



# FinTech, 仮想通貨ビジネス の最新動向

京都大学 公共政策大学院  
教授

岩下 直行

## 1. はじめに

FinTech（以下、フィンテック）の一出現形態となった仮想通貨（暗号資産）は、2016年頃から日本でも多くの人が投資を行うようになり流行しているが、一方で相場の大きな波を受けたり、さまざまな犯罪等も起きている。本稿では、フィンテックと仮想通貨を二大テーマとし、最新動向を考察する。

## 2. フィンテック

### (1) シリコンバレーからの挑戦者 ～フィンテック企業の勃興

日本では50年ほど前に今でいう全国銀行データ通信システムがつくられるなど、ファイナンスとテクノロジーは密接に関連していた。「フィンテック」とは、金融を表すファイナンスと技術を表すテクノロジーを合わせた造語であり、米国の金融業界では2000年代前半から使われていた。大きな変化をもたらしたのは2008年の

リーマンショック後、世界中の金融機関が金融危機のもとで取引を慎重化させていたこともあり、新しい金融サービスを提供する米国シリコンバレー発祥のITベンチャー企業が出現し、新たな金融の担い手の役割を果たすようになった。

フィンテック企業は、ペイメント（お金を決済する）やレンディング（お金を貸す）を扱うところが7割くらいを占めている。例えば、ペイメントの中で最も老舗企業のPayPalは、自らが金融機関間を接続するネットワークインフラや端末機器を持たず、決済のための仕組みの全てをインターネット上で構築している。伝統的な金融機関がシステムインフラの維持管理に膨大な費用を投じているのに対し、PayPalはコスト面で圧倒的に有利な立場にあり、金融業界の深刻な脅威と受け止められている。一方レンディングの中で比較的老舗企業のLendingClubは、自ら融資を行うのではなく、貸し手と借り手とをマッチングさせて手数料を稼ぐ「マーケットプレイス・レンディング」というビジネスを展開している。伝統的な金融機

表1 日米の主要フィンテック企業の業務領域の違い

サービス分野		業務内容	米国の主なフィンテック企業	日本の主なフィンテック企業
伝統的な銀行と競合する領域	融資	・Web上で貸し手と借手を取り、信用格付け等を実施して、貸付をマッチングするサービス。P2P レンディング、ソーシャルレンディングとも呼ばれる。	LendingClub, Prosper, Kabbage,	Maneo,
	決済	・スマートフォン等を利用して個人間送金やクレジットカード決済を行うサービス。伝統的に多くのフィンテック企業が参入してきた。	PayPal, Stripe, Square	LINE Pay,
伝統的な銀行と連携していく領域	PFM	・本人の許諾のもとで多くの銀行の口座情報を集約し、顧客の資産を分かりやすく管理するサービス。	MX, Mint	マネーフォワード, Zaim, マネーツリー
	会計サポート	・小規模企業向けに、売掛金・買掛金・固定資産等の管理、請求書作成、給与・税金支払いといった経理、税務等のサポートを行うサービス。	Xero, ZenPayroll, Zenefits	マネーフォワード, freee, メリービズ
	ロボアドバイザー	・個人の証券投資等への助言やポートフォリオの組成をソフトウェアで行うことにより、安価に提供するサービス。	Motif Investing, Wealthfront, Betterment	お金のデザイン, ZUU, Finatext

関が果たしていた役割を奪う典型的な「中抜き (disintermediation)」ビジネスであり、個人向け融資の分野では、銀行の強力なライバルになりつつある。

インターネットがなかった時代は、事業者が通信プロトコルや端末仕様を定め、システムインフラから業務プログラムまで全てを設計して構築し、莫大な費用が必要であるため、大企業が精緻な事業計画を立てて長期プロジェクトを遂行する必要があった。インターネットが普及した現代は、インターネット上で安価に提供されるシステム基盤を利用することが可能になり、小規模なベンチャー企業がさまざまなビジネスのトライアルを行うことが容易になった。それが金融分野まで及んできたというのがフィンテックだと考えられる。

