デジタルプラクティス　Vol.10 No.3(July 2019)

特集号解説論文

暗号資産への脅威と対策 ― ビットコインの社会への展開による変質 ―

岩下 直行[1]

[1]京都大学

本稿では，ビットコインを始めとする暗号資産（仮想通貨）が社会へ展開していく中で，その情報セキュリティへの脅威と対策を概観することで，情報セキュリティ技術の観点から，今後，ブロックチェーン技術が社会から受容されるための条件について考える．サトシ・ナカモトによるビットコインの提案と実装を契機として，暗号資産は一世を風靡したが，現在は相場も下落し，安全性に対する信頼も損なわれた状態にある．個人のプライバシを守るための匿名の決済手段として提案されながら，当初の構想を逸脱してしまったのは，一般の投資家が秘密鍵を管理できないという現実に対応するためであった．その結果，交換業者がサイバー攻撃の犠牲となり，安全性が損なわれる事態を来した．今後，ブロックチェーン技術が社会に受け入れられていくためには，暗号資産が辿った歴史を踏まえて，利用者サイドにおける秘密鍵管理を含めた情報セキュリティ対策の底辺をしっかり固めていく必要があると考えられる．

1. はじめに

2017年に大暴騰して世間から注目を集めたビットコインは，2018年には暴落し，ハイリスクな投機商品という認識が広まった（**図1**）．他方で，ビットコインから派生したブロックチェーン技術は，次世代の最先端技術として注目され，さまざまなパイロット・プロジェクトが進められている．とは言え，現在までのところ，ブロックチェーン技術の大規模な実装が社会に受容された事例は，ビットコインを中心とする暗号資産（仮想通貨）がほぼ唯一の例である．

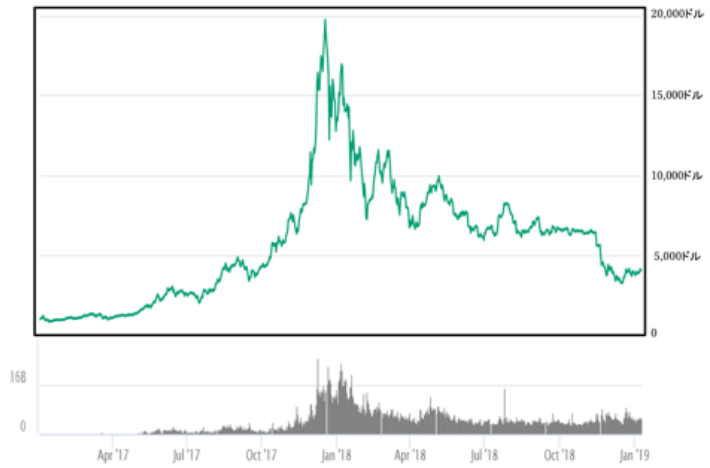

図1　ビットコインの価格の推移（2017～18年）
（出典：coinmarketcap.com）

ブロックチェーン技術は，公開鍵暗号によるディジタル署名とハッシュ関数によるチェイニングという，情報セキュリティ技術の世界ではよく知られた技術によって構築されたものである．そうした技術が，暗号資産への投機という目的とは言え，日本だけで350万人もの利用者を獲得し，ピーク時には数十兆円もの経済価値を持つものとして取引されたという意味では，かつて例を見ない規模で行われた情報セキュリティ技術の社会への展開であったと言えるだろう．

しかし，ビットコインの発展は，バラ色の成功物語ばかりではない．初期の投資家は，きわめて安価に入手したビットコインの価値が上昇することで，経済的な利益を手に入れた．しかし，そうした相場上昇は，ビットコインが金融規制の枠を超えて国際的な匿名の取引が可能であることからもたらされたものであった．その発展は，国際的な資金洗浄やテロ資金の調達に利用され，世界的な金融秩序に混乱をもたらした．

また，相場が上昇した2017年以降の投資家にとっては，相次ぐ交換業者へのサイバー攻撃で資産が奪われ，相場が下落して損失を被ることとなった．情報セキュリティ技術の観点からは，暗号資産というアプリケーションは，そのセキュリティの要諦であるディジタル署名用の秘密鍵を安全に管理することがいかに難しいかを改めて認識させることとなった．

信頼できる第三者が存在しなくても，取引の安全性を高める手段として実装されたPoW（Proof of Work）は，ビットコインの成功の原点であった．ところが，ビットコインの相場の高騰に伴って，PoWを実行すること，つまりビットコインのマイニングを行うことで，高い利益が期待できるようになった．その結果，世界的な資源配分の歪みを生じさせるほどの過剰な設備投資が誘発され，それが地球環境問題を深刻化させるといった副作用が生じた．

ビットコインの発明者であり，初期の開発者であるサトシ・ナカモトは，ビットコインを，インターネット上で見知らぬ同士が匿名のまま金銭的な価値のやり取りができる電子現金として設計した．しかし，ビットコインは，サトシが夢見たであろう世界から逸脱し，当初の構想を実現できていない．その逸脱はどのようにして生じたのか，そしてそれが元に戻ることはあるのだろうか．

本稿では，社会現象にまでなったビットコインやその他の暗号資産の社会への展開を追い，ブロックチェーン技術が社会から受容されるための重要な要点について考える．

2. ビットコイン論文が想定していた世界とその前提条件

サトシ・ナカモトという人物が実在するという証拠はない．そもそも特定の個人の名前なのかどうかすら分からないし，その正体は謎に包まれている．しかし，その謎は脇に置いておこう．彼の残した論文[1]を見る限り，その筆者が現在のようなビットコインを思い描いていたとは考えにくい．

