



BOJ
Reports & Research Papers

決済システムレポート別冊シリーズ

Payment and
Settlement
Systems
Report - Annex

デジタル通貨に関連する
情報技術の標準化

日 本 銀 行
決 済 機 構 局
2021 年 5 月

(決済システムレポート別冊シリーズについて)

日本銀行は、決済システムの動向を鳥瞰し、評価するとともに、決済システムの安全性・効率性の向上に向けた日本銀行および関係機関の取組みを紹介することを目的として、「決済システムレポート」を定期的に公表している。

「決済システムレポート別冊シリーズ」は、決済システムを巡る特定のテーマについて、掘り下げた調査分析を行うものである。今回は、デジタル通貨に関連する情報技術の標準化について考察する。本稿は、日本銀行が2020年10月に公表した「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」において、今後の制度設計面の検討項目のひとつとして掲げた「デジタル通貨に関連する情報技術の標準化のあり方」にかかる検討の一環として取り組んだものである。

決済システムレポートの内容について、商用目的で転載・複製を行う場合は、あらかじめ日本銀行決済機構局までご相談ください。転載・複製を行う場合は、出所を明記してください。

【本レポートに関する照会先】

日本銀行決済機構局決済システム課 (post.pr@boj.or.jp)

デジタル通貨に関連する情報技術の標準化

■要 旨■

金融サービスの分野では、銀行の預金・融資・振込や証券会社の有価証券売買の仲介等の金融取引を円滑に行うため、取引情報を伝送するメッセージフォーマットや付番・コード体系、暗号化方式等の情報セキュリティ技術といった様々な標準化の取り組みが行われてきている。

こうした標準化は、①金融取引を処理するシステム間の相互運用性の確保や、②システムに対する信頼性の確保を通じて、金融機関の事務効率化や顧客の安全性・利便性の向上に寄与してきている。現代の金融サービスが高度な情報技術に支えられる中であって、③先進技術に関する専門的知見を集約・活用する手段として、国際的な標準化活動に民間事業者や専門家など国内関係者が参画することの重要性も増している。

資金決済の世界では、従来からの銀行等による振込・送金のほか、近年は、資金移動業者による多様な資金移動サービスも提供されている。さらに最近では、ブロックチェーンや分散型台帳技術を用いたステーブルコインなど、民間主体が発行する新たなデジタル通貨の可能性を模索する動きもみられる。こうした新たなデジタル通貨を検討していくうえでも、①相互運用性の確保、②信頼性の確保、③専門的知見の集約・活用手段という標準化の意義は大きく、既存の金融サービス分野の国際標準は参考になる。

中央銀行デジタル通貨（CBDC：Central Bank Digital Currency）においても、デジタル通貨における標準化の意義が当てはまる点が多い。日本銀行では、CBDCの検討を進めるに当たって、中央銀行間の強固なネットワークを活かすとともに、民間の事業者や専門家など、幅広い関係者との協力・連携が必要であると認識している。CBDCを巡る国際標準化の分野でも国内関係者としてしっかり連携していきたいと考えている。

[目 次]

1. はじめに	1
2. デジタル通貨における標準化の意義	2
3. デジタル通貨における標準化領域	6
4. おわりに — CBDC に関する標準化のあり方 —	17

1. はじめに

日本銀行は、2020年10月に「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」（以下、「取り組み方針」）を公表した。中央銀行デジタル通貨（CBDC：Central Bank Digital Currency）とは、民間銀行が中央銀行に保有する当座預金とは異なる、新たな形態の電子的な中央銀行マネーである¹。日本銀行としては、現時点でCBDCを発行する計画はないが、決済システム全体の安定性と効率性を確保する観点から、今後の様々な環境変化に的確に対応できるよう、しっかり準備しておくことが重要と考えている。

「取り組み方針」では、個人や企業を含む幅広い主体の利用を想定した「一般利用型CBDC」に期待される機能・役割や具備すべき特性等を整理している。そのうえで、CBDCの検討を進める際に考慮すべきポイントとして、①物価の安定や金融システムの安定との関係、②イノベーションの促進、③プライバシーの確保と利用者情報の取扱い、④クロスボーダー決済との関係を挙げている。

このうち、クロスボーダー決済との関係では、各国CBDCの相互運用性を確保していくことの重要性を踏まえ、データフォーマット等の国際標準化についても各国間で積極的に議論していくことが大切であると指摘している。本稿は、こうした「取り組み方針」の考え方のもと、今後の制度設計面での重要な検討項目のひとつとして、デジタル通貨に関連する情報技術の標準化のあり方について考察を行うものである。

日本銀行決済機構局は、経済産業省に設置された日本産業標準調査会（JISC：Japanese Industrial Standards Committee）からの委託を受け、ISO/TC 68の国内委員会事務局を務めている。ISO/TC 68とは、国際標準化機構（ISO：International Organization for Standardization）において金融サービス分野の国際標準化を担当する専門委員会（TC：Technical Committee）である。本稿では、こうした活動を通じて日本銀行が蓄積してきた知見をもとに、デジタル通貨の標準化の意義や標準化対象となりうる領域について考察している。

本稿の構成は以下のとおりである。次の2節では、金融サービス分野の標準化を参考に、デジタル通貨における標準化の意義を考える。そのうえで、続く3節では、金融サービス分野の国際標準化を紹介しつつ、デジタル通貨に関する具体的な標準化領域を検討する。最後の4節では、CBDCに関する標準化のあり方にも触れながら、本稿を締め括る。

¹ Committee on Payment and Market Infrastructures (CPMI) and Markets Committee, "Central bank digital currencies," March 2018.

2. デジタル通貨における標準化の意義

(1) 標準化とは何か

そもそも「標準化」という言葉は、一般に馴染みが薄いと思われる。JIS（日本産業規格）で知られる国内標準を審議する JISC では、「標準化」を、「自由に放置すれば、多様化、複雑化、無秩序化する事柄を少数化、単純化、秩序化すること」と定義している²。身近な例では、A3 や A4 といった用紙のサイズや、単 3 電池や単 4 電池といった乾電池の仕様がある。これらのサイズや仕様が標準化されていることで、消費者は、メーカーが異なっても同じように使える製品を容易に手に入れることができる。

標準化は、こうした消費者の利便性向上とともに、事業者にとっても様々な意義・効果がある³。例えば、工業製品のサイズや仕様が標準化されることで、大量生産が可能となり、製品価格を下げやすくなるため、市場拡大も図られると期待される。また、製品・サービスの品質表示方法等を標準化することで、取引コストの削減にも寄与する。さらに、標準として世の中に公開されることで、新しい技術の普及や産業の発展にも役立っている。

このほか、近年、情報通信技術の発達によって様々なビジネス分野でデジタル化が進む中、標準化が、製品・サービスの相互運用性（異なるシステムや仕組みを互いに連携させる能力⁴）の向上を通じたネットワーク効果（利用者が多く集まるほど、利用者が得る便益が高まる効果）の発揮につながることを期待されるようになってきている。また、品質管理、環境対応、情報セキュリティといった分野で事業者の体制整備を客観的に評価する仕組みを提供することで、事業者に対する信頼性の確保に役立つ標準も増えている。

(2) 金融サービス分野の標準化

銀行の預金・融資・振込、証券会社の有価証券売買の仲介など、金融機関は多様な金融サービスを提供している。こうした金融サービスの分野でも、金融取引を円滑に行うため、標準化に関する様々な取り組みが行われてきている。

