情報通信の現在と未来を展望する

Vol.26
2016 Summer
ネクストコム

Nextcom

特集 仮想通貨

Feature Papers

Report

Articles

明日の言葉

人が貨幣を求めるのは、貨幣そのもののためではなく、
貨幣で購買できるもののためなのである。
……アダム・スミス

『国富論』に、アダム・スミスは、
「所有する貨幣の名目額が増えることを富と思い込んでいるが、
貨幣は商品交換の媒介にすぎない」と
繰り返し記した。

INDEX
summer
2016

Nextcom ネクストコム

特集

仮想通貨

写真：コインのストック

すでに始まってしまった未来について ―― ㉖

文：平野啓一郎
絵：大坪紀久子

「マイナンバーの行方」

個人情報管理の難しさや、国家による国民の監視強化の懸念など、様々な問題点が指摘される中で、マイナンバー制度がスタートした。早速、郵送による通知漏れや業者の紛失のトラブルなどが報告されているが、制度自体の運用は、驚くほどのスピードで各所に浸透していっている。

私がそれを実感するのは、原稿依頼や講演依頼などである。その謝礼の支払いのために、いちいち、依頼先からマイナンバーの提出を求められる。実際には、納税に関して、今はまだ必ずしもマイナンバーの提出が必要ではないはずだが、特に大学などで講演をする際には、機械的に、その提出要請の書状が届く。

私が驚いたのは、その際にマイナンバーの管理を委託された民間業者の数の多さである。

マイナンバーを自ら管理するという出版社や大学はほとんどなく、大体、どこかの業者が、それを代行している。一斉にそういうことになっているので、準備期間に指導があったのだろう。そして、その連絡をしてくる業者が、毎回、すべて違うのである。

私は最初、マイナンバーの提出に抵抗して、それを講演依頼先に教えなかった。その時は実際、それが通ったのだが、その間のやりとりはかなり面倒で、同様の提出要請が次々に届き始めると、とうとう根負けして、それに応じるようになった。悪徳業者が、架空の業務委託を偽って、書類を送りつけてきたなら、うっかり応じてしまいそうである。

自分のマイナンバーが、これだけの数の業者に既に拡散し、今後、更に様々な場面での活用が期待されているとなると、セキュリティに関しては、かなり悲観的にならざるを得ない。マイナンバーも、「漏洩して不正に用いられるおそれがあると認められる場合」は変更が可能らしいが。

国家は勿論、利便性を第一にこの制度を導入したのであろうが、流出によってもたらされる混乱のコスト、それを予防しながらシステムを維持してゆくコストは、本当にそれに見合ったものなのだろうか。

Keiichiro Hirano

小説家。1975年生まれ。1999年京都大学在学中に『日蝕』により芥川賞を受賞。以後、『葬送』、『ドーン』、『かたちだけの愛』、『空白を満たしなさい』、『私とは何か ―「個人」から「分人」へ』、『透明な迷宮』など、数々の作品を発表。『「生命力」の行方―変わりゆく世界と分人主義』（講談社）。最新刊は『マチネの終わりに』（毎日新聞出版）。

特集

仮想通貨

仮想通貨は単なる「モノ」ではなく、「貨幣」としての機能をもつ。
金融庁も、そんな仮想通貨の位置付けを明確にしようとしている。
欧米同様に、法規制への取り組みも活発化する見込みだ。

特集論文

仮想通貨1

貨幣の歴史にみる仮想通貨の特異性

――国家の通貨高権からCODEによる通貨発行へ――

国立情報学研究所 情報社会相関研究系 准教授

岡田 仁志 Hitoshi Okada

仮想通貨とは、「決済手段」「転々流通性」「国家の裏付けの不在」の３つの要素を備える新しい「お金」である。
とりわけ特異な構造を有する分散型仮想通貨には、中心となる発行主体が存在しない。
果たして仮想通貨とその基礎となるブロックチェーンは、社会を変革するツールとなり得るのか。
これまで実在しなかった非中心的なシステムを読み解く鍵は、人類の歴史にこそ求められる。
イングランド銀行のレポートを手掛かりとして、
貨幣の変遷をたどり、人類にとって貨幣とは何であったのかを考察する。
仮想通貨の登場が国家・社会・経済にどのような影響を及ぼすのかを推量し、
これを制御して社会を豊かにするためのルールの在り方について言及する。

キーワード
分散型仮想通貨　電子マネー　決済手段　ブロックチェーン　Bitcoinシステム

1. はじめに ――仮想通貨とは何か。電子マネーとは何が違うのか

仮想通貨bitcoinの登場をきっかけとして、広義の電子マネーの再定義が試みられている。Bitcoinシステムのような仮想通貨の仕組みは、従来の電子マネーとは何が異なるのであろうか。本稿では、仮想通貨とは、「決済手段」「転々流通性」「国家の裏付けの不在」の３つの要素を備えるものであると定義する[1)]。（図表１）

1.1 決済手段の電子化

「決済手段の電子化」とは、利用者の保持する電子機器に記録されたデジタル・データそれ自体が「価値」を有する場合などのように、有体物以外のものが決済に用いられる場合をいう。それに対して、「決済方法の

電子化」とは、利用者が決済のための「価値」の移転を第三者に対して指図する場合に、その指図を電子機器や通信機器を通じた電子的な方法により行うものである。

仮想通貨bitcoinの利用者は、ブロックチェーンによって非可逆性が保証された状態の「取引記録」に貨幣的価値があるという前提に立つ。すなわち、Bitcoinシステムの「取引記録」を「決済手段の電子化」と見なしているのであって、他の何らかの貨幣的価値に対する移転を指図する「決済方法の電子化」であると見なしているわけではない。従って、仮想通貨bitcoinは「決済手段の電子化」として流通していると見ることができる[2)]。

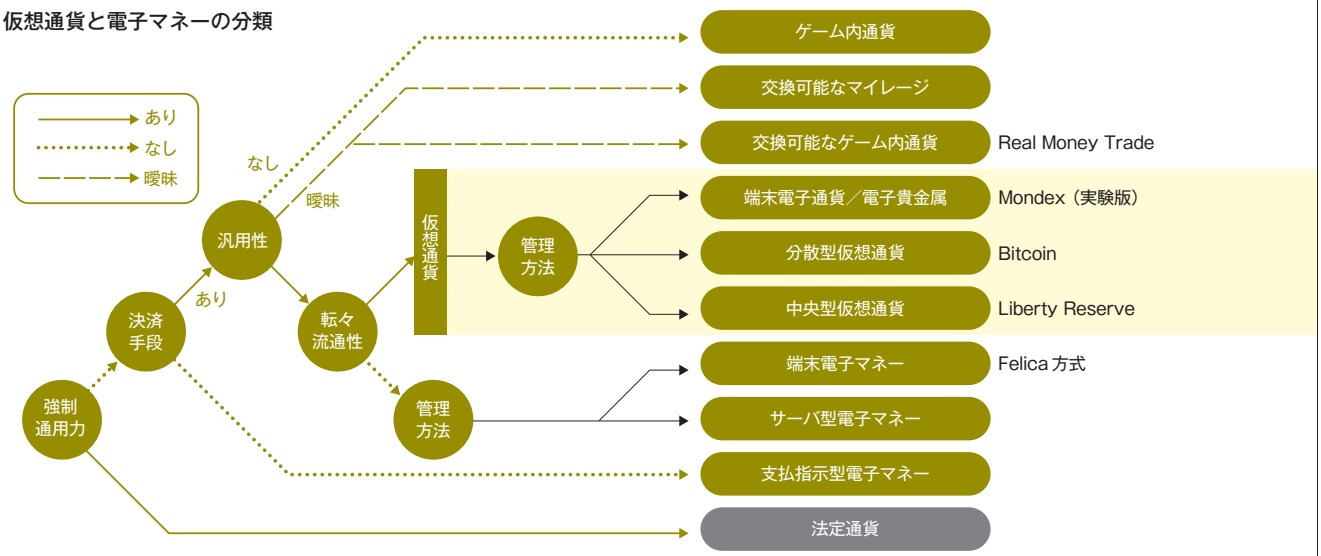
ここで留意すべきことは、このような「取引記録」によって移転されるのは、貨幣的価値を有していると信じられている「量」のみであるということである。これは、仮想通貨bitcoinを「モノ」とは考えないこと、ある種の債権とは考えないことを意味している。

Bitcoinシステムにおいて、貨幣的価値が存在しているのは、ブロックチェーンによって非可逆性が保証された状態の「取引記録」である。ブロックチェーンは、Bitcoinシステムのネットワーク全体で運営されている分散型ファイル・システムであるから、その中に管理されている「取引記録」は、いわゆる電磁的記録ではなく、より抽象的な「情報」と見なすべきである。

この抽象的な「取引記録」がブロックチェーンを介して非可逆的状態に定着されると、Bitcoinシステムの経済の中で、その記載内容である「貨幣的価値の移転」が確定したものとして信頼される。この抽象的な「情報」としての「取引記録」を、Bitcoinシステムの経済の参加者が「貨幣的価値の移転」として信頼する。この信頼が、仮想通貨bitcoinを支払いの手段として用いることを可能にする。

いわば信頼が貨幣的価値を有するのであり、モノ

図表1　仮想通貨と電子マネーの分類



［出典］　岡田仁志・高橋郁夫・山崎重一郎［2015］,『仮想通貨――技術・法律・制度』, 東洋経済新報社, 2015.

としての電磁的記録が移るのではない。抽象的な信頼をあたかもモノのように扱うことができるようにBitcoinシステムは設計されている。このことが分散型仮想通貨の技術的な真新しさであって、この世に存在しなかったものが登場したといわれるゆえんである。

1.2 転々流通性

仮想通貨に求められる第2の要素として、転々流通性が挙げられる。不特定多数の人との間で決済に利用し得るというのを転々流通性（人的に交換可能性が高い性質）というのに対して、いかなるものとも交換し得る性質（物的に交換可能性が高い性質）のことを汎用性と呼ぶことができる。

本稿では、このような流通性・汎用性を有する決済手段に限って、（狭義の）仮想通貨の検討対象とする。他の定義によれば、交換可能なゲーム内通貨、交換可能でないゲーム内通貨、交換可能な企業発行ポイントなどを（広義の）仮想通貨に含む例もある。しかしながら、これらは原則として汎用性を備えておらず、転々流通性を有していない。このため、現状においては、これらを仮想通貨には含めないこととする。

Bitcoinシステムにおいては、価値の保有者同士の価値の移転が実現されており、それ故に仮想通貨bitcoinには転々流通性が認められる。この性質は、従来の電子マネーには一部の例外を除いて備わっていなかったものであり、分散型仮想通貨が現金に類似した動きを見せる根拠となっている。

1.3 国家の裏付けの不在

国家の裏付けが無いということが、仮想通貨の要素の１つに挙げられる。もっとも「国家の裏付け」といっても、それが何を意味するのかを考察するときには、２つのアプローチがある。その１つは、国家が、通貨の発行体としてすべてを管理するという立場である。もう１つは、国家が通貨の流通について、強制通用力を法的に準備するという立場である。通貨それ自体については、必ずしも国家の裏付けは必要条件ではない。むしろ、国家の裏付けというのは、通貨の歴史から見たときには、比較的に新しい現象であった。

分散型仮想通貨の代表であるBitcoinシステムには、国家の裏付けが存在しない。しかしながら、分散型仮想通貨の流通に対して国家が強制通用力を与えるということは不可能ではなく、今後の可能性としては議論に値する。これらに対して、中央型仮想通貨の場合に

図表２　ブロックチェーンおよびBitcoinシステムに関する７つの神話

Myth 1	分散型元帳としてのブロックチェーンは、Bitcoin システムにおける仮想通貨 bitcoin と切り離して成立し得る。
Myth 2	仮想通貨 bitcoin は、数万もの合法的な商店において利用されている。
Myth 3	Bitcoin システムのトランザクションはリアルタイムで処理されている。
Myth 4	Bitcoin システムのトランザクションのコストは限りなくゼロに近い。
Myth 5	Bitcoin システムは、それ以外の決済システムよりもセキュアである。
Myth 6	Bitcoin システムのエコシステムは分散化されている。
Myth 7	Bitcoin システムは、理想的かつ非営利的である。

［出典］ Therese Torris, Busting 7 Blockchain & Bitcoin Myths, Crowded Media Group, 2015.
http://www.crowdfundinsider.com/2015/12/78702-busting-7-blockchain-bitcoin-myths/

は、特定の発行者が存在するのであって、国家を発行者とする中央型仮想通貨を発行することも想定しておく必要がある。

2. ブロックチェーンおよびBitcoinシステムに関する７つの神話

Bitcoinシステムおよびブロックチェーン技術に関しては、インターネット経済を変革する可能性が議論される一方で、その応用の限界についても議論されている。こうした議論の１つとして、貨幣的価値の電子化を実現させたBitcoinシステムに一定の有用性が認められるとしても、Bitcoinシステムを構成する主要な要素であるところのブロックチェーン技術の応用可能性には一定の限界があるのではないかという主張が存在している。

こうした議論をまとめた論稿の１つとして、Therese Torris[2015]は、ブロックチェーンおよびBitcoinシステムに関する7つの神話として、次のように指摘する。(図表2)

7つの神話の1つ目として、次のような疑問を提起する。

Myth 1

分散型元帳としてのブロックチェーンは、Bitcoinシステムにおける仮想通貨bitcoinと切り離して成立し得る。

Bitcoinシステムにおけるブロックチェーンを強固に分散化している要因は、仮想通貨bitcoinに特有の暗号アルゴリズムおよび特有のネットワークプロトコルの存在である。これは、仮想通貨bitcoinのプロセッサーに相当する「マイナー(採掘者)」たちが、競争的にbitcoinの取引を検証して正当性を確認するという方式を決定付けている。従って、

Myth 1のように考えることは、水を構成する分子構造H_2OからOxygenだけを分離しても水の性質が得られると勘違いするのと同じようにナンセンスである。

Therese Torris [2015] がMyth 1のように指摘することは、ある条件の下においては正しい。ここでいうOxygenとは、おそらくBitcoinシステムの一部を構成するブロックチェーンのことを指すと思われる。そして、取引を検証して正当性を確認するためのProof of Workのプロセスが存在しなければ、仮想通貨 bitcoinが成立し得ないとする。ここまでの指摘は、Bitcoinシステムの説明としては確かに正しい。

しかしながら、ブロックチェーンに記録された取引を検証して正当性を確認するための方法は、Bitcoinシステムに実装されているProof of Workのプロセスだけに限られるものではなく、他の方法が存在する。その具体例として、保有量に応じて検証の権限を与えるProof of Stakeの手法や、ブロックチェーンに参加するノードの重要性に応じて検証の権限を与えるProof of Importanceの手法など、複数の手法が提案されている。

このように考えると、「水を構成する分子構造H_2OからOxygenだけを分離しても水の性質が得られるのか」という議論の立て方が、この問題の本質であるのかはやや疑問である。むしろ、ブロックチェーンの性格に応じて、最も適切な検証方法を選択することが好ましい。すなわち、「マイナー」たちが競争的に取引を検証するというBitcoin システムが採用するProof of Work 方式は、ブロックチェーンの正当性を確認する唯一の手法ではない。

あえて、Myth 1の疑問に応えるならば、次のように記述することができよう。

分散型元帳としてのブロックチェーンには、システ

ムを構成するノードの性質によってさまざまなタイプがあり得る。これらは、Bitcoinシステムにおける仮想通貨 bitcoinの正当性を検証するプロセスとは、不可避的に紐付けられるものではない。従って、Bitcoinシステムにおける仮想通貨 bitcoinとはいったん切り離して、Proof of Workのプロセスまたはこれに代替する適切な方法によって、取引を検証して正当性を確認すればよい。

ただし、これらの代替的な正当性を確認する方法については、その有効性は十分に検証された段階にあるとはいえない。それ故に、ブロックチェーンそのものの可能性についての議論と検証は、まだ始まったばかりの段階にあるとみるべきであろう。

3. 貨幣の歴史にみる仮想通貨の性質論

3.1 Old Money, New Money
――貨幣の歴史をたどり、仮想通貨の位置付けを探る

果たして仮想通貨とはいかなる存在なのであろうか。これを探るためのきっかけとして、貨幣の歴史に学ぶという方法が思いつく。貨幣の歴史と仮想通貨の関係について論じたものとして、英国の中央銀行であるBank of Englandの公開した一連の資料は、最も洗練された議論を提供してくれる[3]。

Bank of England が開催したBoE/CCBS Chief Economists' Workshopの資料として、Old Money, New Moneyと題するスライド形式のプレゼンテーション・ファイルが公表された[4]。その冒頭において、Andy Haldane（Chief Economist）は、金融の電子化について見解を述べている。

Old Money, New Money

マネーの大半は、とうの昔からデジタルであった。Bitcoinシステムや、その他の分散型元帳がデジタルであることは、何ら真新しいことではない。デジタル通貨の真価は、ありきたりのテクノロジーを全く新しい構成で組み立てたことにある。金融システムの構造とプロセスは、その時代ごとの技術的制約の範囲内において、最大限の進化を遂げてきた。いまや、電子化の流れを妨げるような制約は、もはや存在しない。

初めて銀行にコンピュータがやってきたとき、確かにシステムはデジタル化された。だが、紙の記録を中央に保管していた時代と比べて、根本的な変化が起こったわけではなかった。新しい技術によって、何が可能となるのかを考え、そこからヒントを得て改革するということはなかったのだ。

New processes lag new technology
…プロセスの革新は、技術革新に遅れて実現する

金融システムがデジタル化されていくプロセスは、1世紀以上も前に起こった、工場が電化されていったプロセスを再現するかのようである。巨大な蒸気機関で動かされていた工場設備を電気モーターに置き換えても、当初は、工場の生産性はほとんど向上しなかったことが研究によって明らかにされた。

ようやく生産性が向上したのは、新世代のエンジニアが電気モーターを使いこなすようになってからだ。彼らは、工場の生産プロセスに無駄がないか再考し、産業には革命がもたらされた。

ここまで至るのに、30年もの歳月を要した。

電気モーターが初めて工場に導入されてから生産性が向上するまでに要した30年という年月は、工場の支配人がリタイアしてエンジニアが世代交代するまでの期間に匹敵する。実のところ、銀行に初めてコンピュータが導入されてから生産性の向上につながるまでには、やはり30年の歳月を費

やしたのである。

3.2 Digital Currencies—What History Teaches Us
デジタル通貨——歴史が示唆するもの

同じく、Bank of England が開催した BoE/CCBS Chief Economists' Workshop の資料において、Michael Kumhof（Senior Research Adviser, Research Hub）は、貨幣の歴史からデジタル通貨の意義を読み解こうとする。そして、交換の媒体（貨幣）を成立させる要素は、テクノロジーとトラストの２つに分解されると説明する。（図表3、図表4、次頁）

これらの図表は、次のように読み解くことができる。

テクノロジーの軸として、貨幣はトークン型の構成とクレジット型の構成との間を振り子のように揺らぎながら発展してきた。ここで興味深いことは、直線的に発展したのではなく、振り子のように長い年月をかけて揺らぎながら発展してきたことである。これは、もう１つの軸である権威の源泉と併せて読むと、螺旋状に発展してきたと読むことができる。

トラストの軸においては、貨幣が成立するための権威の源泉として、古代オリエント帝国の王権のような強い権力を背景として実現されてきた名目的価値が、次第に銀行制度のような民間によって作られた仕組みへと緩やかに移行していく様子が読み取れる。その先に存在する仮想通貨は、国家のみならず民間の発行主体さえも持たない究極的に非主体的な仕組みである。

だが、仮想通貨がすべて非主体的な仕組みであるとも限らない。中央型仮想通貨には主体が存在しており、国家がその発行主体となることもできる。発行主体の存在しない分散型仮想通貨においても、制度の関与が検討される余地はある。1.3節で議論したように、国家の関与には２つの立場があって、通貨の発行体としてすべてを管理するという立場と、国家が通貨の流通について強制通用力を法的に準備するという立場があり得る。後者を念頭に置くならば、国家の権威を源泉としたSovereign Currencyとしての分散型仮想通貨というのも可能性として残る。

3.3 Many Possible Futures
——いくつかの将来像

貨幣の歴史を概観したMichael Kumhofは、貨幣の将来像を見通して次のように論じる。

テクノロジー

貨幣の進化は、トークンの時代へと回帰しているようだ。しかしながら、トークンとクレジットを組み合わせたあらゆるシステムを実現することができる。

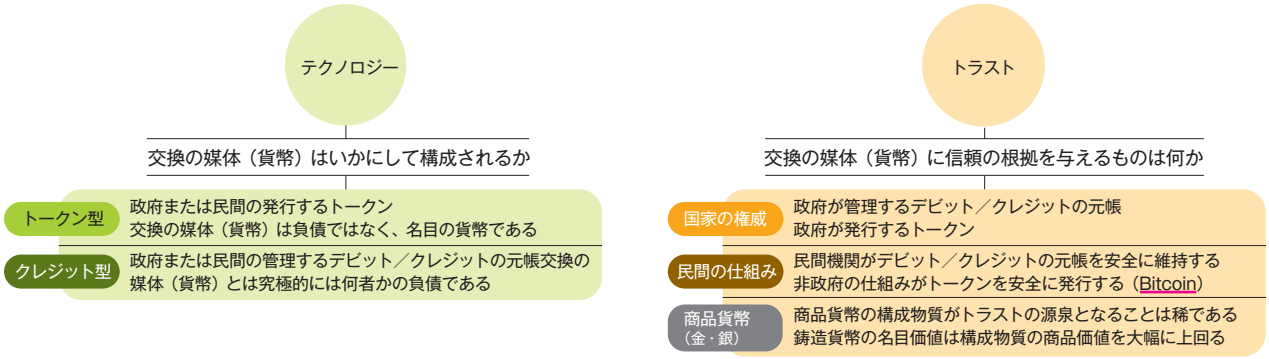
トラスト

分散型仮想通貨は、完全なる意味において民間によるトラストの時代をもたらした。だが、国家が発行するデジタル通貨においては、トラストは再び国家の手に戻り、国家の権威によって独占的にもたらされる。そして、民間の工夫と国家の権威を組み合わせたさまざまなシステムが存在し得る。