ビットコイン論文の題名は「新しい電子現金システムの提案」であった．インターネットのようなオープンなネットワーク上のディジタルデータを利用して，まるで現金のように送金や支払手段に利用でき，かつその取引の匿名性を確保することでプライバシを守る，という電子現金の構想については，1980年代からさまざまな提案があった[2] [3]．その研究は暗号技術の応用として現在まで引き継がれている．そうした研究を源流として，世界各国でさまざまな電子決済手段が提案され，利用されるようになり，わが国では交通系・流通系電子マネーが広く普及するに至った．

しかし，そうした実用的な電子マネーは，多くは発行体の負債として当局に規制され，取引の匿名性もなかった．それは，サトシにとっては理想からほど遠いものであったのだろう．彼は，信頼できる第三者の仲介がなく，匿名での取引が可能であるという前提条件の電子的な支払い手段として，ビットコインを提案した．

とはいえ，技術的にはビットコインは，既知の2つのプロジェクトを組み合わせたものにすぎない．ひとつはSurety.comの電子公証サービス [4] [5] [6]，もうひとつはhashcash[7]というプロジェクトだ．前者からは，ハッシュ関数のリンクを利用したデータの改竄困難化の手法をそのまま流用し，後者からはPoWの考え方を取り入れることで生まれたのがビットコインである．ビットコインは，第三者が仲介しなくとも，インターネット上で匿名での送金が可能であることをもって，電子現金を名乗ったのである．

ここではその原理を細かく解説はしないが，重要なのは，ビットコインを支える発行会社のような組織は存在しないということだ．基本的に，ビットコインのシステムを支えているのは，その趣旨に賛同し，あるいはそこから利益を得ようしている個人が供出する計算機資源であった．そこには明示された契約も，法人化の仕組みもなく，コード（コンピュータのプログラム）だけが存在する．そのコードもまた，自主的に集まった技術者が，相互にレビューしつつ，自由に書き換えることができる．そのコードが，重要な経済的な帰結（たとえば，暗号資産の価格変動や，業者間の主導権争いの決着）を生じさせる．このような，「コードが支配する世界」が到来することは，インターネットが出現した当初から予想はされていた．しかし，それが予想されたよりも早く，数十兆円規模の暗号資産という形で実現することになったことは，人々を驚かせるのに十分であった．

3. ビットコインの黎明期における用途

2009年1月3日に，サトシ本人によって書かれた最初のコードから，ビットコインの最初のブロックが生成された．このプロジェクトを開始した当初のビットコインは，サトシが思い描いている方向に動いているように見えた．基本的に，ビットコインに関心を持っているのは一部のgeekだけだった．彼らは，ビットコインの趣旨に賛同し，自らのPCの計算機資源を供出してマイニングを行い，ビットコインの取引を支えたのである．ビットコインの取引のために必要となる電子署名の秘密鍵は，各ユーザが安全に保管し，自らがその責任を負う構造であった．

ビットコインは一部が法定通貨と交換されるようになり，それなりの相場は成立したが，交換価格はまだとても安かった．基本的にはインターネット上での取引の決済に利用され，とりわけ，麻薬や武器売買などのアンダーグラウンドな取引に利用されることが多かったと言われている．ある程度取引が拡大した2012年頃でも，参加者はgeek限定であり，相場は1BTC=$10前後であった．当時の取引の様子は，後にSilk Road事件として有名になったある裏取引サイトを巡る記事に生き生きと描写されている[8]．その記事の中に，「リバタリアンの王国」という表現があることは示唆的である．政府の介入を嫌い，自己決定権を主張するリバタリアンにとって，ビットコインはある種の福音に見えたことだろう．サトシが理想としたのは，こういう世界であったのではないかと思う．

4. ビットコインの普及期におけるサトシの想定していた世界からの逸脱

4.1 最初の逸脱：素人投資家の参入と交換業者の発展

しかし，こうした牧歌的な時代はすぐ過ぎ去り，2013年になると，ビットコインの市場は大きく変化し始める．3月28日のキプロス危機では，取引が停止された銀行経由の国際送金に代わって，ビットコインを利用する需要が高まり，相場は10倍に急騰した．こうした状態までは，サトシは想定していたように考えられる．

メディア報道も加熱し，多くの素人投資家がビットコインを買いに集まってきた．そこで一般的になったのが，暗号資産の交換業者である．彼らの仕事は2つあった．法定通貨と暗号資産を交換すること，交換した暗号資産を預かることだ．試行錯誤を経て，現在では，暗号資産を交換業者から購入すると，交換業者の保有するアカウントに保管され，投資家の氏名と残高が，取引所のRDBに記録されるシステムが一般的となっている．素人の投資家は，安全に秘密鍵を管理，運用することができないから，これは仕方のない処置だった．しかし，この処置は，サトシが描いた世界からの最初の逸脱であった．

4.2 第2の逸脱：交換業者へのサイバー攻撃

大勢の素人の投資家から大量の暗号資産を預かる交換業者が誕生し，暗号資産の価格高騰もあって，交換業者が日々取り扱う金額はどんどん高額になっていった．そのような肥大化した交換業者が，サイバー攻撃の犠牲となった．暗号資産のビジネスはまだ生まれて時間が経っておらず，交換業者はベンチャー企業ばかりであり，残念ながらそのリスク管理の水準は高くはなかった．世界各国の交換業者がサイバー攻撃のターゲットとされた．