歴史を振り返ると、金融取引がペーパーベースで行われていた時代には、手形・小切手や帳票類の様式等に関する標準化が中心であった。その後、金融取引のオンライン処理が

² 日本産業標準調査会、「産業標準化について」(<https://www.jisc.go.jp/jis-act/>)

³ 標準化に期待される意義・効果については、田中正躬、『国際標準の考え方 グローバル時代への新しい指針』、東京大学出版会を参照した。

⁴ ここでは一般的な定義を示しているが、より厳密にみていくと、相互運用性には様々な達成レベルがある。3 節では相互運用性の具体的な中身にも若干触れる。

進んでくると、取引情報を伝送するためのメッセージフォーマットや付番・コード体系等が標準化の対象に加わり、これによって、金融取引を処理するシステム間の相互運用性が向上することとなった。さらに、金融取引が高度に電子化されると、暗号化方式、ICカード、生体認証といった情報セキュリティ技術が標準化の対象となった。これらの標準化により、金融取引の安全性が一定水準以上に保たれ、取引を処理するシステムの信頼性が確保されるようになった。

このように、現代における金融サービス分野の標準化は、金融取引を処理するシステム間の「相互運用性の確保」や、システムに対する「信頼性の確保」という意義をもたらし、ひいては金融機関の事務効率化や顧客の安全性・利便性の向上に寄与してきている。

標準化の取り組みは、金融のグローバル化の進展に応じて、国際的にも活発に行われるようになってきている。それに伴い、金融業界のほか、金融サービスに関連する技術を持つ事業者や専門家が国際標準化の活動に参画することの重要性も増している。現代の金融サービスは高度な情報技術に支えられており、とりわけ最近のデジタル化や経済のサービス化によって、先進的な情報技術を取り入れることの重要性が一段と増している。こうした状況のもと、近年、標準化の取り組みには、先進技術を始めとする「専門的知見の集約・活用手段」という新たな意義が見出されてきている。

(3) デジタル通貨の標準化

以上の金融サービス分野における標準化の意義（①相互運用性の確保、②信頼性の確保、③専門的知見の集約・活用手段）は、民間主体等で最近検討されているデジタル通貨においても変わらず重要である。

資金決済の世界では、従来からの銀行等による振込・送金のほか、近年は、資金移動業者による多様な資金移動サービスも提供されている。さらに、最近では、デジタル技術を用いた資金決済手段の意味で「デジタル通貨」を捉えたうえで、ブロックチェーンや分散型台帳技術（DLT : Distributed Ledger Technology）を用いたステーブルコインなど、民間主体が発行する新たなデジタル通貨の可能性を模索する動きもみられる。

以下では、こうした新たなデジタル通貨を検討していくうえでの標準化の意義として、①相互運用性の確保、②信頼性の確保、③専門的知見の集約・活用手段の3点について、やや詳しく説明する。

（相互運用性の確保）

資金決済を扱うプラットフォームにおいて、相互運用性の確保は特に重要である。相互運用性の確保は、複数のプラットフォーム間のデータ交換を容易にし、各々のユーザーに対し、単独のプラットフォームを利用するだけでは得られないネットワーク効果を新たにもたらすことになる。

デジタル通貨は、個人や企業など幅広いユーザーを対象に、支払や送金という汎用性の高い資金決済サービスを提供する。このため、異なるプラットフォーム間の相互運用性が確保され、互いのデジタル通貨の交換が可能となれば、取引相手の拡大や、それに伴う取引機会の拡大・多様化といった付加価値をユーザーにもたらし、国民の利便性向上や決済システムの効率化にもつながることとなる。

相互運用性を確保するためには、複数のデジタル通貨のプラットフォーム間をつなぐ「共通の言語体系」を構築すること、すなわち、決済情報を伝送するメッセージフォーマットやデータ項目に関する標準化を進めていくことが効果的である。

例えば、クロスボーダーの資金決済については、銀行等によるクロスボーダー送金の改善が、金融安定理事会（FSB : Financial Stability Board）や、国際決済銀行（BIS : Bank for International Settlement）の決済・市場インフラ委員会（CPMI : Committee on Payment and Market Infrastructures）においても課題とされている。そのうえで、課題を解決する有力な手段のひとつとして、メッセージフォーマットの国際標準を活用したシステム間の国際的な調和が提案されている⁵。

国内の資金決済においても、今後、民間主体が新たなデジタル通貨の発行を検討する場合に、他の決済プラットフォームとの相互運用性の確保に取り組んでいくことは国民の利便性向上や決済システムの効率化に資する。とりわけ現金需要の強いわが国において、現金に近いネットワーク効果を発揮し、民間デジタル通貨の普及を図るうえでは、標準化を通じた相互運用性の確保が重要と考えられる。

（信頼性の確保）

デジタル通貨にとって信頼性の確保は最も重要な要素のひとつである。デジタル通貨を保有し、利用する際、情報が第三者に盗まれたり書き換えられたりすれば、ユーザーは安

⁵ FSB, “Enhancing Cross-border Payments: Stage 3 roadmap,” October 2020

CPMI, “Enhancing cross-border payments: building blocks of a global roadmap Stage 2 report to the G20,” July 2020.

心して日常生活にデジタル通貨を利用できなくなる。デジタル通貨が個人や企業など幅広いユーザーの利用を想定していることを踏まえると、信頼性が損なわれることによる社会的影響は非常に大きい。

デジタル通貨を扱うプラットフォームは、多数の要素技術に支えられたシステムを組み合わせる形で構築される、いわば「要素技術の束」とも言える。それゆえ、デジタル通貨の信頼性を確保するうえでは、各々の要素技術に適合した情報セキュリティ技術の採用とともに、それらの情報セキュリティ技術の統合的な運用のため、安全性の担保策を実体面と手続面の両面で万全に講じていく必要がある。

安全性を実体面から担保するためには、強固な情報セキュリティ技術（暗号化方式、デジタル署名方式等）を採用することが不可欠である。そのための有効な方策の一例として、暗号技術の安全性評価において国際的な信認を得ている機関が定めたセキュリティ基準を用いることが考えられる。特に近年は、量子コンピュータの研究開発が活発化する中、耐量子計算機暗号に関する標準化の取り組みも海外で始まっている。例えば、米国の国立標準技術研究所（NIST : National Institute of Standards and Technology）は、2020年7月に15種類の暗号化方式を耐量子計算機暗号の標準化候補として技術検証を進めており、2022年には、さらに候補を絞り込んだうえで標準案を公表する方針を表明している⁶。デジタル通貨のシステム設計に当たっては、こうした標準の活用とともに、将来的な暗号技術の進展に合わせて暗号化方式をアップデートできる拡張性を持つことが、デジタル通貨への信頼性を継続的に確保することにつながると考えられる。

他方、デジタル通貨の安全性を手続面から担保する方策としては、情報セキュリティの管理手続や関連機器の調達、プライバシー保護に関する体制整備等について、第三者機関による客観的な評価・認証の枠組みを採用することが考えられる。こうした枠組みには、後述するとおり、既に定着しているISO/IEC 27000シリーズ（情報セキュリティ・マネジメント・システム）、ISO/IEC 15408（ITセキュリティの評価基準）のほか、ISO/IEC 27701（プライバシー情報・マネジメント・システム）など様々な国際標準がある。デジタル通貨のシステム設計に当たっては、これらの国際標準に準拠した体制整備手法も参考にしながら検討していくことが重要と考えられる。

