デジタルプラクティス　Vol.10 No.3(July 2019)

特集号招待論文

分散型台帳技術の応用に向けて ―中央銀行の決済システムからみた特徴と課題―

河田 雄次[1]　小早川 周司[2]

[1]（株）三菱総合研究所　[2]明治大学

本稿は，日本銀行が欧州中央銀行と共同で進めている分散型台帳技術の応用可能性に関する調査（プロジェクト・ステラ）の概要を取りまとめたものである．このプロジェクトでは，中央銀行が提供する決済サービスについて，分散型台帳技術を使って再現することができるかを中心に検討を行った．この結果，資金取引を1件ごとにただちに振り替える仕組み（即時グロス決済）のほか，取引の決済にあたって必要となる資金を効率的に利用する機能（流動性節約機能）や，資金と証券を同時に決済する機能を再現できることが確認された．一方，分散型台帳技術を巡っては，実務・技術面からみて，ガバナンスを取り巻く論点のほか，金融取引の秘匿性（プライバシー）の確保や，支払完了性（ファイナリティ）の扱いといった課題も残されている．今後は，民間金融機関やIT企業とも連携しながら，これらの課題の解決に向けた議論を深めていくことが望まれる．

1. はじめに：決済システムにおける中央銀行の役割☆1

本章では中央銀行決済サービスについてその概略を整理してみたい．

1.1　中央銀行の提供する決済サービスの概要

中央銀行は，国民に広く利用される銀行券と，民間金融機関が利用する中央銀行当座預金という2つの決済手段を提供している．我が国では，日本銀行が日本銀行券を発行するとともに，民間金融機関に対して日本銀行当座預金（日銀当預）を提供し，これを通じた資金決済が行われている．日本銀行では，日銀当預を通じた決済サービスが円滑かつ効率的に行われるよう，コンピュータによる処理を行うシステムを導入しており，これを「日本銀行金融ネットワークシステム」（日銀ネット）と呼んでいる．

資金決済における日銀ネットの役割を理解するため，銀行Aが短期金融市場において銀行Bに対してX億円の資金を貸し付けるような事例を想定してみよう（**図1**）．この場合，資金の貸し手である銀行Aが，自らの日銀当預から借り手である銀行Bの日銀当預に対して，X億円の振替指図を行い，日銀ネット内で資金が振り替えられて決済が完了する．日本銀行が提供する日銀当預を使うことによって，取引相手との決済を取消不可能かつ無条件に終了させることができる．これを「支払完了性」（ファイナリティ）と言う．

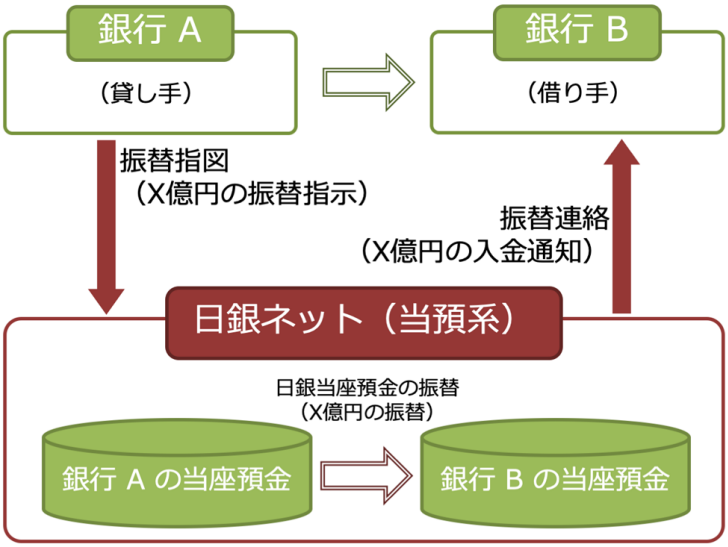

図1　我が国における資金決済の仕組み（1）―文献[1]を参考に作成

このほか日銀当預では，民間が提供する決済システムの最終的な決済や，金融機関同士が行う国債に関する決済サービスのための振替も行っている．個人が銀行口座を使って資金を振り替えるような事例として，銀行Aに預金口座を持つ支払人Xが，銀行Bに預金口座を持つ受取人Y宛てに振込を依頼するようなケースを考えてみよう（**図2**）．振込依頼を受けた銀行Aは，支払人Xが保有する預金口座から資金を引き落とした上で銀行Bにデータを送信し，これを受けた銀行Bは受取人Yが保有する預金口座に入金するという流れになる．ここで，支払人X，受取人Y，金額等に関するデータは全銀ネット（銀行間の内国為替取引をオンラインで処理する全銀システムの運営主体）で集中的に管理・計算され，各銀行の受払差額のデータが日銀ネットに送信される．この時点で銀行Aと銀行Bの債権・債務関係は，銀行Aと全銀ネットの債権・債務，全銀ネットと銀行Bの債権・債務に置き換えられる．これに基づいて日銀ネットでは，銀行Aの日銀当預から全銀ネットの日銀当預に資金が振り替えられるとともに，全銀ネットの日銀当預から銀行Bの日銀当預に資金が振り替えられて決済が完了する．

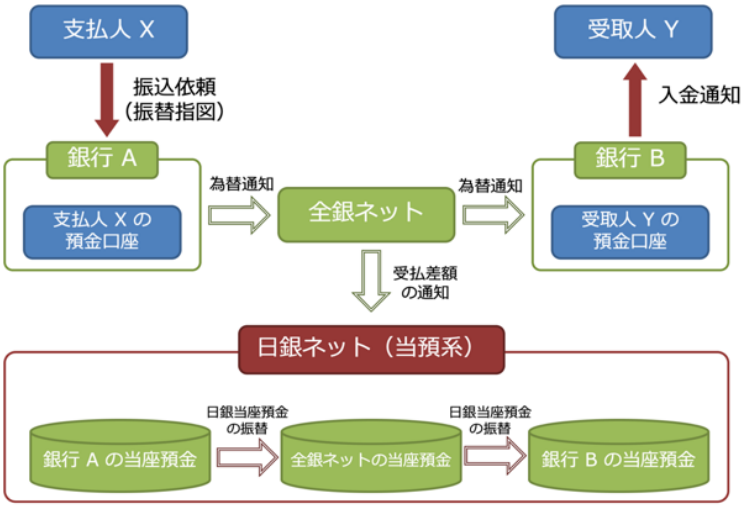

図2　我が国における資金決済の仕組み（2）―文献[1]を参考に作成

後述するように，日銀ネットではこうした取引を1件ごとにただちに行う仕組みである「即時グロス決済」（real-time gross settlement，RTGS）を採用している．これに対して全銀ネットでは，1件1億円以上の大口取引については日銀ネットへ送信し，同ネット上のRTGSで決済が行われる一方で，1件1億円未満の取引については，あらかじめ定められた一定の時刻まで振込依頼を溜めておき，その時点までの銀行ごとの総受取額と総支払額の差額（受払差額）をまとめて決済する「時点ネット決済方式」を採用している．これは，国際的なRTGS化の潮流への対応と従来の振込における利便性の両立を図ったものである．

海外でも，中央銀行が大型コンピュータを使って安全かつ効率的な決済手段を提供するケースが一般的である．たとえば欧州では，欧州中央銀行が域内の民間金融機関に対して当座預金を提供し，これを通じた金融機関同士の資金決済を行うシステムである「ターゲット２」（TARGET 2）や，域内の各国が発行する国債を決済するシステムである「ターゲット2セキュリティーズ」（T2-S）がある．

1.2　中央銀行決済サービスの特徴

このように各国の中央銀行は，民間金融機関の間で行われる取引（ホールセール取引）の決済に加え，家計や企業による銀行口座を通じた取引（リテール取引）の最終的な決済を担っている．これは中央銀行自らが決済システムという金融インフラを運営し，ファイナリティのある決済サービスを提供していることを意味する．こうしたサービスの提供にあたって各国では，決済システムの安全性と効率性の向上に向けて，さまざまな取り組みが講じられてきている．これらの主な特徴を日本銀行の施策に即してみると，以下のようになる．

第1に，日銀ネット上の資金決済および国債決済については，即時グロス決済（RTGS）化が図られていることが挙げられる．RTGS化が図られる前はあらかじめ定められた時点（9:00，13:00，15:00，17:00）を指定して振込依頼を行う時点ネット決済方式を採用していた．しかし，この方式の下では仮に1行でも決済不能に陥ると，その金融機関からの入金をあてにしていた他の金融機関が受払差額を計算し直す必要がある．場合によっては，この差額がプラス（受取超）からマイナス（支払超）に転化して決済不能に陥り，これが連鎖的に拡がり多くの金融機関

