

ところが、注目度が高まった 2014 年 2 月に、当時最大規模のビットコイン取引所だったマウントゴックス (Mt. Gox) が、「預かっていたビットコインのほぼ全額を消失した」と発表して経営破綻しました。他の取引所でのビットコイン価格で計算して、**500 億円近い損失**が発生したとされます。

しかし、**キプロスの金融危機**がビットコインの人気につながったように、世界経済の動向のなかで、ビットコインを資産運用（投資、投機）対象とみる人が広がる可能性はあります。なにより、もしビットコインのような暗号通貨の利用が一般化すれば、少額の国際決済が簡単になります。これほどグローバル化が進んだ現代でも、3000 円相当の外貨を海外の誰かから受け取るうとすると、じつはむずかしいという事情があります。手数料が高すぎて、銀行を通じての送金が事実上使えないからです。

ウェブが登場したとき、「この上でコンテンツを売ってビジネスをしよう」と考えた人は大量にいました。しかし、アダルト関連などごく一部を除き、**一つひとつのコンテンツに課金する私たちのビジネスは、うまくいきませんでした**。記事 1 本単位、動画 1 本単位といった細かな決済をうまくおこなう手段がなかったからです。一つひとつのウェブや動画の製作には当然コストがかかっていますが、1 本単位だと高い金額をつけるわけにもいきません。他方で、100 円、200 円といった小さな額を決済するには、いろいろと問題があります。

もっとも汎用性の高い決済手段はクレジットカードですが、もともと数千円以上の決済のためにつくられたシステムであったため、あまり小さな額の決済には向いていない、という欠点があります。100 円、200 円といった決済をするには、決済時にかかる手数料が大きいこと、利用者側の手間もリスクも大きいことなどがその理由でした。現在はこうした問題点はある程度緩和されてきていますが、2000 年頃までは「クレジットカードでのコンテンツ決済は分が悪い」という見方が主流でした。

確たる決済手段が存在せず、デジタルコンテンツにお金を払ってもらえるかどうかも明確ではない——。そんな中で生まれたのが、広告をウェブの中に貼って、それをみてもらうことで収益を得る手法でした。これは、テレビの民間放送が CM で運営されていることと同じようなビジネスモデルだといえます。決済が介在しない気軽さと、ネット利用者が拡大傾向にあったことが相まって、広告モデルは大きな成功を収めました。現在も、ネットコンテンツの大半は広告収入で運営されています。

特に、2013 年以降に注目を集めているのが、スマートフォンやタブレットをクレジットカード決済端末として使うシステムです。アメリカのベンチャー企業・Square は、コインほどの大きさの「**Square リーダー**」と呼ばれる、超小型カードリーダーを開発しました（図表 1-4）。これを差し込むと、ふだん使っているスマートフォンやタブレットで、どこでもクレジットカード決済が可能になります。このシステムを導入することで、店舗の姿は大きく変わります。

注文と決済は、店員が持ち歩くタブレットでおこないます。紙のメニューの代わりにタブレットをみて注文し、決済時も小型カードリーダーにクレジットカードを通して完了です。タブレットからインターネットに接続してカード決済を完了させるため、巨大なレジスターは必要ありません。しかし、決済手段としてはクレジットカード決済に他ならないため、決済速度や安全性はクレジットカードとまったく同じです。

結果として、**店舗を始めるために必要な事務機材コストは激減します**。実際のところ、机ひとつ・店員ひとりで商売が可能であり、フリーマーケットへの出店に使っているところも少なくありません。また、注文や売り上げはすべて自動的に集計されますから、日々の事務処理の手間も劇的に小さくなります。

ITによる効率化は、従来では維持がむずか

しかったような小さな組織でのビジネスを可能とします。机ひとつ・店員ひとりでも店舗運営が可能になるのは、Squareのような小規模決済を助ける技術が生まれているためです。規模を追わず、コンパクトなビジネスのままで運営を続けていくというやり方を選ぶ場合でも、利益率は上げやすくなっています。「拡大を目指さないやり方」も「小さなところからスピード重視で広げていくやり方」も、20年前に比べてずっと簡単になりました。

このことが示しているのは、現在の変化の本質が「集約」ではなく「多様化」である、ということなのです。

しかし、世の中には「クリエイター志望者」も「パートタイムのクリエイター」もたくさんいます。そのすべてがそこまで積極的であるわけではありません。素晴らしいものを公開しているものの、それで積極的にお金を稼ぎたいとは思っていない人もいます。

