Beyond Finance®

みらいの社会のつくり手に

NTT DATA

【WG5】第10回会合
価値移転プロトコル（電子現金）について
Off-Chain Solution for Tokenization

2025年09月22日
株式会社NTTデータ
金融イノベーション事業本部　次世代決済企画室

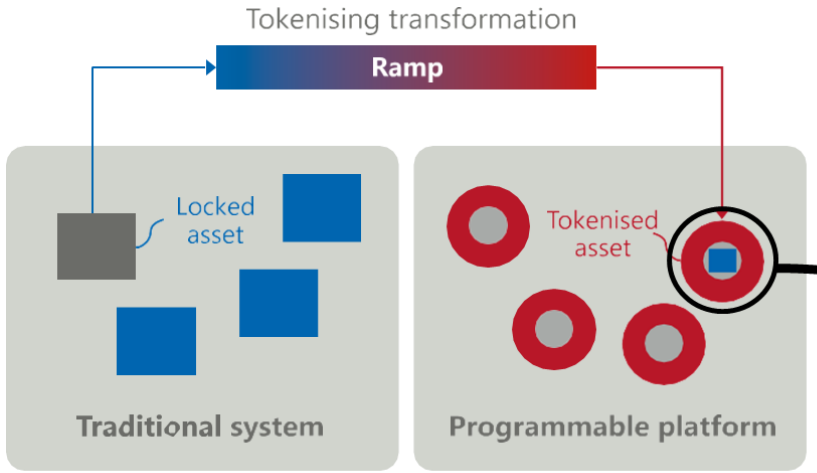
01

価値移転プロトコルについて

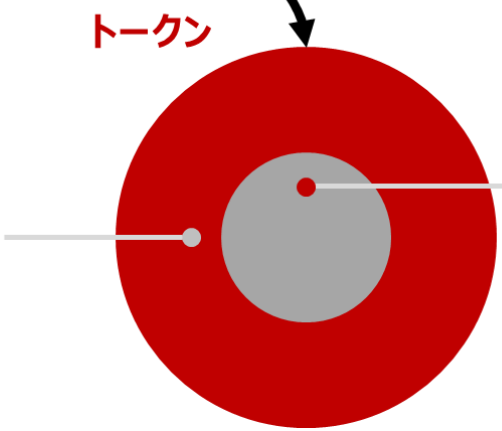
“デジタル化”とは？　“トークン化”と“プログラマビリティ”

Beyond Finance®
みらいの社会のつくり手に

トークン化とは高いプログラマビリティの実現を目指して「従来の伝統的決済システム上の価値」を「プラットフォーム自体が実行環境となるシステム上のトークン」に置き換えるプロセス



金融安定理事会（FSB）：「資産のデジタルな表章（トークン）を作り出し、分散型台帳上に置くプロセス」
国際決済銀行（BIS）：「金融資産や実物資産に関する権利を、**プログラマブルなプラットフォームにおいてデジタルに表章するプロセス**」



ルール
アセットは何ができて、何ができないか（スマートコントラクトで使用）

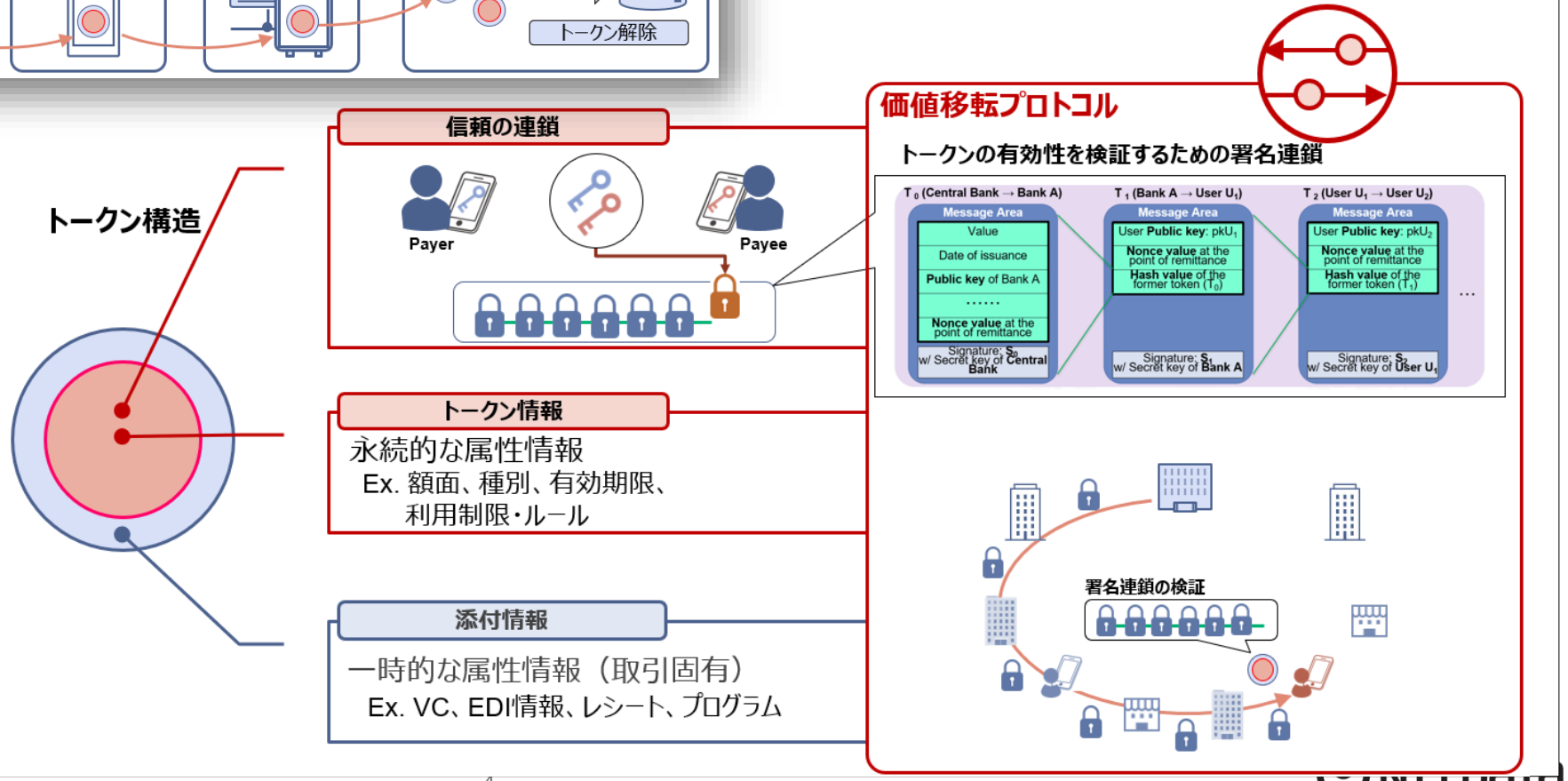
情報
どのようなアセットで、どこから来たのか、誰が所有しているのかなど

NTT DATA

価値移転プロトコルとトークン構造

Beyond Finance®
みらいの社会のつくり手に

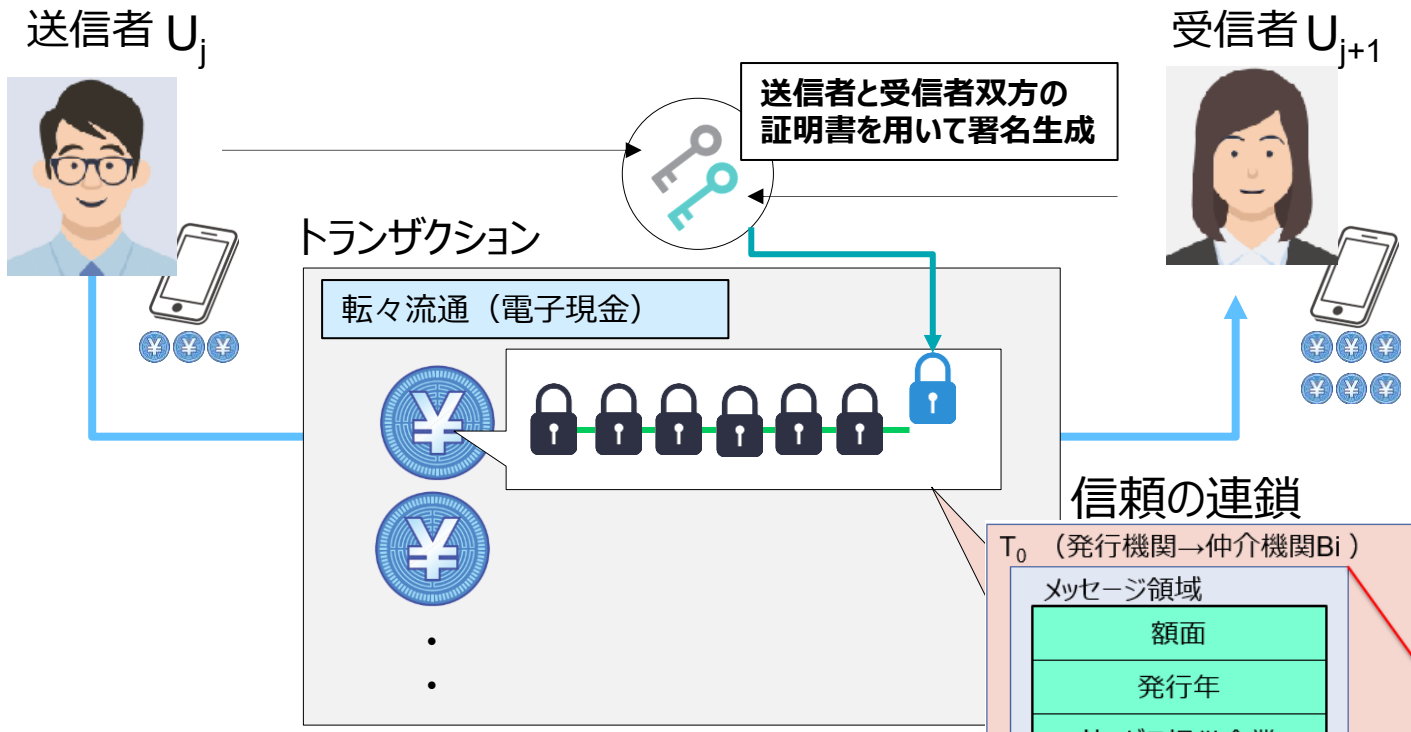
価値移転プロトコルはデバイス間で直接価値や情報を改ざんさせずに安全に転々流通させる技術
プラットフォームの制約を受けることなくお金に色を付けることが可能