の決済が停止する恐れもある．こうした決済不能の連鎖（システミック・リスク）を削減するため，日銀ネットでは2001年から振替指図1件ごとに直ちに決済が行われるRTGS方式に移行している．

第2に，決済サービスのRTGS化に伴って，流動性節約機能が提供されていることである．金融機関はRTGS化によって，振替指図の実行の都度，必要な手許流動性（資金）を準備する必要がある．時には大口の資金の振り替えのため，多額の流動性を手当てしなければならないこともある．しかし流動性節約機能を導入することによって，これらの金融機関ができるだけ効率的に流動性を利用できるような環境が整備されるようになった．ここで，日銀ネットの流動性節約機能についてやや詳しくみてみよう（**図3**）．

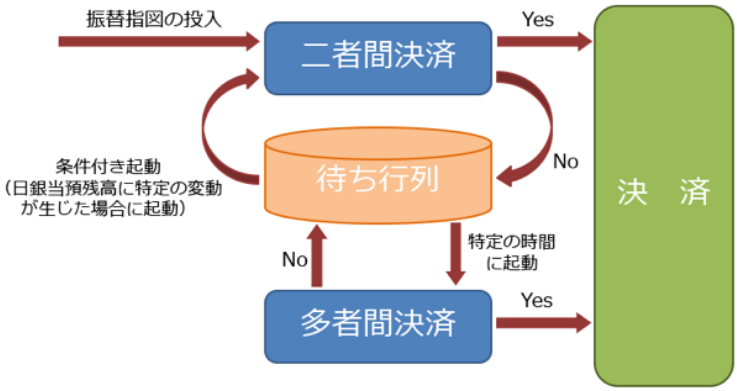

図3　日銀ネットの流動性節約機能―文献[2]を参考に作成

この機能は「待ち行列機能」と「複数指図同時決済機能」によって構成される．このうち前者は，従来，各金融機関の日銀当預が不足していた場合，日銀ネット内で拒絶・返戻されていた振替指図を，日銀ネット内に設けた金融機関毎の待ち行列に待機させる機能のことである．また後者は，二者間での複数指図を同時に決済する機能と多者間での複数指図を同時に決済する機能に分けられるが，具体的には，ある金融機関向けの振替指図が投入されると，日銀ネットがこの金融機関の待ち行列で待機している振替指図を検索して，その中から二者間あるいは多者間で同時に決済できる振替指図の組合せを抽出し，その都度，これらの指図を同時に決済するような機能のことである．

二者間同時決済の仕組みを具体例でみてみよう（**図4**）．図4上図をみると，銀行Bから銀行Aに対して20の振替指図が想定されている．流動性節約機能の導入以前は，銀行Bの日銀当預残高不足（当預残高は0）により，この振替指図は拒絶される扱いとなっていた．しかし，待ち行列機能の導入によって，この振替指図を銀行Bの待ち行列に待機させることが可能となり，その後，銀行Aから銀行Bへの振替指図30が投入されるタイミング（図4下図）で，この指図と銀行Bの待ち行列に待機していた振替指図を同時に決済する―すなわち，これらの振替指図の受払差額（銀行Aから銀行Bへの振替10）のみを振り替える―ことができるようになった．この結果，銀行Aは，従来の枠組みでは30の資金をあらかじめ準備するか，あるいは銀行Bからの入金を待ってから振替指図を行う（この場合，多くの日銀ネット参加者が取引相手からの資金振替がないと自身の資金振替が行えない状態である「すくみ」が起きる可能性がある）かのいずれかの選択肢を取る必要があったが，流動性節約機能を使うと10の資金で決済を進捗させることができるよう

になる．また銀行Bにとっても，従来の枠組みでは20の資金を準備するか，あるいは銀行Aからの入金を待ってから振替指図を行うかの選択肢が考えられるが，流動性節約機能を使うことによって新たな資金を手当てせずに済む．いずれの銀行にとっても，流動性必要額の節約につながると考えられる．

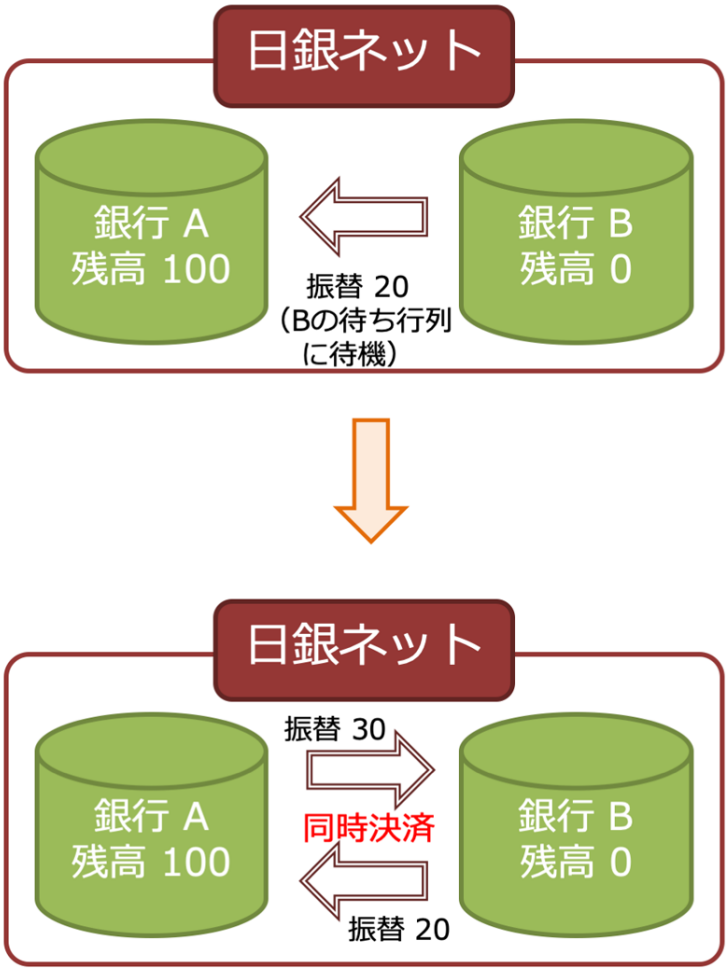

図4　流動性節約機能の具体例―文献[1]を参考に作成

第3に，国債決済については，証券の受け渡しと代金の受け渡しを相互に条件付けることによって，一方の受け渡しが行われない限り，他方の受け渡しも行われないような仕組みが導入されていることである．これを，「証券資金同時受渡」（delivery versus payment，以下DVP）と呼ぶ．こうした仕組みによって，国債を相手方に渡したにも拘わらずその対価である資金を受け取ることができない（あるいは，資金を払い込んだにも拘わらず国債を受け取ることができない）といった「取りはぐれ」のリスクを回避することができる（**図5**）．

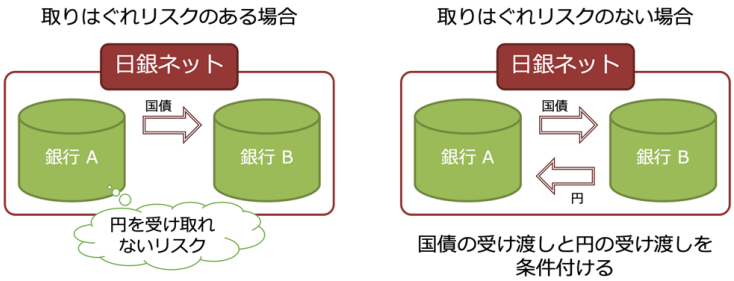

図5　国債決済と取りはぐれリスク

1.3　中央銀行決済サービスのさらなる向上に向けた取り組み

各国では，情報通信技術の発展に伴い，中央銀行自らの決済サービスがこれらの技術を活用することによって，金融インフラの安全性と効率性の向上に寄与するかを不断に点検している．2009年に登場したビットコインを支える分散型台帳技術（distributed ledger technology）についても，中長期的な観点から，中央銀行が管理・運営する決済システムへの応用可能性を調査する必要性が高まっていた．こうした経緯を受けて，日本銀行は欧州中央銀行との間で，2016年12月から分散型台帳技術に関する共同調査（「プロジェクト・ステラ」，以下「ステラ」）に取り組んでいる（文献[2],[3]）．

現時点では，日本銀行や欧州中央銀行の決済システムに克服すべき課題があり，これを解決するために分散型台帳技術を利用するといった問題設定にはなっていない．プロジェクトは分散型台帳技術への理解深耕を目的としており，今後の検討過程で仮にこれまで認識されてこなかった課題が見つかれば，この技術の活用によって，果たしてこうした課題を改善することができるかを確認するというアプローチで進められている．