とはいえ、支払ってもらえればうれしいはずです。ネットで自分の作品や発想を公開することは、ちょっとした隠し芸を披露するようなものです。褒められればもちろんうれしいでしょうが、誰かがちょっとした「おひねり」「投げ銭」をくれたなら、それはそれでうれしいはずなのです。

ネットの本質が多様性であり、それが人間の創造性につながっているのであれば、公園で大道芸におひねりを投げるように、なんらかの報酬を送りたい……こう思うのは自然なことなのです。

しかし、現在ネット上にある多くの決済システムは、「誰から誰に送られたものか」を明確にしなければならぬため、投げ銭のようにお金を受け渡すには向いていません。現金のもつ性質のうち、「誰が誰に渡してもいい」という要素が抜け落ちているからです。ネットで「投げ銭」的な送金を実現しよう……という試みは何度もおこなわれてきましたが、これまではうまくいきませんでした。

西田 ビットコインの取引所を運営しているのは、銀行などの金融機関ではなく、IT関連のベンチャー企業です。マウントゴックスも、そもそもは2009年に設立された、カードゲームの希少なカードを有料で交換するサービスが、ビットコイン取引へと業務を変えていった経緯をもちます。

吉本 それが、世界最大の取引所になってしまった。

西田 金融機関以外が取引を担当してはいけないわけではありません。法的な制約の少ない暗号通貨の場合にはなおさらです。しかし、顧客の大切な資産を預かる立場である以上、信頼性はやはり重要な要素です。

吉本 マウントゴックスの主張は信用できるのでしょうか？

西田 いろいろと疑義も差し挟まれています。ビットコインは本当にほぼすべてが失われたのではなく、一部が詐取されたのでは……と考える人もいます。

通貨には、寿命が長いものも短いものもあります。

「みんなが通貨と信じているうちは通貨として受け入れる」のが、通貨の本質です。

国家通貨の現金（紙幣・硬貨）は、形式的には価値の裏づけがあるようにいわれていますが、その現金が発行された時点で、その価値のほとんどは消えてしまっているのです。しかも、先進国の現代経済では、通貨量（残高）の9割以上が現金ではなく「預金」です。

預金（預貯金）は、民間の金融機関が預かっていて、しかも預金者に金利を支払うために、企業に貸し出されたりしています。金融機関の金庫のなかに、預金の価値の裏づけになるものはほとんど残っていないのです。もし、一定比率以上の預金者が同時に預金を引き出そうとすると、「取り付け騒ぎ」と呼ばれる現象が起きて金融機関の経営が傾くのは、そのためです。

通貨発行による利益を「シニョリッジ (seigniorage)」と呼びます。

...