## (2) 日本の金融機関に期待される対応

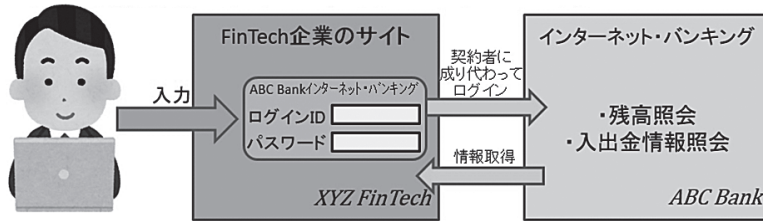
日本の金融業界は1970年代からIT化に取り組み、ITを重要な経営資源と位置付けてきたが、金融機関の業務現場では、「本来ITが持

つ力が十分に発揮されていない」という指摘が聞かれる。堅牢性やセキュリティ、可用性を誇るが、一方で柔軟性に乏しく、維持管理や制度対応に多大なコストと時間を要するため、本来イノベーションの手段であるべきITが、むしろイノベーションを阻害する一因となっている。

また、日本の銀行はIT投資の8割を維持管理に使い、新規投資は2割しか使われておらず、米国に比べ新規投資の比率が少ない。これにより、いろいろな意味で支障がでてくるため、オープンネットワークの利用を前提とした新しい技術を取り入れたり、マルチベンダーでさまざまなビジネスを行うことが必要だろう。

現在、日本のフィンテック企業の業務は「銀行と連携していく領域」だが、米国のフィンテック企業は「銀行と競合する領域」であるという違いがある(表1)。2018年6月、日本でもLINE株式会社がPayPalと同様に無料で送金できる「LINE Pay」事業を拡大しようと、

(1) API接続をしないケース (スクリーンスクレイピング)



(2) API接続を使用するケース (OAuth認証)

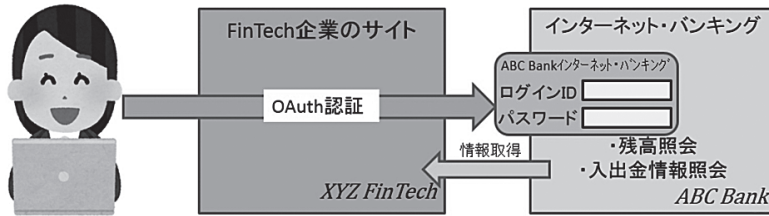


図1 銀行とフィンテック企業のAPI接続の概要

さまざまな広報活動を始めた。LINEのユーザー国内7,500万人が自分たちで決済を手掛けることになると、銀行はフィンテック企業と協力してイノベーションを少しずつ進めていくのは問題になってくる。

### (3) インターネットバンキング ～フィンテックの前提条件

多くの金融機関がインターネット・バンキングを提供して20年ほど経つが、インターネット・バンキング契約口座数は、全ての口座の中の20%弱にすぎない（出所：金融情報システムセンター（FISC）「金融情報システム白書」2016年）。インターネット利用率は、スマートフォンの普及により地域間の格差は縮まってきたが、問題は、銀行の預金、証券会社で預けている株券などの圧倒的な所有者である高齢者がITに対応していない点である。ただし、60代、70代はインターネットの利用率が右肩上がりになっており、いずれすべての年齢層でインターネットを利用する時代にそなえ、銀行ではオープンAPI（アプリケーションプログラミング・インターフェース）化などの取り組みを行って

いる。

### (4) 金融オープンAPI

#### ～イノベーションの次のハードル

銀行法は過去10年間で3回しか改正されていないが、そのうち2016年と2017年の2回は銀行がフィンテックに対応するために改正された。これは公的当局がフィンテックによって銀行に甦って欲しいという期待を表している。

従来のフィンテック企業のソフトを使ってインターネットバンキングに接続する「スクリーンスクレイピング」は、IDとパスワードを第三者であるフィンテック企業に教えるもので、フィンテック企業側に大量の顧客情報が記録されてる。この問題を解決するため、「OAuth認証」を使用し、API接続による情報取得を可能にするオープンAPI化が今の銀行に求められている（図1）。このAPIというレイヤーができると、従来はその銀行が提供するアプリ内でしかインターネットバンクは使えなかったのが、さまざまなフィンテック企業のソフトを介して、さまざまな銀行のサービス提供を受けることができるようになり、大きな変