なお，ステラは複数の中央銀行が協力しながら，金融インフラへの分散型台帳技術の応用可能性を検討する世界初の取り組みである．現在，このような協力関係を通じて分散型台帳技術への知見を深めようとする取り組みが世界的な拡がりをみせている．具体的には，カナダ中銀とシンガポール通貨庁およびイングランド銀行による取り組みのほか，香港金融管理局とシンガポール通貨庁，ブラジル中銀と香港金融管理局による共同プロジェクトが挙げられる．これらの取り組みもステラと同様，各国の中央銀行が管理・運営する金融インフラの課題を克服するために分散型台帳技術の応用を試みるというよりは，まずはこの技術を使ってみることを主眼として立ち上げられたものである．

2.　分散型台帳技術に関する欧州中央銀行との共同調査の概要

金融インフラは一国の経済の根幹をなし，さまざまな経済活動を支える重要な基盤と位置付けられる．これらのインフラが万が一にも円滑に機能しないような場合には，その影響が経済活動全般に及ぶ．従って，中央銀行にとって，金融インフラの安全性がしっかりと確保され，その下で，さまざまな金融取引が安全かつ効率的に行われることは，経済の安定およびその発展にとって重要な前提条件になる．ステラでは，このような観点から分散型台帳技術が金融インフラの安全性と効率性の向上につながるかを検証している．

もっとも，一口に，金融インフラの安全性・効率性と言っても，その意味は多岐にわたる．たとえば，効率性は振替指図の処理速度や一定の時間内に処理可能な件数の多寡などシステムのパフォーマンスのほか，取引処理に必要な流動性の削減やカウンターパーティーリスクの削減，さらには分散型台帳技術の導入に伴うインフラ運営面のコスト削減も，効率性の評価にあたっては重要な論点となる．また，安全性についてみると，障害への耐性が大きな論点と位置付けられる一方で，具体的な「障害」の中身については，サイバー攻撃からシステムダウンまでさまざまなシナリオを想定することができる．これらの論点を網羅的に検討するには時間を要することから，今次プロジェクトでは，分散型台帳技術を定量的に評価することを念頭に置きながら，いくつかの評価軸に焦点を絞って，検討を進めることとした．以下では，プロジェクトの第1期で扱った流動性節約機能の実現と，第2期で扱ったDVP決済の実現を中心に，主な結論を取りまとめることとしたい．

2.1　分散型台帳技術の概要

まず，分散型台帳技術について触れると，文献により区々の定義がなされているものの，概していえば「ネットワーク参加者が何らかのコンセンサス形成メカニズムを通じて台帳を更新することを可能にする技術」（文献[2]）と表現できる．特にビットコインなどの技術の根幹には，信頼できる第三者を置くことなく，互いに信頼関係のない者同士による取引を安全に行うための枠組みを提供するという考え方がある．

また，取引処理の内容は「スマートコントラクト」として実装される．一般に，スマートコントラクトとは，契約内容をプログラムとして記述し，契約の当事者双方の署名を付して分散型台帳に登録することによって，契約が締結されたとみなし，一定の条件が満たされると契約内容が自動的に執行されるものを指す．一定の条件をトリガーとして，プログラムが自動的に執行されることから，契約内容が履行されているかを確認するといったコストをかける必要がない．さらに，プログラムが分散型台帳上にいったん登録されると，契約当事者双方がそのアルゴリズムや執行内容を確認することが可能であり，適切に実装された場合には契約当事者であってもその内容を恣意的に改ざんできないという特徴がある．こうした透明性や改ざん耐性は，スマートコントクトさらには分散型台帳技術の重要な特徴の1つである．

分散型台帳技術はP2P分散システムであり，コンセンサス形成メカニズムも加わるため，日銀ネットなどのような中央集中型システムに比べ，処理速度や処理件数などのパフォーマンスは悪化することが予想されるが，実際にどの程度の悪化で済むのかという点は注目を集めるところであった．また，流動性節約機能のように流動性を一カ所に集約して処理する機能を実現できるのか，日本銀行のような第三者がいない下で取引当事者である金融機関だけでどのようにDVP決済を実現するのかなども多くの中央銀行関係者が注目していた点であった．

プロジェクトの第1期（流動性節約機能の実現），第2期（DVP決済の実現）ともに，ネットワークに参加するノードを金融機関と見立てて実験を行ったが，分散型台帳技術を用いた処理基盤（分散型台帳基盤）としては，第1期ではHyperledger Fabric，第2期ではCorda，Elements，Hyperledger Fabricを用いた．アーキテクチャやコンセンサスアルゴリズム，スマートコントラクトの実装方法などは基盤ごとに相当程度異なるため，詳細については文献[2]および[3]を参照されたい．

2.2　流動性節約機能の実現

プロジェクトの第1期で扱った流動性節約機能を巡っては，そのアルゴリズムを「スマートコントラクト」としてどのように実装できるか，分散型台帳技術を用いることによって安全かつ効率的に処理を実行することができるかを確認することに主眼を置いた．

ステラでは，日銀ネットに参加する金融機関等が流動性節約機能のアルゴリズムについてすでに同意し，それが分散型台帳上に登録されているとみなした上で検討を進めた．具体的には，日銀ネットが流動性節約機能として提供する待ち行列機能と二者間同時決済機能の仕組みをスマートコントラクトとして再現できるかを中心に検討を行った．流動性節約機能の実行にあたっては，対象となる日銀当預の残高や待ち行列を集中的に把握する必要があるため，これを分散環境下で効率的に実現できるかは多くの中央銀行にとって関心のあるテーマであった．このため，ステラを嚆矢として，海外の中央銀行でも流動性節約機能を巡る実証実験が数多く進められた．代表的な取り組み事例としては，カナダ中銀のプロジェクト・ジャスパー（文献[4]）やシンガポール通貨庁のプロジェクト・ウービン（文献[5]）などが挙げられる．

ここで日銀ネットの流動性節約機能について，スマートコントラクトでそのアルゴリズムを実装することを念頭に置いて，より詳しくみると以下のようになる．たとえば，銀行Aから銀行Bに対して振込を行う場合，①銀行Aの振込依頼は，銀行Bの待ち行列を検索し，銀行Bから銀行A宛ての振込依頼が待機しているかを確認する，②こうした振込依頼が待機している場合には，両方（銀行Aから銀行B宛ての振込依頼と，銀行Bから銀行A宛ての振込依頼）を同時に決済できるかを確認する，③残高不足等で同時に決済できない場合には，銀行Aから銀行Bへの振込依頼を単独で即時に決済できるかを確認する，④即時に決済できない場合には，その振込依頼を銀行Aの待ち行列に待機させる，という形で行われる．こうした二者間同時決済は，日銀ネット参加者の日銀当預残高が増加した場合のほか，待ち行列の最上位で待機している振替指図に変更が生じた場合（たとえば，参加者が自分の待ち行列を管理する中で，振替指図の順番や優先順位を変更するなど）に，自動的に発動される仕組みとなっている（**図6**）．

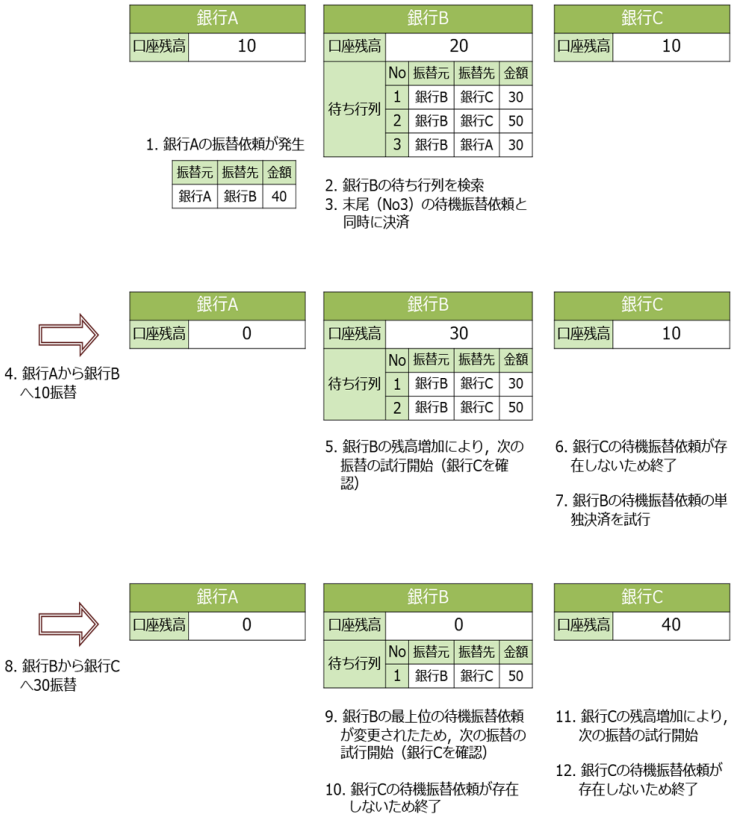

図6　流動性節約機能のイメージ―文献[2]を参考に作成

このようなアルゴリズムはスマートコントラクトとの親和性も高く，ステラにおいて，分散型台帳技術を使って再現できたことは大きな成果であった．その上で，効率性と安全性の評価を行ったが，前述のとおり，それぞれの評価軸を特定し，効率性については処理スピードを，安全性については耐障害性に焦点を当てて，検証作業を進めた．

