だことは、もしかして、それも含めて「シェア」することで、次なる一歩が開けるかもしれない、ということなのだ。

今回「候補者と選挙資金」という題にしたのは、結局、候補者の誕生のひとつの大きなファクターが「資金」だからである。そして、長々交付金を含めた政治資金の内情を書いたのも、政党交付金が選挙の原資というこうした使い方をしたのは果たして正しかったのかどうかという疑問も持っているからだ。民進党から公認料をもらったのは助かったが、立憲民主党の候補として立候補する以上は、民進党からというのはやはり筋違いだ。しかし、公認料が出た時には民進党の総支部長だったわけで……などと考えていくと、結局そうした言い訳ができるシステムこそ、変えていかねばならないのではないかということなのだ。

森友・加計問題での公文書改ざん、自衛隊の日報隠し、北朝鮮問題等々、問題が深刻化すればするほど、佐藤栄作総理が仕掛けた「黒い霧解散」のように、また目くらましで解散、総選挙となる可能性もある。

そして、私たちはまた二〇一七年と同じことを繰り返すかもしれない。民意の本筋とはずれた結果に甘んじながら「選びたい人がいない」と言うのだろうか。

動くのは、今。有権者の側も選挙になる前の「平時」に動くべきなのだ。

例えば選挙のときの公開討論会のようなものを、普段から企画し、現職の国会議員や、それに対抗する政治家を呼んで議論する。そこには次期候補予定者の総支部長だけではなく、地方議員や一般の人も参加できるような形にすれば、地域で次の代表にふさわしい人材を見つけて行くことはできるような気がする。

重ねて言うが、それは選挙前だけでなく、普段にこそやらなければならない。

それを行なうことは今の時代、そう難しいことではないはずだ。私たちはインターネットというツールを使って、その過程を共有することが可能なのだ。また、SNS等で応援の意思や、反対の思いを伝えることもできる。

一時期流行病のように「ネット選挙」が取り沙汰されたが、それは主に候補者の立場からしか捉えられてこなかった。「選びたい人がいない」のであれば、有権者の側、特に、無党派層、SNSも「見るだけ」という人々こそこのツールを十分に機能、活用させて、政党に対しても候補者に対してもコミットできるだけの個々人の意思を伝えることはできるはずだ。そうなれば政党は選挙戦略に反映させるはずだ。

異端の選挙だった二〇一七年の選挙の総括は多角的に行なわれなければならないと思っている。その前史として位置づけられる都知事選挙、特に「鳥越選挙」の検証。本稿では野党側への言及に留まったが、連携一八年を迎える自公協力や、自民党のリクルーティングシステムと世襲、世論調査と選挙報道、またSNSの可能性等も含めて検証し、さらに広く候補者たちを含む有権者に問いかけていきたいと思っている。

なぜなら、また「候補者」は誕生するのだから。

仮想通貨は幻想通貨？

ビットコインの概要と仕組み

中島真志

なかじま・まさし　金融学者。一橋大学法学部を卒業後、日本銀行に入行。現在は麗澤大学経済学部教授。主な著書に『入門 企業金融論』（二〇一五年、東洋経済新報社）、『アフター・ビットコイン：仮想通貨とブロックチェーンの次なる覇者』（二〇一八年、新潮社）など多数。

二〇一七年は、「仮想通貨元年」であったものとされる。仮想通貨の価格は、一年で二〇～五〇倍にも値上がりし、資金を投じて仮想通貨を保有する人の数も増えた。それに伴って、マスコミでも頻繁に取り上げられるようになり、仮想通貨取引業者の派手なTVコマーシャルもあって、ビットコインの名前は広く知られることになった。

本稿では、仮想通貨の代表格であるビットコインを三回シリーズで取り上げることとする。第一回である今回は、まずビットコインの概要と仕組みについて解説することとする。

1　そもそもビットコインとは何か

ビットコイン（Bitcoin）とは、「サトシ・ナカモト」と名乗る人物が二〇〇八年に発表した論文をもとに作成された「仮想通貨」である。

ちなみに、サトシ・ナカモトというのは、謎の人物であり、未だに誰かは分かっていない。名前をみると日本人のようにも思われるが、欧米の暗号関係者と交流が深かったことや、流暢な英語を駆使して論文を書いていることなどから、どうも日本人ではないのではないかとみられている。

