Blockchain の真実と新しい暗号通貨
-後編-

＜終わりの始まり＞

前編でビットコインが通貨として不完全であること、そしてその技術基盤である Blockchain についても公開鍵方式を応用しているがゆえに構造的脆弱性を内包していることを示した。実際 Blockchain に関する数多くの事件は、Blockchain そのものではなく、その外部で起こっている。特に公開鍵をアカウント番号に見立てる仕組は、なりすましや情報改竄の直接の原因となっている。ビットコイン論文の著者（Satoshi Nakamoto）は取引の匿名性を保つため、できる限り頻繁にアカウント番号を変更すること推奨しているが、アカウント番号が都度変わるのではなりすましをし易くするだけであり、セキュリティの観点からはむしろ危険である。これだけでもとても実用に耐える仕組みでないことは明白だが、最近は絶対に安全だと考えられていた Blockchain そのものの構造的欠陥も指摘されはじめた。Blockchain の外部だけでなく内部も問題だというのである。実は Blockchain の仕組は取引記録の繋がりである Chain が分岐する可能性を持っており、事実、ビットコイン以外の用途で実用されていた Blockchain では過去に何度も分裂した例があるが、昨今、ビットコインの Blockchain でも分裂の危機が迫っていると言われている。ビットコインの Blockchain を構成する Block には取引記録が書き込まれるが、過去においてはビットコインの取引数が比較的少なく、すべての取引記録を新たな Block に書き込むことが可能であった。しかし、ビットコインの普及が進むにつれて取引数が増大したため、現在においては、すべての取引記録を書き込むには Block の大きさが小さ過ぎるという状況になっている。したがって、Block の大きさを拡大する等の新たなルール改正を近日中に行わなければ、ビットコインの仕組みが破綻しかねない状況になりつつある。実際、取引記録を Blockchain に追加される新規の Block に書き込ませるための手数料が高くなりすぎて使いにくくなっており、手数料を少なくすると取引の完了までに数日間を要する事態となっている。ここで問題となるのが、新たなルール改正を行えるかということである。ブロックチェーンの仕組みでは中央集権的なルール決定者がいないことが利点と捉えられているが、中央集権的なルール決定者がいないということは、利害の対立するコミュニティ内でのルール改正のコンセンサスを得ることが極めて難しいということを意味する。コミュニティの参加者が満場一致で新たなルールを決定できなかった場合には、Blockchain は分裂してそれ以降は分岐した複数の Blockchain が独立して存在することになる。事実多くの専門家はビットコインの Blockchain の分裂[※1] を予測している。このような Blockchain の分裂は、ビットコインの Blockchain の場合のように Block の大きさの変更のみに起因して生じるのではなく、Blockchain を運用する場合における何らかのルール変更に起因して生じ得る。Blockchain の運用を続けると、どこかのタイミングで、システムの更新が必ず必要になる。つまりそのようなタイミングで Blockchain は分裂の危機を迎え得るのであるから、分裂は Blockchain が構造的に持つ不可避な問題であるということができる。中央集権的なルール決定者を設けることのできるプライベート Blockchain ならこの問題を極小化できると唱える専門家も存在するが、反中央集権を目的として Blockchain を使うというのに、これでは本末転倒である。そもそも、データを改竄しないという点で信頼して中央集権体制を許容するのであれば、Blockchain を利用する意味がない。

Blockchain は、従来から指摘されていた Blockchain の外部の問題だけでなく、内部自体も構造的問題があることが徐々に認識され始めており、早急に Blockchain やそれを応用したビットコインの完全な代替技術を開発し普及することが望まれる。後述する通り、はるかにシンプルに、改竄のないデータベースを提供す

るという目的を達成することができる。

<暗号通貨とは>

前編で、通貨の基本機能は「決済手段」、「価値の保蔵手段」、「価値尺度」の３つであり、信用によって裏打ちされた債務として譲渡可能で、①取引記録や残高を記帳し、その台帳を根拠として発行する方法と、②台帳は持たず金属や紙などに特殊な方法で偽造できないようにして、モノ（貨幣）として発行する方法があるとした。また、ビットコインに代表される現在の“仮想通貨”は機能上通貨としては十分ではないことも説明させていただいた。

