新時代の通貨
ビットコインを超えて

＜はじめに＞

2009 年スイスのダボス会議※1において、セキュリティ大手の代表によって衝撃的なスピーチが行われた。何しろインターネット上で1年間に1兆ドルもの盗難が発生しているという。これまでも巨額の被害が想定されてはいたが、具体的な数字が公表されたことはなかったので、世界に衝撃を与えた。筆者自身もある大使館から、このような発表があるということはその国の外交システムは安全ではないのではないかとの危惧から、このニュースを知らされたのである。調査の結果、

出典：BBC WEB ニュース

この国のシステムは極めてセキュリティレベルが低いことが分かったので、すぐ対策を提案させていただいた。

一般に、情報秘匿、秘密通信、遠隔認証など、およそコンピュータやネットワークを用いるシステムでは高度な暗号技術が使われている。適切に使われれば、ほぼ安全なシステムを構築できる。しかしながら、今日広く使用されている暗号技術は、その使用方法や実装方法が不適切なために、全くその機能を果たしていないことが多い。その結果、頻繁に情報漏えい事件が発生し、ほぼ毎日ニュースとして伝えられている。

インターネットでの例を見ると、昨年春頃、SSL※2（Secure Sockets Layer）の脆弱性が報道された。その後対策が取られたかのような報道があったが、根本的な解決ができないことは、暗号関係者の中では常識である。その基礎技術となっている公開鍵方式の実装に問題があるからだ。

また、暗号技術の 2010 年問題※3は記憶に新しいが、それまで安全とされていた Triple DES※4（Triple Data Encryption Standard）暗号や RSA 暗号※5（公開鍵方式の一種）の 1024 ビット長以下の暗号鍵が使用禁止とされた。過去において、暗号強度について、「現存のスーパーコンピュータでも解読に XX 万年かかるから安全である」かのように表現されることがあった。限られた並列処理のノイマン型コンピュータの時代にはある程度説得力があり、2010 年問題もこの文脈で提案され、より高度なアルゴリズムとより長い暗号鍵を使用することが新しい規格となった。しかしながら、理論的には何億倍の並列処理が可能な量子コンピュータ※6が実用化され始めた今日、「解読に XX 万年かかる」という理論はもはや通用しない。量子コンピュータを使えば、何十万年かかるどころか、数秒で解読できることになってしまうからである。幸い現時点の量子コンピュータの並列処理能力には限界があり、あと数年は従来の暗号方式でも安全かも知れない。

以上のような背景から、セキュリティの新しい枠組みが必要であることは明白であり、一日も早く新たな標準を確立しなければならない。国防、外交における新セキュリティの重要性は言うまでもなく、民間であっても、命を扱う医療業界や通貨を扱う金融業界においても、この新セキュリティが重要な役割を果たすであろう。インターネットを人間の身体に例えるなら、情報伝達は神経系、通貨の流れは循環器系（血液）と考えられる。新セキュリティは、情報を末梢神経まで確実に送り届ける働きを、そしてインターネット活動に必要な代替価値（通貨）を身体の隅々まで行き渡らせることを可能にし、ようやくインターネットが完成する。

＜新しい金融＞

近年、フィンテック※7（FinTech; Financial Technology）関連の話が新聞紙上を賑わせている。金融サービスの多くがインターネットを代表とするIT技術で変革を迫られているというニュースである。投資も貸付も資金調達もすべてネット上で行える時代となった。リテールバンキングはすべてインターネットに移行し、従来のリテールバンクは遠くない将来消滅するという説さえある。実際、シティバンクは来るべく時代を見据えて、リテールの切り離しを実行しつつあり、日本法人が三井住友銀行に売却されたのは記憶に新しい。最近では、ベンチャー企業だけではなく大手銀行も取り残されまいと取り組みを始めた。エコノミスト誌によると2014年だけで世界全体で1兆5千億円を超える投資が行われたという。そんな中で、金融業界が最も注目しているのは、「ビットコイン」であろう。今年に入って、金融庁が通貨としての法制の検討を始めたこともあり、日本銀行でさえも本格的調査、対策に乗り出している。

