

仮想通貨（暗号資産）の動きと今後の展望

岩下 直行 ●京都大学公共政策大学院教授

2018年に日本で起こった多額の仮想通貨盗難事件は、交換業者の不十分な管理体制を浮き彫りにし、業界の勢いを削いだ。法改正や事業者の取り組みにより、利用者保護の体制を早急に敷くべきである。

■仮想通貨（暗号資産）の価格は大暴落

2018年は、仮想通貨の価格が大暴落した年であった（資料1-4-3）。

2017年の仮想通貨の相場の急上昇は、世界的な注目を集めた。ビットコインの価格は、2017年12月には、年初の20倍にあたる2万ドル/BTCにまで上昇していた。この急騰に、主要先進国の中央銀行や財務省の高官からは、相次いで警鐘が鳴らされていた。

明けて2018年1月、仮想通貨の市況は調整局面に入った。ビットコインの価格は、1月18日に1万ドルを割るまで下落し、そこから乱高下を繰り返した。しかし、これは短期間の相場上昇に伴う自然な調整であり、引き続き強気の相場観を維持する市場関係者は多かった。

こうした状況に冷水を浴びせたのは、日本発の仮想通貨盗難事件であった。国内最大手のコインチェックが顧客から預かっていた時価580億円相当の仮想通貨NEMの全額が盗まれてしまったのである。コインチェックは、セキュリティ対策が不十分であったことを認め顧客に損失を補償したが、長期間の営業停止を余儀なくされ、2度にわたる金融庁からの業務改善命令を受けることとなった。その事件が大きく報じられると、ビットコインは再び下落し、4月以降は、1万ドルを回復

することはなかった。

ビットコイン価格は、6月に6000ドルまで低下した後、11月中旬まで6000～8000ドルの範囲で比較的安定していた。しかし、11月下旬から12月上旬にかけて再び急落し、3500ドルを切る水準まで低下した。実に、1年前に記録した最高値の1/6にまで下落したのだ。

■仮想通貨から暗号資産に

この相場乱高下の中、2018年3月のG20ブエノスアイレス・サミットでは、それまでの「仮想通貨」という呼称を改め、「暗号資産（クリプトアセット）」という名称が共同声明に採用された。6月に開催されたG7シャルルボワ・サミットの声明でも、同じ表現が用いられている。一連の国際会議では、ビットコインなどが通貨としての安定性を欠き、投機対象となっていることへの懸念が表明され、その特性に合わせて呼称も変更すべきとされた。これを受けて、国内でも、2018年12月、金融庁が、仮想通貨ではなく「暗号資産」という呼称に統一すると発表した。

■ICOの増加と沈静化、その規制を巡る論議

2017年の仮想通貨の高騰は、ビットコインへ

資料 1-4-3 ビットコイン価格の推移（2017～2018 年）



出典：coinmarketcap.com

の投機だけでは説明できない。2017年初から年末にかけてビットコインの価格が20倍になるとともに、仮想通貨全体の流通総額は50倍近くに増加しているからだ。これは、ビットコイン以外の仮想通貨がビットコイン以上に高騰したことを意味している。その原動力となったのは、ICO（企業が独自にトークンと呼ばれる仮想通貨を新規に売り出して資金調達を行うこと）であった。

2017年には66億ドルに達するICOが発行され、2018年にはその金額が200億ドルに膨れ上がった。それらの多くは取引所に上場されると大きく値上がりして転売された。しかし、こうして集められた資金が、新たな技術開発やブロックチェーン技術の発達を促したかという点、そうはいえない。IPOやベンチャーキャピタルによる資金調達とは異なり、ICOの発行は仮想通貨同士の交換で、株式のような議決権や配当金はなく、借入金のような返済義務も利払いもない。そのため、ICOで調達した資金は返済する必要のないものと考えられ、誠実な製品開発やビジネス化のた

