Payment and Settlement Systems

決済の未来フォーラム
デジタル通貨分科会

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

日本銀行決済機構局

*URL：https://www.boj.or.jp/research/brp/psr/psrb200702.htm/

レポートの目的

- 中央銀行デジタル通貨（CBDC: Central Bank Digital Currency）は、決済システムという視点だけではなく、その発行が金融システムや金融政策に与える影響も含め、検討すべきテーマが多岐にわたる

- 本レポートでは技術にフォーカス。「誰もがいつでも何処でも、安全確実に決済に利用できる」という現金の特性をCBDCが備えるための技術的な課題を整理

- デジタル通貨を取り巻く技術環境の変化のスピードは速く、本レポートは、CBDCの技術的側面に関する予備調査との位置づけ

- 本レポートは、外部の専門家との意見交換における叩き台資料として活用

現金の特性とCBDCの機能

■ 現金は、誰もがいつでも何処でも、安全確実に利用できる決済手段

■ CBDCが現金同等の機能を持つためには、「ユニバーサル・アクセス（Universal access）」と「強靭性（Resilience）」を備えることが望ましい

■ ユニバーサル・アクセス（Universal access）

✓特定の端末に限定せず、操作性や携帯性も確保

✓幅広い世代や訪日外国人による利用可能性を考慮

✓個人から法人だけではなく、個人間も含めた双方向送金（P2P）への対応

■ 強靭性（Resilience）