2.2.1　効率性の評価

まず，効率性の面では，処理に要する時間（レイテンシ）を計測することによって，パフォーマンスを評価した．レイテンシは，分散型台帳が一定時間あたりに処理しなければならない振替指図の件数―トラフィック量（秒間振替指図件数＜request per second，以下RPS＞）―に依存する．中央銀行が運営する資金決済システムでは，振替指図1件ごとの金額は大きいもののトラフィック量自体はさほど大きくない（RPSが約10～70件に止まる）ことから，当初より，トラフィックの多寡がレイテンシに大きな影響を及ぼすとは考えられていなかった．むしろ，現行の資金決済システムが即時決済を実現する下で，分散型台帳技術を使って，どこまで「即時」に近づくことができるかに関心があった．

実験は，分散型台帳基盤であるHyperledger Fabric v0.6.1（コンセンサスアルゴリズムはPractical Byzantine Fault Tolerance）を用いて，検証ノード1台につきメモリ7.5GB，ディスク容量8GBのUbuntu（16.04.1 LTS 64bit）を割り当て，実際の取引明細にもとづく仮想データ（口座数は約200，取引件数は約38,000件／時）を用いて行った．RPSは，実際のトラフィック量に応じた値を用いたほか，最大250件／秒の場合も用いた．処理時間の計測にあたっては，ある取引指図が送信された時刻から当該取引指図の処理結果が台帳上に記録された時刻まで

の時間を個別に記録し，すべてのノードないしコンセンサス形成に必要な数のノード（今回の場合は総ノード数の約2／3）におけるすべての取引指図を対象とした統計量として算出した（**図7**）．

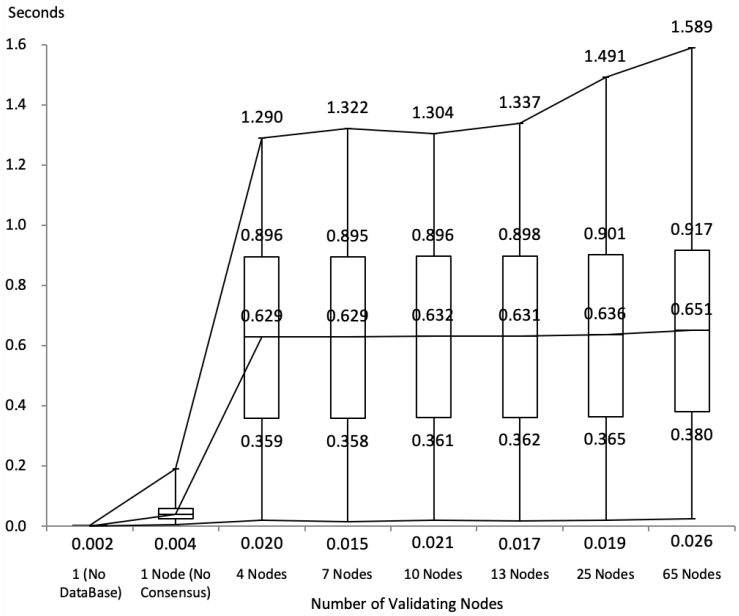

図7　処理時間の計測結果―文献[2]より（横軸は検証ノード台数，縦軸は処理時間（秒）であり，グラフの値は下から最小値，25%点，中央値，75%点，最大値を示す）

計測結果をみると，分散型台帳技術を使ってもレイテンシは，平均して1秒を下回る水準に抑えられ，RTGSシステムとほぼ同等のパフォーマンスを示し得るとの結論を得ることができた．

このほか，レイテンシに影響を及ぼすさまざまな要因として，特に分散型台帳技術では，取引内容を検証する参加者（検証ノード）の参加形態を中心に検証作業を行った．具体的には，ノード数の多寡やノード間の物理的距離によって，レイテンシがどの程度拡大するかを計測した．計測結果をみると，検証ノードが増えれば増えるほどレイテンシが拡大するという傾向が確認されたものの，中央値でみる限り，パフォーマンスへの影響は比較的限定されており，1秒を下回る水準を維持し得たことが分かった（図7）．もっとも，一部の振替指図については処理時間が1.5秒を超えたため，今後，こうした処理時間の遅延をどのように克服していくかが課題として認識された．

また，検証ノードの物理的距離の影響をみると，コンセンサス形成に必要な数のノードが近接しているような場合はパフォーマンスに大きな変化はみられなかったものの，ノードが離散しているような状況では処理時間への影響が大きくなることが確認された（**図8**）．今後，分散型台帳技術を使って，クロスボーダー取引の検証作業を行うような場合には，参加者のロケーションや参加者が集中・離散しているかといったネットワークの形状が，パフォーマンス面で影響を及ぼす可能性があることを示唆するものと言えよう．

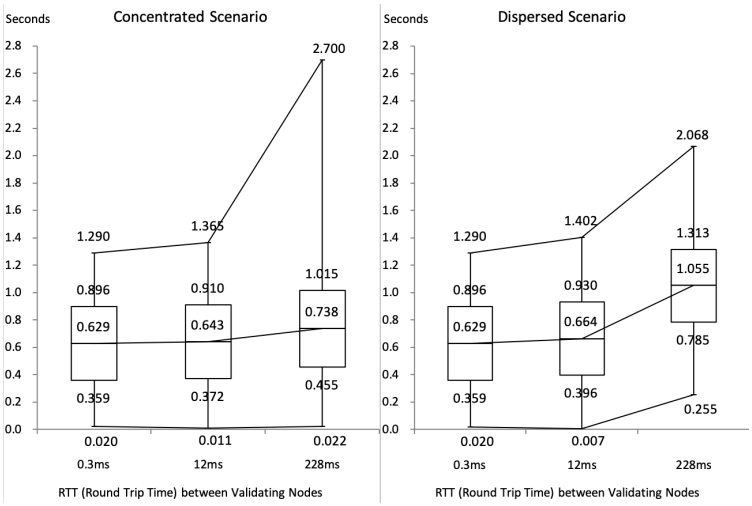

図8　検証ノードの物理的距離の影響にかかる計測結果―文献[2]より（左は検証ノードが集中している場合，右は分散している場合の結果である．左右いずれのグラフも，横軸は検証ノード間の往復遅延時間（ミリ秒），縦軸は処理時間（秒）であり，グラフの値は下から最小値，25%点，中央値，75%点，最大値を示す）

2.2.2　安全性の評価

次に，安全性については，障害耐性を検証する上でのシナリオとして，①一部の検証ノードにおいて障害が発生するような場合，②参加者が誤ったフォーマットの振替指図を送信したような場合を想定し，これらのシナリオの下で，分散型台帳システムが全体として稼働し続けることができるかを検討した．

結論としては，いずれのシナリオの下でも，分散型台帳技術のネットワークは機能を維持し得ることを確認できた．このうち，検証ノードにおける障害発生については，コンセンサスの形成に必要な数のノードが正常に機能している限りにおいては，システム全体として運行を継続することができることが確認できた（**図9**）．これは，分散型台帳技術の最も重要な特徴の1つであり，たとえば，自然災害や人為的なミス等によって，システムの一部が機能しなくなったとしても，他の参加者が台帳を管理し，検証作業を継続することができれば，システム全体としては，運行が続けられることを示唆するものである．

