基礎研レポート

# アジアデジタル共通通貨の提案

国際協力機構専門家 アジア開発銀行コンサルタント　乾　泰司
大阪経済大学経済学部教授　ニッセイ基礎研究所 客員研究員　髙橋　亘
伊藤忠商事理事　石田　護

**■要旨**

本稿[1][2]では、東アジアにおいて国際機関（例えばAMRO）により、ブロックチェーン等の技術を用いたデジタル通貨によってアジア共通通貨を提供することを考察している。デジタル共通通貨は、各国（エコノミー）の政府・中央銀行が各国の国債等を裏付けとして発行されたアジア共通通貨建て債券を資産に持つ発行体（国際機関）が発行するコイン（例えばAMROコイン）として提供される。AMROコインは、発行体から各国中銀・通貨当局を通じて、各国（エコノミー）の銀行・商店等に流通することになる。

アジア共通通貨については、今世紀初めころから欧州のユーロに触発されACU（アジア通貨単位）が試算されるなどの動きがあった。共通通貨は、デジタル通貨によって技術的な実現性は高まったといえる。なお本構想では、各国経済では各国通貨と本デジタル通貨が併存して流通することを想定している。

本構想のメリットとしては、①デジタル通貨としてのメリット、②共通通貨としてのメリットのほか、③多国間体制で公的に管理される通貨であることのメリットが指摘できる。①デジタル通貨は、国際的な送金等の効率性を高めるほか、地域の各国経済で進展する経済のデジタル化を推進する。また疫学的にも感染対策となることも重要である。②共通通貨は、為替リスクを軽減するほか、地域レベルの決済システムを提供することで、サプライチェーンの進展により進んだ生産貿易体制の一体化に対応した金融サービスを提供する。さらに③多国間の公的な体制で管理されることは、プライベイトな通貨より安全な通貨の提供を可能とする一方、大国による国際通貨の支配を抑制し、政治的な公平性を確保できる。

なお本構想は、将来的には世界的なデジタル通貨等への発展も展望できる。

---

1　本稿は、同内容の神戸大学経済経営研究所のディスカッション・ペーパー「アジアデジタル共通通貨についての一考察」（No2020J-09）を転載したものである。また本稿は外国為替貿易研究会発行「国際金融」1327号（2019年12月）掲載の、「国際機関が発行する地域デジタル通貨　（例えば AMRO コイン）についての一考察」を加筆・修正している。

2 Email: 髙橋（wtaka@osaka-ue.ac.jp）

JEL；E42　F33　F36
キーワード：デジタル通貨、アジア共通通貨、ブロックチェーン、口座型、トークン型

## 1――はじめに[3]

本稿では、ASEAN+3[4]域内において国際機関（例えばAMRO[5]）によって国境を越えて域内で流通するデジタル貨幣の発行を考察する。デジタル貨幣としては、ACU[6]のようなアジア共通通貨単位で発行することを想定しており、その点では「アジア共通通貨」発行の提案でもある。ただし、当面は各国が従来通り各国通貨を発行することも前提としており、域内では各国通貨と共通通貨が並行して流通することになる。この点では各国通貨を廃止してユーロを単一通貨とした欧州とは異なっている。将来的にユーロ型の統一通貨を排除するものではないが、むしろ本構想の狙いは、共通通貨の発行流通により域内決済の利便性の向上を図るものである。ASEAN+3 では、国境を越えた決済ではいまだドルが介在している割合が大きい。しかしこれには、為替リスクが伴い域外国である米国の政策の影響を受けるという難点が伴う。これに対し本提案のような共通通貨は、残存する各国通貨との為替リスクは残るものの対ドルよりは小さくなる可能性が高いし、政治的には域内で管理することができる。そして、何よりも共通通貨で決済できる域内に広がる決済インフラが整備されることが大きなメリットとなる。

金融統合については、欧州が先行する。2000 年代初めには、アジアにおいてもアジア共通通貨構想が盛んになりアジア共通通貨単位の計算なども行われてきている。ただこうした動きは、世界的な金融危機で生じたユーロ危機により一転し、ユーロ懐疑論からアジアにおいても共通通貨への情熱も薄らいでいるように見える。ただし、金融統合は、通貨統合と域内決済システムの整備の二つの部分から構成されることには注意が必要である。両者は表裏一体の面もあるが、それぞれを個別の施策としても推進できる。実際、欧州でも通貨統合と並んでユーロ非加盟国も含む域内ワイドの決済機構の整備が確実に進められてきた。まず、域内大口資金決済システム（RTGS）を相互接続した TARGET が整備され、その後、全 RTGS を一つに統合した TARGET2 に発展。また、証券決済システムについても TARGET2-Securities(T2S)が稼働している。更に、現在、TARGET2 と T2S を統合中である。こうしたユーロ圏を超えた域内決済システムの整備が欧州域内の金融市場の発展に大きく寄与し、域内レベルでの産業の発展と金融業の発展に大きく貢献している。

本域内デジタル貨幣構想は、欧州と比べれば小規模であるが最初の域内決済システムの提言でもあ

---

[3] 本稿執筆に当り、高村泰夫氏（財務省）、水野正幸氏（アフラック生命保険）、山寺智氏（アジア開発銀行）、織立敏博氏（日証金信託銀行）など多数の方からご助言を得た。本稿は、それらのご助言や情報を活用しているものの、内容や意見の責任は、筆者に属するもので、JICA、ADB、日本銀行、財務省、AMRO などの組織・機関の公式見解を示すものではないことを付記する。
[4] ASEAN+3 とは、ASEAN10 カ国（インドネシア，マレーシア，フィリピン，シンガポール，タイ，ブルネイ，ベトナム，ラオス，ミャンマー，カンボジア），に日本，中国，韓国の 3 か国を加えた 13 か国および中華人民共和国香港特別行政区を加えた 14 の国と地域（ここでは 14 エコノミーと呼ぶ）で構成。
[5] ASEAN+3 Macroeconomic Research Office
[6] Asian Currency Unit

