中央銀行デジタル通貨（CBDC）におけるセキュリティ考察

日本電気株式会社　シニアエキスパート
デジタルアイデンティティ WG　リーダー
宮川　晃一

1．はじめに

デジタル通貨と聞くと、一般的にはビットコインに代表される仮想通貨（暗号資産）のことを思い浮かべる方が多いかと思うが、ここでは国の通貨すなわち、自国の中央銀行で発行される通貨のデジタル通貨（ 以下、CBDC：Central Bank Digital Currency ）を対象とする。

デジタル通貨については、日本国において現状では導入検討および実験段階にあり、具体的に発行されるかは決定されていないが、現状で考えられるセキュリティ課題、特にデジタルアイデンティティにフォーカスして考察したので解説する。

2．CBDC検討の背景

CBDCのセキュリティ考察の前に、日本におけるCBDCが検討されるようになった背景や諸外国の状況ついて整理した。

2.1 現在通貨の課題

我が国ではデジタル田園都市国家構想をはじめとして、社会基盤そのものがデジタル化に向けて大きく変革をしようとしているが、その中でもデジタル化が難しいとされている1つが「日本銀行券」すなわち「通貨」と言われている。現状「通貨」には以下のような特徴がある。

（メリット）
- ・国内では、いつでも、だれでも利用ができる（ユニバーサル性）
- ・即時に決済が完了できる（即時決済性）
- ・他国の通貨と交換可能（相互運用性）
- ・電力を必要としない（デジタル対比）　　など

（デメリット：主に現金）
- ・「通貨」を持っている人が「所有者」であるため、「通貨」 自身から「所有者」を判別できない
- ・盗難・紛失や火災などの災害に弱い
- ・偽造対策等セキュリティ対策にコストがかかる
- ・資産の把握が難しい　　など

2.2 デジタル時代に向けた課題

一方、デジタル化に向けた課題として、民間の決済サービス（クレジットカード、電子マネー、QRコード決済サービスなど）にて複数の事件・事故が発生しており、その安全性や堅牢性および補償については今後も十分な検討と対策が必要な状況にある。また、同時に中小小売店のキャッシュレス化の促進を行う必要があり、民間レベルで解決するのは難しい実情もある。また、COVID-19を背景にした給付金等の配布については多大なコストをかけて各省庁や自治体等が実施している状況があり、これら課題に対して「デジタル通貨」が果たす役割は大きなものになると思われる。

