NAD Monthly Report.

Market Flash

バーチャル貨幣
ビットコインの謎！？

2014.02

NIHON ALPS DENSHI

バーチャル貨幣の謎

はじめに

最近、「ビットコイン」という言葉をよく耳にするようになりました。先月行われた全銀協会長の記者会見でも記者から「ビットコインをどう思うか」という質問が出たり、黒田日銀総裁も、「ビットコインについて金融研究所を中心に調査・研究している」と述べるなど話題となっています。

そこで、ビットコインについて、このレポートにできるだけわかりやすく簡単に書こうといろいろ調べ始めたのですが、これがまた難解・・・!? 正直今でもその仕組みについて完全には理解していません。

いろいろな資料、著書を読んでみても謎が深まるばかりになりました。そこでもう少し時間をいただき今月と来月の2回に分けてまとめることにしました。

ビットコインの理解しにくいのがどうしてだろうと考えた時、多くの資料、著書（すべて電子書籍）がIT関係者によって書かれているもので、ビットコインのシステムについてかなり専門的な説明になっていること、ビットコインのシステムがいかに優れているのかを中心に説明していること、などビットコイン信奉者からみたビットコインの説明になっていることが原因のように思います。そのため、経済的価値などから見た意見・説明は素人的なものが多く、私などから見ると「何言ってるの」と言いたくなるものが多くありました。半面、ビットコインの仕組み、システムの優れた点が明確にわからないという面があるのも確かです。

今世の中でいろいろとビットコインについて賛否両論があるのは、このITに精通した人(システムという技術面からの意見）と経済に精通した人（経済面から見た意見）の考え方の違いにあるように思えてきました。

いずれにしても注目されている通貨？であり、すでにある程度流通しているのは確かです。私自身は、いくらシステム的に優れたものであってもそれを通貨として流通させるには無理があり、価値のあるものではないという意見でしたが、今後何らかの法規制が定まり、しっかりとした管理がなされるのであれば、紙幣や硬貨に加えて電子マネーという存在ができてきても不思議ではないと考えるようになりました。

さて、前置きはこのぐらいにして本題に入りたいと思います。今月は、まずビットコインをシステム面からみて、ビットコインの仕組みについて説明します。仕組みについてはいくつかの文献から抜粋し（なかなかそれをかみ砕くのが難しいので）、それを理解するための専門用語の説明を加えることにしました。そして、次回は経済面から見たビットコインの価値について書いてみたいと思っています。

1．昨年のビットコイン・マーケットの動向

2013年1月1日のビットコインのレートは、1ビットコイン（BTC）＝13ドルであった。それが、11月29日には1224ドルと100倍近い値上がりを見せた。その後、中国での規制をきっかけに半分程度まで暴落し、2014年1月現在は、950ドル程度で取引されている。

ビットコインが注目されるきっかけとなったのは、昨年のキプロス危機からである。キプロスはもともと観光以外の産業がないため、タックスヘブンとして金融業を中心とした顔があった。そのキプロスがギリシャの財政危機の余波を受け（ギリシャの国債を大量に所有していたため）危機に陥り、EUとIMFから100億ドルの融資を受けた。その条件としてキプロス自身も58億ユーロを捻出しなければならなかった。そこで政府がとった処置が、大口預金に対する資産税の課税であった。つまり、強制的に国民の預金から政府が資金を吸い上げたのである。そして、一部の国民が自身の財産防衛の観点からビットコインに目をつけた。ビットコインに交換すれば、自由に国外にも持ち出せるし、国内でも税金がかかることがないということで注目された。さらに、2013年11月にはキプロスのニコシア大学がビットコインで授業料を納めてもいいという発表をしたことで、世界中から注目されている。

Market Flash

バーチャル貨幣の謎

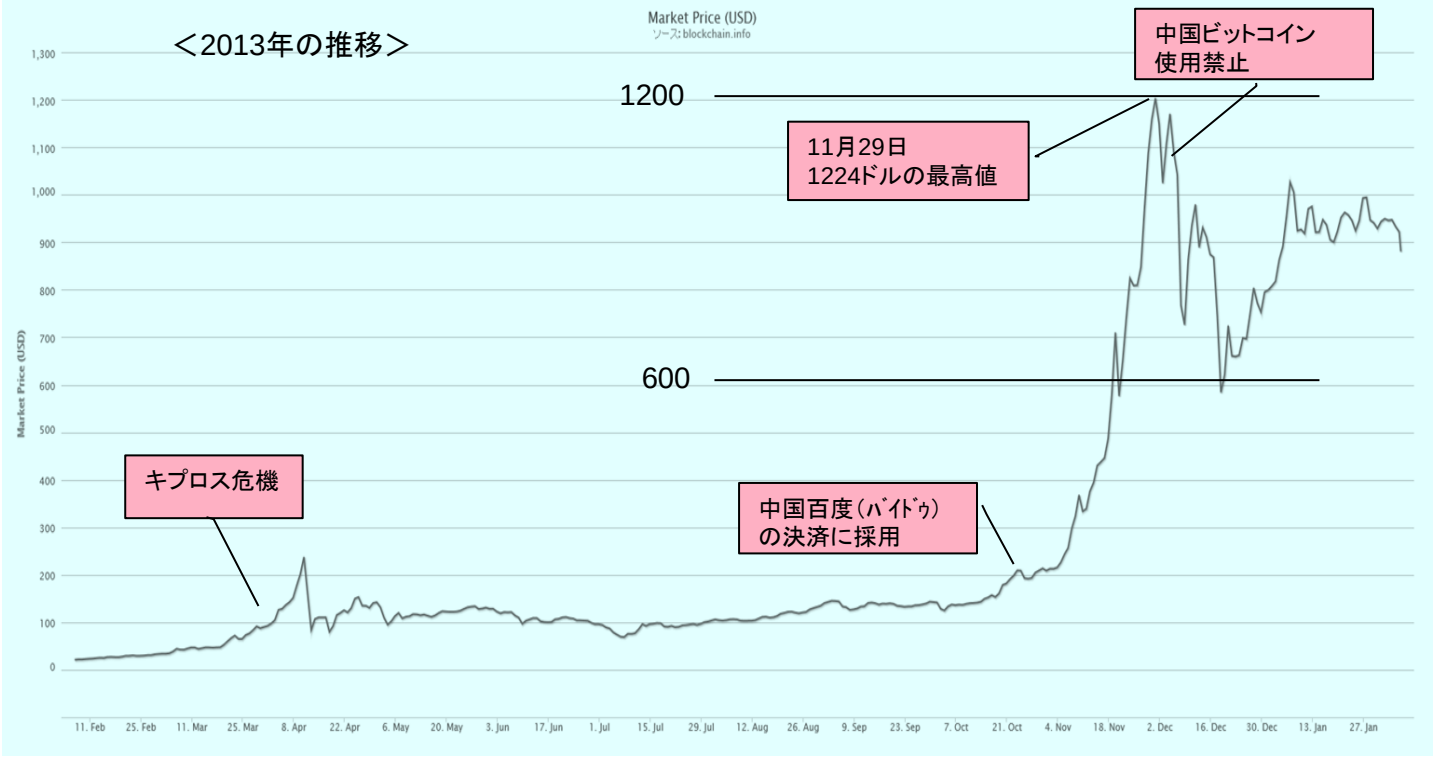
次に、ビットコインの価格上昇の引き金になったのが中国の投資熱であった。中国では、不動産は国の所有となっており、また、国内の証券市場もまだまだ整備されていない状況である。こうした事情から、ビットコインは絶好の投資先として資金が集中したのである。これに拍車をかけるように、中国の検索サイト百度（バイドゥ）がビットコインでの決済を取り扱うようになると、一気にビットコインのレートが上昇。10月1日は141ドルだったビットコインが、11月29日には最高値となる1224ドルまで急騰した。この時期、世界のビットコインの取引の3分の1が中国での取引であった。