現在の仮想通貨は、概ね①のタイプであり、ビットコインやイーサリアムのように台帳上の取引記録から類推される数字を各ユーザーが所有する仮想通貨の量として扱う。前編で説明した通り、どちらも通貨の機能として不十分であり、また、公開鍵方式の証明書と公開台帳を使っているのでセキュリティに限界がある。ビットコイン系の通貨（アルトコイン）はすべてこのカテゴリーに入るが、すべて同様の課題を抱える。①の類似の例として、ペイパル※2やラインペイ※3など同じ事業者に口座を持つ者同士が、金額を収受する方法があるが、暗号技術は限定的にしか使われておらず、暗号通貨と呼べる水準には達していない。

他方、上記②の分類に属するものとして過去に存在し既に破綻したデジキャッシュなどが存在する。デジキャッシュは実際の通貨に基づいて発生された乱数のデータが仮想通貨としての本体であり、銀行が公開鍵方式で署名することでマネーオーダーのような性格を持たせられるとされた。しかし、そこで用いられている暗号技術は、銀行が上述の乱数に銀行自身もその乱数を知得できないような状態で署名を付すために用いられるに過ぎない。かかる技術において暗号化されるのは、そもそも意味を持たない乱数であり、また、署名が付された後の実際に仮想通貨として流通する乱数は、復号化された平文の状態で流通するのであるから、デジキャッシュにおける仮想通貨に暗号技術が使用されているといえるかどうかすら疑義が残る。②の例として、チェック（小切手）のように支払元がもつ暗号鍵で、受取銀行名、決済口座情報と決済金額を暗号化して支払先に渡し、これを受け取った支払先が、別途支払元から受け取った暗号鍵とともに、この“暗号通貨”を受取銀行に持ち込み、決済する方法が考えられる。この場合、暗号通貨の改竄対策に加えて、暗号鍵を持っている人だけが決済できるので、この暗号鍵の授受と管理が重要である。この考え方を基礎として、プリペイド方式で支払済みの金額に相当する乱数を通貨として扱えるように工夫して実用化されているものも存在するが、暗号技術は用いておらず極めて脆弱な仕組である。いずれの方法も、完全暗号を使うことが必須であり、いまだ実用的な暗号通貨と呼べるようなものは存在しない。

このほか、プリペイドの金額をプラスチックカードに記録し、少額決済に使うモンデックスやフェリカ※4（FeliCa）などの仕組みもある。フェリカはソニーが開発した電子カードで、簡単に内容を読み取ったり書き換えたりできないよう暗号化されているが、取引記録や残高を、サーバーだけではなくカードに記録する仕組みであり、“仮想通貨”というよりも“電子通貨”として認識されている。尚、フェリカの情報はカード読取機を介してやり取りする。したがって、読取機が設置してある場所でしか使用できず、読取機を持たない個人のネットショッピングなどでは使用できない。

本来暗号通貨は、暗号技術を用いて通貨に必要な情報を暗号化した譲渡可能な債務と定義されるべきであろう。そのように定義される暗号通貨も、①取引記録や残高に暗号を使う台帳方式と、②価値を暗号技術を使い何らかの偽造困難なモノとして発行する２つの方法が考えられる。しかし、いずれにしても現在までのところ、充分に暗号技術を活用した安全な暗号通貨は無かったと言ってよい。