※本書の内容は私見であり、必ずしも所属企業先の見解と一致したものではありません。

3．CBDCとは

具体的にCBDCとはどのようなものか、特徴などについて整理する。

3.1 デジタル通貨の分類

IMF（国際通貨基金）レポートによると「デジタル通貨」は以下（図01）のように分類される。（発行主体別、価格変動の有無、世界中で発行決済可能かと言った分類）

- CBDCは発行主体が中央銀行である点が他のデジタル通貨と大きな差がある。
- 民間主体のデジタル通貨は価値が変動することや、補償がない場合もある。

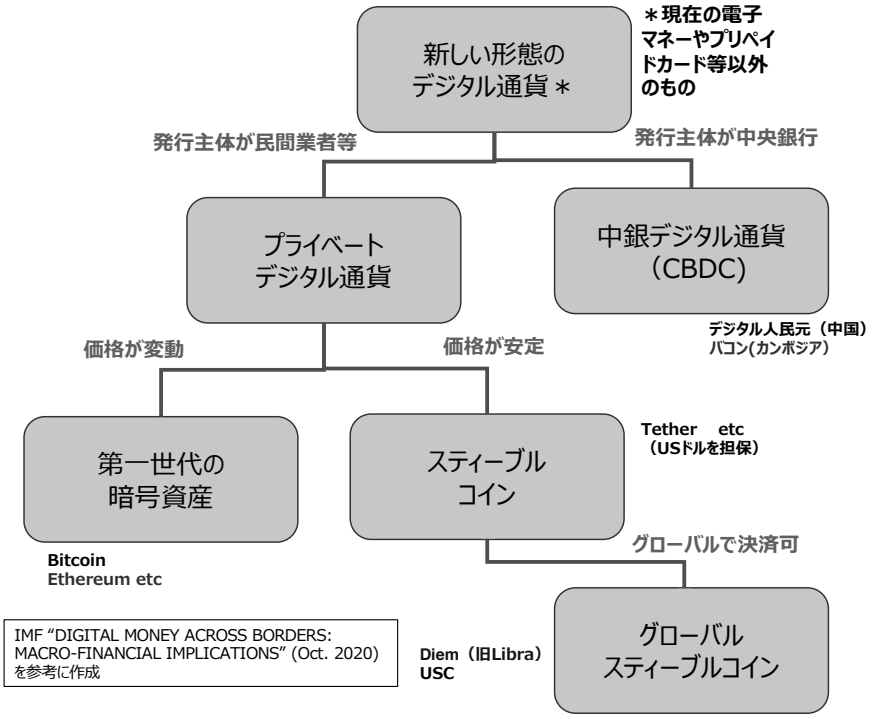


図01　デジタル通貨の分類

3.2 CBDCの特徴

Bitcoinのような暗号通貨が特定の団体や企業などによって発行されるのに対し、CBDCではあくまで各国の中央銀行が発行する。法定通貨ではない暗号通貨はその価値がそのときどきで変化する。一方で、CBDCはあくまで現行の法定通貨と等価であり、その価値は変化しない。こうした価値が特定条件で固定されるデジタル通貨を「スティーブルコイン」と呼ぶ。２章で述べたデジタル化の課題の解決の他にも、CBDCを通じて各国の金融システムが接続されれば、現状でSWIFT(国際送金）を使って行なわれているメッセージ中継がよりシンプルで高速なものになり、送金手数料も安価となるメリットがある。そしてブロックチェーン技術を用いてスケーラビリティやパフォーマン

スの問題を解決できれば、既存金融システムの置き換えで資金の流通がよりスムーズで活発になると想定されている。

CBDCの発行形態や管理方法については以下のようなものがある。また、発行形態と管理方法の組み合わせで4つのモデルがある。（図02）それぞれ、実際に運用するには法的な根拠の整備も含めて検討が必要な状況である。

