



ブロックチェーン技術を活用した新銀行間決済 プラットフォーム実証実験報告書

2019年3月

**一般社団法人全国銀行資金決済ネットワーク
ブロックチェーン実証実験タスクフォース**

目次

1	プロジェクト説明	1
1.1	目的	1
1.2	体制	2
1.3	期間	2
2	プロジェクト活動記録	3
2.1	活動内容	3
2.2	スケジュール	3
2.3	タスクフォース開催実績	4
3	プロジェクト活動結果報告	5
3.1	総括	5
3.2	実証実験概要	5
3.3	実証実験システム概要	6
3.3.1	Hyperledger Fabric の特長	7
3.3.2	システムイメージ	9
3.3.3	システム環境	10
3.3.4	新銀行間決済 PF 実装方式	12
3.4	機能検証実施内容	15
3.5	機能検証実施結果	18
3.6	非機能検証実施内容	21
3.6.1	可用性	21
3.6.2	性能	22
3.6.3	セキュリティ	23
3.7	非機能検証実施結果	25
3.7.1	可用性	25
3.7.2	性能	30
3.7.3	セキュリティ	31
3.8	机上検討実施内容・実施結果	33
3.8.1	机上検討の実施目的	33
3.8.2	机上検討の実施事項	33
3.8.3	机上検討の実施結果	35

4	プロジェクト活動考察	44
4.1	ブロックチェーン技術の活用可能性	44
4.1.1	非機能面の有効性	44
4.1.2	非機能面の課題	45
5	今後に向けて	46
5.1	主な積み残し課題	46
5.1.1	実証実験によって明らかになった検討課題	46
5.1.2	実証実験のスコープ外として不足している検討課題	47
5.2	今後の取組みの方向性	47

1 プロジェクト説明

昨今、金融とテクノロジーの融合（Fintech）の動きが進展するなか、今後の銀行業務・システムに変革をもたらし得る有力なテクノロジーの一つとして、ブロックチェーン技術に対する注目が集まっている。ブロックチェーン技術は、広く様々な分野で調査・研究や実証実験が行われており、実際に証券や貿易金融の分野における実用化もみられる。

このような背景から、全国銀行資金決済ネットワーク（以下「全銀ネット」という。）は、2017年度、「ブロックチェーン技術の活用可能性に関する研究会」を設置しブロックチェーン技術の理解を深めるとともに、考えられる活用方法とそれに伴う課題、今後の検討の方向性を整理し、報告書¹を取りまとめた。

また、本年度は、上記報告書等にもとづき行われた2017年度全銀ネット有識者会議での示唆・提言²等を踏まえ、新たに「ブロックチェーン実証実験タスクフォース」を設置し、ブロックチェーンの資金決済システムへの活用可能性の検討を目的とし実証実験を行った。

本報告書は、「ブロックチェーン実証実験タスクフォース」における活動、および実証実験の実施内容・実施結果等を取りまとめたものである。

1.1 目的

今後のキャッシュレス社会の進展を念頭に、新たな銀行間決済の実現に向けて、ブロックチェーン技術の有用性について検証を行うものである。なお、本実証実験においては、ブロックチェーン技術を活用した小口取引におけるRTGS³の実現を目的としており、これを実現する仕組みとして、銀行間資金決済専用のデジタル通貨⁴（以下「決済用デジタル通貨」という。）を創出するものとする。

¹ 「ブロックチェーン技術の活用可能性に関する研究会」報告書を参照。

https://www.zengin-net.jp/company/pdf/180115_paper4.pdf

² 有識者からは、ブロックチェーン技術に係る実証実験を行うに当たっては、全銀ネットの業務範囲を前提とせず、利用者目線に立った決済サービスの提供といった観点も踏まえてはどうか、という提言があった。詳細は議事要旨参照。

https://www.zengin-net.jp/company/pdf/180115_summary.pdf

³ Real-Time Gross Settlement の略。取引1件ごとに銀行間の資金移動を行い、決済リスクを削減する仕組み。

⁴ 資金清算機関である全銀ネットが、銀行間資金決済のために、加盟銀行に発行（「1マネー＝1円」の固定）するもの。この決済用デジタル通貨の利用により、RTGSのような銀行間決済を行うため、別途の資金清算等が不要となる。

1.2 体制

本実証実験は全銀ネットが主体となり、2018年度の全銀ネット理事行9行が参加、富士通株式会社（以下「富士通」という。）がシステム構築・検証支援を実施した。また、全銀システムの開発ベンダである、株式会社エヌ・ティ・ティ・データ（以下「NTT データ」という。）からも検討の支援を得た。