攻撃者の側からみれば，攻撃対象のシステムの多くはクラウド上に構築され，秘密鍵を含めてリモート運用されているものも多い．交換業者を狙ってサイバー攻撃を仕掛ければ，その秘密鍵を不正に利用して巨額の暗号資産を自らの管理するアカウントに移動させることができるかもし

れない．いったん移動させてしまえば，匿名で送金できるという暗号資産の特徴を悪用して，資金洗浄も自由自在である．その意味で，攻撃者にとって交換業者のシステムを狙うという行為は，きわめて合理的な判断であったのだ．

交換業者がサイバー攻撃を受けると，顧客から預かった暗号資産が不正に流出してしまう．特に，日本では大規模な不正流出事件が相次ぎ，2018年にはコインチェック社が580億円，テックビューロ社が70億円の盗難被害を受けることとなった．両社は顧客に損失を補償したため，消費者被害には繋がらなかったが，攻撃者は特定されず，流出した暗号資産も取り戻されていない．このような犯罪が横行することは，サトシの想定には含まれていなかったことだろう．

ここで，2018年1月に発生したコインチェック事件を詳しく見てみよう．この事件では，国内最大手の交換業者コインチェック社が26万人の顧客から時価580億円相当の暗号資産NEMを預かっていながら，攻撃者にその全額を盗まれてしまった．同社は非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．

金融庁の検査で明らかになったのは，顧客の資産を預かる立場として，コインチェック社の体制はまったく不十分なことであった．コインチェック社は，26万人分の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暗号資産を移転する手続きは，たった1つの暗号鍵によって守られていたにすぎない．その秘密鍵は，常時インターネットと接続された状態にあった．この暗号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（**表1**）．

表1　コインチェック事件におけるNEMの動き（出典：NEMのブロックチェーン情報をもとに筆者作成）

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	NDDZVF32WB
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	NBKLOYXFIVF
2018/1/26 3:00	50,000,000	NC4C6PSUW5	NDODXOWFIZ
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

表1において，「NC3...」というアドレスは，コインチェック社の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NEM580億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．1月26日の午前0時2分に最初の10XEMが送金され，

その後，20分足らずの間に，523,000,000XEMが送金された．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．さらに，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．

今回の事件をきっかけに実施された金融庁による検査では，日本国内のほとんどの交換業者において，組織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．また，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社において，やはりサイバー攻撃により70億円が盗難される事件が起きた．テックビューロ社は事業を売却し，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．

こうした事件で誰もが不思議に思うのは，不正送金された暗号資産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分かった時点で，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易々と越えて，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．我々は，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，ビットコインのノードとして直接接続しているgeekな利用者は，トラストレスの世界で生きている．しかし，自らがノード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（**図2**）．

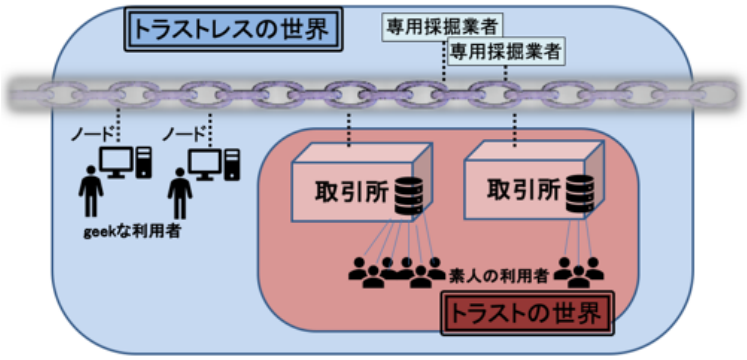

図2　「トラストレスの中のトラスト」構造の問題

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分かる．

4.3　第3の逸脱：専用採掘業者の発展

ビットコインをマイニングする専用のマシンが開発され，マイニングを専ら専門採掘業者（いわゆるマイナーと呼ばれるマイニング事業者）が担うことになったこともまた，サトシの描いた世界からの逸脱である．サトシが想定していたのは，自らのPCを供出する多数のビットコインユーザがいて，彼らが通常のCPUでマイニングに参加し，たまたま運のよい人がブロックの生成に成功して報酬を受け取る世界であっただろう．しかし，GPUやASICで誰よりも早くマイニング競争に勝つことを狙うマイナーが次々に現れると，ビットコインの世界は少数のマイナーに支配される構図が表れてくる．また，マイニングが大量の電力を消費し，地球環境問題を悪化させかねない状態に陥っていくことも，サトシにとって想定外のことだっただろう．

ビットコインにおけるマイニングとは，ハッシュ関数を使って時系列のデータをリンクさせ，（事実上）書き換えることが困難なデータの連鎖を作り出す作業のことである．ビットコインが何がしかの価値をやり取りする手段と位置付けられたのは，インターネットというオープンな環境に置かれながら，データが改竄困難という特徴を持っていたからで，これが最大のメリットと考えられている．その技術を電子現金に使えばビットコインになるが，他の用途にも使えるのではないかということで，ブロックチェーン技術やDLT（Distributed Ledger Technology）といった言葉が使われるようになった．