（発行形態）

・**直接型**：各国中央銀行が直接CBDCを配る

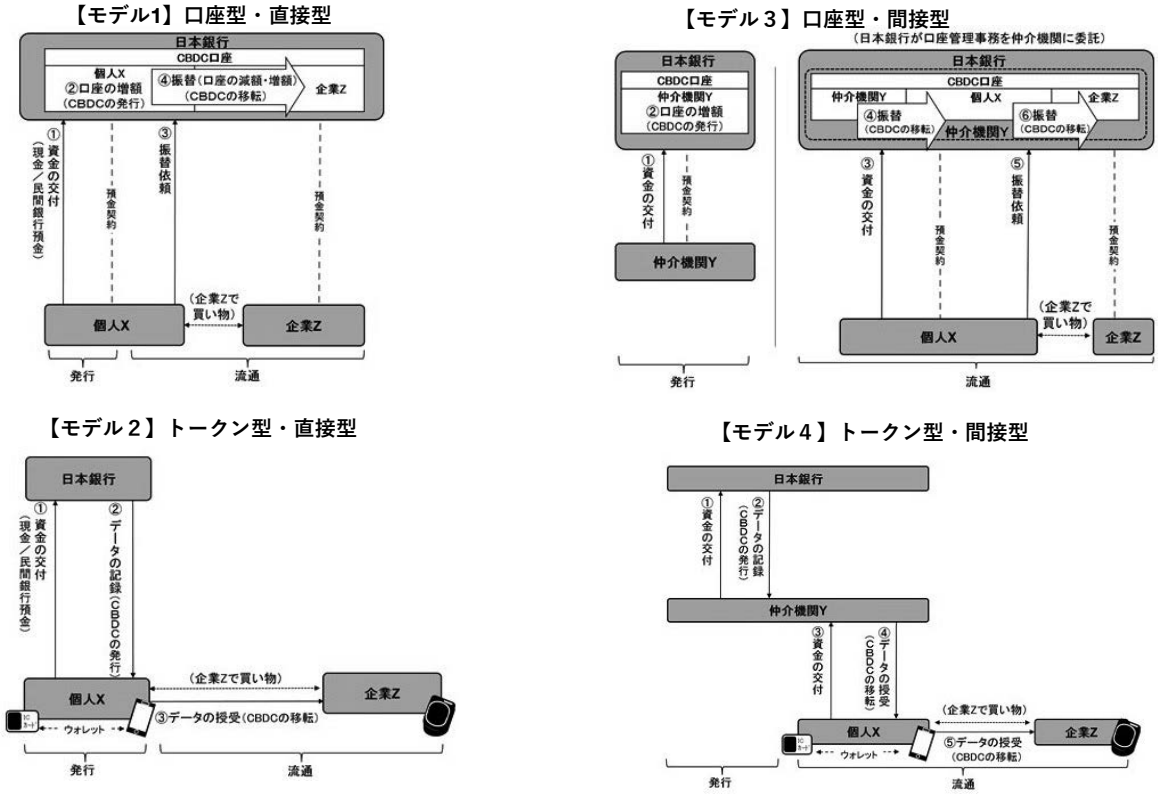
・**間接型**：民間の銀行を介してCBDCを配る

どちらの発行形態においても、AMLのためのKYC機能の実装が必要であり、アプリケーションのセキュリティ対策・機能追加のため継続的なアップデートが必要になる。間接発行の場合はこの役割を銀行が担う形になる。

（管理方法）

・**口座型**：利用者からの振替依頼に基づき、発行者が口座の減額記帳および増額記帳をすることにより、価値が移転する方式。銀行預金がその代表例

・**トークン型**：何らかの媒体に金銭的価値が組み込まれたものであり、銀行券や交通系カードなどの電子マネー等があたる。これらは、紙と電子媒体という違いはあっても、媒体に組み込まれた金銭的価値の移転によって決済を行うという基本的な仕組みは共通である。



https://www.boj.or.jp/research/wps_rev/lab/lab19j02.htm/

出典：中央銀行がデジタル通貨を発行する場合に法的に何が論点になりうるのか：
「中央銀行デジタル通貨に関する法律問題研究会」報告書の概要

図02　CBDCの発行形態と管理方法のモデル

3.3 CBDCの基本要素

CBDCを実装する上で必要な基本要素について以下に解説する。

・ユニバーサルアクセス

現金と同様に、「誰でも使える」原則である。支払いや送金に使用する端末やカードなどによって利用者を制限することがないような工夫が求められる。

・セキュリティ

安心・安全にCBDCを利用するには、偽造や不正行為を排除するために高度なセキュリティ対策が必要である。

・強靭性

「いつでも、どこでも使える」ものとするための原則である。利用者が24時間365日利用できる仕組みが求められる。特に自然災害などで電力が確保できない場合の想定などは重要なポイントとなる。

・即時決済性

現金と同様に決済の支払い完了性ならびに即時決済性が求められる。また、多数の利用者が一斉に決済を行なったとしても問題のない仕組みが要求されることから、十分なシステムの拡張性や柔軟性が求められる。

・相互運用性

民間の決済システムとの相互運用性の確保や将来の高度な決済サービスに適応できるような柔軟な構造が求められる。

4．諸外国および国内の取り組み状況

4.1 諸外国の状況

世界各国の中央銀行は急速に中銀デジタル通貨への関心を高めており、特に新興国で積極的である。中国では基軸通貨米ドル支配からの脱却、人民元の国際化を企図し、デジタル人民元の開発を急ピッチで進めており、大規模な実証実験を進めている。また、多国間によるマルチCBDCの議論も始まっている。

（米国） 米連邦準備理事会（FRB)はCBDCに対し慎重な姿勢だが、他国と協調しながら、技術研究や必要な規制整備の議論は世界の先頭にたって進めていくという考えを示している。
2022年1月、FRBはCBDCに関するディスカッションペーパーを公表し、CBDCへの取り組みをやや前向きに進めていく方向性を示した。