ビットコインは、インターネットを通じてデジタル・データがやりとりされることによって価値が移転する仕組みであり、一般的な通貨が持っている物理的な存在（紙幣やコイン）がないことから、わが国では一般に「仮想通貨」（バーチャル・カレンシー）と呼ばれる。

また、高度な暗号技術を使うことによって、データの複製や通貨の二重使用を防止していることから、海外では「暗号通貨」（クリプト・カレンシー）と呼ばれることが多い。

2 ビットコインの特徴

ビットコインは、これまでの通貨にはなかった様々な特徴を持っており、このため「通貨の革命である」とも言われる。主な特徴としては、以下のようなものがある。

第一に、中央に管理者がいないという点である。各国の通貨の場合には、その国の中央銀行が通貨の発行総量など全体の枠組みを管理しているが、ビットコインの場合には、中央にはそうした管理者がおらず、プログラムが通貨の発行などを制御する仕組みとなっている。このため、ある意味で「ガバナンスがない通貨」となっている。

第二に、独自の通貨単位を持つという点が挙げられる。ドルや円には一〇〇ドルとか、一万円といったかたちで通貨の量を示す単位が存在している。ビットコインの場合には、「BTC（ビーティーシー）」という単位があり、このため円やドルなどの「法定通貨」との間で交換レートが発生する。ビットコインは、1BTCより小さな単位でも取引を行うことができ、0.1BTCや0.05BTCといった小さな単位での取引も可能である。

第三に、発行主体がないという点がある。そもそもビットコインは、誰の負債でもないかたちで、プログラムによってネットワークの参加者に発行されることになっている。この点は、銀行券が「中央銀行の負債」として発行されているのと比べると、大きな違いである。

第四に、「プルーフ・オブ・ワーク」という難しい計算をすることによって安全性を確保しており、この計算の成功者には、リワード（報酬）が与えられることになっている（詳細は後述する）。

第五に、取引の確定までに時間がかかるという点がある。ビットコインの場合には、約一〇分ごとに新たな「ブロック」が作成されて、取引が確定していく仕組みとなっている。

第六に、発行上限が定められていることである。ビットコインは、二一〇〇万BTCという発行上限が決められており、それ以上は発行されないことになっている。これは、通貨が過剰に発行されることによって、インフレ（通貨価値の下落）が発生するのを防ぐためであるものとされている。

3 ビットコインを入手するための方法

ビットコインを入手するためには、以下のような三つの方法がある。

第一に、「買う」という方法である。各国には、「仮想通貨取引所」（仮想通貨交換業者ともいう）があり、ここで、法定通貨（円、ドル等）と仮想通貨を交換することができる。わが国にも、約三〇社の仮想通貨取引所がある。

第二に、「受取る」という方法がある。商品やサービスの対価としてビットコインを受取ることができる店舗が徐々に増えてきている。こうした店舗では、ビットコインによる決済が行われると、顧客からビットコインを受取ることになる。

第三は、「プルーフ・オブ・ワーク」という難しい計算処理を行うことにより、その対価としてビットコインを受取るという方法がある（詳細は後述する）。

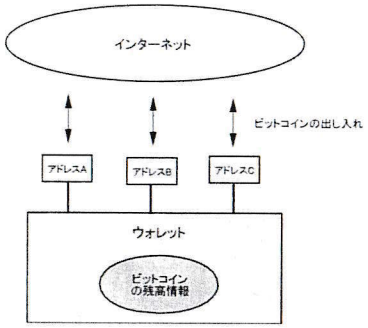
4 ビットコインを支える不思議な仕組み

ビットコインは、従来にはなかったいくつかの「不思議な仕組み」によって実現されている。

1 ウォレットとアドレス

まず、ビットコインの受払いに必要なものについてみておこう。一つは「ウォレット」である。これは電子的な財布であるため「デジタル・ウォレット」とも呼ばれる。通常、ユーザーは、このウォレットを自分のパソコンやスマートフォンの中に作って、自分のビットコインを保管する。次に「ビットコイン・アドレス」である。これは約三〇桁の英数字からなる文字列であり、口座番号のようなものであると考えておけばよい。ビットコインを相手に送る場合には、相手のアドレスを指定してコインを送付することになる。