しかし、中国政府もこのような抜け道を黙ってみているわけにはいかなかった。2013年12月になると、ビットコインでの商取引の禁止を決めた。そのため、ビットコインのレートは急落、12月22日は636ドルまで落ち込んだ。今年に入ってからは持ち直して900ドルから1000ドル程度で推移している。

昨年の流通取引高は右の表にあるように、
約3，075Mドル（3100億円）であった。
マネーマーケットの世界では決して大きな
マーケットとはなっていない。

このように、ビットコインは2013年から注目をされはじめたのだが、この1年間はまさに「博打相場」というものであった。
決して通貨として認められるような相場ではなかった。

Interval	Volume (BTC)	Volume (USD)	Weighted Price
15min	847.45	704,591.82	831.4302
1h	1,524.29	1,269,737.49	833.0030
4h	8,532.15	7,297,458.87	855.2893
12h	13,220.64	11,545,636.26	873.3041
1d	15,170.26	13,338,596.85	879.2598
2d	19,311.11	17,177,811.67	889.5298
7d	36,036.06	32,930,673.26	913.8256
30d	231,943.34	217,910,185.06	939.4975
6m	3,947,310.46	1,920,575,111.85	486.5528
1y	16,230,023.07	3,075,572,576.81	189.4990



Market Flash

バーチャル貨幣の謎

2. ビットコインの生い立ち

ビットコインは、中本哲史（なかもとさとし）という人物が暗号システムについて議論するメーリングリストに2008年に投降した論文に基づいて作られた。この論文では、P2Pでの分散処理で数学的に証明可能なデジタル通貨のシステムについて説明されている。この「中本哲史」という人物がだれなのかは今でも分かっていない。京都大学のある有名な教授ではないかというううわさもある。この論文自体は英語で書かれており、メーリングリストには世界中の人が参加しているので日本人かどうかは不明のままである。

当初は、この論文の内容がはたして実際にワークするのか誰も知りえなかったため、研究者やIT関係者が実験的に作成されスタートした。ところが、2010年5月にラスロー・ハニヤットというプログラマーが面白半分に「誰かビットコイン1万枚とピザを交換してくれ！」と投稿し、イギリスの男性がピザ2枚との交換に応じたのが、ビットコインによる商取引の最初といわれている。ちなみに、今の相場で換算するとピザ2枚で約9億円にもなる。
このようにもともとは研究者たちの間で実験的に始まったものが、徐々に広がりビットコインがお金と交換されるようになってきたのである。2009年に始まったビットコインが現在は世界で1250万BTCで約1兆円に相当するビットコインが流通している。

ビットコインのシステム的な仕組みについて、これまで調べた資料を基に私なりの解釈（IT専門家からはおしかりを受けるかもしれないが・・・）でまとめると以下のような特徴を持っている。

ビットコインとは、

①ハッシュ値を用いた**デジタル署名**の仕組みを使って、コインの所有者が変わってもそれが改ざんされたものではないことを検証できる仕組みとなっている。

②また、そのコインが二重に発行、消費されたものではないことを証明（**二重消費への対策**）する作業が、「**採掘**」或いは「**発掘**」という作業によって行われる。その採掘作業は10分間で行われ、その間に一番最初に検証を終えた人にご褒美としてビットコインが新たに発行される仕組みとなっている。

③その検証＝採掘は、**P2P方式**により世界中のコンピューターによって行われており、全世界で参加しているコンピューター全体で競争をして検証が行われており、そのためこの仕組みは誰かが管理しているものではなく、お互いがお互いを管理するという仕組みになっている。

④ビットコインの発行量にはあらかじめ**上限**が設定されている。

このように、ビットコインはシステム的に強固に設計されており、改ざんされたり二重消費されないようになっている。そして、その検証をすべての参加するコンピューターによって管理されているというものである。
これにより、通貨としても十分信用ができるものであり（この点については、経済的にみると異議があるところではあるが、この点は次号で詳しく見ていく）、将来的に全く新しい通貨として流通しうるものであるというのが、特にIT関係者の意見である。
それでは、各特徴について詳しく見ていこう。

バーチャル貨幣の謎

3. ビットコインの仕組み

まず、ビットコインの基となったという「Satoshi　Nakamoto」の論文の書き出し部分をそのまま抜粋して紹介する。

＊＊＊＊＊＊＊＊＊＊＊＊ビットコイン:P2P 電子マネーシステム＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

中本 哲史　　http://www.bitcoin.co.jp/docs/SatoshiWhitepaper.pdf

＜概要＞

純粋なP2P電子マネーによって、金融機関を通さない甲乙間の直接的オンライン取引が可能になる。電子署名は問題の一部を解決するが、依然信用できる第三者機関による二重使用予防が求められるため、その恩恵は失われる。当システムはP2P電子マネーにおける二重使用問題の解決を提案する。このネットワークは取引に、ハッシュベースの継続的なプルーフ・オブ・ワークチェーンにハッシュ値として更新日時を記録し、プルーフ・オブ・ワークをやり直さない限り変更できない履歴を作成する。最長である一連のチェーンは、取引履歴を証明するだけでなく、それがCPUパワーの最大のプールから発せられたことを証明する。大多数のCPUパワーがネットワークを攻撃していないノード(ネットワーク接続ポイント)によってコントロールされている限り最長のチェーンが作成され、攻撃者を凌ぐ。ネットワーク自体は最小限の構成でよい。メッセージは最善努力原則で送信され、ノードは自由にネットワークから離脱、再接続することができ、離脱していた間のイベントの証明として最長のプルーフ・オブ・ワークチェーンを受信する。

必要なのは、信用ではなく暗号化された証明に基づく電子取引システムであり、これにより希望する二者が信用できる第三者機関を介さずに直接取引できるようになる。コンピュータ的に事実上非可逆的な取引は売り手を詐欺から守り、容易に実施 できる習慣的なエスクロー(第三者預託)メカニズムにより買い手も守られる。この論文では、時系列取引のコンピュータ的証明を作成するP2P分散型タイムスタンプ・サーバーを用いた、二重支払い問題の解決策を提案する。本システムは、良心的なノードが集合的に、攻撃 者グループのノードを上回るCPUパワーをコントロールしている限り安全である。

一つの電子コインは、連続するデジタル署名のチェーンと定義される。電子コインの各所有者は、直前の取引のハッシュと次の所有者のパブリック・キー(公開鍵)をデジタル署名でコインの最後に加えることにより、電子コインを次の所有者に転送する。受取人は一連の署名を検証することで、過去の所有権を検証できる。