化をもたらすのではないかと考えられている。

### (5) 新興国におけるキャッシュレス化進展の影響

2010年の時点では、世界人口の約半分は銀行が使えなかったが、今ではモバイルマネーの使用が進み、かなり解消している。例えば、アフリカのケニアでは、M-PESA（エムペサ）というモバイルマネーがあり、首都近郊以外の電気やガス、水道がない地域でも、携帯電話の電波が届き、受信と電源を確保できれば、モバイルマネーを使用して、決済、送金出金等を行えるようになってきた。また、中国でもスマートフォンのQR決済、Alipay、WeChat Payなどが標準的になり、これさえあれば生活ができる。日本は主要国における対GDP通貨流通残高比率の推移（出所：国際決済銀行 決済・市場インフラ委員会）によると2015年には約20%の利益が使われているが、多くはタンス預金として保存されており、キャッシュレス化という意味では遅れている。

## 3. 仮想通貨

### (1) 仮想通貨って何？

仮想通貨が高騰し、最近では1億円以上稼いだ人を、通称「億り人（おくりびと）」といい、次々に誕生している。仮想通貨に投資する日本の個人投資家は、延べ360万人を数え、仮想通貨をテーマにした書籍や、専門の月刊誌まで登場している。

しかし、仮想通貨は新しい通貨としてほとんど使われていない、株式や社債とは違い配当も金利も償還金も何も手に入らない、購入した価格よりも高値で売却できるのはなぜか、仮想通貨は未来のお金になるのか、などの疑問がある。結論は、現在のお金が仮想通貨に取って代

わられることはなく、最近の高騰は世界的な金融緩和による一時的な現象である。仮想通貨でキャッシュレス化が進むわけではないが、キャッシュレス化は徐々に進むと考えられる。では、仮想通貨とはどのようなものかについて、ビットコインを例として説明する。

### (2) 仮想通貨の主要構成要素

#### ① ノード

ノードとは仮想通貨のネットワークに接続されている通信機器をさし、ビットコインの取引を管理するノード数（パソコン）は全世界に約10,000個ある（2018年9月調査時点）。全世界に散らばったノードを全部一斉に書き換えなければ不正を行えないため、ノード数の多いビットコインが安全だと言われる一つの理由である。ノード数は米国、ドイツ、フランス、中国が上位で、日本は2.52%の244個である。これは直接ビットコインを所有している人、日本ではほとんどが取引関係の業者の数を示している。その取引所に依存して取引を行っているエンドユーザーはビットコインを直接所有していない、というのが問題である。

#### ② 秘密鍵

ブロックチェーンは暗号技術を基にしており、「秘密鍵」と「公開鍵」の二つの鍵で構成されている。ビットコインの秘密鍵の管理方法の一つである「ウォレットアプリ」は、秘密鍵を自分で管理する方法だが、秘密鍵を失くすと復元することができない。そこで普及したのが「ウォレットサービス」という業者に暗号通貨の管理を委託する方式であるが、業者が不正を働いたり、サイバー攻撃を受けて預けてあるビットコインを奪われるリスクがある。

#### ③ ハッシュ関数

ビットコインで利用されているのは、暗号学的ハッシュ関数と呼ばれ、元のデータの長さは

任意でよいが、元のデータを1ビットでも変えたら、全ての256ビットのデータの1つ1つが1/2の確率で変わらなければならないという特殊な性質を持っている。ハッシュ関数によって得られるハッシュ値は、同じ値となることやハッシュ値からメッセージを得ることが(事実上)不可能であるという要件を持つものを使用する。

#### ④競争的マイニング

ビットコインは発行主体を持たず、インターネット上のネットワークで情報が共有され、誰でも利用者となることができ、取引履歴の検証を可能とすることで信頼を確保している。取引データをハッシュ関数を使ってハッシュ値を計算するなど、計算能力を提供してシステム全体の維持管理に貢献すること(=マイニング(発掘))に対し、一定の報酬が与えられ、この報酬を求めて専門業者が膨大な計算能力を投入して競争を行い、マイニングを進めている。2017年から2018年にかけて、マイニング専用設備の大需要が起これ、マイニングにより使用する電力消費が大量になり、エネルギー問題が地球環境問題に発展していくのではないかと懸念している。

#### (3) 乱高下する仮想通貨価格とその原因

ビットコインの価格は、2017年1月に1,000ドル/BTC程度で推移していたが、12月には20,000ドル/BTCと20倍近く値上がりした。また、全ての仮想通貨の時価総額は2017年はじめは日本円にして2兆円だったが、2018年1月には約50倍の90兆円に上昇したことにより、仮想通貨市場全体に占めるビットコインのシェアが減少した。その後、仮想通貨の相場が急落するが、2017年の大相場の背景には、ICO(イニシャル・コイン・オファリング)の影響が大きいと考えられる。