以下、①と②の暗号通貨を現実的に実現する方法について詳述する。

＜新しい暗号通貨（クリプトカレンシー）＞

暗号通貨の②の種類の新しい暗号通貨である“クリプトカレンシー”は、発行者情報や価値情報を直接完全暗号化し、暗号化後の記号列を暗号貨幣とする。さらに、信用情報、使用条件、利息、期限などの条件も合わせて暗号化することで、様々な機能を持つ暗号貨幣を作ることができる。この暗号貨幣は、人類の歴史の中で使用されてきた金属貨幣、紙幣に続く、貨幣の最終形とも考えられる。完全な暗号技術※5を使用することで、改竄、偽造、偽使用も防止する。また、記号列であり媒体を問わないので、電子通貨のケースが多いが、金属に刻印されたり、紙幣に印刷されたりして使用されることも可能である。そして、記号列という実体を持つので、実体のある貨幣として保蔵に適することも特徴の一つである。

クリプトカレンシーは、金属や紙の貨幣をベースとした通貨と同様、国家の信用をベースにした法定通貨としても、他の法定通貨との兌換券としても発行され得るが、香港の法定紙幣のように、銀行やグローバル企業などの発行者または発行グループの信用で発行されてもよい。また信用の保証として、金銀などの貴金属のほか、資源価値を担保として、その兌換性による信用を利用して発行されることも考えられる。

現在の通貨のほとんどは、予め発行量を決めて発行し、一般には国或いは中央銀行が、貨幣を保管・管理しながら市場に流通させるが、クリプトカレンシーでは、予め発行するものに加えて、クリプトカレンシーの使用者が使用の度に発行する“ユーザー発行貨幣”を実現できるという特徴も持つ。つまり、中央集権的な存在だけでなく、誰でもが貨幣としてのクリプトカレンシーを発行できるようなシステムを構築することが可能である。その際、従来のパーソナルチェック同様、個人の預金、プリペイド残額や信用を担保として発行される。尚、世界で１兆ドルを超えるとされる盗難や偽使用の心配なしに、それぞれ従来のデビットカード、プリペイドカード、クレジットカード同様の使用ができる。クレジットカードの利用額を大幅に超える高額決済も可能であり、また、カードリーダーが必要ないのでインターネット上でも使用できる。

クリプトカレンシーは、発行者及び価値を確認のうえ、完全暗号技術を用いて暗号化し暗号貨幣情報（記号列）を発行する。クリプトカレンシーを使用する際には必ず真正性、未使用を確認し、受領者は保蔵または決済する。その都度新たな暗号貨幣情報（記号列）に更新することでより高い安全性を確保できる。

改めて整理すると、クリプトカレンシーは以下の４つのコア機能によって構成され、目的に合わせて応用システムと組み合わせて使用される。

a. 信用（担保）確認機能
   法定貨幣との兌換、または担保を確認する。法定通貨との兌換の場合は紙幣番号、また例えば資源担保の場合はその資源鉱区にナンバーリングしてその鉱区を貨幣情報に加える。
b. クリプトカレンシー発行機能
   発行者情報や価値情報を完全暗号化してクリプトカレンシーを発行する。
c. クリプトカレンシー保管・管理機能
   予め発行する場合、発行済クリプトカレンシーを保管・管理し、市場流通量を調整する。
d. クリプトカレンシー真正確認機能
   クリプトカレンシーを使用する際、本物かどうか、すでに使われたものでないか、確認する。尚、確認情報は、後述するクリプトレッジャーを用いてオープンに記録することもできる。

〈デビットカード型クリプトカレンシーの例〉

ここで、クリプトカレンシーの実用例として、近年急増するカード詐欺（例えば、カード番号を不正取得し

て不正使用する）を防止できる、デビットカード型クリプトカレンシー（DC-CC）を、図を用いて説明する。ユーザーは、DC-CC を使用するために、銀行に普通口座を開設し、DC-CC 専用アプリを例えば自らのスマートフォンにインストールし、銀行より秘密裏に与えられたパスコードでアクティベートして準備した上で DC-CC を以下の手順で使用する。