＜ビットコイン＞

ビットコインとは、公開鍵方式をベースとして電子データを通貨と見做すことをその本質とし、譲渡性のある通貨の正当な所有者を明確にするために、誰にどれだけのビットコインが発行され、誰から誰にいくら支払われたかという決済内容を記録する仕組みを持つ。実際には、ビットコインの世界で決められるある口座に、1億分の1ビットコインを最小単位として、その倍数のビットコインが発行される。さらに、ある口座から別の口座へ何ビットコイン動かしたかという取引記録をブロックチェーンと呼ばれる公開の台帳に記録することで、銀行ネットワークやSWIFT※8などを用いなくても、金融取引ができるとされる。その名前からビットコインは世界最初の「電子通貨（Electronic Currency）」と呼ばれることがある。一方、JRのSUICAに代表されるICカード等の媒体を使って、事前に支払った金額をこのカードを使って支払う少額支払いの仕組みがあるが、これも「電子マネー（Electronic Money）」と呼ばれている。実体を持つ媒体を使用しないで済むビットコインの方がより電子通貨の定義に近いが、実際は両社とも単なる決済システムに過ぎない。また、公開鍵方式とはいえ、暗号技術がベースになっているのでビットコインを世界最初の「Crypto Currency（暗号通貨）」と考える学者もいるが、「暗号化された情報そのものが通貨としての価値と機能を持つ」という暗号通貨の定義から考えると、取引記録を送信記録するだけのビットコインはこれに該当しないことは明らかである。

出典：IT PRO

ビットコインのソフトウエアはすべて公開されている。希望すれば誰でも使用できるので、オープンで民主的であるとされる。また、ブロックチェーン※9と呼ばれる台帳は希望者すべてで共有され、特定の権力者が独占するものではないので、非中央集権的と考えられている。これらの特徴がインターネットの思想に合致していることもあり、先端ネットユーザーに支持され、予想を超えたスピードで広まっている。近年ではアマゾンやデルコンピュータなどのネットショップでも、ビットコインを物品の購入に使用できる。すでにアルゼンチンではコンビニでもペソをビットコインに交換できる。また、もし紙幣が必要になった場合には、専用のATMでビットコインを紙幣に換金することもできる。

＜ビットコインの闇＞

2014年2月、当時世界最大のビットコイン取引所であったマウントゴックス社が114億円相当のビットコイ

ンが消失したと自己申告して破たんした。仏国籍の経営者とはいえ拠点が渋谷にあったため、日本ではそれ以降ビットコインは胡散臭い金融の仕組みと捉えられるようになり、先進国の中では、ビットコインの利用者が増えない稀有な国の１つとなっている。その後、この破たん劇は経営者の自作自演で、自身の儲けのために破たんさせたことが判明し、経営者は逮捕されている。

また、以前よりビットコインの従来通貨に対する交換価値は乱高下し、投機の対象とされることが多い。現在の交換価値は、1 ビットコインあたり 47,617 円であるが、一時は 121,521 円という時もあった。さらに、地下銀行や犯罪資金の洗浄に使われたなどの報告があり、最近では他人のコンピュータに感染させ、ビットコインを不正に犯罪者に発行させるマルウエアさえ見つかっており、感染被害は日本が最大で世界の 4 分の 1※１０を占める。

このように書くとビットコインの闇は深く、決してまともな仕組みではないと思われるかもしれないが、実際には、ビットコインそのものは単なる決済の道具であり、仕組みそのものが悪いわけではなく、従来のプリペイドカードやクレジットカード、電子マネーと大きな違いはない。むしろビットコインは他の決済手段に比較して、現時点ではより安全とさえいえる。

ビットコインは、2008 年に発表されたナカモトサトシという日本名の実在か否かさえ分からない著者の論文が元になっている。この論文を読むと新通貨のカンブリア紀とも考えられる 1990 年代の影響が見える。