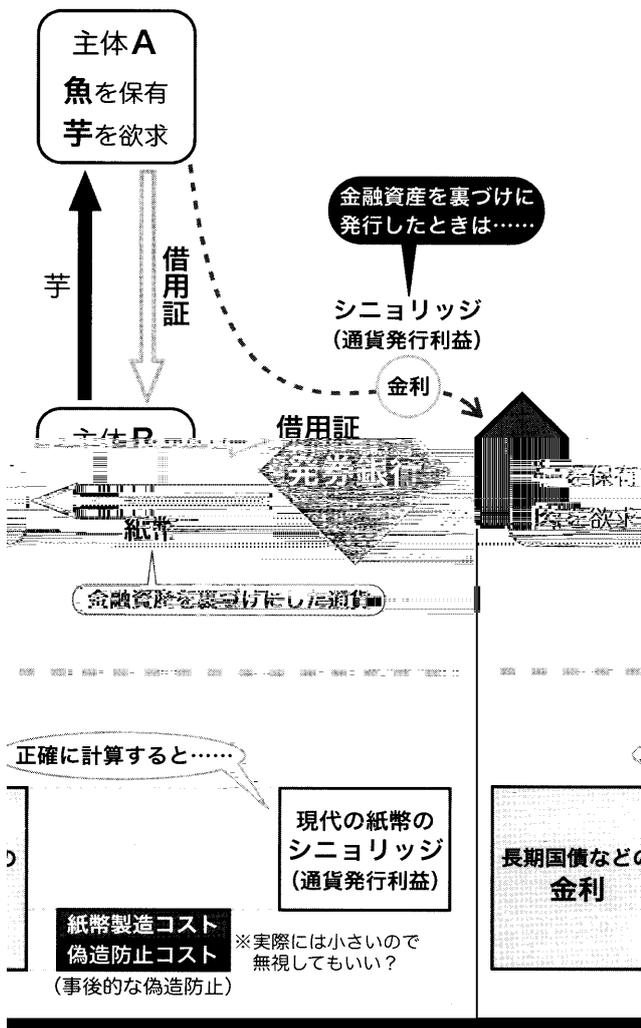
図表 2-4 を修正した図表 2

-5 で説明すると、単純に、主体 A が借用証で約束した金利を発券銀行が受け取るので、その金利がシニョリッジになるという話です。

現実の中央銀行は、国家が発行した長期国債を買い入れてその金利を得るケースが多いので、主に長期国債の金利が収入になります。そこから紙幣製造のコストを差し引き、紙幣発行後（事後的）に紙幣の偽造を取り締まって防止するコスト（これは国家の警察活動のコストにふくまれます）を差し引くと、シニョリッジが求められます（図表 2-5 の下側）。紙幣 1 枚当たりの各種コストは実際には小さいので無視すると、保有する長期国債などの金利がほぼそのままシニョリッジとなります。

いまの日本の場合、通貨発行はさほど大きな利益をもたらしません。日本政府が国債を発行して借金をするときの金利が、歴史的にみて相当に低いことが大きく影響しているのです。

図表2-5 紙幣のシニョリッジは金利



===Web===

- seigniorage
【名】シニョレッジ、通貨{つか}[貨幣{かへい}]発行益{はっこう えき} ◆金などの担保なしで通貨を発行する際に、発行者が発行により得ることができる利益。

===

中世ヨーロッパで絶大な影響力をもっていたキリスト教が、カネを貸して金利をとる行為を禁じていたことです。現代でも、イスラム教は金利を禁じているので、はっきりとした金利のかたちを避けて、実態としていかに金利の要素をふくめるかを工夫したイスラム金融が発達しています。

そして、通貨が異なる国の間でおこなう外国為替なら、為替レート（為替相場）のなかに金利をふくめてしまうことで、実態として金利のやりとりが可能でした。だから中世ヨーロッパでは、外国為替が先に発展し、**金利を禁止していたキリスト教の影響が強いなかでも、銀行業が成長できた**のです。

いままも、企業が**為替レートの先物予約をおこなうと、金利と為替手数料をふくんだ為替レートが提示されます**。手数料や金利は別に計算して示してほしいと考える企業も多いでしょうが、このやり方はキリスト教との関わりで定着したものです。

送金人 A が日本国内の X 銀行から、日本国内に住む受取人 B に現金を送金するとしましょう。わかりやすいのは、Y 銀行にある B の預金口座に送金し、B に現金で引き出してもらうやり方です。日本国内にある銀行は中央銀行（日本銀行）に預金口座をもっていて、この数字を書き換えるだけで、X 銀行から Y 銀行への資金移動は完了します。日本銀行を中心とするこの決済ネットワークを「**日銀ネット**」などと呼びます。

クレジットカー

ドの手数料（とりわけ店側が負担する手数料）は高すぎたともいえます。その根本原因はセキュリティの脆弱さにあります。

ビットコインは、コンピュータ上に記録されたデータを暗号化し、その「一意性」を保証することで、通貨になりうる属性をもたせたデータ、と定義することができます。

コンピュータ上のデータは、本質的にはどれも複製（コピー）が可能です。他方で、通貨が簡単に複製できるようでは困ります。偽札がいくらでもつくれるということですから。

ゲートや Suica 対応レジはすべてネットワークにつながっており、各 Suica カードや携帯電話の利用履歴と残高情報は、JR 東日本などの運営元が管理するサーバーで照合され、情報にまちがいが無いことが確認されます。通常こうした処理は、ほぼリアルタイムにおこなわれており、**管理サーバ上の「Suica にチャージされた金額」とカード上の「使えるはずの金額」は同一であるよう保たれています**。もちろんそうして決済された情報は、駅・店舗と Suica 運営会社の間でやりとりされ、最終的には駅や店舗の売り上げに反映されます。