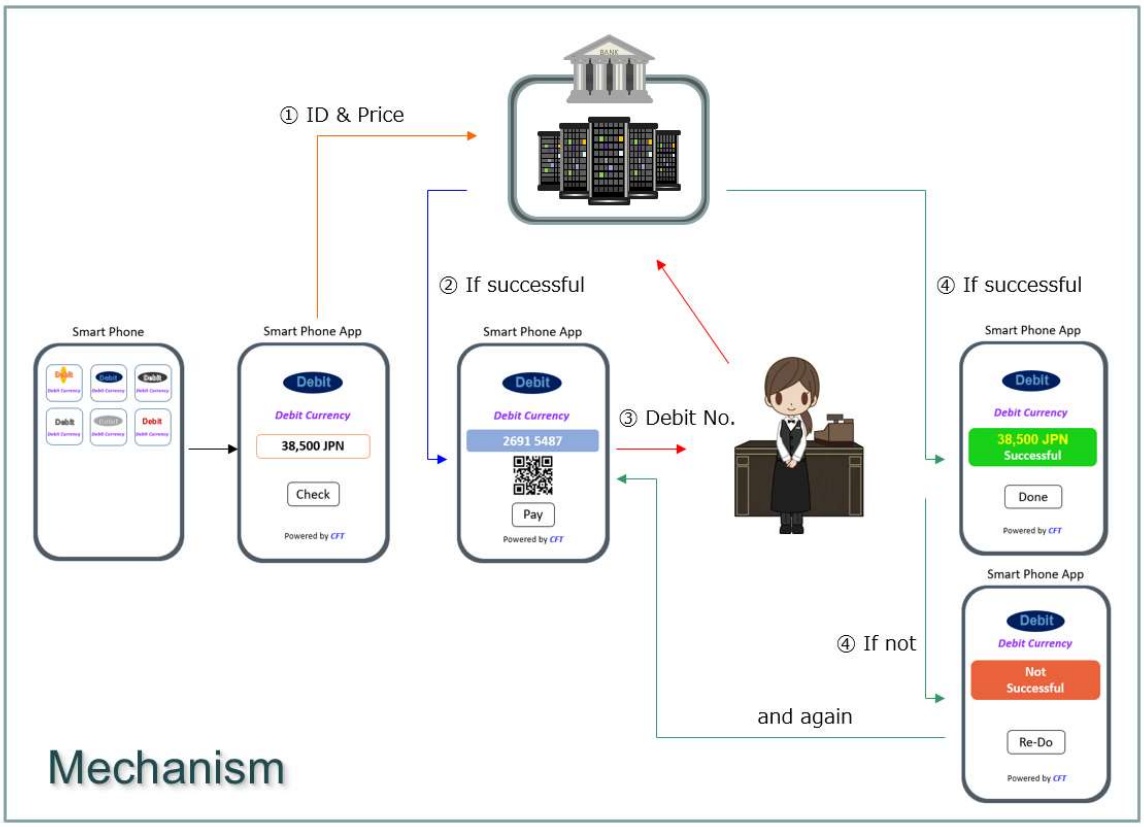
① スマートフォンのデビットカード型クリプトカレンシーアプリを起動して、例えば決済する金額 38,500 円（例）を入力し、ID と共に銀行サーバーへ送信する。

② もし残高が十分あれば銀行サーバーはスマートフォンのアプリに発行許可を与え、スマホ上のアプリは 5 分だけ有効で 38,500 円丁度の金額を決済できる 1 回きり使用可の 8 桁のデビット番号を発行する。このデビット番号は、例えば、38,500 円という価値を特定する情報を暗号化したものである。

③ この番号をお店に伝え、お店はこの番号をそのまま銀行サーバーに送信する。

④ 決済が成功裏に終われば、ユーザーとお店の双方に決済終了のシグナルが送られそこで終了するが、失敗したらデビット番号を再発行してやり直す。

この際、銀行サーバーの口座残高を更新し、データベースに記録する。尚、後述するクリプトレッジャーを用いて記帳しても良い。



＜クリプトレッジャー　―Blockchain に代わる新技術―＞

①の種類の暗号通貨では、取引内容を取引台帳に記録する。この台帳は取引終了後当事者の了解なしに勝手に改竄されることがなく、当事者が求めればいつでも内容をチェックできなければならない。