1990 年代前半に、新時代のゴールドラッシュが突如巻き起こり、米国や英国を中心に新しい通貨の形が次から次に発表され、実用化され、そして淘汰されていった。当時筆者はある機関の調査依頼で 50 社以上の経営幹部の話を直接聞くことができた。彼らが中心に据えていたコンセプトが「電子通貨」であり、その周辺のコンセプトの一つが「電子決済」であった。当初、野心的な研究者のほとんどは、自分こそが本物の電子通貨の創造者になると意気込んでいたが、結局この金鉱脈を探し当てた者はいなかった。今から考えれば、当時の未完成の不完全な暗号技術を用いる故に、本当に安全な電子通貨は作れる由もなかったのである。一方、この狂騒状態を遠巻きに眺めていた研究者の間では、不完全な暗号技術しか存在しないという事実を受け入れて、プロトコルの工夫による新たな決済方法を提案した者がいた。中でも、Digi Cash 社※１１や Cyber Cash 社※１２などは、ネット上で使用できる新たな決済の仕組みを、National West Minster 銀行は、さらに通常の街中での使用をも視野に入れたモンデックスカード※１３の仕組みを提案した。それらはそれぞれ、その後改良を加えられ、他社に受け継がれて現在に至っている。また、公開鍵方式の考え方をそのまま素直に利用して、ネット上で決済する新たなプロトコルも提案された。当時公開鍵方式は、すでに脆弱性が指摘され、技術的には瀕死の状態にありながらも、代替手段がないということで広く使われていた。しかしながら、電子決済として使用するには、あまりにも脆弱過ぎ、いつの間にか忘れ去られることとなった。ビットコインはこの流れを汲む決済の仕組みで、故に当時指摘された脆弱性をすべて包含している。但し 10 年以上遅れて発表されただけに、ブロックチェーンなど、多少の工夫は見受けられる。特に不特定多数による記録保存を、Proof of Work※１４を行うことでセキュリティの 3 要素の 1 つである完全性を担保している点は他に例を見ない。

中央集権的な権威者が存在しなくても、約束事を担保できることを示したことの意義は大きい。公証人の代替サービスになると考える学者も存在する。しかしビットコインの最大の貢献は、これ自体は単なる決済手段に過ぎないものの、ビットコインという名前やマイニングというネーミングによって、近い将来本物の「電子通貨」が生まれる可能性を、多くの人々に予感させたことであろう。

＜新時代の通貨＞

通貨は価値の交換手段として、最初は特殊な形や材質を有する貝殻や石から始まり、中世末期のイタリアにおいて信用をベースにした紙幣が考案され、そして、現在、偽造も不正使用もできない、もっとも安全で使用方法や場所を問わない究極の通貨として、「Crypto Currency（暗号通貨）」が生まれようとしている。

暗号通貨は、暗号化された情報そのものが、蓄蔵、交換などの通貨としての価値を持ち、金属や紙、プラスティックといった媒体を全く必要としない。コンピュータ上またはインターネット上だけでも存在（保存）でき、ネット上での価値の交換にも使用できる。

この新通貨は、従来の通貨と同様に、今後各国政府または各国中央銀行によって発行されるものもあれば、民間団体によって発行されるものも出てくると考えられる。もしかしたらビットコインのように、インターネット上のコミュニティによって“非中央集権的に”発行され“民主的に”共同で運営されていくものも出てくるかもしれない。新通貨の詳細は現時点ではまだ何も決まっていない。従来の通貨の問題点を改善する為、暗号化された情報に、金額以外にも取引記録や有効期限などの情報を包含することができる。一定期間ごとに新札と交換することも可能である。変わったところでは、使用する場所によって価値が変わったり、一定期間使わない場合価値が変更される通貨さえ可能である。

もし、新通貨のカンブリア紀に完全な暗号技術が存在していたら、今頃私たちは暗号通貨の恩恵を受けていたかもしれない。しかし当時はまだそのような暗号技術は存在しなかった。