る。

ここで域内共通通貨の利点を簡述すると、通常指摘される為替リスクの軽減に加えて、通貨危機への耐性の強化という側面がある。1997 年～98 年のアジア危機のように金融危機は、脆弱性を見せた個別の各国通貨へのアタックから始まり周辺に連鎖する。共通通貨はこうした環の弱点をなくす。さらに重要なのは、共通通貨が多国間体制で運営されるという点である。多国間体制では、小国も大国同様に発言力を持つ。国際金融では、現状米国がヘゲモニー国であるが、将来的には中国の力が大きくなることも予想される。多国間体制は、こうした大国の行動を抑制する。

なお、本デジタル通貨構想は、各国通貨との併存を展望しており複雑との指摘もあろうが、ドル化した国ではすでに複数通貨が併存した状態であるし、ビットコインやリブラなどのプライベイトな暗号資産が国際的に通貨として流通すれば、これも既存の法定通貨と併存することになる。こうした状況を展望すれば、本構想のようにプライベイトな通貨に加えて公的な通貨が国際的に流通することは十分意義があると思える。

ASEAN+3 地域では、ユーロに先立つ約 500 年前、中国の明銭である永楽通宝が広く流通していたことが知られている。わが国では、自国の通貨をもたず中国からの渡来銭が流通していた。本デジタル通貨は、永楽銭を現在によみがえらせる構想でもある。当時中国銭は国際貿易を通じて欧州などにも渡った。本構想も、アジアを超えて世界共通通貨の可能性も孕んでいる。


永楽銭:画像提供日本銀行貨幣博物館

## 2――デジタル通貨について

中央銀行が発行するデジタル通貨（CBDC）にいては、既に多くの論稿があり、幾つかの事例も報告されている。これらの中で日本銀行の雨宮副総裁による「日本銀行は、デジタル通貨を発行すべきか」が、明確に中央銀行の考え方・方針を説明している。具体的には、「多くの中央銀行は、近い将来 CBDC を発行する計画はないが、調査解析は行ってゆくというスタンスであり、日本銀行も同様な考え」というものである。同講演の中で、デジタル通貨について「ホールセール型」と「一般利用型」に大別し、各々の特徴を次のように説明している。「ホールセール型」は、参加者が銀行など一部の先に限定されており、金融機関の資金決済を目的とした電子的な中銀マネーの一種であり、これまで既にデジタル化された中銀債務による決済について、分散台帳技術などの新しい情報技術を利用したものである。もう一つの「一般利用型」は、銀行券や貨幣など現金を代替するものであり、「口座型」と「トークン型」に分類される。「口座型」は、個人や企業が中央銀行に顧客口座を開設し口座間の振替により決済を行うものである。「トークン型」は、スマートフォンや IC カードにデジタル通貨を格納し利用者間で金銭的価値を移転することにより決済を行うというもので、「価値保蔵型（stored value）」と

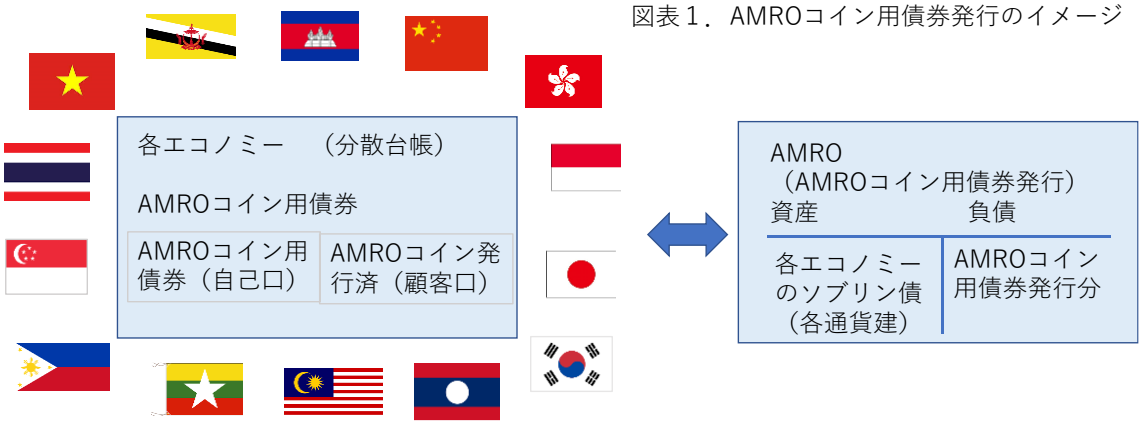
も呼ばれている。現在日本で普及しているプリペイド型の電子マネーは、「トークン型」に分類される。

因みに、「ホールセール型」の考え方は、債券の発行等にも適用され既に実用レベルに達している。本ペーパーでは、「ホールセール型」と「トークン型」を組み合わせることにより、地域デジタル通貨（コイン）を実現する方法について一案を提示している。

## 3――実現方法の例

最近の金融市場インフラにおける技術動向を概観すると、既に分散台帳技術を活用した様々な金融ビジネスが提案され、実際に稼働しつつある。ここでは、プライベイト型分散台帳技術による債券発行の仕組み[7]「ホールセール型」を既存の電子マネー発行や中央集権的な狭義のブロックチェーン技術[8]「トークン型」と組合せることにより、国際機関が発行する地域デジタルコイン（例えば AMRO コイン）を実現する方法について考察する。

図表１．AMROコイン用債券発行のイメージ




まず、ASEAN+3 各国（エコノミー）の政府ないしは中央銀行が、同エコノミーの国債や通貨を AMRO に提供・出資し、それを見合いに、AMRO が、「AMRO コイン発行用債券」を発行・提供する。同債券は、ASEAN+3 の状況を鑑み、通貨バスケット制に基づく「ACU 建債券建」とする。次に、域内の中銀等は AMRO に提供した国債・自国通貨相当の「AMRO コイン発行用債券」を資産として持ち、AMRO コインをそれぞれの経済の金融機関他、店舗、個人に発行する。その際、域内の中銀等は、資産として保有する AMRO コイン発行用債券のうち、AMRO コイン発行相当額を「AMRO コイン発行用債券（自己口）」から「AMRO コイン発行済（顧客口）」に移転させ、管理することなどが考えられる（図表１）。

このように、プライベイト分散台帳技術を活用することにより、ASEAN+3 のエコノミーの中銀等間では、AMRO コインの発行に関する情報をトランスペアレントに相互に把握できるようになると言える。

