

仮想通貨は幻想通貨？

ビットコインの抱える課題・問題点

はじめに

前回、ビットコインの概要と仕組みについて説明した。すなわち、ビットコインでは、P2P型ネットワークやブロックチェーンといった仕組みを採用しており、「ブルーフ・オブ・ワーク」という複雑な計算をすることにより、一定時間ごとに取引を承認している。そして、

の閉鎖により、マウントゴックスにビットコインを預けていた投資家たちは、一切の払い戻しを受けることができなくなり、大騒ぎとなった。

当初、この原因は、外部からのハッキングによって、同社が顧客から預かっていたビットコインが大量に消失したためであるとされた。その被害額は、当時のレートで四七〇億円にものぼる巨額なものであった。その後、取引所の社長がその多くを横領していたことが分かり、業務上横領の罪で逮捕された。

この事件については、「これは一つの取引所の管理に問題があったということであり、ビットコインそのものが悪い訳ではない」としてビットコインを擁護する意見が多かった。しかし、最大手の取引所の突然の閉鎖というこの事件は、ビットコインに対するイメージを大きく低下させ、その信頼性を揺るがすことになった。

そして、仮想通貨の盗難・流出事件は、これで終わった訳ではなかった。たとえば、二〇一六年八月には香港の仮想通貨

なかじま、まろし 金融学者。一橋大学法学部を卒業後、日本銀行に入行。現在は国際社会政策研究センターに在籍。主な著書に『入門 企業価値論』(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権』(二〇一八年、新潮社) など多数。

中島真志

世界 SEKAI 2018.7

その計算に成功した人には、報酬(リワード)として新たなビットコインを付与する「マイニング」という仕組みが導入されており、こうしたいくつかの仕掛けを組み合わせることで、通貨の安全性を確保しているのである。

ビットコインについては、わが国では「通貨の革命である」とか、「夢の通貨」や「未来の通貨」として、バラ色の未来

取引所「ビットフイネックス」で、外部からの不正アクセスにより、七五億円相当のビットコインが盗難にあった。また、二〇一七年二月には、韓国の仮想通貨取引所である「ユービット」がハッキングを受け、六〇億円相当のビットコインが流出している。同社は、即刻取引所を閉鎖するとともに、破産を申請している。そして、今年一月には、わが国で「コインチェック事件」が発生している。これは、コインチェック取引所がハッキングを受け、NEM(ネム)という仮想通貨が五八〇億円分流出したものである。この被害額は、仮想通貨の盗難被害としては過去最大であり、「史上最大のハッキング」とも呼ばれている。さらに、コインチェック事件の直後にも、イタリアの「ビットグレイル」という取引所で、NANO(ナノ)という仮想通貨約二〇〇億円が不正に流出するという事件が発生している(図表1)。

ハッキングなどの攻撃を受けた仮想通貨取引所からの仮想通貨の流出事件は、世界的にみると月に一回程度は発生して

が語られることが多い。しかし一方で、「円や米ドルなどの法定通貨を脅かすような存在にはならない」「邪悪なものである」「金融取引には使えない」といった慎重な見方もあるのも事実である。

シリーズの二回目となる今回は、こうしたビットコインの抱えている課題や問題点に焦点をあててみていくこととする。

1 頻繁に盗難・流出する仮想通貨

ビットコインをはじめとする仮想通貨の問題点の一つは、仮想通貨取引所(仮想通貨取引業者)がときどきハッキングを受けて、利用者が預けておいた仮想通貨が、盗まれたりなくなったりすることである。

最初こうした事件を起こしたのは、東京所在のビットコイン取引所であった「マウントゴックス」である。マウントゴックスでは、二〇一四年二月に突然、すべての取引を中止し、サイトを閉鎖した。当時、同社は、世界最大手のビットコイン取引所であり、全世界のビットコイン取引の七割以上を扱っていた。突然