図1　ウォレットとアドレスの関係



出所：筆者作成（以下同じ）

ウォレットとアドレスの関係を図1に示す。

ウォレットとアドレスの関係をみると、まず、一つのウォレットから、複数のアドレスを作ることができる（図1）。ビットコインのすべてのやり取りは、インターネット上でみることができる。つまり、どのアドレスからどのアドレスへ、何時何分に、いくらのビットコインが送られたのかが、一件ごとに表示されている。しかし、ビットコインのウォレットを作成する際には、特に自分の名前や身分を明かす必要はないため、各アドレスが誰のアドレスであるかは分からない。つまり、アドレスについて個人の特定はできない仕組みとなっており、この点が、本人確認が必要とされている銀行口座との大きな違いとなっている。このため、ビットコインは、高い匿名性を有している。この点は、メリットであるともいえるが、一方で、さまざまな問題を引き起こす原因ともなっている（詳細は後述）。

2 P2P型ネットワークの採用

従来のシステムでは、「クライアント・サーバー型ネットワーク」と呼ばれる仕

図2　P2P型ネットワーク

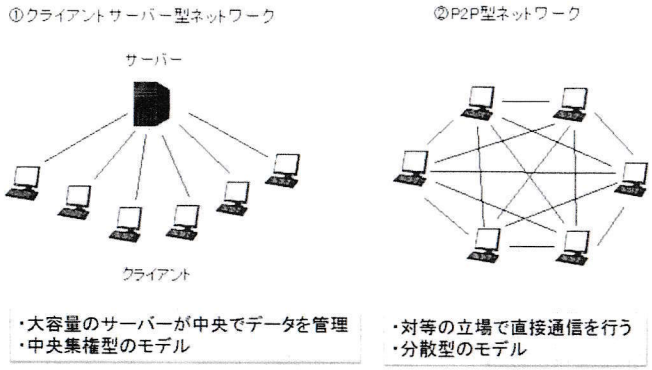
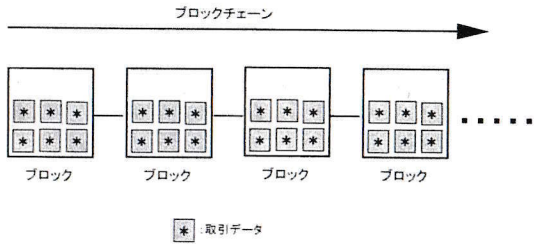


図3　ブロックチェーンのイメージ



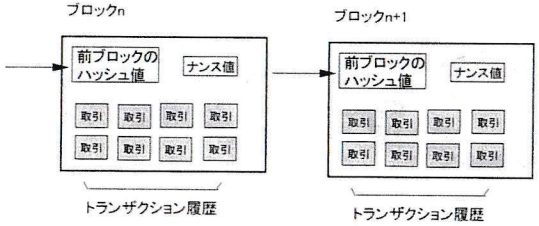
組みをとるのが一般的であった。これは、多数のクライアントに対して、大容量のサーバーが中央に一つだけ設けられ、このサーバーが全体の管理を行いつつ、データを保持・提供するという仕組みである。各クライアントは、サーバーとだけ通信するという「中央集権型」の仕組みとなっていた（図2の①）。たとえば、銀行のインターネット・バンキングの例をみると、銀行のコンピュータがサーバーとして中央でデータを管理し、各顧客のパソコンがクライアントとしてサーバーと通信を行うことになっている。

これに対して、ビットコインでは、「P2P型ネットワーク」という仕組みを採用している。P2Pとは、「peer-to-peer」の略である。P2P型のネットワークでは、ネットワークに接続されたコンピュータ（「ノード」とも呼ばれる）同士が対等な立場および機能で直接通信を行うかたちになる（図2の②）。このため、中央にコントロールする主体がない「分散型」のモデルとなっている。これにより、世界中にあるウォレットが相互に通信を行うことができ、参加者同士が直接的にビットコインを送り合うことが可能になっているのである。

3 安全性を確保するための「ブロックチェーン」

ビットコインの安全性を確保するための仕組みが「ブロックチェーン」である。これは、一定時間の「取引の束」（これを「ブロック」と呼ぶ）を時系列でチェーンのようにつなげて記録していく仕組みである（図3）。ブロックをつなげていく形態がチェーンのようにみえることから、「ブロックチェーン」と呼ばれる。チェーンの過去の取引データを改ざんしようとすると、その時点から最新のブロックチェーンまでをすべて改ざんしなければならないため、過去の取引の改ざんが困難となるような仕組みとなっており、コインの二重使用や通貨の偽造などの不正な取引を防止することが可能になっている。