ビットコインはどこかの企業が開発して運営するシステムではありません。2008 年末に「**中本哲史**」を名乗る人物が、暗号情報についての研究者同士の情報交換ネットワーク上で公開した論文に基づき、さまざまな人々が構築したシステムの組み合わせで実現されています。「中本哲史」が誰で、どんな人物なのか、正体はわかっていません。「中本氏」がどこまでビットコインのシステム開発に関わっているかも不明です。

マイニングという作業により、「世の中にひとつしかないデータ」が生まれるわけですが、ビットコインの場合、その個数は有限で、理論 12100 万 BTC 分、とされています。これは**中本氏が決めた上限**です。中本論文には、通貨が制限なく発行されることで、やがてインフレーション（物価の上昇＝通貨の購買力の下落）がひどくなることを避けようという意図が、はっきりと示されています。

ここまで説明してきたように、ビットコインは「コピーできないデータを流通させるシステ

ム」です。ビットコインそのものがコピーできないのと同様に、誰から誰にビットコインが受け渡されたのかという「取引情報」も暗号化され、複製・変更されないかたちで残ります。当然ですが、他人に取引情報が覗かれることはありません。

その反面で、**秘密鍵**を覚えていないかぎり、自分も取引情報を覗けません。だから、自分自身で注意しないと、消失が起きやすいのです。

では、ビットコインをどうやって流通させているのでしょうか？すでに述べたように、ビットコインはどこかが集中的に管理しているわけではありません。ビットコインの利用者がパソコンにインストールする「ウォレット (財布)」と呼ばれるソフトが、ビットコインを管理する「ピア・トゥー・ピア (P2P) ネットワーク」を構成します。

集中管理するサーバーがなく、利用者のコンピュータをデータが渡っていくようなかたちで構成されるネットワークのことを「P2P ネットワーク」と呼びます。

...

ビットコインの場合、ウォレットごとに特定の文字列が生成されます。これは一つひとつバラバラで、同じものはありません。ビットコイン・ネットワークで送金する際の目印になるもので、メールアドレスや預金の口座番号のようなもの……と考えるとわかりやすいでしょうか。

「ビットコインアドレス・A からビットコインアドレス・B へ、何 BTC 送る」と指定するだけでビットコインの送金がおこなえます。

すでに述べたように、ビットコインではまず、一定時間の間に発生した複数の取引をひとかたまりの「ブロック」として保存していきます。ひとつのブロックには複数の取引が記録されますが、取引情報について、額の多寡は問いません。1000BTC が一度に取引されようが、0.0001BTC の取引であろうが、取引履歴はひとつです。ブロックには、「最後のブロックがつけられた時点からブロックをつくらうとしている時点の間に起こった取引情報」と、「最後につけられたブロックの正しい値」、そして特別な「nonce」ナンセンスと呼ばれる数字がふくまれます。ここから「ハッシュ」と呼ばれる値を計算するわけですが、そのためには、非常に膨大な演算を必要とします。

ビットコインの場合には、生成される「ハッシュ」が鍵の役割を果たします。ハッシュがなんなのか、なぜハッシュが鍵の役割を果たせるのかについては、のちほど詳しく説明します。重要なのは、ハッシュという鍵さえわかっているならば、その内容が正しいかどうかを確かめるのは、簡単かつ短時間の計算ですむ、ということです。逆に、ハッシュから「本当の情報がなんだったのか」を推察するのはきわめて困難です。ブロックの末尾にはこの鍵がくつついており、ブロック・鍵・次のブロック……という風に「鎖」を構成しています。そうして、ブロック同士がつながった状態を「ブロックチェーン」と呼びます。(図表 3・4)

マイニングとは、先ほど挙げた「鍵」となる情報を計算する作業であり、新しいブロックを承認し、ビットコイン・ネットワークを維持する作業そのものです。具体的には、ブロックにふくまれる「これまでの取引情報」「最後につけられたブロックの正しい値」「nonce」という 3 つの値からハッシュを算出するのですが、このハッシュが「特定の値」になる nonce を見つける作業を指します。現状では「ハッシュの頭から特定の桁までがすべて 0 になる」ようにする、ということが条件です。0 が並ぶ桁数はネットワークに参加しているコンピュータの数によって変化するしくみになっています。