✓システム・通信障害への耐性

✓停電時の電力確保

→　課題：オフラインP2P決済機能を多くの人々が利用可能な端末に実現

CBDCの台帳管理

■ CBDCの発行に当たっては、発行残高や取引履歴を記録するための台帳を利用

■ オフライン決済における台帳管理では、以下のうち、③情報の管理場所が重要

①台帳の管理主体：中央・分散の双方でオフライン決済は実現可能

✓中央管理型：大量・高速処理がメリットで、利用実績も豊富

✓分散管理型：強靭性、機能拡張、将来性が特徴

②台帳の記録方法：口座・トークンの双方でオフライン決済は実現可能

✓口座型：ユーザーごとに金銭的価値の総額（残高）を紐付け

✓トークン型：金銭的価値の塊（トークン）ごとにユーザーを紐付け

③台帳情報の管理場所：オフライン決済ではローカル型を利用する必要

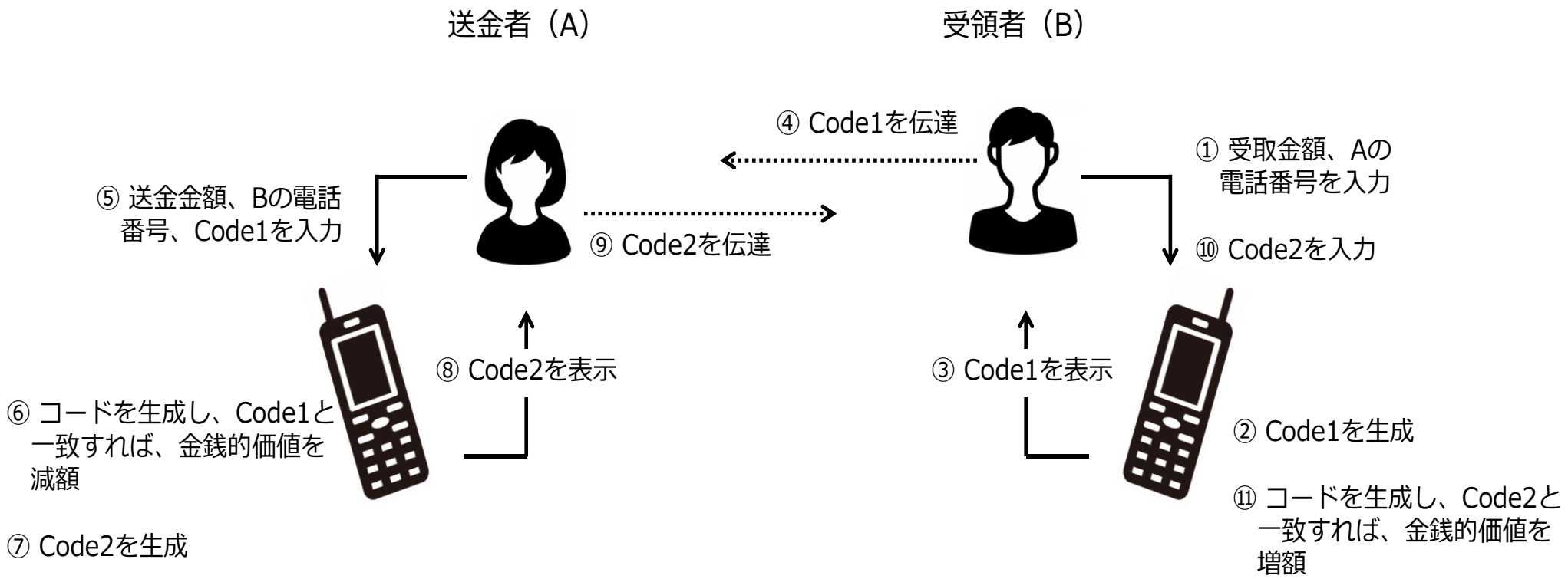
✓リモート型：ユーザーの手元から離れたサーバーで管理

✓ローカル型：ユーザーが自分の端末に金銭的価値を保蔵

ーー　オフライン決済では、台帳と端末への情報記録を適切に行い、二重使用リスクに対応することも重要

オフラインP2P決済に必要な基本機能

■ パイロットプログラム「DigiTally」における送金手順（ケニアにおける実験）



✓送金者と受領者は、それぞれのフィーチャーフォンに同一の情報を入力

✓それぞれのフィーチャーフォンは、同一の暗号技術を利用してCodeを生成

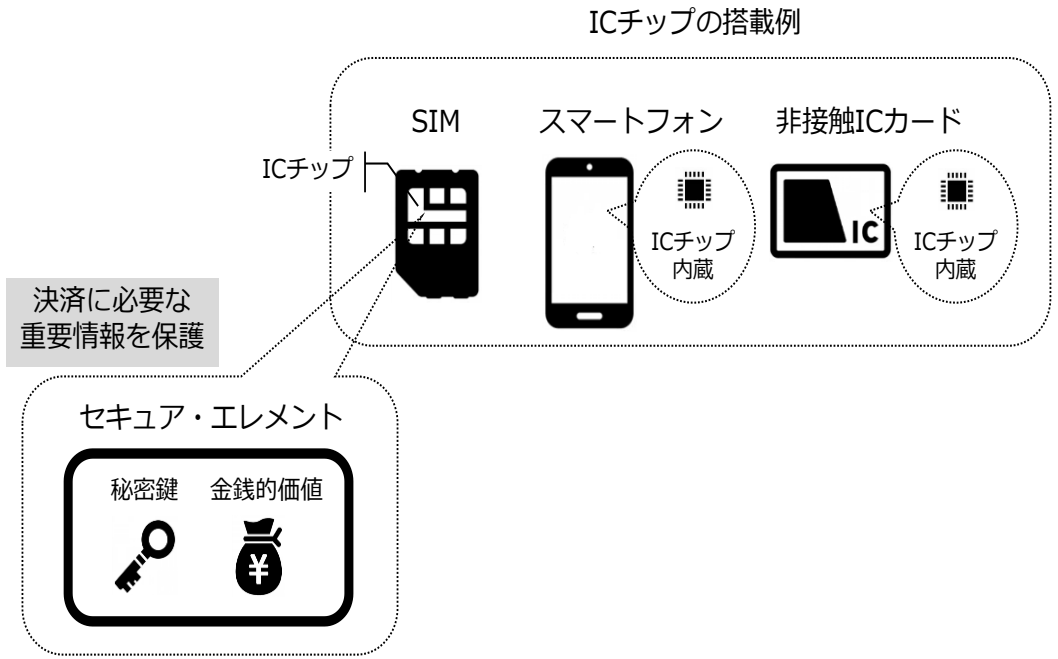
✓Codeを口頭伝達して一致すれば、フィーチャーフォン内の金銭的価値を減額・増額