一般に、ICOとは企業等が電子的にトークン(証券)を発行して、公衆から資金調達を行う行為の総称である。ICOの大半は仮想通貨イーサリアムを基盤に利用し、ERC-20トークンと呼ばれる仮想通貨的なデジタル資産が発行される。ICOが増えるとイーサリアムの需要が増え、相場が上昇した。そして、ビットコインとイーサリアムの値上がり状況をみて、他の仮想通貨にも投資され、一斉に値上がりをはじめたと考えられる。

#### (4) 仮想通貨取引の安全性を巡る話題

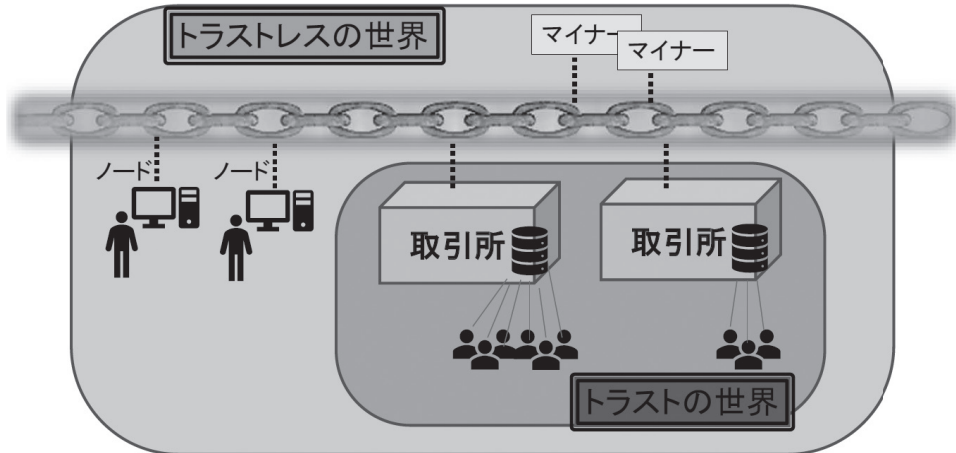
2018年1月のコインチェック社の仮想通貨不正流出事件は、本来、部外者に知られてはならない秘密鍵を攻撃者に勝手に使われて、世界中のコンピュータの情報を書き換える指令が出され、業者のアドレスから、犯人が用意したアドレスに多額の仮想通貨が送金されてしまった。

我々は業者の取引所に依存して、業者のデータベースを使っている「トラスト」の世界(信頼できる中央機関を置く従来の仕組み)で仮想通貨を保持している。ここから、信頼できる中央機関をおかないというポリシーで「トラストレス」と呼ばれる世界に流出してしまうと、もう誰も止められない、どこからも制約を受けないという性格を持っている(図2)。この事件以外にも、仮想通貨交換業者に金融庁が検査入りした結果、さまざまな問題が起こっている。

また、香港の仮想通貨取引所Bitfinexと関係の深いテザー社が発行する仮想通貨テザーは、1Tether = 1ドルでほぼ固定され、お札を刷るかのようにテザーを発行させ、それを用いて、米国の仮想通貨取引所BittrexとPoloniexの二カ所からビットコインを直接購入していた。こうした操作はビットコインの相場操縦を目的に実施されていたのではないかと疑われ、事実関係が分かれば信用を大きく棄



ビットコインの取引のうち、マイニングの対象となるものは、ブロックチェーンの仕組みにより安全性が担保されている。しかし、交換所での取引は交換所限定で処理され、マイニングの対象とならない。取引所経由で間接的に参加している利用者は、トラストの世界に居る。



非中央集権を標榜した仮想通貨の取引の大本が、「信頼できる第三者」にならなければならないという矛盾。

図2 「トラストレスの中のトラスト」構造の問題

損するのではないかと心配されている。

#### 4. おわりに

以上、フィンテックと仮想通貨ビジネスの最新動向をみてきた。このような状況の中、金融

庁では電子通貨も含めて金融業界に関する国の制度を抜本的に見直すことや、仮想通貨交換業等をめぐる諸問題について、2018年3月に「仮想通貨交換業等に関する研究会」を設置するなど、さまざまな取り組みを進めている。

本稿は一般社団法人電気通信協会産業部会が平成30年10月1日に開催した第151回ブロードバンド・ユビキタス調査会における講演から抜粋してとりまとめたものです。