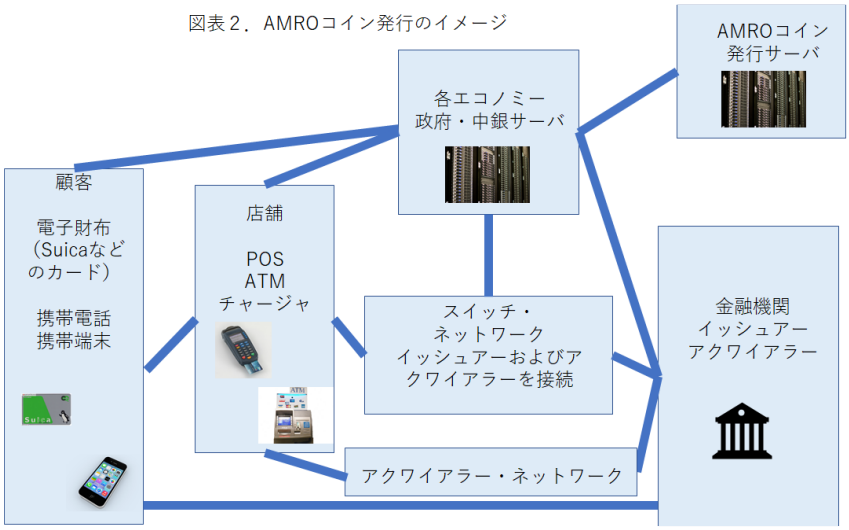
---

[7]「世界初、ブロックチェーンを活用した世銀の債券発行スキーム」（2018.12.3 金融財政事情）、「Project DLT Scripless Bond」（2017 Bank of Thailand）などが挙げられる。なお、世銀の債券発行スキームはイーサリアムを、タイ中銀のものは Hyperledger Fabric を活用。

[8]「中央銀行ないしは同等の機能を有する機関が法定通貨として発行することを目的とした電子マネーおよび電子マネーシステム」が参考として挙げられる。

AMRO コインの発行そのものは、AMRO コイン発行運営体が一元的に行い、域内でのインターオペラビリティを確保する（図表２）。

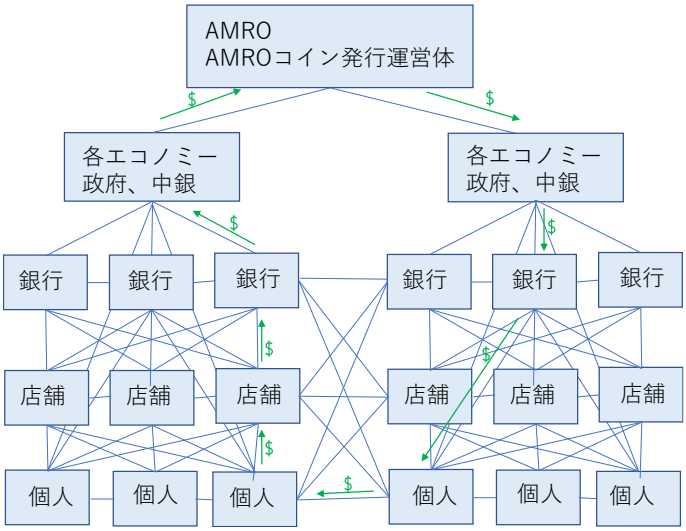
図表２．AMROコイン発行のイメージ




各エコノミーにおいて AMRO コインを発行する場合には、物理的なタンパーレジスタンスを保証するハードウェア（例えば非接触型 IC チップ）、所謂、電子財布や電子金庫内に暗号化により守られたストアードバリューとして、AMRO コインを保管・流通させることになる。

実際の実現方法については、既に実績のある日本の電子マネー発行の仕組みや狭義のブロックチェーンを応用する方法（例えば「中央銀行ないしは同等の機能を有する機関が法定通貨として発行することを目的とした電子マネーおよび電子マネーシステム」）などを参考に、安全で効率的な AMRO コインが提供できるよう検討することが望まれる。一例として、当該電子マネー発行の基本的な考え方、構成、特徴を別添に示す。

図表３．AMROコインのクロスボーダーでの利用




この AMRO コインが実現すると、国（エコノミー）を跨る（クロスボーダーでの）送金が可能となる（図表３）。

なお、他エコノミーが提供する AMRO コインが還流してきた場合には、AMRO コイン発行運営体に戻すこととなる。

## 4――AMRO コインの通貨としての信用力、一般受容性、ファイナリティ

通貨としての性能・機能を議論する場合、信用力、一般受容性、ファイナリティが重要な要素と言われている。通常、中央銀行が発行する通貨は、法的にも強制通用力を持っており、レンダーオブラストリゾートが発行するという中央銀行の信用力に裏付けられている。AMRO コインの信用力については、そのような法的な裏付けがなく、民間のデジタル通貨と同様な方法で安全資産としての AMRO コインの信用力を保証する必要がある。前述の実施方法の例では、各エコノミーの中央銀行ないしは政府が、AMRO コインの発行

に見合う債券などの資産を提供することにより、その信用力を保証することになる。また、AMRO の機能として ASEAN+3 各エコノミーの状況を監視（サーベイランス）・分析を行うことにより、もし何らかの問題が発生した場合には然るべき対応を施すことが可能であり、また、チェンマイ・イニシアティブ（CMIM）による救済手段も整っていることから、AMRO コインは、十分な信用力があると考えられる。次に、一般受容性については、当該通貨が、決済手段として広く人々に受入れられることが前提となるため、AMRO コインにとって最も重要な要件と言える。キャッシュレスが唱えられて既に相当の年月が経つにも拘らず日本では現金、国によって小切手が未だに一般的に通用している。これは、口座振替などの支払手段と比較し、現金や小切手による支払では相手の口座番号といった付加的な情報を知らなくても支払ができるということが、大きな要因の一つと言える。その一例が QR コードである。QR コードは、支払者が相手の口座番号などの情報を入力する手間を（QR コードを読むという行為により）省き利便性を格段に向上させた。これに対し、AMRO コインは「価値保蔵型」の支払手段であり、口座番号といった情報と紐づけられていない為、「カードでタッチする」、「携帯電話間で AMRO コインを送る」などの直接的な手段により支払（価値の移転）を完了することが可能であることが利点といえる。更に、AMRO コインのファイナリティとしては、「価値保蔵型」であることから、価値の移動により、ファイナリティを確保することができ、現金と同様なレベルを提供できるものと考えられる。