⁶ NIST, “Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process,” July 2020

(専門的知見の集約・活用手段)

デジタル通貨は、情報セキュリティやプライバシー、マネー・ローンダリングおよびテロ資金供与対策(AML/CFT)など、安全性やコンプライアンス面の様々な要請に応えつつ、近年の先進的な技術を取り入れた高度な機能性・利便性を備えることが求められるものであるだけに、その開発・提供に当たっては、各方面の専門的な知見を結集する必要がある。

こうした中、国際標準化の意義として、国内外の様々な関係者との議論を深め、幅広い知見を取り入れる手段として活用していくことの重要性が、近年、一層増してきている。特に、ISO/TC 68のほか、ブロックチェーンや分散型台帳技術を扱う ISO/TC 307、情報技術を扱う ISO/IEC JTC 1⁷等において策定された国際標準や標準化活動の動向について関係者と意見交換をすることは、デジタル通貨に今後応用しうる先端的な知見を効率的に収集していく手段として有用と考えられる。

また、国内で研究・開発された優れた情報技術が、デジタル通貨を含めた金融サービス分野に幅広く応用されるよう、ISO/TC 68等の場で、これらの技術を用いた国際標準化を推進していくことも重要である。このことは、国内の専門的知見を集約して新たな技術を生み出すことにつながるとともに、こうした技術を研究・開発した民間事業者が、海外において、金融サービス分野における新たな市場を開拓する契機ともなりうる。

わが国には、デジタル通貨にも適用可能な国際的に有望な技術があるにもかかわらず、こうした技術を持つ事業者が必ずしも国際的に存在感が高いと言えない面があるのも事実である。こうした状況を打開すべく、優れた技術を持つわが国の事業者が ISO 等の国際標準化活動に積極的に参加していけば、先端的な技術動向を触れながら、国際的な議論において主導権を獲得し、自らの収益機会を拓ける手段になると考えられる。

3. デジタル通貨における標準化領域

前節では、デジタル通貨における標準化の意義を 3 つの観点からみてきた。本節では、このうち、主として相互運用性の確保と信頼性の確保という 2 つの意義に照らし、デジタル通貨において具体的にどのような領域が標準化の対象となりうるのかを既存の金融サービス分野の国際標準を参考にみていく。

⁷ 情報技術革新の進展に伴い、コンピュータ技術とネットワーク技術の双方に跨る「情報技術分野」の標準化推進ニーズが増大したことを受けて、1987年に ISO と IEC が合同で設立した技術委員会 (Joint Technical Committee)。傘下には、カードや個人認証に関する標準化を担当する SC17、汎業界的なセキュリティ技術に関する標準化を担当する SC27、生体認証技術に関する標準化を担当する SC37 等がある。

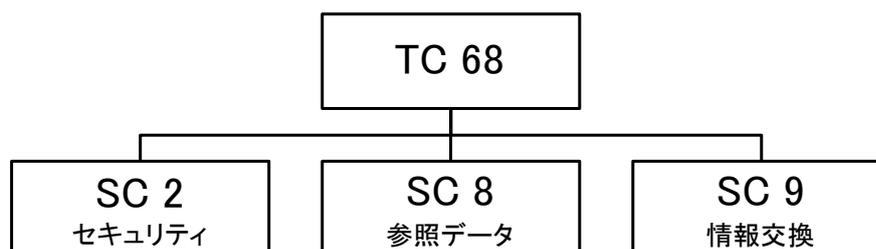
(1) 金融サービス分野における国際標準化活動

金融サービス分野の国際標準を具体的に説明する前に、国際標準の作成主体や作成作業について簡単に紹介したい。

国際的な標準は様々な組織や団体で作られているが、その代表例である国際標準化機関には、初めに触れた ISO のほか、国際電気標準会議 (IEC : International Electrotechnical Commission)、国際電気通信連合 (ITU : International Telecommunication Union) 等がある (末尾 BOX 参照)⁸。このうち、金融サービス分野の国際標準は、主として ISO/TC 68 において作られている。

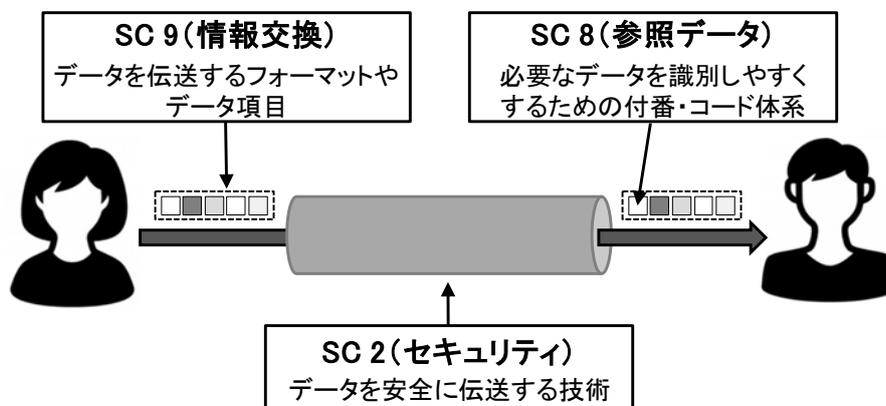
日本銀行決済機構局が国内委員会事務局を務める ISO/TC 68 について具体的にみると、現在、TC 68 傘下には 3 つの分科委員会 (SC : Sub-Committee) が設置され、それぞれの分野ごとに国際標準を検討・作成する作業が行われている (図 1)。

図 1 : ISO/TC 68 の組織構成



これら SC の担当分野は、金融サービスに関するデータ交換を安全・確実に行うための基本要素別に分かれている (図 2)。

図 2 : 金融サービスに関するデータ交換の基本要素



⁸ このような公的な国際標準化機関があらかじめ定められた手続に基づいて制定する標準は「デジュール標準」と呼ばれる。このほかにも、企業間の市場競争で事実上の標準となるような「デファクト標準」や、業界内の複数の企業が集まり、合意形成によって作られる「フォーラム標準」等がある。

すなわち、「SC2（セキュリティ：security）」は、暗証番号の管理、生体認証、暗号化方式など、データを安全に伝送する技術を扱っている。また、「SC 8（参照データ：reference data）」は、必要なデータを識別しやすくするための付番・コード体系を扱い、「SC 9（情報交換：information exchange）」は、データを伝送するフォーマットやデータ項目を扱っている。

（2）デジタル通貨の標準化領域

以下では、この ISO/TC 68 の SC の類型に沿って、①データを伝送するフォーマットやデータ項目、②必要なデータを識別しやすくするための付番・コード体系、③データを安全に伝送する技術の順に、相互運用性の確保と信頼性の確保に資する標準化領域を既存の国際標準を紹介しながらみていく。

（データを伝送するフォーマットやデータ項目）

現代の金融取引は取引者間でデータを交換することによって成り立つ。デジタル通貨に限らず金融取引では、「誰から誰に」、「いつ」、「何を」、「いくら」といった様々なデータを取引者間で交換する必要がある。こうしたデータを円滑に伝送するため、データ項目の種類や条件を含め、それらデータを伝送するための電文様式（メッセージフォーマット）を定めておく必要がある。そのため、金融サービスのオンライン処理化の進展とともに、メッセージフォーマットの標準化が様々な分野で進められてきた。