図4　ブロックの内容



一つのブロックの中には、①一定期間の取引データ、②前ブロックのハッシュ値、③ナンス値、という三つの種類のデータが含まれている（図4）。

このうち「取引データ」は、送金額や送金人などの情報であり、一〇分ごとの取引データがブロックに格納されていく。次の「ハッシュ値」を導き出すためには、

「ハッシュ関数」という計算方法が使われる。ハッシュ関数は、膨大なデータを一定の長さの短いデータに圧縮する手法であり、同じデータからは必ず同じハッシュ値が得られる一方で、少しでも異なるデータからは全く異なるハッシュ値が得られる。ハッシュ関数は、出力値から入力値を推測することができない一方向関数となっている。

最後の「ナンス値」は、次のブロックに使うハッシュ値をコントロールするための数値である。つまり、ブロック全体のデータのうち、「取引データと前ブロックのハッシュ値」はすでに決まっているため、次のブロック用のハッシュ値を変更するために変えることができるのは、ナンス値のみとなっている。

4 複雑な計算をする「プルーフ・オブ・ワーク」

「プルーフ・オブ・ワーク」は、偽造を防止し、取引を承認していくための仕組みである。具体的には、前述の「ナンス値」を計算することを意味する。その際に、次のハッシュ値の先頭に「一定以上の数のゼロ」（例えばゼロが一二個など）が並ぶようにすることが条件とされている。

こうしたハッシュ値を求めるためには、ナンス値にいろいろな数値を入れて、ブロック全体のハッシュを求めてみるという「総当たり法」を行うしか方法はない。少し考えると分かるが、こうした計算を行うためには、かなり膨大な計算量が必要となる。

こうした条件を満たすハッシュ値を導くようなナンス値が求められ、新たなブロックチェーンが作成されることを「取引の承認」と呼び、そのブロックに含まれているすべての取引がその時点で承認され、取引が確定する。ブロックチェーンでは、一〇分ごとに取引がまとめて承認される仕組みとなっている。

5 ビットコインの新規発行「マイニング」

1 マイニングの仕組み

「マイニング」とは、難しい計算（プルーフ・オブ・ワーク）を行って、最初に適切な答えを求めた人に、報酬（リワード）として、新たなビットコインが発行される仕組みのことである。ビットコインでは、新たにコインが発行されるのは、このマイニングが唯一の方法となっている。

マイニングは、ネットワーク上の多くの参加者が一斉に同じ作業を行って解答を求めるが、世界で最初に答えを見つけた第一位の人にしか、リワードは与えられない仕組みとなっている。答を見つけた人は、そのことをネットワーク全体に知らせ、他の参加者は、その答えが正しいかどうかをチェックする。ネットワーク内の他の参加者によって答えが正しいことが確認されると、そのブロックは承認されて、ブロックチェーンの最後尾に追加される。これにより、そのブロック内の取引が承認されて、ビットコインの受渡しが成立したことになるのである。

このプロセスは、鉱山で金（ゴールド）を掘り当てるように、「無から有を生み出す」プロセスであることから、「マイニング」（採掘）と呼ばれている。また、こうした計算作業を行う人のことを「マイナー」（採掘者）と呼んでいる。

2 取引成立のまでの仕組み

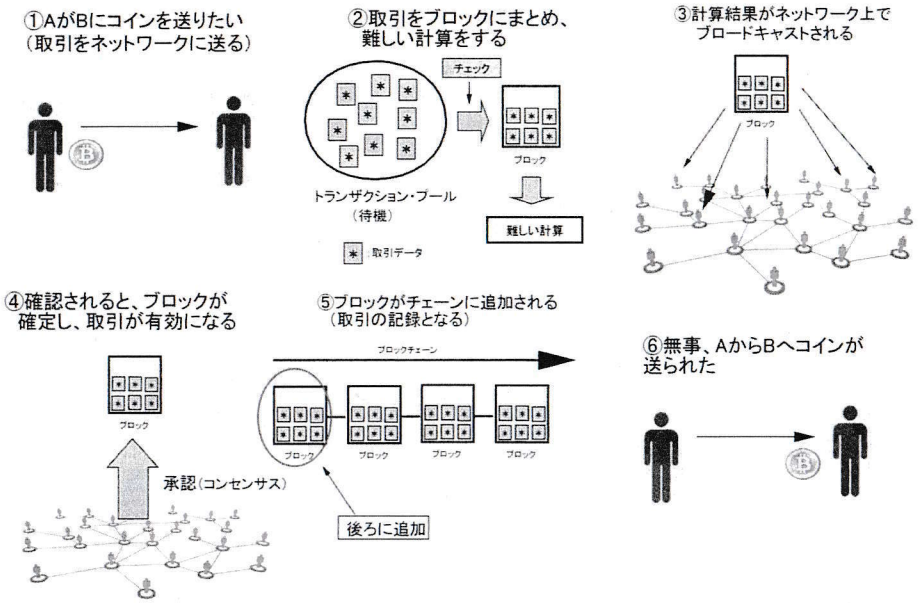
ここまでのビットコインの取引成立までの仕組みをもう一度振り返ってみておくこととしよう（図5）。