表 1.2-1 実施体制

No.	役割	参加企業
1	実施主体	全銀ネット
2	参加銀行 (全銀ネット理事行)	みずほ銀行
3		三菱 UFJ 銀行
4		三井住友銀行
5		りそな銀行
6		常陽銀行
7		福岡銀行
8		西日本シティ銀行
9		三井住友信託銀行
10		京葉銀行
11	システム構築・検証支援	富士通
12	検討支援	NTT データ

1.3 期間

2018年7月から2019年3月までプロジェクト活動を実施した。

2 プロジェクト活動記録

2.1 活動内容

本プロジェクトにおいては、決済用デジタル通貨を用いた銀行間資金決済（RTGS）に係る機能面・非機能面の実証実験および考えられ得る運用面の観点について机上検討を実施した。

2.2 スケジュール

2018年7月から2019年3月までの活動期間における実証実験、机上検討のスケジュールは以下のとおり。



図 2.2-1 プロジェクトスケジュール

2.3 タスクフォース開催実績

本プロジェクト活動期間中に開催した「ブロックチェーン実証実験タスクフォース」は以下のとおり。

開催日	会議体	主な議題
2018年7月25日	第1回タスクフォース	本プロジェクトの進め方について
2018年8月29日	第2回タスクフォース	実証実験の実施目的・実施内容・システム構成等について
2018年9月26日	第3回タスクフォース	実証実験の参加行の募集等について
2018年10月3日	第4回タスクフォース	ブロックチェーン技術の活用可能性に係る実証実験の実施について
2018年10月24日	第5回タスクフォース	実証実験の公表および実験期間中の機能面・非機能面の検証スケジュール等について
2018年11月21日	第6回タスクフォース	実証実験における機能面・非機能面の具体的な検証方法について
2018年12月19日	第7回タスクフォース	机上検討項目および実施事項等について
2019年1月30日	第8回タスクフォース	実証実験の実施状況および業務プロセス・機能要件の概要整理について
2019年2月20日	第9回タスクフォース	ブロックチェーン技術の活用可能性に係る実証実験の実施結果について
2019年2月27日	第10回タスクフォース	ブロックチェーン技術を活用した新銀行間決済プラットフォーム実証実験報告書について

3 プロジェクト活動結果報告

3.1 総括

実証実験結果および机上検証結果を踏まえ、本プロジェクトの実証テーマについて、活動結果を総括する。詳細な報告については後章を参照願う。

◆ 銀行間決済システムへのブロックチェーン適用可能性

小口取引における RTGS の実現に向けては、一定のブロックチェーンの有用性を確認できた。

3.2 実証実験概要

本実証実験においては、決済用デジタル通貨を用いた銀行間資金決済システム（以下「新銀行間決済 PF」という。）が RTGS として機能するかを検証した。当該機能検証に当たっては、銀行間決済のトリガーとなる送金を発生させる必要がある。したがって、本検証においては、暫定的な対応として、メガバンク 3 行および富士通が開発した個人間送金システム⁵（以下「P2P 送金 PF」という。）を活用させていただき、これと連動させることで、送金発生から銀行間決済までの一連の流れを一気通貫で検証した。また、銀行間決済にブロックチェーン技術を採用した場合の非機能面についても検証を行い、技術の有用性を確認した。実証実験のイメージおよび機能面、非機能面における具体的な検証観点は下表のとおり。

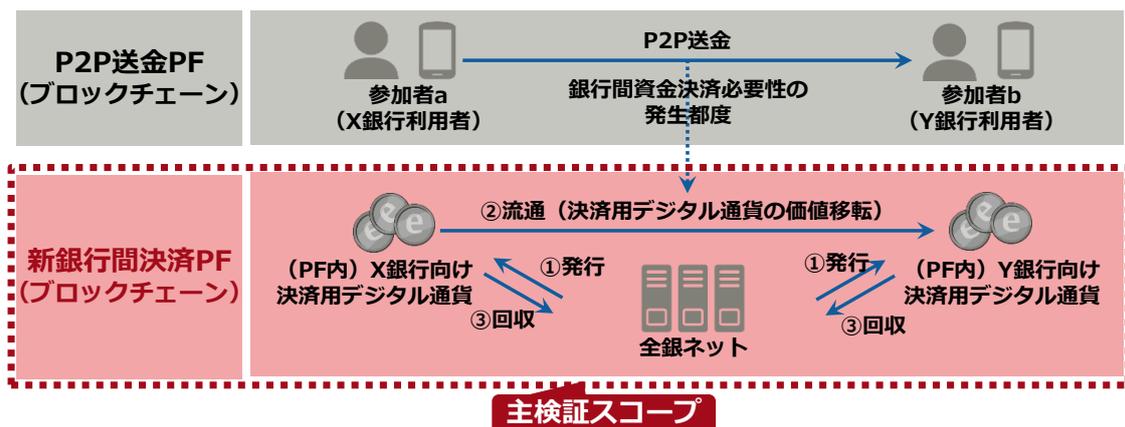


図 3.2-1 実証実験イメージ

⁵ 2017 年度、みずほフィナンシャルグループ、三井住友フィナンシャルグループ、三菱 UFJ フィナンシャル・グループおよび富士通が、ブロックチェーン技術を活用した個人間送金サービスの実証実験を実施した際に構築したシステム。