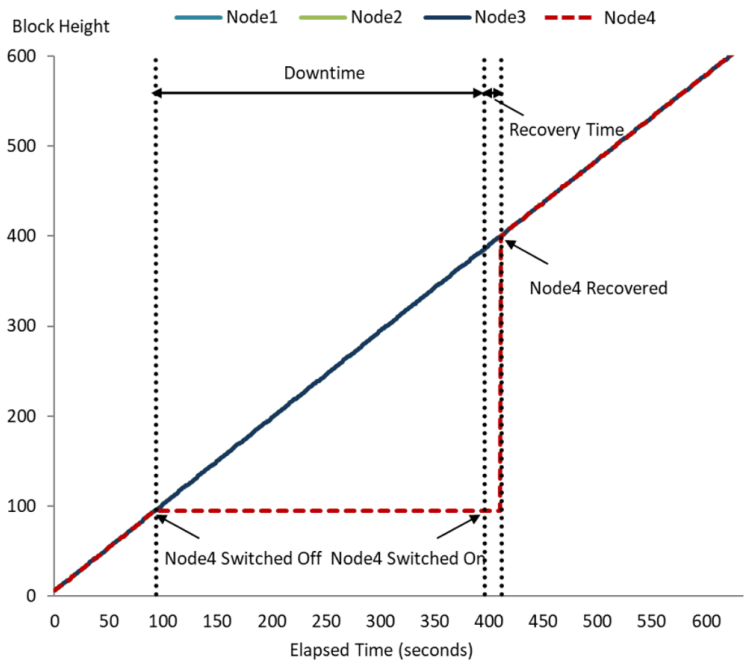

図9　検証ノード障害時のブロックデータの計測結果―文献[2]より（横軸は経過時間（秒），縦軸はブロック高（累積ブロック数）を示す）

さらに，誤ったフォーマットの振替指図が送信された場合についてみると，検証作業の開始に先立って，システムが振替指図のフォーマットを確認し，システム全体としては処理時間が遅れることなく，こうした指図を除外した上で，残りの振替指図を問題なく処理できることが確認された（**図10**）．

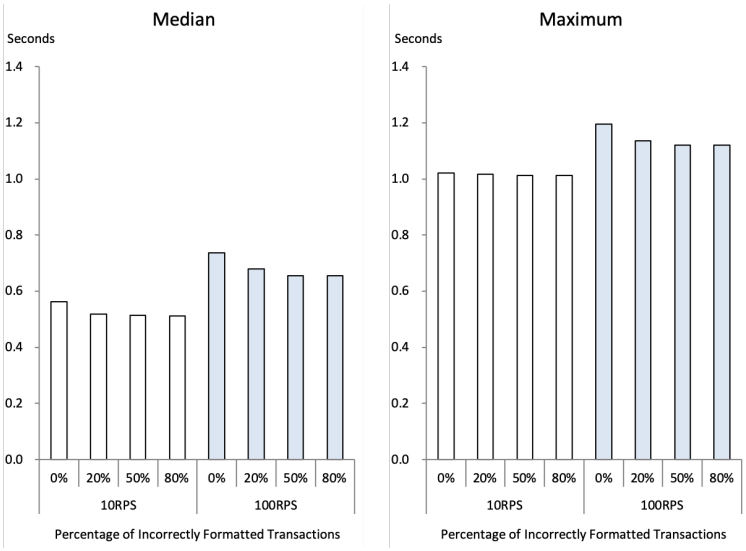

図10 誤ったフォーマットの振替指図が与える影響の計測結果―文献[2]より（左は処理時間の中央値，右は処理時間の最大値の結果であり，左右いずれのグラフも，横軸は不正指図の占める割合（%），縦軸は処理時間（秒）を示す）

2.3　証券資金同時受渡（DVP）決済の実現

次に，DVP決済の分散型台帳技術を用いた実現について述べる．このプロジェクトでは，「信頼できる第三者」がいない下での証券資金のDVP決済をどのように実現するかという点に主眼を置いて分析を行った．なお，ステラと同様に，分散型台帳技術を用いてDVP決済の実現を図った海外中央銀行の取り組みとしては，カナダ中銀（文献[6]）やシンガポール通貨庁（文献[7]）などが挙げられる．

日銀ネットでは，日本銀行という信頼できる第三者が仲介することによって，DVP決済を実現するが，こうした第三者を置かずにDVP決済を履行するのは，既存の枠組みにはないアプローチである．この点についてやや詳しく述べると，日本国債と資金のDVP決済にあたっては，日本銀行がシステム運営主体として，①資金の支払人および証券の引渡人から，決済に必要な資金と証券のそれぞれを確保した時点で受取人の口座に移管する，②万が一，資金・証券の両方あるいはいずれかを確保できない場合には，資金・証券の両方を元の口座（資金については支払人の口座，証券については引渡人の口座）に戻すという操作を行っている（**図11**）．このような枠組みでは，日本銀行という信頼できる中立的第三者が同時受渡を実現する上で重要な役割を演じているが，分散型台帳技術の下では，こうした第三者（システム運営主体）に依存することなく，DVP決済を行うことができるかがポイントとなる．

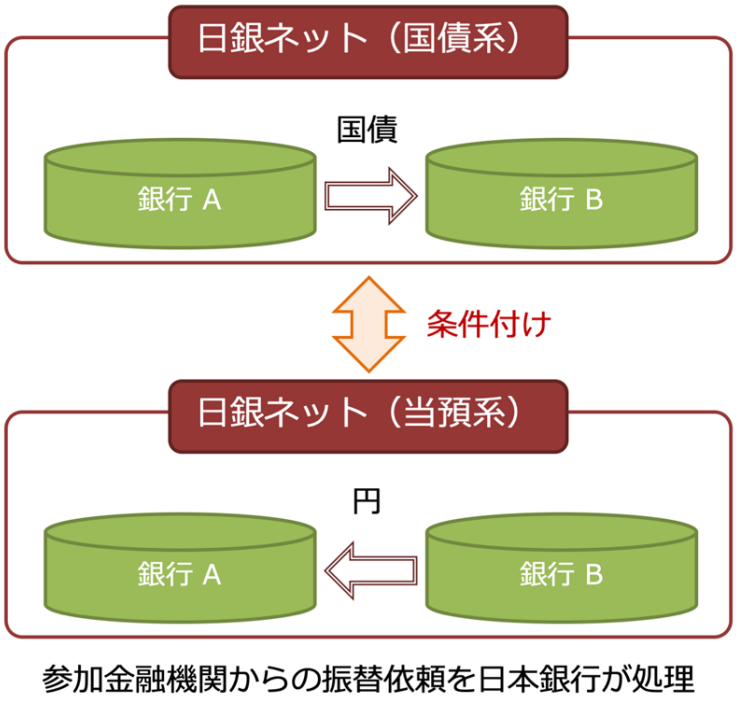

図11　日本国債と円のDVP決済のイメージ

2.3.1　「アトミック性」にもとづくDVP決済の実現

今次プロジェクトでは，コンピュータ・サイエンスで使われている「アトミック性」（atomicity）という考え方を援用して，DVP決済を実現できるかを検証した．すなわち，取引の「アトミックな」処理とは，取引自体を分割・細分化して処理することができず（細分化できない最小単位の処理という意味でアトミックという特徴を持つと考えられている），すべての処理を一括して実行するか，あるいはまったく実行しないかの二者択一しかない処理を指すものである．こうしたアトミック性という特徴を持った取引処理は，DVP決済の基本的な考え方と類似していることから，こうした視点から，信頼できるシステム管理者という主体がいない中でのDVP決済を検証することとした．

具体的には，資金と証券という複数の金融資産を同一のネットワーク上の台帳で管理する「単一台帳方式」と，資金と証券を別々のネットワーク上の台帳で管理する「複数台帳方式」について検証作業を行った（**図12**）．このうち前者は，資金と証券の振替が1つの取引として処理されるものであり，現行の証券決済システムに類似したやり方である．また，後者は，資金と証券を別々のネットワーク上の台帳で管理するため，資金と証券の振替を紐付けるための仕組みをどのようにして備えるかによって，さらにいくつかの方式に細分化される．今次プロジェクトでは，これらの台帳を管理するネットワーク間の接続がない場合（図12の右端）でもアトミックな資産の受け渡しを可能とする手法―これを「アトミック・クロスチェーン・スワップ」（atomic cross-chain swap）と呼ぶ―を使って，DVP決済がどのように実現できるか，そして既存のやり方に比べてどのような変化を生じさせるかを中心に検討を進めた．