ビットコインのデータのリンクの部分の作り方，つまり，マイナーによるマイニング作業を具体的に見てみよう．まず，ビットコインの次のブロックを生成しようとするマイナーは，まだ承認されていないビットコインの取引を検証するところから始める．各取引に利用された電子署名が正当なものか，過去の取引履歴から計算して，取引後のビットコインの残高がマイナスになることがないかなど，ビットコインの取引環境を監視する役割を果たす．そして問題ないと判断された取引を2つずつ組み合わせてハッシュ値を作り，そのハッシュ値同士を組み合わせてハッシュ値を作る．こうしたトーナメント表のような作業を繰り返して，ルート・ハッシュ値を計算する．ここまでの作業負担はさして重くはない．

そして，前のブロックから得られたハッシュ値と，今回得られたルート・ハッシュ値，それにnonceと呼ばれる一種の乱数を組み合わせて，新しいハッシュ値を作る．このハッシュ値が，その時に決まっている条件（たとえば，冒頭20ビットが0）を満たしていれば，それでマイニングは成功である．マイナーは，12.5BTCのマイニング報酬（新規に発行されたビットコイン）を受け取ることができる．

しかし，実際にはそんなにうまくは進まない．生成したハッシュ値は，基本的にすべてのビットがランダムに設定されるから，どのビットも0となる可能性は1/2と考えることができる．このため，$(1/2)^{20}$ の確率でしか，この条件は満たされないのだ．これは，約0.0001%（1/1,048,576）の確率でしかない．そこで，マイナーは，nonceを少し変えてみる．するとハッシュ値はまったく違ったものとなるが，それが条件を満たす確率も約0.0001%である．マイナーが1人しかいない場合，nonceを変えながらこの条件を満たすハッシュ値が見つかる確率が50%になるためには，試行を約72万回行わなければならない．これが，膨大なハッシュ値の計算を行わなければならない所以である（**図3**）．このため，世界中のマイナーが，SHA-256のハッシュ関数の計算のみに特化したASICを多数搭載したマイニングマシンをマイニング工場に設置して，マイニング報酬を求めて，約10分おきの競争を繰り広げているのだ（**図4**）．

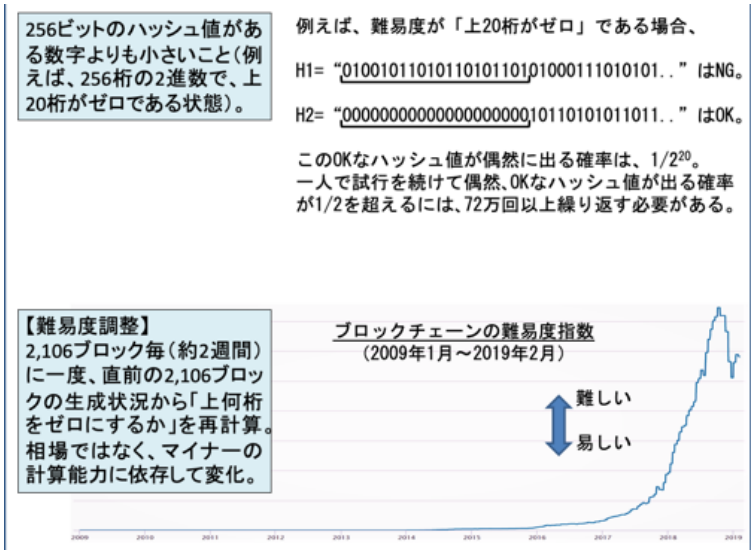

図3　ハッシュ値の満たすべき条件と難易度調整

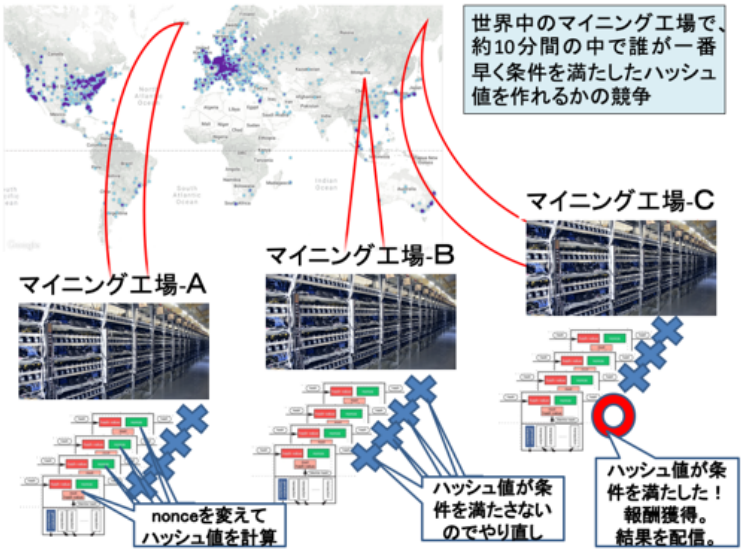

図4　競争的マイニングのイメージ図

マイナーは競争相手よりも一瞬でも早くハッシュ値を探索できれば報酬を得ることができる．このため各マイナーは，計算能力を増強して，より早く探索しようとする．その結果，全体の計算能力が高まると，10分よりも短い時間で探索ができてしまうようになる．その場合，ハッシュ値が満たすべき条件が難しくなる仕組みがビットコインには組み込まれている．冒頭20桁ではなくて，21桁，22桁とゼロとなるべき桁数が増えていく．これが競争的マイニングブロック生成を平均的に10分に保つ仕組みである．