いるとされており、かなり頻繁に起きているのが実態である。これらの盗難や流出の事件では、仮想通貨自体が偽造されたり、二重使用されたりした訳ではなく、ブロックチェーンなどビットコインを支える仕組みが破られたものではない。しかし、いくら「ビットコインそのものに問題がある訳ではない」と言っても、仮想通貨を「通貨」(ないしそれと同等なもの)として流通させるのであれば、その保管や流通の仕組みなども含めた広い意味での「仮想通貨の取引システム全体」として、高い信頼性が求められるのではないだろうか。銀行に預けてある預金や証券会社に預けてある株式が、「ときどき盗まれたり、なくなったりします」というのでは、こうした金融取引を安心して行うことはできない。銀行や証券会社が人々の高い信頼を得て機能しているのは、保管や流通も含めた全体としての管理システムがしっかりと整備されているからである。コインチェック事件では、たつた一つのウォレットに巨額のコインをまとめて入れたうえで、インターネッ

図表1 仮想通貨の主な盗難・流出事件

取引所	所在地	発症時期	流出した仮想通貨	被害額	事件後
マウントゴックス	日本	2014年2月	ビットコイン	470億円	破産申請
ビットコイン・ジャパン	香港	2016年8月	ビットコイン	75億円	全額全額償
ユービット	韓国	2017年12月	ビットコイン	60億円	破産申請
コインチェック	日本	2018年1月	NEM (ネム)	580億円	全額全額償
ビットコイン・ワールド	イタリア	2018年2月	NANO (ナノ)	200億円	破産申請

出所：筆者作成

トにつないだままの状態を保管するなど、かなり杜撰な管理が行われていたことが明らかになっており、仮想通貨事業者の安全性確保は、まだその域には達していないといえるだろう。

型的な事例が「シルクロード事件」である。シルクロード (Silk Road) というのは、米国で違法薬物などを不正に販売していたウェブサイトである。このウェブサイトでは、マリファナ、LSD、ヘロイン、コカインなどの禁止薬物が手広く販売されていた。

この「闇サイト」(ダーク・ウェブ)において、唯一の決済手段となっていたのがビットコインであった。インターネットでの取引の支払いは、クレジットカードや銀行振込で行うのが一般的であるが、そうすると、違法薬物を誰が買ったのかがすぐに特定されてしまう。これに対して、ビットコインでは、どのアドレスから支払いが行われたかは特定することができ、そのアドレスが誰のものかは特定することができない。こうしたビットコインの持つ高い「匿名性」が悪用されて、違法薬物を売買するための「便利な決済手段」として利用されてしまったのである。

シルクロードは、二〇一一年にサイトが作成され、それに気づいたFBI(米

連邦捜査局)が二〇一三年に運営者を逮捕し、サイトは閉鎖された。この二年余りの売上額は、一、三〇〇億円もの巨額に上ったものとされている。

この事件をきっかけに、「ビットコインは違法取引に使われるもの」というイメージが広まった。欧米の銀行関係者が「ビットコインは終わった」「ビットコインはまともな金融取引には使えない」と言うことが多いのは、こうしたイメージに基づくものとみられる。

なお、シルクロードのサイトが閉鎖されたあとも、「シルクロード二・〇」と呼ばれる、シルクロードを模倣した二連の闇サイトが次々に開設されている。一つの闇サイトを閉鎖すると、また別のサイトが立ち上がるという状況であり、捜査当局とのイタチごっこが続いている。「ビットコインによって違法薬物を販売する」という「ビジネス・モデル」がすでに確立されてしまっているのである。

(2) 日本でも危険ドラッグのネット販売に利用

2 犯罪者が愛用するビットコイン

ビットコインの問題点の一つが、高い匿名性を利用して、犯罪に用いられることが多い点である。

(1) ビットコインで違法薬物を販売：シルクロード事件
ビットコインが犯罪行為に使われた典

ビットコインによって違法薬物を販売するという、こうしたビジネス・モデルは、海外のみにとどまらず、すでにわが国にも入ってきている。

二〇一七年十一月に、危険ドラッグ(服法ハーブ)をインターネットで販売していたとして、川崎市の業者六名が逮捕された。これは、違法なドラッグをビットコイン建てでネット販売していたものであり、まさにシルクロードのやり方(ビジネス・モデル)をそのまま模倣した手法であった。三年間で五、〇〇〇人余りに一〇億円以上の危険ドラッグを売りさばっていたものとされている。