（EU） 欧州中央銀行は2020年10月、デジタルユーロに関する報告書（ECB "Report on a digital euro"を公表し、デジタルユーロ発行における原則と要件を定めた。
この報告書に基づき公募した意見を基に、デジタルユーロを発行するか否かの方針を発表する予定。

（インド）インド政府は2022年2月にインド準備銀行がCBDC（デジタル・ルピー）を2023年年度中に導入する計画を発表した。

4.2 国内の状況

日本銀行は、現時点でCBDCを発行する計画はないが、将来必要になった場合に対応できるよう検討を進めており、期待される機能と役割、具備すべき基本的な特性や考慮すべきポイントを整理した。また、システム的な実験環境を構築しCBDCの機能に関する概念実証をおこなっている。また、さらなる検証が必要と判断されれば民間事業者や消費者が実地に参加する形でのパイロット実験を行うことも視野に入れて検討する。としている。
しかしながら、実現までには課題も多く、まだ相当の時間がかかると思われる。民間でも、様々な業界の主要各社

30社以上がそれぞれの分野で求められるCBDCの仕組みの検証を行う「デジタル通貨勉強会」プロジェクトが発足し、2020年11月に最終報告書のリリースと「デジタル通貨フォーラム」の結成を行った。「デジタル通貨フォーラム」では、CBDCそのものではなく、民間銀行主体のデジタル通貨を目指しており、CBDCとは補完する関係として検討がすすめられている。

5．CBDCにおけるセキュリティ考察

CBDCにおけるセキュリティを7要素で分類して考察してみる。また、後半でデジタルアイデンティティの課題について考察した。

5.1　情報セキュリティの7要素

一般的に情報セキュリティはＣＩＡで語られることが多いが、今回はＣＩＡ+4つの要素の7要素にて考察する。各要素の簡単な説明は以下の通りである。

機密性（Confidentiality）　情報が漏れないこと
完全性（Integrity）　情報が改ざんされることなく維持されること
可用性（Availability）　情報を利用したい時に利用できること
真正性（Authenticity）　情報およびその利用者が本物（本人）と確認できること
信頼性（Reliability）　情報システムを構成する機器が意図した通りに動作していること
責任追跡性（Accountability）　問題が発生した時のその動作が開始された元まで追跡できること
否認防止（Non-repudiation）　あとから否認（否定）ができないこと

5.2　CBDCにおける7要素の考察

CBDCの基本要素と特に強く関係性があると思われる事項について考察を行なった。

1）機密性

CBDCでは、誰がいくら保持しているかの情報や、いつ誰がどこでどのような決済にいくら決済したかの情報がデジタルで記録されることになる。このような情報はプライバシーな情報であり、その取得や管理及び利用については十分な検討が必要である。もちろん、デジタル通貨自体へのアクセスは厳密に管理ができる仕組み（デジタルウォレット等）が必須である。また、採用する方式によっては利用するデバイスのセキュア領域や鍵管理などの検討も必要。デジタルアイデンティティとの関係性について後述する。

2）完全性

「通貨」において、その価値が毀損されることは大きな問題である。CBDCにおいても、「改ざん」ができない仕組みが求められる。暗号通貨にブロックチェーンが利用される背景はここにある。

3）可用性

CBDCの基本要素である「強靭性」と関係性がある。利用者が２４時間３６５日利用できる仕組みが求められる。また、誰でも使えるようにしなければならないことから、ユニバーサル性も「可用性」に該当すると考える。

4）真正性

デジタル世界においては、物理世界との結びつきである本人性が非常に重要である。金融の世界ではAMLの観点からKYCが重要視されているがCBDCにおいても、本人確認（個人・法人問わず）が重要事項である。デジタルアイデンティティとの関係性について後述する。

5）信頼性

CBDCの基本要素である「即時決済性」が該当すると考える。多数の利用者が一斉に高度な決済をおこなっても正確、即時処理できるシステムの信頼性を重要である。また、災害や障害にも強い仕組みやシステムが要求される。