マイニングは専用のハードウエアを設置して適切に運用すれば，マイニング報酬の獲得が期待できる．ただし，このマイニング・マシンは大量に電力を消費する．2017年のビットコインの価格高騰の結果，消費電力が急激に増大した．莫大な資金がマイニング産業に投入され，半導体産業のシリコン・サイクルに影響を与えるほどのマイニング・マシンの製造が行われたからである．

この問題を指摘しているサイトDigiconomist.netの推計によれば，マイニングに使用されている電力は，2017年10月頃から上昇率を高め，暗号資産の価格が暴落する中でも，2018年6月頃まで増加を続けた．その結果，1年間換算で約70TWh（テラ・ワット・アワー）に達した（**図5**）．これを国別の消費電力と比較するとオーストリアが最も近い．オーストリア1国が1年間に使用する電力が約70TWhだからである．条件に合うハッシュ値を探索するために費やされたエネルギーは，何か有用なものを生み出すわけではなく，浪費されるだけだ．ビットコインの価格が上昇するということは，この浪費が増大することを意味する．これは，ビットコインの抱える深刻な問題のひとつである．

図5　ビットコイン・マイニングの電力消費量
（出典: Digiconomist.net）

しかも，いったん製造したマイニング・マシンは，ハッシュ関数を高速で計算することに特化した装置であるから，他に転用が効かない．このため，相場が暴落し，マイニング報酬が激減する中でも，マイニング能力は増強され続け，ハッシュ値の探索速度は上がり，それに応じて難易度も難化する．2018年の相場下落の中で，マイニング報酬のドル換算額が下落しても，なかなかマイニング能力は下がらず，消費電力も下がらなかったのは，こうした事情によるものだ．

しかし，2018年11月の相場下落に伴い，マイナーの収益環境が一段と悪化すると，マイニングから撤退する企業が相次いだ．大手マイナーの中でも，採算の悪いマイニング工場を閉鎖する動きが進んだという．その結果，推定消費電力が約40TWhにまで減った．現在のビットコインの相場レベルであれば，当面は消費電力が急増することは考えにくい．Digiconomist.netで1年前に想定されていた悲観的なシナリオでは，2018年末には消費電力は 120TWhを超えるとされていた（**図6**）が，この予測は人類にとって望ましい方向に外れることとなった．

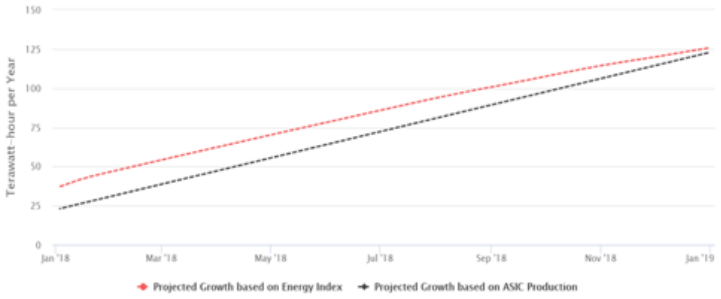

図6　同電力消費量の将来予測推計値（2017年末時点）
（出典: Digiconomist.net）

暗号資産の相場の上がり下がりによって，得をする人も損をする人もいるから，相場がどう動くのが良いかは何とも言えない．しかし，相場の過熱でマイナーが先の見えない資源浪費競争に突入すれば，地球環境問題という形で全人類の不利益となる．その意味で，2017年末に見られたような行き過ぎた相場上昇は望ましくない．今後も，そうした事態に陥るのは避けるべきという理解が共有される必要がある．

4.4　第4の逸脱：アルトコインの増加と51%攻撃

さらに，ビットコインを模したアルトコインが大量に発行され，その時価総額がビットコインを凌駕したこともまた，サトシの描いた世界からの大きな逸脱であった．サトシ論文がビットコインへの51%攻撃を予言していたことは有名だが，それは理論的なもので現実的ではないとしていた．ハッシュ計算能力の51%を占有する者がいたとしても，その人物がビットコインの価値を棄損するような行動をとるはずはない，というのがその理由だった．その論理は，この世の中に暗号資産がビットコインしかなければ正しいが，大小さまざまな暗号資産が混在する世界では，その論理は成り立たない．この結果，実際に51%攻撃による被害が出始めた．これもまた，サトシにとって想定外の事件であっただろう．

2018年5月，Monacoinという暗号資産が攻撃を受け，ロシアの交換業者に1,000万円程度の被害が発生した．その後2週間ほどの間に，Bitcoin Gold，Verge，ZenCashといった暗号資産も類似した攻撃を受け，各々，20億円，2億円，6,000万円程度の被害が発生したと報道されている．

その攻撃方法は微妙に異なっているが，基本的には膨大なハッシュ計算能力を投入してブロックチェーンのマイニングを行い，攻撃者に都合の良いチェーンの分岐（fork）を発生させてそれをチェーンの本流にしてしまうという攻撃方法であった（**図7**）．これらはいずれも，ハッシュ計算能力が攻撃者側に偏った場合に発生すると想定されていた51%攻撃のバリエーションである．