現在の Blockchain は、これらの必要条件を満たすものである。従来は銀行などの権威をもつ第三者機関が取引台帳を管理していたのを、中央管理を不要としたことで注目を集めている。しかしながら、希望する参加者全員が完全な台帳のコピーを持つこのシステムは、台帳の歯抜けを作らないというメリットがあるものの、

前編で指摘した通り１へクサバイトもの巨大な記憶容量を使って稼働する事態となっている。更に、巨大になった１つの Blockchain から網羅的に目的の取引記録を探し出すだけでも大変で、遂に構造的問題が露呈した現在の Blockchain は破たん寸前である。もちろん上述した分裂の問題もある。

Blockchain 同様の改竄不能でいつでもチェックでき、中央管理が要らないという機能は、以下のようなシンプルなプロセスで実施する。とりあえず、「クリプトレッジャー」と称することとするが、この技術は、Blockchain に要求される上述の機能を、膨大な数のサーバーなど必要とせずに実現できる。クリプトレッジャーは、さらに Blockchain では難しい取引内容の機密を保持でき、更にはスマート・コントラクトや保険証券など様々なサービスにも応用できる。

誰でもが自身の意思で、誰にも改竄されない状態で、取引やその他の契約を民主的に記録し保存するには、ある取引の関係者全員の“暗号紋※6”と呼ぶ暗号鍵を使って暗号化した情報を人数分コピーして、全員が保存することで事足りる。また、改竄防止を強化するために、関係者が信頼する第三者の暗号紋を使用することもできる。

手順を説明する。

① 取引成立（Lock-Transaction）
当事者各自は､従来の印鑑と同様の暗号紋を所持し､取引内容をすべての当事者の暗号紋で暗号化する。更に当事者が必要と考えれば、弁護士、公証人等の暗号紋によりさらに暗号化することもできる。

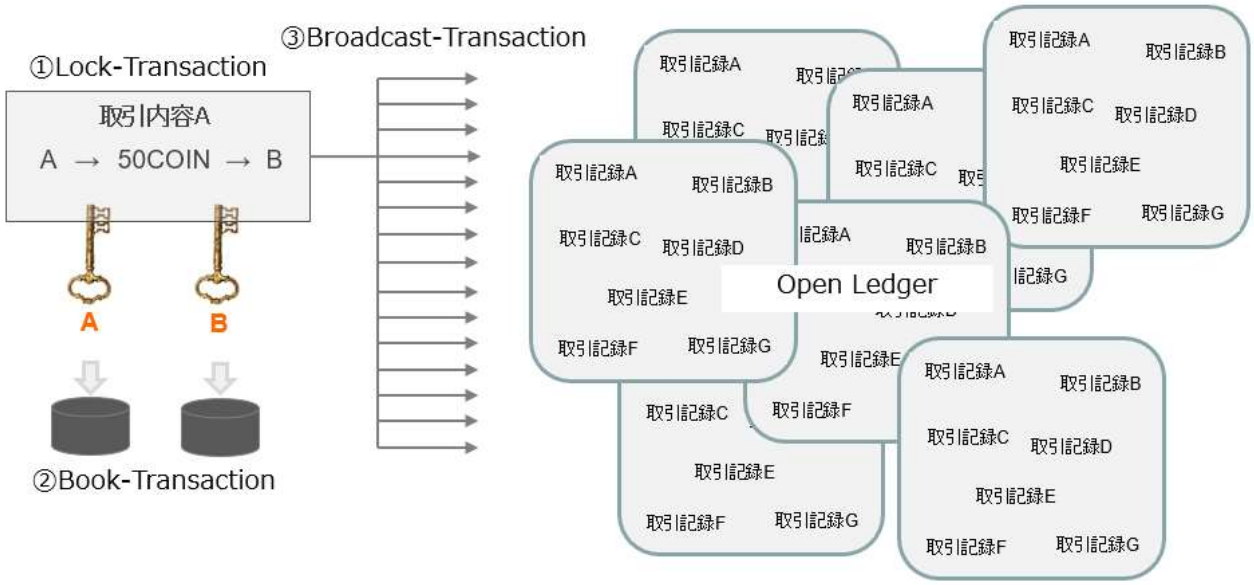
② 取引記帳（Book-Transaction）
この暗号化された情報を当事者全員が複製し所有する。各当事者全員分の暗号紋が揃い、暗号化と逆の順番で使用しなければ復号化は完成せず原本は取り出せない（改竄不可能)。もちろん当事者は全員が揃えば自分たちの暗号紋でいつでも内容をチェックできる。

