基般

5. 暗号技術でお金を実現する
—電子現金からデジタル通貨へ—

松尾真一郎（国立研究開発法人 情報通信研究機構）

お金を電子データで表現するという挑戦

暗号技術を始めとしたセキュリティ技術の普及により，ネットワークを通じたさまざまな新たなサービスが研究されて，そのうちのいくつかが実用化されてきた．そのうちの1つが，お金にまつわるさまざまな処理を行う電子商取引や電子決済と呼ばれる分野である．簡単な例としては，銀行の業務の受付をWebサイト上で行うインターネットバンキングや，クレジットカード支払いの手続きをWeb上の商店で行うことが挙げられる．これらの例は，既存のお金に関係する業務をWebページに置き換えているものである．これらのサービスにおいては，Webブラウザと Webサーバの間の通信の暗号化，認証，商店や銀行におけるデータの保存時の暗号化などに暗号技術が利用されている．つまり，処理に必要な通信メッセージの守秘や非改ざんなどを暗号技術で実現している．

他方で，お金そのものを情報のみで実現したいという要求も当然考えられる．上述の例では，お金の所有権の移動は，銀行やクレジットカード会社を通じて行われる．いわゆる現金では，物理的な紙幣や硬貨を渡すことにより，価値の所有権の移動が行われる．このように，ある物体を移動させることで同時に価値を移動させるという利便性を，電子データ上においても実現するためには，従来の紙幣や硬貨が持っているセキュリティ上の性質を電子データにおいて実現しなければならない．たとえば，硬貨は偽造のためのコストが材料費と製造に必要な費用に非常に近いように設計されており，偽造のためのインセンティブが働かないようになっている．また，紙幣については材料費こそ，紙幣が表す価値に比べて非常に安価ではあるが，紙幣に印刷されている精巧な模様や，紙幣に振られている通番が偽造やコピーの防止に役立っている．

お金を電子データで表現する際には，このような偽造やコピーを防止するための仕掛けを別の技術によって実現する必要がある．このような技術の研究は1990年代後半から行われており，さまざまな実験，実用化が行われている．さらに，近年ビットコインの発明とビジネス化が急速に進んでおり，暗号技術を利用してお金を実現するだけでなく，より高度な経済行為を，信頼できる仲介者を置かずにインターネット上のデータの交換だけで実現できるようになっている．本稿では，お金という，ある意味最高レベルのセキュリティが必要とされるアプリケーションにおいて，暗号技術が果たす役割，社会的視点からのセキュリティ要件，運用や制度とのすみ分け，そして暗号技術によって，より安全で安心できる経済活動を実現するために今後必要な取り組みについて示す．

暗号技術でお金を実現する

本章では，まず最初に，現金としてのお金に必要とされる要件について述べる．金銭的価値におけるセキュリティの観点では，正当なお金の発行機関以外の者がお金を偽造できないこと（**偽造不可能性**）と，お金を持っている者がお金をコピーして複数回使えないこと（**二重使用不可能性**）が挙げられる．一方，現金に求められる性質としては，現金を使う際のプライバシ保護が挙げられる．つまり，お金の支払いにおける**匿名性**，および同じ者による別々の支払いが結びつけられないこと（**リンク不可能性**）が挙げられる．その他，現金が持つ利便性として，支払い時にお金の発行機関や金融機関などに問い合