Michael Kumhofの歴史考証が示唆するもの

分散型仮想通貨は、法人または自然人としての発行主体を置かないことを最大の特徴とするものであるから、これを民間による仕組みであると理解することが果たして妥当であるかは疑問が残る。少なくとも、国家の権威を背景としたトラストの仕組みではないと理解することは妥当であろう。むしろ、Michael Kumhofの歴史考証のユニークな視点は、国家の権威によるトラストの仕組みと民間の工夫によるトラストの仕組みが、時代を経て変化しながらも長い間にわ

図表３ Two Key Characteristics of the Medium of Exchange
―― 交換の媒体（貨幣）を特徴付ける２つの要素



［出典］ Michael Kumhof [2015], A brief history of money, Old Money, New Money, BoE/CCBS Chief Economists' Workshop, Bank of England, 19 May 2015.
http://www.bankofengland.co.uk/research/Documents/conferences/ah0515.pdf （スライド資料を元に要約した。一部の表現を修正している。）

図表４ Five Major Eras in the History of Economic Exchange
―― 経済交換の歴史における５つの時代区分

初期農業帝国――メソポタミア文明（BC600以前）	クレジット型	トークンが発明される数千年前の時代
	国家の権威	公共上または宗教上の根拠から元帳を管理する。市場における物々交換の制約は未解決であった
ギリシャ・ローマ・インド・中国文明（BC600 – AD600）	トークン型	鋳造貨幣の名目価値は商品価値を凌ぐことが通例。この時代の後期には、希少金属の貨幣も登場する
	国家の権威	鋳造貨幣への信頼は国家の権威のみを源泉とする
中世（AD600 – AD1453）	クレジット型	概念上の単位に基づいて元帳を管理
	国家＋民間	割り符や元帳による経済。国家または民間が管理
	国家の権威	わずかに鋳造貨幣も存在した
絶対王政（AD1453 – AD1945）	トークン型／クレジット型	金銀貨および預金通貨の時代
	国家＋民間	銀行の貸付残高を根拠とした預金通貨が流通する。預金通貨は政府／中央銀行のバックアップを前提
	国家の権威	金銀貨は 1204 年以降（殊に 1492 年）重要性を増す
WWⅡ以降（AD1945 –）	クレジット型	銀行が管理する元帳
	国家＋民間	銀行の貸付残高を根拠とした預金通貨が流通する。預金通貨は政府／中央銀行のバックアップを前提

［出典］ Michael Kumhof [2015], A brief history of money, Old Money, New Money, BoE/CCBS Chief Economists' Workshop, Bank of England, 19 May 2015.
http://www.bankofengland.co.uk/research/Documents/conferences/ah0515.pdf （スライド資料を元に要約した。一部の表現を修正している。）

たって共存の関係にあり、必ずしも競合の関係にはないという事実に求められる。もう１つのユニークな視点は、金貨や銀貨に代表されるようなトークンの時代と、古代文明や現代の銀行が管理する元帳のような仕組みとの間を振り子のように揺れ動きながら、今のような銀行システムが形成されてきたという事実に着目したことである。

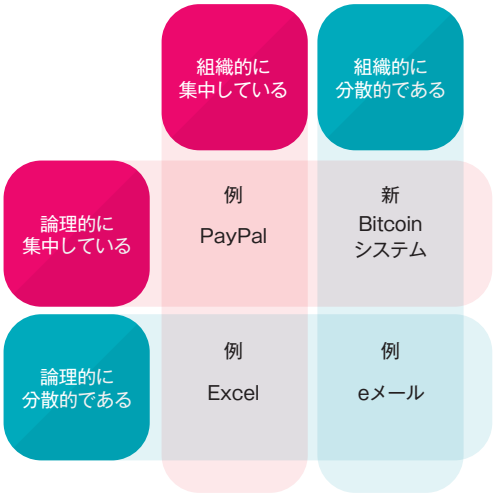
それでは、分散型仮想通貨は将来どのような姿で残るのであろうか。あるいは、将来には残らないのであろうか。このことをMichael Kumhofの歴史考証に重ね合わせて分析してみたい。分散型仮想通貨は分散型元帳をベースとしているため、定義によってはクレジット型に分類されそうである。一方で、人から人へと転々流通する性質を有していることは、あたかも現金と類似しておりトークンに近い役割を果たすといえる。おそらく分散型仮想通貨は、従来の分類におけるトークン型またはクレジット型のいずれかに該当するとはいえない。なぜなら、従来はクレジット型の金融システムは集中された元帳に記録を保存していた。これに対して、分散型仮想通貨の元帳は地理的に１つの地点に存在しているわけではなく、P2Pで構成されたネットワーク上に一意のものとして存在している。

4. 分散的な性質と集中的な性質の中間形

分散型仮想通貨はクレジット型あるいはトークン型のいずれの性質を備えているのであろうか。言い換えれば、集中的な性質あるいは分散的な性質のいずれを備えているのであろうか。分散型仮想通貨に特有のハイブリッドな性質について、Albert Wenger [2014]の論稿は図表５のような2×2のマトリクスで読み解く。

こうして2×2のマトリクスに分類する根拠につい

図表５ Bitcoin:Clarifying the Foundational Innovation of the Blockchain
――Bitcoinシステム：ブロックチェーンの本質的なイノベーションを明確にする



［出典］ Albert Wenger [2014],
Bitcoin: Clarifying the Foundational Innovation of the Blockchain
http://continuations.com/
Posted: 15th December 2014

て、Albert Wenger [2014] は次のように論じる。

従来の電子的な決済システムは、PayPalに代表されるように単一の組織が運営していて、論理的にも一意に統合されていた。これに対して、分散型データベースを組織内で構成する場合には、1つの元帳に対して地理的に分散した各自がアクセスして、それぞれが別のものに加工することができた。eメールはさらに分散的であって、分断されたデータベースに各自がアクセスして、送信者または受信者の一方だけが1個のデータを削除することもできる。

ところが、分散型仮想通貨は特定の主体が運営するものではなく、P2Pネットワークに参加する全員で維持するものであるから、組織的には分散しているのにもかかわらず、論理的には世界に1つだけの元帳を全員が見ている。このようなマトリクス上の組み合わせは、これまでに存在したことがない。それ故に、分散型仮想通貨におけるブロックチェーンという仕組みは、根本論としての新しさを持つのである。

5. FC2016における議論 ——1995年の電子マネー・2016年の仮想通貨

5.1 eCashの設計思想

eCashという電子マネーは、著名な暗号学者であるDavid Chaum博士が開発したものであって、1995年に商用サービスを開始し、実際に電子マネーとしてのeCashが流通した。インターネットが商用利用を開放したときから予言されていた電子マネーが、ついにこの世に登場した瞬間であった。eCashはのちに運営主体を変更して、本拠地をオランダのアムステルダムからパロアルトへ移すのだが、国境を越えて流通するインターネットの特性そのままに、日本においても少額ながら実際に使用された記録を残している。

eCashは、ブラインド署名によって匿名性を実現したユニークな形式であって、本稿で定義するところのサーバ型電子マネーに相当する構造であった。それは、インターネットという自由度の高いネットワークの上で、金銭価値が正しく移転することを実現してみせた初期の試みであった。

これまで各国の中央銀行が発行していた通貨を、それ以外の主体が発行するという事実は、たとえ法定通貨の裏付けの存在するものであったとしても、歴史に残る出来事であった。こうした電子マネーのどれか一つが、法定通貨の裏付けを失っても流通するほどの規模に至れば、独立した通貨としての地位を占める可能性もあったからである。インターネットという統制の及ばない領域において、現実世界に代わる通貨が登場しようとしていた。

こうして、インターネット上に新たな通貨が流通することの意味が、あらゆる機会を捉えて話し合われた。結局のところ、インターネットに新たな経済圏を出現させるほどの影響を持った通貨というのは、当時はついに現れることはなかった。だが、インターネット時代における通貨の役割とは何かという問題に、多くの専門家が知見を提供したことは、その後のインターネット社会の進歩と変化に備える礎となった。

5.2 カリブ海の島国を舞台として

Financial Cryptographyという会議は、1997年から続く金融暗号学者の会議であって、2016年には20年目の開催を迎えた。Anniversaryとして企画されたパネル討論には、RSA暗号の祖の一人であるAdi Shamir博士や、eCashの開発者であるDavid Chaum博士らも登壇した。

金融を支える技術は、長らく米国と欧州が意見を交えながら規制の在り方を議論してきた。しばしば中南米諸国で開催されてきた会議には、両岸から技術者と政策学の研究者が集まり、忌憚のない議論が繰り返された。2014年からは、Workshop of Bitcoinが併催されるようになり、仮想通貨の技術と政策について議論を深める場となった。

分散型仮想通貨は国家のコントロールの及ばない貨幣的価値を流通させることによって、これまでの国家・経済・社会の枠組みに再考を促そうとする。それらの多くは制御できない性質を最大の特徴としているが、これに統制をもたらすのが人智である。開発者の手を離れて自由に流通する貨幣的価値を一元的にコントロールする主体がなくとも、これを社会の道具として御すことは人智の及ぶところである。

21世紀の発明品である分散型仮想通貨を使いこなせるか否かは、これからの技術の進歩と政策の行方にかかっている。20世紀末に多くの人が否定した電子マネーは、いまや生活を支える基盤となった。未知の技術に対する疑念を越えて、有益な道具へと変えていくことができるだろうか。歴史の教訓に学びながら、仮想通貨の将来を見通したいと思う。

Hitoshi Okada

岡田 仁志

国立情報学研究所 情報社会相関研究系 准教授

東京大学法学部第一類・第二類卒業。大阪大学大学院国際公共政策研究科博士後期課程中退。博士(国際公共政策)。2000年より現職。

総務省情報通信政策研究所特別上級研究員を兼任。総合研究大学院大学複合科学研究科情報学専攻准教授を併任。電子情報通信学会 技術と社会・倫理研究会副委員長。IEEE SSIT Japan Chapter Vice Chair。主たる共著書に『仮想通貨――技術・法律・制度』(東洋経済新報社・2015年)など。

注

1) 岡田仁志・高橋郁夫・山﨑重一郎 [2015]による定義論に依拠している。
2) 決済手段の電子化としての貨幣的価値そのものをbitcoin通貨と呼び、決済プラットフォームとして貨幣的価値の流通を可能にしている仕組みをBitcoinシステムと峻別する呼び方も存在する。本稿ではこの峻別法を試みるが、両者は不可分一体であって常に峻別できるとは限らない。
3) 本章での議論は、Bank of England [2015], Old Money, New Money, BoE/CCBS Chief Economists' Workshop, 19 May 2015に依拠している。
4) Andy Haldane [2015], Old Money, New Money, BoE/CCBS Chief Economists' Workshop, Bank of England, 19 May 2015. http://www.bankofengland.co.uk/research/Documents/conferences/ah0515.pdf

特集論文

仮想通貨2

仮想通貨の健全な発展について考える

松山短期大学 学長／教授

上杉 志朗 Shiro Uesugi

仮想通貨は、近年注目を集めている金融分野における情報技術革新「フィンテック」の最先端にある。
フィンテックを利用しているのは、既存の金融関連企業だけではない。
むしろ、技術革新をうまく利用して金融サービスに新規参入する事業者が目立つ。
仮想通貨をフィンテックの一つとして捉える考え方がある。
必ずしも仮想通貨はデジタル技術を前提としているものではない。
しかし、情報技術論的視点から仮想通貨を捉えると、ビッグデータ関連の技術や、
ブロックチェーン技術など、デジタル技術が基盤となっている。
社会の在り方や働き方に大きな影響を与える可能性があり、
必要に応じて新たな規制が考慮される場合があろう。

キーワード
フィンテック　ビッグデータ　決済機能　ブロックチェーン　サイバネティックス

1. はじめに

メディアや市場においては、フィンテック（FinTech）という言葉が盛んに用いられており、『FinTech革命』（日経BPムック）と題するムック本も発行され、フィンテック関連株が人気を集めたりしている。フィンテックは情報技術（IT）の中でも最も有望で将来性のある技術革新（innovation）であり、殊に、仮想通貨ビットコインで実装されたブロックチェーンの技術は、大発見かつ大発明である。国際的な金融機関の合従連衡の中で生き残りをかけているメガバンクは、フィンテック関連の国内外のベンチャーに多額の投資を惜しまない。

確かに、フィンテックや仮想通貨の潜在性は大変魅力的でかつ大規模なものだ。現実のシステム開発や、遅れまいと進む制度の整備は、この大きな潜在性への

期待をかき立てるものだ。しかし最近のトレンドを少し引いたところから見てみると、混沌とした状況が見える。新しくて熱狂を招く部分と、静かに進行している革命が入り交じっていて、うねりをなしている。

そこで、本論では、もつれた糸を解きほぐし、混沌を少しでも見やすくできないか、そのような視点から論じてみた。まずは、最近とみに注目を集めているフィンテックが、以前からもてはやされてきているビッグデータとの関係でいえばどのようなものか考えてみたい。次に、フィンテックがこれほどまでに注目を集めるようになったきっかけをつくった仮想通貨について、そのフィンテックにおける位置付けに着目して述べてみたい。最後に、今後の規制の在り方について述べよう。

2. フィンテックとビッグデータ

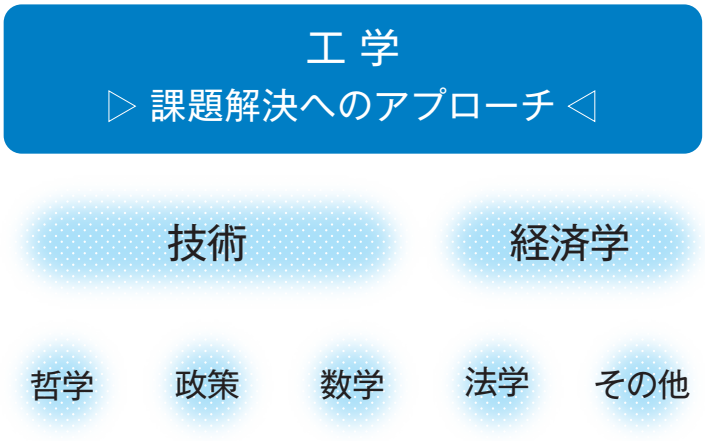
2.1 フィンテック

フィンテックは、FinTechすなわち、Financial（金融）とTechnology（技術）という英語単語の冒頭部分をつなぎ合わせたものとして定義される。中でも、情報通信技術を駆使して、これまでの金融とは異なるビジネスモデルやサービス、システムなどの提供がなされるイメージが強い。それでは、金融と技術の融合は今に始まったものなのだろうか。

日本には、昭和の終わりから平成の初めにかけてのバブルのころにもてはやされた金融工学があり、Financial Engineeringと同様に取り扱われてきた。大手の証券会社や都市銀行などの金融機関においても、理工系学部や大学院の出身者の採用が目立ったものだ。そのころは、数理モデルを用いて、証券や債券のオプションなどデリバティブと呼ばれる金融派生商品の開発にこれら「理系」の頭脳を活用したり、経営情報システムを与信先企業の財務分析に適用したり、金融機関自身のALM（Asset Liability Management：資産・負債総合管理）に活用したりすること一切、つまり、金融業界における工学的アプローチが金融工学として扱われていた。

もっとも、一橋大学教授の祝迫得夫によれば、米国においてFinancial Engineeringといえば「数量的な側

図表1　工学と技術の関係



面を重視した目的志向型のファイナンスという学問の実践」という、金融の「実務家の側（Practitioners）の立場から見て必要な知識、特に数量的なスキルに限定」されたものを意味しており、上記のような日本のバブルのころにもてはやされた金融工学は金融工学ではない、とされており、誤用もしくは誤訳と解される。

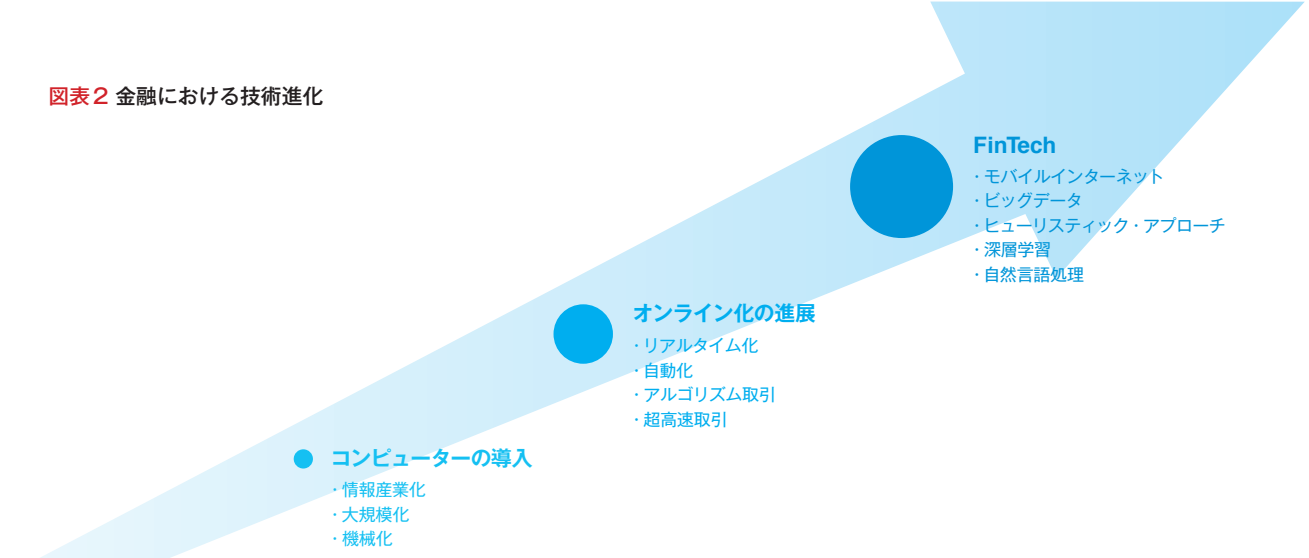
このような混乱が生じるのは、工学（Engineering）と技術（Technology）の概念に包摂関係があって、技術は工学を構成する要素概念だからである。つまり、工学は、ある分野における課題を解決するために必要な一連の手法を総括する概念であり、技術的、政策的、経済的、哲学的、法学的、数学的とさまざまなアプローチを駆使する（図表1）。金融において、技術的側面に重心を据えて、その視点から課題を解決する工学的アプローチをするならば、それは、金融技術であり、金融工学の一部であるという関係が描ける。しかも、金融分野においては、技術革新が新しくパラダイムそのものを創り出したり、古いビジネスモデルを完全に書き換えるようなことが起こったりするため、技術と解決すべき課題との主客逆転が起こったりして混乱を招く。

例えば、コンピューターという技術革新によって、銀行の記帳がシステム化されると、大量に、より早く、正確に記帳処理ができるようになったが、それだけにとどまらなかった。データ化の技術自体が、オンライン化へとさらに技術進化を加速させ、銀行業の在り方そのものを、データ処理能力が特定の企業の競争力を規定するようなビジネス、言い換えると、情報産業へと変貌させた。

フィンテックは、広義に考えると、このような連綿と続く金融の情報化と、それと同時進行している金融産業のデータ処理産業化から情報処理産業への進化の大きな流れの上に乗っている。革新的情報技術が開発されるたびにそれを取り込み進化し、その進化がさらに技術革新を生むというフィードバックを繰り返しながら歩んでいる（図表2）。

従って、狭義のフィンテックが、近年の革新的情報技術、例えば、モバイルコンピューティングの進化やブロックチェーンの発明、人工知能を利用したビッグデータの解析などを格別に取り上げていることは驚くに値しない。これまでにも、オフショア市場や、デリバティブ、オプションの発明や、オプションのデリバティブ、クレジットデフォルトスワップ（CDS）の発明、システムトレーディングなど、ノーベル賞を授与されるほどの

図表2 金融における技術進化



革新的技術が鳴り物入りで供されてきたことからも明らかだ。

しかしながら、金融の世界にビッグデータ解析の技術が応用されることは、それまで行われていた顧客プロファイルの統計的な分析などとは格段に違う意味を持っている。

2.2 ビッグデータ

2013年に公刊された、鶴田規久監修・日本IBM金融インダストリー・ソリューションによる『2020年金融サービス――ITと融合するリテール金融の未来像』（東洋経済新報社）は、フィンテックという言葉を喧伝することなく、金融業界のリテールビジネスにおける情報技術の利用を明確かつ網羅的に描いているのだが「リテールにおけるフィンテック」と題してよい内容だ。この中で描かれているように、未来の金融サービスにおいては、20世紀的な常識では、手間ばかりかかって収益につながらない、と考えられたようなリテールビジネスが、銀行、証券、ノンバンク、保険などの金融業界において、十分にビジネスとして成立する。ただし、その背景にあるのは、個人レベルにほぼ普及し尽くしているスマートフォンや携帯電話、ICカード式電子マネーやポイントカードといったネットワーク型のハードとソフト（アプリ）が一体化したインフラに加え、ウェブサイトのcookieやオンラインゲーム、今後はマイナンバーなど、これらのインフラの上で動くネットワーク型のサービスが、それぞれは別々の顔を持ちつつ個人に提供されていながら、統合的に個人の行動履歴や購買履歴などの情報を収集するメカニズムと、それを分析する統計的ならびに数理的手法が必要である。