(<http://pr.fujitsu.com/jp/news/2017/10/10-2.html>)

表 3.2-1 機能面・非機能面の検証観点

検証カテゴリ		検証主体	検証概要
機能面		全銀ネット 参加銀行 富士通	ブロックチェーン技術を活用した「決済用デジタル通貨」が小口取引に対する銀行間資金決済スキーム (RTGS) として正しく機能するかを確認する。
非機能面	可用性	全銀ネット 富士通	ブロックチェーンおよびブロックチェーン以外のシステムコンポーネントにおいて業務継続を可能とする構成を確認する。
	性能		必要なレスポンス、スループット性能が発揮できるかを確認する。
	セキュリティ		ブロックチェーン技術を活用する場合に考慮すべき特有のセキュリティ対策について考察する。

3.3 実証実験システム概要

本実証実験に当たっては、新銀行間決済 PF を新規に構築した。新銀行間決済 PF は、全銀協「ブロックチェーン連携プラットフォーム」(以下「BC 連携 PF」という。)を用い、ブロックチェーンソフトウェアは、BC 連携 PF 上で利用可能な Hyperledger Fabric⁶を利用した。Hyperledger Fabric のバージョンは本プロジェクト開始当時(2018年7月)の最新版であった V1.2 を採用した。

また、本実証実験においては、メガバンク 3 行および富士通が構築した P2P 送金 PF も利用しているが、本実証実験の主検証スコープは、新銀行間決済 PF であることから、本書においては記載の対象外としている。

⁶ ブロックチェーンフレームワークであり、The Linux Foundation が運営する Hyperledger Project の一つ。Hyperledger は、産業間共通のブロックチェーン技術推進のために設立されたオープンソースソフトウェアの共同開発プロジェクト。

表 3.3-1 実証実験システムの利用プラットフォーム

プラットフォーム	用途	ブロックチェーン環境	ブロックチェーン外環境
P2P 送金 PF	銀行間決済のトリガーとなる他行宛送金取引（インターバンク送金）を発生させるために利用。	BC 連携 PF (Hyperledger Fabric V1.0)	FUJITSU Cloud Service For OSS
新銀行間決済 PF	インターバンク送金に伴う銀行間決済（RTGS）の実証を行うために利用。	BC 連携 PF (Hyperledger Fabric V1.2)	FUJITSU Cloud Service For OSS

3.3.1 Hyperledger Fabric の特長

本項は、新銀行間決済 PF に採用した Hyperledger Fabric の特長について記載する。

(1) Hyperledger Fabric の台帳の概念

Hyperledger Fabric の台帳は、Bitcoin のようなデータ管理とは異なり、World State とブロックチェーンから構成される。World State およびブロックチェーンの概要は以下のとおり。

表 3.3-2 Hyperledger Fabric における台帳の構造

種類	格納データ	データ構造
World State	トランザクション（以下「Tx」という。） 実行結果（最新値）	Key - Value ストア形式
ブロックチェーン	World State を更新したトランザクション履歴	複数の Tx が格納されたブロックのチェーン構造