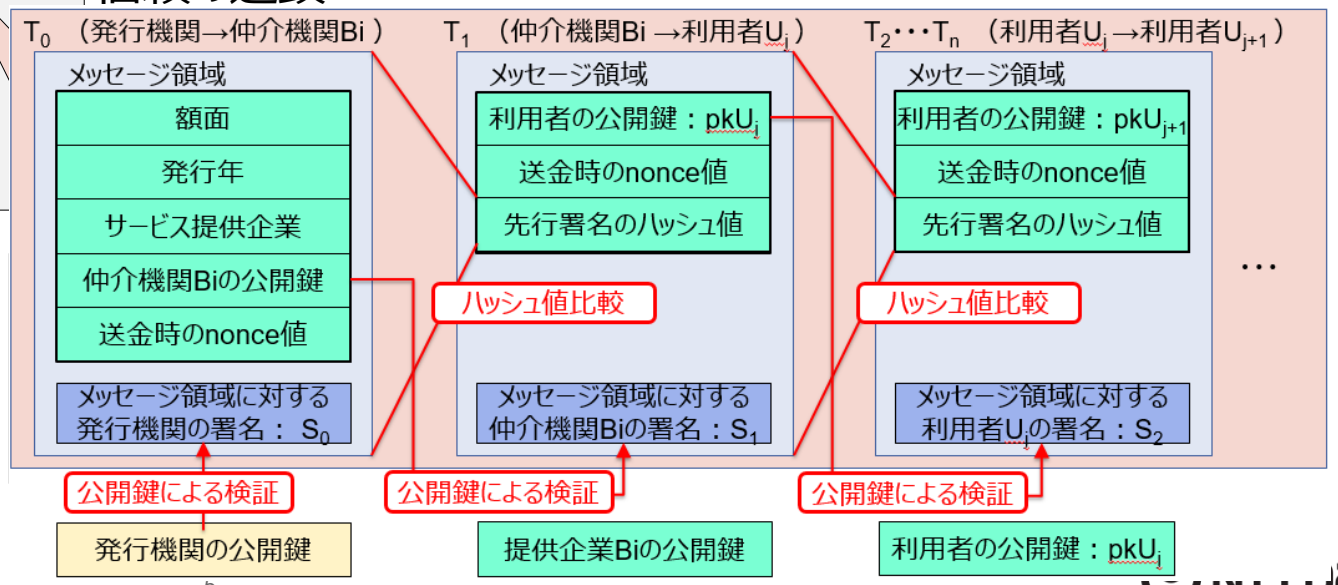
（参考）価値移転の仕組み

Beyond Finance®
みらいの社会のつくり手に

流通する電子現金自体に検証に必要な「署名データの連鎖」を格納することで、当事者間で正当性を確保可能とする



「送り手と受け手の双方の証明書を用いて署名し、各通貨内に移転を記録(署名生成・連鎖)
受け取る際には発行機関から順次署名の連鎖を検証することで電子現金の正当性を担保