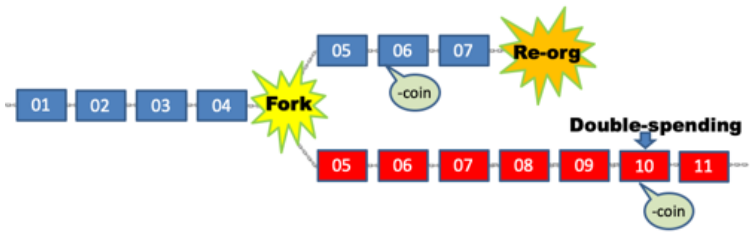

図7　ブロックチェーンに対する51%攻撃の概要

こうした攻撃については，理論的にはその存在が指摘され，攻撃方法の詳細や必要なハッシュ計算能力についても試算が行われていたが，莫大な費用が必要であり，実現性は低いと考えられていた．ところが，ここに来て，相次いで被害が発生している．その対象は，主要な暗号資産（ビットコイン，イーサリアム等）を除く，「非主流派」の暗号資産であった．

こうした攻撃はなぜ実現したのであろうか．1つの原因は，非主流派の暗号資産が高い価値を持つようになったということである．暗号資産の流通総額のシェアを長期時系列でみると，2017年前半まではビットコインが9割前後を占め，それ以外の暗号資産（アルトコイン）はほとんど無価値であった．しかし，2017年後半から，アルトコインが急速に値上がりし，ビットコインのシェアは4割を切る水準となった．

これらの非主流派の暗号資産は，元々マイニングに参加するマイナーの数も少なく，利用しているハッシュ計算能力はあまり大きくはなかった．価格の上昇に伴い難易度調整は行われたものの，ビットコインなどの主流派の暗号資産との計算能力の格差は元々大きかった．今回の攻撃は，この計算能力格差を突いたものであった．攻撃が相次いだ背景としては，計算能力の格差がそのままだったのに比べて，通貨の価格は2017年後半に急上昇した結果，攻撃者側が得られる利益が増大したことが大きい．

こうした非主流派の暗号資産は，多くはビットコインの模倣ではあるが，先行する主流派の暗号資産との差別化を意識して構築されてきた．たとえば，利用するハッシュ関数は，ビットコインが利用するSHA-256とは異なるものが用いられている．同じハッシュ関数を利用すると，ビットコインのマイナーが保有する膨大なハッシュ計算能力によって，容易にマイニング報酬を独占され，ブロックチェーン自体も恣意的に作成されかねない．このため，非主流派の暗号資産は，既存のマイナーにマイニングされにくい特徴を持ったハッシュ関数を利用してきたのだ．

しかし，暗号資産の数が増え，さまざまな主体がマイニングに参入するとともに，ハッシュ計算能力自体が時間貸しされるようになる．たとえば，www.nicehash.comというサイトでは，マイニングのためのハッシュ計算能力をインターネット上で売買している．必要なハッシュ関数ごとに価格が付き，たとえば，SHA−256を0.10PH/s（peta-hash/second，毎秒10^{15}（＝千兆）回のハッシュ計算を行う速度）で24時間分購入した場合，37.56ドルといった価格で取引されている．

このようにハッシュ計算能力自体がコモディティ化し，また自由にハッシュ関数を選択してマイニングできるようになると，非主流派がこれまでとってきた戦略では，攻撃を防ぐことができなくなる．所要ハッシュ計算能力に大きな乖離がある場合，主流派の暗号資産用に利用されていた計算リソースを，非主流派のマイニングに転用が可能なのだ．攻撃者側は，自らハードウェアに投資することなく，時間貸しのハッシュ計算能力を匿名で購入して攻撃を仕掛けることが可能になる．

もちろん，こうした攻撃自体は，犯罪的な行為と考えられるが，それを取り締まる法律もなければ法執行も不可能だ．2017年後半の大相場に伴い極端に値上がりした非主流派の暗号資産の多くは，安全性や攻撃への対応という面で，十分に検証されてはいない．マイニングのためのハッシュ計算能力が適切に分散しているか，ノードが相応に立っているか，コミュニティでしっかり仕組みが精査されているか，攻撃に迅速に対応する能力を持っているかなど，各暗号資産の安全性が適切に価格に反映されなければ，今回のような攻撃は引き続き発生すると考えられる．

4.5　ビットコインのスケーラビリティ問題

ビットコインは取引を実行してからマイニングが行われ，検証に10分程度かかる．ところが，2016年から2017年にかけて，時には何時間も決済が検証されないトラブルが増えた．取引内容を格納するブロックは平均10分に1回生成されるが，ブロックのサイズに上限値（1MB）があるため取引の数が増えると格納しきれず，あふれた取引が検証されなくなったのだ．1日の取引件数にして40万件程度が上限となったのである．取引を承認してもらうためにマイナーに対して支払う手数料も，それまではほぼ無料であったものが高騰していた．こうした問題を，ビットコインのスケーラビリティ問題という．

その解決策として提案されたのは，①ブロック内の冗長な署名データを削除する，SegWitという手法を導入すること，②ブロックのサイズの上限値を引き上げること，の2つであった．これに対して，ビットコインのシステム開発者は①を，採掘業者は②を主張し，両陣営の溝が埋まらなかった．

2017年7月にコア開発者側が見切り発車的に①を導入しようとして期限に設定した2017年8月1日が分裂の日として注目され，相場急落の観測が広まった．仮に合意のないままにSegWitが強行されてしまうと，両陣営が支持するビットコインの分岐が2つできてしまうことになる．そういった事態の解決策は存在せず，利用者が損失を被るリスクがあったのだ．

しかし期限が到来する直前に，①と②の折衷案として，「SegWitは直ちに採用し，ブロックサイズの拡張は11月に改めて採否を協議する」という方針が提案され，決定的な対立は回避された．