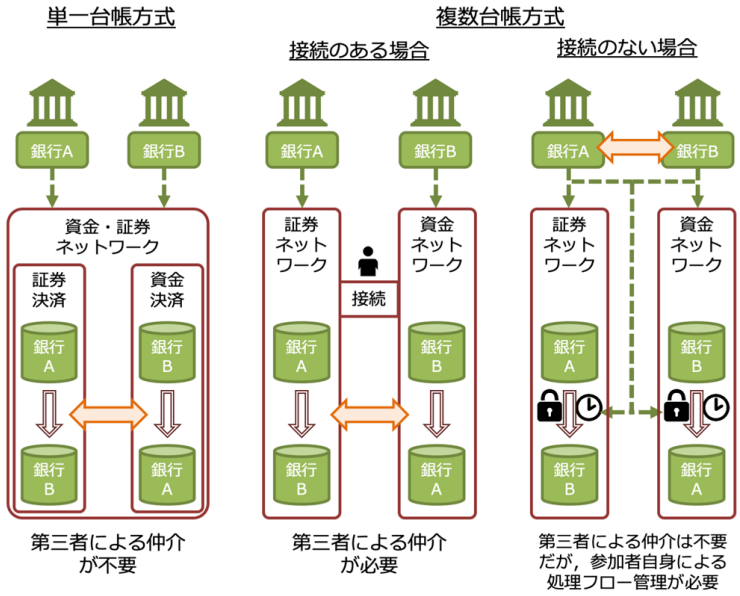

図12　DLT環境下でのDVP決済の実現方法―文献[3]を参考に作成

アトミック・クロスチェーン・スワップにおいて重要なのは，複数の異なる資産のアトミックな受け渡しを実現する技術である「ハッシュ・タイムロック・コントラクト」（Hashed Timelock Contracts，以下HTLC）である．HTLCについて具体的に説明すると，①銀行Aが生成した乱数（シークレット）のハッシュ値を用いて受渡対象となる資産（たとえば，証券）をブロックする，②銀行Bは銀行Aの生成したハッシュ値を用いて受渡対象となる資産（たとえば，資金）をブロックする，③双方の資産がブロックされた後，銀行Aはシークレットを用いて受取予定となっている資産（たとえば，資金）のブロックを解除し，それと同時に，銀行Bに対してシークレットが開示される，④銀行Bは，このシークレットを用いて受取予定となっている資産（たとえば，証券）のブロックを解除するという仕組みを通じて，資産の受け渡しを実現する．ここで一方向ハッシュ関数を用いる限り，合理的な想定に基づけば，ハッシュ値から元の値を得ることは不可能であるため，シークレットがない限りブロックの解除は行えない．さらに，このコントラクトには，タイムアウト機能が付されており，事前に定めた時間内に必要な処理が完了しなかった場合には，資産は元の所有者に返還される仕組みになっている（**図13**）．

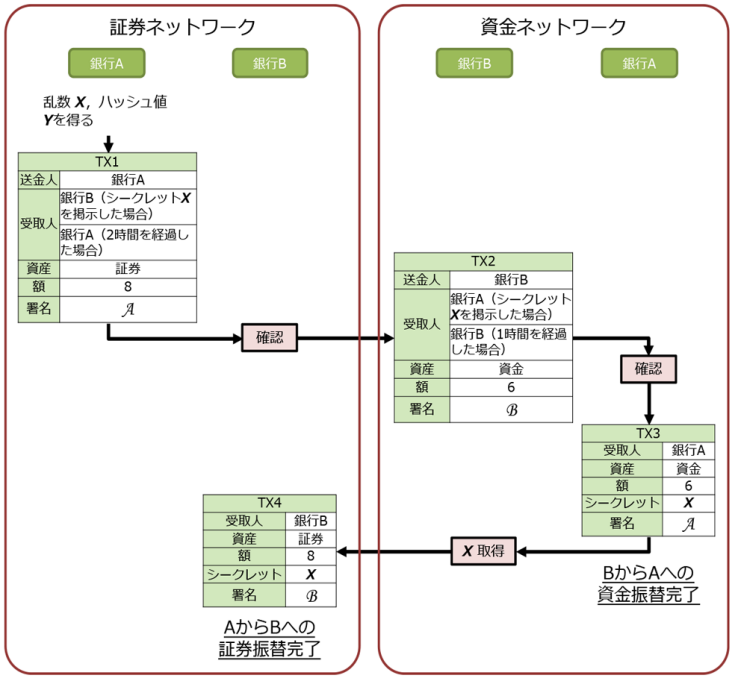

図13　アトミック・クロスチェーン・スワップのイメージ―文献[3]を参考に作成

以上のような仕組みを使うことによって，中央銀行といった信頼できる第三者に依存することなく，かつ台帳を管理するネットワークの間で一切の接続がないような場合でも，これらのネットワークを跨いで複数の資産の受け渡しを行うことができることが確認された．ここで実験は，分散型台帳基盤であるCorda release-V2，Elements v2.14.1.1，Fabric v1.1.0-alpha を用いて，ノード1台につきメモリ7.5GB，ディスク容量8GBのUbuntu（16.04.1 LTS 64bit）を割り当てて行ったが，1取引あたり数秒程度の処理時間であった．

第三者に依存することなく，異なるネットワーク間で一切の接続がなくとも，それぞれの資産を条件づけて交換を可能とする仕組みは，金融インフラの柔軟性や頑健性を高める上できわめて興味深いものと考えられる．

ただし，分散型台帳技術は未だ成熟途上であり，現時点ではいくつかの課題が挙げられる．その中でも最も大きな課題は，特定の場合においてアトミック性が成り立たないという点であろう．すなわち，図13において銀行AによりTX3が送信された後，障害等の何らかの理由で銀行BがTX4を送信しない場合は，タイムアウト時間が経過した後には銀行Aは（すでに得ている資金に加え）証券も払い戻すことが可能となる．こうしたリスクに対処する方法として，タイムアウト時間を長く設定することや他の参加者にTX4の送信を依頼するなどの運用面での対応が挙げられているが，現状では，取引当事者が各プロセスのタイミングを管理することが前提となっている．この点は，現状のアトミック・クロスチェーン・スワップの問題点を浮き彫りにするものであり，さらなる改良が求められると言えよう．

3. 分散型台帳技術の特徴と中央銀行システムへの応用にあたっての課題

分散型台帳技術の応用可能性を巡っては，この技術がより安全，迅速かつ安価な金融取引を可能にし，ひいては金融インフラの安全性と効率性の向上に資するかという点に関心が寄せられてきた．今後，この技術の応用をさらに検討していくにあたっては，実務面と技術面の両面において，課題をあぶりだしていく必要がある．本章では，それぞれに残された検討課題の中で，優先順位が高いと思われる論点をいくつか挙げてみたい．

3.1　実務面からみた特徴と課題

まず，実務面から見た分散型台帳技術の特徴と検討課題について，効率性と安全性を中心にいくつか挙げてみたい．

3.1.1　効率性の観点：中央銀行システムにとっての付加価値，コスト面でのメリット

まず，効率性の面からは，分散型台帳技術が中央銀行の提供する決済サービスにどのような付加価値を生み出すかを検討する必要がある．これまでのプロジェクトでは，すでに提供している中央銀行サービスについて，分散型台帳技術を使うことによって再現できるかを中心に検討作業を重ねてきた．しかしながら，今後は，我が国の金融インフラ全体をみたときに，果たして分散型台帳技術によって，より利便性の高いサービスを実現できるかを含めて，検討する余地があると考えられる．

たとえば，証券決済について言えば，証券取引の約定確認，清算（クリアリング），決済，証券の保管に至るさまざまなアレンジメントについて，約定確認システムの運営者，証券取引所，清算機関，決済銀行，カストディアン，さらには証券集中保管機関といった多くの機関が業務を分担している．こうした中で，やや大局的な視野に立って，中央銀行を含めたこれらの機関が担当する業務を分散型台帳技術を活用することによって効率化できるかを検討していくこともできるかもしれない．

さらに，分散型台帳技術の導入によるコストの削減効果等についても，今次プロジェクトでは検討対象外としてきたが，今後は，前提条件をつけながらも，中央集中型のシステムを分散化させることによるコスト面での影響について詳しく検討していくこともできよう．その際には，中央集中システムの管理・運営にかかる費用のみを対象とするのではなく，参加金融機関等も含めた金融インフラ全体としてのコスト削減につながるかをみていく必要もあろう（**図14**）．