オフラインP2P決済に必要な基本機能

①金銭的価値の安全な保蔵

✓SIMカード内のICチップに内蔵されたセキュア・エレメントに金銭的価値を保蔵

✓セキュア・エレメントは攻撃への耐性（耐タンパー性）を備えており、暗号技術の重要情報（秘密鍵）の保管にも利用



②ユーザー間の情報伝達

✓端末間の通信機能は利用せず、必要な情報（決済金額、送金者と受領者の電話番号、Code）を口頭で伝達

オフラインP2P決済に必要な基本機能

③認証：保有者認証と端末認証

✓保有者認証：PW入力により、端末の利用者が正当な保有者であることを確認

✓端末認証：暗号技術（共通鍵暗号方式）を用いて取引相手の端末の正当性を確認

④決済指示

✓ユーザーが決済金額、取引相手、Code等を端末に入力し、決済指示を伝達・実行

⑤電力確保

✓電池切れ時は、乾電池による給電が可能

（DigiTallyの課題）

✓情報伝達（上記②）では、口頭伝達の負担が発生

✓取引相手の端末認証（③）では、口頭伝達負担への配慮から、十分な強度の暗号技術の利用が困難で、安全性に課題

✓決済指示（④）では口頭伝達と手作業が発生し、利便性に課題

ユニバーサル・アクセス端末：スマートフォンを用いる手法

①金銭的価値の安全な保蔵

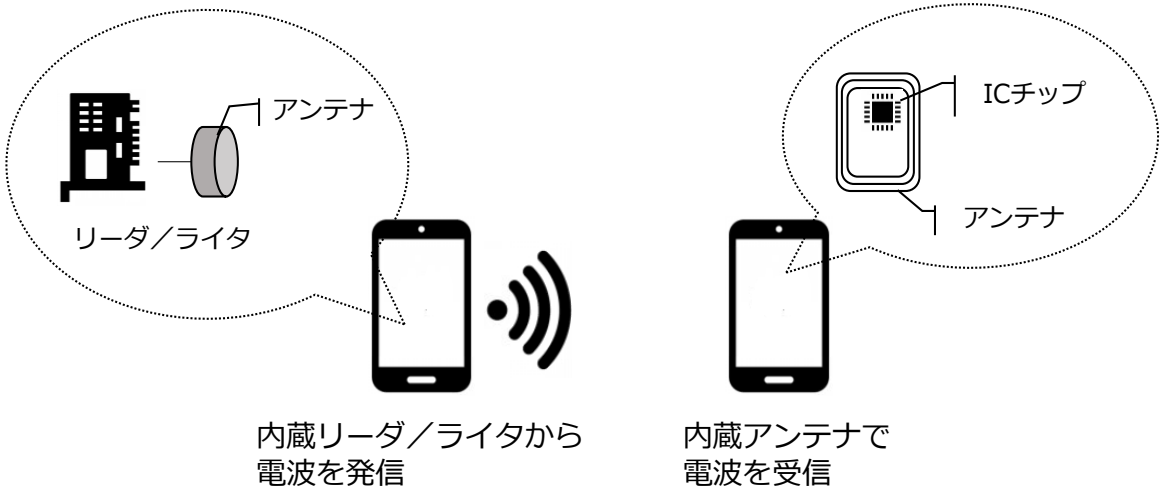
✓フィーチャーフォンと同様、セキュア・エレメントの利用が想定される

②ユーザー間の情報伝達

✓NFC（Near-field communication、下図）等の無線通信が想定される

✓電波受信アンテナと電波発信機能を備えた「リーダ/ライタモード」機能が搭載された機種ではNFCの利用が可能

✓情報伝達に手作業が不要で、認証では安全性の高い十分な長さの暗号文を利用可能



無線通信により端末認証、決済指示を行う

ユニバーサル・アクセス端末：スマートフォンを用いる手法

③認証

✓保有者認証：PWや生体認証が利用可能

✓端末認証：暗号技術を用いて取引相手の端末の正当性を確認

④決済指示

✓リーダ/ライタモードを用いた金銭的価値の記録が可能とみられる

⑤電力確保

✓電池切れ時は、乾電池による給電が可能

（スマートフォンの課題）

✓スマートフォンの普及率は65%（2018年）で、ユニバーサル・アクセスが課題

✓金銭的価値の保蔵（①）では、既存のセキュア・エレメントを利用する場合はライセンス料等が生じる可能性があるほか、新規開発の場合は追加費用が発生

✓決済指示（④）では、リーダ/ライタモードなどのフィージビリティ・チェックが必要であり、機能の安定性や処理性能の検証が課題

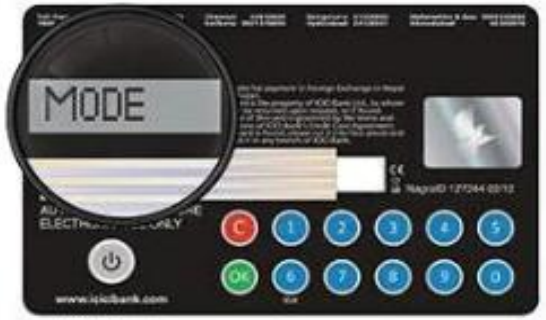
ユニバーサル・アクセス端末：カード等の新たな端末を用いる手法

実装イメージ

✓金額を入力・表示するための小型テンキー、モニターをカード上に搭載し、電池もカードに内蔵（下図）

✓カード同士を近付けて決済する方法では、カード間で情報を伝達するための無線通信機能を利用

テンキー、モニター搭載型カードの例（出典：icicibank.com）



①金銭的価値の安全な保蔵

✓他の手法同様、セキュア・エレメントの利用が想定される

②ユーザー間の情報伝達

✓無線通信のためのリーダ/ライタ機能の搭載が想定される