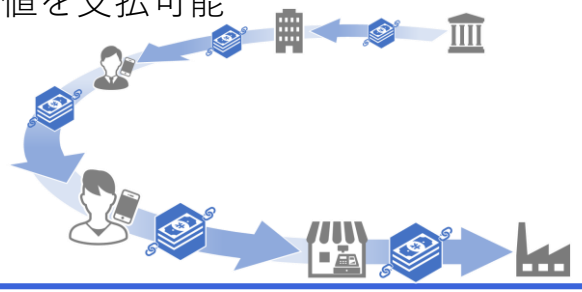
価値移転プロトコルの利点

Beyond Finance®
みらいの社会のつくり手に

従来技術と比較して、価値移転プロトコルに準拠したシステムでは様々なメリットを享受することが可能

転々流通性の実現

二者間で決済が完結でき、受取者は即時に価値を支払可能



性能上限の解消・設備コストの低減

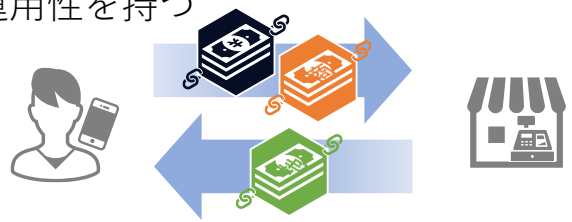
台帳への処理集中が解消。性能上限がほぼ存在せず、設備コストも低減される

ふるまいの制御

用途や利用可能地域などの制限、高額転売の抑止、有効期限の設定など

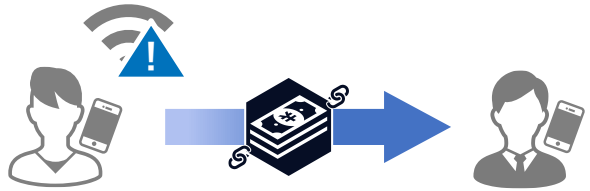
トークンの相互運用性

PFではなくプロトコルであるため、同じプロトコルに準拠しているトークンは相互運用性を持つ



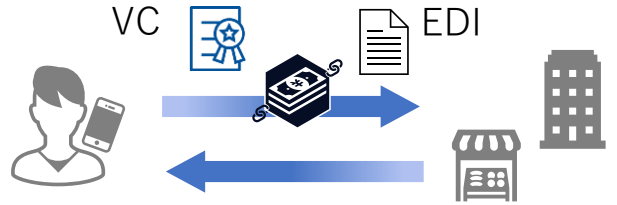
障害に対する強靭性確保

通信手段透過なので障害発生時もローカル通信によってデバイス間で決済可能



価値と情報のAtomicな転送

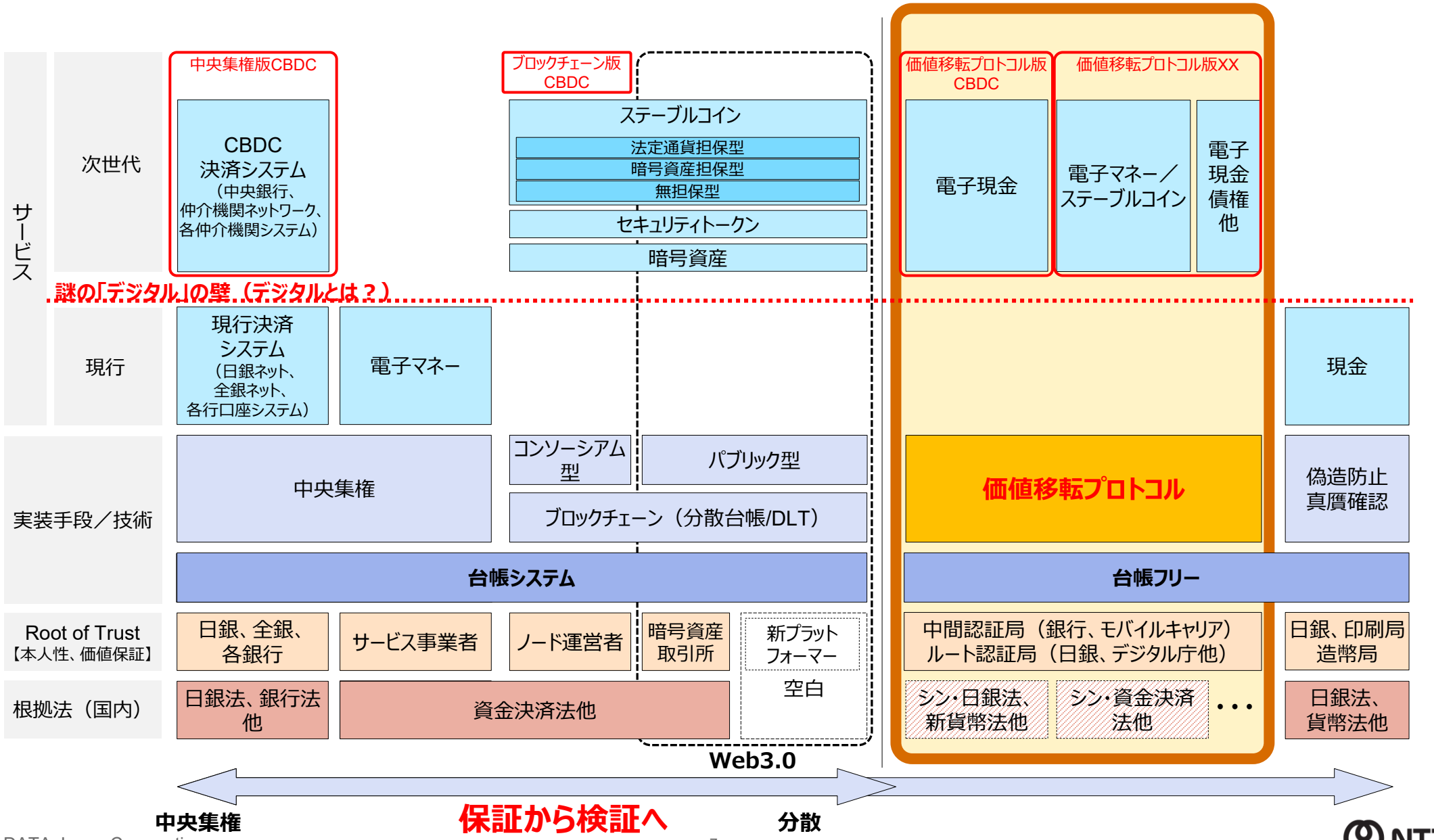
VCやEDI、内訳等の同時送付や、クーポンや領収書、診療明細等の返信等



NTT DATA

価値移転プロトコル（電子現金）と従来技術の世界観

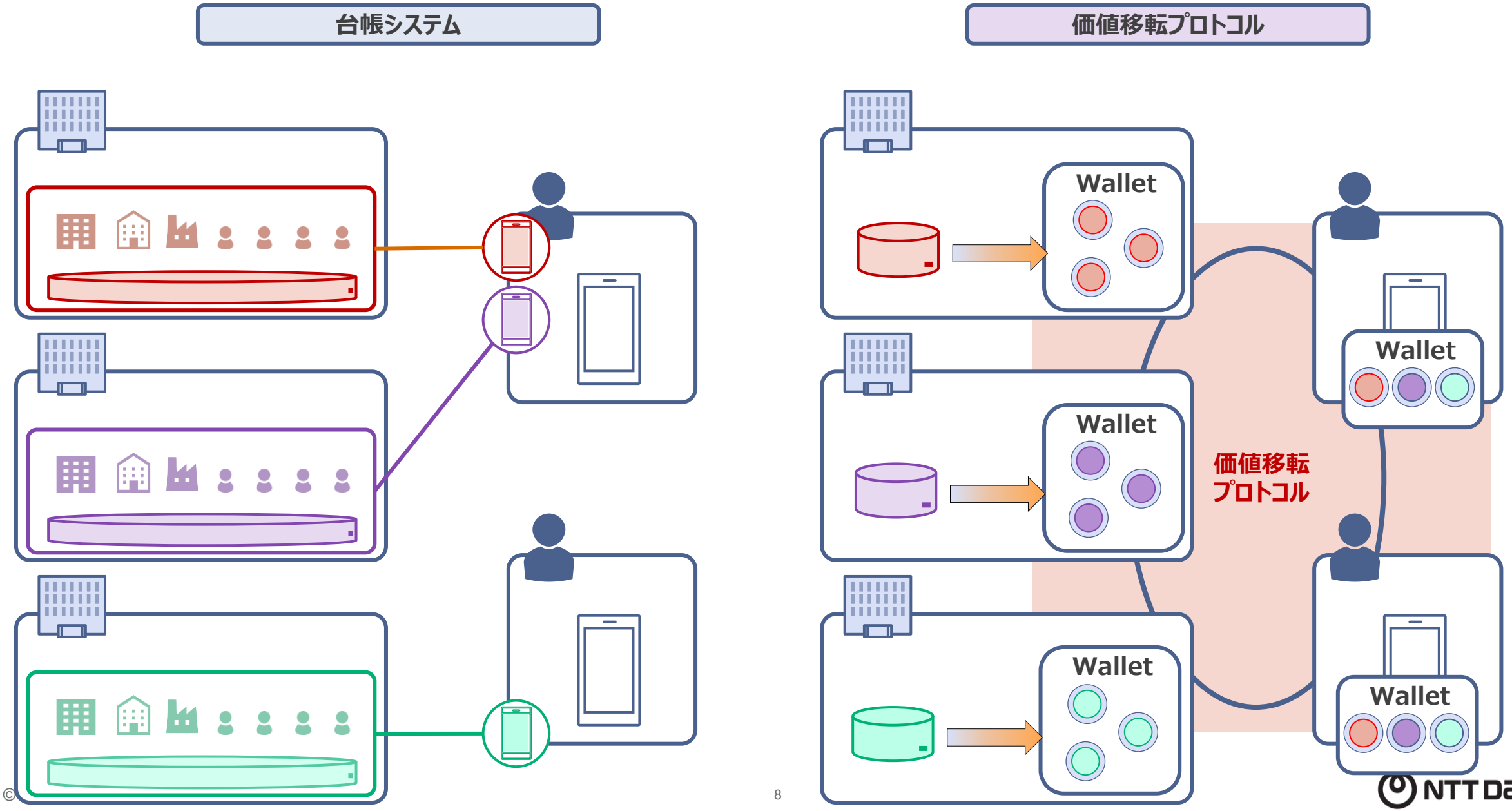
Beyond Finance®
みらいの社会のつくり手に



NTT DATA

脱サイロ化の実現　～プラットフォームからプロトコルへ～

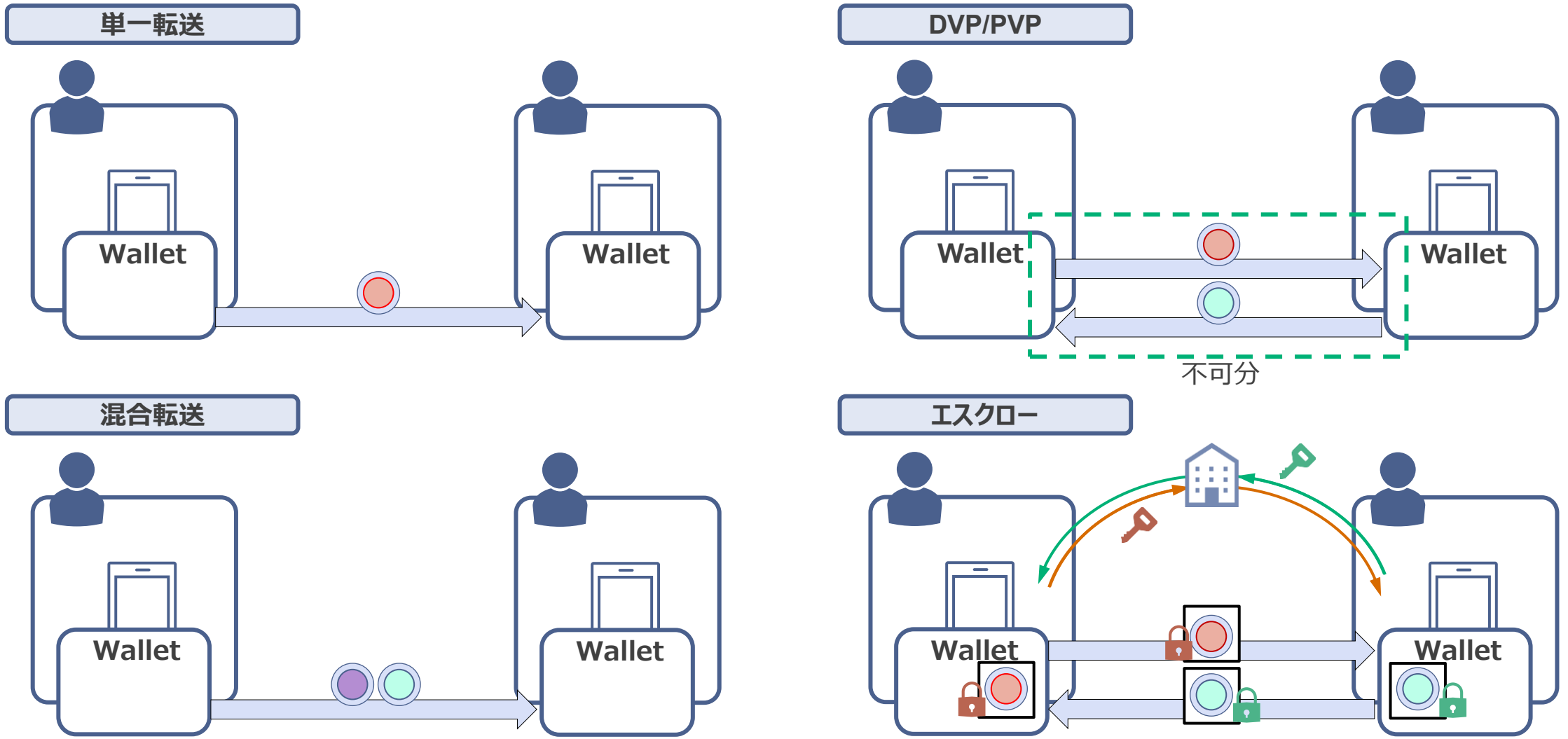
Beyond Finance®
みらいの社会のつくり手に



NTT DATA

各種転送方式

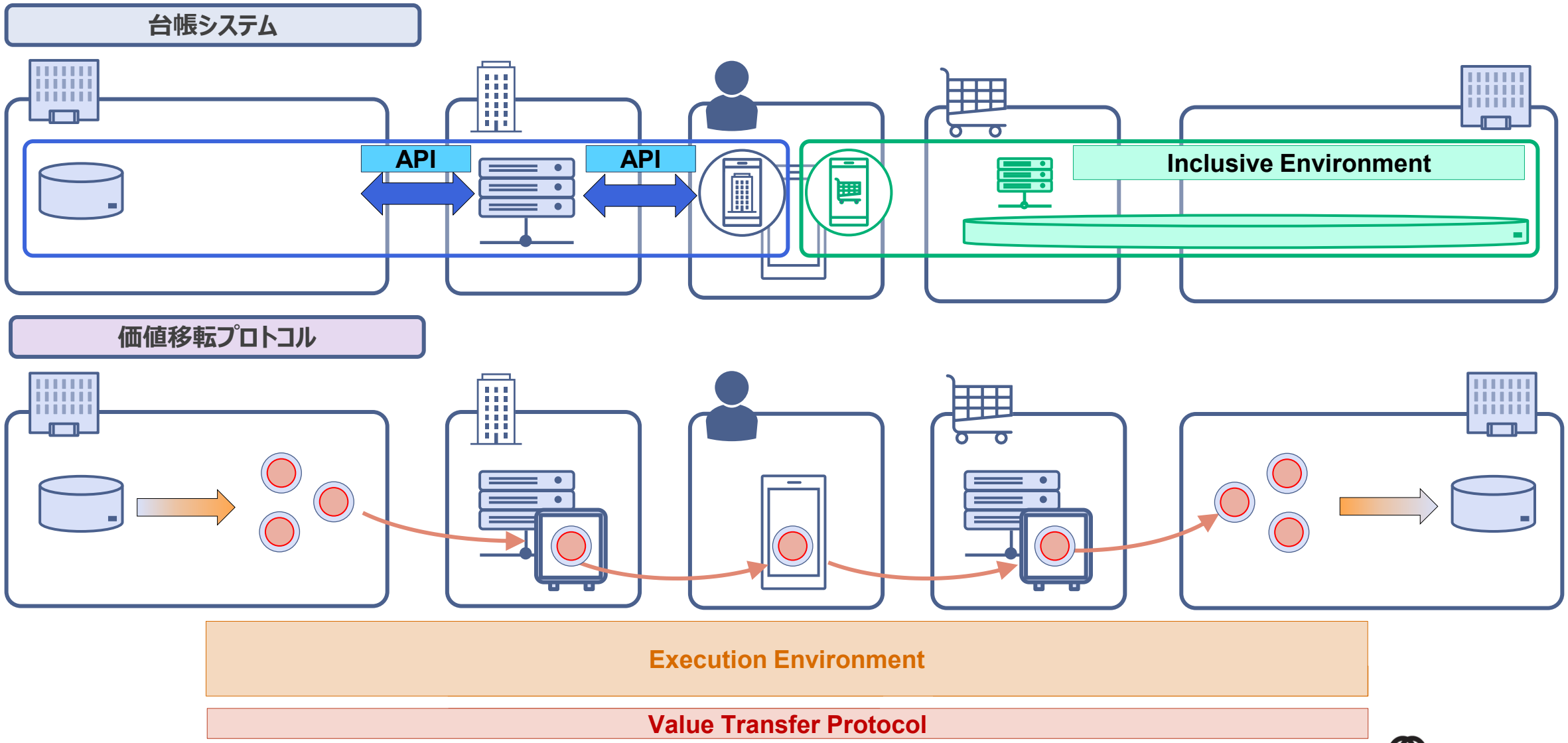
Beyond Finance®
みらいの社会のつくり手に