無論、問題は受取人には過去の所有者がコインを二重使用していないことを検証できないことにある。一般的な解決法は信用のおける中央機関もしくは造幣局を間に入れ、全取引を監視させることである。
取引がなかったことを明確にするには全取引を監視する必要がある。造幣局モデルでは造幣局が全取引を監視し取引の順番を決定していた。これを第三者機関なしに行うには、取引が公開され、参加者たちが受け取った順番の唯一の取引履歴に合意することのできるシステムが必要となる。受取人は取引毎に、取引が行われた時点で大多数のノードがそのコインが初めて使用されたことに賛同したという証明を必要とする。

＊＊＊

理解できたであろうか？
もう少し部分的に他の資料を基に説明しよう。

バーチャル貨幣の謎

①デジタル署名の仕組み

（WIDE　Project編集　ビットコイン-人間不在のデジタル巨石貨幣　より一部抜粋）

ビットコインでは、「デジタル署名 」の技術を用い、コインの現在の所有者が誰であるかを明確にする。

このデジタル署名とは、各自の「公開鍵」K と「秘密鍵」K−1 の「鍵ペア」<K,K−1 > を持ち、公開鍵 K は公開し、秘密鍵 K−1 は隠し持っておく。秘密鍵で暗号化したデータは、ペアとなる公開鍵でしか復号できない。

あるデータ m に対しデジタル署名を施す際は、まず m に「暗号学的ハッシュ関数5」H を適用した固定長（実際の関数により異なるが 160bit, 256bit 等）の値である H(m) を計算する。この値を「ハッシュ値」と呼ぶ。ハッシュ値を秘密鍵 K−1 で暗号化した {H(m)}K−1 を「デジタル署名」または単に「署名」と呼び、m とともに相手に送る。

相手も m からハッシュ値 H(m) を計算し、それが署名を公開鍵 K で復号して得られる内容と一致するかを確かめる。このことを署名の「検証」と呼ぶ。一致しているならば、次のふたつのことが言える。

1. 間違いなく本人が署名を行った（秘密鍵は本人のみが使用できるように隠されているため）。
2. 署名された後、データは改竄されていない。

ビットコインでは、このように所有者が次の所有者にビットコインを渡すときにそれぞれの検証作業を行い、正しいビットコインであることを検証するものである（この検証作業は後述）。そして、その履歴はそのコインのデータとして蓄積されて公開される。

ここで、かなり専門的な用語が出てきたので早くも頭が痛くなってくる。ハッシュ値とは？　ハッシュ関数とは？
そこでこの専門用語について簡単に説明しているものを載せておく。これが理解できないとビットコインの入り口から分からなくなってしまう。

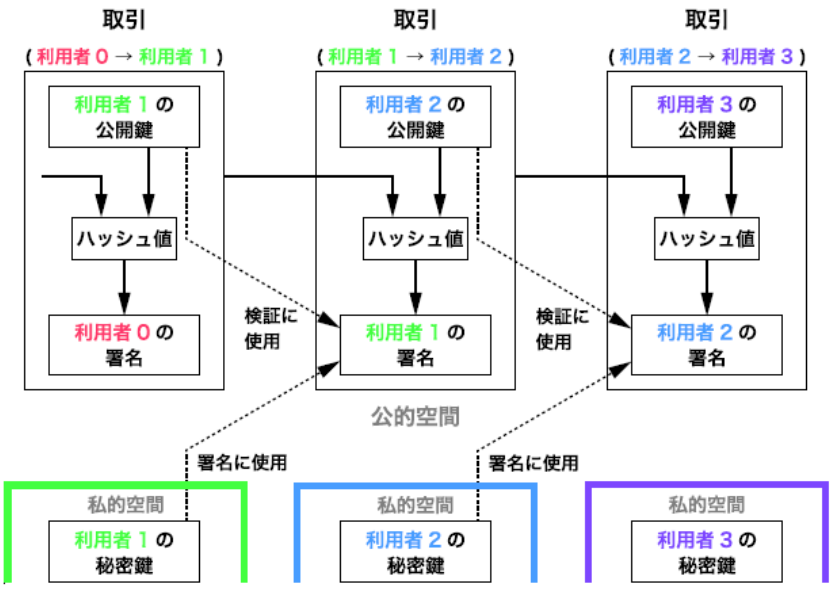


図 1: 署名チェインにより表現された電子コインの取引

Market Flash

バーチャル貨幣の謎

解説：ハッシュ値とは？（ITプロより抜粋）

情報処理の世界ではテキスト・データであっても画像データであっても、すべてのデータは0と1を組み合わせて表現します。つまり、どんなデータ（ファイル）であっても、一つの数値とみなすことができます。ハッシュ値とは、あるデータ（つまり数値）を、ハッシュ関数と呼ばれる関数で演算した結果です。このとき、ハッシュ値は基のデータのサイズに関わらず、128～512ビット程度の一定の長さになります（長さはアルゴリズムによって異なります）。ハッシュ（hash）という言葉は、「切り刻む、細かくする」という意味があります。基のデータを約束事（アルゴリズム）に従って細かく切り刻んで、一定の長さに整えたものというように、考えておけばよいでしょう。（**図1**）。

図1　ハッシュ値とは

基のデータ（ビット列）をハッシュ関数という特別な関数を使って計算すると、決まった長さのビット列になる。それがハッシュ値である。

また、次のような特徴を持っている

●異なる基のデータから同じハッシュ値が得られることはほとんどない
●ハッシュ値とハッシュ関数が分かっていても、基のデータを算出できない

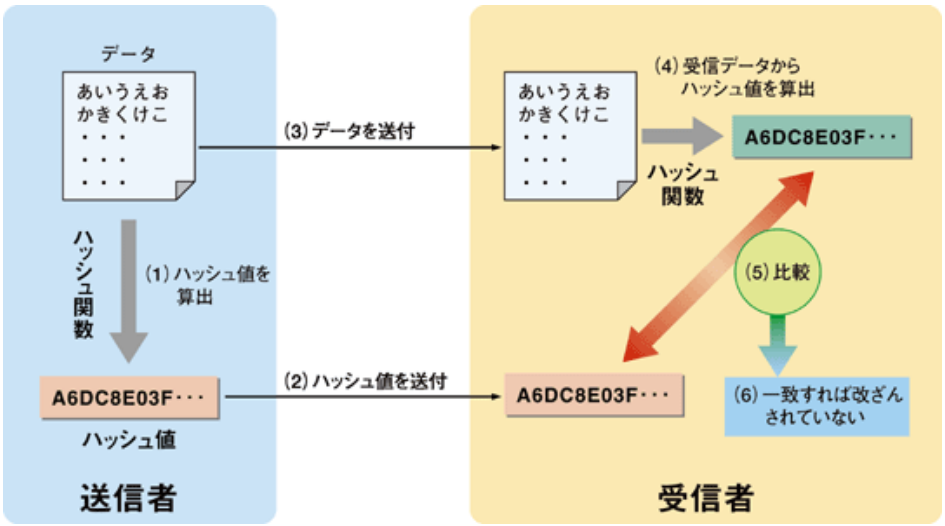
ハッシュ値の使い方（1）---改ざんの検知

それぞれの特徴に対応した使い方の例を見てみましょう。

まずは、『異なる基のデータから同じハッシュ値が得られることはほとんどない』という特徴を生かした使い方の例として、「改ざんの検知」を見てみましょう（**図2**）。