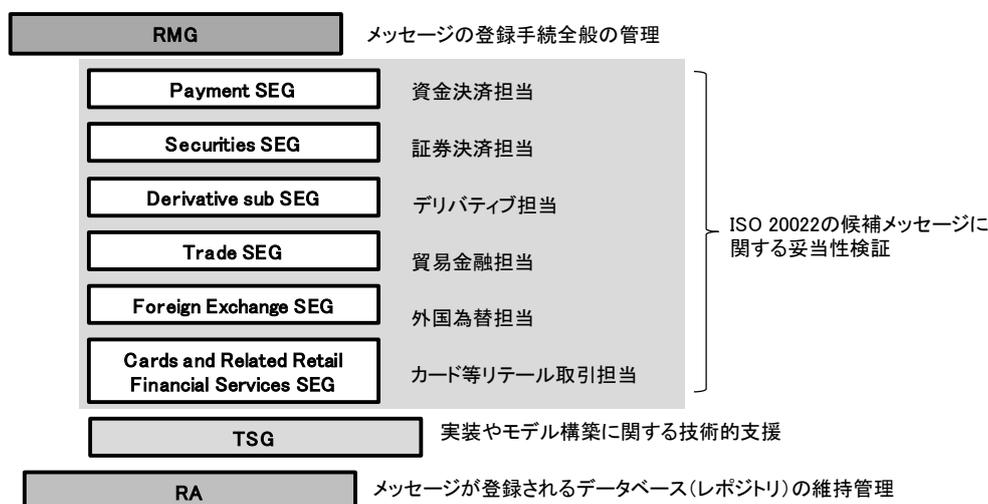
従来、こうしたメッセージフォーマットの国際標準は、例えば、クレジットカード取引等では ISO 8583、証券受渡しでは ISO 15022 など、金融サービスの分野別に存在していた。しかし、2004年に金融サービス分野全般を対象とする統合的な国際標準 ISO 20022 が作られたことにより、金融サービス分野におけるメッセージフォーマットの国際標準は、この ISO 20022 の枠組みのもとで検討・開発されることが一般的となっている。

ISO 20022 では、様々な金融サービス分野の特性に応じたメッセージフォーマットの標準を作成できるよう、金融関係者から提案がなされたメッセージフォーマットの標準案の妥当性を検証し、標準に仕上げていく標準評価グループ（SEG：Standards Evaluation Group）が 6 つの分野別に設置されている⁹。こうした検証を経て完成したメッセージフォーマットは、登録機関（RA：Registration Authority）が維持管理するデータベース（「レポジトリ」と呼称）に登録されることで標準となる。これら一連の手続全体は、登録

⁹ メッセージフォーマットの実装や、ビジネスモデルやメッセージモデルの構築に関する技術面のサポートを行う技術支援グループ（TSG：Technical Support Group）もある。

管理グループ (RMG : Registration Management Group) により管理されている (図 3)。

図 3 : ISO 20022 の標準化に関わる主な組織



ISO 20022 の最大の特徴は、具体的なメッセージフォーマットだけでなく、その前提となるデータ項目の種類、条件等を定義したメッセージモデル、さらに業務フローを表したビジネスモデルも、標準としてあわせて登録されていることにある (図 4)。

図 4 : 標準としての登録対象

登録対象	主な内容	記述言語
フォーマット	メッセージフォーマット	XML schema ¹⁰ ASN.1 ¹¹
メッセージモデル	メッセージの種類、条件等	UML ¹²
ビジネスモデル	業務フロー	UML

このようにフォーマット、メッセージモデル、ビジネスモデルと 3 階層に分けて標準化することは、様々なレベルの相互運用性の向上に対応できる利点がある。すなわち、相互運用性の達成レベルには、①システム間で電文の授受が直接できるよう、フォーマットを揃えるレベル、②フォーマットは異なるが、フォーマットの変換を通じてシステム間でデータの授受が過不足なく行えるよう、データ項目の種類や条件を揃えるレベル、③シス

¹⁰ XML schema : XML フォーマットを定義するための記述言語。XML (Extensible Markup Language <拡張可能なマークアップ言語>) とは、1998 年に World Wide Web の標準化団体である W3C が公開したデータ記述用言語。柔軟性や拡張性が高く、プラットフォームへの依存度が低いなどの利点がある。

¹¹ ASN.1 (Abstract Syntax Notation One) : ISO と IEC の合同技術委員会 (ISO/IEC JTC 1) と国際電気通信連合の一部である国際通信標準化部門 (ITU-T) が共同で開発したデータ記述のための国際規格。ASN.1 では、名前と型によって定義されるオブジェクトを列挙してデータ構造を定義することが特徴のひとつである。

¹² UML (Unified Modeling Language <統合モデリング言語>) : 主としてオブジェクト指向の分析・設計においてシステムの振る舞いをモデル化する際の表記法を規定した言語。

テム間での連携を高めるよう、業務フローを揃えるレベルなど、様々な達成レベルが考えられる。ISO 20022 は、こうした様々な相互運用性の達成レベルに合わせて、柔軟に活用できる利点を持っている。

以上のとおり、ISO 20022 は、資金決済を含めた幅広い金融取引に適用することが可能なメッセージフォーマットの国際標準である。既に資金決済の分野では、顧客送金用決済指図 (pacs.008¹³) や金融機関間送金用決済指図 (pacs.009) といったメッセージフォーマットが標準として登録されており、これに準拠したメッセージフォーマットの国際的な利用も進んでいる。

前節では、複数のデジタル通貨のプラットフォーム間をつなぐ「共通の言語体系」を構築すること、すなわち、決済情報を伝送するメッセージフォーマットやデータ項目に関する標準化を進めることが、デジタル通貨の相互運用性を確保するうえで効果的と述べた。そのメッセージフォーマットの国際標準として ISO 20022 を活用していくことはひとつの選択肢である。銀行等によるクロスボーダー送金の改善を課題に掲げる前述の FSB や BIS/CPMI の報告書でも、その課題を解決する有力な手段のひとつとして、ISO 20022 メッセージを活用したシステム間の国際的な調和を求めている。

(必要なデータを識別しやすくするための付番・コード体系)