6）責任追跡性

何か問題が発生した場合、その処理が行われたログを確実に保管しておくことは重要である。仮に係争になった場合にも耐えられるような仕組みが必要である。デジタルアイデンティティとの関係性について後述する。

7）否認防止

決済や送金においては、確実に行われたことを保証する必要がある。それは、決済や送金がされてないと相手から否認された時の重要な証拠になり得るからである。デジタル署名技術などの活用が考えられる。

5.3　CBDCにおけるデジタルアイデンティティの重要性

「インターネット上ではあなたが犬だと誰も知らない」（On the Internet, nobody knows you're a dog）（図03）という有名な戯画がある。お分かりのとおり、インターネットを通した端末を操作しているのは正当な本人ではないかもしれないことを示唆している。

CBDCの実現には確実なデジタルアイデンティティ管理の実現が不可欠である。現在、金融口座開設時には犯罪収益移転防止法に則した「本人確認」が金融機関の業務としてマネーロンダリングを防止することを目的に行われている。

出典：Wikipedia: On the Internet, nobody knows you're a dog
https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

図03　On the Internet, nobody knows you're a dog

CBDCにおいは、３.２文で述べた4つのモデルのどれにおいても「本人確認」は非常に重要な事項であり確実に実施する必要がある。よって、CBDCにはAML/KYCの機能実装は不可欠であり、かつ様々な決済や送金の高度化や自動化に柔軟に対応できる AML/KYCが必要である。

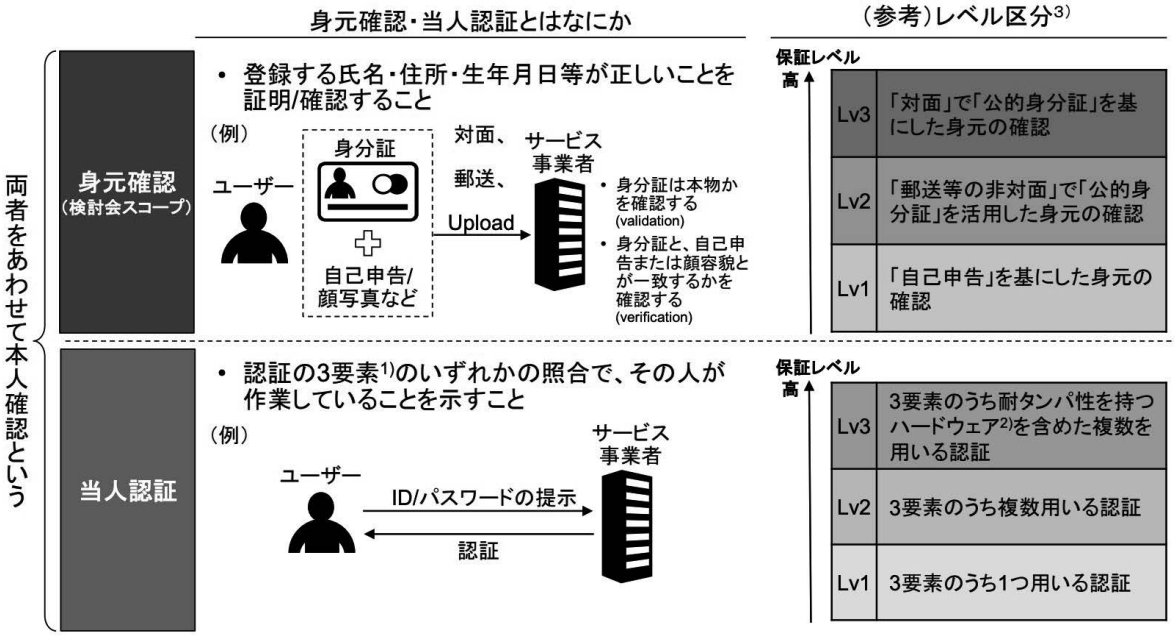
ここで、今一度確認すべき事項として「本人確認」がある。「本人確認」には「身元確認」と「当人認証」の2つの