条件を満たす nonce を発見するには、数値を実際に当てはめて計算していくしかありません。対象となる数字の数は膨大であるため、効率的な手法で計算をおこなったとしても、適合する nonce は、試行回数に対してある一定の確率でしか見つかりません。最初に nonce を見つけ、新しいブロックを承認した人には、ビットコインが「報酬」として与えられます。この報酬が、ネットワークを維持する作業をおこなううえでのインセンティブになっているのです。

最新のブロックを見つけたということは、その時点で「最長のブロックチェーンを構成した」ということでもあります。

===Web===

nonce

【1名】1.目下、さしあたり

2.《コ》ノンス、使い捨て乱数データ、ワンタイムパスワード◆通信などでセキュリティー保護のため、そのたびに生成される補助的変数。

【1形】その場限りの、臨時の【2名】1.〈英俗〉性的異常者、強姦犯人、幼児に性的いたづらをした犯罪者

2.〈英俗〉卑劣な〔見下げ果てた〕やつ

3.〈米俗〉ナンセンス、たわ言、くだらない〔ばかげた〕話〔こと〕

=====

たとえば「IBM」を「HAL」にするような「文字をひとつずつ前にずらす」というルールで暗号化されたものは、そのルールを知っている人になら簡単に元の情報を理解できます。

暗号化とは、ある数値（記号）を別の数値に変換する作業、ということができます。秘密鍵方式の場合、暗号化に使う作業と、それを読み取る「平文化ひらぶんか」に使う作業は同じものです。これが「秘密鍵」にあたります。

公開鍵暗号では、暗号化に使う鍵と平文化に使う鍵を分けるしくみを採用しました。秘密鍵方式ではひとつの鍵しか使いませんが、**公開鍵暗号では2つの鍵を使う**のです。

暗号化に使う鍵は「公開鍵」と呼ばれます。公開鍵はその名のとおりに、世の中に公開してもいい鍵です。しかし、公開鍵で暗号化すると、今度は「秘密鍵」でしか平文化できなくなります。秘密鍵はその所有者しか知らない鍵で、他人に伝える必要がありません。公開鍵暗号を使うことで、秘密鍵を伝えることなく暗号を受け渡すことができるわけです。

そのようなしくみを、どうやって実現するのでしょうか？ 秘密鍵暗号ならなんとなく理解できますが、「鍵が公開されているのに、特定の人しか平文化できない暗号」といわれても、ピンと来ないかもしれません。そこで、世界初の公開鍵暗号であり、最も広く使われているものである「**RSA 暗号**」を例に、そのしくみを簡単に解説してみましよう。RSA 以外にも公開鍵暗号は複数存在します。

図表3-7 RSA暗号のしくみ

RSA暗号の求め方	
説明	実例
1 任意の素数 p および q を定める	$p=101, q=997$ とする
e と $(p-1) \times (q-1)$ の最大公約数が1となるような e を算出	
2 ただし、通常 e は「3」もしくは「65537」を使う	$e=65537$
3 $n=p \times q$	$n=101 \times 997=100697$
4 公開鍵は (e, n)	公開鍵は (65537, 100697)
5 $1=d \times e \pmod{(p-1) \times (q-1)}$ を満たす d を求める	$1=d \times 65537 \pmod{(101-1) \times (997-1)}$ $d=82673$
6 秘密鍵は (n, d)	秘密鍵は (100697, 82673)

RSA暗号の使い方	
説明	実例
1 秘密にしたい情報の平文 M を定める	$M=100$ とする
2 $M^e \pmod n$ を求める	$C=100^{65537} \pmod{100697}$ $=83021$
3 上記の結果が暗号文 (C) となる	暗号文は 83021
4 平文にする際には、 $C^d \pmod n$ を求める	$M=83021^{82673} \pmod{100697}$ $=100$
5 上記の結果、平文 M がわかる	平文は 100

「mod」という記号もありますが、これは「2つの数字を割り算して出た余り」を指す**モジュロ演算**と呼ばれるものです。

ハッシュタグの「ハッシュ」も、ここで話題にするハッシュと同じ意味をもちます。ハッシュとは、「あるものを示すために使う短い符丁」のことです。ハッシュタグは「話題の符丁」ですし、コンピュータ技術として使われる場合には、「内容が正しいことを示す符丁」になります。

ハッシュという符丁を使う理由は、データ量を大幅に削減できるからです。ハッシュをつくるときには、ある種の計算をおこないます。そういう意味ではこれもまた暗号化の一種なのですが、一般的な暗号とは異なり、「元のデータに復元できない」かたちで短くします。

