金にかかる債務を負うことを定めていることを前提に、カード加盟店が利用者にカード利用を承認した際に更改契約をした旨の通知（民法 514 条 1 項後段）があったと解し、この時に更改の効力が発生したと考えられる。

いずれにせよ、更改の効力が発生した後は、カード会社が新たな債務の債務者となり、従前の債務は消滅するため、カード加盟店は利用者に対して代金を請求することはできない。

ロ．法律構成を踏まえた検討

イ．でみたとおり、カード加盟店が利用者に対して直接請求が可能となりうるのは、立替払構成のうち、第三者弁済構成と併存的債務引受構成の場合である。加盟店規約等において、利用者への直接請求の禁止が明記されているものもあるが[28]、そうした文言が必ずしもすべての規約等に含まれているわけではない。こうした中で、かつクレジットカード取引がこれらのいずれかの法律構成によっていると評価できるのであれば、設例 1（カード会社が破産した場合）において、カード加盟店（前払式発行者）は、利用者に対してカード利用代金（1 万円）を請求しうることとなる。これに対して、債権譲渡構成、免責的債務引受構成および更改構成の場合には、カード加盟店が利用者にカード利用を承認した時点でそれぞれの効力が発生するとすれば、カード加盟店は利用者に対して代金を請求することはできないと考えられる。

以上のように考えたうえで、実際のカード会社各社の規約等をみると、「立替払」との記載のあるものが多いようであるが、当該記載に加えて「債権譲渡」の文言が

平時においては、まずカード会社に請求するものとされていると考えられる。

27 片岡［2021］82～83 頁参照。

28 例えば、カード加盟店において信用販売の手続きが完了した以降は、カード会社がカード加盟店に対する立替払を完了したか否かを問わず、利用者に対して商品等の代金を直接請求する権利を行使しない等と定めているものがある。

併記されているものも複数みられる。また、「立替払」と書かれているものであっても、法律構成としてそれが何を指すかは、規約等の文言から必ずしも明らかではない[29]。このように、現行の規約等は特定の法律構成に依拠した規定とはなっておらず、債権譲渡構成と立替払構成が混在している状況にある[30]。

こうした中、仮にカード会社が破産した場合、クレジットカード取引の法律構成が立替払構成のうち第三者弁済構成ないし併存的債務引受構成であることを理由として、カード加盟店が利用者に対して直接請求を行う可能性もあると考えられる[31]。その際、利用者は、カード加盟店から受けた請求の当否を判別できない中、①支払を拒んだ場合には債務不履行となるリスクがあるほか、②支払を行っても、クレジットカード取引の法律構成が債権譲渡構成、立替払構成のうち免責的債務引受構成または更改構成であることを理由として、カード会社の破産管財人から請求を受ける可能性があるという、法的に不安定な立場に置かれる可能性がある。こうした場合の利用者の対応策として供託を行うことも可能であるが、利用者の予測可能性を高めるためには、契約上、あらかじめ法律関係が明確になっていることが望ましい。そのうえで、①や②のような事態を回避するためには、債権譲渡構成、立替払構成のうち免責的債務引受構成または更改構成を前提として、カード加盟店が利用者に直接請求することはできないことをあらかじめ規約等で明確にしておくことが考えられる[32]。

こうした対応が望ましいことは、次のようなクレジットカード取引の実態からも肯定されるように思われる。すなわち、利用者としては、カード利用に伴う支払は、口座引落などを通じてカード会社に対して行われることで完結するものであり、カード加盟店に対して支払を行う必要はないとの認識を持つのが自然である。したがって、カード会社による口座引落の前であっても、よもやカード加盟店から直接請求を受けることは想定しておらず、仮にこうした請求が行われれば、利用者にとって不意打ちとなる。また、カード加盟店がカード会社から支払を受けると、カード加盟店が利用者に対して請求することはなくなるところ、カード会社から

29 契約当事者の合理的な意思解釈によるとされる。経済産業省［2021］48頁。

30 加盟店相互開放（国際ブランドの提供する決済業務を介して、他のカード会社が提携する加盟店を利用することができること）が進むもとで、立替払構成をとるカード会社の加盟店において、債権譲渡構成をとるカード会員によるカード利用が生じること、またはその逆が生じること等を背景に、さまざまな法律構成が混在している状況にあるという指摘がある。吉元［2015］39頁、350～351頁。

31 本稿では、カード会社・カード加盟店・利用者の三当事者によるオンアス取引を検討の対象としているが、実際には、オフアス取引が広く行われているほか、カード加盟店とカード会社の間に決済代行業者が当事者として加わる場合もある。カード会社とカード加盟店の間に入る決済代行業者の破産により、代金を受領していない加盟店が債権譲渡を取り消して、利用者に請求する可能性について言及したものとして、吉元［2015］355頁。

32 なお、利用者がカードによる支払を行った場合について、カード会社が当該債務を免責的に引き受けることを明示し、利用者はカード加盟店に対して代金債務を負わない旨を明示的に規定している加盟店約款もみられた。

カード加盟店への支払が行われる時期は、両者間の契約（加盟店規約）によって定まっており、利用者はこれに関知しえない。このため、利用者が、カード加盟店からの請求が正当な請求として認められるかどうかを外形的に判断するのは困難である。

また、カード会社としては、カード加盟店から利用者に対して直接請求を行いうるとなると、カード加盟店が利用者から直接支払を受けた金額について、カード会社からカード加盟店へ支払う金額から控除するといった対応などを求められる可能性もある。しかしながら、こうした正規のキャンセル手続を踏まないかたちでの対応を認めると、余計な事務コストが生じて取引の効率性が阻害されるほか、誤払い・誤引落しなどの事務ミスの原因ともなりうる。こうしたことから、カード会社においても、カード加盟店から利用者への直接請求は想定していないと考えられる[33]。