めに有効活用されることは少なかった。巨額の資金を集めたICOプロジェクトの多くは、さしたる活動もしないままに消滅してしまっている。

こうした実態を反映して、取引所で転売されたICOトークンは大きく値下がりし、そのほとんどが発行時の価格を大幅に下回った状態が続いている。2017年から仮想通貨の高騰を演出したICOというエンジンは、2018年の半ばでその力を失ったのだ。

日本では、2017年から仮想通貨交換業者の登録制度が開始されており、ICOの発行を行うこと自体が規制されてきた。このため、テックビューロが実施したCOMSA（2018年12月現在ではトークンの価格は発行時の1/20に下落している）以外は、国内ではICOが実施された事例はない。ICOを計画しながら実施できなかった企業からは不満の声が聞かれるものの、結果としてみれば、大規模な投資家の損失を生まなかったという意味で、相場が急騰して投資家が過剰な値上がり期待を持っていた時期にICOが実質的に規制されてい

たことは、社会的には好ましい結果になったということができる。

なお、ICOという手法にながしかのイノベーションを促進する意味があるとの意見もあり、十分に投資家保護の仕組みを整備したうえであれば、今後、国内でもICOを解禁することはありうる。そのための規制のあり方が、金融庁の設置した研究会で議論された。

■相次いだ交換業者へのサイバー攻撃とその帰結

2018年前半の相場下落の原因と名指しされたコインチェック事件はなぜ起こったのだろうか。顧客の大事な資産である仮想通貨を預かる立場として、コインチェックの管理体制はまったく不十分であった。コインチェックは、26万人の顧客から預かったNEMをたった1つのアカウントで管理していた。そのアカウントから仮想通貨を移転する手続きは、たった1つの秘密鍵によって守られていたにすぎない。暗号を解く秘密鍵は、常時インターネットと接続された状態にあった。この秘密鍵の管理が杜撰であったため、サイバー攻撃を受け、鍵が不正に利用されて、NEMが送金されてしまったのである（資料1-4-4）。

資料1-4-4において、「NC3…」というアドレスは、コインチェック名義のアドレスである。このアドレスに、顧客から預かったNEM 580億円分が保管されていた。他方、「NC4…」というアドレスは、犯人が用意したものである。2018年1月26日の午前0時2分に最初の10 XEMが送金され、その後、20分足らずの間に、523,000,000 XEMが送金された（XEMはNEMの単位）。犯人は、このアドレスからさらに別の複数のアドレスに送金している。午前3時、4時、8時にも、NC3からNC4への不正な送金を行っている。

もちろん、最も糾弾されるべきなのは、この不

正送金を実行した犯人だ。正体不明のこの犯人は、自らが管理することになった580億円分のNEMを、少しずつインターネット上で他の通貨と交換し、資金洗浄を進め、まんまと逃げおおせてしまった。

今回の問題は、コインチェックだけの問題ではなかった。事件をきっかけに実施された金融庁による検査では、ほとんどの仮想通貨交換業者で、管理運営上の重大な問題が指摘され、業務改善命令が出されることになった。そうした是正措置が進められていた最中、2018年9月に、大手交換業者であるテックビューロにおいて、やはりサイバー攻撃により70億円が盗難にあう事件が起きた。テックビューロは事業を売却し、顧客は被害額を補償されたが、相次ぐ盗難事件に業界の信頼は大きく失墜した。

日本は、他国に先駆けて仮想通貨の交換業者を規制する法律を施行し、その登録制度を運用してきた。しかし、それは資金洗浄やテロ資金調達を防止することが主眼であった。現在の仮想通貨法は、交換業者が多額の顧客資産を預かる存在であることを意識した、十分な利用者保護の仕組みを備えていない。法律制定時には想定されていなかった状況が生じている以上、それに対応した法改正を検討する必要があるだろう。業界も、信託や保険といった仕組みを活用して、自主的に被害を限定する取り組みを進めるべきである。また、セキュリティ対策の基準を制定し、情報公開を徹底することにより、利用者の不安の払拭に努める必要がある。今回のような事件が再び起きないように、常にセキュリティ対策を最新のものとする工夫も必要である。こうした対策についても、金融庁の設置した研究会で議論の対象となった。

