

デジタル決済の匿名性とプライバシー

「匿名性」の強い現金に代わる新たなデジタル決済が普及しつつある。さらに中央銀行デジタル通貨（CBDC）の発行も多くの国で検討されている。これらの新たなデジタル決済手段で「匿名性」のデメリットを解消すると同時に、決済の「プライバシー」を保護するための制度設計が求められる。

デジタル決済の匿名性の所在

デジタル決済は、現金決済のような完全匿名性を持ってはいない。急速に拡大するデジタル決済の世界、とりわけ検討が進んでいる中央銀行デジタル通貨（CBDC）において匿名性をどのように確保すべきだろうか。

Bitcoinに代表される暗号資産も現金に似た一定の匿名性を持つ。Bitcoinでは、「いつ、あるアカウント（ID）から、どのアカウントに、いくら移動したか」というトランザクションはブロックチェーン上に完全に記録されるが、そのアカウントを持っている「誰か」を特定するための情報が乏しいため、結果的に匿名性が高い決済を実現している¹⁾。

逆に最も「実名」に近い取引は銀行口座を介する取引だろう。厳格な本人確認（KYC）が行われた銀行口座間での振替に匿名性はほぼないと言える。また、電子マネーやクレジットカードでは、アカウントを開設する際にその決済事業者による本人確認が行われているため、決済事業者はトランザクションの中身を相当程度把握できており、これらの決済の匿名性も低い。さらに、電子マネーやクレジットカード決済は、最終的には銀行口座からの引き落としや振替に紐づくことが多いため匿名性はさらに抑制される。

匿名性がプライバシーか

こうしてみると、デジタル決済の匿名性は「銀行口座」「アカウント」「トランザクション」の3つの視点から、それぞれ匿名性の有無・強弱を分

解して整理すると分かりやすくなる（図表参照²⁾。

一般に、デジタル決済手段は、支払側と受取側のアカウント情報（ID）と、取引額、取引日時などのトランザクションが完全に捕捉可能である。そのため、デジタル決済において「匿名性」を確保することは原理的に難しい³⁾。

一般の市民にとって個々の取引内容はプライバシーに属するものであり、デジタル決済によってすべての取引情報が記録・監視の対象となる事態は好ましいものではない。特に現在日本を含めた多くの国で導入が検討されているCBDCでは、政府や政府に準ずる機関が個人個人の決済を記録・監視できるようになることへの警戒感が高い。しかし一方で、デジタル決済の普及によってマネーロンダリングや脱税などの脱法行為を抑制する効果はおおいに期待できることも事実である。

その意味で、デジタル決済においては「匿名性」に代わる「プライバシー」に配慮した制度設計が求められることになる。

プライバシーを確保できるCBDCのあり方

CBDC発行の議論の主要論点の一つである「匿名性」

図表 デジタル決済の匿名性の強弱

匿名性	銀行口座	アカウント	トランザクション
強	(該当なし)	ランダム文字列 Eme3kIImaMLt4	暗号化
↑↓	口座番号	ID/クレジットカード番号 R-kashiwagi 1234-5678-9012-3456	トークン化
	弱	口座所有者情報	実名/銀行口座紐づけ