## 5――シニョレッジの配分

AMRO コインの発行の裏づけになる AMRO コイン発行用債券は AMRO のバランスシートの負債側に立つため、当該負債に見合う安全な資産が ASEAN+3 の中央銀行や政府機関から提供されることとなる。その資産（の運用等）から得た利益から、運営コストおよび将来のサービス拡張などに必要となる投資分を差し引いた金額は「シニョレッジ」として参加各国に配分される。「シニョレッジ」は、ASEAN+3 の中央銀行や政府機関から提供される安全な資産の出資額に応じて配分される。後述の通り、ドル化している国にとっては、AMRO コイン発行によるシニョレッジの配分を受けることは、メリットとなるが、自国通貨が流通する国では、AMRO コイン流通分シニョレッジが減少することを考えるとメリットは限定的と言える。

## 6――AMRO コインのメリット

このような地域デジタル通貨として AMRO コインを導入すると、次の通り様々なメリットを享受できることになる。メリットは、①デジタル通貨としての特性に加えて、②国境を超えるクロスボーダーな共通通貨としてのメリットがある。さらに、③プライベイトではなく公的管理が行われる通貨としてのメリットが指摘できる。

(1) 廉価な国際送金・国際決済の実現

前述のとおり AMRO コインを利用することにより、クロスボーダーでの労働者送金が自由に、手数料なしで、行うことができる。特に、携帯電話間での AMRO コインの移動が実現すると、個人間で、AMRO コインの転々流通性が確保される。従って、銀行口座を持たない人が多い開発途上国におけ

る送金や、更には、海外で働いている人が自国の家族に送金する場合（労働者送金）にも利用できる。また、マイクロファイナンスの実施・返済等にも利用可能となる。

さらにAMROコインにより従来と比較し廉価な手段で企業間の送金を行うことができる。ASEAN＋3地域では、サプライチェーンが発達しており、企業の製造・販売活動はすでに国境を越えて地域として一体化している。このため貿易面では、FTA（自由貿易協定）が締結され制度面での整備がされてきた。一方金融サービスは分断化されていた。デジタル共通通貨による地域ワイドの決済制度の整備によって、金融サービス面でも産業面での経済統合に映じた一体的なサービスが提供されることになる。

(2) 開発途上国（特にドル化国）への安定した通貨制度の提供

公的なデジタル共通通貨を導入することによって、現状では、通貨制度が安定しない国においても、AMROコインを法貨とすることにより安定した通貨を利用することができるようになる。また、ドル化している国にとっては、ドルに換えAMROコインを採用することにより、上記の通り、シニョレッジの確保が可能となる。

(3) 経済コストの削減

またこれは途上国に限らないが、デジタル通貨を導入することにより、社会的に経済コストが低下する。AMROコインは、利便性が高く、レジなどにおける支払に要する時間が短縮し省力化につながる（商店などによる利用者の利便性向上）。また、普及が進みコインを代替することにより、商店や金融機関における物理的なコインの取扱に必要なワークロードおよびコストの削減が期待できる。

(4) 安全性の確保

デジタル通貨が、公的に供給されることによって、より安全性の高い通貨が提供される。AMROコインでは、民間のデジタル（仮想）通貨のような、交換業者による受託仮想通貨の流出、交換業者の倒産といったリスクはないと言える。また、マネーロンダリング・テロ資金供与対策が可能であり、Financial Action Task Force (FATF)やBank Secrecy Act (BSA)への対応も可能となる。

(5) 感染症の物理的・直接的な伝染防止への寄与

支払手段として銀行券やコインを使った場合には、手渡しとなる場合が一般的であり、通貨を介してウイルスや病原菌が物理的・直接的に媒介する危険性がある。これに対し、AMROコインといったデジタル通貨を利用する場合には、(i) NFC（非接触型ICチップ）を内蔵するカードやモバイルデバイスをPOS端末に接触すること、(ii) モバイルデバイスや端末付属のスキャナーによるQRコードの読取り、(iii) モバイルデバイス間の電子的な授受、などにより、物理的な媒介物なしに通貨（データ）を伝達することで支払を完了することが可能となる[9]。従って、AMROコ

[9] Auer et al.(2000)の指摘によれば、紙幣を通じた感染率は、接触型のクレジットカードのターミナルやPINパ

インの利用により、ウイルスや病原菌の直接的な伝搬を相当程度抑えることが可能となると言える。

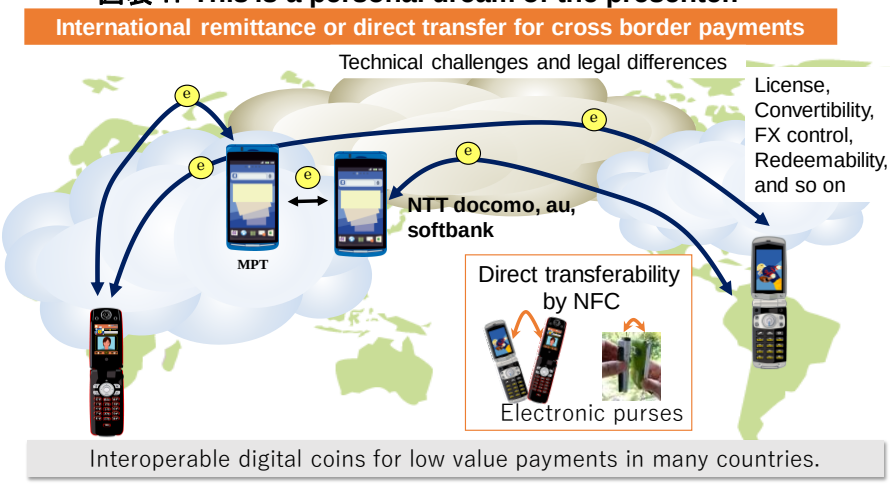
(6) 公平なサービスの提供

公的な枠組みでデジタル通貨が提供されることはより公平なサービスを提供できる。ASEAN+3 の国（エコノミー）の中には、全国民ないしは住民に国民番号や社会保障番号といった個別の ID が付与されており、同 ID と一意に紐着いた写真付きに身分保障カードを発行している国も見受けられる。そのような国においては、同 ID カードに非接触型 IC チップ（例えば NFC[10]）といったセキュリティレベルの高い AMRO コイン用電子財布を導入することにより、全国民が、AMRO コインを公平に利用することが可能となる。また、この ID カードは、社会保障や年金などの給付にも利用でき、更には、他国からの労働者送金の受取手段としても利用可能となる。