ビッグデータがフィンテックの文脈で重要なのは、上記の大きく分けて2つの側面からだ。まず、個別の個人情報を統合するという点だが、特定の個人へのサービスの精度を向上させるために用いられると、より高い満足度をもたらし、差別化ができる。また、与信上の危険を正確に判断できると、リスク別の課金条件を定めて損失を減らすことができる。いずれの場合にせよ、金融業界の利益に貢献する。

次に、分析手法についてだが、従来の統計的手法では、サンプルから母集団を推計して、個別の行動の推計に還元させてきたが、ビッグデータを分析する際には母集団そのものを対象として、その母集団の特徴を描くことができるようになった。母集団全体のプロファイルを高い精度で認識できるようになったわけで、結果として、一個人のプロファイルの特定にしても、精度が上がりプライバシーの侵害が問題になるほどだ。アメリカで、スーパーマーケットから女子高校生にマタニティー用品やベビー用品の割引券入りのダイレクトメールが届いたことに驚いた父親が抗議したところ、父親が知らなかっただけで事実妊娠していたのだった、という話は有名である（Duhigg 2012）。

さらに、データの集め方が変わったことによって従来型の統計的手法の精度が向上したこと以外にも、データ解析方法が革新的な進化を遂げている。人工知能と呼ぶにふさわしい深層学習（Deep Learning）手法に代表される機械学習の研究と実用化が加速度的に進展してきており、1997年にIBMのディープ・ブルーがチェスで人間を破って以来、後継のワトソンが2011年にアメリカのクイズ番組 Jeopardy! で優勝したり、自然言語処理が実用化レベルに達したりしてきたが、2016年にはGoogle傘下のディープマインド・テクノロジーズが開発したアルファ碁が人間のトップ棋士を破るまでに至っている。これは、コンピューターが、自然言語処理を人間のように行い、人間の学習スタイルを学習して、構造化されていないデータを取り扱いながら、自ら探索的に解決手段を考え出して物事を解決するものだ。いわば人間の能力を凌駕する能力を

持った人間的な思考をする機械だけれども、「サイバネティックス」の発案者であるウィーナーが『人間機械論』(1979)の中で「学習機械」と呼んでいるものに他ならない。

ウィーナーは言う。「学習機械においては、その機械が習うことのできることと、できないこととを区別することが肝腎である。ある一定の種類の行動を統計的に優先して選び、しかもそれ以外の行動もとる可能性をもつ機械を作ることもできるし、行動の或る諸特性が厳格かつ不変に決定される機械も作れる」(同書188ページ)。そしてそのような機械は、ドミニコ教団の修道僧デュパール神父がウィーナーのサイバネティックスを評して、「統治機械(machine à gouverner)」で描くように、「人類を自動的に管理する」には「無力」であるとする。機械による統治が危険なのではなく、むしろ「あたかも機械によって算出されたかのような狭くて人間の可能性を無視した政治的技術によって管理しようとすること」が「危険」であるという(同書193ページ)。そして、その根拠として「機械が支配しうる社会は、エントロピー増大の最終段階にあるような社会であり、そこでは確率など問題にならず、個人の間の統計的差異は無視しうる。幸いにも、われわれはまだそんな状況に達してはいない」(同)と結んでいる。

同書は情報学のロードマップを考える上でさまざまな示唆に富んだ書物であることはもちろん、自動機械が「奴隷労働と経済的に同等」(同書170ページ)であるので「奴隷労働と競争するどんな労働も、奴隷労働の経済的条件を甘受しなければならない」(同書170ページ)、そして「新しい産業革命は両刃の剣である」(同書171ページ)と指摘する。ブリニョルフソン等が『ザ・セカンド・マシン・エイジ』(2015)で描いている世界をすでに予言している。1954年に刊行された第2版が原書であるので、半世紀超経て、われわれはウィーナーが危惧した社会に住んでいることになろう。

3. 仮想通貨

ビッグデータがフィンテックの車の両輪のうちの一つだとすると、もう一方の車輪は仮想通貨だ。ここで注意しなければならないのは、本来ならば、ビッグデータと仮想通貨を並列で論じることには無理があるということだ。まず、仮想通貨は必ずしも電子媒体を前提とはしていない。切符やクーポン券のように紙媒体の仮想通貨であっても一向に不都合はない。仮想的に通貨の役割を果たすことができるモノであれば、かつて地域通貨が全国で盛んに興ったときに、愛媛県の玉川町(現在は合併して今治市)で使われていた地域通貨「バンブー」のように、輪切りにした特産の「竹」で

も構わない。

しかしながら、フィンテックの文脈で語られる仮想通貨は、電子的媒体を使用することを前提としている。そして、恐らくこのことが、金融業界において静かな革命が進行していることを見えにくくしている、もしくは、その逆にあまりに誇大に語られるが故にかえって事の重大さを見えにくくしている原因ではないか。

そもそもフィンテックと仮想通貨の議論では、岡田仁志他が『仮想通貨』(2015)で行っているように、「技術」「法律」「制度」から複合的にアプローチをかける必要がある。同書では、米国のFBI(Federal Bureau of Investigation連邦捜査局)による定義「ネットワーク、代表的には、インターネット、を通じて流通(circulated)する決済の手段(medium of exchange)であって、国家の裏付けを有しないものと定義される仮想通貨は――ビットコインのような分散型の決済の仕組みでも、リバティ・リザーブのような中央管理型の決済の仕組みであってもありうる」(同書3ページ)を整理して、「国家の裏付けがなく、ネットワークを通して流通する決済手段」(同書3ページ)と定義している。ネットワークの利用を前提として論じられるのが現在の傾向だ。

繰り返しになるが、仮想通貨は、電子媒体に実装され、ネットワークを介することになり、金融に革命的な変化を引き起こしている。つまり、情報技術の一応用分野として大きな存在となっている。そうだからこそ、現在における金融分野の技術的革新、フィンテックの主要な要素となっている。では、なぜ電子化された決済手段が革命的なのか、まず、仮想でない通貨について述べ、次に仮想通貨について述べながら考察してみよう。

3.1 仮想でない通貨

一般に、通貨は国家が定めてその圏内で通用させている決済手段である。従って、その通用範囲に大きな経済的影響力を及ぼし、国家的権威の象徴でもある。現代社会では、貨幣や紙幣が代表例だが、手形や小切手、要求払い預金、国債なども通貨の機能とされる3つの特徴を持っている。すなわち、交換機能、保蔵機能、尺度機能である。

3.1.1 特徴

歴史的には、貨幣経済の進化に伴って通貨は発達してきた。通貨の機能が維持されなければ大きな社会的混乱を招く。また、通貨を発行すると、発行者には大きなシニョレッジ(seigniorage:通貨発行特権、またその利益)がもたらされる。そこで、国家が通貨を管理監督する仕組みが発展して、その制度的フィードバックも働き、さまざまな金融機能が開発され、技術革新とともに市場が拡大した。このようなフィードバック

が繰り返されて、現在では、実体経済の規模の何倍もの金融市場規模が作り出されている。

例えば、ユーロの例をとってみよう。欧州連合は一つの国家的権威である。複数の国家が連合体として一つの国家を形成している。その経済圏内で通用するのがユーロだ。イギリスが欧州連合を離脱したいと言ったときに現実味を帯びてくるのは、イギリスはユーロを通用させておらず、独自の通貨ポンドを堅持しているからだ。通貨に関わる国家的権威と権益を維持しているので、欧州連合を離脱しても、ユーロ圏から仲間外れにされようがなく、困らない。これが、ギリシャのように経済危機に瀕した場合には逆に働いて、ユーロ圏から切り離されることがギリシャの脅威になる。国家的権益の共同利用をストップされるのと同じだからだ。

現代社会において、通貨は必ず制度的に定められるべきものだ。世界が法治国家からなっているとすると、制度的に定めるということは、法的に定められるということと同義だ。従って、通貨をどのように定義するか、そして、運用上の規則においては、通貨の価値を維持するためにどのような制度と法律を定めるかは国家の関心事となる。そこで、通貨として定めていないが、通貨のように受け止められ、通貨のように振る舞う「モノ」や「コト」は、自国の通貨制度に有害でないかどうか見極めなければならない。その結果次第では、単に法律に定めがない通貨様の「モノ」「コト」が、通貨類似の「疑似通貨」としての振る舞いを通して不法に用いられないように制度を整備しなければならない。また、「疑似通貨」が通貨の領域を侵す違法性を持つのかどうかについて検討しなければならない。

3.1.2 決済機能概念の重要性

通貨様の「モノ」「コト」には、前払式証票（いわゆるプリペイドカードや商品券など）のように、消費者保護の観点から法律で規制されている場合があるので、必ずしも国家的に通貨を防衛する必要から制度設計がなされているとは限らない。しかしながら、通貨にも疑似通貨にも共通するのは、尺度化が可能な「価値」があって、他者との交換が可能だということだ。物々交換とは異なる方法で、価値をやり取りするために使うことができる。ここで重要なのは、「価値」を尺度化（測定）できるだけではなくて、交換が後々のトラブルの種にならないように、交換の記録が第三者にも公正に伝えることができるという機能だ。これは決済機能に他ならない。

それでは、逆に決済機能を設計するとすれば、どのような要件が必要か。実は、先ほど述べた「記録を第三者に公正に伝えることができる」というだけで必要十分だ。要するに、克明な記録があれば、通貨を使用しようとしまいと決済は完結できるわけだ。決済で用

いられる技術的要件は「いつ」「どこで」「誰が誰に」「いくら」「何のために」「どのように」支払ったかという情報を記録することだ。乱暴な言い方をすれば、5W1Hの情報を真正に確実に記録し、必要な第三者と共有できる技術があれば、決済機能が実装できる。

帝京大学教授の宿輪純一は『決済インフラ入門』(2015)で「国内・海外の金融機関(銀行)間における資金そして証券の「決済システム」に加え、リテール部門の電子マネー、クレジットカード、新しい仮想通貨なども含めた「決済スキーム(仕組み)」などを全体として「決済インフラ」と再定義」(同書4ページ)している。このことは、決済機能が情報技術を利用して電子的に実装されているからこそ重要である。

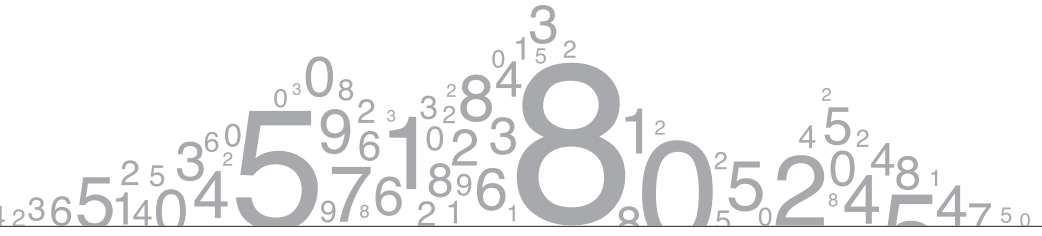
3.2 仮想通貨

岡田他(2015)が想定する仮想通貨は、国家の裏付けがないことから、まず、通貨の定義から外れる。次に、ネットワーク上を転々流通する決済手段であるので、通貨様の機能があることになる。さて、ここで注意をしなければならないのは「仮想」という日本語である。先に通貨様の機能を持った「モノ」「コト」を疑似通貨と呼んだ。「疑似」と「仮想」には大きな違いがある。「疑似」の場合は、「似て非なる」という意味が強い。「記録を第三者に公正に伝えることが決済機能である」、「決済機能は疑似通貨だ」という論理関係からすると「記録は疑似通貨である」という関係が成立する。情報技術を記録システムに応用して、通貨のようだが似て非なる仕組みを作る、と言い換えることができる。

これに対して「仮想」の意味は「仮想敵国」のような場合に使われる「仮に考える」ではなく「バーチャル(virtual)」という意味だ。この「バーチャル」は「リアル(real:現実)」の対義語、すなわち「ノン・リアル(non-real:非現実)」ではない。「バーチャル・リアリティ(仮想現実)」と言ったときの「仮想」は「サイバーワールドの中で構築されているリアル」である。従って、仮想通貨は本来ならば「サイバーワールドの中で利用されている通貨」と理解されるべきだろう。

3.2.1 電脳空間に作られた通貨

それでは、サイバーワールドとは何か。ウィーナーが語源となる「サイバネティックス」概念を提唱した際には、それは、物理的な制御をするための仕組みや、フィードバックを発信し、また取り込むような自動制御を司る方法が何かを明らかにするという概念であった。こんにちの文脈でいえば、自動制御のプログラムやアルゴリズム、シミュレーションなど、電子化、デジタル化された情報によって作られている世界だ。コンピューター上に構築されるので電脳空間とも呼ばれる。



3.2.2 ブロックチェーン技術

ネットワーク化された電脳空間において利用される決済手段を、仮想通貨にする技術として脚光を浴びているのが、ビットコインで実装されたブロックチェーン技術だ。取引記録は、近畿大学教授の山﨑重一郎が「時制式三式簿記」と名付けた「インプット」「アウトプット」「未使用のアウトプットを管理するデータ（Unspent Transaction Output=UTXO）」からなるブロックのチェーン（連鎖）からなっている。送金者が「インプット」部分に、自身の公開鍵を埋め込み、電子署名をし、「アウトプット」部分に受け手の公開鍵のハッシュ値と金額を埋め込んでブロックの元となる「データの塊」を作り、「マイニング」と呼ばれるブロックチェーン作成競争に参加している集団（マイニングプール）に送ると、約10分間の計算競争の結果、参加者全員による検証可能な「プルーフ・オブ・ワーク」が添付されて、それまでのブロックチェーンに追加される。中央集権的な管理者を置くことなく、システムに参加している全員が同じ情報を共有していることで、取引の真正性を確認でき、かつ改変ができないようにしている技術である（日経BPムック142～148ページ）。

この技術が優れている点はいくつかあるが、第一に、システムの構築に数十億円規模の投資をすることもなく、同等の国際決済システムを構築したことだ。第二に、スマートフォンとインターネット接続環境さえあれば、決済活動が完結できるということだ。第三に、スクリプト言語機能により、送金以外のアプリケーションを派生させることができることだ。改変不可能な記録技術の部分を取り出したり、管理者がいなくても国を越えて記録を転々流通させたりすることに利用することができる。多くの関係者が関与する国際的な契約を締結する際に、膨大な量に及ぶデューデリジェンス（Due Diligence：詳細調査）に際して、書類のアップデートへの電子署名などで応用ができそうだ。

ブロックチェーンをリテールに利用するというアイデアは、フィンテックの中では、既存の金融機関の危機意識を煽（あお）っているのではないか。これまで、金融機関は決済業務の信頼性を向上させるために多額の投資をしてきた。フィンテックに置き換えられてしまっては大変だ。新規参入コストが安い決済業務は脅威だ。

3.2.3 仮想通貨に対する規制

とはいえ、2014年に東京で起きたビットコイン交換所の大手企業マウントゴックス社の倒産は教訓を残した。さらに、ビットコインがマネーロンダリングなど違法な目的の温床として用いられても困る。これまで日本政府は、ビットコインは物であり、通貨ではない、としてきたが、方針を転換して、通貨としての法的規制の対象とすることとした。フィンテック関連の競争で諸外国に遅れを取ってはならじ、との気持ちもあろうが、放任しておいて社会的な問題へと発展する危険性を読み取ったこともあろう。健全な形で発展することが期待される。とはいうものの、通貨として国家がどのように関与するのか、特に中央制御機構を持っていないピア・ツー・ピア型の仮想通貨の場合、困難が多いのではないか。

4. 未来

締めくくりに、未来の展望をしたい。フィンテックが世界的に取り沙汰されるようになった背景には、ビッグデータやブロックチェーンに代表される情報技術の革新的進化がある。これまで金融とは無関係と考えられてきた企業が、想像もしない方法で今後も参入してくる可能性がある。世銀グループによるDigital Dividends（デジタルの配当）をテーマにしたWorld Development Report 2016（WDR2016）の27ページにはThe four digital

enablers（4つのデジタル・イネイブラー）が掲げてあり、その第一がDigital financeだ。その中でも「金融関連規制が､急速な技術進化についていけないならば､これらの技術革新が金融システム全体を損ないかねない」とくぎが刺されている。必要以上に自由な競争を阻害することはないが、規制が必要な場合には、大胆な対応が求められる。特に、国境を越える決済はニーズが大きく、金融インフラの整っていない途上国での利用価値が高いだろう。しかし、エネルギーの使用量が大きくエントロピーの増大に資する。ウィーナーが予言したような、機械が支配する社会に無批判につながるようなことがないように心したい。

Shiro Uesugi

上杉 志朗

松山短期大学 学長／教授

1965年京都府生まれ。89年大阪大学経済学部卒業後、東京銀行入行。本店、外務省派遣、融資渉外業務を経て、ハーバード大学ケネディスクールに留学し98年修了。帰国後東京三菱銀行融資企画部勤務を最後に退職。2001年大阪大学大学院国際公共政策研究科博士後期課程修了後、松山大学経営学部専任講師。以来、准教授、教授、豪州国立大学客員研究員等を経て、15年4月より現職。専門は、経営情報論。博士（国際公共政策）。

参考文献

Duhigg, Charles, (2012), "How Companies Learn Your Secrets," The New York Times Magazine, FEB. 16, 2012.（ http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&hp=&pagewanted=all,　2016/3/10 アクセス）

ブリニョルフソン, エリック他 (2015)『ザ・セカンド・マシン・エイジ』村井章子訳、日経 BP社

International Bank for Reconstruction and Development / The World Bank, (2016), World Development Report 2016 –Digital Dividends

祝迫得夫 (1999)「「金融工学」とは何か？── ファイナンスと金融工学の間」http://www.ier.hit-u.ac.jp/~iwaisako/essays/WhatFE.htm (2016/3/10 アクセス)

泉留維「国内における地域通貨の動向」(2002年8月現在) http://izumi-seminar.net/sites/default/files/imported/pdf/CCs_MAP200208.pdf (2016/3/10 アクセス)

日経 BPムック (2015)『FinTech革命 ── テクノロジーが溶かす金融の常識』日経 BP社

岡田仁志・高橋郁夫・山﨑重一郎 (2015)『仮想通貨 ── 技術・法律・制度』東洋経済新報社

宿輪純一 (2015)『決済インフラ入門』東洋経済新報社

鶴田規久監修・日本 IBM 金融インダストリー・ソリューション (2013)『2020年金融サービス──ITと融合するリテール金融の未来像』東洋経済新報社

ウィーナー , ノーバート (1979)『人間機械論 ── 第2版』鎮目恭夫・池原止戈夫訳、みすず書房

ウィーナー , ノーバート (1962)『サイバネティックス── 動物と機械における制御と通信 ── 第2版』池原止戈夫・彌永昌吉・室賀三郎・戸田巌訳、岩波書店

山﨑重一郎 (2015)「FinTechの中核技術『ブロックチェーン』完全解説」日経 BPムック『FinTech革命』p142-153、日経 BP社

特集論文

仮想通貨3

仮想通貨Bitcoinを支える技術

神奈川大学 工学部 電気電子情報工学科 教授

木下 宏揚 Hirotsugu Kinoshita

仮想通貨として普及しつつあるビットコインは、
物理的な通貨との置き換えが可能な初めての実用的な電子現金である。ビットコインは既に多くの
セキュリティシステムなどで用いられている要素技術やP2Pネットワークを効果的に組み合わせることにより、
取引で不正が行われていないことを参加者全員で見届けることを可能にし、
「採掘」による報酬というインセンティブを導入することで
システムを持続的にうまく機能させるという興味深い仕組みで仮想通貨を成立させている。
本稿では、ビットコインで用いられている要素技術について紹介した上で基本的な原理について解説し、
なぜ仮想通貨として成立するかという観点から考察を行う。

キーワード
仮想通貨　電子現金　ビットコイン　カラードコイン

1. はじめに

金融（Finance）とIT技術（Technology）が融合したFintechが注目を集めている。特にネットワークやモバイル端末を利用した決済と、これに付随して得られた情報のビッグデータとしての解析や、ユーザが個人情報を提供する代わりにユーザの嗜好を考慮した情報やサービスの提供など、さまざまな応用が期待されている。既に、SuicaやEdyなど日本ではカード型の電子マネーが普及しているが、これらは紙の現金と取って代わるものではない。ビットコインは紙の紙幣に取って代わる可能性を持った初めての実用的な電子現金であり、今後の発展の動向が注目されている。本稿では、ビットコインで用いられている要素技術について紹介し、決済の技術的な枠組みについて解説する。

2. 電子現金としてのビットコイン

決済を、金銭的価値の移転のタイミングという観点で分類すると、多くのカード型電子マネーで用いられている「前払い」、クレジットカードの「後払い」、そして現金やデビットカードの「即時払い」がある。従って、現金の置き換えとなり得る電子現金は「即時払い」