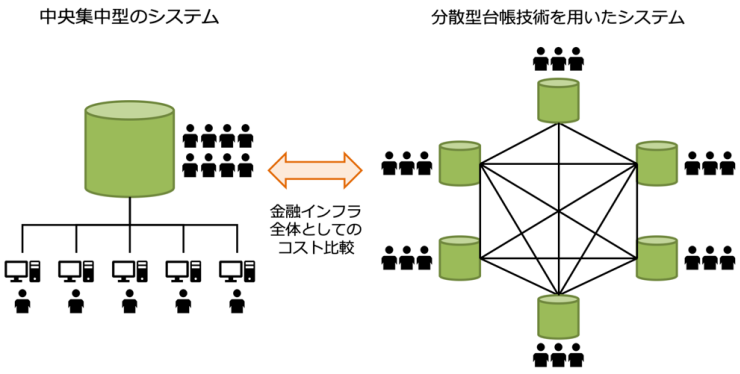

図14　コスト削減効果の検討範囲のイメージ

3.1.2　安全性の観点：頑健性やサイバー攻撃耐性の十分性について

次に，安全性の検証作業にあたっては，サイバー攻撃からのシステムの頑健性をどのように評価するかを含めて検討していく余地があろう．

もとより，多くの国では，中央銀行当座預金の開設や，中央銀行との取引，さらには中央銀行が運行する決済システムへの参加には厳格な要件が課されており，こうした参加者がサイバー攻撃を仕掛ける可能性はきわめて低いと考えられる．さらに，日銀ネットについて言えば，セキュリティ対策として，日本銀行と参加者との間は，これら以外の相手との通信をしない形でネットワークが接続されていたり，参加者ごとに使用することができる端末や利用者が限定されていたり，さらには送受信データの機密保持や改ざんを防止するためのさまざまな措置が講じられるなど，システムの堅牢性はきわめて高い．このため，サイバー攻撃というシナリオを想定するにあたっても，こうした中央銀行システムの特徴を考慮した上で，蓋然性の高いシナリオを設定すべきであろう．

この点に関連して言うと，国際的には，決済・市場インフラ委員会（CPMI）および証券監督者国際機構（IOSCO）による「金融市場インフラのためのサイバー攻撃耐性に係るガイダンス」が公表されている．このガイダンスは，CPMI-IOSCOの「金融市場インフラのための原則」（FMI原則）を補足することを目的としているが，たとえば，①サイバー攻撃の検知に用いるモニタリングとプロセスのツールの活用，②サイバー攻撃による障害発生後2時間以内に重要な業務を安全に再開し，障害発生日の終了までに決済が完了できるよう，システムとプロセスを設計・テストすることの必要性（2時間以内の業務再開＜2hRTO＞）等についてガイダンスを提供し，サイバー攻撃の事前阻止，攻撃への迅速かつ効果的な対応および安全な復旧に向けて，金融界の取り組みを促している．こうした国際的に合意された目線は，分散型台帳技術を応用した金融インフラの堅牢性を高める上でも参考になる可能性がある．

ネットワークに参加する各ノードへのサイバー攻撃を事前阻止する手段として，サイバー攻撃を受けるリスクを減らすようインセンティブ付けすることも考えられる．たとえば，秘密鍵の管理を専門の事業者（暗号資産カストディ事業者等）に一部委託し，決済業務と鍵管理業務を極力切り離す方法なども考えられる．しかし，この場合も，分散した秘密鍵の管理態勢やその運搬方法等についてセキュリティをどのように確保するかを考える必要があり，金融インフラ全体からの視点が必要とされよう．

また，サイバー攻撃は分散型台帳に書き込まれた時点で初めて成功したことになるが，他方で分散型台帳は基本的に事後に書き換えることは非常に難しいという特徴がある．2hRTOの実現にあたっては，非常時についての参加者間の事前の合意と，問題発生時に即時にそれを実施する体制も考える必要があろう．

3.1.3　分散型台帳技術とガバナンス

最後に，一国の経済の根幹をなす重要な金融インフラへの分散型台帳技術の応用にあたっては，その効率性と安全性を確保し，向上を図っていく際に，どのようなガバナンスが望ましいかについて検討する必要があるようにみえる．

分散型台帳技術の根幹には，信頼できる第三者を置くことなく，互いに信頼関係のない個人同士による取引を安全に行うための枠組みを提供するという理念がある．こうした分散型台帳技術の本来の理念に則り，信頼できる第三者を置かずに，さまざまな主体による検証を促す場合には，それらの主体に対して，共通のプロトコルを定め，その仕様の維持・管理ならびに技術の進

展に伴う向上を図るといった役割を誰が担うのか，そしてプロトコルの更新等が必要な場合にすべての参加者にどのようにエンフォースメントを図るのかといった問題が生じる．これは，金融インフラへの分散型台帳技術の応用にあたって最も重要な論点の1つと言えよう．

この点について，分散型台帳基盤であるビットコインでは，関係者間の対話を通じた解決策が模索された．しかし，ブロックサイズを巡る対立にみられたように，すべての関係者の合意を得ることはきわめて難しく，結果として，ビットコインの分裂をもたらした．他方，別な分散型台帳基盤であるイーサリアムでは，特定の管理主体を必要とせずに分散型台帳上に登録されたスマートコントラクトが管理する自律分散型組織（Decentralized Autonomous Organization, DAO）という概念が提案されたが，これまでの事例からは，緊急時の対応をプログラム上で行うことへの限界も明らかになっている．

今後，分散型台帳技術が成熟するに従って，それを支えるコミュニティやガバナンスのあり方，さらには金融インフラへの活用にあたっての組織体の在り方を巡って，さまざまな試行を経ながら発展していくと考えられる．

3.2　技術面からみた特徴と課題

次に，技術面から見た分散型台帳技術の特徴と検討課題についても，効率性と安全性を中心にいくつか挙げてみたい．

3.2.1　効率性の観点：プライバシーの確保と効率性の向上

金融取引においては，その内容を当事者以外の第三者へ明かさないというプライバシーや機密性の確保が重要である．このため，銀行間での取引は，各国とも信頼できる中立的第三者（中央銀行等）が運行するシステムを使って決済するのが一般的である．

この場合，当該の中立的第三者はすべての取引内容を把握することができることになるが，これは効率性の観点からも重要である．たとえば，日銀ネットが提供する流動性節約機能の1つである多者間同時決済機能は，全参加者の口座の残高と待ち行列を一元的に把握することによって，資金効率を向上させる仕組みとなっている．具体的には，①多者間同時決済機能を定刻に起動する，②起動時点におけるすべての参加者の待ち行列にある取引を対象として，それらがすべて同時に決済された場合の残高を計算し，資金不足がなく決済可能であれば，すべての取引を同時に決済する，③決済が可能でなければ，最大の赤残を抱える口座の待ち行列にある取引のうち，取引額が大きいものを除外して，残りの取引が同時に決済された場合の残高を再計算する，④このプロセスを決済可能な組合せが見つかるまで繰り返すといった手順を踏むことによって実行される（**図15**）．こうしたアルゴリズムを効率的に進めるには，中立的第三者が全参加者の口座残高や待ち行列に関する情報を一元的に把握することが望ましい．

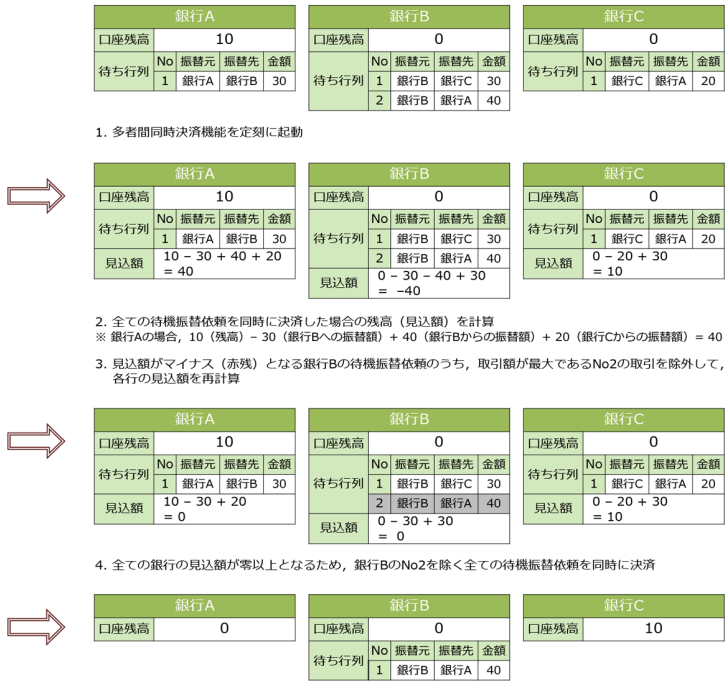

図15　多者間同時決済機能のイメージ―文献[2]を参考に作成

このように，プライバシーと効率性にはトレードオフの関係が存在することから，分散型台帳技術を応用する場合にも，プライバシーを確保しつつ，如何に効率的に処理を進めるかが課題となろう．