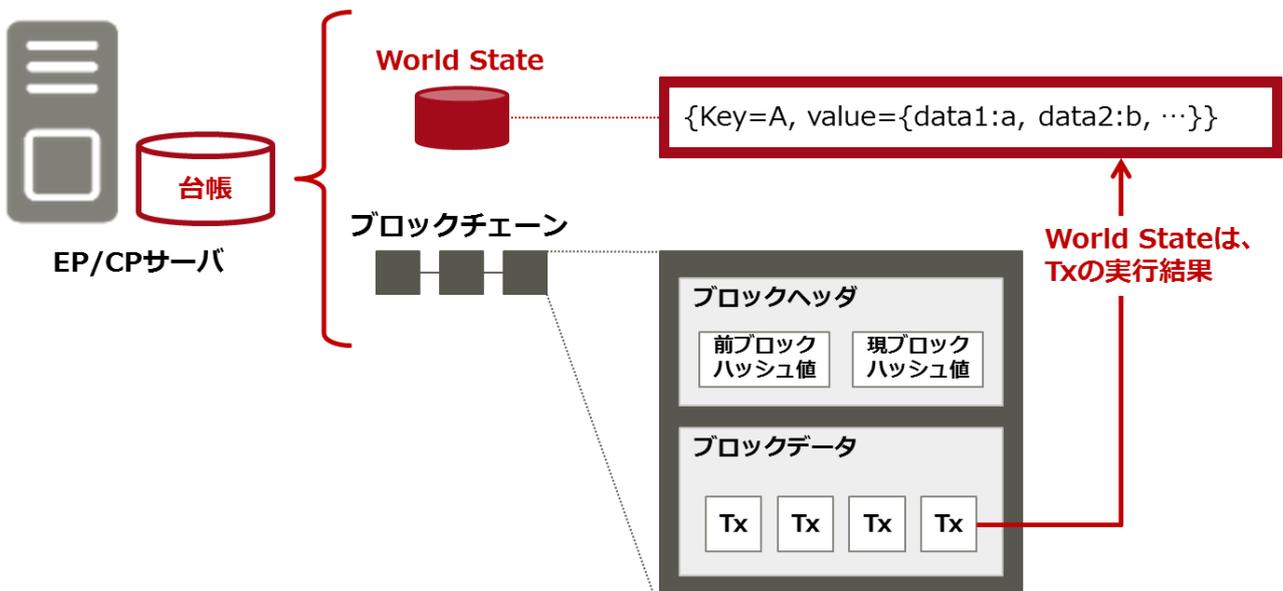


図 3.3-1 World State とブロックチェーンの関係性

(2) Hyperledger Fabric の主な設定項目

Hyperledger Fabric には、ブロックチェーンネットワークのデザインを決定するに当たり、主に考慮すべき設定項目として、「組織」、「チャンネル」、「合意形成アルゴリズム」および「合意形成ポリシー」の概念が存在する。それぞれの概念に対して、本実証実験における設定方針・設定値を以下に示す。

表 3.3-3 Hyperledger Fabric における主な設定項目・設定方針・設定値

設定項目	設定項目の意味	設定方針	設定内容
チャンネル	台帳の共有範囲を制限する概念。 組織のグループ単位でチャンネルを設定することが可能。	台帳の分割用途はないため、1 とする。	1
組織	チャンネルの設定や合意形成ポリシーの設定単位。 ピアノードのグループ単位で組織を設定することが可能。	合意形成ポリシー（後述）に 2/3 を設定するため、3 を設定する。	3

設定項目	設定項目の意味	設定方針	設定内容
合意形成 アルゴリズム	Hyperledger Fabric は、Ordering Service と呼ばれる合意形成アルゴリズムが利用可能。 Ordering Service の冗長化有無により、「Solo : 冗長化なし」「Kafka : 冗長化あり」が選択可能。	非機能検証での可用性確認を予定しているため、Kafka を選択する。	Kafka
合意形成 ポリシー	Tx, ブロック確定の際に条件となるポリシー。 本ポリシーを満たす組織からの承認が得られた場合のみ Tx, ブロックが確定する。	以下双方の条件を満たす構成とする。 ・ 合意形成ポリシーが過半数を設定可能 (2n-1 n:自然数) ・ EP/CP が冗長化構成かつ最も性能が発揮可能 (≥ 2)	2/3

3.3.2 システムイメージ

本実証実験システムは、P2P 送金 PF と新銀行間決済 PF 間を接続し、P2P 送金 PF 利用者のスマートフォンで指示された送金が銀行間送金であった場合、新銀行間決済 PF に自動的に連携し銀行間決済が実施されるものとした。また、新銀行間決済 PF には、管理用途として決済用デジタル通貨の残高・取引の照会および決済用デジタル通貨の発行・回収が可能な Graphical User Interface (以下「GUI」という。)を用意した。