たとえば、「アルファベットを順に0から25までの数字に置き換えて、すべてを足す」というルールがあったとしましょう。10文字の英文字の単語は、必ず「0」(aが10文字)から「250」(zが10文字)までの数字になります。元の情報は「アルファベット10文字」ですが、計算後には10進数で3桁、コンピュータで広く使われる16進数では2桁にまで圧縮されます。このような変換処理が「ハッシュ化」であり、最後に残った数字が「ハッシュ」です。

ビットコインは、日常的な取引に使ううえで**2つの欠点**もっています。ひとつは、現金との交換を担当するしくみが規定されていないこと。もうひとつは、決済を受け取る側で**取引情報が確認されるまで10分の時間がかかる**ことです。一般的なオンライン決済では遅くとも数秒から数

十秒で終わりますので、現在のどの決済手段と比べても「きわめて遅い」といえます。特に個人の買い物などの用途では、不便な要素です。すでに述べたように、どちらもビットコインの特徴を決めるうえで重要な部分であり、そう設計されたもの……というべきですが、不便であることに変わりはありません。

そうした部分をカバーするのが「取引所」の役割です。

一般的に、**ゲーム内貨幣**は、ゲームをプレイしていれば自動的に蓄積されていきます。モンスターを倒したり、作物を収穫したりすれば、その分の対価が手に入るためです。どれだけの対価を得られるかには、運・不運もつきまといまいます。しかし一般には、プレイヤーの手元に残るゲーム内資産の量は、そのプレイヤーがゲームをプレイした時間に比例します。その世界で長くすごせばすごすほど、たくさんの資産を手に入れていくわけです。

ここでひとつの問題が発生します。誰もがゲームを長時間プレイできるわけではありません。ゲーム内で強くなりたいけれど、プレイ時間はあまり割けない……という人も当然います。そうした場合、対応策はないのでしょうか？

もちろんあります。長時間プレイした人からゲーム内貨幣を「現実の貨幣（通貨）」で買うのです。こうしたしくみは「**RMT（リアルマネー・トレード）**」と呼ばれます。売る側は、ゲーム内貨幣が余った人から買い取って売る……というパターンもありますが、ほとんどの場合、ゲーム内貨幣を稼ぐためのプレイヤーを用意し、ゲーム内でモンスターを狩ったり作物を収穫したりして、販売するためのゲーム内貨幣を別途集めます。

そうした「**RMTのためにゲーム内で稼ぐ集団**」は、**中国などの労働賃金が低い地域で組織的に集められ、長時間交代で途切れることなく「労働」としてゲーム内貨幣を集め続けています**。先ほど述べたように、長時間プレイすればするほど資産は集まりますから、一般的なプレイヤーよりも多くの資産を、彼らは手にすることになります。こうした人々を「**ゴールド・ファーマー**」などと呼びます。また、人手を使わず、別途用意したソフト（**BOT**などと呼ばれます）を使い、収集活動を自動化する場合があります。そうして集めたゲーム内資産に**労働対価を超える値段をつけて換金すれば、RMTの運営元は多額の現金を手にする**わけです。

中央銀行は、その生い立ち（発展プロセス）を考えても、**過度に信用するのは危険な国家機関**だといえます。ただし、日本銀行の信用と円が暴落する危険性は、すぐには結びつきません。これまで強調してきたのは、単に、いまの日本銀行は日本円の信用を高めるのに役立っていないという内容です。また、高度経済成長が終わってからの日本銀行は、政治家による不適切な影響を強く受けやすく、**ずっと信用に値しない中央銀行であった**といえます。

中央銀行には、3つの大きな役割があります。すでに紹介してきた役割で、「**発券銀行**」「**銀行の銀行**」「**政府の銀行**」の3つです。経済学のテキストには、いかにもこの順で重要な役割であるかのように並べられていたりしますが、歴史的には、3番目の「**政府の銀行**」として設立されたという経緯があります。

いまのような中央銀行制度が世界標準の経済社会制度になったのは、イギリスがイングランド銀行を設立して成功し、フランスでもナポレオン・ボナパルトがフランス銀行を中央銀行とし、とりわけイギリスの経済的な繁栄が中央銀行制度を世界に広めたからです。