筆者は、このカンブリア紀の頃より、暗号技術の完成が、インターネット時代の最重要技術になると認識し、開発を進めてきた。その結果、21 世紀に入ってすぐ従来の暗号技術の問題点を解決し、その最初の応用製品として、2015 年に暗号通貨そのものの開発に成功した。今秋には最初の製品とサービスを日本で始めるべく準備中である。

※1. ダボス会議（世界経済フォーラム）

ビジネス、政治、アカデミアや、その他の社会におけるリーダーたちが連携することにより、世界・地域・産業のアジェンダを形成し、世界情勢の改善に取り組む、独立した国際機関として、ジュネーブに本部を置きスイスの非営利財団の形態を有している。1971 年にスイスの経済学者クラウス・シュワブにより設立された。スイスのダボスで開催される年次総会が特によく知られており、約 2500 名の選ばれた知識人やジャーナリスト、多国籍企業経営者や国際的な政治指導者などのトップリーダーが一堂に会し、健康や環境等を含めた世界が直面する重大な問題について議論する場となっている。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/世界経済フォーラム）

※2. SSL

インターネットなどの TCP/IP ネットワークでデータを暗号化して送受信するプロトコル（通信手順）の一つ。データを送受信する一対の機器間で通信を暗号化し、中継装置などネットワーク上の他の機器による成りすましやデータの盗み見、改竄などを防ぐことができる。SSL は公開鍵証明書による通信相手の認証（一般的にはサーバの認証）と、共通鍵暗号（秘密鍵暗号）による通信の暗号化、ハッシュ関数による改竄検知などの機能を提供する。Web アクセスに使われる HTTP と組み合わせ、Web サイトで認証情報や個人情報、決済情報などの送受信を安全に行う手段として広く普及している。

（出典：IT 用語辞典 e-words　http://e-words.jp/w/SSL.html）

※3. 2010 年問題

「暗号の 2010 年問題」とは，暗号技術の寿命が尽きることで起こる問題のこと。米国政府の使用する暗号技術を決めている米国国立標準技術研究所（NIST）が，弱い暗号技術の使用を 2010 年に停止する方針を発表したことがきっかけで注目を集めている。

現在使われている暗号技術は，1)暗号鍵が十分長い，2)解読の近道がない――ようにして，現実的な時間で解けなくすることで安全性

を確保している。しかし，暗号の解読にかかる時間は，コンピュータの性能向上によって短くなる。また，暗号技術に欠陥が見つかり，解読の近道が見つかってしまうこともある。例えば鍵の長さ 112 ビットの 3DES は，条件によっては 56 ビットの鍵と同じ程度の強度しかないことがわかっている。世界最高速のコンピュータなら解読できてしまう可能性がある。

NIST の方針によって使用停止になる暗号技術は，「ぜい弱性のない共通鍵暗号方式の鍵の長さに換算して，80 ビット以下の強度しかない暗号技術」というもの。例えば，鍵の長さ 112 ビットの 3DES のほか，公開鍵暗号では鍵の長さ 1024 ビットの RSA，ハッシュ関数では SHA-1 などである。Web アクセスや VPN 通信，認証などで一般に広く使われている暗号が含まれている。これらの暗号技術は 2010 年までに，例えば鍵の長さ 112 ビットの 3DES は AES(Advanced Encryption Standard)といった，より安全な暗号技術に切り替えることになっている。

（出典：IT PRO　http://itpro.nikkeibp.co.jp/article/Keyword/20090119/323069/?rt=no）

※4. DES 暗号

アメリカ合衆国の旧国家暗号規格、もしくはその規格で規格化されている共通鍵暗号である。ブロック暗号の一種であり、1976 年国立標準局（NBS）がアメリカ合衆国の公式連邦情報処理標準（FIPS）として採用し、その後国際的に広く使われた。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/Data_Encryption_Standard）

※5. RSA 暗号

RSA 暗号とは、桁数が大きい合成数の素因数分解問題が困難であることを安全性の根拠とした公開鍵暗号の一つである。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/RSA 暗号）