本実証実験のシステムイメージを以下に示す。

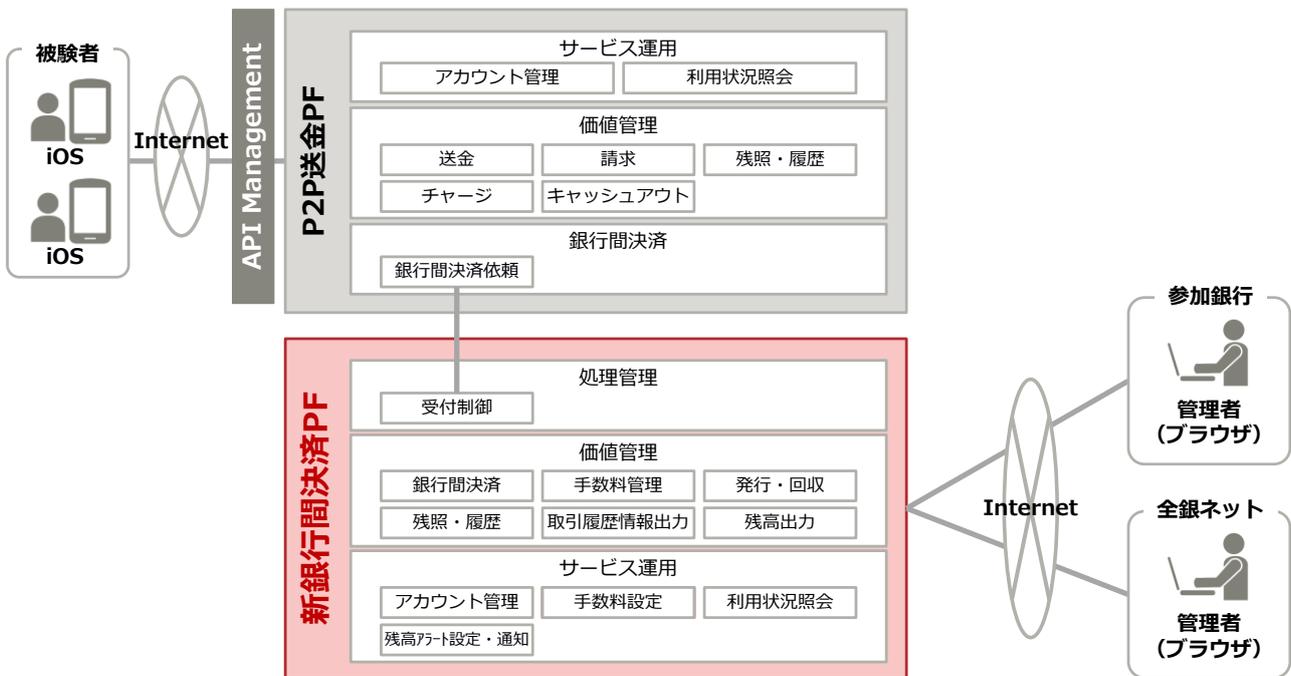


図 3.3-2 システムイメージ

3.3.3 システム環境

本実証実験のシステムは可用性の確認が可能となるよう、全種類のサーバに対して冗長化構成とした。また、業務サーバはこれらの中で最も負荷がかかることを加味し、3 台構成とした。EP/CPサーバにおいては、合意形成ポリシーの設定値の観点から3 台構成とした。

新銀行間決済 PF におけるハードウェア一覧、物理構成図を以下に示す。

表 3.3-4 ハードウェア一覧

#	サーバ種類	台数	クラウド環境/スペック
1	業務サーバ	3	FUJITSU Cloud Service for OSS
2	DB サーバ	2	- CPU 8 コア
3	EP/CP サーバ	3	- メモリ 32GB
4	CA サーバ	2	
5	Ordering Service サーバ	2	
6	Kafka サーバ	4	
7	Zookeeper サーバ	3	