このように、ビットコインの持つ高い匿名性は、マネーロンダリングや違法な取引に利用されやすいというデメリットと紙一重である。ビットコインは、現金と違って持ち運びや物理的な引き渡しの必要がなく、電子的にインターネット上で取引が完結するため、犯罪者側から見ると、「現金よりも格段に便利な手段」ということになる。このため、「犯罪者が愛用するビットコイン」としての性格

を有することになっているのである。

(3) 身代金はビットコインで払え

二〇一七年には、ビットコインと犯罪との結びつきが問題となる別の事件が発生した。「ランサムウェア」という身代金要求型のウイルスが五月に世界中にばらまかれ、身代金として、ビットコインによる支払いが要求されたのである。ランサムウェアは、パソコンやシステムをウイルスに感染させて乗っ取ったうえで、「データやシステムを復旧させなければ、身代金を払え」と要求する犯罪ソフトである。

このときには、日本を含む一五〇カ国以上にウイルスがばらまかれて、世界中の多くのシステムやパソコンがロックされてしまった。感染画面には、「システムを復旧させなければ、三〇〇ドル(約三万円)相当のビットコインを支払え」という要求が表示され、送付先として犯人のビットコインのアドレスが堂々と書かれていた。銀行口座であれば、すぐに本人が特定されてしまうため、犯罪者が

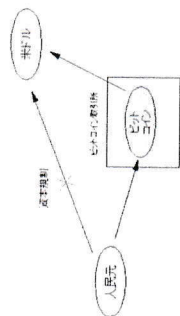
自分の口座番号を指定して送金を指示するなどということは到底ありえない。しかしビットコインの場合には、アドレスを明らかにしても、それが誰のアドレスかは分からないため、自分のアドレスを指定した身代金の要求が可能となっているのである。感染した先には、企業や病院のコンピュータなども含まれており、かなりの感染先がこの身代金を支払ってしまったものとされている。

これまでランサムウェアの犯罪では、身代金の支払いが、犯人側にとって身元が判明したり、逮捕されたりする大きなリスクとなっていたが、ビットコインでは、高い匿名性を活かして、身分を特定されることがなく、安全に身代金を受け取ることが可能となっている。「インターネットを通じて、どこの国からでも素早く送金できる」というビットコインの性格が、グローバルな犯罪集団に悪用されてしまっているのである。

3 規制の抜け穴に使われたビットコイン

犯罪への利用以外にも、ビットコイン

図表4 資本規制の回避とビットコインの利用



出所：筆者作成

ビットコインの大量利用に気が付いた中国政府は、二〇一七年秋に上記の三つの取引所に対し、強制的な閉鎖を命じた。このため、現在、中国国内の取

支配が及ばない金融システムを作りたい」という意図で開発されたものであり、根本には、かなり「反権力、反政府の思想」が根強くあるものと言える。この時期の中国では、ある意味で、このサトシ・ナカモトの「誰にも管理されずに」という思想がまさに実現していたのである。しかし、「キャピタル・フライト」（資本逃避）が利用目的の殆どを占めるというのは、通貨のあり方としていかなるものであろうか。とても正常な姿とは言えないのではないだろうか。

こうした規制をかくぐるためのビッ

取引所ではビットコインの取引ができなくなっている。

4 マイニングの集中化

ビットコインの取引の承認には、マイニング（採掘）が必要となっていることは、前回に述べた。では、ビットコインは誰が採掘しているのであろうか。一般的には、世界中の不特定多数のマイナー（採掘者）たちが手分けして、この作業を負担し、皆でビットコインの仕組みを支えているといったイメージが持たれているようである。しかし、実は、このマイニングについても、少数のマイナーが大きなウェイトを占める寡占構造が発生していることが問題視されている。

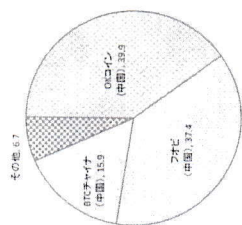
ビットコインのプログラムでは、マイナーが多くなるにしたがって、採掘が段々と困難になるように設定されている。このため、マイニングへの参加者が増えるのにしたがって、ブロックを生成するための「採掘難易度」が急激に上がってきている。したがって、素人がパソコンでできるような世界ではなくっており、