である必要がある。現金機能としては、「価値保蔵手段」、「価値の基準」、「価値交換手段」がある。また、これらの機能を実現するためのよりプリミティブな機能としては、金額などを表現する「情報」、出所などを保証する「証拠」、所持している者に価値の行使の権利を与える「象徴」がある。一方、プリペイド型の電子マネーのように、支払いのたびに発行者機関へ還流する「クローズドループ型」と、現金のように転々流通性のある「オープンループ型」がある。以上のような特性や、ネットワークや電子化されたデータの特性などを考慮して、電子現金が備えている条件として以下の6項目が岡本、太田（1991年）により提案されている。

1. **独立性**　物理的な耐改ざん性や信頼できる第三者機関に依存していない。
2. **安全性**　コピーして二重払いに使用できない。
3. **プライバシー保護**　流通する使用者の追跡や取引内容など、プライバシーが保護される。
4. **オフライン性**　支払い時に使用者間のプロトコルがオフラインで実行できる。
5. **転々流通性**　使用者間を転々と流通可能である。
6. **分割可能性**　少額に分割して支払いに充てることが可能である。

ビットコインでは、1、2、5、6については条件を満たしている。プライバシーについては所有者を識別するためのビットコインアドレス同士の取引の関連性を捕捉可能なため完全とはいえないが、アドレスと所有者の実名の紐付けは一般にはできないため、一般的な意味でのプライバシーは確保されているといえる。オフライン性については満たしていないが、現在のネットワーク環境を鑑みれば大きな問題にはならないと考えられる。また、これらの条件以外に、現金では支払いの処理を行ったことで決済が完了する「完了性」が重要視されるが、ビットコインでは取引が完了したことを確率的に納得するためには数十分を要するが、これも実用的には容認できる程度と思われる。

3. 要素技術

3.1 ナカモトサトシは現代のマルコーニ？

ビットコインでは、いくつかの暗号関連技術を使用しているが、これらは、特に最先端の技術というわけではなく既にさまざまなセキュリティシステムで用いられている。しかし、提案者のナカモトサトシが既存の技術を組み合わせて改良することで、初めて実用的な電子現金の構築に成功したという点では、無線通信においてマルコーニがヘルツの送信機、コヒーラ（検波器）、アンテナの技術を改良して組み合わせて実用化させたことと似ているといえる。以下にビットコインで用いられている要素技術について説明する。

3.2 一方向性ハッシュ関数

一方向性ハッシュ関数は、メッセージダイジェストとも呼ばれ、データの指紋のようなものであり、少ない情報で元のデータが改ざんされていないかどうかの検査を行うことができる。一方向性ハッシュ関数hは、$y=h(x)$においてxからyを求めるのは、計算量的に易しい問題であるが、逆に、yからxを求めることが計算量的に困難になっており、基本的には総当たりで求めるしかない。入力サイズにかかわらず出力サイズは一定なので、異なる入力x_0, x_1に対して等しい出力が得られる場合があるが、$y_0=h(x_0)$におけるx_0とy_0から$y_0=h(x_1)$となるx_1を発見することが計算量的に困難でなければいけない。これによりデータの変造が防止できる。さらに、$h(x_0)=h(x_1)$のように、同じ出力を得る異なる入力の組を求めることも困難でなければならない。また、入力が1bit変更されたとき、出力のできるだけ多くのビットが変化することが望ましい。

ビットコインでは出力が256ビットのSHA256と160ビットのRIPEMD160の2種類の一方向性ハッシュ関数が用いられている。ビットコインではハッシュ関数を$y=RIPEMD160(SHA256(x))$、あるいは$y=SHA256$

(*SHA256*(*x*))のように二重に使用し、要求される出力のサイズによって使い分けている。

3.3 公開鍵暗号とデジタル署名

公開鍵暗号は、暗号化と復号化で異なる鍵を用いて、一方の鍵を公開鍵として公開し、もう一方を秘密鍵(プライベート鍵)として使用者の秘密にしておくことで秘匿性を保つ方式である。公開鍵暗号の暗号化は、ある種の一方向性関数(ハッシュ関数ではないが、逆関数を求めることは計算量的に困難な関数)を用いる。秘密鍵を知っていると逆関数を求めることが容易になるように、特別に仕掛けをした「落とし戸付き一方向性関数」が用いられる。一方向性関数なので原理的には暗号化していない平文と暗号文の対応表を作成することで解読が可能であるが、暗号化は一定のサイズのブロックごとに行うため、対応表による解読は計算量的に不可能となる。公開鍵暗号を逆向きに適用し、秘密鍵でデータを処理したものを署名文とすれば、秘密鍵を知る人しかその情報を作成し得ない情報のため、署名の機能を果たすことになる。署名の確認は署名文に公開鍵を用いて処理すればよい。実際には一方向性ハッシュと組み合わせて用いることが多い。ビットコインではデジタル署名用の楕円曲線暗号(ECDSA Secp256k1)が用いられる。Secp256k1はビットコイン以外ではあまり用いられていないが、一般的に用いられている楕円曲線暗号と比較して処理速度が30%程度高速である。また、楕円曲線の作成者が意図的にバックドアなどを仕掛ける可能性も低い。公開鍵は、楕円曲線のX座標とY座標それぞれ32byteにヘッダを加えた65byteからなっている。

3.4 P2Pネットワーク

現在の主なインターネット上での通信やサービスはクライアントサーバモデルが用いられており、情報やサービスの提供はもっぱらサーバの役割であり、原則としてクライアント同士が直接通信することはない。それに対してP2P(Peer to Peer)は参加するノードが対等に通信を行う。情報はバケツリレー式に伝達され、ノード全体で情報が共有される。ビットコインでは、すべての参加者の取引の記録がネットワークに送信され、参加者全体で共有される。また、取引の正当性を保証するブロックやブロックを連鎖させたブロックチェーンがネットワーク全体で共有される。

3.5 Base58 符号化

電子メールなど表示可能な文字(ASCIIコードなど)しか扱えないメディアで2進数で表されたデータを送る場合に何らかの方法でデータを文字コードに変換する必要がある。一般には64種類の文字に変換するBase64がよく用いられているが、ビットコインでは人間がアドレスを手で入力したり、コピーアンドペーストが容易になるように、英数字以外の文字や紛らわしい“0(ゼロ)”、“O(オー)”、”I(アイ)”、“l(エル)”などを除いた58種類の文字に変換するBase58符号化が用いられる。

4. Bitcoinの仕組み

4.1 取引の基本

ビットコインは、コインという名前がついていても、実際のコインのように固定された額面があるわけでなく、任意の価格に分割して使用可能になっている。ビットコインの取引は、複数のコインを合わせて入金として使用することができる。また、取引の出金は、1個または2個のコインとして使用できる。

取引は時制式三式簿記に基づいて行われる。図表1のように、三式簿記では資産=負債=予算として扱われ、出金の部分はUTXO(Unspent Transaction Output)と呼ばれている。すなわち、取引の入力のビットコインの合計金額と出力のビットコインの合計金額が等しくなる。

4.2 ビットコインウォレット

ビットコインウォレットは、ビットコイン自体を入れておくわけではないが、取引を行うための処理を行うクライアントソフトウェアであり、所有しているビットコインの秘密鍵のコレクションを含むファイルを保持している。ビットコインでは、秘密鍵が通貨の象徴的機能の一部を果たしていると考えられる。すなわち、図表2のように対応している秘密鍵を保持していることが、コインを行使する権利を保持していることになる。象徴的機能の残りの部分は、後述のブロックチェーンに未使用状態のコインが存在していることである。ビットコインウォレットには、ビットコインアドレスに対応する公開鍵と秘密鍵のペア、取引記録、取引の正当性を示すブロックチェーンの一部などが含まれている。

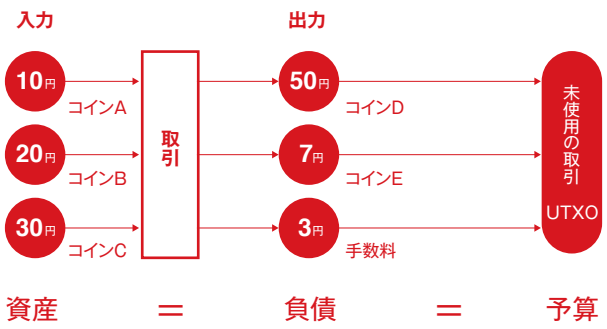
ウォレットクライアントは、以下のように分類できる。

- 完全クライアント
  数十GBにもなるビットコイン開闢（かいびゃく）以来のブロックチェーンをすべてダウンロードするので、インストール後に使用できるようになるまで時間が掛かる。
- SPV（Simple Payment Verification）クライアント
  数十MB程度の各ブロックのヘッダーのみをダウンロードするため負担が軽い。ある取引が正当なブロックに含まれているかどうかを少ない情報で検出できる。
- サーバクライアント型
  P2Pとして動作する完全クライアントのサーバにクライアントとして接続する方式である。取引の正当性はSPVと同様に検証する。秘密鍵はクライアント側にある。
- ブラウザベース
  ウェブ上のサービスとして、ウォレットのクライアントを提供する。ビットコインに対応する秘密鍵はサーバ上にあるので、ローカルなウォレットを安全に保たなくてもよいが、サーバは信頼できないといけない。また、取引のプライバシーを向上させやすい。
- ペーパーウォレット
  秘密鍵を、QRコードなどを用いて物理的な紙に印刷して保存する。ネットワークを通した不正侵入などに対して安全なので、高額のビットコインの保存に適している。

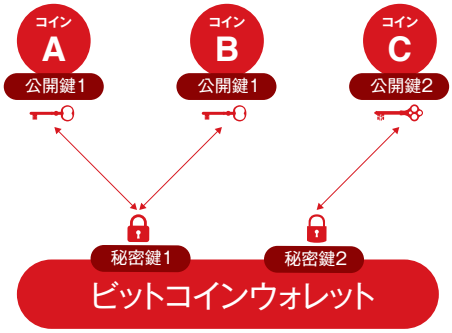
4.3 ビットコインアドレス

まず、ビットコインと紐付けられるデジタル署名用の楕円曲線暗号（ECDSA Secp256k1）の秘密鍵と公開鍵を生成する。この秘密鍵を持っているユーザのみがその権利を行使できる。ビットコインアドレスは図表3に示すように、公開鍵を基にして生成する。ここで、

図表1　ビットコイン取引の基本



図表2　ビットコインウォレット



RIPEMD160、SHA256は一方向性ハッシュ関数を表している。バイナリデータは、BASE58により表示可能な文字のみで構成されている。

一般に、ビットコインアドレスから直接使用者を特定することはできないが、特定のビットコインアドレスに関する取引やアドレス間の取引の追跡は可能である。従って、ビットコインアドレスと使用者の紐付けが、何らかの手段で判明してしまうと、プライバシーが損なわれる恐れがある。ビットコインアドレスを使い捨てにして新しくしていくことで、取引の追跡をある程度防ぐことはできる。また、民間で運営されているビットコイン交換所を経由させることで、さらに追跡を困難にさせることができる。

4.4 取引記録

ビットコインの取引は、まず受領者のビットコインアドレスを支払者に送信し、支払者は受領者のビットコインアドレス宛てに金額と共に送金を行う。取引の入力は支払い金額に応じて複数のビットコインを選択することもできる。入力のビットコインの合計金額を、1個のビットコインとして出力するか、2個の出力に分割する。お釣りが必要な場合は、二つの出力のうち一方をお釣りとして自分宛てに支払い処理を行う。取引では、入力金額の合計＝出力金額の合計＋取引手数料となる。取引手数料は、後述の採掘者への報酬として支払われる。今のところ、手数料はチップのようなもので義務ではない。受け取ったビットコインを次の支払いに充てるには、取引内容が正当なものと認められるまで数十分程度かかる。

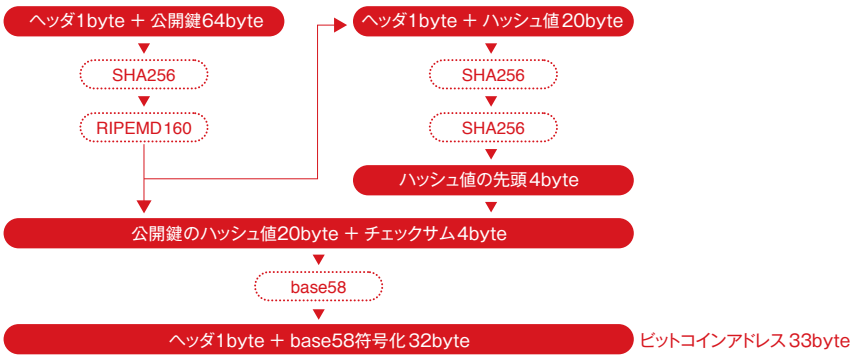
次に、取引記録のデータ構造を示す。主な内容は、取引の入力となる所有しているビットコインの個数と各コインに関する情報のリストと、取引の出力となるビットコインの個数と各コインに関する情報のリストとなる。

フィールド名	内容
Version no	現在は 1
In-counter	入力となる取引の個数
list of inputs	入力となる取引のリスト
Out-counter	出力となる取引の個数
list of outputs	出力となる取引のリスト
lock time	ブロック高または取引完了のタイムスタンプ

ロックタイムは値に応じて二つの意味合いがあり、一つは取引は完了し取引記録が取引の正当性を保証するためのブロックチェーンに登録された時刻を示している。もう一つは、取引が未完了でブロックチェーンの長さを示すブロック高を表している場合がある。

取引記録の入力のリスト（list of inputs）は、以下のような入力のビットコイン情報が含まれている。

図表3　ビットコインアドレス



フィールド名	内容
Previous Transaction hash	前の取引記録に SHA256 を 2 重に適用したハッシュ値
Previous Txout-index	前の取引記録の出力インデックス
Txin-script length	署名スクリプトのサイズ
Txin-script / scriptSig	署名スクリプト
sequense no	通常すべてのビットが 1 で未使用

前の取引記録とは、入力となるビットコインを受け取った取引で用いられたときの情報で、前の所有者がコインを現在の所有者に譲渡したという署名と現在の所有者の公開鍵のハッシュ値を格納している。この情報全体に、SHA256を2回適用したハッシュ値がPrevious Transaction hash であり、これが前の取引の正当性を示す証拠の一つになる。出力インデックスは前の取引の出力の何番目かを示している（出力が一つなら0番目）。署名スクリプトは、該当するコインを受領者への支払いに充てたことを示すための署名を格納する。

取引記録の出力のリスト（list of outputs）は、以下のような入力のビットコイン情報が含まれている。

フィールド名	内容
value	取引記録からの出金額、単位は 10^{-8}*BTC*
Txout-script length	取引出力スクリプトのサイズ
Txout-script/scriptPubkey	公開鍵スクリプト

公開鍵スクリプトは、受領者の公開鍵のハッシュ値が格納され、コインが受領者の所有に移転することを表している。署名スクリプトと公開鍵スクリプトは「ビットコインスクリプト」と呼ばれ、逆ポーランド記法を用いFORTHのようなスタックベースで記述されるスクリプト言語で記述される。署名スクリプトは取引の入力で用いられ、支払者の秘密鍵による取引記録全体の署名を生成し、これを格納する命令と支払者の公開鍵を格納する命令で構成される。公開鍵スクリプトは取引の出力で用いられ、受領者の公開鍵のSHA256とRIPEMD160を二重に用いてハッシュ値を求め、これを格納する命令で構成されている。

具体的な取引の手順は、以下のようになる。

1. 所有しているビットコインの中から支払いに充てるアドレスを選択する。
2. 署名スクリプト以外の入力や出力などの取引記録を用意する。
3. 署名を行うための仮のデータとして、署名スクリプトの代わりに支払者の公開鍵をSHA256とRIPEMD160を用いたハッシュ値の公開鍵スクリプトを仮に記入しておく。入力が複数の場合は、署名する入力以外の署名スクリプトはゼロにしておく。
4. 取引記録全体のSHA256ハッシュを2回適用したものに、Secp256k1のECDSAでデジタル署名したものと支払者の公開鍵を、署名スクリプトとして仮のスクリプトと置き換える。

取引の検証は、支払者の公開鍵を署名スクリプトから取り出し、SHA256とRIPEMD160でハッシュ値を求め、これを署名スクリプトに置き換え、支払者の署名の対象となる情報を再現する。この取引記録全体に、SHA256のハッシュ関数で2回処理したハッシュ値を求め、支払者の公開鍵で署名を確認する（図表4）。

4.5 ブロックチェーン

取引記録の署名は、支払者から受領者にコインの権利が移転したことを示しているが、二重の支払いが行われていないかどうかは署名を検査しただけでは分からない。そこで、取引記録をブロックと呼ばれる形に取りまとめ、さらにブロックをブロックチェーンと呼ばれる連鎖にして、これをP2Pネットワークで共有することにより、ある取引が二重払いに使用されておらず、正当なものであることをビットコインの使用者全体で保証する。採掘者と呼ばれる人は、平均して10分ごとに、その間に行われたビットコイン全体の取引をブロックにまとめて、ブロックチェーンの最後に付け加える（図表5）。

4.6 マークルツリー

ある取引記録がブロックに含まれているかどうかを少ない情報量で確認できるようにするために、ブロックに取り込む取引記録は、SHA256を2回適用したハッシュ値を、マークルツリーと呼ばれる二分木にハッシュ値として記録する。採掘者は以下の手順でマークルツリーを作成する。

1. P2P ネットワーク経由で取引記録を収集する。
2. 各取引記録に SHA256を2回適用したハッシュ値を求める。
3. ハッシュ値を2個ずつペアにして連結し、SHA256を2回適用したハッシュ値を求める。
4. これを繰り返し、ツリーの根に当たる部分であるマークルルートハッシュを求める。

図表6のように、取引記録とハッシュ値よりマークルルートハッシュを求めることができる。ブロックチェーンには、取引記録の完全な情報が記録されているが、SPVなどの軽量のクライアントでは、ブロックチェーンのうちブロックヘッダのチェーンのみ保持し、注目する取引からルートに至るノードのハッシュ値に必要なものだけあればよい。全体の情報が必要な場合は、P2Pネットワークから入手可能である。例えば図表6では、取引記録0がルートハッシュに含まれているかどうかを検査するためにMerkle Root Hash, Hash0, Hash00 のみあればよい。

4.7 ブロックの構造

約10分ごとの取引記録を取りまとめたブロックは、以下のように構成される。

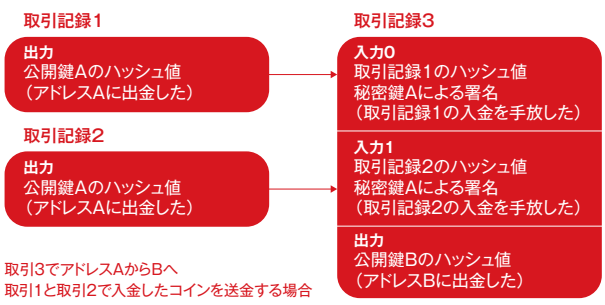
フィールド名	内容
Magic no	常に 0xD9B4BEF9
Blocksize	ブロックサイズ
Blockheader	6項目のヘッダ
Transaction counter	含まれる取引記録の数
Transactions	取引記録のリスト

このうち、ブロックヘッダは以下の内容で構成される。

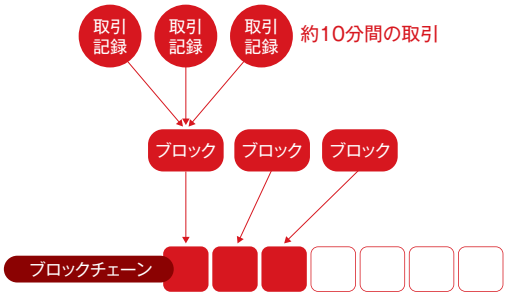
フィールド名	内容	更新
Version	バージョン番号	
hash Prev Block	前のブロックヘッダの SHA256 を 2 回適用した ハッシュ値	新しいブロックが到着した時
hashMerkle Root	ブロックに含まれるすべての取引に基づく SHA256 を 2 回適用したハッシュ値	取引が受け入れられるごと
Time	現在のタイムスタンプ（UNIX 時間）	数秒ごと
Bits	浮動小数点で記述したプルーフオブワークの ターゲット	プルーフオブワークの困難さが変更された時
Nonce	0 で始まる 32bit の数	ハッシュで 1 つずつ増やして施行

hash Prev Block はブロックチェーンの最後のブロッ

図表4　取引の例



図表5　ブロックチェーン



クの後に新しいブロックを接続するために直前のブロックのハッシュ値を記録する。これにより新しいブロック以前のブロックチェーンが改ざんされていないことが保証できる。Merkle Root Hashにより、ブロックに含まれている取引記録が確定され、改ざんできないことが保証される。Bitsは、図表7のように、採掘者がブロックに取り込まれた取引記録が正当なものであることを保証するプルーフオブワークで発見すべき目標値の最大値を表していて、3byteの仮数部分Sと1byteの指数部分E（単位はbyte）で表現されている。目標値は$S\times8^{E-3}$となる。すなわち、SHA256のハッシュ値の32byteのうち、先頭から$(32-E)$byteは0が連続し、Sが3byteが続き、残りの$(E-3)$byteは0となる。Nonceは、プルーフオブワークで目標値以下のハッシュ値を発見した時のNonceの数値を表している。目標値は2016ブロックが処理されるたびに平均10分で発見できるように調整される。