以上のような考え方は、クレジットカードを利用して前払式支払手段にチャージする場合についても同様に当てはまる。

(2) 利用者の対応

クレジットカード取引の法律構成が必ずしも明確ではない中、利用者としては、法的に不安定な状況を解消するために、破産したカード会社が発行したクレジットカードを利用した取引を、カード加盟店との間で合意により解除することが考えられる。平時においてはこうした合意解除が認められることを前提に、約款等においてその手続が定められており、カード加盟店と利用者の間で売買契約等の解除を行い、カード加盟店からカード会社に当該解除について連絡を行ったうえで、利用代金の引落しのキャンセル、または、すでに引落しが行われている場合には返金処理が行われる、という流れとなる。こうした解除が可能であれば、それ以降、利用者はカード会社やカード加盟店からクレジットカード利用に関して請求を受けることはない。

もっとも、カード会社の破産時においても、こうした解除を利用者とカード加盟店の間で行い、利用者がクレジットカード取引の法律関係から抜け出すことができるかは不明確である[34]。

また、設例 1 において、利用者がクレジットカードで購入したのは前払式支払手

33 割賦販売法の枠組みをみると、包括信用購入あっせんが登録制とされ（同法 31 条）、資本金（最低額 2 千万円以上＜同法 33 条の 2 第 1 項 3 号、同法施行令 5 条 2 項＞）や純資産（純資産比率が 90％以上＜同法 33 条の 2 第 1 項 4 号＞）といった要件が課されている。登録制の趣旨は包括信用購入あっせん業者の財産状態の健全性を確保し、カード加盟店が確実に代金等の回収を行うことができるようにするためであるとされている。経済産業省［2021］192 頁。

34 割賦販売契約において売買契約と立替払契約を別個のものとしている後述（5 節（3）ロ.）の最高裁

段であり、仮に解除による返金等が行われると、保有者に対する前払式支払手段の払戻しを禁止する規定（資金決済法 20 条 5 項）との関係についても、検討を要すると考えられる。

5. 設例 2：前払式発行者の破産

(1) 前払式加盟店の請求

設例 2 において、前払式加盟店は、利用者が 2 千円の商品を購入した（D）後、前払式発行者から 2 千円の支払を受ける立場にある（E）。もっとも、前払式発行者が破産した場合には、十分な弁済を受けることができない可能性がある[35]。この場合、前払式加盟店は、前払式発行者の破産により十分な弁済を受けられないことを理由に、利用者に対して商品の代金（2 千円）を直接請求することは可能であろうか。この点、前払式支払手段についてもこれまでさまざまな法律構成が議論されていることから、以下では、それぞれの法律構成について整理したうえで、前払式加盟店の利用者に対する請求の可否について検討する。

イ. 前払式支払手段の法律構成

（イ） 債権譲渡構成

債権譲渡構成としては、利用者がチャージにより前払式発行者に対して有する金銭債権を前払式加盟店に対する代金債務の代物弁済[36] として利用者から前払式加盟店に譲渡すると考える構成[37] のほか、4 節（1）イ.（イ）のクレジットカード取引の法律構成における債権譲渡構成とパラレルに考え、前払式加盟店が利用者に対して有する取引代金債権が、前払式支払手段を利用した場合に前払式発行者に譲渡さ

判例（最判平成 2 年 2 月 20 日判時 1354 号 76 頁）を前提にすれば、売買契約を解除しても、利用者とカード会社間の立替払契約に基づく請求を拒むことは難しいという結論になる。また、解除をカード会社の破産管財人に対して主張できるかという問題がある（民法 545 条 1 項但書き）。

35 発行保証金に対して優先弁済権を有するのは前払式支払手段の保有者であり（資金決済法 31 条 1 項）、前払式加盟店はこれに含まれない。

36 小塚・森田［2018］23 頁では、電子マネーによる支払の法的性質について、約款に「加盟店に対しては電子マネーにより代金の支払いができる」と定められているところを文字通りに読めば、電子マネーという電子データの移転による代物弁済（民法 482 条）を加盟店が包括的に承諾していると考えられると指摘されている。電子マネー自体の法的性質については議論があるところ（債権であるとする説、一種の価値と捉える説などがある）ではあるが、本稿では立ち入らない。

37 電子マネーに関する勉強会［1997］23 頁、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］17 頁。

れるという構成も指摘されている[38]。債権譲渡の効力は、利用者が前払式支払手段を前払式加盟店での支払に利用した時点で発生すると考えられる。

設例2について債権譲渡構成を適用した場合には、前者の考え方によれば、利用者が前払式加盟店において前払式支払手段（2千円分）を利用した時点で、利用者が前払式発行者に対して有する2千円分の金銭債権が前払式加盟店に代物弁済として譲渡され、利用者の前払式加盟店に対する代金債務は消滅する。また、後者の考え方によれば、利用者が前払式加盟店において前払式支払手段（2千円分）を利用した時点で、前払式加盟店が利用者に対して有する2千円分の取引代金債権が前払式発行者に譲渡され、利用者の前払式加盟店に対する代金債務は消滅する。このため、いずれの考え方をとっても、前払式支払手段を利用した時点以降、前払式加盟店は利用者に対して直接請求することはできない。

（ロ） 免責的債務引受構成

免責的債務引受構成では、①前払式発行者と前払式加盟店との間の契約（加盟店規約）において、利用者が将来、前払式加盟店に対して負う代金債務を前払式発行者が免責的に引き受ける（民法472条）旨の包括的合意があり、当該合意のもとで利用者が前払式支払手段の発行を受けることにより債務引受契約が成立、②利用者が前払式支払手段を利用した時点で、前払式発行者が利用者の前払式加盟店に対する代金債務を免責的に引き受け、その後、前払式発行者が前払式加盟店に代金を支払う、という構成をとる[39]。免責的債務引受の効力発生時期は、利用者が前払式加盟店において前払式支払手段を利用した時点と考えられる。