図2　ハッシュ値を改ざんした例

送信者が作成したハッシュ値と受信者が作成したハッシュ値が同一ならばデータが途中で改ざんされていないことが確認できる



送信者は、自分が作成したデータのハッシュ値を演算して（1）、
これを事前に受信者に送ります（2）。
また送信者は作成したデータも受信者に送ります（3）。
受信者は、送信者が使ったものと同じハッシュ関数を使って受信データのハッシュ値を演算します（4）。
そして送信者から事前に入手していたハッシュ値と、受信者自身が算出したハッシュ値を比べ（5）、
それらが全く同じならばデータが通信経路上で改ざんされていないと判断します（6）。

バーチャル貨幣の謎

もし、基データを盗聴した悪意のある第三者が、本文内容を変更して、受信者に送ったとします。するとハッシュ関数の特徴である「異なる基のデータから同じハッシュ値が得られることはほとんどない」ことから、送られてきたハッシュ値（送信者が作成したもの）と受信者が作成したハッシュ値は全く別のものとなり、データが通信経路上で改ざんされたことを検知できます（**図3**）。

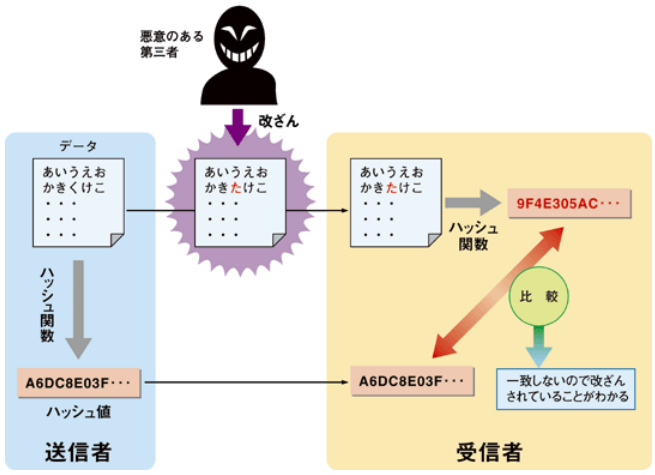


図3　通信経路上でデータの改ざんがあると
送信者が作成したハッシュ値と、
受信者が受信データから算出した
ハッシュ値が異なるため、
データが改ざんされたことが分かる

ハッシュ値の使い方（2）---パスワードの保存

次に『ハッシュ値とハッシュ関数が分かっていても、基のデータを算出できない』という特徴に基づく使い方の例として、「サーバーなどにアクセスしてくるメンバーのパスワードを保存する場合」を見てみましょう（**図4**）。パスワードをそのままの形で保存しておくと、悪意のある第三者がそのディレクトリにアクセスできた場合にパスワードが漏洩してしまう可能性があります。そこで、サーバーにはパスワードそのものを保存せず、パスワードのハッシュ値と、それが誰のものであるか、という情報だけを保存しておくのが一般的です。

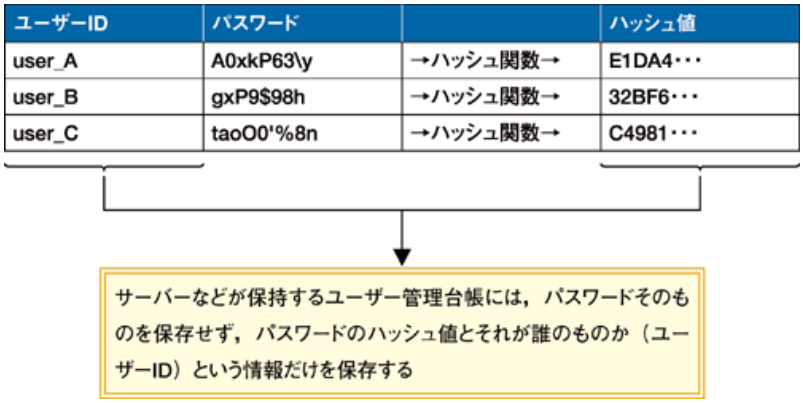
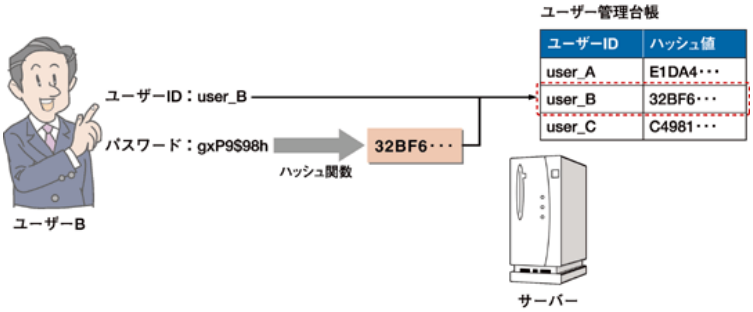


図4　パスワードの保存にハッシュ値を使う例
パスワードそのものを保存せず、パスワードの
ハッシュ値とそれが誰のものであるか、
という情報を保存しておく

そして、ユーザーがアクセスする場合は、入力したパスワードを基データとしてハッシュ関数を使ってハッシュ値を算出し、保存されているハッシュ値と比較します。これらのハッシュ値が同じであれば、基のパスワードは正しいと判断できます（**図5**）。



Market Flash

バーチャル貨幣の謎

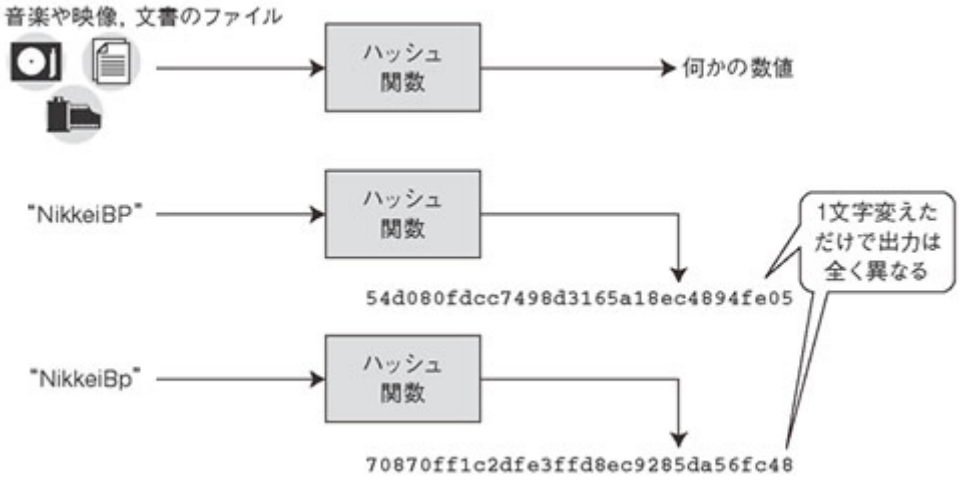
図5　入力されたパスワードを基にしてハッシュ関数でハッシュ値を計算し、保存してあるハッシュ値と比較する