4.8 プルーフオブワーク

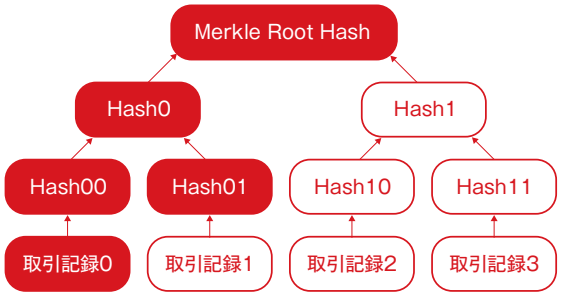
プルーフオブワークでは、ブロックヘッダをSHA256を2回適用で求めたハッシュ値がBitsで指定された目標値以下になるように、ブロックヘッダに基づくハッシュ関数の入力値を求める計算となる。入力値のうち、ブロックヘッダのNonce以外の部分は固定値なので、後半のNonceを0から1ずつ増加させて総当たりで求める計算となる。試行1回で正解が求まる確率はSHA256の出力256bitが目標値以下となる確率なので$S\times8^{E-3}\times2^{-256}$となる。

採掘者は条件を満たすNonceを最初に発見し、これが参加者に承認された場合、報酬として新規のビットコイン（現在は25BTC）とブロックに含まれる取引の手数料を得ることができる。この新規のコインはブロックの最初の取引記録であるコインベース取引として表現される。この場合、入力に相当する取引は存在しないため、取引記録の入力は意味を持たないが、通常、Transaction hashは0、Previous Txout-indexは-1（すべて1のビット）で表現する。また、取引記録の出力の出金額は採掘された25BTCとブロック中の取引手数料の合計となる。新規ブロックが生成された場合、その情報はP2Pネットワーク全体に送信される。プルーフオブワークは、採掘者が取引記録を取りまとめ、改ざんできないようにブロックを生成するために費やした労力の証拠となる。

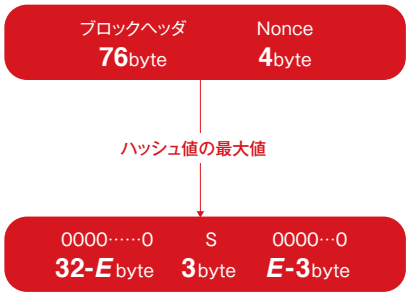
4.9 ブロックチェーンの分岐

ビットコインの開闢以来、ブロックチェーンは正当なブロックは一つの連鎖を構成している。チェーンの中で最初のブロックから何番目のブロックであるかは「ブロック高」と呼ばれる。しかし、図表8のように、新規のブロックの生成がほぼ同時に発生したり、

図表6　マークルツリー



図表7　プルーフオブワーク



あるいは故意に改ざんした不正なブロックが生成されたりした場合、P2Pネットワークの情報伝達の遅延や一時的にオフラインであったノードの再接続に起因して、ブロックチェーンに異なる複数のブロックが接続され、チェーンが分岐してしまうことがある。その後、それぞれの分岐に、さらにブロックが接続され伸びていく可能性があるが、ビットコインでは最も長い分岐が正当なブロックチェーンであるというルールがある。従って、一つのチェーン以外はやがて成長を止めてしまう。

ある取引が成立した時点で取引記録が正当と確定するわけではなく、正当なものと認められるためには、約10分程度経過して取引記録がブロックに取り込まれ、さらに、そのブロックのあとに数個のブロックが接続され、チェーンが成長していくことを見届けることが必要となる。

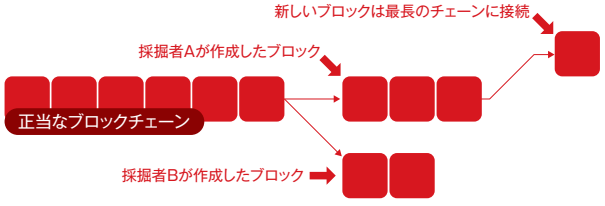
4.10 カラードコイン

カラードコインは、ビットコインの転々流通性や二重利用ができないといった機能を利用して、債券などの資産（Asset）の発行と流通を可能にしたシステムである。実装方法としては、ビットコインの取引記録中のスクリプトを利用して機能を拡張したOpen Assets Protocolがあり、図表9のように、ビットコインの上位レイアとして位置付けられる。ビットコイン層では極少額（$600\times10^{-8}BTC$）の価値を移転することになるが、これと紐付けしたアセットを流通させることで、取引前後のアセットの総量の保持や転々流通性が実現できる。応用分野としては、個人情報とカラードコインを積極的に連携させて、商品や店舗の推薦システムに利用したり、企業による債券や手形の発行、家や車の鍵などトークンとしての利用などが考えられる。

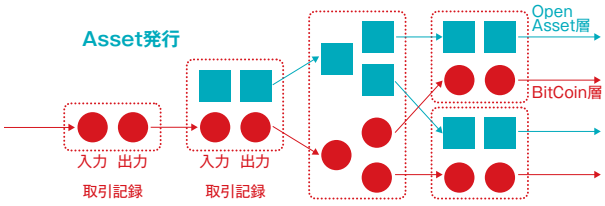
5. ビットコインはなぜ成立するか

一般に、現在の法定通貨は中央銀行が発行し、流通に際しては国債などの債券と引き換えに供給する債務と考えられるため、シニョリッジ（通貨発行益）は、債券の金利程度と考えられる。また、法定通貨の価値は、国家の経済規模と信用から形成されている。しかし、ビットコインは発行に際し、このような債権・債務関係が存在しないと考えられている。シニョリッジは、採掘者が新規のコインの発行分から発掘のためのハードウェアの減価償却費と電気代を引いたものとなるので、法定通貨と比較して極端に大きいわけではない。採掘によりビットコイン経済全体での流通量は、その分増加しているため、そのコストを参加者全体で広く薄く負担していることになる。価値に関しては、電子現金として情報セキュリティ的に長期にわたり安全であり、投機目的と決済に必要な実需との需給バランスで他の法定通貨との交換が成立し、また貨幣として通用力を持ち、ビットコイン経済の参加者が価値がある

図表8　ブロックチェーンの分岐



図表9　Open Assets Protocol



と信じていることで保証されているといえる。

セキュリティ上の安全性では、各取引において、支払者のデジタル署名により、価値が受領者に移転したことの証拠を残し、プルーフオブワークの結果として、各取引がブロックに取り込まれ、そのブロックが最長のブロックチェーンに含まれているブロックの正当性が保証されることで担保されている。また、これらが正しく作成されているかどうか参加者すべてが確認可能である。ただし、最長のブロックかどうかは参加者により多数決的に選択されるため、過半数の参加者が結託すればこの仮定は成り立たなくなるが、現実的にはこれは無視できるリスクであると考えられている。プルーフオブワークのインセンティブは、採掘したビットコインと手数料収入であるが、採掘に対する報酬は約４年ごとに半減していくので、将来的には手数料が主なインセンティブになる可能性がある。また、現在のプルーフオブワークは既に採掘者の寡占化が進んでおり、将来にわたってインセンティブが維持できるかどうかは不明確である。

6. まとめ

ビットコインは初めての実用的な電子現金システムであるが、決済システムとして定着するためには、解決しなければならない問題点もある。プルーフオブワークは、無意味な計算をすることに意味があるが、採掘者は寡占化されており、安定的にインセンティブを維持する方法の検討が必要である。また、電力消費をムダにしないために、セキュリティや公平性を担保した上で、有益な計算を行う手法の構築なども期待される。Open Assets Protocolを用いれば、例えば、日本銀行がビットコイン上の日本銀行券を発行することも可能となるので、債券の発行と流通も今後期待される分野である。

Hirotsugu Kinoshita

木下 宏揚

神奈川大学 工学部 電気電子情報工学科 教授

1962年生まれ。1986年電気通信大学電気通信学部電波通信学科卒、1987年東京工業大学大学院理工学研究科博士前期課程修了、1990年東京工業大学大学院理工学研究科博士後期課程修了。工学博士。1990年東京工業大学助手、1994年玉川大学専任講師、1995年神奈川大学助教授、2002年より現職。

情報セキュリティ、個人情報保護、デジタル著作権管理、デジタルアーカイブなどの研究に従事。

参考文献

Satoshi Nakamoto,“Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2009.

岡田仁志, 高橋郁夫, 山﨑重一郎「仮想通貨と電子マネーの分類」『仮想通貨――技術・法律・制度』, 東洋経済新報社, 2015.

“bitcoin wiki”,The Bitcoin Community, https://en.bitcoin.it/wiki/Main Page,2016.

T.Okamoto and K.Ohta, “Universal Electoronic Cash”, Advances in Cryptology CRYPTO '91 Proceedings, Springer-Verlag,1992, pp324-337.

「セット割引」と独占禁止法

法政大学 法学部 教授

岸井 大太郎 Daitaro Kishii

規制改革の進展に伴い、電力・ガス、情報通信などの公益事業分野における「セット割引」が拡大している。
セット割引は、一般的には、効率性を向上させ競争を活発にするものであるが、
市場支配的な事業者等が行う場合には、競争者を市場から排除し競争を制限する行為として
独禁法上問題になる場合がある。特に、それは、不当廉売に当たらなくても、
競争排除型の抱き合わせ販売に類似する行為として違法となる可能性がある。
このような観点から、欧米で採用されている「割引寄与（discount attribution）」基準の意義と
問題点を検討した上で、日本における独禁法違反の有無の判断基準を検討する。

キーワード
独占禁止法　セット販売　不当廉売　抱き合わせ販売

1. はじめに

1-1「セット割引」の定義と検討の対象

本稿は、近年注目を集めている、電力・ガス、情報通信などの公益事業分野におけるセット割引を中心に、独占禁止法上の評価を検討しようとするものである[1)]。「セット割引」とは、ⓐ複数の商品・役務をセットで購入する場合に、ⓑ別々に単品で購入するより値引きされるもので、ⓒ単品ごとの購入の選択肢は残されているものを指す[2)]。値引きの形態としては、直接の料金の減額のほか、キャッシュバック、ポイント加算、あるいは一定の商品・サービスの無料提供などを広く含む。また、基本料金部分か従量料金部分か、工事費・管理費などの付加サービス部分かなども問わず、さらに、個別の割引金額が示されている必要もない。単品よりもセットが、対価の面で経済的に有利であると評価されるものであればよい。また、セット販売の主体が単一の事業者であれば、その取引ないし供給の形態には、自己が製造・販売する場合のほか、卸・代理等の形で他の事業者の商品・役務を販売する場合や、他の購入先を指定する場合なども含まれる[3)]。

なお、セット割引には、流通分野においてメーカーが流通業者に提供する各種のリベートなども含み得るが、本稿では、主に公益事業分野を念頭において、これらのサービスを購入・利用する最終消費者ないしは

事業者ユーザー向けのセット割引を中心に、独禁法上の問題点を検討することにする。

1-2 セット割引の効率性と競争促進効果

セット割引は、さまざまな分野・領域で広く行われており、一般的には、以下のような効率性を有している[4]。第1は、範囲の経済によるコスト低下、企業の取引コストの削減、消費者による探索コストの削減などのコスト節約効果である。第2は、複数の商品・役務がセットにされることでトータルの効用の上昇や品質の維持が可能になる、セット化により新たな製品・サービス（統合商品）を生み出すなどの、効用・品質の維持・向上や、新製品のイノベーション促進効果である。第3は、価格差別の手段としてセット割引がなされることによる、効率性の向上である[5]。例えば、ブロードバンドと固定通話がセット割引で提供されると、以前に単品のみで販売していたときには一方のみを購入して利用していた顧客が、双方のサービスを利用するようになり、市場の拡大と産出量の増大が生じる。あるいは、有料テレビ番組のパッケージでの割引販売は、個々の消費者には不要な番組が含まれていても、消費者はそれがなければ得られないサービスの提供を受けることができ、また、パッケージ全体としての支払い意思を反映した価格設定であれば、それは異なったサービスに対する異なった評価を反映するものであり、経済厚生の低下をもたらさない。

そして、以上のような効率性は、価格の低下、品質・サービスの向上、多様で新しい商品・役務の創出、新規参入の促進などの競争促進効果を生じさせることになる。

しかし、このように言うことは、セット割引が独禁法上問題ないことを意味しない。以下、セット割引が、独禁法上どのような違反行為類型に該当する可能性があるか、またその場合の違法性の判断基準について検討してみることにしたい[6]。

2. セット割引と独禁法の違反行為類型

2-1 セット割引と「不当廉売」

第1に、セット割引は、それが値引きの一種である点に着目すると、不当廉売規制の適用が問題になる。すなわち、個々の商品・役務の割引後の価格のいずれか一つが、供給に要する費用（コスト）を著しく下回っている場合には、それぞれの商品・役務の不当廉売として、また、セット全体の価格が、対象となる商品・役務のコストの合計額を下回っている場合には、当該セット商品・役務の不当廉売として違法となる可能性がある[7]。この点は、異論のないところである。

他方、セット割引は、専ら不当廉売の観点からのみ問題にすれば足りるとする見解もあり得る。割引は価格の引き下げに他ならないから、不当廉売に該当する場合以外に規制を拡大することは、まさに独禁法が保護しようとしている価格競争そのものを制限し、消費者厚生を低下させるとするのである。しかし、セット割引は、不当廉売規制が想定している通常の値引きとは幾つかの点で異なっている部分があり、これを不当廉売のみに解消するのは適切ではない。

まず、不当廉売が単一の商品・役務を対象としているのに対し、セット割引は、それぞれが別個に取引される「複数」の異なる商品・役務を対象とする行為である。次に、値引きは、その複数の商品・役務を合わせて購入する場合にのみ供与されるのであり、それは単なる値引きではなく、セットで購入するという「条件」が付された値引きである。このような「複数性」と「条件性」を伴う値引きであることから[8]、以下に見るように、そのような特性に固有の独禁法上の問題を惹起する可能性が生じる。

2-2 セット割引と「抱き合わせ販売」

①抱き合わせ販売との類似性

上記のような「複数性」と「条件性」に着目すると、セット販売は抱き合わせ販売と類似性ないし共通性が

ある。すなわち、セット販売は、メインとなる商品・役務（ここでは「連結（linking）商品・役務」と呼ぶ）と、これにセットされる他の商品役務（ここでは「被連結（linked）商品・役務」と呼ぶ）で構成されており、この点は、抱き合わせ商品・役務と被抱き合わせ商品・役務で構成される抱き合わせ販売とパラレルに考えることができる。そして、セットで購入すると値引きされるという「条件性」は、利益ないし不利益によって被連結商品・役務を購入するように仕向けるという点で、需要者に購入“させる”行為に類似するものと評価することができる[9]。このように見ると、連結商品・役務の市場において市場支配力ないし経済力（ブランド力等）を有する事業者が行うセット割引は、連結商品・役務の水平的レバレッジ[10]により、被連結商品・役務の市場における競争排除効果を生じさせる、抱き合わせ販売類似の行為と捉えることが可能である[11]。

②セット割引と購入の「強制（させる）」

ただし、セット割引は、単品で購入する選択肢が残されており、直接的な「強制（させる）」は存在しないから、この点をどのように考えるかが問題となる。「強制」は、日本法においては「客観的に見て少なからぬ顧客が他の商品の購入を余儀なくされる」場合を言うとされているが[12]、セット割引について、その存否はどのように判断されるのだろうか。

第1に、「強制」を広く捉えると、セットで割引がされるということは、単品で購入すると割引が受けられないという経済的不利益ないしペナルティが課せられることだから、セット割引自体が強制に当たるとする考え方もあり得る[13]。しかし、そこで需要者は、割引によって誘導されているという側面はあるが、これを一律に“余儀なくされる”という意味での「強制」に当たると解するのは、取引の実態や需要者の意識から乖離した擬制的な議論であると言わざるを得ない[14]。あるいは、そこで割引に引き付けられる需要者の数ないし広がりを問題にすることも考えられるが、需要者の意識や行動はさまざまであるから、結果として購入しているという点だけから強制を導き出すのには無理がある。また、強制の存在は、“手段それ自体が違法”[15]であるとか、“当然違法”[16]であるとの解釈と結び付くことになるが、このような一律の評価は、前述したセット割引の競争促進効果に照らして適切ではない[17]。

第2に、他方で、「強制」を狭く捉え、セット割引の場合には、セットで購入することが“唯一の実現可能な選択肢”である場合に限定するというアプローチもあり得る[18]。例えば、単品での購入価格が高く設定され、セットでの購入以外の選択肢が現実的でないような場合である。これが、抱き合わせに匹敵する「強制」があるとすることに異論はない。しかし、このような“拒否的高価格”に該当しない場合であっても、需要者は、連結商品・役務の市場支配力をテコにしたセットでの割引購入に誘導されているという側面があるから、そこでの被連結商品・役務の購入決定が、連結商品・役務とのセットによる金銭的なインセンティブに影響されてなされているという点で、需要者の選択の人為的な歪曲が生じている[19]。そして、これにより需要者がライバルの商品・役務を選択・評価（テスト）する機会が低下したり時間的に遅らされたりされ、被連結商品・役務の市場におけるライバルの競争機会が侵害されるおそれが生じることになる[20]。取引の実態や需要者の意識の多様性に鑑みて、このような行為それ自体を一律に問題とすることは適切ではないが、それが競争者を排除し、市場の競争を制限する場合を規制することは、可能かつ必要である。

以上のように考えると、セット割引は、レバレッジによる競争排除が問題になるという点では抱き合わせ販売と共通する性格を有しているが、その判断基準として需要者の「強制」の有無を問題にすることは、必ずしも適切ではない。「強制」の判断基準の不明確性は、抱き合わせ販売自体においても指摘されてきたところであるが[21]、セット割引の場合には、この批判がよりいっそう当てはまる。そこでは、強制の有無にかかわらず、当該行為によって、被連結商品・役務の市場の需要者が競争者の商品・役務に転換（スイッチン

グ）するインセンティブが人為的に低下させられ、競争者が排除されることが問題であり[22]、そのような実態に即した違法性の判断基準が求められているということができる。

2-3 セット割引と「忠誠リベート」

セット割引は、「忠誠リベート」との類似性が指摘されることがある。忠誠リベートは、自己との取引比率などの忠誠度に応じてリベートを支払うものであり、経済的利益により、排他条件付取引に類似する競争者との取引の制限効果を有することが問題とされる。セット割引も、被連結商品・役務を競争者でなく自己から購入するように仕向ける割引として捉えると、これと共通性を有することになる。これについては、次のように考えることができる。

第1に、忠誠リベートは、「単一」の商品・役務に関するリベートを問題にするのが通例であるから、この点で、「複数」の商品・役務を前提とするセット割引と区別される。ただし、両者は重なり合う部分がある。例えば、複数の商品・役務を対象にした忠誠リベート（忠誠セット割引）はセット割引としての側面も有する。また、単一の商品・役務についての忠誠リベートであっても、そこに製品の品種や規格などの点でバリエーションが存在し、競争者と競合するコンテスタブルな商品・役務と、行為者が独占的に供給する非コンテスタブルな商品・役務に分かれている場合、それらを一括した忠誠リベートが課されると、非コンテスタブルな部分の市場支配力ないし経済力の非コンテスタブルな部分に対するレバレッジが生じるという点で、セット割引と共通する部分がある[23]。

第2に、他方で、忠誠リベートは、複数の商品・役務か否かにかかわらず、自己との取引比率などの「忠誠度」をリベート供与の条件としているのに対し、セット割引は、複数の商品・役務を「セットでの購入」が割引の条件であり、忠誠度のいかんは直接の条件とされていない。両者には、何がリベートないし割引の「条件」とされるかに違いがあり、この点は、違法性の判断基準を考える場合にも異なる扱いを必要とする[24]。そこで、本稿では、レバレッジによって競争者との取引を制限するという面で共通性があることは認めつつ、割引の条件の内容が異なる点から両者を区別して扱い、忠誠度による割引を伴わない、純粋なセット割引を念頭において検討することにする。

3. セット割引の違法性判断基準

それでは、セット割引の違法性判断基準を検討してみよう。その場合の適用法条としては、排除型私的独占（独禁法2条5項、3条前段）、抱き合わせ販売（不公正な取引方法・一般指定10項）、取引妨害（同14項）などが考えられるが、抱き合わせは前記の強制要件の問題があることから、ここでは、排除型私的独占と競争減殺型の取引妨害[25]を念頭において検討することにしたい。

3-1 行為者の「市場支配力」・「他の商品・役務」

まず、排除型私的独占では、行為者が連結商品・役務の市場において市場支配力を有することが必要である。また、シェアが高くなくても強力なブランド力などを有する場合などには、取引妨害が問題となり得る。セット割引は市場支配力ないし経済力のレバレッジが問題であるから、これらは必須の条件である。次に、被連結商品・役務は、連結商品役務と異なる“他の商品・役務”であることが必要であるが、これは抱き合わせ販売の要件に準じ、独立して取引の対象とされているか否かで判断される[26]。

以上を公益事業分野に当てはめると、問題になり得る事業者としては、エネルギー分野では、全面自由化前の供給地域で100％近いシェアを占めてきた既存の電力会社および既存の都市ガス会社、電気通信では、ブロードバンド契約数シェアが約70％を占めるNTT東西および関西地域で50％のシェアを占めるケイ・オプティコム、移動体通信で第1位・43％の加入者シェアを占めるNTTドコモなどが想定される。また、