設例2について免責的債務引受構成を適用した場合、利用者が前払式加盟店において前払式支払手段を利用した時点で、利用者の前払式加盟店に対する代金債務（2千円）は前払式発行者に免責的に引き受けられることにより消滅する。このため、その時点以降、前払式加盟店は利用者に対して直接請求することはできない。

（ハ） 支払委託構成

支払委託構成では、利用者と前払式発行者の間において、利用者があらかじめ前払式発行者に提供した資金を用いて代金債務を弁済してもらうという委託関係があると考える。そして、前払式加盟店と前払式発行者の間の契約（加盟店規約）において、利用者が将来、前払式加盟店に対して負う代金債務については、利用者からの委託に基づき前払式発行者が弁済する旨の包括的合意があると整理される。実際には、前払式発行者は、前払式加盟店から受領した売上情報に基づいて前払式加盟店への支払を行うこととなり、当該支払が行われるまでは、利用者の前払式加盟店

38 杉浦・片岡［2003］24頁。
39 電子マネーに関する勉強会［1997］22頁、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］16～17頁。

に対する債務は消滅しない[40]。

設例 2 について支払委託構成を適用した場合には、利用者は、前払式発行者に対して前払式加盟店に対する債務の弁済を委託しているものの、前払式発行者による前払式加盟店への支払は完了しておらず、利用者の前払式加盟店に対する債務も消滅していない。そこで、前払式発行者の破産手続開始決定があると、利用者・前払式発行者間の委託関係は終了し（民法 653 条 2 号）、前払式加盟店は、破産した前払式発行者の代わりに利用者に対して直接請求することも可能という帰結となる。

ロ．法律構成を踏まえた検討

上記イ．でみた前払式支払手段の法律構成のうち、どの法律構成が妥当かとのコンセンサスは今のところ確立されていない。前払式発行者と利用者の間の契約（会員規約）をみると、中には、利用者が前払式加盟店で商品を購入した際に、前払式支払手段が利用者から前払式加盟店へ移転し、当該移転がシステム上完了した旨の表示がされた時点で、支払が完了（利用者の債務が消滅）することを定めているものがみられる。また、前払式発行者と前払式加盟店の間の契約（加盟店規約）には、商品等の代金額に相当する前払式支払手段にかかる情報の移転が完了した時点や、アカウント内の残高の減算が完了した時点で、利用者の前払式加盟店に対する代金債務が消滅するといった定めがみられる。さらに、プリペイド・カードを利用した時点で利用者の前払式加盟店に対する債務を前払式発行者が免責的に引き受けることを明示している定めもみられる[41]。

こうした内容が規約等において明記された取引であれば、商品購入に際して前払式支払手段による支払を行い、それに相当する残高がアカウントから減算されれば、利用者の前払式加盟店に対する債務は消滅していると解釈でき、その時点以後は、前払式加盟店から利用者に対する請求を行うことはできないこととなる。

もっとも、すべての規約等において、前払式支払手段が利用された時点で利用者が前払式加盟店に対する債務を免れる旨が明記されているわけではない。このため、こうした点が規約等で明らかではないケースでは、前提となる法律構成次第で、利用者に対して代金請求を行うことができる主体は変わりうる。

利用者としては、既に発行されて自らのアカウントに残高として記帳されている前払式支払手段を利用した後、前払式発行者とは別に前払式加盟店から支払を求め

40 電子マネーに関する勉強会［1997］22 頁、デジタルマネーの私法上の性質を巡る法律問題研究会［2024］17 頁。

41 前払式証票の規制等に関する法律を受けて作成されたプリペイド・カード取引標準約款等において、プリペイド・カードを利用した場合、加盟店は、カードを利用した所持者の代金支払を免責する旨を規定している（プリペイド・カード加盟店規約例 2 条）。この趣旨は、前払式発行者が代金決済をした時ではなく、プリペイド・カードを利用した時に利用者が免責を受けると規定することで、利用者が前払式発行者だけではなく前払式加盟店からも請求を受けることによる二重払いを強いられることがないようにするためとされている。片岡［1991］161 頁。

られるとは、通常、想定していないであろう。前払式支払手段の利用者の多くが一般消費者であることを踏まえると、こうした前払式加盟店から利用者への請求を認めることは、消費者保護の観点からも適切でないように思われる。

なお、前払式支払手段は「対価を得て発行される」（資金決済法 3 条 1 項）ものであり、チャージする際の入金と前払式支払手段の発行が同時に行われるのが基本である。ここで、同条のいう「対価」とは、必ずしも現金に限られず、経済的な価値があるものはすべて含まれるという解釈[42]を前提とすれば、利用者がクレジットカードを利用することにより前払式発行者（カード加盟店）が獲得する代金債権についても、「対価」に該当することとなる。そうだとすれば、利用者の前払式加盟店に対する債務の存否は、チャージ手段がクレジットカードであるか現金であるかにかかわらず、前払式支払手段の法律構成によって決まるべきものと考えられる。

そして、利用者保護の観点からは、前払式支払手段の取引における法律構成については、利用者が前払式支払手段を利用した時点で利用者の前払式加盟店に対する債務が消滅するとする、債権譲渡構成または免責的債務引受構成とすることが適当と考えられる。また、特定の法律構成が妥当するとまではいえなくても、少なくとも規約等において、利用者が前払式支払手段を利用した時点以降は、利用者は前払式加盟店との関係では免責される旨を明らかにすることが望ましいであろう[43]。

(2) カード会社の対応（加盟店契約の解除の可否）

前払式発行者が破産した場合には、現金でチャージした利用者は、前払式発行者に対する権利（未使用残高相当分）について、発行保証金の還付手続（資金決済法 31 条 2 項 2 号）により優先弁済を受けることとなるが、供託義務が未使用残高の 2 分の 1 以上であることとの関係で全額の弁済を受けられない場合には、残額について破産手続によって権利を行使することとなる。