NTT DATA

プログラマビリティ

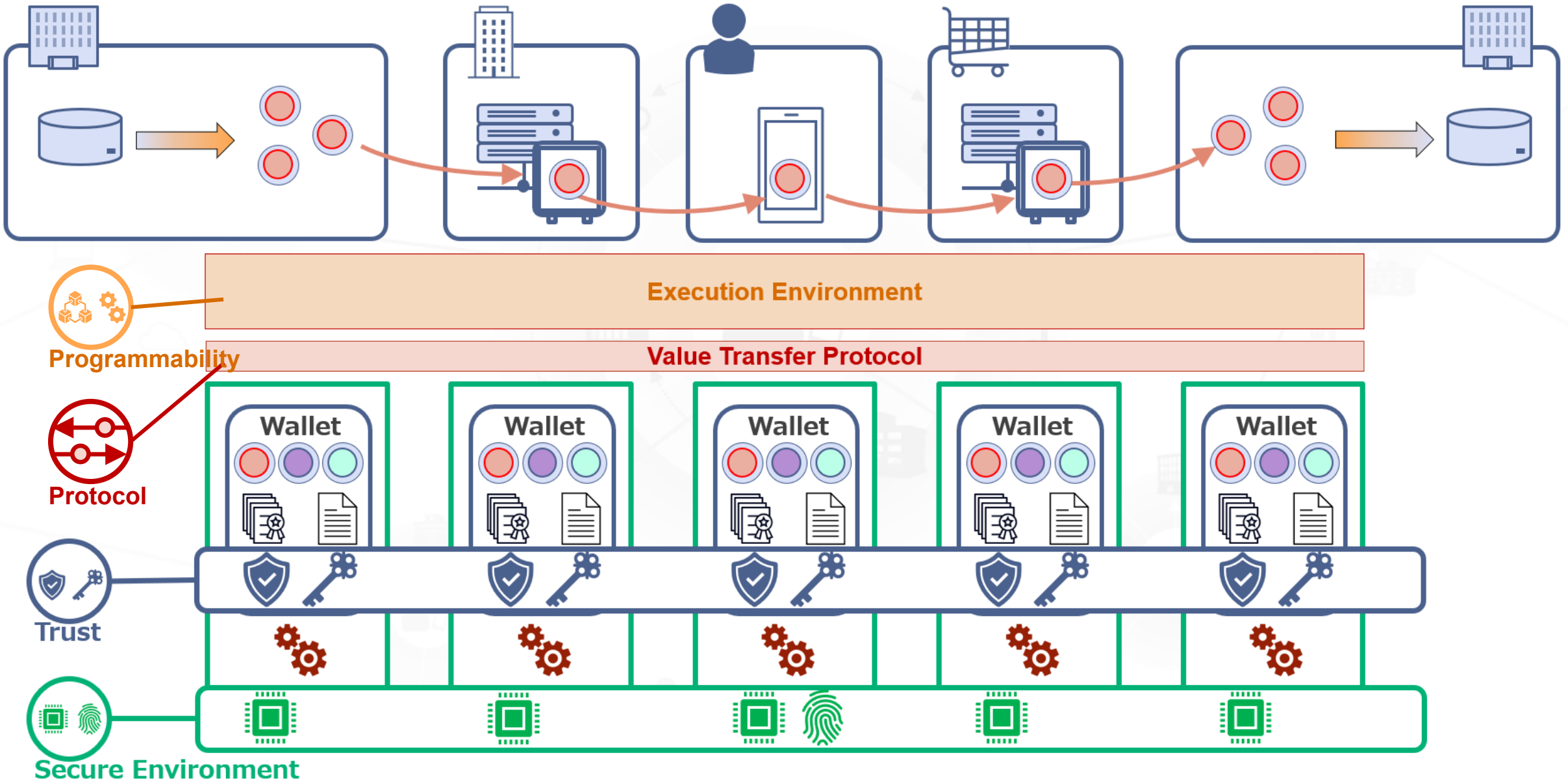
Beyond Finance®
みらいの社会のつくり手に



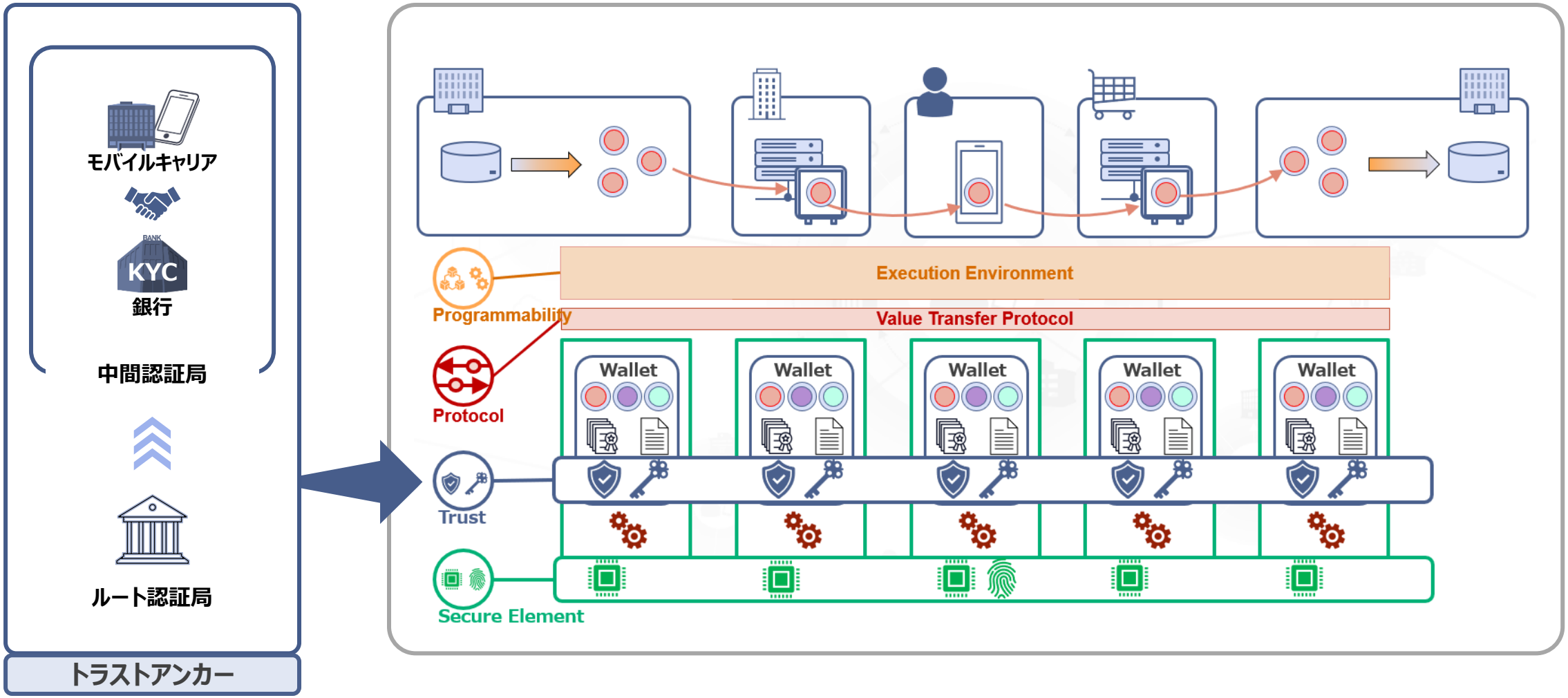
NTT DATA

Walletとそれを支えるTrust、Secure Element

Beyond Finance®
みらいの社会のつくり手に



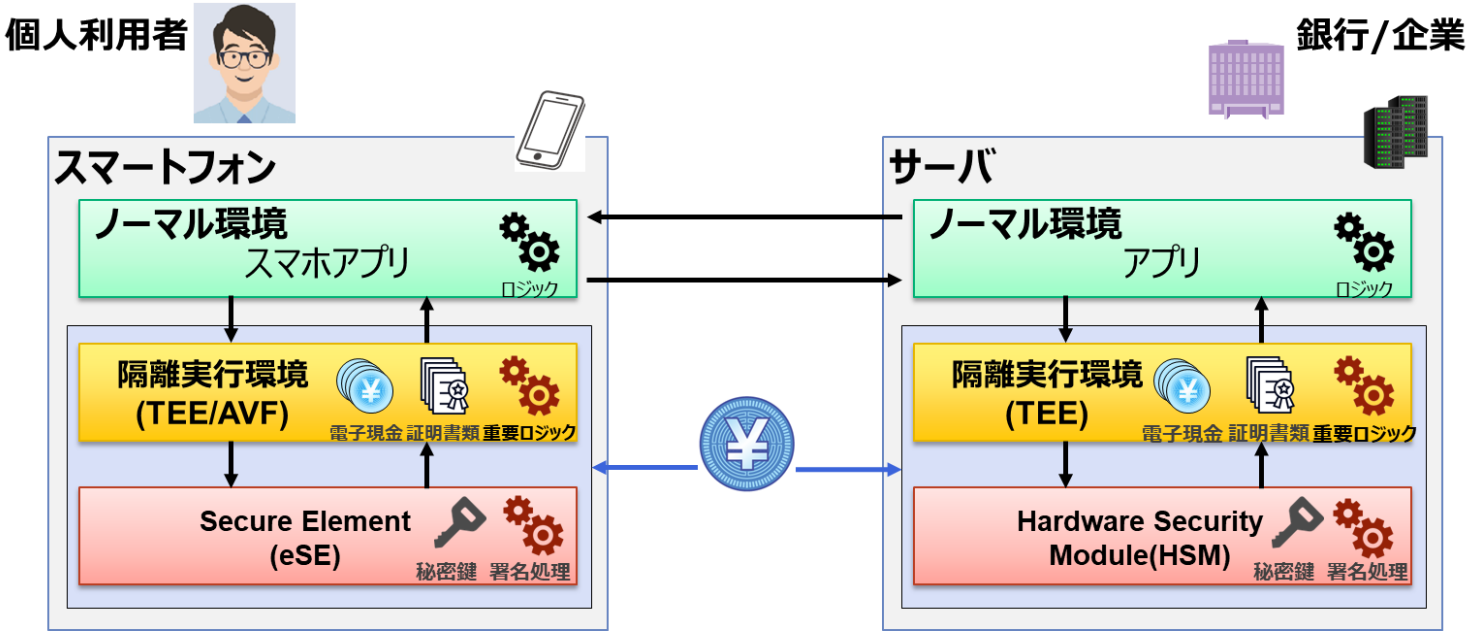
Digital Identity Walletとトラストアンカー



価値移転の署名・検証ロジックや秘密鍵等を守る仕組み

Beyond Finance®
みらいの社会のつくり手に

署名・検証ロジックの改ざんや秘密鍵の漏洩によって電子現金の偽造や複製などの不正が起きないように、これらを隔離実行環境やセキュアデバイスで保護し、安全な価値移転を実現する。



耐タンパ性

デバイス	ロジックの保護	秘密鍵の保護
スマホサイド	**Runtime Application Self Protection(RASP)** スマホアプリに対する不正な入力や攻撃の検知及び阻止 **構成証明(アテステーション)** 実行するアプリケーションの改ざんを検知する技術 **Trusted Execution Environment(TEE)/AVF** 隔離された環境でアプリケーションを実行するための技術	**embedded Secure Element(eSE)** 外部からの解析攻撃への耐性を備えたチップの機能
サーバサイド	**Trusted Execution Environment(TEE)** 通常のOSから隔離された環境でアプリケーションを実行するための技術 **構成証明(アテステーション)** 実行するアプリケーションの改ざんを検知するための技術	**Hardware Security Module(HSM)** 外部からの解析攻撃への耐性を備えた秘密鍵管理専用のアプライアンス機器／クラウドサービスの機能