※6. 量子コンピュータ

量子力学の原理を情報処理に応用するコンピュータ。極微細な素粒子の世界で見られる状態の重ね合わせを利用して、超並列的に計算を実行するコンピュータである。

原子の内部構造のような極めて微細なスケールの世界は、物体に働く古典力学とは原理の異なる量子力学が支配している。素粒子の状態を表す属性は、複数の状態が同時に実現している「重ね合わせ」という状態にある。これを「量子ビット」（qubit：quantum bit）と呼ばれる情報の表現として利用することにより、並列的な計算を実現するというのが量子コンピュータの基本的な原理である。

（出典：IT 用語辞典 e-words　http://e-words.jp/w/量子コンピュータ.html）

※7. フィンテック

Finance と Technology を掛け合わせた造語で、メガバンクやカード会社等の金融機関やその情報子会社、金融系システムインテグレーター、金融×IT 分野で活躍するスタートアップなどから生まれた新しい金融サービスを意味する。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/Fintech）

※8. SWIFT

Society for Worldwide Interbank Financial Telecommunication の略称。金融機関間の通信ネットワークを運営する非営利団体。国際銀行間の送金や決済をおこなうためのネットワーク。7,000 以上の金融機関向けに機密メッセージの配信をおこなっている。

（出典：野村證券　ttps://www.nomura.co.jp/terms/japan/su/swift.html）

※9. ブロックチェーン

暗号化と分散ネットワーク技術を活用し、書き換えや改ざんが不可能な形で何らかの記録（例えば元帳／台帳など）を共有する仕組み。

（出典：@IT　http://www.atmarkit.co.jp/ait/articles/1601/21/news024.html）

※10. ビットコイン被害

ビットコインの「発掘（マイニング）」をユーザの PC 上で無断で行う、ビットコイン発掘不正プログラムの被害が世界的に確認されている。この感染被害は特に日本とアメリカで多いことも確認できた。日本が全体の約 1/4 にあたる 24%で最も多く、アメリカは 21%の感染があり、併せて全世界の感染台数の 4 割以上を占める。

（出典：トレンドマイクロ　http://blog.trendmicro.co.jp/archives/8271）

※11. Digi Cash 社

電子決済システムの権威、デビッド・チョーム博士によって創立され、電子キャッシュ「e キャッシュ」を提供しており、1995 年 10 月 23 日、アメリカのマークトゥエイン銀行で初めて採用された。この「e キャッシュ」は RSA 社の「公開鍵暗号方式」と呼ばれる暗号技術をベースとしていた。ビットコインとは異なり銀行が秘密鍵で署名するシステムであった。

（出典：InterntRoad 等から要約、加筆）

※12. Cyber Cash 社

1994 年に設立され、インターネット上での決済に関する技術とサービスを提供していた。このサービスは、クレジットカード情報を暗号化するウォレット（電子財布）プログラム（＝「サイバーキャッシュ・ウォレット」）と暗号化したカード情報である「サイバーコイン」を小売店に送信し、さらに小売店からサイバーキャッシュ社のサーバーに送信され、金融機関に利用者の確認を要求して結果を小売店に返すというもので、利用者にとっての使い勝手は現金に近いものであった。

（出典：InterntRoad 等から要約）

※13. モンデックスカード

ナショナル・ウエストミンスター銀行とモンデックス・インターナショナル社が 1990 年に開発した。IC カードの中に貨幣価値のデータを記録し、取引時にそのデータを増減させるため、オフラインでの取り扱いが可能。 IC カードに記録される情報は、貨幣価値だけなので匿名性が保持されている。その後、モンデックス・インターナショナルはマスターカード・インターナショナルに買収された。ナショナル・ウエストミンスター銀行は RBS の子会社となった。

（出典：Wikipedia　https://ja.wikipedia.org/wiki/モンデックス）

※14. Proof of Work

ビットコイン取引の未承認ブロックを承認する一連の作業で、仮想通貨としての信頼性を担保している。

ブロックを承認するには相応の計算量が必要で、悪意を持ったものがブロックチェーンの記録を改ざんすることを防ぐことが出来る。

（出典：bitbank から要約　https://bitcoinbank.co.jp/about/mechanism2/proof_of_work.html）