もっとも、設例 2 ではクレジットカードによる支払を選択したため後払いとなっており、いまだ利用者はチャージ代金相当分の 1 万円の支出を負担していない。利用者としては、未使用残高に相当する金額の支払を行わないという主張が可能であれば、チャージ代金のうち 8 千円について、損失負担を免れることができることとなる。

このように利用者が支払を拒めるか否かを検討する前に、まず、クレジットカード取引の仕組みにおいて、カード加盟店が破産した場合にカード会社はどのような

42 高橋・堀・森［2023］103 頁。

43 第三者型前払式支払手段については、利用者保護の観点に加え、決済手段として広く用いられるため、前払式加盟店を保護する観点から、発行者の登録制（資金決済法 7 条）や純資産額要件（同法 10 条 1 項 2 号）が定められている。

対応をとることとなるかについて確認する。

カード会社は、まず（i）破産したカード加盟店に対する支払を選択することができる。この場合には、カード会社は、利用者に対して1万円を請求することになる。このほか、（ii）カード加盟店の破産を受けて、加盟店契約を解除する、またはカード加盟店に対する未払分の支払を留保するという選択肢も取りうる。カード会社各社の加盟店規約をみると、カード加盟店が破産申立てを受けたことを理由とする解除または支払留保にかかる条項が含まれているものが多い。

(3) 前払式発行者と利用者の関係

イ. 不安の抗弁権

カード会社が、上記（ii）の対応を採った場合には、カード加盟店（前払式発行者）の破産管財人としては、設例1で検討したクレジットカード取引の法律構成のうち、第三者弁済構成や併存的債務引受構成を前提に、直接利用者に履行を求めることが考えられる。このとき、利用者としては、既に商品の購入に利用した2千円は支払うとしても、8千円については、破産したカード加盟店（前払式発行者）の提供する決済サービスにおいて前払式支払手段を利用するのが困難であることを理由に、支払を拒むことはできないだろうか。

ここで考えられる利用者の主張として、不安の抗弁権がある。不安の抗弁権とは、当事者の一方が先履行を約束した双務契約において、相手方に信用不安・財産状態の著しい悪化等の事態が生じ、反対債務の履行を受けられない可能性（反対給付リスク）が生じた場合に、双務契約における両債務間の対価的牽連関係を考慮に入れ、信義則を媒介にして、先履行義務者が自らの先履行を拒絶することができる権利をいう[44]。

不安の抗弁権については、下級審裁判例において認められたケースはあるが[45]、民法に直接の規定が設けられているわけではなく、これを制度としてどのように捉えるかは解釈論に委ねられている[46]。不安の抗弁権が認められる要件として、①先履行の合意があること、②反対給付リスクの現実化、③両当事者が予見することができなかった事情を挙げる考え方があり、これらを満たす効果として、履行の拒絶が認められるとされている（なお、損害賠償・解除の可否については議論がある）[47]。

44 潮見［2017］312頁以降。
45 東京地判平成2年12月20日判時1389号79頁など。
46 潮見［2017］318頁。なお、法制審議会民法（債権関係）部会でも規定の新設が議論されていたが、最終的に明文化は見送られている。
47 潮見［2017］311～326頁。

上記の①から③の要件を設例 2 に則してみると、①前払式支払手段は、本来は利用者が先履行義務（先に対価を支払う）を負うことが前提とされているもとで、②前払式発行者の破産[48] により、未使用残高が使用できない可能性が高く、③前払式発行者の破産は両当事者とも予見することができなかった事情である、といえる。そうだとすれば、利用者としては、まずは前払式発行者に対して不安の抗弁権を主張し、支払を拒む余地も認められるべきではないかと考えられる。特に、前払式支払手段の法律構成が明確ではなく、前払式加盟店が利用者に請求権を有するか否か、また前払式発行者の利用者に対する債務が未履行か既履行かが明らかではない時点では、まずは履行を拒絶することに意義があると考えられる[49]。この場合には、設例 2 において利用者から前払式発行者に対する履行の拒絶が認められるのは、未使用残高の限度内（1 万円全額ではなく、すでに商品等の購入に利用した 2 千円を除いた 8 千円分）ということになろう。

ロ．抗弁の接続（割賦販売法 30 条の 4）の類推適用の可否

イ．では（ii）カード加盟店（前払式発行者）の破産を受けて、カード会社がカード加盟店への支払を行わない場合を検討したが、（i）カード加盟店（前払式発行者）が破産したにもかかわらず、カード会社がカード加盟店に対する支払を行ったうえで、利用者に対し 1 万円を請求する場合、利用者としてカード会社からの請求を拒絶することはできるだろうか。ここでは、抗弁の接続の類推適用の可否について検討する。

抗弁の接続について定める割賦販売法 30 条の 4 は、消費者保護の観点から、購入者等と販売業者等との間で「生じている事由」をもって、購入者等が包括信用購入あっせん業者（カード会社）の支払請求に対抗できる場合があることを認めている[50]。同条は、① 2 ヵ月を超えない範囲の支払猶予を除外している（同法 30 条の 4、2 条 3 項 1 号）ほか、②金額が 4 万円以上であること（同法施行令 21 条 1 項）を要件としている。この点、設例 2 では、①についてはマンスリークリア（商品等を購入した翌月に一括で支払う方式）であることを前提としており、②についてはチャージ金額が 1 万円であることから、いずれの要件も満たさず、利用者はカード会社からの支払請求を拒むことはできない[51]。

48 破産の場合における、不安の抗弁権の成否については、松井［2016］580～582 頁参照。先履行義務の履行期が①破産手続開始の申立て前、②申立てと開始決定の間、③破産手続開始決定後に到来する場合に分けた検討を行っている。