まず、AがBにビットコインを送りたい場合には、A→Bの取引をネットワークに送る。各取引は、ネット上の「トランザクション・プール」と呼ばれる場所で待機している。マイナーは、トランザクション・プールの中から、自分が新たなブロックを作るための大量の取引を集めてきて、自分の作るブロックの中に入れる。その際には、同じコインの二重使用が行われていないか、残高の不足している参加者がいないか、などのチェックを行ったうえで取引データを自分のブロックに入れる。マイナーは、自分のブロックを圧縮したハッシュ値が「一定以上の数のゼロ」（例えばゼロが一二個など）が並ぶようにするようなナンス値を膨大な計算作業によって求める。

すべてのマイナーが一斉にマイニングを行い、答えを見つけたマイナーは計算結果を「ブロードキャスト」という方法によって、ネットワーク上の他の参加者に広く通知する。そして、計算結果の通知を受けたネットワーク上の参加者は、その答えが正しいかどうかを検証する（通知されたナンスを入れて計算してみたハッシュ値が、条件を満たしていることを確認するだけであるため、検証は容易に行うことができる）。

この確認作業ができると、このブロックが承認されたことになり、新たなブロックチェーンが従来のブロックの連なりの最後尾に追加されることになる。これにより、ブロックチェーンが確定し、取引が有効になるため、AからBへのビットコインの受渡しが無事に行われたことになるのである。

図5　ビットコインの取引成立までの仕組み



3 安全性確保に不可欠

初めてビットコインの仕組みを学ぶ際に、上記のように「複雑な計算をすると通貨がもらえる」という点が、なかなか理解しにくい点であるものと思われる。通常、通貨は何らかの対価を伴って発行されたり、支払われたりするためである。

ビットコインが「計算の実行による通貨の発行」という不思議な仕組みをとっているのには、理由がある。それは、ビットコインの安全な取引を確保するうえで、このプルーフ・オブ・ワークが必要不可欠な作業となっているためである。誰かがこの計算を行って、一定期間ごとに「取引の承認」を行っていかない限り、ビットコインのブロックチェーンは先に延びて行かない。その場合、ビットコインの安全性は確保されず、たえず偽造や二重使用のリスクに晒されることになる。したがって、この重要な作業を自発的な無償でのボランティア活動に任せておくことはできず、ビットコインの安全性を確保するためには、二四時間三六五日のいつでも確実にマイニングが行われるようにしておくことが必要である。そのために、計算作業に対しては、リワードの付与という経済的インセンティブが与えられることになっている。

すなわち、ビットコインでは、マイニングに対する報酬を求めて、各参加者が利己的に行動することが、全体としては、ビットコインのシステムを正しく機能させ、全員の利益になるという巧妙な仕組みとなっているのである。

ビットコインがこうした計算処理による取引の承認という仕組みを取っている点は、前述したP2P型ネットワークを採っている点とも深く関与している。他のシステムのようなクライアント・サーバー型ネットワークであれば、中央で管理を行うサーバーが取引を承認すれば済むため、こうした全員参加型の取引認証の仕組みは必要ない。中央でのコントロールをなくした「分散型のシステム」であるからこそ、こうした複雑な取引承認の仕組みが必要となっているのである。

こうした仕組みの下で、マイナー（採掘者）たちは、新たなコインという報酬を得るために、二四時間三六五日にわたり、せっせと大量のコンピュータを動かして複雑な計算を行っている。それによって、ビットコインの安全性が確保され、ブロックチェーンの仕組みが維持されている。すなわち、①ビットコインの安全性、②マイニング、③新規通貨の発行、の三つは、密接に関連したワンセットのメカニズムとなっているのである。

以上、今回は、ビットコインの概要と仕組みについて解説を加えた。次回は、ビットコインの問題点について論ずることとする。