電力、都市ガス、ブロードバンド、モバイル通信、固定通話、有料TVなどは、いずれも独立して取引の対象とされているから、個々のサービスを相互に“他の商品・役務”であると考えて問題ない。

3-2 排除行為該当性と「割引寄与」基準の評価

排除行為ないし不当な妨害行為に該当するか否かの判断基準として、米・EUでは「割引寄与（discount attribution）」基準を用いるアプローチが有力である。そこで、まずこれについて検討してみよう。

①「割引寄与」基準の内容と考え方

「割引寄与」基準とは、被連結商品・役務のセット販売価格から、セット割引による割引額の総額を差し引いた金額が、被連結商品・役務のコストを下回るか否かを問題にするものであり、排除行為に該当するか否かの判断基準として、EU機能条約（TFEU）102条に関するEC Guidance（para23）およびシャーマン法2条に関するアメリカのCascade Health判決[27]で採用されているものである。その場合、コスト以下か否かの判断基準として、アメリカでは平均可変費用（AVC）が、EUでは長期平均増分費用（LRAIC）が用いられており、固定費部分や統合によるコスト節約が含まれるか否か違いがあるが、両者の基本的な考え方は共通である。

以上のような「割引寄与」基準は、以下の点に特徴がある。第1に、この基準は、セット割引を不当廉売とのアナロジーで捉え、被連結商品・役務を販売する「同等に効率的な競争者」が、コスト面で当該割引に対抗できるか否かを問題にするものである。すなわち、需要者はセット割引による節約総額と、被連結商品・役務のみをライバルから購入する場合の価格の有利さとを比較するから、この基準に該当する場合、同等に効率的なライバルであっても、行為者のコストを下回る価格を提示しなければならず、対抗不可能となると考えるのである。そこには、セット割引も値下げ競争の一種であるから、不当廉売に準じた抑制的な基準を採用すべきであり、さもないと過剰規制になるとする基本的な政策判断がある[28]。第2に、このような理解から、割引寄与基準は“セーフハーバー”としての意味を持たされ、これに抵触しなければ、原則として違法にならないとされる。すなわち、EUでは、この割引寄与基準によるコストが長期平均増分費用を下回らないかぎり、通常、委員会はそれ以上の審査を行わないとされ、またアメリカでは、訴訟においてシャーマン法2条違反を立証するためには、原告が、割引寄与基準によるコストが平均可変費用以下であることを証明しなければならないとされている。

②割引寄与基準の意義と問題点

割引寄与基準に該当する場合、同等に効率的なライバルであっても、コスト面で行為者のセット割引に対抗する余地がほぼ完全に失われるから、それは、競争者の競争機会が侵害されることを示す有力な徴表の一つだと言うことができよう。しかし、この基準に対しては、以下に見るように、その理論的な前提も含めて種々の批判があり、特に、これをセーフハーバーとして利用し、割引寄与基準に抵触しなければ原則として違法に問わない、とすることは問題があると考えられる[29]。

第1は、不当廉売とのアナロジーの有効性である。「複数性」と「条件性」を特徴とし、連結商品・役務のレバレッジを伴うセット割引は、セット全体で利益を上げることが可能だから、割引寄与基準でコスト割れであっても、短期の利潤犠牲を伴っていない。それは、不当廉売が想定する単品の価格引き下げと異なり、経済合理性に反する行為ではなく、また長期的に維持可能である。セット割引は、先に検討したように、不当廉売ではなく競争排除型の抱き合わせ販売と共通する性格を有すると考えるべきものである。

第2は、「同等効率性」基準を用いることの妥当性である。同等に効率的でない、その意味で行為者よりも効率において劣る競争者であっても、市場支配力に対する有効な競争的牽制力として働き得ることについては多くの指摘があるが[30]、同等効率基準はこの点を考

慮することができないとの批判である。すなわち、(1)セット割引をめぐる価格引き下げ競争は行為者のコストを上回る水準でなされることも多く、そこではより効率の劣る競争者であっても牽制力となり得ること、(2)スケールメリットやネットワーク効果が作用している商品・役務においては、セット割引による需要者の囲い込みによって、効率的なライバルとなり得る競争者の事業機会を閉ざしてしまう危険性があること、(3)セット割引によって複数の市場に一括して参入する必要性が高まり、被連結商品・役務市場の参入障壁が増大して新規参入が難しくなるおそれがあること、等の事情が無視され、反競争行為を正当化することになる危険が生じるのである。

第3は、ノーマルな価格引き下げ行動を抑制する「過剰規制」になるという政策判断についてである。EC GuidanceもCascade Health判決も、割引寄与基準によるコストを上回るセット割引であっても、競争者を排除する可能性が残ること自体は否定していない。それにもかかわらず、その基準を採用したのは、過剰規制の危険に対する考慮である。しかし、確かに通常の不当廉売が対象とする単品の廉売は、ノーマルな価格引き下げ行動一般と区別するのが難しいから、そこで過剰規制の危険を考慮する必要性が高いと言えるが、ここで問題にされるセット割引は、連結商品・役務の市場で市場支配力を有する事業者により、前記の「複数性」と「条件性」を伴って行われる行為であり、廉売一般はもちろん、セット割引全体の中でも、限定された行為を対象にしている。また、そこでは個々的に単品の値下げをするという選択肢が残されている。従って、ノーマルな価格引き下げ競争まで制限する過剰規制となるおそれは、不当廉売規制に比べて小さく、これを同列に論じるべきではない[31]。

なお、そこでは、予見可能性の観点から、行為者が事前に行為の違法性の有無を判断できることが強調され、この点からも、行為者のコストのみを参照して判断できる割引寄与基準が適切だとされている。しかし、これは、今述べたノーマルな価格引き下げ行動一般と区別がつかないという判断を前提にするからこのような議論になるのであり、忠誠リベートなどを見れば分かるように、独禁法は、価格に関連する行為であっても、常に行為者のコストのみを参照して事前に予測できる基準でなければならないとしているわけではない。

第4は、割引寄与基準によるコスト計算が複雑化する場合があることである[32]。まず、2つの商品・役務のセット割引であれば計算は比較的簡明だが、3つ以上になると、それぞれの値引き分をどのように割り当てるかの判断が難しくなる。また、設定価格の変動が激しい場合には、どの水準を計算の基礎とするかの判断も難しくなる。この基準をセーフハーバーとして実務上有効に運用できるのか、疑問が残るのである。

もちろん、最初に触れたセット割引の競争促進効果に鑑みて、過度の規制が価格競争を制限する可能性に配慮することは必要である。しかし、上記の問題点を踏まえて考えると、割引寄与基準をセーフハーバーとすることは、逆に、過剰規制ではなく「過少規制」に陥る危険があると言わねばならない。また、それは、抱き合わせ販売と類似の性格を有する行為であるにもかかわらず異なる規制基準が適用されるという、“規制内容の不均衡”を生じさせる点でも問題がある。

3-3 行為要件（排除行為該当性）の判断基準

それでは、セット割引の排除行為該当性ないし不当な妨害行為該当性は、どのような基準で判断したらよいだろうか。以下、その主要な考慮要素を検討してみたい[33]。

①需要者の取引先転換のインセンティブの低下

先述したように、セット割引は、割引による誘導効果により、被連結商品・役務の市場の需要者が競争者の商品・役務に転換するインセンティブが人為的に低下させられることが問題であるから[34]、まず、この点を具体的に見る必要がある。第1に、そこでは、行為者の連結商品・役務の市場支配力ないし経済力に起因して、需要者が行為者の当該商品・役務を購入する必

要性ないし選好度が高いことが条件となる。これは、代替性を欠く独占的な商品・役務である場合のほか、ブランド力などと相まって代替的な取引先を容易に見いだせない場合などがこれに該当する[35]。第2に、そこで需要者が、被連結商品・役務を購入するにあたって、連結商品・役務とのセット割引による金銭的利益が選択の理由とされていることが必要である。その場合、品質やブランド等が考慮要因の一つとされていても、セット割引による金銭的利益が取引先選択の主要な要因となっている場合には、需要者の選択の歪曲が生じていると評価される[36]。

②競争者による対抗の困難性

次に、①に該当するセット割引に対して、単品ないし行為者より少ない商品・役務のレパートリーで競争しようとする既存ないし新規の競争者が、当該セット割引に有効に対抗できるか否かが問題となる。そこでは、競争者が対抗するのにどの程度の割引を行わなければならないか、その割引が競争者にとって維持可能かが問題となる[37]。

具体的には、第1に、行為者が被連結商品・役務についてスケールメリットやネットワーク効果などの点で優位性を有しており、当該セット割引によって競争者が事業継続に必要な最低供給量が維持できなくなるなどの事情がある場合には、対抗が困難だと判断されやすい[38]。この場合、効率的なライバルとなり得る競争者の事業機会を閉ざしてしまうことが問題だから、行為者よりもコスト面で劣ることは、行為を容認する理由にはならない。

第2に、ライバルが、行為者に比肩し得るセット割引を、追加のコストや時間的ラグを要することなく容易に模倣可能か否か、具体的には、競争者による連結商品・役務の生産ないし卸購入の可能性のいかんも重要な考慮要素となる[39]。これに関しては、公益事業分野では事業法による規制が存在するのが通例であるが、それがどの程度有効に機能しているかは別問題であるから、その効果や有効性のいかんも含めて模倣の実際の難易度を評価し、対抗可能性の有無・程度を判断することになる[40]。第3に、行為の対象範囲や期間の長さも重要な考慮要素となる[41]。その場合、ここで念頭に置いている公益事業のセット割引は、広く一般の消費者を対象とし、また長期間継続する方策として実施されるのが通例であるから、この面では競争者による対抗の困難性が認められやすいと考えられる。

③「割引寄与」基準の位置付け

先述したように、割引寄与基準によるコストを上回る割引であっても、上記の総合考慮の結果、事業活動の困難性が生じると判断されれば、排除行為に該当する。他方、割引寄与基準に該当する場合には、競争者が行為者のセット割引に対抗して事業を行うことができる可能性が低いこと、当該基準によるコスト計算が比較的簡便で利用しやすいことから、割引寄与基準によるコストを下回る場合には、排除行為に該当する可能性が高くなると考えてよい。その意味で、実際の判断においては、割引寄与基準は有用な考慮要素となり得る[42]。ただし、それはセーフハーバーではないから、あくまで排除行為該当性を判断する考慮要素の一つにとどまり、これに該当しないことが排除行為該当性を否定する理由とはならない。また、割引寄与基準を考慮要素の一つとして排除行為該当性が認められ違法とされた場合であっても、それが排除措置などにおける違法状態の解消の基準となるわけではないことに注意する必要がある[43]。

3-4 反競争効果と正当化事由

最後に、排除行為ないし不当な妨害行為に該当するセット割引は、反競争効果の要件（競争の実質的制限ないし競争減殺）を充足する必要がある。また、その競争促進効果との関係で、正当化事由についても検討する必要がある場合が生じる。

①市場閉鎖効果

セット割引において、問題となるのは、連結商品・

役務における市場支配力ないし経済力の被連結商品・役務の市場へのレバレッジであるから、基本的に、競争への影響を見る「一定の取引分野」は、被連結商品・役務の市場であり[44]、反競争効果は、当該市場において「市場閉鎖効果」を生じさせるか否かで判断される[45]。その場合、行為者が、被連結商品・役務の市場において、価格支配力の意味での市場支配力を有することになる必要はない。当該市場の競争者が、他に代わり得る取引先を容易に見いだすことができない程度に市場が閉鎖されれば、ライバルコストが引き上げられ、反競争効果が生じることになるからである。その程度は、市場における競争の状況、行為者のシェアや順位などを総合的に見て判断することになるが、例えば、獣医の診療サービスの提供におけるセット割引が問題とされたイギリスのIDEXX事件[46]では、ライバルと競合する診療サービスのシェアは約5%にとどまることから、市場閉鎖効果が生じることはないとされている。他方、医薬品のセット割引が違法とされたアメリカのSmithkline事件[47]では、行為者のシェアが4－5割程度に達し順位が1位に上昇したことが示されている。なお、同じく市場閉鎖効果が問題とされる日本の排他条件付取引の規制においては、有力な事業者によって行われ、順位が1位で閉鎖シェアが3割程度に達する場合に違法とされている[48]。これらの事例から一義的な基準を導き出すことはできないが、少なくとも行為者の被連結商品・役務の市場シェアが3－5割程度で順位が1位に達すれば、市場閉鎖効果が認められる可能性が高くなると言うことができよう。

その場合、競争の実質的制限を要件とする排除型私的独占では、市場支配力の形成・維持強化が必要であるが、これを価格支配力の意味での市場支配力に限定する通説・判例の立場に立つと[49]、上記のような市場閉鎖効果を生じる場合を規制することが難しくなる。そこで、適用法条としては私的独占以外に取引妨害の規定も用い、競争減殺効果の有無についても判断することが必要であり、実際の規制においては、この規定が重要な役割を担うと考えられる。

②競争促進効果と「正当化事由」

セット割引は、先述したように効率向上による競争促進効果を有する場合があるから、この点も比較衡量した上で、反競争効果の可否についての判断を下す必要がある。その場合、「他の商品・役務」との関係をどのように考えるかが問題となる。排除行為該当性の判断は「他の商品・役務」であることが前提となるが、この基準は、両者が強い補完関係にあるとか、密接な技術的関連性を有するなど、複数の商品・役務がセットで提供されることにより明白な効率性の向上をもたらす場合を除外する、という機能を果たしている[50]。その点で、効率向上による競争促進効果との衡量は、他の商品・役務の判断において、実質的に行われていると評価することも可能である。

ただし、はじめに述べたように、セットでの提供が効率向上による競争促進効果をもたらす可能性はこれ以外にも存在するから、行為者側からそのような主張がなされた場合には、これも考慮する必要がある[51]。その場合、「他の商品・役務」であれば、それはセットによる明白な効率性のゲインを欠くことを意味するから、上記の市場閉鎖効果が認められれば、正当化事由が存在することについては、行為者側に証拠提出責任ないし争点形成責任があると解すべきである。

そこで、具体的に効率性が問題となり得るケースとしては、例えば、ⓐTVの有料番組のセット割引のように、価格差別による消費者厚生の向上と産出量の増大をもたらす場合、ⓑ固定通話とブロードバンドのセット割引のように、市場や技術の発展によって両者の連関がより密接になり、別個の商品・役務として購入する消費者が著しく減少することが予想される場合などが考えられる。このうち、ⓐについては、効率性向上が確実であること、実際に競争促進につながること、他に代替的方法がないこと等の条件を満たす場合には、正当化事由を認めることができよう[52]。また、ⓑについては、複数の商品・役務の一体的な販売が一般化し、新たな商品・役務の取引分野に移行することが近い将来に確実であると評価されるか否かが問題で

あり、これは、本稿で詳論しないが、被連結商品・役務の市場を別個の取引分野として画定できるかという論点とも交錯するものである[53]。

4. おわりに

セット割引は、一般的には競争促進的であり、何ら非難に値しないものである。しかし、以上から、市場支配的な事業者等が行う場合には、不当廉売に当たらなくても、競争者を市場から排除する行為として独禁法上問題になる可能性があることが明らかになった。現在、公益事業分野で行われているセット割引は、情報通信のように事業法による規制がなされていたり[54]、電力・ガスのように全面自由化の開始段階であったりすることから、直ちに本稿で検討した違法性判断基準に抵触するとは考えられないといえる。しかし、今後、自由化の進展や競争の激化により、独禁法上問題がある行為が発生する可能性があり、これに対する注意を怠らないことが必要である。また、本文中（3－3②）で指摘したように、競争者によるセット割引の模倣可能性が高まれば、独禁法違反行為も生じにくくなる。この点で、事業法による接続・託送の規制の強化や卸取引市場の整備を図って当該サービスの調達を容易にすることが、独禁法違反の可能性を未然に低下させることにつながる点にも注意すべきである[55]。

Daitaro Kishii
岸井 大太郎

法政大学 法学部 教授
1953年、東京都生まれ。東京大学法学部助手、法政大学法学部助教授を経て、現在、法政大学法学部教授。1989-1991ロンドン大学（LSE）客員研究員、2004-2005法政大学法学部長、2010-2015法政大学大学院法務研究科教授（兼任）、2010～公正取引委員会・独占禁止法懇話会会員。著書は『経済法―独占禁止法と競争政策―（第8版）』（共著、有斐閣2016）、『情報通信の規制と競争政策―市場支配力規制の国際比較―』（共著、白桃書房2014）など。

注

1) 本稿は、2015年10月17日に白鴎大学で開催された、経済法学会のシンポジウム「ネットワーク産業の規制改革と競争政策」における筆者の報告ならびに討論の内容を敷衍（ふえん）し展開させたものである。当日発言をいただいたシンポの報告者および池田毅弁護士ほかの参加者に感謝を申し上げる次第である。なお筆者の報告原稿「ネットワーク産業における規制改革の展開と課題－『市場形成』型規制と競争政策」については、日本経済法学会年報36号（有斐閣2015。9）3頁以下、17頁（注57）を参照。また、当日のシンポにおける討論の記録は、同年報37号（2016年9月刊行予定）に掲載される予定である。

2) EUではmixed bundling、アメリカではbundled discountsと呼ばれているものがこれに当たる。なお、無償での商品・役務の供与は、別途、利益による顧客誘引ないし景品付販売として問題になる可能性があるが、これは本稿の検討対象からは除外する。

3) 業務提携という形をとる場合もあり得る。なお、複数の事業者による共同販売は、カルテル規制の問題を生じるが、この論点は本稿では扱わないことにする。

4) 例えば、G.Niels /H.Jenkins,/J.Kavanagh, Economics for Competition Lawyers（2011）P.253-257など参照。

5) ただし、独占者による価格差別によって消費者厚生を悪化させる場合はあり得る。N.Economides, Tying, bundling, and loyality/requirement rebates, in Research Handbook on the Economics of Antitrust Law（2012）p.121以下。これは、前記のシンポジウムで鳥居昭夫教授が指摘した論点であり、後に述べる正当化事由の判断においては、考慮要因の一つとなり得る。ただし、そこでは消費者余剰を減少させる“搾取”が問題であり、その判断にあたっては、行為がなされない場合の“推定価格（but for price）”との比較が必要になることから、その算定も容易ではない。それゆえ、排除効果を問題にする本稿では、問題の指摘にとどめることにする。

注

6) セット割引は「混合型企業結合」の規制においても問題となり得る。田辺治・深町正徳『企業結合ガイドライン』(商事法務2014) 195頁以下。ただし、そこでは、当該企業結合によって可能となるセット割引等によって、市場の排他性ないし閉鎖性が生じることが問題であり、行為それ自体が独禁法に違反するか否かは問題にされていない。そこで、この点は本稿では問題の指摘にとどめ、正面からは扱わないことにする。

7) 公正取引委員会・経済産業省「適正な電力取引についての指針(平成28年改訂) 第2部1－2(1)①イⅰ(ⅰ)、公正取引委員会・総務省「電気通信分野における競争の促進に関する指針」(平成28年改訂) Ⅱ第2(2)アなど参照。

8) S.P.Gates, Antitrust by analogy :developing rules for loyalty rebates and bundled discounts, Antitrust Law journal Vol.79 (2013) pp.99-.p.123

9) 公正取引委員会「排除型私的独占に関する独占禁止法上の指針」(平成21年) 第2-4(1)は、主たる商品と従たる商品を「別々に購入した場合の合計額よりも低くなるため多くの需要者が引き付けられるときも、実質的に他の商品を購入させているのと同様」とする。

10) 抱き合わせにおけるシカゴ学派の「独占利潤拡張不能理論」の批判については、G.Niels/H.Jenkins,/J.Kavanagh, a.a.O., p.257-260参照。そこでは、被抱き合わせ商品に規模の経済性が存在し、またスイッチングコストなどの点で完全競争ではない場合には、抱き合わせによりライバルコストが引き上げられ、排除効果が生じることが指摘されている。

11) このような観点から、抱き合わせとセット割引を共通の類型として扱うものとして、Guidance on the Commission's enforcement priorities in applying Article 82 of the EC Treaty to abusive exclusionary conduct by dominant undertakings (2009/C 45/02) (以下"EC Guidance"と略す) Para47-62、伊永大輔「EUにおける市場支配的地位の濫用に係る指針(下)」公正取引711号48頁以下参照。

12) 藤田屋事件審決(公取委平成4・2・28審決、審決集38巻41頁)

13) このような解釈を示唆するものとして、E. Elhauge, United States Antitrust Law and Economics, (1st ed. 2008) p.410-411

14) N. Economides/I. Lianos, The elusive antitrust standard on bundling in Europe and in the United States in the aftermath of the Microsoft cases, Antitrust Law Journal (2009) Vol.76,p.483-,p.530

15) 前掲・藤田屋事件審決。また独占禁止法研究会報告「不公正な取引方法に関する基本的な考え方」(1982) 第2部6も参照。

16) アメリカ法では、「強制(coercion)」が存在することが、抱き合わせ販売を当然違法とするメルクマールの一つとされている。

17) S. P. Gatesa.a. O. ,p.124-126 は、それはセット割引に対する「非合理的な懐疑主義」「過度の不信」であるとする。

18) このようなアプローチをとるものとして、アメリカのOrtho事件(Ortho Diagnostic v Abbott, 920 F.supp.455) 参照。

19) この点を指摘するものとしてEuropean Commission, DG Competition discussion paper on the application of Article 82 of the Treaty to exclusionary abuses (2005) para182