現在，分散型台帳基盤ごとに，取引内容をどこまで，どの参加者に対して開示するかを巡って，さまざまなアプローチが提案されている．たとえば，シンガポール通貨庁の取り組み（文献[5]）では，複数の分散型台帳基盤を用いて流動性節約機能を実現させることに焦点を当てた上で，多者間同時決済に際しては，ある基盤では参加者間で取引額を公開する必要があったことや，別の基盤では参加者間で（取引額は公開しないものの）各取引の識別子を公開した上で，参加者間を順に周回して処理する必要があることなどが報告されており，プライバシーの確保と効率性の向上を巡ってはさらに改善の余地があることが指摘されている．

3.2.2　安全性の観点：ファイナリティの確保

決済完了性（ファイナリティ）とは，決済が完了すると，その後で当該取引を取り消すことができないことを指す概念である（ここでは，決済完了性を記録の「確定性」という意味で使っており，法的な論点は含まれない）．ファイナリティがあることは参加者の決済リスクを削減することにつながる．FMI原則においても「ファイナルな決済を日中随時または即時に提供すべきである」（原則8）と定められており，中央銀行が提供する決済システムがファイナリティを備えていることはきわめて重要な特徴と考えられている．また，DVP決済においては，片方ないし双方の引渡が後から覆ることのないよう，資金決済システムと証券決済システムの両方がファイナリティを備えていることが必要となる．

翻って，分散型台帳技術の下では，ファイナリティはコンセンサス・アルゴリズムによって異なるのが現状である．たとえば，ビットコインで用いられているProof of Workというコンセンサス・アルゴリズムでは，ファイナリティが確率的にしか担保されない．これはある取引の存在

の有無やその時間順序が後から覆る可能性があるということを意味する．片方の引渡が後から覆る可能性が完全には消えないため，たとえばProof of Workの下ではDVP決済は実現できないと考えることもできる．また，Proof of Workを用いる一部の暗号資産で，取引が後から覆ることを利用して，暗号資産取引所に対してチェーンの再編成を用いた攻撃が生じたことも，ファイナリティが確率的であることの弊害と捉えることもできる．一方，ビットコインとは異なる分散型台帳基盤であるHyperLedger Fabricで以前に使われていたPractical Byzantine Fault Toleranceではファイナリティが確保されている．

一般に，ビットコインのような誰でも参加可能な分散型台帳基盤では，参加者の数は常に変動しているため，先に取引を記録してしまい，その後でトランザクションの時間順序などについて参加者間で合意を取る場合が多く，この場合ファイナリティは確率的にしか担保されないことになる．他方で，HyperLedger Fabricのような参加者を許可制とする分散型台帳基盤では，事前に全参加者を把握できるため，参加者間で合意を取った上で取引を記録することが可能であり，ファイナリティがある場合が大半と考えられる．

もっとも，ファイナリティは，コンセンサス・アルゴリズム以外にも，運用で確保することや法的に確保することもできる．最近では，ビットコインのような誰でも参加可能な分散型台帳基盤の場合でも，処理能力を高めるために，参加者間の合意を少数の特定ノードに限定する取り組が多く見られる．この考えを推し進めて，制度面や規制面などコンセンサス・アルゴリズム以外の何らかの形で，ある瞬間におけるマイニングを1台のノードに限定すれば，ファイナリティを常に担保することはできる．ファイナリティは技術的にはすでにさまざまな形で議論されているものの，このように決済システム全体として捉えた議論はまだ緒に就いたばかりである．今後，金融インフラへの分散型台帳技術の応用にあたっては，ファイナリティをどのような仕組みを通じて確保するのが最も望ましいかという点について，さらなる検討が求められよう．

3.2.3　インフラ・デザイン

最後に，分散型台帳技術を用いた金融インフラをどのようにデザインしていくかという論点が考えられる．さまざまな金融資産を扱う決済システムは，ネットワークを通じての相互依存性がきわめて高いことから，分散型台帳技術のネットワーク同士，分散型台帳技術のネットワークと非分散型台帳技術のシステムとの接点をどのように設計していくかといった論点がある．

仮に中央銀行システムに分散型台帳技術を応用する場合，円や国債などがネットワーク外でやり取りされているとすると，それらの資産の数量を，ネットワーク内のディジタルなトークンの数量と整合性を持たせるために，誰がどのように同期を図るのかといった論点がある．たとえば，ドイツ連邦銀行（ブンデスバンク）とドイツ証券取引所の取り組み（文献[8]）では，資金と証券をそれぞれ管理する主体が，取引時間終了後に都度ネットワーク内のトークンを回収し，翌日取引開始時に再配布するというアイディアが示されている．

逆に，中央銀行システムに分散型台帳技術を応用しない場合でも，こうした技術を応用する，他のシステムとの接点に関する論点がある．この点に関連して，イングランド銀行がRTGSシステムの高度化に関する検討作業を続ける中で，①現時点では，同行自身が運営するシステムへの分散型台帳技術の採用は時期尚早ながら，②RTGSシステムを使った高度な中央銀行サービスを提供するために，分散型台帳技術等を使った決済システムとの相互運用性（interoperability）を検証するための実証研究に着手することを明らかにした（文献[9]）．

こうした検討を経て，分散型台帳技術を含む金融インフラの将来像に，どのようなビジョンが提示されるか，その帰趨に注目していきたい．

4. おわりに

本稿では，日本銀行が欧州中央銀行との間で取り進めている分散型台帳技術の応用可能性に関するプロジェクトに基づいて，中央銀行からみた同技術の特徴と課題を取りまとめた．

各国の中央銀行は，金融インフラの効率性と安全性の向上に向けた中央銀行サービスの高度化を進めており，この中には，即時グロス決済化の実現，流動性節約機能の提供，さらには証券資金の同時受渡の実現といった取り組みが含まれる．こうした下で，ステラでは，分散型台帳技術を使うことによって，これらの機能を再現できることが確認され，当初の目的を達成し得たと評価することができる．その一方で，実務・技術的にみて，これまでのプロジェクトではカバーしきれていない論点も残されている．この中には，当該技術とガバナンスに関する問題のほか，金融取引の秘匿性（プライバシー）の確保や，ファイナリティを巡る問題などが含まれる．

今後は，民間金融機関やIT企業と連携しながら，これらの課題の解決に向けた議論を深めていくことが重要である．

参考文献

1）日本銀行金融研究所（編）：日本銀行の機能と業務, 有斐閣 （2011）.
2）日本銀行，欧州中央銀行：分散型台帳技術による資金決済システムの流動性節約機能の実現, https://www.boj.or.jp/announcements/release_2017/rel170906a.htm/ (2017)
3）日本銀行，欧州中央銀行：分散型台帳技術によるDVP決済の実現, https://www.boj.or.jp/announcements/release_2018/rel180327a.htm/ (2018)
4）Bank of Canada : Project Jasper : A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement, https://www.payments.ca/sites/default/files/29-Sep-17/jasper_report_eng.pdf (2017)
5）Monetary Authority of Singapore : Project Ubin : SGD on Distributed Ledger, http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf (2017)
6）Bank of Canada : Jasper Phase III Securities Settlement Using Distributed Ledger Technology, https://www.payments.ca/sites/default/files/jasper_phase_iii_whitepaper_final_0.pdf (2018)
7）Monetary Authority of Singapore : Delivery Versus Payment on Distributed Ledger Technologies Project Ubin, http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20DvP%20on%20Distributed%20Ledger%20Technologies.pdf (2018)
8）Deutsche Bundesbank and Deutsche Borse Group : BLOCKBASTER Final Report, https://www.bundesbank.de/resource/blob/766672/29feab3f9079540441e3abda1ed2d2c1/mL/2018-10-25-blockbaster-final-report-data.pdf (2018)
9）Bank of England : RTGS Renewal Proof of Concept : Supporting DLT Settlement Models, https://www.bankofengland.co.uk/news/2018/march/rtgs-renewal-proof-of-concept (2018)

脚注

☆1　本稿は，筆者達が日本銀行在籍中に担当したプロジェクトの概要を取りまとめたものである．なお文中で示された意見は，筆者個人のものであり，日本銀行の公式見解を表すものではない．

河田 雄次（非会員）kawada@mri.co.jp

慶應義塾大学大学院理工学研究科基礎理工学専攻修了．2015年から（株）三菱総合研究所主任研究員，2016年から2018年まで日本銀行に出向．

小早川 周司（正会員）econkoba@meiji.ac.jp

オクスフォード大学大学院経済学博士課程修了（D.Phil）．日本銀行企画局参事役，決済機構局参事役等を経て，2019年より明治大学政治経済学部教授．

採録決定：2019年4月15日
編集担当：荒木 拓也（日本電気（株））