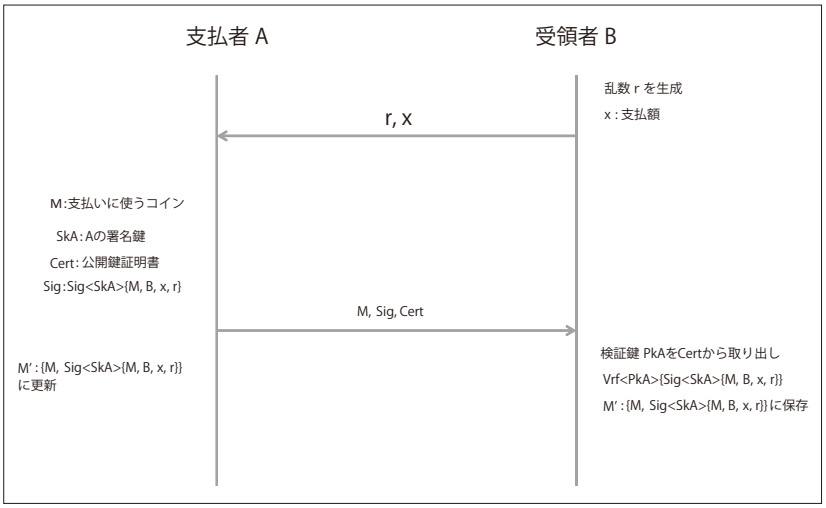

図 -1　電子現金における支払いプロトコル

わせをする必要がないこと（**オフライン性**），お金自体を自由に移動させることができること（**転々流通性**）が挙げられる．

このような要件を実現するための電子現金，電子マネーのための研究は，1980 年代から行われるようになり，1990 年代から盛んになった．David Chaum らは 1985 年にブラインド署名技術を用いた匿名性を有する電子マネーを発表し，1988 年にはオフラインでの支払いが可能となる方式を提案した．さらに，1993 年には二重使用の防止を IC カードのような耐タンパデバイスを用いて実現する方式が Stefan Brands によって発表された [1)]．日本では，NTT と日本銀行による研究がなされ，1990 年代後半には実証実験も行われた．

この当時に研究された電子現金方式の考え方の 1 つを簡単に示す．100 というデータを，そのまま 100 円という価値を表すために使うとなると，誰もが自由に価値を創造できることになってしまう．そのため，100 というデータに対して発券銀行（たとえば日本銀行）が秘密鍵で電子署名を付与し，電子署名とペアで扱うことで，まず偽造不可能性を実現する．次に二重使用の防止を考える．100 というデータと電子署名は，いつでもコピーすることが可能であり，このままでは二重使用を防ぐことができない．そのため，電子現金の支払いを行う際には，電子現金の受領者が支払者に乱数を送付し，その乱数と電子現金のデータを組にして，支払者の電子署名を付与する．このテクニックはチャレンジ・レスポンスと呼ばれるが，この技術により通信データをコピーして利用した際に，二重使用を検出することが可能になる．受領者が電子現金を受け取るときには，支払者の電子署名を検証することで，その正当性が検証できる．支払いは電子署名の付与と検証で行うため，支払いの際のオフライン性も確保することできる．また，データ自体を送信することで転々流通性も確保できる．匿名性については，電子署名に用いる公開鍵と秘密鍵のペアと，実名の関係を秘密にすることで実現する．この例における支払いプロトコルを**図 -1** に示す．

この方式の安全性の基礎となる大きなポイントは，発券銀行，および各利用者の鍵ペアの管理が正しく行われるということが前提になっているということである．つまり，発券銀行は信頼できる第三者（TTP）であり，各利用者の鍵ペアは耐タンパ性が担保された IC カードに格納されている必要がある．そのため TTP の運用を正しく行うためのハードウェア，ソフトウェア，および運用のコストや，IC カードのコストなどが掛かることが，この方式のデメリットである．また，あくまでも日本銀行券（紙幣）の範囲でお金を作ることを目的としていたため，法律的には前払式証票の規制等に関する法律（いわゆるプリペイドカード法）の範囲内の運用とされ，転々流通が可能なプリペイドカードとしての位置づけであった．その意味で，いわゆるお金を実現する方式としては，機能的にはかなり自由度の高い方式であり，暗号技術の応用としては意欲的な技術であったが，一方でお金としての信頼性を担保するためには，暗号技術以外の運用面と法律面での制約が大きかったといえる．

より現実的な電子マネーへ

我々にとって，電子マネーという言葉が生活に入り込んだのは，2000年代にICカードや携帯電話に搭載されたICチップを利用し，プリペイド（チャージ式）やポストペイド（後払い式）の支払いをできるようにしたサービスが登場したことがきっかけであった．これらのサービスは，前章で示した電子現金とは異なり，個別のICチップの内部に金銭的価値の残高を記録しておく方式をとっている．ICチップ内部のデータは共通鍵暗号技術を利用して保護されているほか，ICチップ自体の耐タンパ性によっても保護されている．また，支払いなどの際に，ICチップに記録されている残高情報を書き換える必要があるが，この書き換えのプロトコルについても暗号技術が用いられている．

このような残高管理型の電子マネーの場合には，個別のカード内の残高情報の書き換えが正しく行われること，および残高情報の偽造が行われないことがセキュリティ上の大きなポイントとなる．そのために，残高管理型の電子マネーを実現するために，ICカードのセキュリティを厳重に設計しているほか，カードの故障や不正の発見のために，個々のカードの残高を定期的にバッチ処理で確認できるようにしている．このような設計は，電子マネーのアプリケーション，たとえば鉄道の自動改札機において大量の人流に対応する必要があり，高速処理を実現するために行われている．そのため，このタイプの電子マネーでは，いわゆる利用者間の譲渡ができないようになっている．暗号技術は，主に残高の書き換え部分に利用され，そのほかにハードウェアのセキュリティ技術によって実現されていると言ってよい．