20) このような需要者によるテストの機会の縮減を指摘するものとして、前掲・EC Guidance para22。なお、筆者は、このような需要者による競争者の商品・役務の評価機会について、ドイツの業績競争論との関係で「業績比較の機会の縮減・消失」「競争者の業績による市場参加機会の縮減・排除」として論じたことがある。拙稿「ドイツ競争法における『業績競争』理論(二)」法学志林83巻4号(1986) 61頁以下、94-97頁参照。

21) 白石忠志「独禁法における『抱き合わせ』の規制(下)」ジュリスト1010号78頁以下は、「強制」と「条件づけ」の境界が不分明で「『強制』概念は融通無碍に拡張可能」だとする。

注

22) Faul/Nickpay, The EU Law of Competition (3rd.ed.2014) p.446-447

23) 忠誠リベートが違法とされた日本のインテル私的独占事件(公取委平成17・4・13勧告審決)も、競争者と競合するCPUとインテルが独占するCPUを一括した忠誠リベートである点で、このような側面を有している。忠誠リベートについては、早川雄一郎「競争者排除型行為規制の目的と構造(一)～(四)」法学論叢175巻1号～177巻12号(2014-2015)参照。

24) このような区別をするものとして、前掲・EC Guidance Para37,59。忠誠リベートにおいては「吸引効果(Suction effect)」が問題となる。早川・前掲、法学論叢175巻6号106頁以下。

25) これについては、瀬領真悟「流通・取引慣行と独禁法」日本経済法学会編・経済法講座第3巻『独禁法の理論と展開[2]』(2002) 214頁以下、根岸哲編『註釈独占禁止法』(有斐閣2009) 511頁以下(泉水文雄執筆)等を参照。なお、取引妨害の場合には、「不当に」の要件が行為要件と効果要件を兼ねることになる。

26) 前掲・排除型私的独占ガイドライン第2-4(1)。「他の商品」性は、後述するように「正当化事由」の判断ともリンクしている。この点につき、川濵昇「独禁法上の抱き合わせ規制について(二完)」法学論叢123巻2号23頁以下も参照。

27) Cascade Health Solutions v. PeaceHealth (515 F.3d 883) 同判決については、早川雄一郎「複数商品リベート・セット割引規制における“Discount Attribution”基準」公正取引770号54頁以下参照。

28) EC Guidance para23. さらに、前掲 Cascade Health 判決では、価格引き下げ行動は基本的に効率性を反映するものであり、また、そうでない廉売による競争制限が成功する可能性は低いとする、廉売一般に関する“事実認識”が参照されている。

29) 以下については、Gates.a.a.0., N.Economides/I.Lianos, a.a.0.,等を参照。

30) 不当廉売規制に関し、この点を詳細に論じるものとして、川濵昇「不当廉売規制の残された課題」RIETI Discussion Paper.13-J-057(2013)。また、滝川敏明「抱き合わせ・バンドリング規制のEC・米国比較」公正取引705号(2009) 8頁以下も参照。

31) この点では、支配的事業者によるセット割引が、通常の廉売と異なり、ⓐ単品の価格を高くした上での「見せかけの割引」となる場合があること、ⓑセット割引に競争の重点が移って単品の値引き競争が行われにくくなり、全体として見ると価格競争が減少する可能性があることにも注意すべきである。E.Elhauge, United States Antitrust Law and Economics, (2nd ed.2011) p.409-410

32) D.Geradin,A.Layne-Farrar,N.Petit, EU Competition Law and Economics (2012) p.225

33) 排除行為該当性は「諸要素を総合的に考慮して判断すべき」ことについては、NTT東日本私的独占事件(最判平成22・12・7審決集57巻2号213頁)参照。競争減殺型の取引妨害が問題となる場合も、これに準じて考えることができる。

34) なお、行為の「人為性」は、これに関する判断で尽くされるから、あらためて別個に検討する必要はないと考えられる。

35) その場合、レバレッジが問題だから、当該支配力ないし経済力の内容のいかんは問わない。従って、例えば、ネットワーク施設の保有に起因する、既存の電力会社、都市ガス会社、NTTグループ等の“安定性”に対する信頼などもカウントされる。

36) この点に関しては、JASRAC私的独占事件(最判平成27・4・28判例タイムズ1414号123頁)における「包括徴収」方式の排除行為該当性の評価も参照。

37) 例えば、薬品メーカーによる、病院に対する、特許権を有する独占製品と競争製品をセットにした総割引率3%のバンドル割引がシャーマン法2条違反とされたアメリカのSmithkline判決(Smithkline v. Ellilly 575 F.2d.1056)では、競争メーカーが当該割引に対抗するためには、病院全体で16%、大規模病院向けでは35%の値引きが必要とされ、対抗不可能であったことが認定されている。

注

38) 抱き合わせ販売とされた事例であるが、郵政公社による、法的独占が認められた私人向け郵便と競争的なビジネス向け郵便のセット割引がTFEU102条違反とされたEUのDe Post-la Poste事件（5December 2001, 2002/180/EC）では、ライバルが必要なクリティカル・マスを維持できないことが重視されている。

39) 獣医の診療サービスの提供におけるセット割引のTFEU102条該当性が問題とされたイギリスのIDEXX事件（November2011, CE/9322/10）は、この点を強調する。なお、EC Guidance Para61は、模倣が容易であれば通常の不当廉売基準を適用するとしている。

40) 例えば、ブロードバンドサービスに関しては、NTT東西によるフレッツ卸が利用できるから、模倣は比較的容易だと言えよう。他方、電力や都市ガスは、数量や価格の面で、卸市場における実際の調達可能性が限られていることも少なくないと考えられる。

41) 前掲・NTT東日本私的独占事件、JASRAC私的独占事件参照。

42) その場合、セット割引は長期に維持可能だから、アメリカの平均可変費用基準は適切ではない。N. Economides/I. Lianos. a. a. O., P.511

43) なお、割引寄与基準を需要者に対する「強制」の有無のメルクマールと位置付ける考え方（前掲、Cascade Health判決など）があるが、先に述べた強制の不明確性から見て、このような振り分けは妥当ではない。

44) このほか、連結商品・役務の市場支配力を維持・強化する可能性もあるが、それは、被連結商品・役務の市場閉鎖効果の波及効果の問題であるので、ここでは扱わないことにする。

45) S. P. Gates, a. a. O., p.135、E. Elhauge（2nd.ed）,a. a. O., p.409-410等を参照。

46) 前掲・注40参照

47) 前掲・注38参照

48) 東洋精米機事件　東京高判昭和59・2・17審決集30巻136頁など参照。また、抱き合わせ販売の競争減殺効果が問題とされたマイクロソフト事件（公取委審決平成10・12・14審決集45巻153頁）でも、シェアは不明だが順位が1位に上昇したことが認定されている。

49) 岸井大太郎・大槻文俊・和田健夫・川島富士雄・向田直範・稗貫俊文『経済法―独占禁止法と競争政策［第8版］』（有斐閣2016）11-12頁。根岸哲「『競争の実質的制限』と『競争の減殺』を意味する公正競争阻害性との関係」甲南法務研究4号（2008）1頁以下参照。

50) N. Economides/I. Lianos. a. a. O., p.528参照。

51) 抱き合わせ販売につき、Faul/Nickpay,a.a.O.,p450-454などを参照。

52) この点は、「効率性」に関する「企業結合ガイドライン」第4-2（7）が参考になる。

53) なお、H. Hovwnkamp/E. hovenkamp, complex bundled discounts and antitrust policy,57 Buffalo Law review 1277は、3品目以上のセット割引において、一部の品目の競争者を完全に排除する場合でも、他の品目で競争が活発であれば競争促進的であることを指摘するが、これも正当化事由ないし市場画定の問題として考えるべきものである。

54) 総務省「NTT東西のFTTHアクセスサービス等の卸電気通信役務にかかる電気通信事業法の適用に関するガイドライン」（平成27・2）

55) 例えば、EUの情報通信における模倣可能性の容易化の規制につき、岸井大太郎・鳥居昭夫編著『情報通信の規制と競争政策』（白桃書房 2014）192頁以下参照。

「Pacific Telecommunications Council'16」参加報告

東平 福美
慶應義塾大学 政策・メディア研究科 後期博士課程

2016年1月17日から20日まで、ホノルルにてPTC（Pacific Telecommunications Council）年次総会が開催された。アジア・太平洋地域の情報通信やICTに携わっている通信事業者、政府、大学等の関係者が一堂に会し、次世代を見据えた通信政策、技術・システムについて意見を交換した。

◆PTCとは

公益財団法人KDDI財団の海外学会等参加助成を受け、筆者は2016年1月17日から20日まで、ホノルルにて開催されたPTC（Pacific Telecommunications Council）年次総会に参加した。

PTCとは太平洋電気通信協議会のことであり、毎年年次総会をハワイ・ホノルルで開催している。PTCは、高度情報化社会を築くための共通理解と認識を醸成することを目的とし、アジア・太平洋地域の情報通信関係者を中心に、広く全世界の情報通信に関する政策、機構、技術・システム、事業・利用等、あらゆる問題について自由に意見を交換・討議する場として、1980年1月、ハワイ州法下で設立された非営利の公益法人（米国法人）である。アジア太平洋地域の情報通信開発に興味があればだれでも参加できるという趣旨から、会員は主官庁、通信事業者、メーカー、大学・研究所、コンサルタント会社、利用者（商社、金融業者等）まで幅広い層を持つユニークな団体として注目されており、欧州からも多数参加している（PTC日本委員会HPより引用）。

今年は"Reimagining Telecoms"というテーマのもと、4日間という短い期間ではあるが、世界79カ国・地域から2,000人以上が参加した。215人のスピーカーによる55の招待講演やさまざまなセッションが行われた。招待講演や各セッションで取り上げられた内容は、電気通信の価値を再想像・創造することであり、もはや電気通信はネットワークでもコミュニケーションのツールでもなく、それ以上の価値を持つものであり、その価値とはどのようなものなのかについて議論がなされた。また、電気通信における電力消費の問題とそのエコ化について焦点が当てられ、各通信事業者、各国の取り組みを知ることができた。前述どおり、多種多様な参加者がいるため、各通信事業者が現在の技術やシステム、さらには将来の5Gなどのプランについてプレゼンを競って行うセッションもあれば、その隣では、研究者たちが各自の研究成果を発表している。また、同時進行で何百というビジネス交渉が行われている。それぞれの参加者は皆対等な立場で討議、意見交換することができ、同じ事柄でも各自のバックグラウンドを生かして、異なる側面から見解を述べているため、新しい気づきが至るところにあり、大変有意義で活気溢れる学会であった。

◆自身の研究テーマ
～太平洋島嶼（とうしょ）地域の情報通信技術の発達と学びの形の変化～

筆者は現在、博士課程に所属し、太平洋島嶼（とうしょ）国・地域の遠隔教育について研究している。昨年5月に福島

Pacific Islands Telecommunications Association によるセッションの様子

Opening Receptionの様子

で行われた第7回太平洋・島サミット（PALM7）は記憶に新しいが、日本は太平洋島嶼国・地域に対して、防災、環境保全、インフラ整備などを中心に積極的に交流かつ援助を行っている。その一つに教育も含まれているのだが、筆者は、島同士をつなぐ遠隔教育という側面から、フィジーにある南太平洋大学（The University of the South Pacific）の衛星通信ネットワークを中心に、通信と国際協力の在り方について調査している。

今回のPTCへ参加した目的としては、太平洋島嶼国・地域の方々とのネットワーク作りと、現在、これらの地域で行われている情報通信事業について、技術面、政策面からの生の声を聞くことであった。太平洋島嶼国・地域はグローバルな観点からも極めて魅力ある市場であり、PTCのフォーラムの参加者も、欧米をはじめ、アジア、オセアニアを代表とする通信事業者、研究者がこぞって太平洋島嶼国・地域の情報通信の拡大を目指してさまざまな戦略的取り組みを行っており、この地域だけのセッションも複数準備されていた。太平洋島嶼国・地域からも各国の政府関係者が参加し、ビジネスはもちろんのこと、システムやプロジェクトの実現に向けて皆が率直に意見交換や交渉をしており、筆者も駆け出しの研究者ではあるが、期待以上の情報を得るとともに、ネットワークの構築ができた。また、企業・政府と大学の連携による国際協力を間近で見ることができ、大変貴重な話を伺うことができたことは、今後の博士論文の方向性を決める一助となったと言っても過言ではない。政府のODAや国際機関に頼るだけでなく、各企業の行う取り組みと合わせて、一研究者としての立ち位置を知ることができたように思う。さらに、PTCの年次総会が開催されるのが毎年ホノルルということで、米国からの参加者が半数を占めているのだが、米国の太平洋島嶼国・地域への交流の拠点としてのハワイやグアムの存在の大きさをあらためて感じることができた。各先進国がなぜ太平洋島嶼国・地域を支援するのか、それぞれ理由は異なるかもしれないが、その援助の事例を比較検討することで、最も良い情報通信と教育の援助の形を見つけることができるのではないだろうか。

今回のPTC年次総会では、多くのセッションで「ブレンド」という言葉がキーワードとなっていた。情報通信は、今後、さまざまなモノやコトとされてブレンドされていく。PTCはビジネスという側面がどうしても前面に出てしまいがちだが、一方で研究者のリサーチグループもあり、若手の研究者には学会参加の補助などもしている。また、学会最終日には通信事業者と研究者に分けて、優秀な発表を表彰する場も設けられており、ビジネスとアカデミックの両方に力を注いでいると感じられた。アジア・太平洋地域の情報通信の普及・促進という一つの目標に向かって、バックグラウンドの異なる者同士が日々切磋琢磨し、このPTCという空間で各自の考えを持ち寄ってブレンドさせるというのは大変価値がある。自身もPTCで得た知識を社会に還元できるよう、今後一層研究に励むとともに、このような機会を提供してくださったビジネスとアカデミックのブレンドの公益財団法人KDDI財団に深謝する。

Fukumi Higashihira

東平 福美

慶應義塾大学 政策・メディア研究科
後期博士課程
慶應義塾大学文学部卒業、慶應義塾大学大学院政策・メディア研究科修士課程、コロンビア大学大学院修士課程修了。現在は慶應義塾大学政策・メディア研究科後期博士課程に在籍しながら、東京大学大学院工学系研究科、立教大学、早稲田大学にて非常勤講師として教鞭を執る。専門は、遠隔教育、日本語教育である。

デュッセルドルフ特許法大会（Düsseldorfer Patentrechtstage）に参加して

玉井 克哉
東京大学 先端科学技術研究センター 教授／信州大学 経法学部 教授

本年3月10日・11日に開催されたデュッセルドルフ特許法大会に参加し、ドイツにおける最高レベルの実務家とディスカッションする機会を得た。その模様を報告する。

◆デュッセルドルフでのカンファレンス

欧州特許法は後述のように激動期にあるが、今日の実務については、ドイツのデュッセルドルフが圧倒的な存在感を放っている。それは、EU域内での特許権侵害訴訟の約7割がドイツで提起され、そのうちの約7割がデュッセルドルフ地裁で提起されるという事実による。要は、EU域内で提起される特許訴訟の約半分が、デュッセルドルフで提起されるというわけである。

ここで取り上げる「標準必須特許」のみならず、特許法の領域では、新たな論点が提起されることが多い。特許制度の対象となる技術に国境はないから同じ問題が各国で提起されることも多いのだが、米国と並び、欧州の動向は常に注目の的である。米国では第二審段階で連邦巡回区控訴裁判所が集中管轄を有しており、そこで展開された法律論が合衆国最高裁で修正されなければ、それが判例として法的な拘束力を持つことになる。他方欧州では、形式上は28の加盟国の一つにすぎないドイツの、形式上は16の特許侵害事件管轄裁判所の一つにすぎないデュッセルドルフ地裁、その控訴審たるデュッセルドルフ高裁、そして上告審たる連邦大審院（BGH）のラインで、法的にはドイツ国内でのみ通用する判例が形成される。その影響力は事実上のものにすぎないが、全事件の半分がそのラインで処理されるのであるから、実際上の意義は大きい。

こうした状況は、当事者の選択の結果でもある。欧州における特許侵害事件がデュッセルドルフに集中し、同地の裁判官が豊富な経験と深い洞察を蓄積しているため、新たな論点に直面した特許権者が依拠すべき判決を求めてデュッセルドルフで訴えを提起するようになるのは、当然の勢いである。そのため、新たな問題が真っ先に同地で処理され、その動向が全欧州、あるいは全世界の耳目を集めることとなるのである。

今回、筆者が参加したのは、デュッセルドルフ大学の主催で毎年行われるカンファレンスである。そこには、同地の地裁と高裁で多数の特許事件に関与し、現在は連邦大審院（BGH）特許専門部で裁判長を務めるペーター・マイヤー＝ベック氏が総括報告を行うためか、全ドイツから、最高レベルの実務家が多数参加する。筆者は、旧知の同大学ブッシェ教授から招待を受けることができた。

◆標準必須特許（standard essential patents）

今回、筆者が参加したのは、標準必須特許の扱いが数年来の問題となっているからである。現在のスマートフォン端末には、3G、LTE、Wi-Fi、Bluetooth等の

開会時の模様


壇上のブッシェ教授（左）とマイヤー＝ベック判事

規格が用いられている。そして、その一つ一つが数千もの特許発明を必須の技術として採用している。従って、理論的には、そうした特許発明についての権利者すべてが許諾しなければ、全世界の携帯端末が使用できないことになる。

他方で、スマートフォン・ビジネスが発展するに伴い、特許権を用いて他社を牽制しようという動きが顕著になってきた。その中でも、グーグル社やサムスン社が、他社から取得した標準必須特許を用いてアップル社やマイクロソフト社を牽制する姿勢をあらわにしたことから、世界各国で同時並行的に多数の訴訟が係属した。

この件に関するドイツの基本判例は、2009年に連邦大審院（BGH）が出したオレンジブック判決（Orange-Book-Standard）であった。これは比較法的には特許権者に有利なものだったが、2015年7月16日、EU裁判所（CJEU）が一連の係争における特許権の効力を制限する方向での判決を下したことで、両者の関係が問題となった。BGHの判決は国内法たるドイツ特許法の解釈（「独禁法違反の抗弁」の成立要件）を示したものであるのに対し、CJEUの判決はEU独禁法の解釈（特許権行使が独禁法違反となる要件）を示したものであるから、形式的には優劣がない。だが、実質的に方向が違うのは明らかであって、両者の関係は大きな問題である。

この問題に関しては、EU全体を統括するCJEUの判決がBGHの判決を実質的に変更したものだと理解する向きが、わが国では多い。しかし会議参加者の代表的な理解は、「両者は適用の局面を異にしており、矛盾するものではない。今後の問題は、両者の適用範囲について限界線を引くことである」（ブッシェ教授）、あるいは「両者の事案は異なるが、『ライセンスを受ける意思のある者』に対する特許権の行使が独禁法違反となり得る点で、基本的な方向は共通する」（マイヤー＝ベック首席判事）というものであって、わが国でこの問題を扱う上で、貴重な示唆を得ることができた。

◆全体的な感想など

今回参加した研究集会は、議事のほぼすべてがドイツ語でなされ、外国からの参加はごく少ない（今回は178名中6名。うち日本人2名）。いわば、気心の知れた最高レベルの専門家が立ち入った議論を行い、今後の実務をリードする場である。今年も、2017年から施行開始予定の欧州統一特許制度が公式プログラムで取り上げられる傍ら、昨年のテーマだった標準必須特許の扱いについて、コーヒー・ブレークやレセプションにおいて、そこここで話題となった。そうした場に参加するのは、活字などで公表された媒体を通じた情報収集に増して、重要なことがある。海外学会等参加助成制度によってその機会を与えていただいた公益財団法人KDDI財団に、衷心より感謝申し上げたい。

Katsuya Tamai
玉井 克哉

東京大学 教授／信州大学 教授
1983年東京大学法学部卒業、同年東京大学法学部助手、1988年学習院大学法学部助教授、1990年東京大学法学部助教授、1997年東京大学教授（先端科学技術研究センター）。2016年4月より信州大学教授（経法学部）兼任。1989-92年マックス・プランク知的財産法研究所（ドイツ）、1999-2000年ジョージ・ワシントン大学及び連邦巡回区控訴裁判所（米国）に留学。専攻は知的財産法、行政法。現在の研究テーマは、(i)標準必須特許、(ii)ネットワーク時代の著作権法、(iii)個人データ保護法、(iv)営業秘密法制、及び(v)米国における「主権免責」原則の取扱い。

やさしいICT用語解説 ⑬

大槻知明教授に聞く

5G

5G（第５世代移動通信システム）をめぐる動きが活発になってきた。
関連情報サイトでの発信も増えている。5Gの本質的な特徴とは何なのか。
5Gについて、電子情報通信学会「通信ソサエティ」副会長を務める
慶應義塾大学理工学部の大槻知明教授に聞いた。

Q 「5G」という言葉を目にする機会が増えました。そもそも5Gとは何ですか。

大槻（以下同） 現在のモバイル通信の主力である「第4世代移動通信システム（4G）」の次の世代の移動通信システムのことです。欧米や日本などでは2020年のサービス開始を目指しています。

モバイル通信のトラフィック量は、毎年2倍のスピードで増加し、20年には10年の1,000倍になると予測されています。5Gでは、急増するトラフィックだけでなく、IoTやM2Mなどによるデータを収容することもテーマになっています。