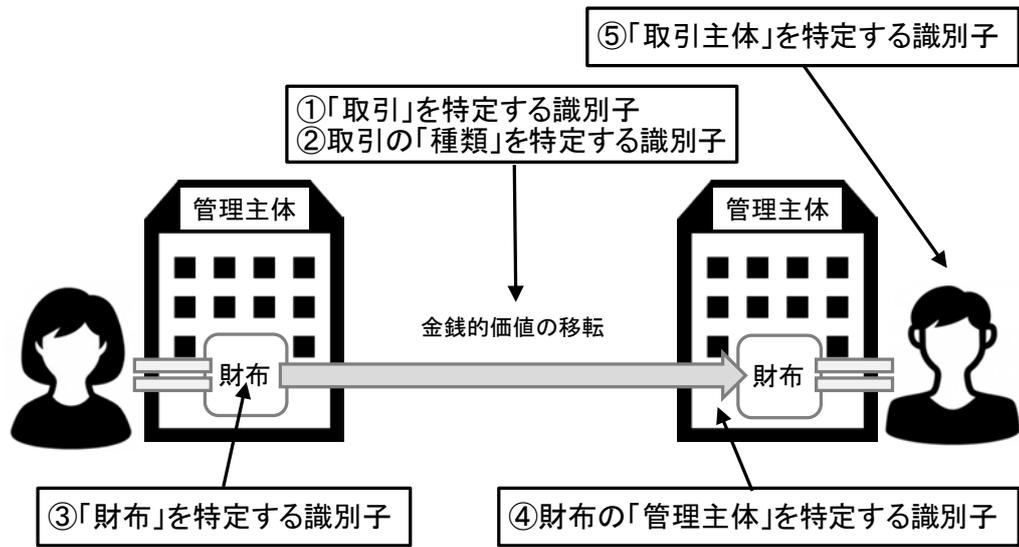
金融取引のデータを伝送する際、多くのデータの中から必要な情報を確実に識別できるようにすることも、相互運用性を確保するうえで重要である。このため、あらかじめ決められたルールに基づいて、取引や関与する主体等に数～数十桁の番号やコードを割り振る場合が多い。こうした付番・コード体系は「識別子 (identifier)」と呼ばれ、国際的な金融取引の場面では、古くから様々な付番・コード体系に関する国際標準が定められてきた。

デジタル通貨において参考とすべき識別子は、金銭的価値の移転や格納の場面に着目すると、以下の5つが考えられる (図5)。

- ①金銭的価値の移転に関する「取引」を特定する識別子
- ②金銭的価値の移転に関する取引の「種類」を特定する識別子
- ③金銭的価値を格納する「財布」を特定する識別子
- ④金銭的価値を格納する財布の「管理主体」を特定する識別子
- ⑤金銭的価値の移転の「取引主体」を特定する識別子

¹³ この例のように顧客送金用決済指図、金融機関間送金用決済指図など、特定の用途のために標準化されたメッセージフォーマットのセットごとに記番号が付されている。

図 5：金銭的価値の移転・格納の場面で活用される識別子

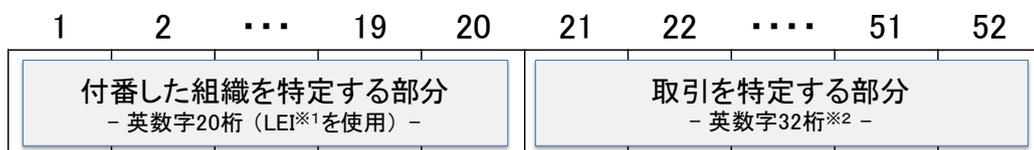


①金銭的価値の移転に関する「取引」を特定する識別子

金融取引では、多くのメッセージの中から個々の取引を特定するために、取引ごとに付番する実務が行われている。資金決済でも、例えば、銀行等によるクロスボーダー送金では SWIFT gpi (global payments innovations) において UETR (Unique End-to-end Transaction Reference) という固有番号を取引ごとに付す扱いとなっている。

もっとも、この UETR を含め、資金決済における個々の取引を特定する識別子は ISO の国際標準となっていない。その他の分野では、現在のところ、店頭デリバティブ取引において、UTI (Unique Transaction Identifier) と呼ばれる個々の取引を特定する識別子の国際標準 ISO 23897 がある (図 6)。

図 6：ISO 23897 (UTI) の付番体系



※1 LEIについては図11を参照。

※2 英字は大文字のみ使用可。

今後、デジタル通貨における金銭的価値の移転において、個々の取引の識別子を検討する場合には、こうした既存の国際標準や資金決済分野における議論の展開を参考にしていくことが考えられる。

②金銭的価値の移転に関する取引の「種類」を特定する識別子

金融取引では、通貨の種類（幣種）や取引が行われる取引所など、取引の種類を識別して特定するための国際標準が作られている。例えば、金融取引に用いる幣種に関しては、日本円を JPY または 392、米国ドルを USD または 840 といった形で、3桁の英字または数字のコードで表す付番体系の国際標準 ISO 4217¹⁴がある（図7）。デジタル通貨の幣種を特定する場合にも、この国際標準は参考になる。

図7：ISO 4217 の付番例

通貨	英字	数字	通貨	英字	数字
ユーロ	EUR	978	日本円	JPY	392
スイスフラン	CHF	756	米ドル	USD	840
英ポンド	GBP	826	豪ドル	AUD	036

このほか、例えば、複数の民間主体が同一の通貨建てのデジタル通貨を発行するような場合には、複数種類のデジタル通貨（例：デジタル通貨A、デジタル通貨B）を識別する必要性も考えられる。少なくともそれらデジタル通貨間の交換を行う場面では必須である。この点、現時点では、銀行等による送金に関連して、こうした識別を目的とした国際標準は存在しないが、暗号資産やセキュリティトークンなど、分散型台帳技術を活用したデジタルトークン¹⁵では、複数種類のデジタルトークンを識別することを目的とした識別子（DTI：Digital Token Identifier）の国際標準案（ISO/DIS 24165）が検討されている（図8）。デジタル通貨でも、このような識別子を参考にしていく余地がある。

図8：ISO/DIS 24165（DTI）の付番体系

1	2	3	4	5	6	7	8	9
デジタルトークンの種類を特定する部分 - 英数字8桁 ^{※1} -								C/D ^{※2} - 英数字 1桁 -

※1 英字はA,E,O,I,U,Y以外の大文字のみ使用可。1桁目は0を使用不可。

※2 C/D(check digit、チェックディジット)は、記番号の入力ミス等を避けるための検査符号。

¹⁴ ISO 4217 では、「価値の交換媒体であり、地理的な位置を基として通貨当局が責任をもって発行するもの」を「通貨（currency）」と定義し、それに対して具体的な英字と数字のコードを付している。

¹⁵ ISO/DIS 24165 では、デジタルトークンを、「発行、保存、交換、所有権の記録、または取引の検証に分散型台帳技術を使用した、代替可能性（fungible:デジタル資産の個々の単位間で相互に代替可能であること）のあるデジタル資産であり、通貨（currency）ではないもの。」と定義している。

③金銭的価値を格納する「財布」を特定する識別子

デジタル通貨では、金銭的価値に関する情報は、ユーザー間で伝送するためだけでなく、それをユーザーに帰属する「財布」に格納するためにも用いられる。このため、「財布」を特定する識別子も必要となる場面が考えられる。

銀行等による送金では、預金口座が金銭的価値を格納するいわば「財布」であり、口座番号が「財布」を特定する識別子である。銀行の口座番号に関する国際標準には、既に ISO 13616 (IBAN : International Bank Account Number) があり、海外の銀行では広く用いられている¹⁶ (図9)。

図9 : ISO 13616 (IBAN) の付番体系

1	2	3	4	5	6	7	33	34
国名コード※1 - 英大文字2桁 -		C/D※2 - 英数字2桁 -		金融機関と口座番号を特定する部分※3 - 英数字 最大30桁 -					

※1 ISO 3166-1で標準化された国名を特定するためのコード。

※2 C/D (check digit, チェックディジット) は、記番号の入力ミス等を避けるための検査符号。

※3 金融機関コードと口座番号を組み合わせると国ごとに付番される。

民間主体が発行する新たなデジタル通貨を巡る構想では、金銭的価値に関する情報をユーザーに紐付ける方法として、「口座型」と「トークン型」に分類する場合がある。両者の定義は様々であるが、ユーザーごとに金銭的価値の総額(残高)を紐付けるタイプを「口座型」、金銭的価値の塊(トークン)ごとにユーザーを紐付けるタイプを「トークン型」と定義するのはその一例である¹⁷。いずれにおいても、ユーザーに帰属する「財布」を特定する識別子の付番体系の標準化を考えるうえでは、既存の口座番号に関する国際標準は参考となりうる。