③ ブロードキャスティング（Broadcast-Transaction）
さらに、暗号化された取引内容のデータを、ボランティアにより維持管理される多数の安全な記帳システム（場合によっては精算メカニズム等を持つオープン台帳）にブロードキャストして記録することにより､当事者全員の結託によって事後に記録を改竄することも防止できる｡オープン台帳(Open-Ledger)に記帳された情報は、前述の通り当事者全員の暗号紋が揃えば変更できるが、これらオープン台帳に残されたデータを参照することで、当事者全員の結託による不正も防止できる。これは当事者がデータを紛失した場合のバックアップともなるので、将来の紛失に対応することも考えられる。オープン台帳は多数であるのが望ましいが、クリプトレッジャーではデータの真正性は原理上暗号技術によって担保されるのであるから､多数決理論でデータの真正性を担保する Blockchain のノードのように､原理上その数が要求されるものではない｡また､原則としてすべてのノードで Blockchain のデータの全体を記録し続けることが必要となる Blockchain の場合とは異なり､クリプトレッジャーでは､各オープン台帳に記録されるデータは同じである必要はない。つまり、クリプトレッジャーで扱われるデータ量は軽く、またその運用コストは低い。

このように、①取引成立と②取引記帳の２つのプロセスだけで、中央管理不要でいつでも内容をチェックできる安全な記帳システムが構築できる。多数のノードも多数の善意も合意形成のためのプルーフ・オブ・ワークも必要ない。ブロードキャスティング機能を使えば当事者全員による改竄まで防止できるにもかかわらず、Blockchain では困難だった取引内容の秘匿も可能である。

クリプトレッジャーは､その課題を解決しつつ Blockchain に変わる技術であるといえ､もちろんその他の用

途はあるものの、より安全な仮想通貨或いは仮想貨幣を低コストで実現できる技術であるといえる。



＜結論＞
これまで、暗号技術の未完成を大きな理由として、究極の通貨と言われる“暗号通貨”を作り出す試みはことごとく失敗してきたし、現存するものにも不安定な要素が存在する。しかし近年遂に暗号技術が完成し、この究極の暗号技術を利用して“クリプトカレンシー”の開発に成功した。匿名性をもつもの、ユーザー自身が発行できるもの、資源を担保とするもの、有効期限をもつもの、利息を持つものなど、様々なクリプトカレンシーの発行が可能となった。
また、個人や会社が発行者となるクリプトカレンシーにおいて、受領者を特定し、その受領者情報も発行時にクリプトカレンシーに埋め込んだ暗号貨幣情報（記号列）を併せて発行するならば、送金にも応用できるはずだ。それは、現在の全国銀行資金決済ネットワーク（全銀ネット）※7や SWIFT※8などを用いる送金も根本から変革を迫ることになろう。
金融の激変が予想される。

※1. Blockchain の分裂

仮想通貨「ビットコイン」相場に急ブレーキがかかっている。今春以降、ビットコイン価格は急騰し、５月には一時、過去最高の１ビットコイン＝３４万円台に上昇した。しかし、足元では３０万円を割り込む水準にある。重荷となったのはビットコインの記録方式の「規格」をめぐる分裂問題だ。先行きの不透明感から、投資家が他の仮想通貨に資金を分散する動きも出ている。