この結果，当初危惧されていた分裂は回避されたが，採掘業者の一部が，ビットコインを分岐させて新しい暗号資産を作り出すことを表明し，別の形で分裂が発生した．ビットコインの相場は，分裂はしたものの騒動を無難に乗り切ったことが評価され，一段と高騰することとなった．

その後，11月に予定されていたブロックサイズ拡張は，準備が整っていないことから延期されたが，にもかかわらず相場の高騰と取引の繁忙は続いた．特に，2017年末にビットコインの相場が一時20,000ドルにまで高騰する局面があり，投機目的での売買件数が急増した．その結果，スケーラビリティ問題はより深刻化し，2017年末には1日に支払われる手数料が総額20億円を超える日もあるほどであった．

ところが，2018年に入ってからのビットコインの相場下落と取引鎮静化に伴い，スケーラビリティ問題は自然消滅してしまった．ビットコインのブロックサイズは上限に張り付いておらず，手数料もほぼゼロになっている．とはいえ，根本的な問題が解決されたわけではなく，再び取引量が拡大すれば，問題が再燃する可能性は高い．こうした危ういインフラの上で，投機目的の取引が続けられているのが，暗号資産の市場なのである．

5. 当面の考え得る対策

このように考えていくと，サトシの提案したビットコイン技術が輝いて見えたのは，当初想定した前提条件が満たされていた2009〜2012年頃だけであった．その後，相場は上昇したものの，サトシが想定していたような電子現金としての利用は，すっかり影を潜めた．安価な国際送金と期待された時期もあったが，現在では相場の変動が激しいため送金手段には向かない．むしろ，投機目的で取引が集中すると，取引件数が上限に達し，決済が滞ってしまう．これでは，便利な電子現金として使うというわけにはいかないだろう．

これらの逸脱は，起きるべくして起きたものである．ビットコインの初期の関係者は，法定通貨との交換相場の上昇を歓迎したし，取引件数の上限値を引き上げる交渉にもあまり積極的ではなかった．いったんは決済手段，支払手段のために生まれたビットコインも，法定通貨との交換価値が上昇すれば，投機商品となってしまった．ビットコインの成功を模倣して作られたその他の暗号資産も，目的とするところはほぼ同じである．このため，暗号資産は通貨としての機能を欠き，投機対象となってしまった．こうした認識から，かつては仮想通貨という呼称であったものが，現在の暗号資産という呼称に変更されているのである．

暗号資産は元々それ自体が価値を持つものではなかったので，人々の値上がり期待だけで値動きすることになり，相場は一方方向に振れやすい．2017年末に高値を付けた後，2018年には相場は暴落し，年末の価格は最高値の1/5のレベルにまで下落した．サトシが描いた世界から逸脱したビットコインは，元々デザインされた用途には使われておらず，今後使われるようになるとも考えにくい．そういう実態が正確に理解されれば，過去に見られたようなブームが再来するとは考えにくい．

今のビットコインをなにがしか修復して，将来の決済手段に転用しようとする提案もあるが，そのような修復は難しいし，仮に技術的に可能であったとしても関係者が合意して抜本的な修復を加えることはほぼ不可能であろう．もしインターネット上で利用する電子現金の仕組みが必要であるならば，別途ゼロから作ったほうがよほど現実的である．そういう意味からは，ビットコインや暗号資産の将来を考えるうえでは，投機商品として売買されている実態は受容し，資金洗浄等の不正利用の禁止や消費者保護の視点からの規制を課しつつ，過剰な期待が実態の伴わない値上がりを起こすことのないように，冷静に内容の理解を進めていくことが必要であろう．その観点からは，業者の不正防止，犯罪被害防止のための情報共有や，消費者教育が重要になるのではないだろうか．

また，現在の暗号資産は，秘密鍵管理を利用者に丸投げしているという意味で，不完全なアプリケーションだと言える．現実問題として，一般の利用者に秘密鍵を安全に管理させることは難しい．だとすれば，一般の利用者は，誰かを信頼して鍵なり資産なりの管理を任せる必要がある．つまり，ビットコインの支持者が理想として掲げた非中央集権やトラストレスといったキャッチフレーズは，実は幻影にすぎなかったことになる．現在の暗号資産は交換業者に全責任を持ってもらう仕組みになってしまっており，だとすれば，信頼できる交換業者に頼るしかないことになるからである．

交換業者が信頼できるかどうかを一般の利用者に判断させることは難しい．現在の日本の暗号資産の交換業者規制の仕組みでは，交換業者に銀行などの金融機関に準じたリスク管理を求めており，こうした政府による規制が，信頼性のシグナルとして機能することが期待できる．ただし，そうした法制度を備えている国は多くはない．日本の業者規制は厳しすぎるとの批判もあり，国境をまたいで容易にサービスを展開できてしまう暗号資産の取引においては，国内の業者のみを厳しく規制することには限界がある．資金洗浄やテロ資金調達を阻止するといった目的も含めて，暗号資産を規制する国際的な枠組みが必要とされている．