イングランド銀行は、50歳を過ぎたニュートンがイギリスの王立造幣局監事になる2年前の、1694年に設立されました。1716年にはフランスで、のちのフランス銀行の原型となる王立銀行が設立されました（王立銀行になったのは1718年からです）。

イングランド銀行はそのまま現代まで続いている中央銀行ですが、設立時には、中央銀行の役割のうち「**政府の銀行**」としての役割だけを担っていたのです。**王族などの浪費と戦争のために莫大な金額に膨らんだ国家債務を整理**するために（国家の借金をうまく処理するために）、そして、戦争継続のための資金をさらに国家に提供するために、イギリスやフランスなどで設立され、のちに世界中に広まったというのが、中央銀行の生い立ちです。フランスの王立銀行を創立したジョン・ローは、王立銀行に紙幣を発行させ（王立銀行は中央銀行ではないので話が複雑ですが）、**国家債務をうまく消す企みの中心的な役割**を担わせました。

高校の世界史の教科書な

どでは、ナポレオンの業績のひとつとして、フランス銀行（中央銀行）の設立が挙げられていますが、当時の中央銀行は、戦争に明け暮れる国家が**国民に戦費負担をさせるためのしくみ**であったことを、きちんと意識して評価すべきでしょう。

第二次世界大戦後に日本で起きたハイパーインフレは、戦費調達のために発行された国債を日本銀行が無制限に引き受けたことが大きな要因になっています。

ギリシャの危機はなぜ起き、どうして沈静化したのかを、明確に示すグラフが212ページの図表4・6です。ユーロ圏の中央銀行である ECB（欧州中央銀行）が公表している「**労働コスト上昇率ベースの実質実効為替レート**」のデータをグラフ化してあります。ユーロ圏にあって、同じユーロを使っているのですから、ギリシャとドイツの間の為替レートは「1ユーロ=1ユーロ」で完全に固定されています。

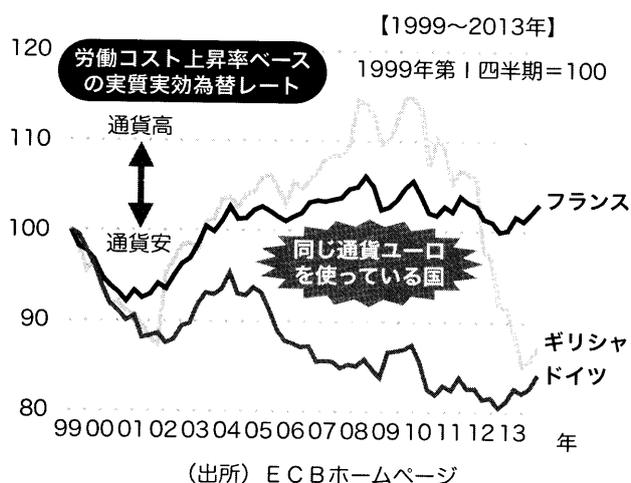
ところが、為替レートには「名目・実質」のちがいがあり、「2国間・多国間」のちがいがあります。私たちがいつもみている為替レートは、**物価の調整をしていない**という意味で「名目」であり、かつ「2国間」の為替レートです。

しかし、実質的な通貨の価値は「**その通貨でどれだけのモノが買えるか**」で評価すべきものです。物価が2倍になれば、同じ1ユーロで買えるモノは半分になりますから、1ユーロの実質価値は半分まで安くなったとみるべきなのです。こうして**物価を調整したあとの為替レートが「実質為替レート**」です。そして、企業の競争力をみたいなら、物価よりも賃金などの労働コストを調整したほうがいとされています。その調整したのが「労働コスト上昇率ベースの実質為替レート」です。

また、たくさんの国と貿易しているなら、主要な貿易相手国すべての通貨との間の、平均的な為替レート変動をみたいところです。そうして多国間の為替レートをみるのが「**実効為替レート**」です。また、実質かつ実効の為替レートをみるのが「**実質実効為替レート**」です。