デジタル通貨ビットコインの発明

2009年5月にSatoshi Nakamotoを著者とする，ビットコインの提案論文[2]が発表された．この論文の概要の最初の文に象徴的に書かれているように，この技術はP2P（Peer-to-Peer）技術を導入することで，それまでの電子現金や電子マネーで必要であった信頼できるお金の発行機関を，P2Pのノードに分散された元帳（Public Ledger）という形で実現した．そのため，偽造や二重使用の防止というセキュリティの機能の安全性は，P2P技術の性質と組み込まれている暗号技術の安全性だけに依存し，信頼できる機関の運用の正当性の証明が不要になったことが大きな利点である．一般的にビットコインを説明する際に，国家の信用を背景にしておらず，国家が管理する通貨でないことが，しばしばその機能的な特徴として挙げられる．これは，国家と同等の信用を持たなくても，ビットコインの技術によって，改ざんが不可能で，かつ第三者が公開検証可能なPublic Ledgerを運営可能であり，そのPublic Ledgerに記録されるデータ自体を人々が金銭的価値があると考えれば，Public Ledgerそのものが，価値とその流通を管理できるからである．ビットコインは，Public Ledger上に，人々が合理的に金銭的価値を認められるようなロジックを構築したものであり，国家でなくても信頼できる価値の管理が可能であることを数学的に示すことができるようになったといえる．

ここで，ビットコインがどのように実現されているかを簡単に示す．ビットコインは，Public Ledgerを管理するBlockchainと呼ばれる技術のレイヤと，Blockchainの管理内容を通貨として見なすアプリケーションのレイヤから構成されている．Blockchainとは，共通的に管理すべきデータをP2Pネットワークの参加ノードに分散して記録するとともに，時刻tにおける記録のデータをアップデートする際には，時刻tにおけるデータに対して暗号学的なハッシュ関数を用いたハッシュ値を計算し，そのハッシュ値を時刻t+1におけるデータに含めて電子署名を作成する．時刻t+1から時刻t+2に移るときは，時刻t+1のデータのハッシュ値を時刻t+2のデータに含めていく．このようにハッシュ値を次の時刻のデータに含めるように計算することで，個々の書き換えの前後性を第三者検証が可能な形で保証することが可能となる．この

ような技術は，Blockchain 以前にも存在しており，ISO/IEC 18014-3 で規程されているリンクトークン方式のタイムスタンププロトコルや，ヒステリシス署名などはその代表例である．

Blockchain の特徴的な部分は，電子署名の対象となる管理対象のデータが P2P ネットワークで分散されていることである．そのため，1 カ所で情報を管理する場合に比べ情報の紛失に対する堅牢性が高まる．また，P2P ノードに分散管理されている情報から，Public Ledger の情報はいつでも第三者検証可能であり，Public Ledger が不正に書き換えられていないことを，データを保管するセンターの厳密な運用に依存しなくても実現することができる．

続いて Blockchain を用いて通貨（ビットコイン）を実現する仕組みを簡単に説明する．ビットコインにおいては，Public Ledger に記録される情報は，ビットコインを保有する利用者が保有するビットコインの数量であり，利用者の公開鍵と紐付けられている．そして，利用者間でビットコインの移動が行われる際に，誰から誰にどの数量のビットコインが移動したかを Public Ledger に記録していく．現実的には，定期的（ビットコインでは 10 分に 1 回）に複数の資金移動のデータをまとめて，電子署名を付与していく．また，ビットコインでは流通するビットコインの数量が約 2,100 万 BTC（ビットコインの流通単位の 1 つ）と決められているが，Blockchain 技術により，この数量を超えるようなビットコインの偽造や二重支払いは発生しないようになっている．

ビットコインは，前述の通り，Blockchain 技術を用いることで従前の電子現金や電子マネーで必要とされていたコストの掛かる運用や運用体の信用が不要になっている．その意味では，お金の実現に際して，暗号技術（数学の応用）と P2P（ネットワーク技術）という技術が貢献している部分が増大していることは確かである．

一方で，ビットコイン の技術コンセプトについては，その有用性が認められているものの，お金を実現するという点では，これからさまざまな検討が行われる必要があるという初期の段階といえる．現在の経済におけるお金は，一般的に国，あるいはその連合体が発行することになっており，その価値については国による信頼の裏付けがされている．