AVF（Android Virtualization Framework）：
チップ間の非互換性を解決するためにGoogleが提唱している新しい隔離実行環境技術

NTT DATA

NTTグループ連携による競争力創出

Beyond Finance®
みらいの社会のつくり手に

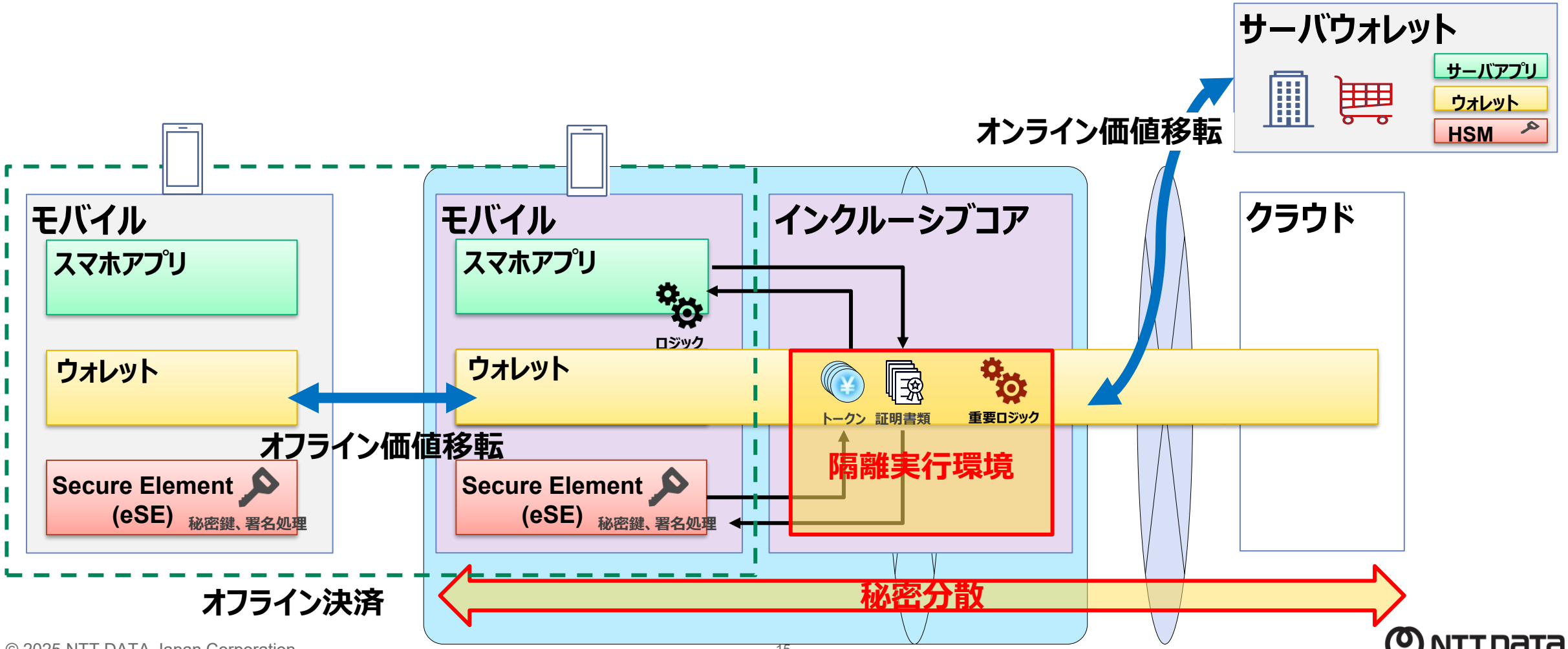
グループ横断（下図参照）の強みを連携し、リテール（モバイル）／エンタープライズ（サーバ）双方における
セキュアレイヤを構築し、デジタル社会における“オセロ盤の端”を確保すると共に、標準化活動を進めていく。

NTT DATA

インクルーシブコア（In-Network-Computing ）との連携について

Beyond Finance®
みらいの社会のつくり手に

価値移転プロトコルを通信インフラ（エッジ）と連携させることで可用性、安全性を確保
オンライン／オフライン双方において透過に価値移転を実現できる技術（防災・強靭化）



NTT DATA

参考文献のご紹介

Beyond Finance®
みらいの社会のつくり手に

本章の内容は下記金融研究所様との共同研究論文もお読みいただけると幸いです。

日本銀行金融研究所
Institute for Monetary and Economic Studies, Bank of Japan

サイト内をキーワードで検索　English

トップ | 研究所概要 | 論文 | Newsletters | 国際コンファランス | 研究会 | 歴史統計ほか

シェアする　ポストする　印刷　記事を閉じる

金融研究 第４４巻第３号 (2025年7月発行)

本文[1,288 KB PDF]

関連刊行物
DPS-E
DPS-J

台帳を用いない決済方式に関する技術面からの一考察

田村裕子、阿部正幸、奥田哲矢、津川天祐、宮澤俊之、山村和輝、赤羽喜治、田口智貴、平栗勇人、増田博人、山田健斗

本稿は、サービス事業者を介さず、台帳を用いることなく決済を可能とする決済方式について、その技術的側面から考察を行うものである。これは、現金に見立てた電子データの送受信によって決済を行う手段であり、暗号技術に関する研究分野では、「電子現金」という名称で検討が進められてきた。1990年代にはいくつかの実証実験が行われたが、当時の技術水準ではユーザビリティを確保することが難しかったものと推測される。そこで、本稿では、この間の技術進展および社会ニーズを踏まえて電子現金方式の再整理を行うとともに、スマートフォンを用いた実機検証を通して、現在の技術水準であればユーザビリティの高い電子現金を提供できる可能性があることを示す。また、技術的側面から、電子現金のさらなるユーザビリティ向上とプライバシ強化に向けて、電子現金を任意の金額に分割・集約可能な方式、および、同一ユーザが使用した電子現金の相互の関連付けを困難とする方式を提案する。なお、本稿はあくまで電子現金にかかる技術面からの考察を行うものであり、法律や制度、実運用等、社会実装に向けた実現可能性は検討の対象外であることには留意されたい。

キーワード：スマートフォン決済、デジタル決済、電子現金、電子マネー、プライバシ保護

金融研究 第４４巻第３号 ：全文 [2,318 KB PDF]

https://www.imes.boj.or.jp/research/abstracts/japanese/kk44-3-3.html
2025年7月掲載

1．はじめに 1
2．電子現金方式の基本構成 3
（1）台帳方式と電子現金方式との違い 3
（2）電子現金方式に求められる性質 6
（3）基本方式 8
（4）セキュリティに関する考察 16
（5）プライバシ保護と透明性に関する考察 18
3．電子現金方式の実機検証 20
（1）過去の実証実験 20
（2）実機検証の概要 21
（3）実機検証結果 26
4．電子現金方式の効率化に向けた検討 27
（1）電子現金の送受信にかかる効率化 28
（2）電子現金の還収にかかる効率化 30
（3）変動額面方式に関する考察 30
（4）プライバシを強化した電子現金方式 33
5．おわりに 39
参考文献 41
補論 1．認証機関の機能を分割した場合の証明書発行手順 44
補論 2．電子現金方式の効率化 45
（1）電子現金の送受信にかかる効率化 45
（2）電子現金の還収にかかる効率化 48
補論 3．プライバシを強化した電子現金プロトコル 49
（1）Σプロトコル 50
（2）3 つの実現方法 51

NTT DATA

02

「幅広い状況下で使える」ためのディスカッション

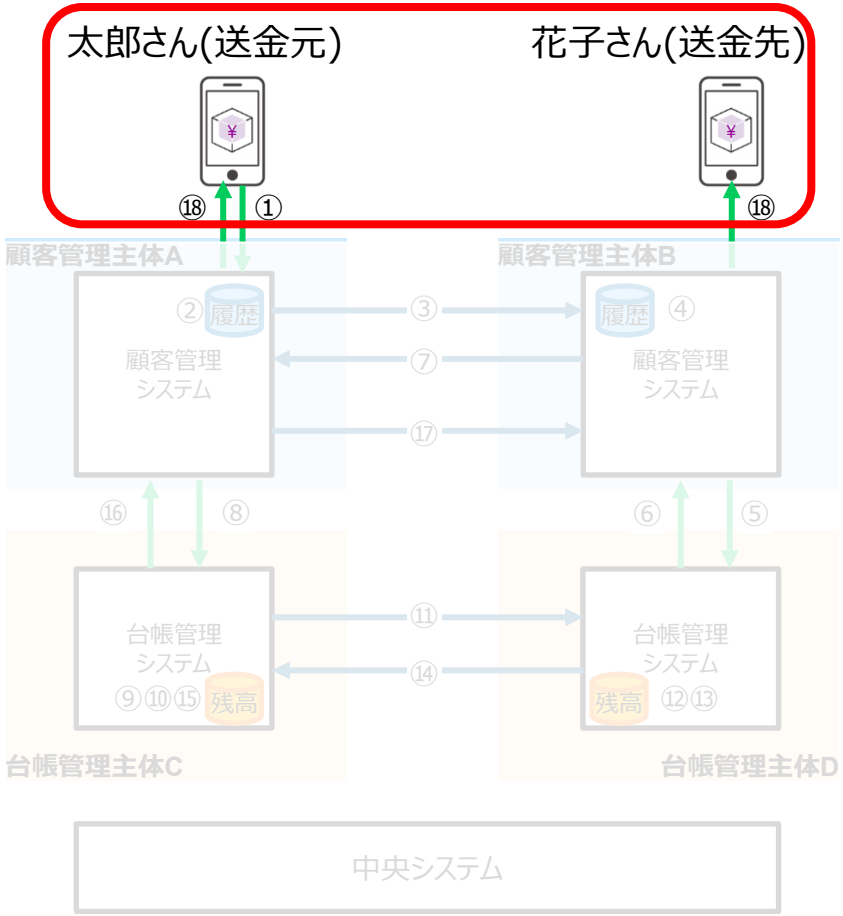
1.2. プレゼンの目的と前提となる考え方

【WG7】第6回会合 弊社資料
「民間決済ネットワークにおけるエラー制御を踏まえたCBDCシステムへの示唆について」より

以下の視点を出発点として、考察を経て、論点を抽出し、アプローチの方法や視点を拡げることを目的としています

実験用システムは顧客管理システムと
台帳管理システムの４つのシステムで構成

送金元アプリで「振込」を行い
「送金元への応答」と「送金先への通知」で相互に目視確認



出発点とする視点・考え方

1 送金元・送金先双方の確認を前提

対面での決済シーンにおいては、送金元と送金先の双方のアプリにて、正常に決済処理が完了した旨の通知を確認することで、完了する流れを前提とする

2 オフライン決済機能は考慮しない

エラーの発生により、オンラインでの取引結果が曖昧な場合でも、アプリ側でオフラインで取引を扱い、あとでオンラインで同期をとって、結果整合性を確保するなどの発想も考えられるが、今回は、オンライン処理のみで、整合性を確保する前提とする

3 台帳更新後の結果の通知は、顧客管理主体Aを起点に行う

処理手順のとおり、結果の通知は顧客管理システムAを起点に行うものと考え、顧客管理システムAが正常に処理できない場合は、顧客管理システムBにもその影響が波及するものと考える