コインチェック事件で誰もが不思議に思うのは、不正送金されたNEMが犯人のアドレスに送金されていることは確認できるのに、それを取

資料 1-4-4 コインチェック事件における NEM の動き

時刻	金額 (XEM)	送金元	送金先
2018/1/26 8:26	800,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 4:33	1,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 3:35	1,500,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 3:29	92,250,000	NC4C6PSUW5...	NA6JSWNF24Y...
2018/1/26 3:28	100,000,000	NC4C6PSUW5...	NDZVF32WB...
2018/1/26 3:18	100,000,000	NC4C6PSUW5...	NB4QJJCLTZW...
2018/1/26 3:14	100,000,000	NC4C6PSUW5...	NDZZJBH6JZP...
2018/1/26 3:02	750,000	NC4C6PSUW5...	NBKLOYXEIVE...
2018/1/26 3:00	50,000,000	NC4C6PSUW5...	NDODXOWEIZ...
2018/1/26 2:58	50,000,000	NC4C6PSUW5...	NA7SZ75KF6Z...
2018/1/26 2:57	30,000,000	NC4C6PSUW5...	NCTWFIOOVIT...
2018/1/26 0:21	3,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:10	20,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:09	100,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:08	100,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:07	100,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:06	100,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:04	100,000,000	NC3BI3DNMR2...	NC4C6PSUW5...
2018/1/26 0:02	10	NC3BI3DNMR2...	NC4C6PSUW5...

出典：NEM のブロックチェーン情報をもとに筆者作成

り戻すことができないという点である。これがもし、銀行預金であったなら、盗まれた大金がどこかの預金口座にあることがわかった時点で、当局によって差し押さえられ、最終的には盗まれた人に返還されると期待できたであろう。

ビットコインが注目され始めた当初から、その背景に特殊な思想があることが注目されてきた。それは、信頼できる中央機関を決して置かないというポリシーで、「トラストレス」と呼ばれる考え方のことだ。ビットコインは、こうした特徴を持つからこそ、法律や政治体制の違いによる国境の壁をやすやすと越えて、国際的な利用が可能になったと考えられる。

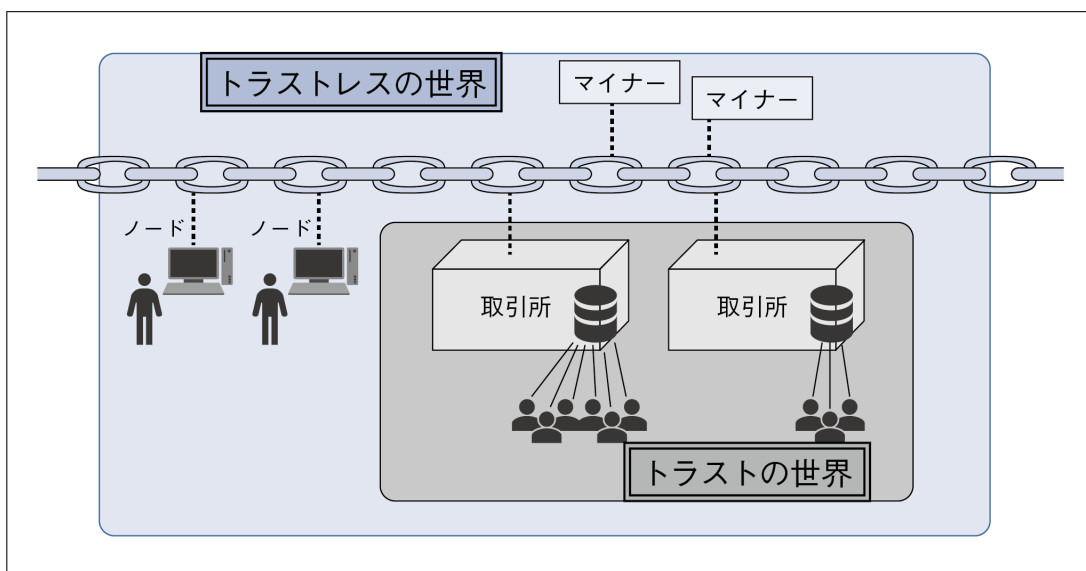
これに対し、信頼できる中央機関を置く従来の仕組みを「トラスト」の世界と呼ぶ。一般の人々は、政府、中央銀行、裁判所といった信頼できる中央機関の存在を前提に構成された世界に住んでいるから、トラストレスの世界は、きわめて特殊な、危なっかしいものに見える。とはいえ、ビットコインの存在は認知され、トラストとトラスト