49 いったん不安の抗弁権により履行拒絶した後に、破産手続開始決定がされた場合には、破産管財人が契約を双方未履行の双務契約として解除するならば、不安の抗弁権は問題とならないことになる。松井［2016］580 頁。

50 経済産業省［2021］167～171 頁。

51 前払式支払手段のサービスのうち割賦販売法 30 条の 4 の要件を満たすケース（チャージ可能な上限額が 4 万円以上のサービスや、支払方法がマンスリークリアだけではなく分割払いやリボ払いが可

また、同条の類推適用の余地について、学界では、購入者を保護する観点から、立替払契約と売買契約という 2 つの契約について、多角的法律関係や複合契約論など[52]、直接の契約関係がない当事者にも契約上の規律を及ぼす考え方について議論が深められている。しかし、同条の趣旨について、立替払契約と売買契約が別個の契約であることを前提としつつ、購入者保護の観点から、売買契約上生じている事由を、立替払契約の当事者である包括信用購入あっせん業者（カード会社）に対抗しうることを創設的に認めたものであるとする最高裁判例[53、54]の立場を前提とすれば、カード加盟店（前払式発行者）の破産にかかる設例 2 において、抗弁の接続の類推適用は容易には認められないと考えられる[55]。

さらに、割賦販売法の改正の方向について検討した経済産業省［2015］14〜16 頁でも、マンスリークリア取引は抗弁の接続の適用対象とはならないとしている。その理由として、①分割払いと同様の誘引性があるとはいえず、相談発生率も高くないこと、②採算性の高くないマンスリークリア取引について、イシュアーの追加的負担を正当化することは困難であること、③事業者に対する負担が利用者に転嫁された場合、取引の利便性が後退しうること等を挙げている。

以上のとおり、設例 2 において利用者が、割賦販売法 30 条の 4 の類推適用により抗弁の接続を主張してカード会社からの請求を拒むことは困難と考えられる。

ハ．前払式支払手段のチャージ取引の解除

イ．およびロ．では、前払式発行者（カード加盟店）の破産管財人またはカード会社から請求を受けた場合に、利用者が履行を拒絶できるかを検討したが、そもそも、前払式発行者と利用者双方の債務が未履行であると評価されるのであれば、設例 2 では前払式発行者（カード加盟店）が破産していることから、前払式発行者と

能なサービスもある）では、同条に基づき、カード会社からの請求を、未使用残高の限度内で、拒むことができると考えられる。この場合、前払式発行者の破産により、前払式支払手段の未使用残高が使えなくなることが、前払式発行者に対して「生じている事由」（同法 30 条の 4）であると考えられる。

52 学説の状況については、都筑［2016］68 頁以降に詳しい。当事者が選択した売買契約と立替払契約という 2 つの契約を、代金不払いの売買契約と不払い売買代金債権の売買契約に組み替えることで抗弁の接続と同様の効果を認めるという考え方（山田［1991a, b］）や、第三者与信型販売は、売買と与信の発生・履行・存続における牽連性が、商品引渡債務と与信債務の間にも延長されるという考え方（千葉［1999］）等をはじめとして、近時までさまざまな議論が積み重ねられている。

53 最判平成 2 年 2 月 20 日判時 1354 号 76 頁。

54 最判平成 23 年 10 月 25 日民集 65 巻 7 号 3114 頁も、売買契約と一体的に立替払契約の効力を否定することを信義則上相当とする特段の事情（①販売業者とあっせん業者との関係、②販売業者の立替払契約手続への関与の内容および程度、③販売業者の公序良俗に反する行為についてのあっせん業者の認識の有無および程度）がない限り、売買契約と別個の契約である立替払契約は無効とはならないと判示する。

55 中村［2014］132 頁は、オフアス取引なども念頭においた場合には、多数当事者契約の理論はさらなる検討が必要である旨を指摘している。

利用者の契約は、双方未履行の双務契約として破産法 53 条の適用を受けうるという論点がある。

破産法 53 条の適用の有無を検討するに当たって、利用者と前払式発行者（カード加盟店）の間の契約における双方の債務の履行状況について考える。利用者が払込みを行う債務については、クレジットカードの利用により、前払式発行者（カード加盟店）がカード会社にカード利用代金の請求権を有することから履行済みと解する余地もあるが、まだ前払式発行者に対する入金が完了していないという点を重視すれば、未履行と評価できる。また、前払式発行者の債務については、チャージの段階で前払式支払手段を発行している点を捉えれば既履行であるが、前払式発行者が負う債務の内容を、前払式支払手段を発行しただけではなく利用者に前払式支払手段を発行したうえでチャージ金額相当分の決済サービスを提供することまでだとすると、未履行と解することができる。

上記を踏まえると、設例 2 における前払式発行者（カード加盟店）と利用者の間の契約が双方未履行の双務契約（破産法 53 条）と整理できる場合には、契約を解除するか、または債務の履行を求めるかの選択権は前払式発行者の破産管財人が有するが、迅速な清算手続を進める観点からは、契約の解除が志向されることになる。

このようにして前払式支払手段のチャージ取引が 8 千円の限度で解除されれば、利用者は支払を行う必要がなくなり、損失を負担することはないという帰結になる。

ニ．解除と前払式支払手段の払戻し禁止規定

資金決済法では、前払式支払手段の払戻しは原則として禁止されている（資金決済法 20 条 5 項）。このため、ひとたびチャージが行われて前払式支払手段が発行された以上、チャージ取引の解除により払戻しを受けることは原則として認められない。もっとも、クレジットカードを利用して前払式支払手段をチャージした場合、カード会社から前払式発行者（カード加盟店）に支払が行われるまでに一定のタイムラグが生じる。このようにカード会社から前払式発行者（カード加盟店）への支払が未実行の状態にあるチャージ取引の解除については、実際の払込みが行われていない以上、同条が禁止する払戻しには当たらないと解することはできるだろうか。