(出所) 野村総合研究所

NOTE

- 1) ただし、暗号資産を法定通貨に現金化する際は、取引所を通じて何らかの銀行口座を介する必要があるため、現金化に際しての匿名性は大幅に低下する。
- 2) 決済に関する匿名性のフレームワークは、デイヴィッド・パーチ（著）、松本裕（訳）『ビットコインはチグリス川を漂う マネーテクノロジーの未来史』みすず書房（2018年）pp.156-159を参照した。
- 3) ただ、デジタル決済でも匿名性を高める手段はないわけではない。個々の取引を強度に暗号化することで取引の真正性を確保すると同時に、取引内容の秘匿化は可能である。ただしそれでもトランザクションは完全に補
- 4) 足される。
- 4) 例えば中国のデジタル人民元でもある程度の匿名性には配慮されている。デジタル人民元、匿名で利用できるのは限定的—中国中銀当局者 Bloomberg <https://www.bloomberg.co.jp/news/articles/2021-03-22/QQCOTZDWRGGA01>
- 5) CBDCの発行形態の類型化は、小泉雄介「中央銀行デジタル通貨における個人情報保護と日本での発行モデル」日本セキュリティ・マネジメント学会誌 Vol.35, No.2（2021年11月22日）を参照。
- 6) https://www.jstage.jst.go.jp/article/jssmjournal/35/2/35_3/_article/-char/ja/ 「アイデンティティの7原則」は元マイクロソフトのアイデンティティ・アーキテクトだったキム・キャメロンが2005年に整理したインターネットにおけるアイデンティティ開示の原則をまとめたもの。

をどのように保持すべきだろうか。現金の過度の匿名性の問題は広く認識されているが、「いつ、誰から、誰に、いくら移動したか」といった完全に記録可能で実名性しかないようなCBDCは忌避されるだろう⁴⁾。そのため、一定のプライバシーが保護できるような制度設計がCBDC発行に際して必要になる。前述の「銀行口座」「アカウント」「トランザクション」の各視点からみると、次のようなアイデアが考えられる。

◇「間接発行型」が望ましい

CBDCには発行主体たる中央銀行が直接利用者に口座を開設させる「直接発行型」と、CBDCの発行主体は中央銀行としても、利用者は口座を日銀内に開設するのではなく、市中銀行の口座を利用する「間接発行型」がある⁵⁾。プライバシーの観点からは間接発行型がより望ましいといえる。このような発行形態は電子マネーやクレジットカードと同等のプライバシーになるだろう。

◇アカウントの複数保有

またもう一つはCBDCを受け取り、実際の決済に利用する際のアカウントの匿名性を高める方法も考えられる。CBDCをチャージするアカウント（「ウォレット」というほうがいいかもしれない）を複数持てるようにし、それぞれのアカウントに決済額の上限に応じて段階的な匿名性を持たせることも可能だろう。特に少額決済に特化したウォレットはある程度の匿名性を持たせる一方で、高額な決済には実名性を強めることが考えられる。

◇トークンの活用

また利用時にも直接CBDCのやり取りを行うのではなく、CBDCに紐付いたトークンを用いることも考えられる。このトークンは電子マネーのように一旦CBDCをなんらかの代替ポイントに置き換えて、そのポイントを通

じた決済を行う形態だ。こうすることでプライバシーは保たれる。

これらのアイデアは、利用者の決済時のプライバシーを保護するとともに、仮にAML/CFLや犯罪収益、脱税といった事態が懸念される際には司法の判断を仰ぎつつ、保管された取引データを犯罪捜査に活用できるようにする（「実名性」のメリットを活用する）ための制度設計といえる。

その意味で、次世代の決済は利用シーンに応じて、プライバシーをコントロールできる機能が必要だ。例えば、日々の決済では匿名に近い決済で十分だが、高額な取引や、権利移転を伴うような決済ではより実名性の高いアカウントでの決済が求められるといったように、決済の重要度に応じた段階的なプライバシー保護ができるような「スマート」な決済制度が必要だと言える。

そして、このような「スマート」な決済制度においては、十分なKYCを経た銀行口座が当面の間、重要な基盤となろう。デジタル決済の隆盛は銀行口座の重要性を高める方向に作用していくと筆者は考えている。

また、デジタル世界でのアイデンティティ開示の基本原則として広く参照されている「アイデンティティの7原則」⁶⁾の中で特に重視されているのが「開示する情報は必要最低限であるべき」とする一項だ。決済のプライバシーもこの原則に従うべきだろう。

Writer's Profile



柏木 亮二 Ryoji Kashiwagi

金融デジタルビジネスリサーチ部
エキスパートリサーチャー
専門はIT事業戦略分析
focus@nri.co.jp