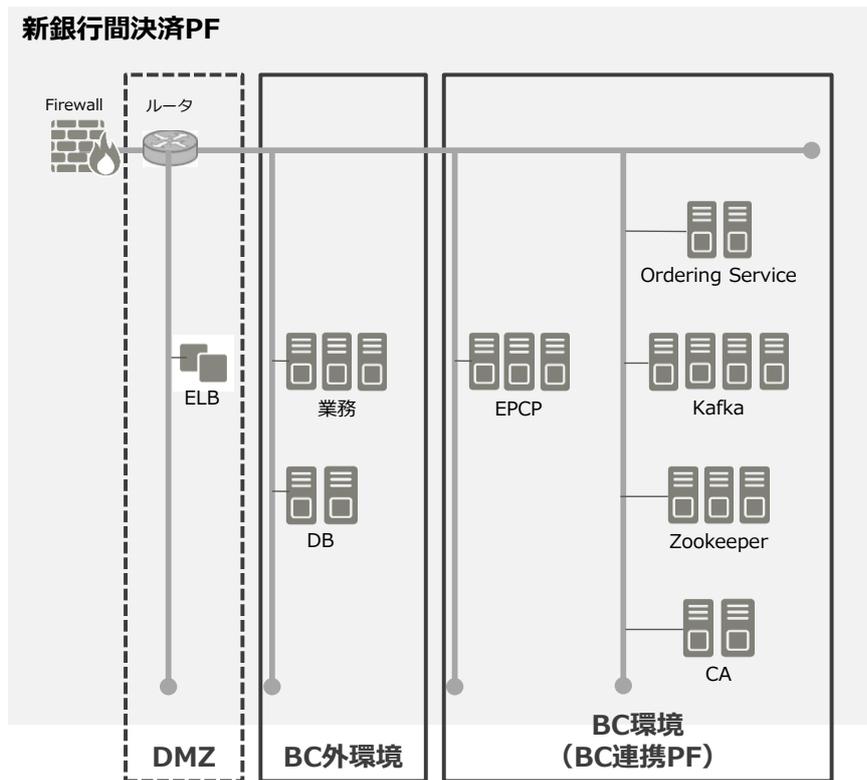


図 3.3-3 物理構成図

新銀行間決済 PF におけるソフトウェア一覧、論理構成図を以下に示す。

表 3.3-5 ソフトウェア一覧

#	サーバ種類	ソフトウェア	バージョン等
1	業務サーバ	Red Hat Enterprise Linux	7.3 (64bit)
2		Interstage Application Server Standard-J Edition	12.1
3		Spring boot	1.5.3
4		Hyperledger Fabric SDK	1.2.0 (Java 版)
5		jackson	2.8.10
6		joda-time	2.9.9
7		validation-api	1.1.0
8		Lombok	1.16.16
9		icu4j	60.2
10	DB サーバ	Red Hat Enterprise Linux	7.3 (64bit)
11		Enterprise PostgreSQL	9.6
12	EP/CP サーバ	Red Hat Enterprise Linux	7.3 (64bit)
13	CA サーバ	Docker	17.06.1-ce

#	サーバ種類	ソフトウェア	バージョン等
14	Ordering Service サーバ	Docker-compose	1.15.0
15	Kafka サーバ Zookeeper サーバ	Hyperledger Fabric	1.2.0

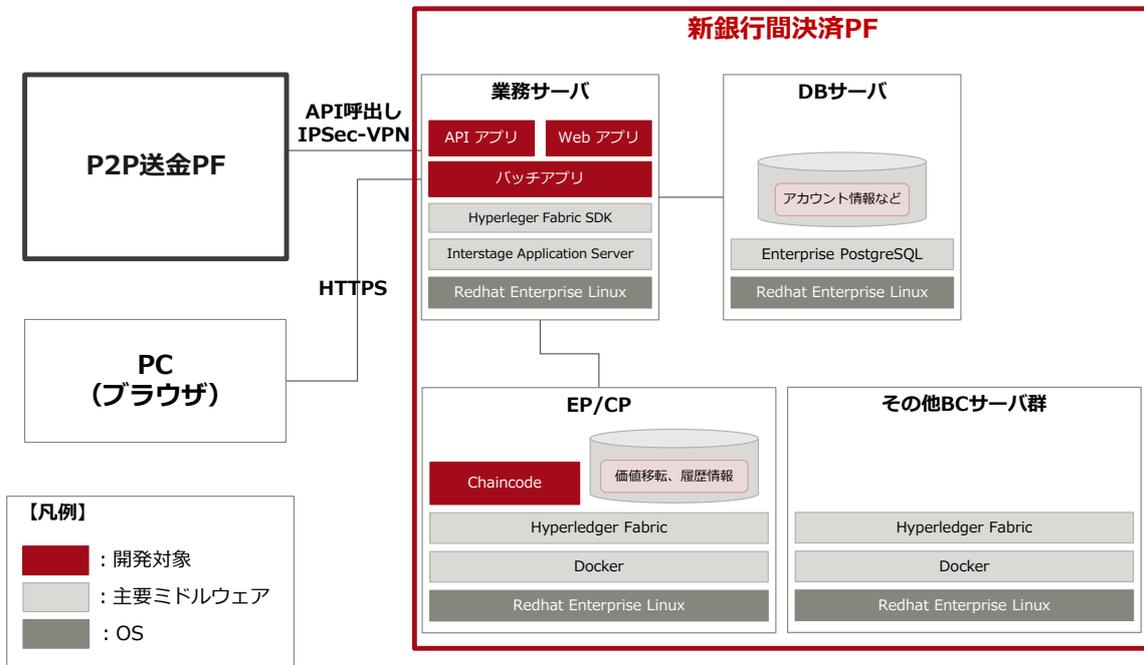


図 3.3-4 論理構成図

3.3.4 新銀行間決済 PF 実装方式

本実証実験においては、実証実験の性質・期間・コストを加味し、機能面・非機能面の確認に必要な最低限の機能のみを実装した。新銀行間決済 PF における実装のポイントを以下に示す。