5Gの技術目標は各国ともほぼ同じです。つまり、①大容量化＝10年に比べて1,000倍のトラフィック量に対応する、②高速化＝第4世代のLTEの100倍程度のデータ伝送速度、③低遅延性＝データ送受信の遅延が0.1ミリ秒以下、④多数接続＝LTEの100倍以上の端末が同時接続する、⑤省電力化＝デバイスの電池寿命を10倍にする、などが掲げられています。

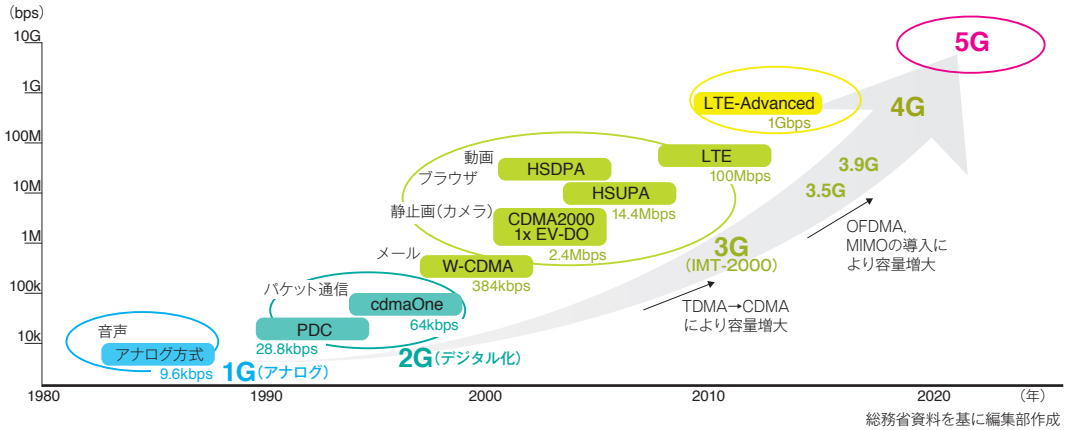
Q 5Gには、従来にはない技術が必要ですか。

第4世代のLTEやLTE-Advancedをさらに高度化させた技術と、5G向けとして新たに開発された技術が共存する形になるでしょう。ただ、4GまではCDMAやOFDMAなどの伝送変調方式の改良のほか、MIMOなどの伝送技術も開発されました。5Gの技術目的はそれだけでは実現できず、さまざまな技術の“合わせ技”が必要です。要素技術だけでなくネットワーク全体のアーキテクチャというか、モバイル通信のエコシステムの在り方が問われています。

高速・大容量伝送を実現するには、伝送のための帯域幅を広げたり、単位面積当たりの基地局（セル）を増やすなどの取り組みが必要です。しかし“プラチナバンド”の700～900MHz帯などで使える帯域幅は狭く、まだ未開拓の領域で帯域幅を広く取れる5～6GHzの利用を主に、さらなる高周波の利用もテーマになっています。高周波になるほど特性が光に近くなるので直進性が強くなり、基地局がカバーできるエリアは狭くなります。しかし一方で、関連技術との親和性が良いというメリットがあります。

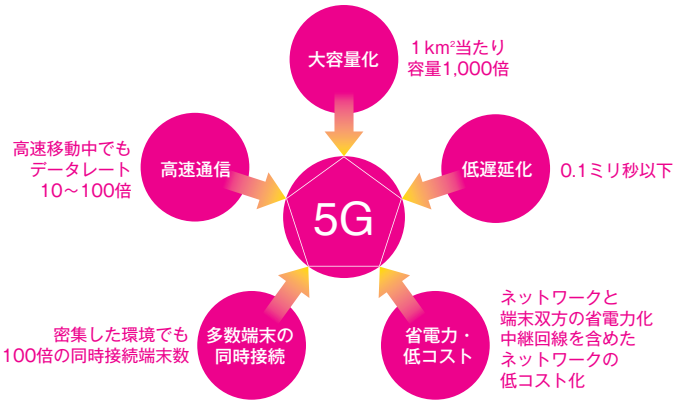
まず「スモールセル（Small Cell）」で1基地局のカバーエリアを狭くします。その上で、第4世代で実用化されているMIMOの発展系である「マッシブ（大規模）MIMO」を使います。MIMOは、複数のアンテナを同時に使って大容量データを高速に伝送する技術ですが、高周波になるほどアンテナは小さくて済みます。同じスペースならば基地局も端末もたくさんのアンテ

図表１ 無線伝送技術の進化



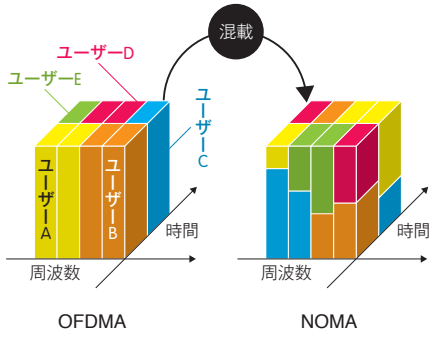
総務省資料を基に編集部作成

図表２　第５世代移動通信システムの要求条件



総務省資料を基に編集部作成

図表３　NOMA（非直交多元接続）の考え方



ナを装備できるので大容量・高速伝送ができます。また、多くのアンテナで鋭いビームを形成できるため、端末にダイレクトに伝送できれば電波伝搬の損失を減らせます。つまり、伝送の空間的な利用効率を上げるのです。

Q　5Gで投入される革新技術はありますか。

例えば「非直交多元接続（NOMA）」があります。従来の伝送は、データを時間をずらすか周波数をずらすかして順番に並べて送り出すイメージです。Aさんの次がBさんで、再びAさんのデータを送る。しかしNOMAでは、Aさんだけでなく、BさんもCさんのデータも、あたかも積み木を積んだかのような“混載”で同時伝送します。帯域を有効に使え、伝送スピードを上げられます。

また、低い周波数と高い周波数を同時に利用することを目指した連携技術として「ファントムセル」や「フレキシブル・デュープレクス」などの技術も提供されています。

ファントムセルは、制御信号とユーザーデータを分離して異なる周波数に振り分けるもの。フレキシブル・デュープレクスは、従来は単独で使われてきたFDDやTDDなどの伝送方式をより広い周波数帯で柔軟に使い分ける技術で、周波数帯域の効率的な利用を目指します。

Q　5Gはどのように使われ、私たちの生活をどのように変えるのでしょうか。

スマホのよほどのヘビーユーザーでもない限りは「5Gでなければ困る」ということはないでしょう。ただ新しいモバイル環境が出現するのは確かです。

例えば、高精細ビデオ映像のようなリッチコンテンツの超高速通信、高密度で人がいる場所での高品質な通信、IoTでの活用、クルマや各種の機械の自動運転制御（だからこそ超低遅延かつ高信頼性が要求されます）、遠隔医療などが想定されています。特にIoTでは、各種のデータを大量に収集できるようになるので新しいビジネスが出現する可能性があります。クラウドサービスとの連携も容易になるので、予想外の利用法が出てくるでしょう。

個人的には、人がたくさんいるスタジアムのような場所での使われ方に興味があります。オリンピック会場で、クラウドにある競技映像を自分の好みで再生して選手データも確認する。それが容易にできるとしたら目の前で展開される競技の見方は劇的に変わります。

Q　国際標準化の動きはどうなっていますか。

モバイル技術の国際的なコンソーシアムである3GPPが、2016年3月に「5Gについての技術議論を始める」と発表しました。18年末頃には第1弾の標準化が公表され、以後、順次なされていくと思います。標準化された技術や実用化された技術を織り込みながら、第4世代のネットワークに重なる形で20年にはサービスが開始されるのは間違いないと思います。

【略語説明】IoT…Internet of Things／M2M…Machine to Machine／LTE…Long Term Evolution／CDMA…Code Division Multiple Access（符号分割多元接続）／OFDMA…Orthogonal Frequency Division Multiplexing Access（直交周波数分割多重接続）／Cell…セル（1つの基地局がカバーする通信可能範囲）／MIMO…Multiple Input Multiple Output／NOMA…Non-Orthogonal Multiple Access（非直交多元接続）／FDD…Frequency Division Duplex（周波数分割複信）／TDD…Time Division Duplex（時分割複信）／3GPP…The 3rd Generation Partnership Project

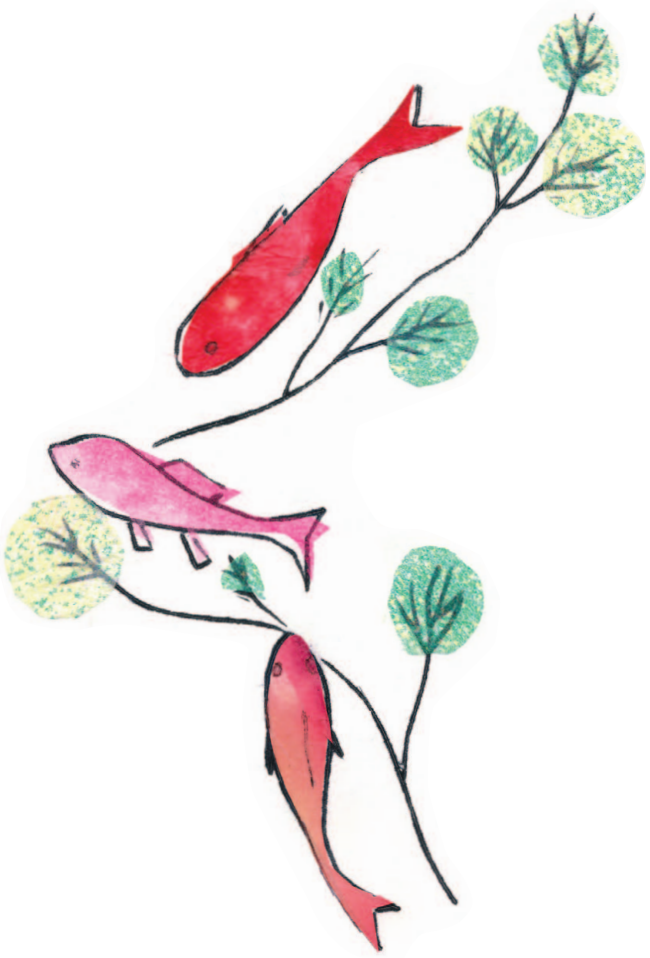
取材協力
大槻 知明（Tomoaki Otsuki）
慶應義塾大学 理工学部 情報工学科 教授
1994年慶應義塾大学大学院博士課程修了。博士（工学）。専門は無線通信、光通信、センサー、情報理論など。

彼らの流儀はどうなっている？

執筆：吉田 将之　絵：大坪 紀久子

たぶんキンギョにも感情体験がある。それを意識的に経験してはいないだろうけれど……。
いずれ心を理解できるときがくる。

キンギョもいろいろ考えている



感じ・考える

キンギョにも個性がある。ランチュウとかの品種のことではない。確かに、キンギョは皆同じに見える。ひらひらと泳ぎ回り、ときおり水底をつついている。しかしそれを言ったら、キンギョから見た人間も似たようなものだ。水槽をのぞきこむ、小突く、ただ通り過ぎる。

よく見ていると、キンギョの行動には個体ごとに一貫した傾向がある。すなわち個性を持っている。種としてある範囲に収まるとしても、1尾ずつ、極めて個魚的な内面を持っているようだ。

キンギョの行動は、反射の連鎖だけで成り立っているわけではない。経験によって行動が変化する。しかし単なる学習機械でもない。感じ、考えている。あしき擬人化だという批判も受ける。しかし、利得と損失の計算則のみで動物の行動を説明し

Masayuki Yoshida　広島大学 大学院 生物圏科学研究科 准教授

1965年生まれ。鹿児島大学卒業、広島大学で博士号取得。
英国ブリストル大学研究員などを経て現職。専門はバイオサイコロジー。
動物の脳が“気持ち”や“感じ”をつくりだす仕組みの解明に取り組んでいる。

たとして、豊かな生命世界の理解に到達できるのだろうか。

本能行動や学習の積み重ねだけでは対応しきれない状況も多々ある。

学習した行動や生まれ持った行動の呼び出しにはゆらぎがある。ゆらぎが良い方向に振れれば、事態をうまく切り抜けられる。そこに感情の機能を加えれば、行動が一貫性を持ち、生存力を高める。

不利になることもある。感じ、考え、実行するとき、キンギョなりの主観的世界が確かにあるだろう。

恐怖の脳内表現

わたしは恐怖の仕組みを研究している。恐怖を体験しているとき、特定の身体反応が現れる。人が恐怖を感じるような状況にキンギョをおく。するとキンギョは、人間と同等の身体反応を示す。彼らの小さな脳の中にも、人間と同様の恐怖の表象とでもいうべきものが作られているのだろう。脳の基本構造は共通なのだから。

今、自分は恐怖を感じているんだというメタ認知的な部分は、我々の肥大化した大脳皮質で作られるとしても、恐怖体験そのものはキンギョにもあって不思議ではない。

客観的、つまり証拠を共有できるように説明したい。だからキンギョの恐怖反応を数値化し、脳活動を記録し、薬物の効果を調べる。飼育にも気をつかう。快適な生活を提供しないと、恐怖の反応は引き出せない。

心を理解できるか

人と人との間であれば、他人の行動の裏にある感情はなんとなく分かる。この「分かる」というのがくせものだ。脳内のネットワークの動作や化学物質の分泌状態の変化で説明されても、それは他人の気持ちが分かるという感覚には合致しない。相手の主観を自分の主観で再現して、それを経験しているのである。それは必ずしも相手の主観のコピーではなく、あくまでもこちらの主観による再現である。誤解が生まれる大きな余地ありだ。

人以外の動物に対しては、その主観を人間の主観で再現することは難しい。またそのように努力しても、必ずしもその動物の心の理解には近づけない。どうするか。

ある状況下で動物の脳の中で起きていることを明らかにする。これを人間と比較して、動物が感じ、考えていることを合理的に説明していく。他人の気持ちが「分かる」ようにはいかなくとも、キンギョの心の理解に近づくことができるはずだ。

論文公募のお知らせ

**本誌では、我が国の情報通信制度・政策に対する研究活動の活性化を図るため、
新鮮な視点を持つ若手研究者の方々から論文を公募します。**

【公募要領】

申請対象者：45歳以下の研究者（大学院生を含む）で、日本に在住する方
＊過去4年間にNextcom誌に論文をご執筆された方、常勤の公務員（研究休職などを含む）、KDDIグループ関係者は応募できません。

論文要件：情報通信の制度・政策に関する未発表論文（日本語に限ります）
＊情報通信の制度・政策の参考となる内容であれば、情報通信以外の公益事業に関する論文も含みます。
＊技術的内容をテーマとするものは対象外です。
およそ1万字程度（刷り上がり10頁以内）

選考基準：情報通信分野における制度・政策に対する貢献度を基準に、監修委員会が選考します。
（査読付き論文とは位置付けません）

公募論文数：毎年若干数

公募期間：2016年4月1日～9月10日
＊応募された論文が一定数に達した場合、受付を停止することがあります。
＊掲載は2017年3月もしくは6月発行号を予定しています。

選考結果：2016年11月ごろ、申請者に通知します。

著作権等：著作権はご執筆者に属しますが、「著作物の利用許諾に関する契約」を締結していただきます。

執筆料：掲載論文の執筆者には、5万円をお支払いいたします。

応募：応募方法ならびに詳細は、下記「Nextcom」ホームページをご覧ください。

その他：1. 掲載論文の執筆者は、公益財団法人KDDI財団が実施する著書出版助成に応募することができます。
2. 要件を満たせば、Nextcom論文賞の選考対象となります。
3. ご応募いただいた原稿はお返しいたしません。

詳細については「Nextcom」ホームページ
http://www.kddi-ri.jp/nextcom/index.html をご覧ください。

お問い合わせ先：〒102-8460　東京都千代田区飯田橋3-10-10 ガーデンエアタワー 33階
株式会社 KDDI総研 Nextcom編集部

2016年度著書出版・海外学会等参加助成に関するお知らせ

本誌では、2016年度も公益財団法人KDDI財団が実施する著書出版・海外学会等参加助成に、候補者の推薦を予定しております。

【著書出版助成】

助成内容： 情報通信の制度・政策の研究に関する著書出版への助成

助成対象者： 過去5年間にNextcom誌へ論文をご執筆された方*

助成金額： 3件、各200万円

【海外学会等参加助成】

助成内容： 海外で開催される学会や国際会議への参加に関わる費用への助成

助成対象者： Nextcom誌に2頁程度のレポートをご執筆いただける方*

助成金額： 北米東部 最大50万円　北米西部 最大40万円　ハワイ 最大30万円
その他地域 別途相談（総額300万円）

＊常勤の公務員（研究休職などを含む）、KDDIグループ関係者は応募できません。

推薦・応募： 監修委員会において審査・選考し、公益財団法人KDDI財団への推薦者を決定します。
応募方法ならびに詳細は、下記「Nextcom」ホームページをご覧ください。

詳細については「Nextcom」ホームページ
http://www.kddi-ri.jp/nextcom/index.html をご覧ください。

お問い合わせ先：〒102-8460　東京都千代田区飯田橋3-10-10 ガーデンエアタワー 33階
株式会社 KDDI総研 Nextcom編集部

人が貨幣を求めるのは、貨幣そのもののためではなく、
貨幣で購買できるもののためなのである。
……アダム・スミス

何のためにおカネはあるのか？

髙橋秀実

おカネとは何か？

その謎を解明すべく滋賀県で始められた「地域通貨」を取材したことがある。独自のおカネ（券）を発行し、人々がそれを使って地域内でサービスやモノを購入する。新たなおカネの循環。かつてアダム・スミスが指摘したように、貨幣自体は富ではない。「人が貨幣を求めるのは、貨幣そのもののためではなく、貨幣で購買できるもののため」（『国富論』*）。つまりおカネは交換手段にすぎない、という原点に立ち返る試みだったのである。

ところが、この地域通貨は普及しなかった。人々は自分が「できること」と、誰かに「してほしいこと」をユーザー登録するのだが、「できること」はたくさん登録されるのに、「してほしいこと」がほとんどなかった。通貨を受け取る側ばかりになってしまったのである。それに「できる」といっても「○○について語れる」という自分の趣味を押しつけるようなものが目立ち、そうなると「できる」というより、相手に聞いてほしいことで、通貨を受け取るのか払うのかよく分からなくなってしまったのだ。

経済学的には需要と供給の不一致ともいえるのだが、よくよく考えてみれば、本当に「できること」と「してほしいこと」が合致すれば、そのまま実行すればよいので通貨の出番はない。「できること」「してほしいこと」ではなく、「してあげること」「してもらうこと」と言い換えれば済むことなのである。

果たしておカネは交換手段なのだろうか？

私は考えさせられた。人に何かをしてもらったとき、私たちは負い目を感じる。それを清算するためにおカネがあるのではないだろうか。そもそも「払う」は「祓う」に由来するわけで、おカネは負い目を祓い清めるためのもの。「してもらう」の「もらう」も「も（守）る」に由来し、守られることを意味する。つまりその人の保護下に入るということで、

article：**Hidemine Takahashi**
ノンフィクション作家。1961年生まれ。東京外国語大学モンゴル語学科卒業。
主な著書に『やせれば美人』『男は邪魔！「性差」をめぐる探究』『損したくないニッポン人』『不明解日本語辞典』など。最新刊に『人生はマナーでできている』（集英社）。
『ご先祖様はどちら様』で第10回小林秀雄賞、『「弱くても勝てます」開成高校野球部のセオリー』で第23回ミズノスポーツライター賞優秀賞受賞。

それがイヤな場合におカネで払う（祓う）。恩を着せられるのを拒否するようなもので、おカネは本質的に手切れ金なのである。

歴史をたどれば、日本は江戸時代まで公式な貨幣はほとんどつくっていない。長きにわたって中国の貨幣や鐚銭（ニセガネ）が流通していただけで、基本はずっと物々交換。裏を返せば、人間関係を祓わずに守ってきたのである。アダム・スミスの言い方を借りるなら、おカネではなく関係こそが富。人がおカネを求めるのは、人との縁を切るためであって、交換手段というより独立手段ではないだろうか。

*『国富論（二）』アダム・スミス著
水田洋監訳、杉山忠平訳　岩波文庫　2000年

背景

アダム・スミス(1723～1790年）の思想は、イギリス産業革命の理論的支柱となり、資本主義経済の発展の礎となった。「貨幣＝富」と考える重商主義を批判し、「真の貧富は消費財が豊富か否かで決まる」と論じた。

編集後記

今号の特集は、「仮想通貨」としました。いかがでしたでしょうか。私個人としましては、通貨の性格を、通貨高権や通貨の歴史という切り口で学ばせていただきました。また、従来にない変革が起きる原理を、技術に関する論文で学ばせていただきました。奥が深いテーマであると、あらためて痛感した次第です。

次号の特集は「IoTとイノベーション（仮称）」を予定しています。ご期待ください。（しのはら）

Nextcom（ネクストコム） Vol.26 2016 Summer
平成28年6月1日発行

発行　株式会社KDDI総研
〒102-8460 東京都千代田区飯田橋3-10-10 ガーデンエアタワー
TEL：03-6678-6179　FAX：03-6678-0339
URL：www.kddi-ri.jp

編集協力　株式会社ダイヤモンド社
株式会社メルプランニング
有限会社エクサピーコ（デザイン）
印刷　瞬報社写真印刷株式会社