一方で，前述の通りビットコインは国の信頼の裏付けがないため，決済手段として安定した価値を表現するための枠組みのコンセンサスが作られていない．そのため，ビットコインの価値そのものが投機的な側面を持っており，既存の経済システムとの整合性を取るための仕組みについて，今後十分に議論をする必要がある．さらに，Satoshi Nakamoto が提案した当初のビットコインをベースとして，その後さまざまな改良が施された亜流と言うべき方式が提案，実装されている．しかし，安定した経済基盤となるためには，技術が提供する機能，安全性，信頼性に対して，十分な社会的合意が必要となる．このような今後の課題を解決するための方向を次章で述べる．

デジタル通貨が安全に普及するために必要なこと

本章ではデジタル通貨が今後のネットワークにおける経済インフラストラクチャになるために検討されるべき事項について述べる．

1 点目は，技術的な課題である．まず，インターネットが階層モデルによるアーキテクチャによって整理されて発展したように，Blockchain 技術，そしてビットコインのような決済のための技術に必要とされる情報システム全体のアーキテクチャを確立する必要がある．現状，このようなアーキテクチャは十分確立されておらず，そのため技術の信頼性を確認することが難しいといえる．**図 -2** は，デジタル通貨が信頼性を得るために必要と考えられる技術のレイヤの例を示したものである．Blockchain 技術は，電子署名，ハッシュ関数，共通鍵暗号などの暗号アルゴリズムという基盤的な暗号学的な演算の技術と，P2P ネットワークの技術によって作られている．その上に，Blockchain を構成する暗号プ

レイヤ	セキュリティ上の要件	対応する既存の国際標準
運用	セキュリティポリシー，監査，透明性	ISO/IEC 27000 シリーズ
実装	セキュリティ設計，プライバシ設計，攻撃対策技術	ISO/IEC 15408
応用プロトコル	プロトコルの安全性評価	ISO/IEC 29128, IETF
基盤プロトコル	プロトコルの安全性評価	ISO/IEC 29128, IETF
暗号技術	暗号技術の安全性評価	ISO/IEC, NIST

図 -2　デジタル通貨の安全性を確保するために必要な技術と運用

ロトコルのレイヤがある．そして，その上に P2P による Public Ledger の書き換えやお金の移動を保証する決済プロトコルとしてのレイヤがある．ここまでは，暗号技術を形作る数学やプロトコルのレイヤとなる．さらに，これらの技術を安全にソフトウェアやハードウェアに落とし込む実装のレイヤ，そして方式や実装では実現できないセキュリティや業務を行うための運用のレイヤが存在する．まずは，デジタル通貨にかかわる諸技術や課題をレイヤ分けして，各レイヤにおいて安全性や性能の議論が行えるようにすることが必要である．

その上で，セキュリティの課題に焦点を当てると，一番下の暗号技術そのもののレイヤの安全性は，日本における電子政府推奨暗号を定める CRYPTREC において十分に評価されており，CRYPTREC の評価結果を参照することでその安全性の確認を行うことができる．Blockchain プロトコルの安全性については，学術的には十分な議論ができておらず，Blockchain の更新が正しく行われることを理論的に示す研究成果も限られている．また，その上の決済プロトコルの安全性についても，理論的な検証が必要な段階である．この評価は Blockchain やビットコインプロトコルのセキュリティのみならず，利用者のプライバシ保護についても，今後評価を行う必要がある．暗号プロトコルに関しては，本小特集「2. SSL/TLS と暗号プロトコルの安全性―恒久的に噴出する脆弱性との戦い―」で述べられている CELLOS（暗号プロトコル評価技術コンソーシアム）を始めとして，その評価の動きが本格化しており，今後デジタル通貨のようなプロトコルに対しても評価が行われるようになることを期待したい．

実装のレイヤについては，既存の ISO/IEC 15408（コモンクライテリア），CMVP (Cryptographic Module Validation Program) などの枠組みにおいて保証することが望ましい．