この点について、資金決済法 20 条 5 項が払戻しの原則禁止を定めているのは、仮に自由な払戻しを認めると元本の返還が約束されることとなり、出資の受入れ、預り金及び金利等の取締りに関する法律（以下「出資法」という）2 条 1 項に定める「預り金」の禁止に該当するおそれがあるほか、送金手段としての利用が可能となると銀行法が禁止する「為替取引」に該当するおそれがあるためである[56]。もっ

56 高橋・堀・森［2023］165 頁。

とも、クレジットカードによりチャージされた前払式支払手段については、実際にカード会社から前払式発行者に資金の払込みがされていない間は、「預り金」の要件[57]の1つとされる「金銭の受入れ」を充足していないと捉えることもできる。また、払込みが未実行である間にチャージ取引が解除されても、利用者のカード会社に対する債務を消滅させるに過ぎず、実際に資金の払戻しがされるわけではないことから、為替取引に該当するとも考え難い[58]。このように考えると、前払式支払手段のチャージ取引の解除は、資金決済法20条5項が禁止する前払式支払手段の払戻しには該当しないと解することができる[59]。

これに対して、前払式支払手段のチャージ取引が行われた時点で、前払式支払手段は発行され、未使用残高が現に計上されている以上、たとえ実際の入金が未了であっても、チャージ取引の解除は資金決済法20条5項が禁止する前払式支払手段の払戻しに該当し、未使用残高の減算は認められないという考え方もありうる。実際、金融庁の事務ガイドラインでは、カード会社と前払式発行者が同一主体の場合で、クレジットカードで購入された前払式支払手段の代金が未収となっていて、その額が把握できる場合には、その額を基準日未使用残高（同法3条2項）から控除することを認めている[60]。これを逆に捉えれば、カード会社と前払式発行者が同一主体でない場合には、代金が未収であっても基準日未使用残高に計上することが求められる、すなわち、発行保証金による保全の対象となるということになる。そうだとすれば、利用者は、前払式支払手段のチャージ取引について、入金までを必ず行うことが求められ、利用者保護は、資金決済法に定める保全義務および優先弁済（同法14〜16条、31条）によることとなろう。

57 出資法2条2項は「預り金」について「不特定かつ多数の者からの金銭の受入れであつて、次に掲げるものをいう。一　預金、貯金又は定期積金の受入れ　二　社債、借入金その他いかなる名義をもつてするかを問わず、前号に掲げるものと同様の経済的性質を有するもの」と定めている。そして、事務ガイドラインでは、出資法2条2項に定める「預り金」について、「預金等と同等の経済的性質を有するものとされており、次の4つの要件のすべてに該当するものとされている。①不特定かつ多数の者が相手であること②金銭の受け入れであること③元本の返還が約されていること④主として預け主の便宜のために金銭の価額を保管することを目的とするものであること」と説明している（金融庁「事務ガイドライン第三分冊：金融会社関係2. 預り金関係」2-1-1）。

58 「為替取引」について最高裁（最決平成13年3月12日刑集55巻2号97頁）は銀行法2条2項2号にいう「為替取引を行うこと」とは、「顧客から、隔地者間で直接現金を輸送せずに資金を移動する仕組みを利用して資金を移動することを内容とする依頼を受けて、これを引き受けること、又はこれを引き受けて遂行することをいう」とする。

59 前払式支払手段の払戻しには該当しないとしてチャージ取引の解除が認められた場合には、利用者は前払式発行者の破産管財人に対して、解除した金額に相当する請求権を有すると考えられる。もっとも、同時に、利用者の未使用残高はその分減額されて、資金決済法31条による還付を受けられないと考えられる。この場合には、当該請求権が、破産手続上どのような債権として認められるかによって、利用者としては資金決済法による還付を受ける方が経済的に有利な帰結となる可能性もある。

60 金融庁「事務ガイドライン第三分冊：金融会社関係5. 前払式支払手段発行者関係」I-2-2。

6. おわりに

日本では前払式支払手段をクレジットカードで購入（チャージ）するサービスが広く利用されているが、それぞれの取引について複数の法律構成が考えられ、いずれか1つに確定することなく実務が動いているのが実態である。そうしたもとで、本稿では、決済サービスの提供者が破産した場合の設例を想定して、一定の法律構成を前提とした場合に利用者が不利益を被ることはないかとの観点から検討を行った。

その結果、まず、カード会社が破産した場合について、カード会社からチャージの対価にかかる入金を受けられないカード加盟店（前払式発行者）が、第三者弁済構成や併存的債務引受構成といった法律構成を前提に、利用者に対する請求を行う可能性は排除しきれないことを示した。もっとも、利用者としては、クレジットカードを利用してカード会社に対する債務を負って前払式支払手段の発行を受けた以上、カード加盟店（前払式発行者）から直接請求を受けることは想定していない。このため、カード加盟店（前払式発行者）が利用者に対して直接請求を行うことができない法律構成をとることが適切であり、利用者に直接請求することを禁止する旨を規約等において明示しておくことが望ましく、そうすることが取引当事者の認識とも合致すると考えられる。

次に、前払式発行者（カード加盟店）が破産した場合についても、支払委託構成を前提とすると、前払式加盟店は商品購入等の代金について、利用者に直接請求することが可能という帰結となることを示した。しかし、利用者としては、一度発行された前払支払手段を用いて商品等を購入した以上、前払式加盟店から追加的な支払を求められることは想定していないと考えられる。このため、前払式発行者が破産した場合についても、前払式加盟店から利用者に対する直接請求を行うことを規約等で禁止するのが望ましいと考えられる。