側面がある。「身元確認」は、ユーザー当人の実在性を確認し、「当人認証」は、ユーザーの行為を確認する。通常両方の組み合わせを通じて「本人確認」が行われる仕組みである。（図０４参照）

また、５. 1の７要素の「機密性」「真正性」はまさに「本人確認」そのものである。CBDCにおけるKYCは「身元確認」であり、実際に利用する場合は「当人認証」によって真正性が担保され利用する。「身元確認」は初回時の確認（On Boarding）とその後の継続的に確認（On Going）するものに大別されるが、CBDCのユニバーサル性を考慮しながら継続的に「身元確認」を行うには、CBDC利用者の信頼の源泉（トラストアンカー）が必要になる。

CBDCの利用者という側面から考えると、個人以外にも法人や訪日・在留外国人等もあるため、CBDCにおけるトラストアンカーおよび保証レベルをどのように定義するかは、今後真剣に検討が必要と思う。欧州にて構想中の欧州デジタルIDウォレット（European Digital Identity Wallet）等を参考にすべきと考える。

CBDCは現金と同様の機能を持たせるべきとの意見もある。現金は持っている人が所有者であり、決済する度に「本人確認」をされることは高額な決済を除いてほぼない。CBDCにおいても、少額決済においては匿名性を持たせる必要があるとの意見である。これは、Pseudonymization（注１）と言われる手法で匿名化（仮名化）を行うことが可能になる。仮名化は匿名化と違い可逆性があるのが特徴とされる。よって、「責任追跡性」が失われることがない。CBDCはこのように一定のプライバシーに配慮したものでなければ、国際的な相互運用は難しいと思われる。



1)認証要素は「生体」（顔・指紋など）・「所持」（マイナンバーカードなど）・「知識」（パスワードなど）に分かれる
2)マイナンバーカードなど、内部の情報に対する不正な読み出しが困難である物理装置
3)「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（2019年2月CIO連絡会議決定）のレベル区分

出典：オンラインサービスにおける 身元確認手法の整理に関する 検討報告書
https://www.meti.go.jp/press/2020/04/20200417002/20200417002-1.pdf

図０４　本人確認とは

6．最後に

現在、日本のCBDCについては具体的な実施計画はないものの、世界情勢を見ながら実証実験を進めつつ議論が深まって行くと思われる。今回はデジタルアイデンティティに少しフォーカスして考察したが、他にも検討すべき技術課題（例えば、CBDCにリンクする形でのデジタルウォレット技術の標準化など）や法的課題（日本銀行法の改定など）が多くある。CBDCは今後のデジタル時代には必須のインフラとなることから、これら課題を慎重に議論し進めて欲しいと思うが、セキュリティと利便性のバランスを高次元でバランスした安心・安全の仕組みをぜひ構築して欲しい。

【参考文献】

[1] 日本銀行：中央銀行デジタル通貨に関する日本銀行の取り組み方針
https://www.boj.or.jp/announcements/release_2020/data/rel201009e1.pdf

[2] 日本銀行：中央銀行デジタル通貨：エグゼクティブ・ペーパー
https://www.boj.or.jp/announcements/release_2021/data/rel210930e1.pdf

[3] 井上哲也：デジタル円 日銀が暗号通貨を発行する日－日本経済新聞出版 (2020/7/18)

[4] 木内 登英：決定版　銀行デジタル革命―現金消滅で金融はどう変わるか
東洋経済新報社 (2018/8/24)

[5] IMF “DIGITAL MONEY ACROSS BORDERS: MACRO-FINANCIAL IMPLICATIONS” (Oct. 2020)
https://www.imf.org/en/Publications/Policy-Papers/Issues/2020/10/17/Digital-Money-Across-Borders-Macro-Financial-Implications-49823

[6] デジタル通貨勉強会
https://about.decurret.com/dc-forum/studygroup.html

[7] デジタル通貨フォーラム
https://about.decurret.com/dc-forum/

注1）Pseudonymization
スードニマイゼーション（Pseudonymization）：仮名化
氏名や住所などの個人データのうち、「誰」と特定できる部分を「仮名」に暗号化し、データから直接個人を特定できなくすること。