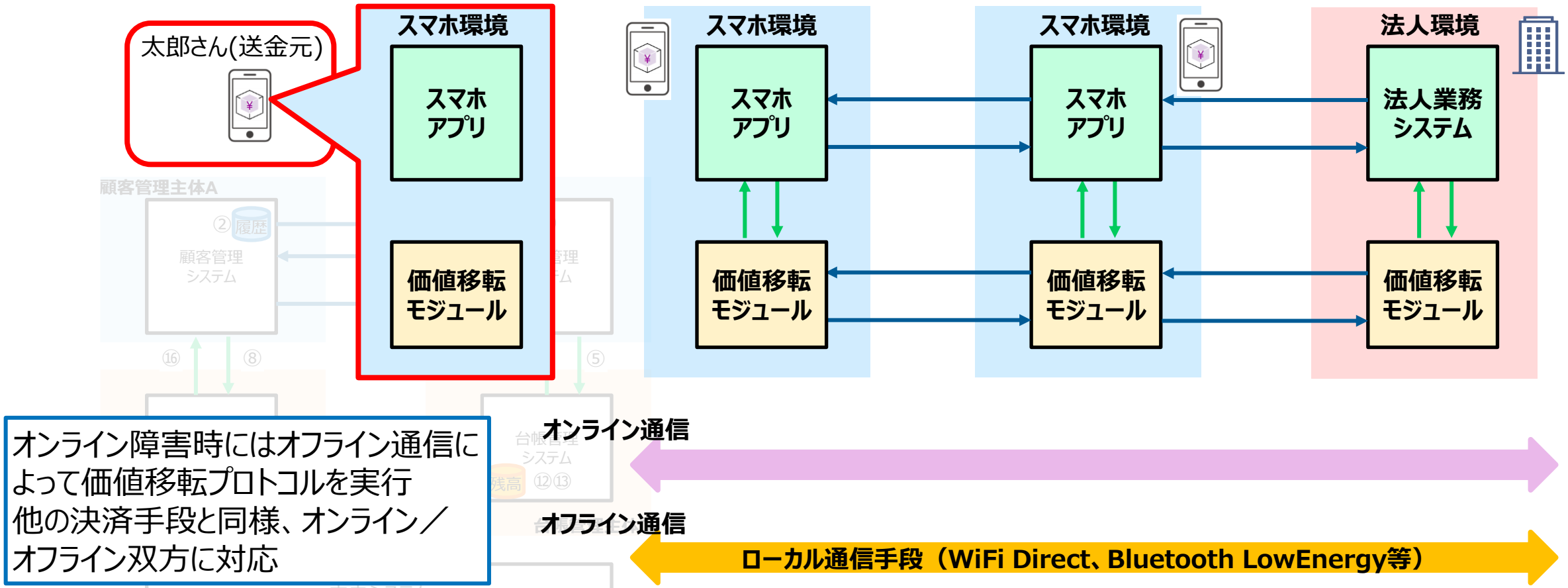
4 送金先に入金された残高は、即時に利用される可能性がある

⑬で入金完了し、ファイナリティが確定した後は、不可逆であり、残高は即時利用される可能性があることを前提とする

2.1. 価値移転プロトコルにおける検討の方向性

Beyond Finance®
みらいの社会のつくり手に

各デバイス／システム環境はアプリと価値移転モジュールの二層より構成され、アプリ＝モジュール間通信が利用者間通信にはアプリ間通信、モジュール間通信があり、WG7での議論と類似の構成。対応策も流用可能と思量



オンライン障害時にはオフライン通信によって価値移転プロトコルを実行
他の決済手段と同様、オンライン／オフライン双方に対応

NTT DATA

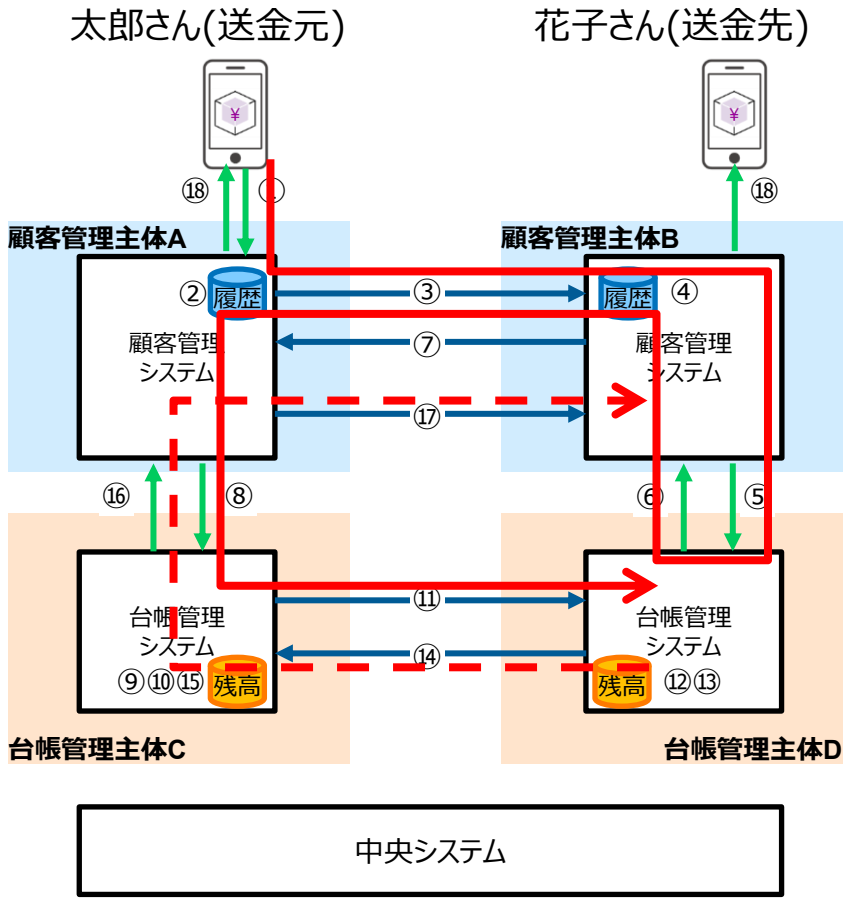
1.1. 題材とするユースケースについて

【WG7】第6回会合 弊社資料
「民間決済ネットワークにおけるエラー制御を踏まえたCBDCシステムへの示唆について」より

実験用システムにおける以下の代表ケースを題材に、エラーケースを抽出します

題材とするユースケース例

送金元アプリで「振込」を行い
「送金元への応答」と「送金先への通知」で相互に目視確認



	行為者	処理内容
①	太郎	Aに送金指示
②	A	取引履歴を確認し、太郎が送金可能かを判定
③	A	送金先（花子）を特定し、Bに送金を通知
④	B	取引履歴を確認し、花子が受取可能かを判定
⑤	B	Dに台帳更新許可トークンを発行依頼
⑥	D	Bに更新許可トークンを発行
⑦	B	Aに了解を返送
⑧	A	Cに送金指示
⑨	C	送金にあたって残高不足していないか太郎の台帳を確認
⑩	C	**太郎の台帳を留保付で減額記帳**
⑪	C	Dに増額指示
⑫	D	⑥と⑪を突合のうえ、保有上限確認
⑬	D	花子の台帳を増額記帳（決済ファイナル）
⑭	D	Cに完了を通知
⑮	C	**太郎の台帳の留保を取る**
⑯	C	Aに完了通知
⑰	A	Bに完了通知
⑱	A、B	Aは太郎宛、Bは花子宛に取引の完了を通知