さらに、前払式発行者（カード加盟店）の破産により未使用残高が使用できなくなった場合について、カード会社・カード加盟店間の契約の解除の可否を検討したうえで、加盟店契約が解除された場合の前払式発行者（破産管財人）から利用者に対する請求の可能性と、これに対する利用者の抗弁権の主張の可否についても検討した。また、前払式発行者と利用者の間のチャージ取引にかかる契約関係が、破産法上、双方未履行双務契約と評価しうることも指摘した。その際、前払式発行者（破産管財人）が契約解除を選択する場合には、前払式支払手段における払戻しの原則禁止との関係が問題となりうることを示した。

本稿では、取引の当事者について、もっとも単純化したオンアス取引を検討対象とした。しかし、実際のクレジットカード取引では、イシュアーとアクワイアラが

分かれるオフアス取引が主流であるほか、クレジットカードと前払式支払手段それぞれについて、決済代行業者が間に入る場合なども少なくなく、取引のタイミングや当事者の関係はさらに複雑である。そうした複雑なケースについての検討は残された課題としたい。

参考文献

片岡義広、「プリペイド・カード取引標準約款等の概要」、『別冊 NBL』22 号、商事法務研究会、1991 年、146～165 頁

――――、「クレジットカード等契約の法律構成の可能性」、『CCR』10 号、2021 年、70～84 頁

金融庁、「金融庁の 1 年（2022 事務年度版）」、金融庁、2023 年（https://www.fsa.go.jp/common/paper/2022/zentai/all.pdf、2024 年 4 月 10 日）

経済産業省、「産業構造審議会商務流通情報分科会割賦販売小委員会報告書～クレジットカード取引システムの健全な発展を通じた消費者利益の向上に向けて～」、経済産業省、2015 年（https://www.meti.go.jp/shingikai/sankoshin/shomu_ryutsu/kappu_hambai/pdf/report_02_01.pdf、2024 年 4 月 10 日）

――――、『令和 2 年版割賦販売法の解説』、日本クレジット協会、2021 年

小塚荘一郎・森田　果、『支払決済法［第 3 版］』、商事法務、2018 年

潮見佳男、『新債権総論 I』、信山社出版、2017 年

清水　巖、「クレジット・カード取引の法構造―2―」、『法律時報』46 巻 6 号、1974 年、295～304 頁

杉浦宣彦・片岡義広、「電子マネーの将来とその法的基盤」、金融庁金融研究センターディスカッションペーパー、金融庁金融研究センター、2003 年（https://www.fsa.go.jp/frtc/seika/discussion/2003/20030828-2.pdf、2024 年 4 月 10 日）

高橋康文編著・堀　天子・森　毅、『新・逐条解説資金決済法［第 2 版］』、きんざい、2023 年

玉垣正一郎、「クレジットカード決済システムの構造―各種手数料の意義―」、『現代消費者法』36 号、2017 年、49～56 頁

千葉恵美子、「『多数当事者の取引関係』をみる視点」、伊藤　進・國井和郎・堀　龍兒・新井育文編『現代取引法の基礎的課題 椿寿夫教授古稀記念』、有斐閣、1999 年、161～199 頁

千葉恵美子編、『キャッシュレス決済と法規整―横断的・包括的な電子決済法制の制定に向けて―』、民事法研究会、2019 年

都筑満雄、「複合契約論のこれまでと今後」、『別冊 NBL』161 号、商事法務研究会、2016 年、68～77 頁

デジタルマネーの私法上の性質を巡る法律問題研究会、「デジタルマネーの権利と移転」、『金融研究』第 43 巻第 1 号、日本銀行金融研究所、2024 年、1～48 頁

電子マネーに関する勉強会、「電子マネーの私法的側面に関する一考察：『電子マネーに関する勉強会』報告書」、『金融研究』第 16 巻第 2 号、日本銀行金融研究所、1997 年、1～45 頁

中村　肇、「日本におけるクレジットカード契約の法的性質論―多数当事者間取引

の一例として―」、『CCR』3 号、2014 年、114～136 頁
松井和彦、「不安の抗弁と倒産手続―民法（債権関係）改正論議を手がかりに」、『阪大法学』66 巻 3・4 号、2016 年、109～136 頁
山田誠一、「『複合契約取引』についての覚書（1）」、『NBL』485 号、1991 年 a、30～40 頁
―――、「『複合契約取引』についての覚書（2・完）」、『NBL』486 号、1991 年 b、52～63 頁
山本正行、『カード決済業務のすべて』、金融財政事情研究会、2012 年
吉元利行、「クレジットカード取引における利用者保護：その現状と課題」、九州大学学術情報リポジトリ、2015 年（https://catalog.lib.kyushu-u.ac.jp/opac_download_md/1654632/law0124.pdf、2024 年 4 月 10 日）

金融研究所の概要

金融研究所（Institute for Monetary and Economic Studies, IMES）は 1982 年 10 月に日本銀行創立百周年を記念して、日本銀行の内部組織の 1 つとして設立されました。その主な目的は、(1) 金融経済の理論、制度、歴史に関する基礎的な研究の充実を図り、日本銀行の政策の適切な運営に役立てること、(2) 学界等との交流を促進すること、(3) 外部の研究活動の便宜に資する各種情報、資料等を公に提供することです。

主な活動

研究活動

・金融経済の基本的問題に関する理論・実証的研究。
・金融関連の制度基盤（法律・会計・中央銀行制度等）に関する研究。
・金融関連の情報技術に関する研究。
・金融経済の歴史に関する研究。
・金融経済に関する歴史的資料の収集・保存・公開（アーカイブ・貨幣博物館）。

顧問および客員研究員の招へい

・国内外の有力学者若干名に研究所顧問（非常勤）を委嘱し、研究所の運営、研究活動の進め方、内外学界との交流等に関する助言を受けています。
・国内外より学者数名を客員研究員として招へいし、研究活動の強化を図っています。