慣れないとわかりにくいデータですが、重要度が高く、どこの国の中央銀行も計算して公表しています。

図表4-6 ユーロ危機の根本原因



ドイツ、フランス、ギリシャの3カ国は同じユーロを使っていますが、労働コストや物価の上昇率に差があったために、実質的な為替レートは大幅に異なる動きをしています。

ギリシャで危機が起きた2010年までのグラフだけに注目すると、ギリシャとフランス

の為替レートがとても高く、ドイツの為替レートがとても安くなっていました。なぜでしょうか。

ギリシャとフランスの労働コストの上昇率が、長期にわたってドイツより高かったから

です。原理を説明するために、現実とは異なりますが、単純な数値例で考えましょう。

通貨統合がおこなわれた時点の労働者の1時間当たりの労働コスト（時給と考えてかまいません）が、ギリシャでもドイツでも10ユーロだったとします。それから10年が経過して、ギリシャの労働コストは10%上がり、ドイツでは10%下がったとしましょう。両国でひとりの労働者が1時間に10個つくれるモノがあって、それは変わらずに、時給などの労働コストだけが変わったとします。

ギリシャとドイツで、1ユーロの労働コストをかけて、何個のモノがつくれるのでしょうか。当初はどちらも1時間10ユーロのコストで10個つくれましたから、1ユーロで1個ずつつくれたはずですが、したがって競争力に差はなかったでしょう。

10年後に、労働コストが10%上がったギリシャで10ユーロ分だけ働いてもらおうと、10%少ない労働時間になり、9個しかつくれません。労働コストが10%下がったドイツで10ユーロ分だけ働いてもらおうと、10%余分に働いてもらえますから、11個つくれます。

同じ1ユーロの労働コストでつくったモノを輸出しようとする、ギリシャは0.9個しか輸出できないのに対し、ドイツは1.1個輸出できます。これを同じ1ユーロで売れば、ドイツ企業が競争に勝つのは明らかです。実質的には、ギリシャの1ユーロは、かつての0.9ユーロの価値しかないのに、名目上は1ユーロのままだから、実質的には10%高すぎるのです（過大評価されているのです）。他方で、ドイツの1ユーロはかつての1.1ユーロの価値があるのに、名目上は1ユーロで固定されているから、実質的に10%安すぎるのです（過小評価されているのです）。

実際の数値はこんなに単純ではありませんが、ギリシャ経済が危機に陥る前には、ギリシャのユーロがドイツのユーロに比べて、実質的に大幅な過大評価になっていたことはたしかです。このために、ユーロ圏全体を巻き込む危機が起きたのです。ギリシャは、とにかく自国の景気を悪化させる経済政策をおこない、賃金を下げることで、強引に労働コストを引き下げ、実質実効為替レートを急落させました。それが図表4-6の2011年以降のグラフにあらわれています。

これほど急激に実質実効為替レートを下げたことの代償として、ギリシャの2011年から3年間の経済成長率は、マイナス7.1%、マイナス7.0%、マイナス3.9%と、とてもひどい数字が並びました。2010年の経済成長率もマイナス4.9%で、リーマンショック直後の2009年もマイナス成長でしたから、そこから5年間で2割以上も経済が縮小してしまっただけになります。ここまでしてもなお、2014年3月上旬までに合意するはずのギリシャへの融資に、IMFとEUが合意しませんでした。そのなかで、ギリシャに対して「まだ競争力を回復させるための経済改革が不十分だ」と指摘されていました。

ユーロで通貨を統一してしまっ

たために、為替レートを変えて調整するというやり方が効かないことが、最大の問題です。ユーロによる通貨統合は、経済的には明らかに失敗だったようです。ただし、政治的な意図もあってのことですから、失敗と決めつけるわけにはいかないでしょう。

他方で、江戸幕府が倒れた経済的原因として、幕末の急激なインフレ（物価上昇）があります。その原因のひとつが、幕府の通貨政策（いまでいえば中央銀行の金融政策）でした。幕府が通貨制度を利用して借金返済をしようとするなかで、計数貨幣としての銀貨をつくり、銀貨の価値を過大評価させて流通させたため、逆に金貨の価値を著しく過小評価する通貨体系になっていました。

その後、開国を余儀なくされて、アメリカと1858年に締結した日米修好通商条約の第5条に「外国と日本の同種類の貨幣は同量で交換する」といった内容があったため、日本国内で過小評価されていた金貨が流出し、代わりに、過大評価されていた銀貨が流入しました。

金貨がどんどん海外に流出して巨額損失を被ったのですが、これを食い止めるために、幕府は小判の金含有量を大幅に引き下げる悪鋳あくちゅうをおこないました。これが激しいインフレを招き、国民の暮らしが悪化しました。そして幕府は消滅し、幕府発行の国家通貨も運命を共にしたわけです。