(7) 地域活動の活性化およびグローバル展開の展望

AMRO を中心とする中央銀行や政府機関が AMRO コインに関する議論を行う過程で地域会合の活性化や意思疎通の一層の円滑化が期待できる。場合によっては、通貨統合といったことも展望可能と言える。多国間の枠組みで通貨が提供されることは特に重要である。欧州中央銀行の事例にもあるように、多国間の枠組みでは、大国も小国も同じ権利を有している。このため、国際通貨は国際的なインフラであり大国が国際通貨を牛耳るという不適切な状態を回避することができる。

**図表4. This is a personal dream of the presenter.**




Note: This slide shows only a possible future image and does not explain any current solutions.

なお、本方法は、ASEAN+3 および AMRO という地域および機関だけでなく、ASEAN+3 を G20 に、AMRO を IMF に、ACU を SDR[11]に読み替えることにより、よりグローバルに展開できる可能性があると言える（図表４）。

(8) 「共通通貨」であり「単一通貨」ではないこと

---

ッドよりも低いとされている。

10 Near Field Communication

11 Special Drawing Right

本構想では、各国（エコノミー）ではAMROコインと各国通貨が併存して流通していることを想定している。欧州の場合は、1998年に、従来の共通通貨でなく各国通貨をユーロという単一通貨に統合することで、欧州金融市場を単一の市場とすることを目指した。これは当時の欧州の経済統合に向けた強い政治的な意思を反映している。単一通貨は、欧州に効率的な金融市場を推進したという大きなメリットがあった一方、加盟各国の金融政策の自由度を奪うなどデメリットがあったことは周知のとおりである。一方本構想のような各国通貨と併存した共通通貨は、金融市場の統合という点では、複雑となり単一通貨に劣るが、より柔軟性を持った仕組みであること、また欧州に比べ東アジアでは、政治的な意思は相対的には弱いことから、本構想では、共通通貨の導入としている。

## 7――課題と今後の対応

AMRO コインを実際に利用する場合、まだ多くの課題が残っている。例えば、日本では Near Field Communication（NFC）といった非接触型ICチップを搭載したスマートフォンやタブレット型端末が普及している。一方、日本以外では、プリペイド型の通信料金として通信会社等に価値を保存し、支払に利用できる国も多い。一般受容性の観点からは、全国民に国民IDが入った非接触型ICカードの配布や、それを読取る端末を提供するなどの対応が望まれる。また、AMROコイン運営センターをどの国に設置するのか、そのバックアップセンターはどうするのか、POS 端末などとのインターフェイスをどのような仕様にするのか等、AMROコインを実用的なレベルに持ち上げるためには、まだまだ多くの技術面での課題が残っていると言える。

また、各国政府が発行主体（AMRO）に資金拠出をする際の仕組み（法的根拠、予算、プロセス）、発行主体（AMRO）における業務としての位置付け、幾つかの国が発行を計画しつつあるCBDCや既存の仮想通貨や既存の金融システム（メガバンク等）との調整、金融政策への影響はどのように考えるのか、といった制度面、政策面での課題を解決する必要がある。更に、そもそも通貨単位として、何を採用するかという問題が残っている。ASEAN+3地域の通貨を考える場合、通貨バスケット制度（ACU建て）とすることが、理想と思われる。しかし、欧州でのユーロ誕生までの労力と時間を考えると、それは容易な事ではない。従って、まずは、米ドル建ての地域コインを発行するということも考えられる。更には、リブラ（通貨バスケットを活用）といった新しいサービスやそこで使われている技術を調査・検討し適用を試みることも重要と言える。

従って、AMROコインを実現するに当たっては、このような課題を洗い出し、実プロジェクトとして立ち上げることを展望し準備する必要がある。その為には、AMRO内に検討チームを組成し、1-2年程度を目途に対応策を検討し、ASEAN+3 代理者会合や総裁会合に諮れるレベルの検討結果を策定することが望まれる。いずれにせよ、より具体的な事項につき検証するとともに、AMRO（ASEAN+3）内に議論の場を設けることが考えられる。

## 8――おわりに

デジタル通貨を発行すること自体は、技術面でも運用面でも既に実用可能な段階に達している。ただ、一国のリーガルテンダーとして発行するか否かは、まだ議論の余地があるように見受けられる。そのような中で、デジタル通貨の特性を鑑みると、むしろ先にクロスボーダーで利用可能な小口の送金手段として、ないしは「価値保蔵型」の前払支払手段として、例えば ASEAN＋３地域で通用するような形で、導入することが考えられる。クロスボーダーでの取引、経済活動が安定的に伸びている ASEAN+3 地域では、地域の金融経済の発展・安定化に資するだけでなく、エコノミーを跨いで働く人にとって利便性が高まり、経済的にもメリットを享受できるようになることが展望される。
更に、もし AMRO コインが定着し、AMRO の通貨発行体としての信用力が十分に認められた暁には、AMRO コインを ASEAN+3 各国から提供される資産を超えて AMRO 独自に発行できるようになることを展望したい。