④金銭的価値を格納する財布の「管理主体」を特定する識別子

デジタル通貨では、金銭的価値を格納する「財布」の特定とあわせて、その財布の「管理主体」である銀行や決済事業者等を特定することも必要となる。そのために活用しうる

¹⁶ わが国の銀行等では、3桁の店番号と7桁の口座番号なら成る日本独自の付番体系が預金口座に用いられている。

¹⁷ 日本銀行決済機構局、「中銀デジタル通貨が現金同等の機能を持つための技術的課題」、2020年7月の定義に沿った分類。「口座型」と「トークン型」の分類については、例えば、Alexander Lee, Brendan Malone, and Paul Wong, "Tokens and accounts in the context of digital currencies", FEDS Notes, Board of Governors of the Federal Reserve System, December 2020での考察もある。

既存の識別子として、ISO には法人を特定するための識別コードに関する国際標準がある。

例えば、クロスボーダー送金において金融機関を特定するための識別子として国際標準 ISO 9362 (BIC : Business Identifier Code) がある (図 10)。このほか、主に店頭デリバティブの取引報告に用いる目的で、金融取引に参加する取引主体 (法人・ファンド) を特定する識別子として国際規格 ISO 17442 (LEI : Legal Entity Identifier) がある¹⁸ (図 11)。

デジタル通貨を格納する財布の「管理主体」を特定するうえでも、こうした既存の国際標準を活用していく余地がある。

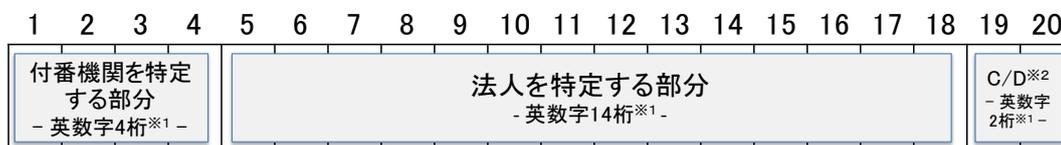
図 10 : ISO 9362 (BIC) の付番体系



※1 ISO 3166-1で標準化された国名を特定するためのコード。

※2 英字は大文字のみ使用可。

図 11 : ISO 17442 (LEI) の付番体系



※1 英字は大文字のみ使用可。

※2 C/D (check digit、チェックディジット) は、記番号の入力ミス等を避けるための検査符号。

⑤金銭的価値の移転の「取引主体」を特定する識別子

デジタル通貨においても、資金決済における一連の情報の流れは、個別の取引とこれにユーザーとして関わった「取引主体」を紐付けることによって完結する。

ISO の国際標準では、こうした「取引主体」を特定する識別子として、前述のとおり、法人の場合には ISO 17442 (LEI) や ISO 9362 (BIC) がある。他方、自然人の「取引主体」を特定する識別子に関し、ISO の既存の国際標準はないが、現在 TC 68 のもとで、自然人を対象としたコード体系に関する国際標準の検討が進められているところである (ISO/DIS 24366 <NPI : Natural Person Identifier>)。

¹⁸ 最近では、店頭デリバティブの取引報告以外にも LEI の活用事例は増えている。例えば、「金融サービスで用いる法人の ID ナンバーにかかる国際的議論の現状」(日銀レビュー 2019-J-7、2019年7月)を参照。

デジタル通貨に関する「取引主体」を特定する方法として、付番体系を考える場合には、こうした国際標準を参考にしていく余地がある。

(データを安全に伝送する技術)

金融取引において、金銭的価値に関するデータを安全に伝送するためには、情報技術の進展に応じた適切な情報セキュリティを確保する必要がある。金融サービス分野では、信頼性確保の観点から、従来より、情報セキュリティの技術・手法・手続等に関する多面的な国際標準化が行われてきた。

例えば ISO/TC 68 では、暗証番号の管理、生体認証、暗号化方式等の様々な国際標準が策定されてきた(図 12)。銀行等の ATM で使われる暗証番号 (PIN) はその一例である。また、最近では、要素技術の発展や各種デバイスの普及に対応して、スマートフォンを用いたオンラインでの本人確認 (ISO/WD 5158、いわゆる e-KYC)、QR コード決済のセキュリティ技術 (ISO/WD 5201)、ブロックチェーン・分散型台帳技術のセキュリティ技術 (ISO/WD 24374) に関する国際標準も検討されている。

図 12 : ISO/TC 68 が策定した情報セキュリティ関連の国際標準

国際規格の名称	規格の概要
ISO 9564 暗証番号 (PIN) のマネジメントとセキュリティ	金融機関の取引カード等とともに利用される暗証番号 (個人識別番号 <PIN : Personal Identification Number>) の設定、保管、入力、送信等に関する一般的な規則を定めた規格。
ISO 11568 金融のリテール向けサービスの鍵管理	リテール金融分野、特に CD/ATM や POS システムで PIN を暗号化する際、CD/ATM とセンターが暗号鍵を安全に共有するための鍵管理方式を定めた規格。
ISO 13491 リテール金融で用いるセキュアな暗号装置	リテール金融取引において利用される物理的かつ機能的にセキュアな暗号装置 (SCD : Secure Cryptographic Devices) に要求される機能に関する規格。
ISO 13492 ISO 8583-1 のデータ要素を暗号化する際の鍵管理	ISO 8583 (金融取引カード用の通信メッセージ) のデータ項目の鍵管理情報等に、共通鍵暗号アルゴリズム、DEA (Data Encryption Algorithm)、TDEA (Triple Data Encryption Algorithm) を適用する際の要件を定めた規格。

ISO 16609 共通鍵暗号を利用したメッセージ認証の 要求事項	共通鍵暗号を用いてメッセージの完全性を保ち、メッセージが許可されたソースから発信されたことを確認するための、送信プロセスと独立した手順を定めた規格。
ISO 19092 生体認証におけるセキュリティの枠組み	金融業務において生体認証を利用する際のセキュリティ確保のための枠組みを定めた規格。
ISO 20038 AES を用いた鍵ラップ	AES (Advanced Encryption Standard) 暗号鍵を伝送する際のパッケージ化する方法を定めた規格。
ISO 21188 金融機関のための公開鍵基盤にかかる運用および方針の枠組み	金融業務で公開鍵基盤（PKI：Public Key Infrastructure）を利用する際に必要となる証明書ポリシーや認証局運用規程等の作成方法を定めた規格。
ISO 22307 プライバシー影響評価（PIA：Privacy Impact Assessment）	個人情報の収集を伴うシステムの導入・改修時のプライバシー問題の回避・低減を目的として事前にリスク評価する手法等を定めた規格。