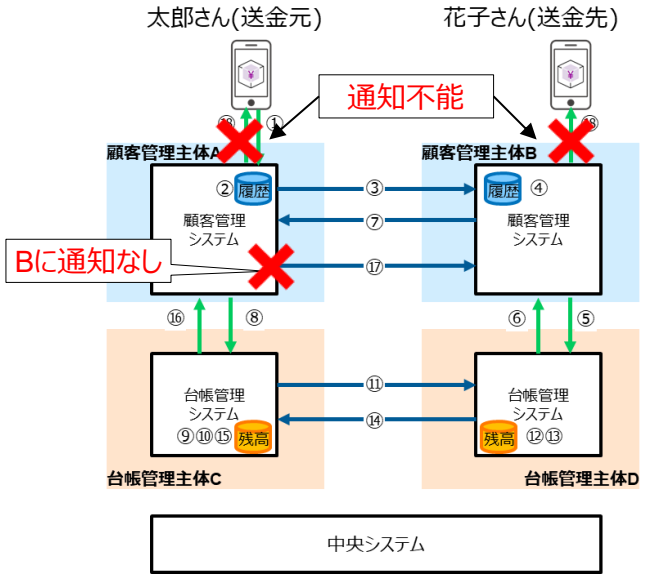
減額留保

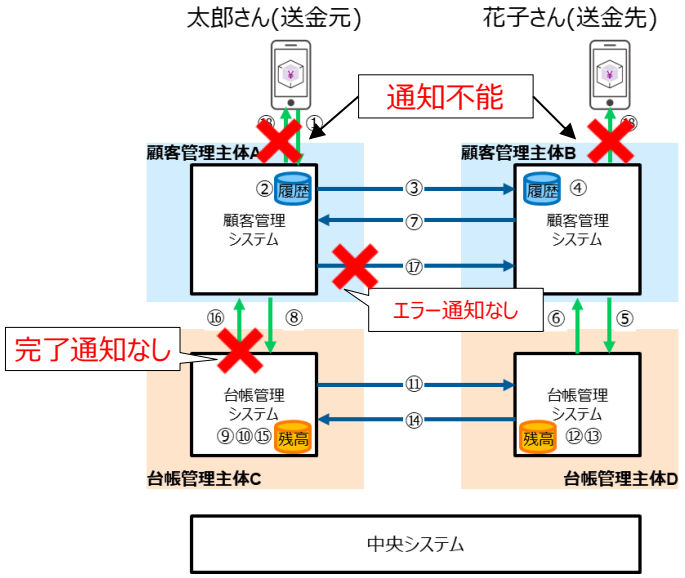
2.2. CBDC実験用システムを例とした課題認識

【WG7】第6回会合 弊社資料
「民間決済ネットワークにおけるエラー制御を踏まえたCBDCシステムへの示唆について」より

いずれのケースも、現場で再実施をした場合2重決済となる影響が懸念されるため、これに対処する制御が必要

【ケース①】顧客管理システムAの障害



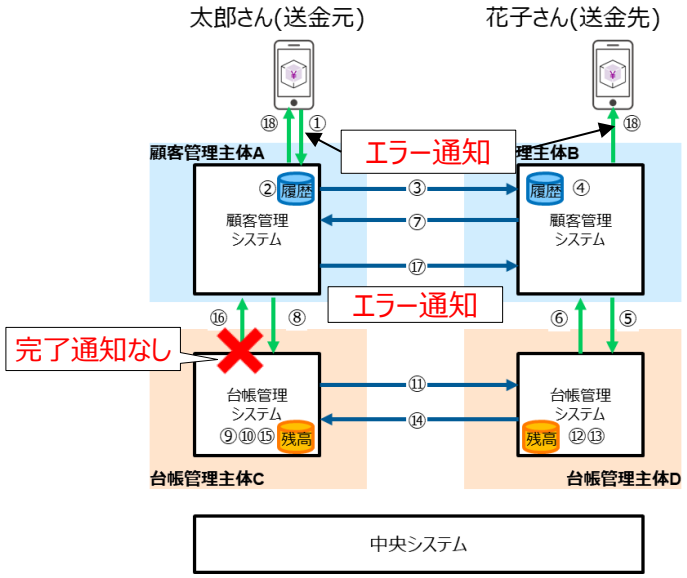


【課題】
決済完了後、結果を通知する前に障害が発生した場合に、どのように対処するか
【運用への影響】
- 仕向・被仕向ともに
- 現場で再実施した

しない

決済結果不定による利用者の二重支払いのリスク

【ケース②】台帳管理システムCの障害



【課題】
決済完了しているが、エラー通知が発生することにより、台
なる
決済されてい

タイムアウトエラーによるリカバリ処理及び処理中の送金先残高利用のリスク

4.2. 送金先通知後に端末発で残高を利用可能化する

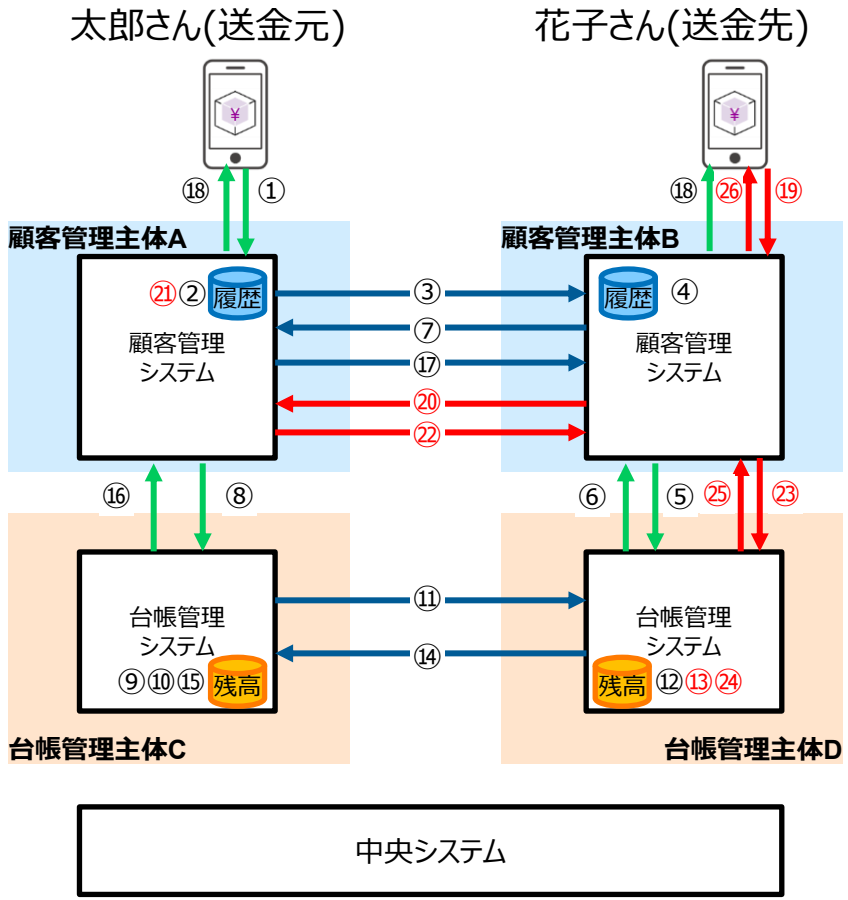
【WG7】第6回会合 弊社資料
「民間決済ネットワークにおけるエラー制御を踏まえたCBDCシステムへの示唆について」より

送金先台帳を留保付で増額記帳し、通知受信後、送金元の通知完了を確認の上、

対策の一つとして増額留保による二段階処理を議論

題材とするユースケース例

送金元アプリで「振込」を行い
「送金元への応答」と「送金先への通知」で相互に目視確認



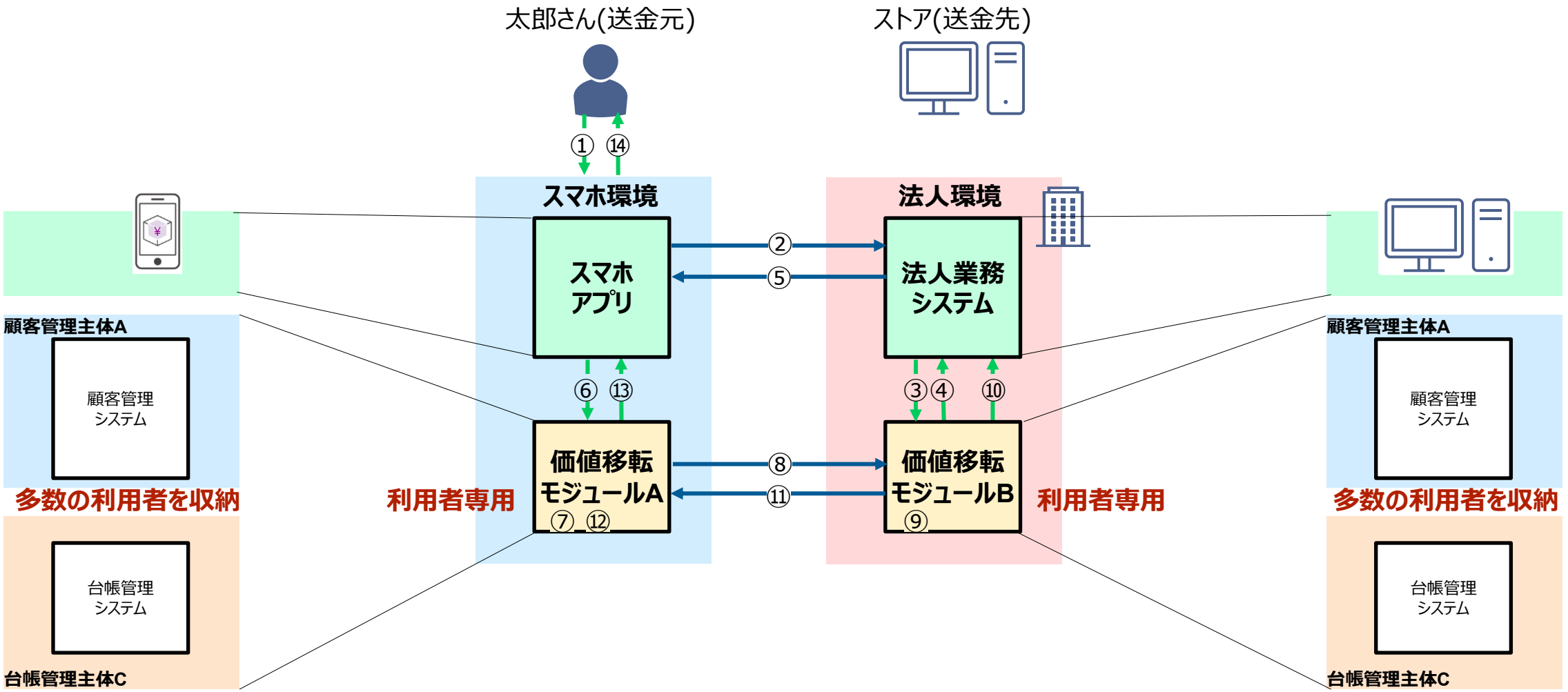
	行為者	処
		①～⑫の処理は
⑬	D	**花子の台帳を留保付で増額記帳**
⑭	D	Cに完了を通知
⑮	C	太郎の台帳の留保を取る
⑯	C	Aに完了通知
⑰	A	Bに完了通知
⑱	A、B	Aは太郎宛、Bは花子宛に取引の完了を通知
⑲	花子	完了通知受信後、Backgroundの自動処理でBに残高利用確認要求を指示
⑳	B	Aに完了通知確認要求を依頼
㉑	A	送金元に完了通知の送信を正常に完了していることを判定
㉒	A	Bに完了通知確認応答を返送
㉓	B	Dに利用可能許可要求を依頼
㉔	D	**花子の台帳の留保を取る（決済ファイナル）**
㉕	D	Cに利用可能許可完了応答を返送
㉖	B	花子宛に残高利用確認要求の完了を通知

＋増額留保

価値移転プロトコルにおける実験用システムとの対応関係

Beyond Finance®
みらいの社会のつくり手に

論理的には類似な構成ではあるものの、対応関係には以下のような異同があることに留意

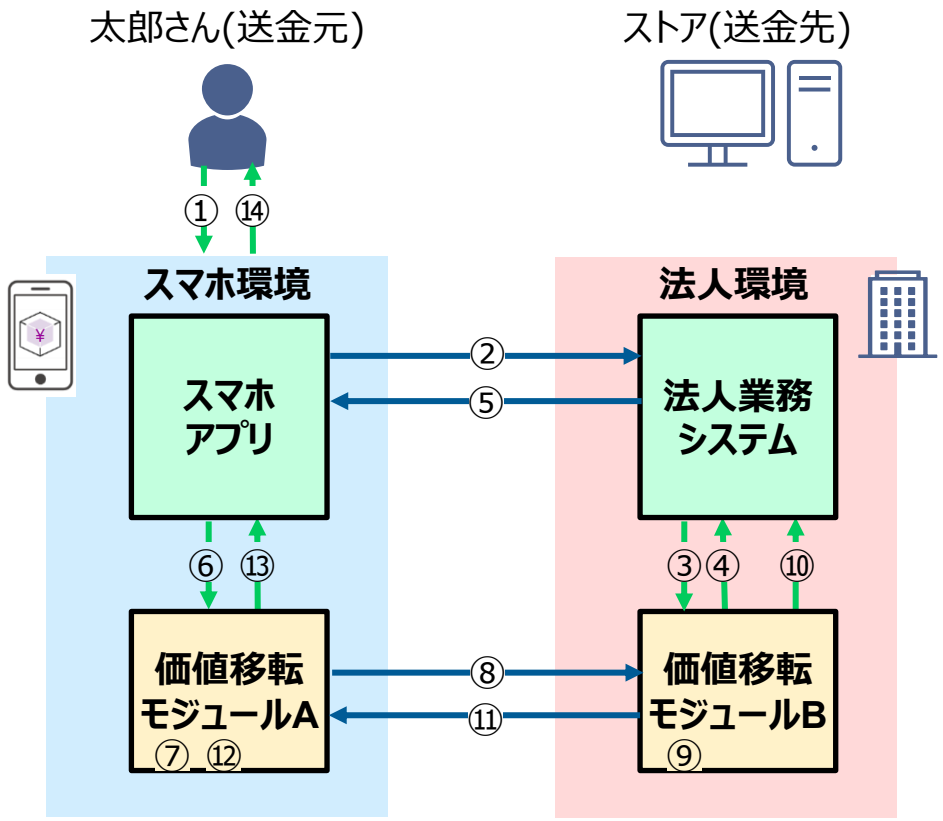


NTT DATA

減額留保だけの場合

Beyond Finance®
みらいの社会のつくり手に

減額留保だけが実装されている場合の処理フローは以下の通り



	主体	処理内容
①	太郎	スマホアプリに送金指示
②	スマホAP	送金情報を法人システムに連携
③	法人シス	送金情報を移転モジュールBに連携し取引IDを発行依頼
④	B	送金情報を確認し、取引IDを発行
⑤	法人シス	**取引ID、接続先情報等を連携**
⑥	スマホAP	送金情報、取引ID、接続先情報等をモジュールAに連携、移転指示
⑦	A	**移転対象トークンへの署名とロック**
⑧	A	モジュールBへトークン等移転
⑨	B	トークン受領処理（増額）
⑩	B	法人システムに受領通知
⑪	B	モジュールAへトークン受領通知
⑫	A	**移転対象トークンの削除（減額）**
⑬	A	スマホアプリに移転完了通知
⑭	スマホAP	太郎に送金完了表示