## 参考文献


雨宮正佳「日本銀行はデジタル通貨を発行すべきか」日本銀行、2019 年
雨宮正佳「中銀デジタル通貨と決済システムの将来像」日本銀行。2020 年
石田護　「为什么日中需要货币合作―经济上的要求和地缘政治含义」、『国際経済評論』、中国社会科学院経済与政治研究所、2007 年第 1 期
石田護「关于东亚共同体的重新思考:从功能路径到制度路径」、『国際経済評論』2014 年第 3 期、中国社会科学院経済与政治研究所、（「東アジア共同体再考：機能的アプローチから制度的アプローチへ」、『国際金融』、2014 年）
乾泰司「中央銀行ないしは同等の機能を有する機関が法定通貨として発行することを目的とした電子マネーおよび電子マネーシステム」、特願 2007-207208、2007 年
金融庁「仮想通貨交換業等に関する研究会報告書」2018 年、
金融法務研究会「仮想通貨に関する私法上・監督法上の諸問題の検討」2019 年
髙橋亘、「甦る永楽銭」『フィナンシャル・フォーラム』、京都総合研究所、2020 年
高村泰夫、生田駿至、澤田亮太郎「アジアの地域金融協力関連の会議について」、財務省、2018 年
津野大紀「円とアジア通貨の更なる利便性向上策の検討」、財務省、2017 年
中山靖司、森畠秀実、阿部正幸、藤崎英一郎　「電子マネーの一実現方式について」『金融研究』16 巻 2 号日本銀行金融研究所、1997 年
中山靖司、太田和夫、松本勉「電子マネーを構成する情報セキュリティ技術と安全性評価」『金融研究』18 巻 2 号　日本銀行金融研究所、1999 年
中山靖司、「電子マネー技術と特許」、IMES Discussion Paper Series No.98-J-33、 日本銀行金融研究所、1998 年、
柳川範之、山岡浩巳「情報技術革新・データ革命と中央銀行デジタル通貨」、日本銀行ワーキングペー

パーシリーズ　No19-J-1、2019 年
Auer, Raphael, Giulio Cornell and John Frost “Covid-19,cash, and the future of payments” BIS Bulltein No3, Bank for International Settlement, 2020
Adrian. Tobias, and Tommaso Mancini-Griffoli,”The Rise of Digital Money”,IMF、2019
Bank of Thailand,”Project DLT Scripless Bond”2019,
Brunnermeier, Markus K., Harold James, Jean-Pierre Landau, “The Digitalization of Money”, Working Paper 26300, National Bureau of Economic Research, 2019
Inui.Taiji,”A proposal to start a survey on electronic coins as a common currency issued by an international organization choosing SDR as the currency unit:a proposal for BIS”2010
Inui, Taiji,”Common Electronic Coin: a proposal for IMF”2014
Ishida. Mamoru, “Exchange Rate Instability: Japan’s Micro-Macro Experiences and Implications for China” in “China and World Economy”, Vol.14, No.2, Institute of World Economics and Politics, Chinese academy of Social Sciences, 2006
Lagarde. Christine,”Winds of Change: The Case for New Digital Currency”, IMF,2018
Nakamoto, Satoshi,”Bitcoin: A Peer-to-Peer Electronic Cash System”2008
Release master,”hyperledger-fabricdocs Documentation”Hyperledger, 2019
Takahashi.Wataru,”Financial Cooperation in East Asia: Potential Future Directions”Chap 2 in “Trade, Investment and Economic Integration of Volume II for Globalization, Development and Security in Asia”, World Scientific、2014

別添

中央銀行ないしは同等の機能を有する国際機関が法定通貨として
発行することを目的とした電子マネーおよび電子マネーシステム

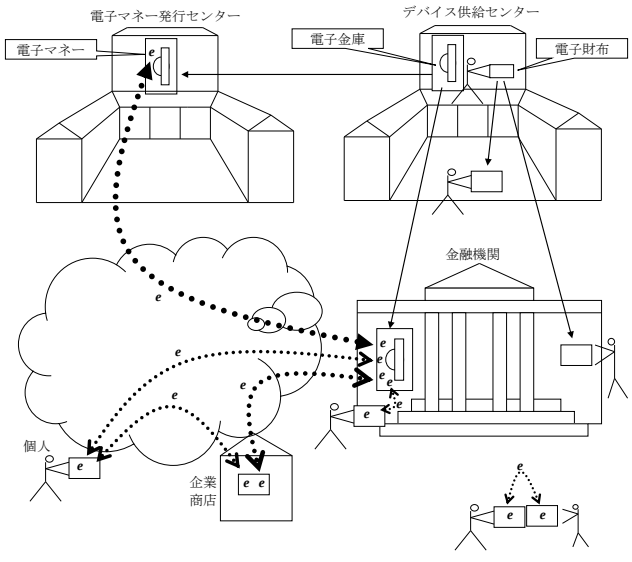
中央銀行などが法定通貨ないしは共通通貨として発行することを想定した電子マネーに関する技術である。特に、(1)中央銀行などの機関が電子マネーを発行する技術、(2)発行された電子マネーを政府機関ないしはそれに相当する組織が製作・提供する電子財布（同機関が承認する電子金庫を含む）に安全に保管する技術、(3)電子マネーが電子財布間を安全かつ確実に移動する技術、および(4)不正な電子マネーを発見（検知）する技術、等について記述。

注）本別添は、2007年に作成した文書の概要であるが、当時は、デジタル通貨という言葉がまだ一般的には使われていなかったことから、本別添ではデジタル通貨を電子マネーと記述している。また、各々の技術要素は、既に当時から安定的に使われているものであり、本案は、それらを組み合わせたものと認識している。従って、ここで示す技術要素は、既に安定したものと言える。今後、検討を進めるに当たっては、適切な技術・製品を調査選定し、より使い勝手が良く、安全で安定したサービスを提供できるように改善することが望まれる。

## 1. 概要

電子マネーを発行する電子マネー発行センターと物理的なタンパーレジスタンスを保障する電子財布を提供するデバイス供給センターを主要構成要素とする電子マネーシステムを提供する(図１参照)。電子マネーの認証には、電子マネー発行センターを認証局（CA）とするPKI技術を利用し、電子財布の認証には、デバイス供給センターを認証局（CA）とするPKI技術を利用する。本電子マネーシステムでは、秘密鍵のみならず公開鍵も含め全ての暗号鍵および電子マネーそのものが本電子マネーシステムの外部に露出しない仕組みを提供。また、電子マネーが偽造、改竄された場合に、そのような不正を速やかに検知するとともに不正への適切な対応が可能な仕組みを持つ電子マネーシステムを提供する。