(1) 新銀行間決済 PF 機能

本実証実験における新銀行間決済 PF においては、主に P2P 送金 PF とのシステム間連携機能、全銀ネット管理者、銀行管理者の利用を想定した GUI 機能および各種レポーティングのバッチ機能を実装した。本実証実験システムにおいて、具備した機能は以下のとおり。

表 3.3-6 新銀行間決済 PF 機能一覧

#	機能 カテゴリ	機能	IF	機能概要	利用主体
1	処理管理	受付制御	システム間 連携	P2P 送金 PF からの銀行間決済依頼を受け付ける。	P2P 送金 PF
2	価値管理	銀行間決済	システム間 連携	決済用デジタル通貨の銀行アカウント間価値移転を行う。	P2P 送金 PF
3		手数料管理	システム間 連携	銀行間決済の際、設定された手数料を算出し、手数料情報を生成する。	P2P 送金 PF
4		発行・回収	画面 (ブラウザ)	決済用デジタル通貨の発行・回収を行う。	全銀ネット
5		残照・履歴	画面 (ブラウザ)	決済用デジタル通貨の残高照会、決済用デジタル通貨の発行・回収、銀行間決済の履歴を参照する。	銀行、 全銀ネット
6		取引履歴情報 出力	バッチ (ファイル)	銀行ごとに決済用デジタル通貨の取引履歴情報を日次でファイル出力する。	銀行、 全銀ネット
7		残高出力	バッチ (ファイル)	全銀行の決済用デジタル通貨残高を日次でファイル出力する。	全銀ネット
8	サービス 運用	アカウント 管理	画面 (ブラウザ)	ログイン・ログアウト、パスワード変更等のアカウント管理を行う。	銀行、 全銀ネット
9		手数料設定	画面 (ブラウザ)	銀行間決済の手数料を設定する。	銀行
10		利用状況照会	画面 (ブラウザ)	指定期間の銀行間決済状況を照会する。	全銀ネット
11		残高アラート 設定・通知	画面 (ブラウザ)	決済用デジタル通貨の残高アラート値の設定、決済用デジタル通貨残高が残高アラート値を下回った場合の通知を行う。	銀行

(2) 決済用デジタル通貨残高管理方式

Hyperledger Fabric を利用して価値管理を行う場合は、World State の Key-Value を用いることが一般的であり、今回であれば各銀行が保有する決済用デジタル通貨の残高を管理項目として充てることが考えられる。

しかし、Hyperledger Fabric の仕様を踏まえて内部排他制御処理との干渉が発生するかどうか

を慎重に考慮し、項目化の検討を行うべき必要がある。

本実証実験については、同一キー（銀行）に対し、秒間数十～千といった取引が発生するユースケースが想定される。この場合内部排他制御の対象となるものと考えられ、取引集中に対して多数の取引が失敗し重大な問題に直面することが想定される。

【Hyperledger Fabricの内部排他制御の課題】

World Stateで最新残高を管理した場合、同一銀行に対し、短時間に集中して取引があった際、1件目は成立するが2件目以降の処理が失敗する。



図 3.3-5 内部排他制御の課題

当問題を回避するため新銀行間決済 PF は以下の方式を採用した。銀行間決済取引においては、キーの衝突を回避するために、コンポジットキー（複合キー）による取引明細を作成し、残高を利用する場面で都度取引明細より最新残高を算出することとした。しかし、取引明細は時間の経過とともに単調増加となるため、残高取得処理の高速化を図るためにも定期的に集計し集計結果を格納しておく方式とした。

【本実証実験システムでの対応方式】

銀行間決済時は、ユニークキー（取引日時+銀行）による取引明細を作成し、内部排他を回避する。残高取得時は、定期的に取引明細を集計した結果と集計結果以降に蓄積した取引明細を合計値を算出する。