2重支払いの検知

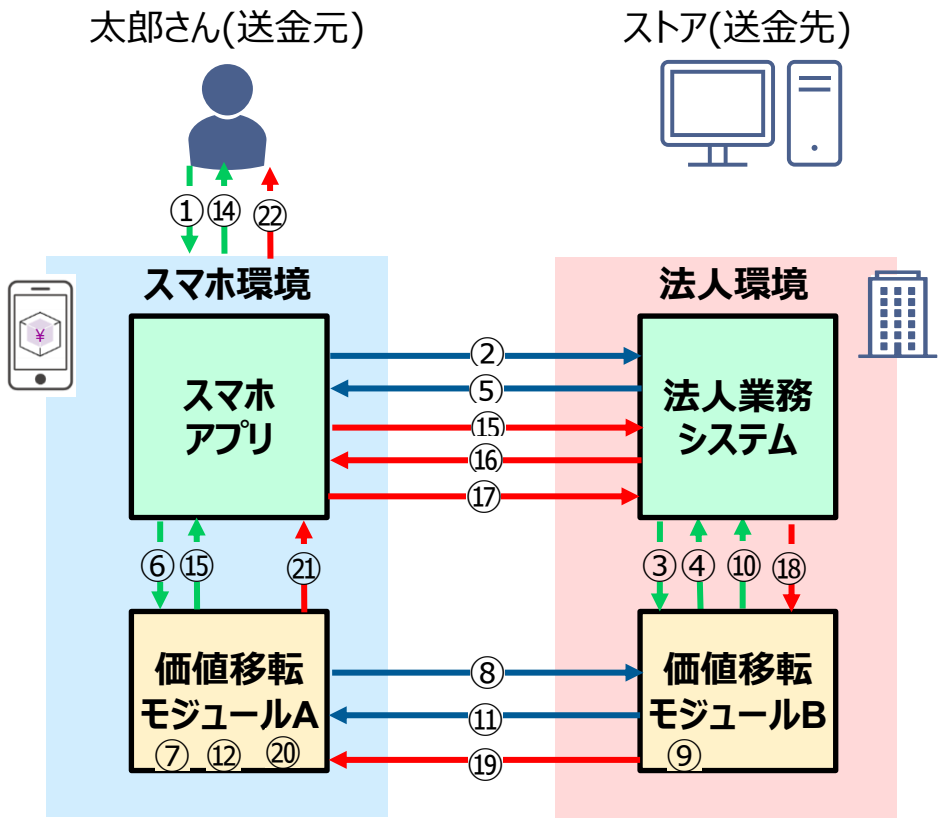
減額留保

NTT DATA

減額留保だけの場合

Beyond Finance®
みらいの社会のつくり手に

リカバリ対応のフローとタイムアウトエラー処理におけるリスクはWG7における議論と同様



	主体	処理内容
⑮	スマホAP	法人システムに取引ステータス確認要求
⑯	法人シス	スマホAPに取引ステータス（OK）を連携（NGの場合は別処理）
⑰	スマホAP	法人システムにトークン受領通知再送を要求
⑱	法人シス	モジュールBへトークン受領通知再送を要求
⑲	B	モジュールAにトークン受領通知再送
⑳	A	移転対象トークンの削除（減額）／既に削除済みの場合処理なし
㉑	A	スマホアプリに移転完了通知
㉒	スマホAP	太郎に送金完了表示

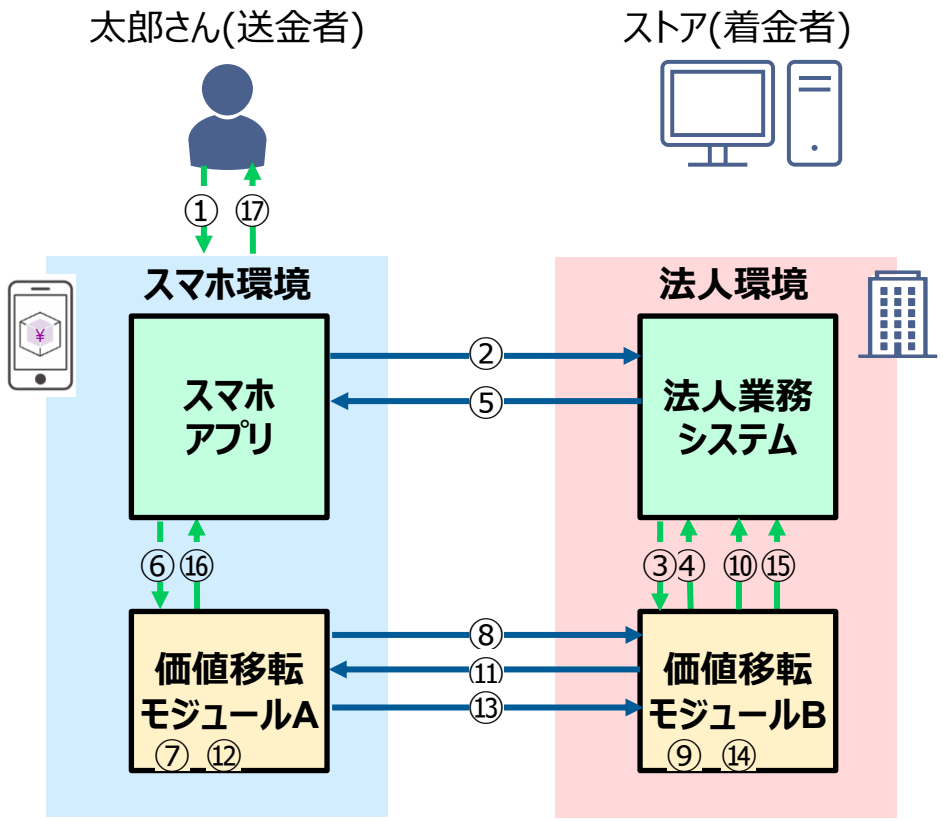
タイムアウトエラー処理中に法人システムの別プロセスが
当該トークンを使って支払いをしてしまうリスク

NTT DATA

増額留保も盛り込んだ場合

Beyond Finance®
みらいの社会のつくり手に

減額留保に加え増額留保も実装されている場合の処理フローは以下の通り



	主体	処理内容
①	太郎	スマホアプリに送金指示
②	スマホAP	送金情報を法人システムに連携
③	法人業務	送金情報を移転モジュールBに連携し取引IDを発行依頼
④	B	送金情報を確認し、取引IDを発行
⑤	法人業務	取引ID、接続先情報等を連携
⑥	スマホAP	送金情報、取引ID、接続先情報等をモジュールAに連携、移転指示
⑦	A	**移転対象トークンへの署名とロック**
⑧	A	モジュールBへトークン等移転
⑨	B	**留保付でトークン受領処理**
⑩	B	モジュールAへトークン受領通知
⑪	B	**法人システムに留保付受領通知**
⑫	A	**移転対象トークンの削除（減額）**
⑬	A	モジュールBへ減額完了通知
⑭	B	**増額トークンの留保解除**
⑮	B	法人業務へ受領完了通知
⑯	A	スマホアプリに移転完了通知
⑰	A	太郎に送金完了表示

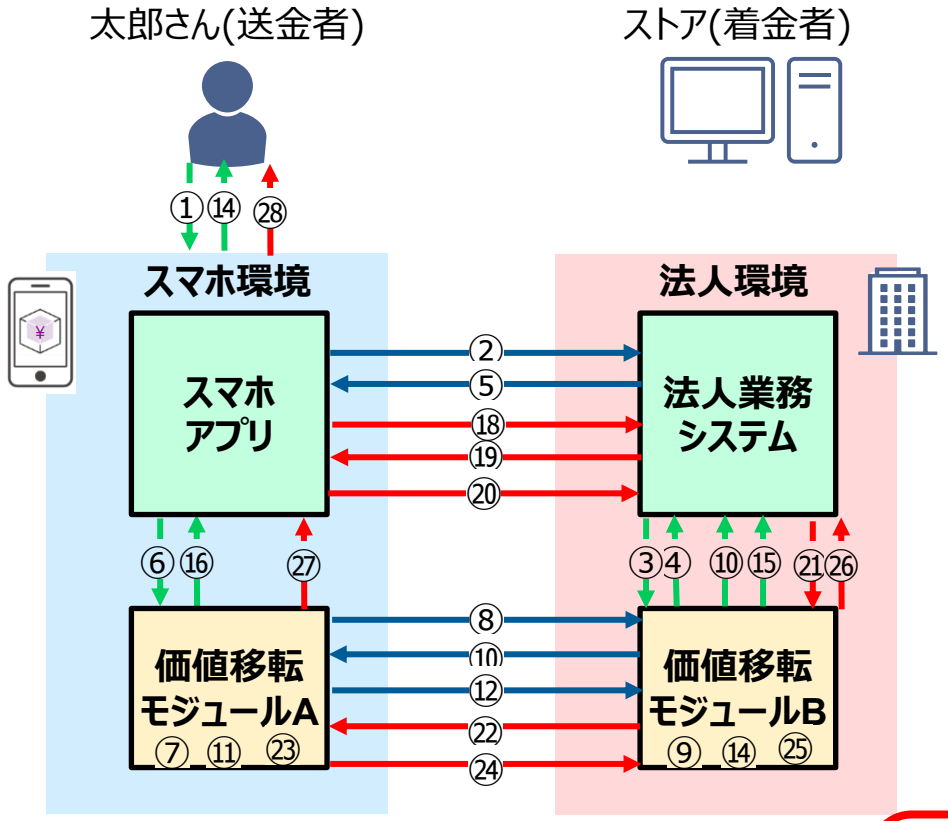
減額留保

増額留保

増額留保も盛り込んだ場合

Beyond Finance®
みらいの社会のつくり手に

増額留保があることでリカバリ中やタイムアウトエラー処理中に起こる送金先残高の利用防止には効果的と思量



	主体	処理内容
⑱	スマホAP	法人システムに取引ステータス確認要求
⑲	法人シス	スマホAPに取引ステータス（増額留保）を連携 **（NGの場合は別処理）**
⑳	スマホAP	法人システムにトークン受領通知再送を要求
㉑	法人シス	モジュールBへトークン受領通知再送を要求
㉒	B	モジュールAにトークン受領通知再送
㉓	A	移転対象トークンの削除（減額）／既に削除済みの場合処理なし
㉔	A	モジュールBへ減額完了通知
㉕	B	増額トークンの留保解除
㉖	B	法人業務へ受領完了通知
㉗	A	スマホアプリに移転完了通知
㉘	スマホAP	太郎に送金完了表示

増額留保でタイムアウトエラー処理中に二重支払いを防止。
タイムアウトにより増額留保トークンは削除、減額留保トークンは署名
復号により利用可能なトークンに復元

4.3. 2段階処理の副作用（3/3）

【WG7】第6回会合 弊社資料
「民間決済ネットワークにおけるエラー制御を踏まえたCBDCシステムへの示唆について」より

下記2点の副作用などが想定されるため、仲介機関ごとの個別最適化を超えて、NWシステムのようなハブを設けることが、CBDCシステム全体の安定性や運用効率の確保に寄与すると考えられる

1 通信・再送・例外処理・接続維持等の周辺的な負荷の増加

２段階処理で、さらにシステム間に跨る通信が増加するため、通信・再送・例外処理・接続維持等の監視など、仲介機関が担う、周辺的な負荷は増すと考えられる

価値移転プロトコルでは2段階処理による通信ストロークの増加、エラーハンドリングなどの処理は増加するものの、負荷は各利用者のデバイスやっステムに広く分散される

2 各システムのトラフィック量の増加

全体負荷を１万tpsと仮定した場合において、各システムの負荷は、1万tpsをベースとして、仲介機関の分散度合いに応じて、追加となり、トラフィック量も相応となり、安定性や運用効率を確保するための難易度は相対的に高くなると考えられる

最後に

Beyond Finance®
みらいの社会のつくり手に

価値移転プロトコルにおける決済システムの構成や考え方は従来のシステムの考え方と異なる部分が大きい一方で、
今回のディスカッションテーマのように同様の枠組みの中で対処方針を見出すことができるものもあると思量。
引き続きフォーラムでの議論を通じて選択肢としての磨き上げを行ってまいります。

NTT DATA

Beyond Finance®

みらいの社会のつくり手に