【図1】

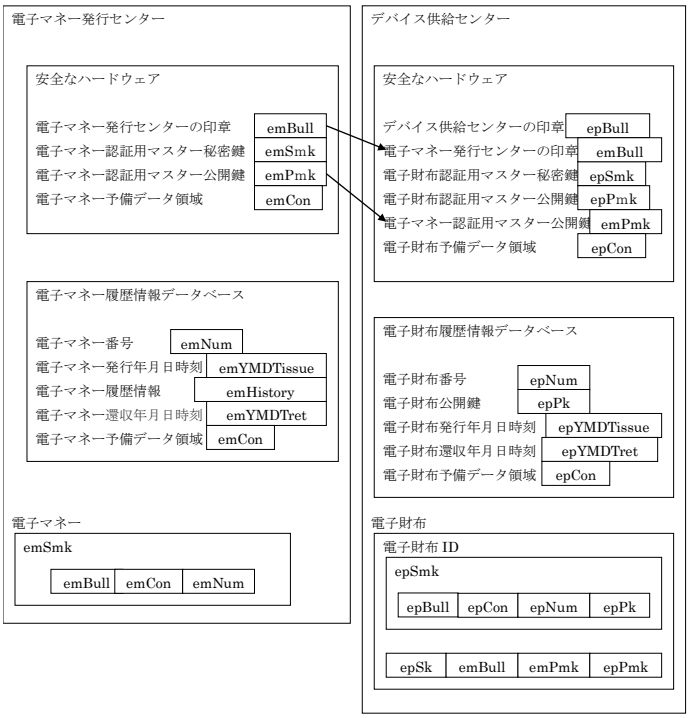



電子マネー発行センターは、中央銀行ないしはそれに類する機関が運営し、デバイス供給センターは、政府機関ないしはそれに類する機関が運営する。

## 2. 電子マネーおよび電子財布の発行

電子マネー発行センターでは、1組の電子マネー認証用マスター秘密鍵および電子マネー認証用マスター公開鍵を生成し、同センター内にある物理的にも情報セキュリティ的にも守られた安全な場所に電子マネー認証用マスター秘密鍵を保管する(図２参照)。電子マネー番号は、十分な桁数を持つ数字であり、初期値から順次数を増してゆく。電子マネー番号の位取記数法（10進数、16進数など）については、各システムにより決定する。「電子マネー番号」、「電子マネー発行センターの印章」、および将来、機能を追加するための「電子マネー予備データ領域」を合わせたものを電子マネーの1単位とし、電子マネー発行センター内にある電子マネー認証用マスター秘密鍵により暗号化することにより電子マネーを発行する。

【図2】




電子マネー発行センターでは、発行した電子マネー番号をキーとする電子マネー履歴情報データベースを構築し、発行年月日発行時刻および電子マネー予備データ領域を記録する。また、電子マネーが戻ってきた場合の各電子マネーの履歴情報格納場所を確保する。

デバイス供給センターでは、1組の電子財布認証用マスター秘密鍵と電子財布認証用マスター公開鍵を生成し、同センター内にある物理的にも情報セキュリティ的にも守られた安全な場所に電子財布認証用マスター秘密鍵を保管する(図２参照)。ICチップないしは同等以上の物理的セキュリティ、演算機能、データ保管機能を持つハードウェアを製造し、電子財布とする。電子財布は、デバイス供給センターでのみ初期設定を行うものとする。全ての電子財布に電子財布番号を付ける。

デバイス供給センターでは、各電子財布に固有の電子財布秘密鍵および電子財布公開鍵を生成する。「電子財布公開鍵」、「電子財布番号」、将来の機能追加のための「電子財布予備データ領域」、「デバイス供給センターの印章」、を合わせ電子財布認証用マスター秘密鍵で暗号化したものを「電子財布ID」と呼ぶこととする。

デバイス供給センターでは、各電子財布に電子財布IDを格納する。また、デバイス供給センターでは、各電子財布に「電子財布認証用マスター公開鍵」、「電子マネー認証用マスター公開鍵」、「電子マネ

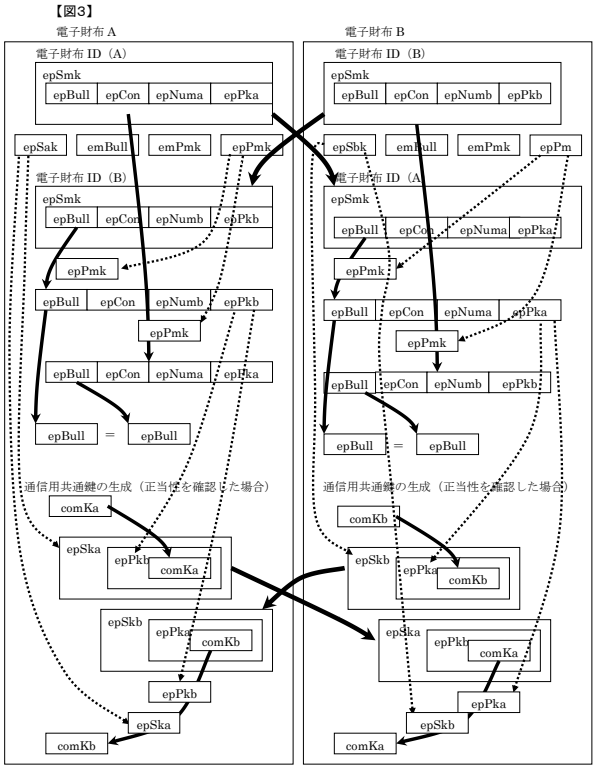
 

一発行センターの印章」、「電子財布秘密鍵」を格納し、これらのデータが、電子財布から漏洩しないように物理的セキュリティを確保する。特に、電子財布秘密鍵は、デバイス供給センターで発行された後は、各電子財布秘密鍵に対応する電子財布内以外には露出しないよう十分なセキュリティを確保する。

デバイス供給センターでは、電子財布番号、電子財布公開鍵、電子財布発行年月日時刻、電子財布還収年月日時刻、電子財布予備データ領域を電子財布履歴情報データベースに保管する。

## 3. 電子財布間の相互認証および一時的な通信用共通暗号化鍵の生成

まず、一方の電子財布(電子財布A)からもう一方の電子財布(電子財布B)に電子財布Aの電子財布IDを送る。電子財布Bでは、電子財布Aから送られてきた電子財布IDを電子財布認証公開鍵で復号化し、「デバイス供給センター印章」を確認することにより、電子財布Aが正規の電子財布であることを認証する(図３参照)。