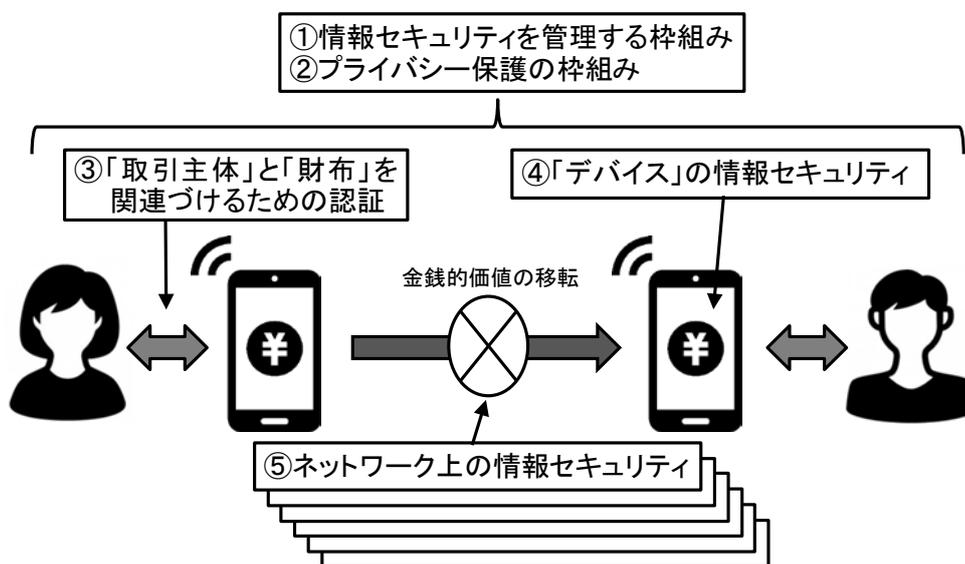
TC 68 以外でも、ISO 関係では、金融サービス分野の情報セキュリティに関連する国際標準として、ISO/IEC 27000 シリーズ（情報セキュリティ・マネジメント・システム）、ISO/IEC 15408（IT セキュリティの評価基準）、ISO/IEC 27701（プライバシー情報・マネジメント・システム）、ISO/IEC 29100（プライバシー・フレームワーク）、ISO/IEC 29134（プライバシー影響評価のガイドライン）など、幅広く策定している。

これらの国際標準をもとに、デジタル通貨の情報セキュリティに関連する標準化領域を考えると、大きく以下の5つに分けることができる（図 13）。

- ①情報セキュリティを管理する枠組み
 - ②プライバシー保護の枠組み
 - ③「取引主体」と「財布」を関連づけるための認証
 - ④「デバイス」の情報セキュリティ
 - ⑤ネットワーク上の情報セキュリティ

上述のとおり、デジタル通貨を扱うプラットフォームは「要素技術の束」であり、関連する情報セキュリティ分野も様々な領域から成り立っている。それらの要素技術には実績のある汎用技術も少なくない。こうした中、プラットフォーム全体について適切なセキュリティ水準を確保するためには、単独の国際標準でカバーするのではなく、デジタル通貨のシステムの仕様に応じて、採用する要素技術に適合した国際標準を選択し、柔軟に組み合わせながら適用していくことが考えられる。

図 13：デジタル技術を用いた資金決済における情報セキュリティ関連の標準化領域



4. おわりに — CBDC に関する標準化のあり方 —

本稿では、金融サービス分野における国際標準を参考にしながら、デジタル通貨における標準化の意義と対象となりうる領域について考察してきた。最後に、中央銀行が発行するデジタル通貨である CBDC に関する標準化のあり方に触れながら、本稿を締め括る。

デジタル通貨における標準化の意義を改めて整理すると、第 1 に、伝送するメッセージフォーマットやデータ項目、付番・コード体系に関する標準化を進めることにより、デジタル通貨間の相互運用性を確保すること、第 2 に、データを安全に伝送するための情報セキュリティに関する適切な国際標準に準拠することにより、デジタル通貨の信頼性を確保することである。これらの点は、CBDC についても当然に当てはまる。

特に CBDC をクロスボーダー決済にも用いることを想定した場合、相互運用性や信頼性の確保は極めて重要である。近年、この分野では、グローバル化の進展や世界規模のステーブルコイン構想の影響もあって、より便利で安価な決済を望む声が強まっており、FSB、CPMI や G20 等では、海外送金の仕組みを改善するための議論が進められている。そこでは、例えば、複数の国の CBDC を相互に交換できるようにするなど、CBDC の枠組みをクロスボーダー決済の改善に活用する案も検討されている。

CBDC の検討を進めるに当たり、中央銀行にとって重要なことは、自国の決済システムの安定性や効率性を確保・改善していくことである。そうした観点から、現行のクロスボーダー決済が抱える課題は、まずは既存の決済システムの改善等によって解決していくこと

が望ましい。もっとも、既存システムの大幅な見直しは容易ではなく、今後の状況次第では CBDC を活用した枠組みが選択肢として浮上する可能性も考えられないではない。そうした状況に備え、異なる CBDC 同士が円滑かつ安全に交換できるよう、標準化を通じた相互運用性や信頼性の確保について検討を進めておくことは有用である。

標準化を進めるに当たり、本来競合関係にある民間事業者間における協調は、得てして難航しがちである。しかし、中央銀行の場合にはそうした問題は少ない。この点、日本銀行を含む 7 つの主要中央銀行と BIS は、2020 年 10 月に「中央銀行デジタル通貨：基本的な原則と特性」と題する共同報告書（以下、「共同報告書」）を公表し、CBDC の検討を進める際の「基本原則」や CBDC が具備すべき「基本的特性」をまとめるなど、緊密な協調関係を構築している¹⁹。「共同報告書」では、各中央銀行は、CBDC の研究当初からクロスボーダーでの相互運用性の可能性を考慮すべきとされており、日本銀行も、こうした考え方にに基づき、他の中央銀行と連携しつつ、実務的な論点や課題に関する検討作業を精力的に進めている。

CBDC の検討に取り組む国が増えてくる中であって、このように、CBDC のあるべき姿や標準化について積極的に情報発信していくことは、今後、7 つの中央銀行が、技術と理論の両面において、CBDC を巡る世界の動きを主導していく足掛かりになると考えられる。また、こうした中央銀行間の信頼関係をベースに、それぞれが相互運用性の確保に向けた取り組みを進めておけば、仮に将来、日本銀行が CBDC を発行することとなった場合、単独の CBDC では得られない、ネットワーク効果を通じた付加価値を新たに得ることができると考えられる。

将来的には、相互運用性の確保に向けた中央銀行による検討の成果を、ISO 等の国際標準として具体化していく場面もありうる。ISO/TC 68 では、最近、CBDC を含むデジタル通貨に関する調査を行うためのグループ（ISO/TC 68/AG 5）を新たに組成した。日本銀行としては、CBDC の国際標準に関する取り組みがわが国にとって適切な形で進むよう、本グループへの参画を含め、引き続き、ISO/TC 68 の活動に積極的に取り組んでいく考えである。また、今後とも、国際標準を巡る他の中央銀行の動向を感度高く注視していきたい。

上述のとおり、CBDC に関する検討を進めるに当たっては、国内の他の決済システムとの相互運用性を確保していくことも重要である。CBDC という決済手段を土台に民間の事

¹⁹ 主要中央銀行による中央銀行デジタル通貨（CBDC）の活用可能性を評価するためのグループ（カナダ銀行、イングランド銀行、日本銀行、欧州中央銀行、スウェーデン・リクスバンク、スイス国民銀行、米国連邦準備制度、国際決済銀行）、「中央銀行デジタル通貨：基本的な原則と特性」、2020 年 10 月。