会議の開催

・海外中央銀行、国際機関の研究者や内外の著名学者を交えた会議を開催。
・外部の研究者、専門家を交えた研究会、セミナー等を適宜開催。

刊行物の発行

金融研究、Monetary and Economic Studies、IMES Discussion Paper Series、日本銀行の機能と業務、国際コンファランス議事録等を公刊（刊行物の一覧は後掲）。

貨幣博物館

国内を中心とした貴重な貨幣や貨幣にかかわる資料を貨幣博物館に展示するとともに、貨幣に関する歴史資料をホームページ等で公開（博物館の案内は後掲）。

歴史的公文（歴史的文書）の公開

日本銀行に関連する歴史的資料のうち、歴史的価値を有するものについて、日本銀行金融研究所アーカイブで保管・整理し、一般に公開（アーカイブの案内は後掲）。

研究の委託

人員面、資料面の制約等から所内での研究が困難なテーマについて外部の学者等に研究を委託。

主な刊行物

金融研究

邦文機関誌、年 4 回程度発行。金融研究所の研究論文や各種ワークショップの模様、研究会報告等を公表。

Monetary and Economic Studies

英文機関誌。『金融研究』と同様、金融研究所の研究論文等を公表（『金融研究』掲載論文の英訳のほか、英文オリジナル論文を含む）。

IMES Discussion Paper Series（E-Series：英語版、J-Series：日本語版）

金融研究所スタッフおよび外部研究者による研究成果の未定稿を随時公表。学界、金融機関、関係者等から、広くコメントを求めることを目的としている。

国際コンファランス議事録

- *Growth, Integration, and Monetary Policy in East Asia*（*Monetary and Economic Studies*、Vol. 25、No. S-1、2007年）
- *Financial Markets and the Real Economy in a Low Interest Rate Environment*（*Monetary and Economic Studies*、Vol. 24、No. S-1、2006年）
- *Incentive Mechanisms for Economic Policymakers*（*Monetary and Economic Studies*、Vol. 23、No. S-1、2005年）
- *Challenges for Sustained Economic Growth under Changing Economic, Social, and International Environments*（*Monetary and Economic Studies*、Vol. 22、No. S-1、2004年）
- *Exchange Rate Regimes in the 21st Century*（*Monetary and Economic Studies*、Vol. 20、No. S-1、2002年）
- *The Role of Monetary Policy under Low Inflation: Deflationary Shocks and Policy Responses*（*Monetary and Economic Studies*、Vol. 19、No. S-1、2001年）
- *Monetary Policy in a World of Knowledge-Based Growth, Quality Change and Uncertain Measurement*（Palgrave、2001年）
- *Towards More Effective Monetary Policy*（Macmillan Press、1997年）
- *Financial Stability in a Changing Environment*（Macmillan Press、1995年）
- *Price Stabilization in the 1990s: Domestic and International Policy Requirements*（Macmillan Press、1993年）
- *The Evolution of the International Monetary System: How Can Efficiency and Stability Be Attained ?*（University of Tokyo Press、1990年）
- *Toward a World of Economic Stability: Optimal Monetary Framework and Policy*（University of Tokyo Press、1988年）
- *Financial Innovation and Monetary Policy: Asia and the West*（University of Tokyo Press、1986年）
- *Monetary Policy in Our Times*（MIT Press、1985年）

なお、2008 年以降に開催された国際コンファランスについては、議事要旨等を *Monetary and Economic Studies* に所収。

日本銀行の機能と業務（有斐閣、2011 年発行）
　日本銀行がどのような役割・機能を担い、また、これを果たすため、どのような業務を行っているのかについて、網羅的かつ具体的に解説。

貨幣博物館 常設展示図録（ときわ総合サービス、2017 年発行）
　貨幣博物館の展示資料を紹介した図録です。

日本銀行金融研究所（IMES）
〒103-8660 東京都中央区日本橋本石町 2-1-1
TEL：03-3279-1111、FAX：03-3510-1265
E-mail：imes.journals-info@boj.or.jp
ホームページ：https://www.imes.boj.or.jp

資料公開サービス

以下の資料公開サービスを行っておりますので、ご利用下さい。

(1) 貨幣博物館の公開

2015 年 11 月、貨幣博物館はリニューアルオープンしました。日本の貨幣を中心に、和同開珎や大判・小判の実物、貨幣に関する絵画など、貴重な資料を多数展示するとともに、所蔵資料を貨幣博物館ホームページ等で一般に公開しています。20 名以上の団体で見学を希望される場合は予め電話でご連絡下さい。

開館時間：9 時 30 分～ 16 時 30 分（入館は 16 時まで）
休 館 日：月曜日（ただし祝休日は開館）
年末年始（12 月 29 日～ 1 月 4 日）
※最新の情報は下記の当館ホームページで
お知らせいたしますので、ご確認下さい。
貨幣博物館ホームページ：https://www.imes.boj.or.jp/cm/
〈連絡先〉金融研究所　貨幣博物館
TEL：03-3277-3037（直通）

(2) 日本銀行が保有する歴史的公文（歴史的文書）の公開

金融研究所では、日本銀行に関連する歴史的資料のうち、歴史的価値を有するものについて保管・整理し、一般に公開しています。閲覧をご希望の方は、当館ホームページ掲載の目録で検索のうえ、予めメール・電話にてご連絡下さい。

歴史的公文の目録：https://www.imes.boj.or.jp/archives/hozon.html
〈連絡先〉金融研究所　アーカイブ
E-mail：imes.archives@boj.or.jp
TEL：03-3277-2151（直通）

金　融　研　究（第 44 巻 第 1 号）
ISSN 2759–5099
2025 年 1 月 20 日　発行
日本銀行金融研究所長
編集兼発行者　渡 辺 真 吾
発　行　所　日本銀行 金融研究所
郵便番号 103–8660
東京都中央区日本橋本石町 2–1–1
電　話：（03）3279–1111（大代表）

国際文献社
本誌に関する照会は、日本銀行金融研究所までお寄せ下さい。