そして最大の課題になるのは運用である．我が国においては，現時点でデジタル通貨に関する技術的興味はある程度存在するものの，一方で諸外国に比べて普及の見通しが立っていないのは，2014 年に Mt. Gox による事件が発生したことが大きい．この事件の全容はまだ明らかになっていないが，Blockchain 技術やビットコイン技術そのものの問題ではなく，利用者から集めた資金や口座の管理，そしてビットコインと資金を連携させるシステムとその運用の問題だと考えられている．しかし，このような事件が起きると，Blockchain やデジタル通貨技術そのものの瑕疵と見なされる可能性があり，将来的に有用に活用していくことに対してブレーキとなってしまう．この課題を解決するために重要なことは，セキュリティ上の問題が技術レイヤでどこまで解決できていて（あるいは解決すべきで），どこが技術ではカバーできないのかを明らかにすることである．技術で守れない範囲は，人を含めた運用でカバーする必要がある．お金を扱う，いわゆる重要インフラと考えられるシステムにおいては，技術面，および運用面での監査が，その信頼性確保に重要な役割を担っている．その監査を正しく行うためにも，技術と運用の責任分界点を示すことができるようになることが重要だ．

さらに，デジタル通貨の普及にあたってクリアしなければいけないことが，法制度との整合性の確保である．以前の電子現金，電子マネーは，プリペイ

ドカード法の範囲内で運用されていたため，法的整合性についてはクリアしていたが，デジタル通貨については，新たな議論が必要とされている．法制度を考えるためには，前述のセキュリティのための技術と運用の役割分担を明確にすることと同時に，技術面・運用面でのブレのない標準を定めていく必要がある．金融・決済のためのシステムとして必要とされる技術的な要件，運用的な要件を定めることで，法制度や規制のための基準が定まり，利用者から見た際の信頼性が高まっていくと考えられる．これは，電子署名法において，別途基準を満たす電子署名技術が技術標準などに従って検討されて，指定されていることと同じである．暗号技術においては，日本では CRYPTREC，米国では NIST（National Institute of Standard and Technology）が標準を定め，ISO/IEC SC27 において国際標準化も行われている．また，暗号プロトコルについても，ISO/IEC, IETF, IEEE などで標準化が行われている．2015 年の 4 月には，ISO/IEC TC68 においてデジタル通貨の調査を行う研究グループが立ち上がっており，今後標準構築に向けた動きが進むことが期待される．

他方，Blockchain やビットコインの技術を活用するための基盤の研究が 2015 年の早い時期から欧米において活発になっている．たとえば，Intel, Citibank, NASDAQ などは，独自に Blockchain 研究のための研究所を立ち上げ，研究員を世界中から集めている．また，ビットコインのスタートアップ企業に対しても，初期のインターネットに比べても急速に投資のための資金が流入しており，1,000 億円単位での資金がスタートアップ企業に投資されている．このように急速に資金が入ると，信頼できる技術標準の確立よりも，ビジネスが優先される傾向が高くなる可能性がある．そのため，MIT メディアラボが中心となり，MIT-DCI（Digital Currency Initiative）と呼ばれる組織が立ち上がり，技術面，制度面，および社会的影響について，学術的な側面からの中立的な立場での研究開発が始まっている．日本においても，デジタル通貨に対する制度面での検討が始まっているが，学術的な側面からも類似の中立的な検討を行い，安全と安心が確保されたデジタル通貨と Blockchain 技術の活用が望まれる．

今後への期待

1980 年代以降，安全なお金の流通をネットワーク上で実現するという試みは，暗号を用いて新たなサービスと価値を創造するという目標の中でも，最も期待され，かつ挑戦的な目標であった．1990 年代の電子現金，電子マネーの試みは，インターネットが単なる通信の手段に過ぎなかった時代のものだった．現在 P2P や SNS の発達などでインターネットがコミュニティ，経済，そして民主主義のための大きな基盤と拡大していく中で，Blockchain とビットコインは，インターネットという基盤が新たな経済的な仕組みを生み出す可能性を示している．ビットコインそのものは，暗号技術の応用的コンセプトとして提案されたが，ビットコインの登場によりさまざまな研究者と技術者が，さらなる応用とイノベーションを模索している．その新たな基盤が，暗号を適切に，素敵に使っていくことで，より信頼性を高める形で使われていくようになることを期待したい．

参考文献

1) Brands, S. : Untraceable Off-line Cash in Wallets with Observers, CRYPTO 93, Springer-Verlag.
2) Nakamoto, S. : Bitcoin : A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf

（2015 年 8 月 17 日受付）

松尾真一郎 ■ smatsuo@nict.go.jp

1996 年 NTT データ通信（株）入社．情報セキュリティと暗号技術の研究開発に従事．2009 年より情報通信研究機構．ISO/IEC SC27/WG2 国内小委員会主査．暗号技術検討会構成員．暗号プロトコル評価技術コンソーシアム（CELLOS）技術 WG 主査．