レスの両者が併存する状況が続いてきた。

たとえば、ビットコインのブロックチェーンに直接接続して取引しているプロの利用者は、トラストレスの世界で生きている。しかし、直接ブロックチェーンに接続することのできない素人の利用者は、取引所にビットコインを預け、取引所に依存してビットコイン取引を行っている。この場合、そうした一般の利用者にとって、取引所こそが「信頼できる第三者」であり、そこにトラストの構造が存在する（資料 1-4-5）。

今回流出した NEM は、トラストレスの世界で盗まれ、資金洗浄された。信頼できる中央機関はなく、国家権力を含め、何者も情報を恣意的に書き換えることはできないという建前だ。今回の NEM の問題をみれば、それが両刃の剣であることがわかる。

仮想通貨という異質な存在を、国家が適切に制御すること、つまり、その利点を生かし、欠点を補うことができるだろうか。この新たな課題に向き合うためには、国際的な規制対応も含め、関係



出典：筆者作成

者が知恵を絞っていくことが必要となるだろう。

■ハッシュ戦争とステーブルコイン疑惑と相場下落

2018年末における世界的な仮想通貨の相場下落の原因と指摘されているのが、ビットコインキャッシュ (BCH) をめぐる「ハッシュ戦争」と、ステーブルコイン (価格安定型仮想通貨)、テザーをめぐる疑惑である。

仮想通貨ビットコインキャッシュは、2017年7月にビットコインから分岐して誕生した仮想通貨だが、これがさらに分裂した際に、採掘業者同士の主導権争いが発生し、相場の下落要因となった。

また、ビットコインに次いで大きな取引金額を持つテザー (USDT) が、その運営の不透明さや疑惑を指摘され、1USDT = \$1.00 のペッグ (固定相場) が維持しにくくなっていることも、大きな重石となった。テザーは、10月中旬以降、ター

ゲットからの乖離を繰り返しており、暗号資産市場の資金が逃げ場を求めて移動を繰り返した結果、市場全体に同時並行的な下落が生じたと考えられる。

本来、暗号資産は金利や配当を生むものではないし、満期金の償還があるわけでもないから、そもそも理論価格を計算することができない。購入時の価格よりも高値で売却できれば売却益が得られるという投機目的で保有されてきたものだ。2018年にはそういう局面はほとんど出現しなかった。本来、まったくキャッシュフローを生まず、安定した相場が立つ理論的背景を持たない暗号資産が、かなりの期間、比較的安定した価格で維持されていたこと自体が、むしろ不自然であった。相場は今後も波乱があるだろうが、再び高騰するシナリオは考えにくい。多くのエコノミストが「暗号資産の本源的価値はゼロ」と主張しているが、冷静にそうした意見に耳を傾けるべき時期に来ているといえるだろう。



1996, 1997, 1998, 1999, 2000...

[インターネット白書ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2019年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<https://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp

©1996-2019 Impress R&D