このようにしておけば、悪意のある第三者がサーバーへ不正侵入し、パスワードのハッシュ値を盗み出すことができても、ハッシュ関数の二つめの特徴である「ハッシュ値とハッシュ関数が分かっていても、基のデータを算出できない」からパスワードを復元することができません。そして、（当然ですが）パスワードが復元できなければ、これを用いてなりすましをすることができません。

解説：ハッシュ関数とは？

ハッシュ関数とは、何らかのデータを入力して、ある数値を出力するようなブラック・ボックスだと考えてください。

ハッシュ関数には数値化できるデータなら、何でも入力できます。ある文字に割り当てられた文字コードから、何らかの数値を出力できます。文字や数値だけでなく、画像や音楽のような音声情報も数値化されているので、同じです。



ハッシュ関数は、どんな大きさの情報でも入力できます。しかし出力されるのは、そのハッシュ関数で定められた長さに決まっています。

　インターネットでよく使われるハッシュ関数に、MD5とSHA-1があります。MD5では128ビット、SHA-1では160ビット長の数値を出力します。この出力値をハッシュ値といいます。

　一冊の本の中のすべての文字を160ビット長の数値に変換することもできますが、ハッシュ値だけから元のデータを復元することはできません。そのためハッシュ値はダイジェスト（消化物）といわれることもあります。

いかがでしょうか？多少は理解できたでしょうか？

ビットコインは、このハッシュ値によって暗号化され、所有者はKeyを使うことによってそのコインが改ざんされていないということを検証できるシステムとなっているのである。これにより所有者が安全に利用できる仕組みとなっている。

Market Flash

バーチャル貨幣の謎

②二重消費への対策（WIDE project ビットコインから抜粋）

ビットコインのもう一つの特徴として、二重消費への対策がある。それは、相手にコインを渡しても、手元にコインのデータのコピーを残しておいて、それを別の相手に対して使うような利用者を防ぐ対策である。

ビットコインでは、全世界でのすべてのビットコインによる取引の順序が一意に定まるように、ビットコインのネットワークに参加するコンピューター間で合意形成し、二重消費を監視することにしている。取引のデータはネットワーク内に公開され、ネットワークに参加するコンピューター群は、複数の取引をまとめてデータのブロックに格納し、ブロックを時系列に並べていく。このデータの構造をブロックチェインと呼び、全世界で唯一のものをネットワーク内で維持する。すなわち、ネットワークに参加するすべてのコンピューターが、同じブロックチェインのコピーを持つ。ブロックチェイン内の取引はネットワークにより「承認」されているとみなされ、二重消費の場合等、それらに照らして正しく検証できない取引は拒否される。

ビットコインでは、一度承認された取引が改竄されることを困難にするため、ブロックチェインへのブロックの追加にコストを設けている。具体的には、ブロックは数学的な方法で言わば《採掘》《発掘》(mining)されなければならないことになっており、そこに大きな計算パワーが必要になる。《採掘》は競争的プロセスである。

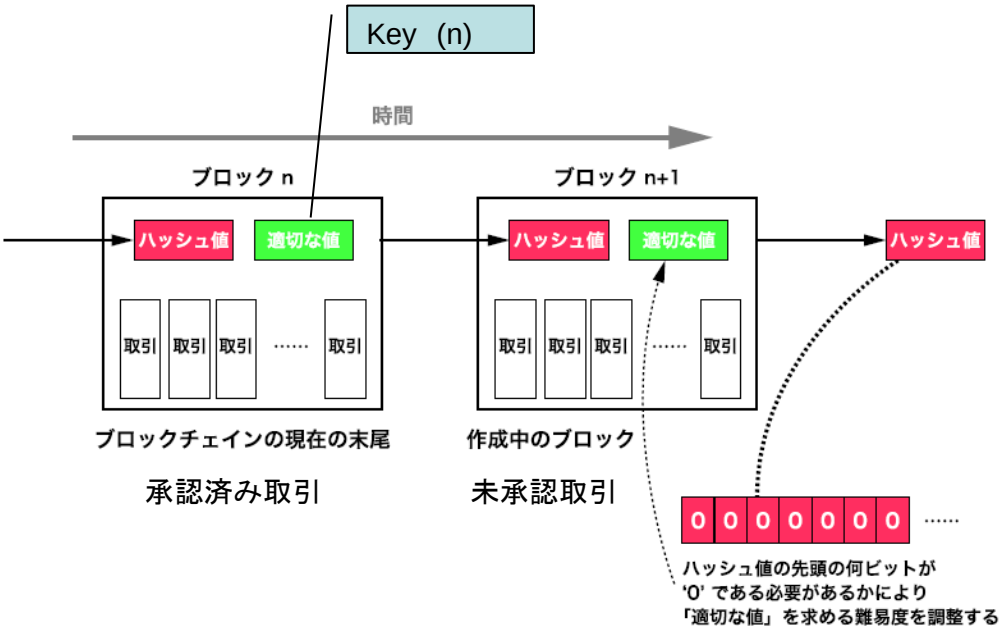


図 2: 二重消費や改竄の防止機構としてのブロックチェイン

バーチャル貨幣の謎

＜採掘作業の内容＞

ビットコインの取引は、各取引ごとにその履歴が記録され、さらに100～1000といった単位でブロックにまとめられ記録されていく。
このブロック毎にまとめられた取引記録に番号がつけられ、チェーン上につながって、取引記録全体として、保管されることになる。
検証作業とは、検証済みの記録に、（未承認の）新しい取引記録のブロックをつなげて追加していく作業である。
ブロックを元帳の末尾に正しくつなぐためには、つなぐための「キー」となる値を見つけ出さなければならない。
そのキーを見つけるには高速なコンピューターを使っても時間がかかるが、一旦そのキーがみつかれば、iphoneでも簡単にそれが正しいということを検証でき、ビットコインの参加者はだれもが、それが正当な取引であることを確認できる仕組みとなっている。

採掘とは、具体的には、この「Key」の値を見つけることである。
具体的には、承認したい取引の記録（ブロック）がある。これをブロックn+1とする。そして、この取引の元帳の最後に記録されている取引ブロックをブロックnとする。

まず、ブロックnの記録をハッシュ値に置き直してHnを求め、これと、「Key」の2つの値をさらにハッシュ関数に入れて、ハッシュ値Hn+1を得る。
そして、このHn+1 の値の先頭に0の値が32個並べばそのブロックをつないでいいという決まりになっている。この数値になるようなKeyn+1を探すのが採掘の作業である。
ハッシュ値をつくって、先頭にゼロが32個ならぶというのは、とんでもなく低い確率であるが、それができるまで、ひたすらKeyn+1の値をランダムにつくって、ハッシュ関数にいれて、ゼロが32個並ぶかどうかを計算していく。（難しい計算ではなく、ひたすら単位数字を1つ1つあてはめていくだけらしい）

これが採掘者が実際にやっていることである。そして、適切なkeyの値が得られたら、それが正解。そして、それを見つけた人（毎ブロック先着1名のみ）は、検証作業をしたご褒美・報酬として新しいビットコインをもらえるのである。現状では、25ビットコインが得られる。（約250万円）