業者が様々な決済サービスを国民に提供できるようになれば、CBDCは、現金や中央銀行預け金と異なる、デジタル社会ならではの決済プラットフォームとして機能する。その際、国内からクロスボーダー送金に至るシームレスな資金移動を実現しようとするれば、国内においても、国際基準を念頭に置きながら、システム間の接続を検討していく必要がある。日本銀行としては、わが国のCBDCシステムが「ガラパゴス化」することがないよう、国内における相互運用性の議論についても、国際的な調和を意識して進めていくことが重要と考えている。

2節では、デジタル通貨の分野で標準化を進める意義の一つとして、内外の専門的な知見を集約することや、国内の優れた情報技術を幅広く活用していくことの重要性を述べた。要素技術の選択やシステム設計に資する知見を効率的に収集する観点から、既存の国際標準や最新の標準化の動向を把握することは有用である。また、国内の優れた情報技術が国内外のデジタル通貨に幅広く応用されるよう、技術の研究・開発に関わる関係者には、国際標準化の議論に積極的に参画していくことが望まれる。

この点は、CBDCについても同様である。日本銀行では、2020年7月にISO/TC 68 国内委員会の事務局機能を金融研究所から決済機構局に移管した。これは、国際標準に関する調査・分析機能と、決済システムの企画立案機能のシナジーを発揮させることを通じて、CBDCを含む、わが国決済システムのさらなる改善に取り組んでいこうとする姿勢の表れでもある。もちろん、決済システムの構築は、中央銀行だけで進められるものではなく、幅広い関係者との協力・連携も不可欠である。日本銀行としては、民間事業者や有識者が標準化活動に積極的に参加し、最先端の議論に加わるよう、ISO/TC68の活動等を通じて必要なサポートを行っていく方針である。日本銀行は、こうした取り組みが、日本の優れた技術が国際標準の重要な要素となり、海外市場で広く活用されることにつながっていくと考えている。

以 上

BOX : 主な国際標準化機関と ISO/TC 68 における国際標準化プロセス

金融サービス分野を含めた国際標準を策定する主な国際標準化機関としては、①ISO (国際標準化機構)、②IEC (国際電気標準会議)、③ITU (国際電気通信連合) がある (図 14)。これらの国際標準化機関は、リエゾン (liaison、連携役) と呼ばれるメンバーを互いの会合に派遣するなど継続的な連携関係を保つことにより、国際標準の重複回避や整合性確保を図っている。

図 14 : 主な国際標準化機関

名称	概要
国際標準化機構 (ISO : International Organization for Standardization)	機械、化学、材料、建築、サービス等の様々な分野における国際標準化を担う非営利団体。1947 年設立。スイス・ジュネーブが本拠地。
国際電気標準会議 (IEC : International Electrotechnical Commission)	電気、電子分野の国際標準化を担う非営利団体。1906 年設立。スイス・ジュネーブが本拠地。
国際電気通信連合 (ITU : International Telecommunication Union)	電気通信分野の国際標準化を担う非営利団体。標準化のほか、電気通信分野に関する制度の検討、電気通信技術の開発や通信周波数の管理等を行っている。1865 年創設の万国電信連合と 1906 年創設の国際無線電信連合が 1932 年に合体して設立された国際連合の専門機関のひとつ。スイス・ジュネーブが本拠地。

以下では、日本銀行決済機構局が国内委員会事務局を務める ISO/TC 68 に関連して、ISO における国際標準の作成プロセスを紹介する。

このプロセスは、ISO 専門業務指針 (Directives) で定められており、次の(1)から(6)までの段階を経て国際標準の確定 (国際規格の発行) に至るものである²⁰。このうち、確定前の(1)~(5)の案段階にある場合には、どのプロセスにあるかがわかるように、ISO/WD、ISO/CD 等の表記がなされている。本稿でも、確定前の案段階については、この表記を用いている。

(1) 提案段階 : 新作業項目提案 (NP : New working item Proposal)

各国加盟機関、専門委員会 (TC : Technical Committee)、分科委員会 (SC : Sub-Committee) の幹事等が新たな規格の策定や規格改定の提案を行う。

²⁰ このようなプロセスを経て確定した国際規格 (IS) のほか、ISO では、将来的に国際規格 (IS) として合意される可能性はあるものの、標準化の対象となる技術等が開発途上であるなど直ちに国際規格として発行することができないものをまとめた「技術仕様書 (technical specification : TS)」、規範性を持たない収集データを含んだ「技術報告書 (technical report : TR)」等が公表されている。

(2) 作業段階：作業原案 (WD : Working Draft) の作成

提案の承認後、TC/SCの作業グループ (WG : Working Group) において WD の策定に当たる専門家を TC/SCの幹事が P メンバー (主たる議論の参加国) と協議して任命。WG において WD を検討・作成する。

(3) 委員会段階：委員会原案 (CD : Committee Draft) の作成・投票

WD は CD 案として登録されると、TC/SC の P メンバーに意見照会のために送付される。総会でコンセンサスを得るか、P メンバーの投票にかけて 2/3 以上の賛成を得た場合に CD が成立する。

(4) 照会段階：国際規格案 (DIS : Drafted International Standard) の照会・投票

登録された DIS は TC/SC メンバーだけでなく、全メンバー国に照会とコメントを求めるために送付される。

その後、承認基準 (①投票した TC/SC の P メンバーの 2/3 以上が賛成し、かつ、②反対が投票総数の 1/4 以下の場合) を満たしている場合に、最終国際規格案 (FDIS : Final Drafted International Standard) として登録される。

ただし、反対やコメントの内容を踏まえ、委員長の判断により、FDIS 投票を省略し、国際規格の発行段階に進むことができる。実際に、TC 68 では FDIS 投票が省略されることが多い。

(5) 承認段階：最終国際規格案 (FDIS : Final Drafted International Standard) の策定・投票

ISO の中央事務局が FDIS として登録された案を全メンバー国に投票のため送付し、投票を実施。①投票した TC/SC の P メンバーの 2/3 以上が賛成であり、かつ、②反対が投票総数の 1/4 以下の場合に、承認され国際規格として成立する。

(6) 発行段階：国際規格 (IS : International Standard) の発行

FDIS の承認後、正式に国際規格として発行される。

これらのプロセスに要する期限について、ISO 専門業務指針では NP 提案の承認から 36 か月以内に国際規格を定めるとしている。もっとも実際には、NP 提案の前に、アドホックグループ (AHG : Ad Hoc Group) やスタディグループ (SG : Study Group) を設置し、年単位の時間をかけて、標準案の実質的な検討が行われることも珍しくない。

したがって、36 か月以内という期限は、こうした議論を経た後に NP 提案を行い、承認を得て WG を設置してから、実際に IS の発行までに要する期間である。特に新しい規格の場合、IS の発行までに要する期間が 36 か月を大幅に下回ることはまれである。したがって、全体で見ると、新たな IS 策定には、早いものでも数年²¹、通常は 5 年以上の期間を要するのが実務的な現状である。

²¹ ISO は、昨今のデジタル化等に伴う技術革新のスピード・アップに対応するため、18 か月間で IS 発行にまで至る迅速手続 (Fast-Track Procedure) を導入したが、各国で一定の実績のある標準に適用を限るなど、一定の条件が付されている。