（出典：産経ニュース　http://www.sankei.com/economy/news/170629/ecn1706290034-n1.html）

※2. ペイパル

PayPal（ペイパル）とはアメリカ企業 PayPal 社が提供する、オンライン決済サービス。PayPal を使うとインターネット上で安全に、且つ、低料金で、国内外の支払い決済・海外送金が可能とする。

※3. ラインペイ

LINE Pay（ラインペイ）は、LINE の友だち同士でお金を送ったり、ネットショッピングや対応サービスの決済に使ったりできるモバイル送金・決済サービス。実店舗でも使える「LINE Pay カード」が登場したことで活用の幅が広がっている。

※4. フェリカ（FeliCa）

ソニーが開発した NFC (Near Field Communication)準拠の無線方式を利用した非接触型 IC カードの技術方式。相互認証や通信路にオープンスタンダードなセキュリティーアルゴリズムを採用している。公共交通機関の乗車券システムから、電子マネー、マンションの鍵まで幅広い用途で使われている。JR グループの少額決済機能を持つ乗車券システムはその代表例である。

※5. 完全な暗号技術

歴史的に暗号技術は、暗号鍵の配送問題と、暗号アルゴリズムの完全性（解読不可能証明）の 2 つを問題として抱えている。暗号鍵の配送問題とは、暗号化と復号化に同じ暗号鍵を用いる共通鍵方式において、暗号化をする側から復号化する側へ安全に暗号鍵を配送することであり、公開鍵方式及びこれを発展させた公開鍵基盤は配送問題を解決したとして広く使われてきたが、実際は解決していないことが指摘されている。また、暗号アルゴリズムの完全性とは、完全なアルゴリズムで暗号化された暗号文は、暗号鍵が無い時には決して解読できないことを数学的に証明することであり、かつて、情報理論の父クロード・シャノンは 1949 年に発表した論文「秘匿系での通信理論」の中で、ワンタイムパッド暗号を紹介し、「解読不可能」であることを数学的に証明した。しかし、完全にランダムな乱数を通信文本体と同じかそれ以上の長さ分作成し適切に管理するのは困難で、一般的には用いられていない。情報通信が社会の基本インフラになる中、莫大な計算を極めて短い時間でこなす量子コンピュータが開発され従来暗号を一瞬で解読することが現実となりつつあり、筆者が開発に関わった u-VKS 暗号など 2 つの問題を解決した完全暗号は何よりも重要な技術と考えられている。

※6. 暗号紋

人間の指紋のように、個人個人が持つ暗号化するための固有の暗号鍵の事を指す造語。暗号紋は複数持てるが、必ず個人に属し、他人と共有しない。この暗号紋で暗号化すれば、同じ暗号紋なしに復号化できない。

（公開鍵の場合は、対になるもう一方の暗号鍵なしに復号化できない）

※7. 全国銀行資金決済ネットワーク（全銀ネット）

全国銀行資金決済ネットワーク（全銀ネット）は、日本のほとんどの金融機関が加盟する、金融機関相互間の内国為替取引をオンライン処理する「全国銀行データ通信システム（全銀システム）」を運営する一般社団法人をいう。日本の社会的基盤である金融機関間の資金決済を円滑・安全かつ効率的に実施し、信頼ある金融インフラを構築することによって、国民生活の向上に資することを目的としている。

（出典：iFinance　http://www.ifinance.ne.jp/glossary/finance/fin096.html）

※8. SWIFT

SWIFT（スイフト）は、"Society for Worldwide Interbank Financial Telecommunication"の略で、日本語では「国際銀行間金融通信協会」とも訳され、世界各国の金融機関などに高度に安全化された金融通信メッセージ・サービスを提供する、金融業界の標準化団体。資金付替や顧客送金、外国為替、証券取引、デリバティブなどの安全性の高いグローバルな金融メッセージ・サービスを提供する。

（出典：iFinance　http://www.ifinance.ne.jp/glossary/finance/fin009.html）