採掘するには、無料で提供されている採掘ソフトを使えばだれでも参加可能である。しかし、とにかく早い者勝ちなので、より高速で計算できるコンピューターを使ったほうが有利になる。ビットコインが注目されるようになってからは、パソコンショップで売っているようなパソコンではとても勝ち目がない状況になっている。採掘専用で作られたコンピューターが高値で取引されたりしており、かなり高性能化されたコンピュータを使用しない限りビットコインを獲得することができなくなっている。また、このようなコンピューターを使用するためには電気代だけでも採算が合わないという状況である。そこで、共同で採掘するような会社も設立されて、参加者のコンピュータを動員して採掘し、採掘したビットコインを分配することをビジネスにしている。

バーチャル貨幣の謎

では、この採掘はなぜ行われているのであろうか？

この採掘作業こそが、ビットコインの二重消費を防いでいるシステムなのである。
もし悪意のある者が、取引記録を改ざんしようとした場合、或いは、二重に発行して別の取引記録を作成したような場合、過去の取引記録もすべてその数値に辻褄があるようにすべて改竄しなければならない。しかも、Keyは連結しているので改ざんした部分以降のKeyを全部改竄しないといけない。そのような作業と、世界中のコンピューターで正しい値を見つけ出す作業と競争して、それよりも早く実行しなければいけないのである。採掘作業は10分に1回行われているので実質的には、誰かが改ざんすることは、世界中のコンピューターを支配でもしない限り無理なのである。
これが、ビットコインの安全を担保する仕組みの核となっている。

③P2P方式
そして、この監視を可能にしているのが、P2Pというシステム。P2Pというのは、ネットワークにつながったコンピューター同士で直接データをやり取りし、受け取ったデータをさらに次のコンピューターに渡すというバケツリレーのような通信方式のことをいう。

P2Pといえば、Winnyというファイル交換ソフトが有名である。Winnyでは、まずWinnyがインストールされているコンピュータで共有されているファイルの一覧が次々、バケツリレーされていく。そして、途中でリレーしているコンピュータにもそのデータを残していくのである。その結果、ファイルが分散して保存されることになり、誰が削除しても他のパソコンに保存されているので理論上は永遠に保存されることになる。
ビットコインはこの特徴を生かしてすべての取引履歴を残していくのである。

ビットコインの取引が記録された帳簿データは、ビットコインを利用しているパソコンすべてにコピーされる。新しい取引が発生すると、帳簿に新たに追加するために、複数のコンピュータからチェックが入り、確認されれば新たに記述されていく。ビットコインで取引すると、取引完了までに10分ほど要するのだが、この時間で確認作業が行われているのである。（採掘時間10分とはこのことをいっているのである）

このように、取引が検証されて、過去のデータと一緒にして改竄されないようにし、さらに、P2Pの技術で世界中にコピーされていることで、ビットコインは管理されている。だれが判断しているのではなく、すべて数学的に証明できる数字として管理されていることでビットコインを担保している。

これがビットコインの仕組みである。

バーチャル貨幣の謎

用語解説：P2P

ピアトゥピアまたは**ピアツーピア**（peer to peer）とは、ネットワーク上で対等な関係（Peer、ピア）にある端末間を相互に直接接続し、データを送受信する通信方式、通信モデル、あるいは、通信技術の一分野を指す。**P2P**と略記することが多い。
なお近年、特に匿名ユーザーによるインターネット上のファイル共有を目的に、P2P技術を応用して作成されたソフトウェアが社会的に注目を浴びている（Winnyなど）。

P2Pは、ネットワークに接続されたコンピューター同士が端末装置として対等の立場、機能で直接通信するものである。P2P通信の一例としては、インターネットに接続した一般ユーザーの複数パソコン同士が互いのIPアドレスを呼び合う直接通信が挙げられる。

P2Pに対置される用語として、クライアント・サーバー方式がある。クライアント-サーバ方式では、ネットワークに接続されたコンピューターに対し、クライアントとサーバに立場、機能を分離していて、典型的には多数のクライアントに対してサーバーが一つである。クライアントはサーバーとだけ通信でき、あるクライアントが他のクライアントと通信するにはサーバーを介す必要がある。

クライアント-サーバ方式では、クライアント数が非常に多くなると、サーバおよびそれにつながる回線に負荷が集中するのに対して、Peer to Peer方式は、端末数が膨大になっても特定端末へのアクセス集中が発生しづらいという特徴があるため、ここ数年、商用的にも注目を集めており、特にIP電話や動画配信サービスなどへの応用例が増えてきている。

P2P型ネットワーク

コンピューター同士が対等に通信を行うのが特徴である。

クライアント・サーバー型ネットワーク

サーバー（図中央）とクライアントは一対一の通信を行うのが特徴である。

バーチャル貨幣の謎

④ビットコインの上限

ビットコインは、永遠に生成されるのではなく、6,929,999番目のブロックが記帳されるときが最後になるように設計されている。
なぜ6,929,999なのか？それは設計者が決めた仕様としか言いようがない。
6,929,999番目のブロックを記帳するまで、採掘が行われ続けるが、報酬はだんだんと減っていく仕組みになっている。最初の210,000ブロックまでは、1ブロックごとに、50ビットコインが生成されて採掘した人に与えられる。
そして、210,000ブロックが終わり、210,0001ブロック目から、420,000ブロックまでの人に対しては、25ビットコインが与えられ、次の420,001ブロックから640,000ブロックまでは12.5ビットコインというように210,000ブロック毎に、1/2になっていく仕組みとなっている。
時間がたつにつれてどんどん採掘からえ得られるビットコインが減っていくような仕様である。

1ブロック毎に50コインからはじめて、210,000ブロックごとに半減し、6,929,999番目のブロックが最後ということは、生成されるビットコインの総量は、約2100万枚となる。これがビットコインの発行上限である。
2月11日現在、発行されているビットコインは、285282ブロック。これを数量に計算すると、210,000までが50BTC、それ以降が25BTCなので、
210,000　X 50　+ 85,282　X　25 = 12,632,050　これが現在のビットコインの総発行量となる。
では、6,929,999番目の記帳が終わるのはいつになるのだろうか。
10分で、1ブロックが記帳・承認されるので、これを計算すると、

6,929,999 ブロック（総量）＊10 分　= 約132年

ビットコインの発行は、2009年から始まっているので、2141年頃、最後の6,929,999番目のブロックが記帳されて、最後のビットコインが発行されるということになる。

⑤その他の仕組み

ビットコインでは、システムをより実用的にするために、他にも幾つかの興味深いアイデアが採用されている。
ビットコインの設計では、BTCの寿命は永遠であり、秘密鍵の損失等の理由でコインが実質的に無効とならない限り、取引の履歴は伸張し続ける。ネットワーク内でデータが際限なく増え続けることを避けるため、参照されなくなった過去の取引データを適宜、破棄できるようにブロックのデータ構造が工夫されている。

さて、ビットコインのシステム的な仕組みが少しでも分って頂いたであろうか？
冒頭で申しあげたとおり、私自身、このシステムをすべて理解しているわけではない。しかし、全く知識のなかった時のビットコインに対する根拠のない疑念は少し晴れたように思う。
このビットコインが今後通貨として有効に流通するかの議論は次回にするとして、金融の専門機関（日銀やFRBなども含む）も研究・調査し注目している理由は理解できた。