ユニバーサル・アクセス端末：カード等の新たな端末を用いる手法

③認証

✓保有者認証：PWや指紋・顔等の身体的特徴を用いた生体認証が利用可能

✓端末認証：暗号技術を用いて取引相手の端末の正当性を確認

④決済指示

✓モニター、テンキーに加え、リーダ/ライタ機能が必要

⑤電力確保

✓小型電池は利用可能であるが、十分な寿命と充電機能の確保が必応

（カード等の新たな端末の課題）

✓ユニバーサル・アクセスの確保に資するとみられる一方、必要な機能の開発には一定の期間とコストが発生

✓ユーザー間の情報伝達（②）や決済指示（④）に必要なリーダ/ライタ機能の小型化のほか、テンキー、モニター、十分な寿命や充電機能を備えた小型電池（⑤）の開発が重要

オフライン決済：セキュリティ確保のためのセーフガード

セキュア・エレメントに関する論点

- ✓リスク：攻撃の巧妙化・複雑化に伴う秘密鍵の盗取やCBDCの不正記録
- ✓対策：定期的な端末交換を通じた安全性の確保。カード型の場合は、クレジット・デビットカードのように有効期限を設けることが有効

暗号技術に関する論点

- ✓リスク：量子コンピュータの実用化など攻撃の計算能力向上に伴い、暗号技術のセキュリティは低下
- ✓対策：セキュア・エレメントの一定期間毎の交換や、量子コンピュータなどを用いた不正に対応するための新たな暗号アルゴリズムの実装

管理者によるモニタリングの限界に関する論点

- ✓リスク：脅威の常時把握が困難で、脆弱性発覚時でも、決済サービスの利用停止などの対応を採ることが困難
- ✓対策：端末のセキュリティ確保に加え、CBDCの保蔵金額や利用金額に上限を設け、被害規模を限定

オフライン決済：プライバシーの確保とAML/CFTへの対応

匿名性やプライバシーに関する論点

✓暗号技術や仮名の利用により、一定の匿名性を確保可能

✓ただし、以下のAML/CFT対応との両立が課題

管理者や公的当局による決済情報の把握に関する論点

✓リスク：ユーザーの端末がオンライン接続されなければ、決済情報の把握は困難。決済情報が把握できない状態を一切許容しない場合は、オフライン決済の利用を禁じる必要

✓対策：オフライン決済を許容しつつ、不正取引のリスクを抑制する場合は、オンライン接続の都度、決済履歴の台帳記録を求め、異常取引を把握。また、保蔵金額や利用金額を限定する方法も想定される

――　プライバシー、AML/CFTは、中央銀行が直接所管する分野ではなく、公的当局が決済以外の観点も含め様々な観点から多角的に検討する必要

まとめ

CBDCが現金同等の機能を備えるための課題

- ✓ユニバーサル・アクセス：多様なユーザーが利用可能な端末の開発
- ✓強靭性：通信・電源途絶への耐性を備えたオフラインP2P決済機能の確保

ユニバーサル・アクセス端末によるオフラインP2P決済の実装上の課題

- ✓スマートフォン：オフラインP2P決済の実用化に向けた機能の安定性や処理性能の確保が重要
- ✓カード：情報伝達や決済指示に必要な機能（リーダ/ライタ）や、テンキー、モニター、電池等の開発に時間とコストが必要

オフライン決済で考慮すべき論点

- ✓セキュリティ：金銭的価値の安全な保蔵、暗号技術の強化、モニタリング制約を踏まえた取引制限の導入
- ✓プライバシーとAML/CFT対策：双方の両立、追跡可能性の確保、取引制限の導入

以　上