マイニング専用のコンピュータ設備を設けた大規模な「マイニング・ファーム」（組織化された採掘集団）が大きな役割を果たすようになっている。

図表5は、世界のマイナーのシェアをみたものであるが、上位の二三社で約八〇%のシェアを占めており、かなりの寡占化が進んでいることが見て取れる。そして、このうち一〇社が中国のマイニング・ファームであり、中国勢のシェアは合わせて七割にも達している。ほとんど、中国のマイニング・ファームの独壇場になっていると言えるだろう。

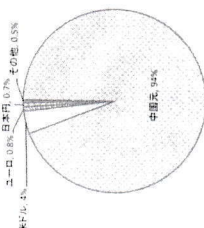
このように中国勢のプレゼンスが大きくなっているのは、先進国などに比べて、中国の電気代が大幅に安いことが大きな要因となっている。マイニングは、大規模なコンピュータ設備を二四時間三六五日稼働させて、大量の電気を消費するため、電気代の安さが立地の大きな要因となる。こうしたマイニング・ファームでは、体育館のような広大な施設に、ビットコインのマイニングに特化した専用のコンピュータを大規模に揃え、報酬（リ

図表2 ビットコイン取引所のシェア（単位：%）



出所：http://data.bitcoincharts.org（2017年8月までの2年間）

図表3 ビットコイン取引の通貨別シェア



出所：http://data.bitcoincharts.org（2017年8月までの2年間）

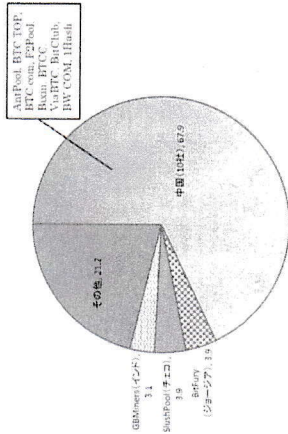
別シェアをみても、中国人民元による取引が、やはり九四%と圧倒的なウェイトを占めている（図表3）。この期間には、米ドルは四%、ユーロや円はそれぞれ一%未満のウェイトしかなかったのであ

設けるなどの厳しい資本規制を敷いて、資本の国外流出を防止した。

こうした厳しい資本規制を回避して骨抜きにする手段として使われたのが、ビットコインだったのである。ビットコインは、資本規制の対象には含まれていなかったことから、中国の富裕層は、人民元をいったんビットコインに換え、たうえで、あとでこのビットコインを必要に応じて米ドルなどの外貨に換えるという動きに出たのである（図表4）。つまり、この時期には、世界中のビットコインの九割以上が、中国当局の資本規制を回避し、形骸化するための手段として使われていたことになる。

ビットコインの発明者であるサトシ・ナカモトは、「誰にも管理されずに、自由に世界中に送金できるようにしたい」として、ビットコインを作ったものときれている。これは、一見すると素晴らしい発想のようにみえるが、ここでいう「誰にも」とは、通貨を管理する立場にある政府や中央銀行のことを意味している。つまり、これは換言すれば「政府の

図表5 世界のマイナーシェア



出所: 2017年8月現在 (注) https://btc.com/stats/pool

ワード)を目当てに巨額の投資を行って、大々的にマイニングを実施している。

今現在も、一〇分に一回のペースで、ビットコインのブロックが作られ続けている。そして、マイニングに成功したマイナーには、リワードとして一〇分ごとに二・五BTC(五月下旬のレートで約一〇〇万円)ずつのビットコインが付与されているが、この新規発行されるコインの七割は、中国勢が手に入れているのである。こうした状態は、ビットコイン業界内における発言力が中国の一部のマイ