次回は、1. ビットコインの流通の仕組み・実態、2. ビットコインの価値、3. ビットコインの問題点について書いてみたい。

Market Flash

イエレン・新FRB議長

2月から新たに米連邦準備制度理事会（FRB)の議長に就任したジャネット・イエレン女史をご紹介する。
米国での金融政策を一手に握る重要人物であり、彼女の一言一言にマーケットは耳を澄ませている。

ジャネット・イエレンは、ニューヨーク州ブルックリン生まれのアメリカ合衆国の経済学者である。現在、連邦準備制度理事会の副議長である。1997年から1999年にはビル・クリントンの大統領経済諮問委員会委員長となり、さらに2004年からはサンフランシスコ連邦準備銀行の議長となった。

＜1月31日CNN記事より以下抜粋＞
任期切れとなるバーナンキ現議長の後任として、来月からFRB史上初の女性議長が世界に多大な影響力を持つ中央銀行を率いることになる。そんなイエレン氏にまつわる知られざる5つの顔を紹介する。

1. 豊富な経験の裏付け

イエレン氏は米ニューヨーク・ブルックリンの生まれの67歳。学者としてキャリアを築いてきたが、公共政策の実務家としての豊富な経験も併せ持つ。オバマ大統領は報道陣に対し昨年10月、「彼女はタフな指導者であり、その手腕は実証済みだ」「ジャネットこそ、この役割にふさわしい」「彼女は10年以上にわたってFRBを指揮する立場にいる」と評した。
イエレン氏は、米ブラウン大経済学部を最優秀の成績で卒業、続いて米エール大で学び、1971年に博士号を取得している。
米ハーバード大、英ロンドン大学経済政治学院（LSE）などで教壇に立った後、米カリフォルニア大バークレー校のハース・ビジネススクールで26年間にわたり教授職を務めた。

2. 経済学一家

家庭も経済学との結びつきが強い。夫のジョージ・アカロフ氏も学者であり、ノーベル経済学賞を受賞している。両氏は77年、共にFRBで働いていた時に出会った。息子のロバート氏も現在、英ウォリック大経済学部で助教を務めている。

3. コミュニケーション力が鍵

イエレン氏は97年、当時のクリントン米大統領に指名され、大統領経済諮問委員会の委員長に就任した。クリントン氏は就任に際して、「彼女は一流の著述家であり思想家だ。我が国のために尽力してくれるだろう」と述べた。
今日では経済政策について語ることが多いイエレン氏だが、高校時代には学生新聞「パイロット」紙の編集長を務めていた。米紙ニューヨーク・タイムズによると、同校では新聞編集者が卒業生総代にインタビューするのが伝統で、63年に総代となったイエレン氏は自己インタビューを敢行している。

4. 狭い金融業界

イエレン氏とならぶ有力候補として名前が取り沙汰されたラリー・サマーズ元財務長官。イエレン氏は76年、学生だったサマーズ氏にマクロ経済学を教えたことがある。今回の次期FRB議長選びをめぐっては、報道が過熱する中、サマーズ氏自ら指名選考から外してほしいと願い出た。
イエレン氏の指名に向け、300人あまりが同氏を次期議長に推す公開書簡に署名、オバマ大統領に送付していた。同氏の指名は市場関係者やエコノミストによって広く歓迎された。

5. 2歩先を読む

オバマ大統領はイエレン氏を正式指名する際、その判断力と市場の動きへの理解を称賛しつつ、「副議長として昨年、模範的な働きをしてくれた」「住宅市場バブルや金融セクターの行き過ぎ、景気後退のリスクについて、早い段階から警鐘を鳴らしていた」と指摘、同氏が予見していた経済問題の数々を列挙した。

Market Flash

～日本経済～

- 日本経済は着実に回復に向かっている
- 消費税増税前の駆け込み需要が顕在化
- 輸出の減少にも歯止めがかかりつつある

日本経済は回復している。個人消費は雇用環境の改善に加えて、消費税増税を前に駆け込み需要が徐々に顕在化し堅調に推移している。また、輸出は、欧米中の緩やかな回復と円安により緩やかに増加している。内需についてみれば、設備不足感の高まりなどから、設備投資は緩やかに増加が続くものとみられる。さらに、補正予算の実行により公共投資が本格化しつつあることも大きな後押しとなっている。

個人消費の動向をみると、11月の消費総合指数は前月比+0.8%の上昇。12月の小売業販売額は前月比▲1.1%と2か月ぶりに減少したが、10-12月期は前期比+1.5%と大きく増加している。1月の新車販売台数は、10-12月期平均+14.6%からさらに10.5%増加しており、増税前の駆け込み需要は1997年の消費税増税前を大幅に上回っている。
消費マインドも景気ウォッチャー調査では、冬のボーナスが増加する中で年末商戦が好調であって、高額品、自動車、家電を中心に売上が増加したことが指摘されている。
4月以降の消費税増税後は一時的にかなりの落ち込みが予想される。その後の回復については、今後の雇用・所得活況の改善次第ではないだろうか。まずは業績拡大が続く大企業の賃上げ動向に注目したい。

一方、輸出の動向を見てみよう。
11月の輸出数量は前年同月比+6.2%（10月は+4.4%）の増加となった。日銀発表の11月実質輸出は前月比+0.1%の増加となった。全体的には、回復の勢いには欠くものの、海外経済が持ち直すことで輸出の減少には歯止めがかかりつつある。
輸出数量について、地域的にみると、アジア向けが前年同月比+6.0%（10月は+2.0%）、米国向けは+2.9%（10月+5.3%）、EU向けは+0.4%（10月+8.0%）と各地域とも増加している。アジアの中では、中国向けが+20.0%と大幅に増加。用品別にみると、輸送用機器のほか、一般機械、化学製品、電気機器などが増加しており、回復が遅れていた一般機械や電気機器においても持ち直しの動きがみられる。

企業の生産活動はどうであろうか。
12月の鉱工業生産指数は前月比+1.1%（11月▲0.1%）と2か月ぶりに上昇した。汎用・生産用・業務用機械工業や建設関係の橋梁・鉄骨を含む金属製品工業が全体を押し上げた。
企業の収益状況も改善している。
上場企業の7割は2014年3月期で増収増益を見込めそうである。全体では売上高が前期比1割増え、経常利益は3割増となる見通しである。
設備投資についても緩やかに増加している。先行指標の機械受注は、12月で前月比▲15.7%と大きく下落したが、これは前月の大型案件の反動の影響が大きい。10～12月期でみると前期比+1.5%と3四半期連続で増加している。

こうした景気回復の基調が見えている一方で、日本の株式市場は年初から大きく下落している。
2月4日には、610円安の14,008円で取引を終えた。昨年末の16,291円から実に2,283円（14%）の下落である。これはまずは、年末の行き過ぎた過熱感からの下落でもあるが、そのきっかけとなったのは、米国FOMCによる「量的緩和縮小」である。これにより、ブラジル、アルゼンチン、トルコといった新興国から資金が流出し、各通貨が急落したことから、米国株式市場が326ドルの下落を示すなど動揺がみられたことが原因と考えられる。ただ、米国経済自体はしっかりとした回復を示してきており日経平均も14,000円を下値のめどと考えてもいいだろう。