このように考えると，結局のところ，すべて自らの責任で資産を管理し，インターネット上でどの国の規制にも縛られずに経済活動を行うという，本来サトシが夢見たであろうコードが支配する世界を実際に構築するのは，実は必ずしも容易ではなく，また望ましくもないことのように思える．最終的に，国民の生命財産を守るのは各国の政府であり，資金洗浄やサイバー攻撃のリスクを考えたときに，ある程度の規模以上の経済取引については，何らかの形で国家権力によるチェックと後ろ盾があったほうが安全だというのが，これまでの暗号通貨を巡るさまざまな事件から得られた教訓である．問題は，そうした現実と，国家権力からのプライバシ保護との関係をどう整理するかにある．たとえば，一定金額未満の取引についてのみ匿名取引を認める，といった妥協案も考えられるが，そうしたルールが守られていることをチェックする仕組みまで考えた場合，技術的な対応だけでは問題は解決できないように思われる．

6. おわりに

暗号資産は社会的な大ブームを巻き起こし，日本だけで350万人もの投資家が暗号資産を保有するに至った．情報セキュリティ技術の実装例としては，かつてない規模の大成功を収めたアプリケーションである．他方で，その当初構想からの逸脱が生じた原因が，一般利用者による秘密鍵管理の問題であったことは，情報セキュリティ技術の現実への応用を考えていくうえで，多くの示唆を持つものといえる．

電子署名法や電子政府を巡る議論においては，高度な情報セキュリティの実現が求められ，ディジタル署名に利用する秘密鍵の管理については，安全な専用デバイスへの格納を前提として，厳格な運用基準が定められた．しかし，そうした鍵管理の運用上のコストが，一般利用者への情報セキュリティ技術の普及を妨げてきたことは否定できない．実際，PEMやPGPなど，暗号化電子メールの技術は1990年代に確立しており，実務上も切実なニーズがあるにもかかわらず，電子メールへのディジタル署名の付与や文面の秘匿化は，いまだに限定的にしか普及していない．その背景には，鍵管理に代表される運用上の課題が解決されていないことが挙げられよう．

ビットコインは，こうした課題を利用者側に任せることで，当初の急速な普及を実現した．geekが利用者であった黎明期には，鍵ペアの生成から安全な管理までを利用者自らが担うことで，ユーザコミュニティ全体として，一定のセキュリティ水準を達成していたと考えられる．

しかし，そうしたやり方には限界があった．geekではない，大勢の一般投資家が参入してきた結果として，個々のユーザがセキュリティに責任を持つ形態から，複雑なセキュリティを交換業者に任せ，ユーザはIDとパスワードといった簡単に扱える認証手段に頼るようになったのだ．そして，こうした認証手段の変換サービス提供者ともいえる交換業者の元には，大きなリスクが潜在し，サイバー攻撃を受けてそれが顕現化する事態を招いたのである．

こうしたビットコインや暗号資産の経験を考えれば，いわゆるパブリック・ブロックチェーンと呼ばれる技術が本当に信頼して利用できるかは，ユーザを含めたシステム全体の運用管理に依存していることが分かる．すべてのユーザがgeekになれない以上，利用者の運用管理に依存することは，現実には難しい．特に，大きな経済的価値を取り扱うものであった場合，サイバー攻撃のリスク対策を一般のユーザに委ねる仕組みは成立しないであろう．

いずれは，一般ユーザが安全に，かつ過剰な負担を感じることなく秘密鍵を管理できる環境を整備していくことが，社会のインフラとして必要になるだろう．そのためには国民全員に秘密鍵を格納したICカードを配布するといった施策が必要だが，それだけでは十分ではない．すべてのユーザがデバイスの操作に習熟するとともに，その効果をある程度正確に予測できていることが必要である．たとえば，ほとんどの日本人は印鑑の機能と効果について，ある程度の常識を共有している．それと同じ程度には，秘密鍵の格納されたデバイスについての情報セキュリティの知識が共有される必要がある．

そのような環境が実現しない限り，パブリックなブロックチェーンの効果を過度に期待するべきではない．むしろ当面の間は，ユーザの教育やデバイスの共通化が図りやすい，利用者の範囲を限定した，プライベート型，あるいはコンソーシアム型のブロックチェーンが現実的な解となると考えられる．

参考文献

1）Nakamoto, S. : Bitcoin : A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf (2008)
2）Chaum, D. : Blind Signatures for Untraceable Payments, Advances in Cryptology

Proceedings of Crypto. 82.
3）Okamoto, T. and Ohta, K. : Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility, Advances in Cryptology - EUROCRYPT'89, LNCS 434, pp.134-149, Springer-Verlag (1989).
4）Haber, S. and Stornetta, W. S. : How to Time-stamp a Digital Document, In Journal of Cryptology, Vol.3, No.2, pp.99-111 (1991).
5）Bayer, D., Haber, S. and Stornetta, W. S. : Improving the Efficiency and Reliability of Digital Time-Stamping, Sequences II Methods in Communication, Security, and Computer Science, pp.329-334, Springer-Verlag (1993).
6）Haber, S. and Stornetta, W. S. : Secure Names for Bit-strings, In Proceedings of The 4th ACM Conference.
7）Back, A. : Hashcash - A Denial of Service Counter-measure, http://www.hashcash.org/papers/hashcash.pdf (2002)
8）Bearman, J. : SILK ROAD : THE UNTOLD STORY, https://www.wired.com/2015/05/silk-road-untold-story/

岩下 直行（非会員）iwashita.naoyuki.7e@kyoto-u.ac.jp
1984年 慶大・経済卒業．同年，日本銀行入行．2005年 金融研究所・情報技術研究センター長，2014年 金融高度化センター長，2016年 FinTechセンター長．現在，京大・公共政策大学院教授．

採録決定：2019年3月13日
編集担当：粟津 正輝（（株）富士通研究所）