ビットコインと暗号（TBSラジオ「日本全国8時です」2014．2．20）

今月初め、江戸時代後期から明治時代前期の京都に開設されていた「山本読書室」という名前の私塾の土蔵を調査した結果、幕末から明治にかけての重要な文書が数万点発見されたというニュースがありました。

その中で話題になったのが、明治政府ナンバー２の右大臣で、明治４年から２年近く欧米を視察した「岩倉使節団」の特命全権大使として活躍した岩倉具視が西南戦争の時期に使用した暗号表が出てきたということでした。

これは二重の円盤で、それぞれ周囲にカタカナが書いてあり、内側の円盤の文字はイロハニホヘトの順番に文字が並んでいますが、外側の円盤には一定の規則のない順番で文字が並んでいる道具です。

この表を使って内側の円盤に書かれている「イロハ」を外側の円盤の対応する場所にある文字に変換すると「ヤクノ」になりますので、この「ヤクノ」を文書にして送れば、途中で盗まれても内容は分からないということになります。

岩倉具視が当時、大阪に居た大久保利通に送った暗号文もあるそうですが、受取った大久保利道は同じ暗号表の外側の円盤で「ヤクノ」を探せば、内側の円盤を見て「イロハ」だということが分かるという仕組です。

しかし、毎回同じ規則で変換していると、何通かの文書が盗まれたときに類推されてしまいますので内側の円盤を回転させて５種類の組合せで変換できる工夫がしてあります。

明治初期に政府の要人が暗号表を使っていたことは興味がありますが、失礼ながら暗号技術としては初歩的な方法で、２０００年前にシーザーも使っていた換字式暗号といわれるものです。

それ以後、暗号はそれほど進歩しませんでしたが、１９世紀末に無線通信が発明され、暗号技術が飛躍しました。

モールス符号で無線送信している情報は周辺で自由に受信されてしまうので、秘密の通信ができなくなってしまったのです。

そこで文章を複雑な規則で原型を留めないように変形し、解読の鍵を持った人だけが最初の文章に戻せるようにする「共通鍵暗号」技術が登場しました。

ところが問題は、その鍵を盗まれてしまうと筒抜けになってしまうことです。実際、ドイツが第二次世界大戦で使った「エニグマ」という暗号装置は難攻不落でしたが、その鍵となる「コードブック」が連合軍の手に落ちて情報が筒抜けになってしまったという事例があります。

ところが次にコンピュータが登場して、様々な鍵を高速で試してみることができるようになり、「共通鍵暗号」は十分ではないということになり、それを防ぐために「公

開鍵暗号」といわれる技術が登場し、現状では難攻不落といってもいい状態になりました。
　これは受信する立場の人が２個の鍵を用意し、一つの鍵はだれにも公開し、もう一つの鍵は自分しか知らない状態にします。
　送る側の人は文書を公開されている鍵で暗号にして送るのですが、公開された鍵だけでは開けることがでず、受取った人は自分だけ持っている鍵で文章を元に戻すという仕組です。
　どのくらい難攻不落かというと、現在の「公開鍵暗号」の鍵には数百桁の素数が使われますが、仮にスーパーコンピュータで片端から試して見ようとすると、１００分の１秒で一連の数字を試すことが出来たとしても、１の後に０が１４０個並んだほどの年数がかかるほどの安全です。

　この先端の暗号技術を使って世界規模で取引をしているのが最近話題の「ビットコイン」です。
　ビットコインは番組でも断片的に紹介されているようなので、要点だけ説明しますと、紙幣や硬貨などの実体はなくインターネットの内部の情報しか存在しない仮想通貨といわれるものですが、実際に送金、買物、支払もできる通貨です。
　しかし、一般の通貨や電子マネーのように価値を保証する政府や企業が存在する訳ではなく、様々なコンピュータの中に分散して記録があるだけという、これまでの通貨に慣れた人にとっては極めて頼りない存在です。
　しかも情報として記録されているだけであれば、誰かが記録を書き換えたり消したりすれば混乱になるのですが、その保護は「公開鍵暗号」に依存しています。

　「ビットコイン」は今週に『ニューズウィーク』も特集を組んでいるほど話題になっていますが、現在、議論されているのは、これが通貨、電子マネーに次ぐ第三の通貨になるかという問題です。
　これまでも仮想通貨といわれる貨幣は何度も登場しましたし、現在でも「ライトコイン」「ネームコイン」「ピアコイン」「プライムコイン」「クオークコイン」「ワールドコイン」など、林立状態です。
　これらに共通する問題はいくつかありますが、まず高度な暗号を解くことによって送金や取引が成立するので、時間がかかることです。
　「ビットコイン」の場合、１回の取引に丸１日かかることもありますし、世界でまだ２万店程度しかないビットコインで支払うことの出来る店頭で支払のために情報を提示すると、ビットコインであるかを確認するのに１時間近くかかることもあるようです。

　一般の通貨は金やドルに交換できるという建前で価値が保証されていますが、仮想通貨は供給量が有限であるということで価値を維持する仕組です。

これには２つの問題があり、先程紹介したように、次々と仮想通貨が登場することによって供給量が自在に増大していくとわかれば、一気に価値が下落してしまうことになります。

さらに供給量が有限の通貨が大規模に普及するようになれば、経済が発展していくときに足枷になるという心配もあります。

そして多くの人が疑心暗鬼なのは、このような国家の保証のない通貨は１６世紀のオランダのチューリップバブル以来、すべて破綻しており、ビットコインも同じ道を辿るのではないかということです。

しかし、通貨ではありませんが、これまで政府や大企業の支配を脱却して成功した技術があります。インターネットです。

この技術が登場したとき、電話網のように政府やそれに匹敵する大企業が運営するシステムと違い、小さな企業が細切れで運営し、アドレスの割り振りも民間団体がおこなう通信について、多くの学者が反対しました。

しかし、結果としてインターネットなしの世界は想像できない社会になっています。

そのような事例を考えれば、ビットコインや類似の仮想通貨もまったくの幻想と言えないかも知れません。