2月15日現在

～米国経済～

- イエレン新議長はこれまでの政策継続を強調
- 大寒波の影響が製造業と個人消費に影響
- 雇用環境は引き続き順調に改善

2月から新しい米連邦準備理事会(FRB)議長となったイエレン議長の初の議会証言が注目された。
その場において、イエレン議長は冒頭で、「現在の米連邦公開市場委員会(FOMC)のアプローチを尊重すると強調したい」と発言し、雇用最大化に向けて証券購入など非伝統的手段を展開してきた路線を全面的に支持し、今後も踏襲すると宣言した。また、量的緩和縮小により新興国から資金が流出し、新興国通貨不安をもたらしているとのマーケットの見方に対して、新興国通貨不安の米国経済への影響は限定的とし、段階的な量的緩和縮小を継続するとの姿勢を示した。

また、米国経済に対する見方は、昨年後半に大幅に勢いを強め、第3四半期、第4四半期の成長率は、年換算平均で3.5%以上となり、前半より1.75%も高いペースで拡大していると指摘。雇用環境の改善も見られ失業率は量的緩和を始めてから1.5%も改善している。ただ、物価上昇率は未だに低い。金融政策においては、雇用情勢がさらに改善し、物価がFOMCの長期目標に向かって上昇していくようであれば、今後も量的緩和縮小を継続する可能性が高いとしながら、たとえQE3(債券購入による量的緩和)が終了したあとも相当の期間は非常に緩和的な政策を維持するのが適当であるという考えを強調した。

このようにイエレン議長は、米国経済に自信を持ちながらも更なる雇用環境の改善、物価上昇のために超低金利政策を継続していく姿勢である。
では、直近足元の米国経済の内容はどうであろうか。
年末、年始の大寒波の影響により、今年に入ってからの米国経済指標は予想を下回るものが多くなっているが、概ね良好な状態を維持している。

製造業の業況を示す製造業ISM指数は、1月は51.3と12月の57.0から5.7ポイント低下。昨年5月以来の低水準となった。市場予測の56.0も大きく下回っている。
また、1月の新車販売台数は前年同月比▲3.1%の減少の101万2582台となった。大きな市場を抱える東海岸や自動車産業が集結する五大湖周辺、南部を寒波が襲ったためである。各社とも供給能力が低下し法人向け販売が減少、且つ、消費地での寒波により人出が減少した。

1月の雇用統計では、非農業雇用者数は11.3万人の増加と前月から増加幅が拡大したものの市場予想の18万人を下回った。主因は、小売業で1.3万人の減少。年末商戦はまずまずであったものの大規模な販売促進により利益率が低下、そのため1月は雇用者数を大幅に削減したものとみられている。1月の失業率は0.1%低下の6.6%となっている。

2013年10-12月期の実質GDP成長率は、前期比年率3.2%と、2011年4-6月期から11期連続のプラス成長を維持した。
10-12月期のプラス成長の要因は個人消費にあった。継続的な雇用・所得環境の改善が個人消費を押し上げ米国経済を牽引しているのである。
2013年通年では、実質GDP成長率は、前年比+1.9%となり、2012年の+2.8%から鈍化したものの、2011年の伸び率を上回った。
2013年は、いわゆる「財政の崖」に伴う実質増税、3月からの強制的財政支出の削減、10月の一部連邦政府機関の封鎖など、政府・財政が年間を通して景気の足を引っ張る結果となった。
今年はその圧力が弱まるため、民需主導型の経済成長が続くものと思われる。

～欧州経済～

回復に勢いが・・・！

2014年に入り、ユーロ圏経済はやや勢いがで始めているようである。牽引役はやはりドイツではあるが、今まで懸念されていたイタリア、スペインといった南欧諸国でも製造業を中心に持ち直しを見せている。一方で、ユーロ圏第二位のフランスが以前として回復力に乏しく新たな病原とされている。

ドイツは、2013年の実質GDP成長率が前年比+0.4%となり、3年連続の減速となったが、第4四半期については前期比+0.25%と3期連続のプラス成長を維持した。また、スペインは、第4四半期の実質GDP成長率が前期比+0.3%と2期連続のプラス成長、イタリアでも10期ぶりのプラス成長になる可能性が強い。

2014年に入るとさらに回復ペースを早めているようである。成長率と関連性の高いユーロ圏合成PMIは、1月が53.2と2年半ぶりの高水準を記録。中でも、製造業のPMIの改善が目立っている(52.7➡53.9)

こうした中、フランスの景気低迷は変わらない。フランスの問題は、肥大化した公的部門、増大した財政赤字、過剰な規制とそれに伴う競争力の低下である。オランド大統領は、今年に入って「責任協定」という新たな政策を打ち出している。これは、2017年までに300億ユーロの企業の社会保障負担を軽減することで雇用コストを引き下げる。その財源を追加の歳出削減で賄うことで肥大化した公的セクターの縮小も狙うという政策である。企業の雇用創出の数値目標を課すことになっており、反対論も多く今後の議論の行方が注目される。

ユーロ圏は、景気底入れから回復基調に入りつつあり、今まで資金調達に難のあったアイルランド、ポルトガル、スペインなどが債券を発行して資金調達ができるようになってきている。ユーロ危機のリスクは今は減少してきていると言っていいであろう。

～中国経済～

7%台の高成長の維持

中国経済は、力強さにはかけるものの7%台の高成長を維持している。しかし、内部は解決しなければいけない問題が山積みである。その一つが、昨年末のレポートでも特集したシャドーバンキングである。今年に入って、具体的にある信託商品がデフォルトを起こすと噂され、短期金利が急上昇した。結局は、償還期限直前に元本償還を行うと発表され事なきを得た。「新たな投資家と合意に達した」と説明しており、詳細は不明。どうも政府が地方政府に対して圧力を掛け何らかの形でかいもどさせたというのがもっぱらの噂である。

シャドーバンキング商品の本格的なデフォルトは初となるため金融不安が懸念されていた。

これは、氷山の一角でしかなく、まさにシャドーバンキング崩壊の始まりではないかと懸念される。

中国経済全体は、7―9月期に底入れし、2013年の実質GDP成長率は、+7.6%と政府目標を達成した模様である。2014年の経済政策は、12月の中央経済工作会議において、「穏健な金融政策と積極的な財政政策を維持し、経済成長率は合理的な伸び(7.0%~7.5%程度)を維持させる」

という内容が採択された。

政府としては、2013年より経済成長が鈍化しても、住宅価格、不動産価格の高騰や地方政府の行き過ぎた成長率重視主義を是正しようとしている。

7.5%以上の成長を遂げても低成長と言われるのは潜在成長率を今までと同様に見ているからであり、潜在成長率が7%と見れは好景気である。政府もそのような見方をしており、そのため過熱気味の投資を抑えるべく金融政策を引き締め気味にコントロールしていると思われる。

中国経済を見る場合、今後は成長率そのものよりも、いろいろな歪(都市・農村問題、政治的腐敗、シャドーバンキングなど)がどのように、どの程度まで是正しようとしているか、その達成度合いに注目すべきであろう。