電子財布Bは、認証結果を自らの電子財布秘密鍵および電子財布Aの電子財布公開鍵で暗号化し、電子財布Aに送る。その際、電子財布Aの正当性が確認できた場合には、今回の通信を暗号化するための一時的な通信用共通暗号化鍵を生成し、認証結果と併せ、前述のとおりの方法で暗号化し、電子財布Aに送る。電子財布Aでは、電子財布Bから送られてきた認証結果などの情報を自らの電子財布秘密鍵および電子財布Bの電子財布公開鍵で復号化する。

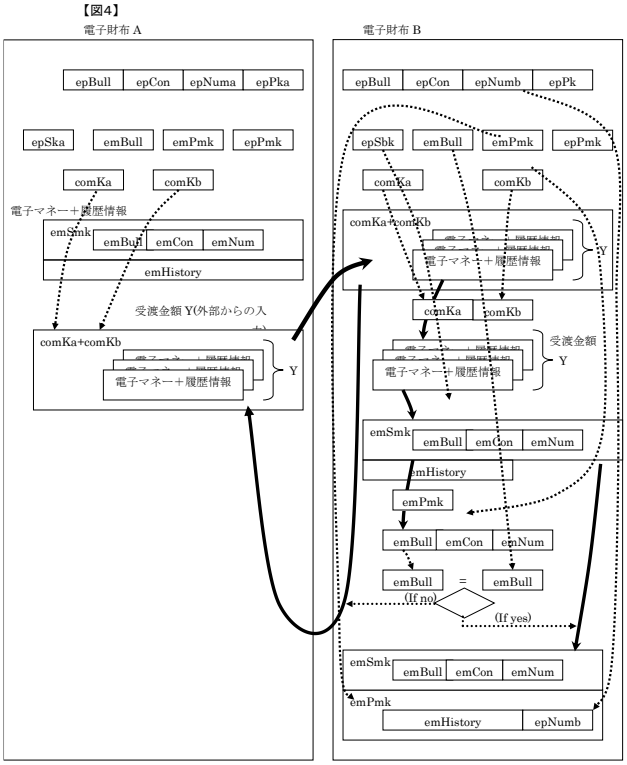
電子財布Bから電子財布Aに対しても同様な手順で電子財布IDを送ることにより、相互に認証を行い、相互に正当性を確認した場合には、通信用共通暗号化鍵を共有する。

## 4. 電子財布間での電子マネーの受け渡手順

電子財布間の相互認証が確立すると、電子財布間で電子マネーの受け渡しが行われる。指定された金額を仕向側電子財布から被仕向側電子財布に受け渡す。まず、仕向側電子財布において指定された金額と同数の電子マネーを集める。各電子マネーには、履歴情報が付加されている。履歴情報が付加された電子マネーを一括し、前述の通信用共通暗号化鍵（comKaおよびcomKb）で暗号化した上で、被仕向側電子財布に送る。被仕向側電子財布では、受け取った電子マネーを通信用共通暗号化鍵(comKaおよびcomdKb)で復号化した後、各電子マネーを電子マネー認証用マスター公開鍵で更に復号化し、電子マネー発行センターの印章を取り出す。各電子マネーに対し、この電子マネー発行センターの印章が、被仕向側電子財布に保管してある電子マネー発行センターの印章と同じであることを確認することにより、各電子マネーの正当性を確認する。また、受け取った電子マネーの数が、指定された金額に相当することを確認する。確認結果を仕向側の電子財布に通知する(図４参照)。

【図4】




正当性を確認し受け取った各電子マネーについては、付加されているこれまでの履歴情報に電子財布番号を追加し、履歴情報全体を電子マネー認証用マスター公開鍵で暗号化する。正当性を確認できなかった場合には、受け取った電子マネーを仕向側電子財布に送り返す。

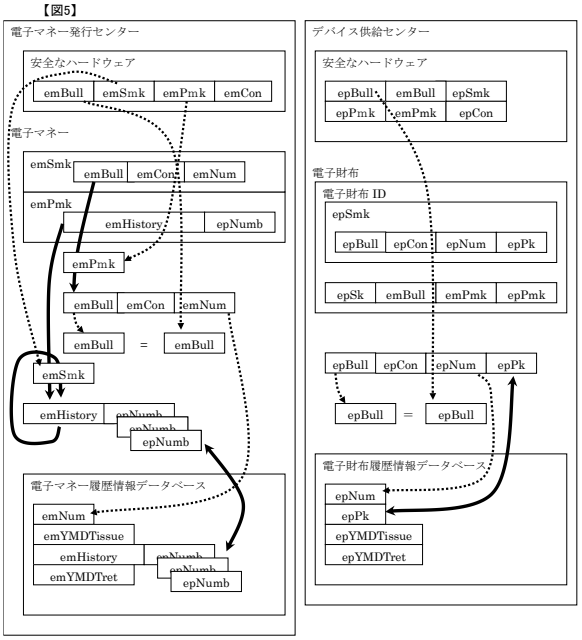
同一のセッション中における電子財布間の全ての通信は、通信用共通暗号化鍵で暗号化する。

## 5. 電子マネーおよび電子財布の不正な複製の検知方法

電子マネー発行センターに戻ってきた電子マネーについて、まず電子マネー認証用マスター公開鍵により復号化し、「電子マネー発行センターの印章」が正当なものであることを確認する。次に、履歴情報を、電子マネー認証マスター秘密鍵により繰り返し復号化することにより、当該電子マネーが今回発行された後に経由した全ての電子財布番号を抽出し、電子マネー履歴情報データベースに格納する。これを、当該電子マネーの履歴情報データベースで整合性を確認し、不正な複製の無いことを確認する(図５参照)。もし、履歴情報に不整合が検出された場合には、予め決められた先に通知する。

【図5】




電子財布は一定期間毎に、回収し、複製や改ざんなどの不正が行われていないかを電子財布データベースの記録をもとに確認する。

電子マネーの不正な複製などの可能性がある場合には、問題が発生した可能性のある電子財布番号を電子金庫に通知・連絡する。また、当該電子財布が使われた場合には直ちに電子金庫から電子マネー発行センターおよびデバイス供給センターに報告される。