あると言えるだろう。しかもこのマイニング用の電力消費量は、毎月増加の一途にあり、さらに増え続けている。

ビットコインのマイニングのためにマイナーが行っている計算は、「ハッシュ値」という新たなブロックを作るための使い捨ての数値を計算することである。つまり、それ自体にはまったく意味のない計算を行うために、マイニングのためのコンピュータを二四時間三六五日にわたってフル稼働させているのであり、人類にとって何の役にも立たない無駄な計算に、これほど膨大な電力を使ってしまうてよいのかということは当然、問題になりうるだろう。これは、ある意味で大量の電力の「無駄遣い」であり、「浪費」であると言えるのではないだろうか。

マイニングの七割を世界最大の石炭消費国である中国が占めているという事実からすると、ビットコインは、環境問題にも深刻な影響を与えているものとみられる。つまり、「ビットコインは地球にやさしくない」のである。このまま、ビットコインのマイニング競争が加熱して

ナーに集中していることも意味しており、「マイニングの集中化」として、関係者の間でも問題視されている。

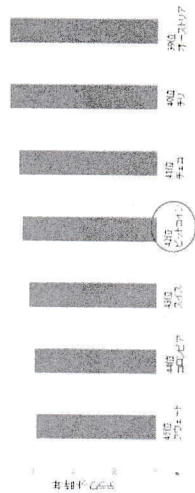
サトシ・ナカモトの設計思想では、幅広い参加者がマイニングを行い、みんなが協力してビットコインの仕組みを支え、報酬としての新規コインを、みんなで少しずつ平等に受け取っていくというものであったはずである。しかし、現状は、こうした設計思想からは大きくかけ離れて、一部の採掘集団のみが新規発行されたコインを集中的に受け取るという状態になっている。この面でも、サトシ・ナカモトの描いていたユートピア的な世界とは程遠い状況になっているのである。

大量の電力を浪費するマイニング

前述したように、マイニングを行うために、マイナーは大量のコンピュータを二四時間三六五日にわたって稼働させている。実は、このために世界中で膨大な電力が消費されているのである。

ビットコインのマイニングに使われている電力を国としてカウントすると、世

図表6 国別の電力消費量



出所: BitcoinEnergyConsumption.com
(注1) ビットコインのマイニング用の電力を含めて、国としてカウント
(注2) 2018年5月時点

界で四二番目の電力消費国の位置づけにある(図表6)。これは、スウェーデン、デンマーク、アイスランドなどの電力使用量を凌いでいることを意味しており、東京都内のすべての世帯の電力消費量の約二倍にもあたるものとされている。すでに欧州の中規模国において国民全体が使う電力の総量を上回る電力が、ビットコインのマイニングのために消費されているのであり、「常軌を逸した電力消費量」で

いけば、環境破壊へのインパクトはさらに強まっていく可能性が高いものとみられる。こうした面からも、ビットコインの仕組みの中長期的な「サステナビリティ」(持続可能性)には疑問の余地があるものと言えよう。

おわりに

ビットコインは、「夢の通貨」としてもてはやされることが多いが、上記のように、その利用状況や仕組みなどについて深く調べていくと、いろいろな面で問題点や課題があることが浮き彫りとなってくる。

第一に、仮想通貨取引所からビットコインなどの仮想通貨が盗難・流出する事件がかなり頻繁に発生しており、取引システム全体としての保管や流通には、問題が少なくないことである。

第二に、高い匿名性を有することから、違法薬物の販売やランサムウェアなどの犯罪行為に使われるケースが多くみられており、「犯罪者が愛用するビットコイン」になってしまっていることである。

第三に、ビットコインは、もともと「誰からも管理されない」ことを目的に作られたこともあって、政府や中央銀行などの規制(資本規制など)をかいくぐるための脱法的な手段として使われる可能性があることである。中国で、それが実際に現実のものとなっていたことは、上記でみたとおりである。

第四に、少数のマイナーが大きなウェイトを占める寡占構造が発生していることであり、マイニングによるリワードがこれらの少数の業者によって、独り占めされる状態となっていることである。

第五に、マイニングを行うために大量の電力が消費されており、こうした電力の浪費が長期的に持続可能かどうかには、疑問符が付くことである。

以上、今回は、ビットコインの課題や問題点について考察を加えた。次回は、ビットコインの今後の展望について論ずることとする。