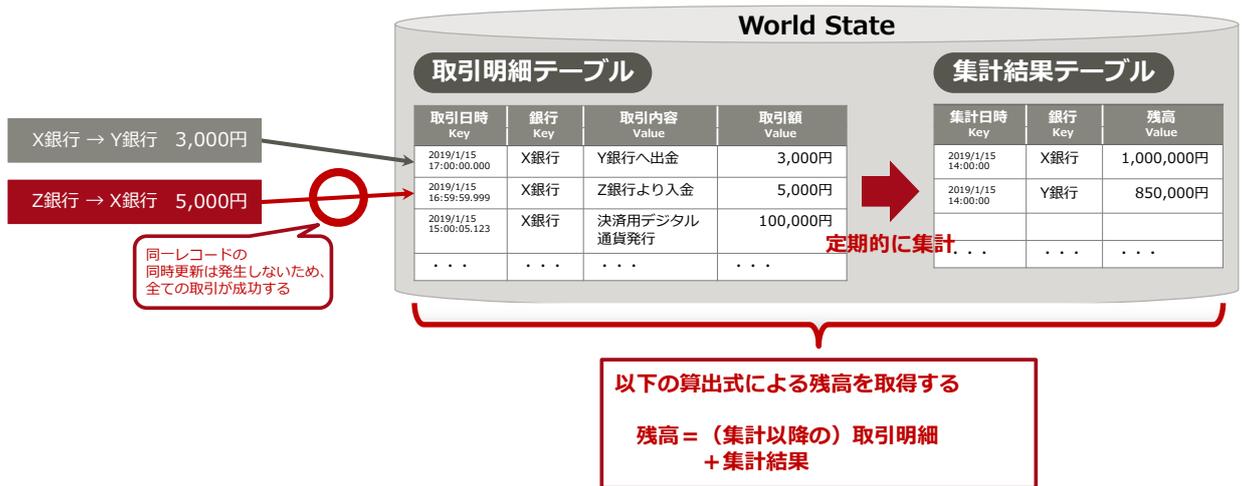


図 3.3-6 新銀行間決済 PF での残高管理方式

(3) 決済リスク回避方式

本実証実験で構築したシステムにおいては、決済用デジタル通貨不足による決済リスクを回避するために「残高アラート」および「取引停止閾値」の2つの仕組みを具備した。それぞれの仕組みは以下のとおり。

表 3.3-7 決済リスク回避方式

#	決済リスク回避の仕組み	目的	仕組み発動時の挙動	実証実験での設定値
1	残高アラート	銀行担当者に対し、決済用デジタル通貨残高の減少を注意喚起し、決済用デジタル通貨発行を促す	銀行担当者が管理端末操作時、画面にアラート表示する	銀行が変更可 (初期値：300万円)
2	取引停止閾値	銀行間決済時、リアルタイムでの残高不足が判定できないため、取引停止閾値を設け、P2P送金を事前に停止することで、決済用デジタル通貨不足を防止する	インナーバンク、インターバンク双方の P2P 送金が利用不可となる	100万円

3.4 機能検証実施内容

機能検証においては、本実証実験システムの新銀行間決済 PF に具備した機能が正しく動作するかの確認および RTGS として正しく機能するか検証を実施した。以下に新銀行間決済 PF の動作確認観点を示す。

表 3.4-1 新銀行間決済 PF の動作確認観点

#	機能分類	確認項目	想定結果
1	銀行間決済	インナーバンク送金	銀行間決済が実行されないこと。
2		インターバンク送金	銀行間決済が正しく実行されること。
3	決済用デジタル通貨発行・回収	決済用デジタル通貨発行	指定の銀行に決済用デジタル通貨が正しく発行できること。
4		決済用デジタル通貨回収	指定の銀行から決済用デジタル通貨が正しく回収できること。

#	機能分類	確認項目	想定結果
5		決済用デジタル通貨 回収（異常系）	指定の銀行から残高を超えた決済用デジタル通貨 が回収できないこと。
6	決済リスク 回避方式	残高アラート	決済用デジタル通貨残高が残高アラート値を下回 った場合、アラート通知が正しく機能すること。
7		取引停止閾値	決済用デジタル通貨残高が取引停止閾値を下回っ た場合、P2P 送金が利用不可となること。

RTGS としての機能検証においては、「残高の整合性確認」および「取引の完全性確認」の 2 点の
確認を日次で実施し、P2P 送金 PF を含めた実証実験システム全体として不整合が発生していないこ
とを確認した。以下に RTGS の検証観点を示す。

表 3.4-2 RTGS の検証観点

検証観点	検証主体	実施概要
決済用デジタル通貨 残高チェック	全銀ネット 参加銀行 富士通	決済用デジタル通貨残高の理論値を机上計算し、当該理論値と 新銀行間決済 PF が保有する残高が一致することを確認。
取引履歴チェック	全銀ネット 参加銀行 富士通	新銀行間決済 PF の取引履歴と P2P 送金 PF の取引履歴を突合 し、銀行間決済に関わる取引の件数・内容が一致することを確認。

これら RTGS の 2 つの検証観点に対する具体的な実施方法を以下に示す。

表 3.4-3 決済用デジタル通貨残高チェック実施方法

	実施概要
実施手順	① 取引履歴をもとに決済用デジタル通貨残高理論値を机上算出 ② ①の理論値と新銀行間決済 PF が保有する決済用デジタル通貨実値を突合し、突合結 果に矛盾がないことを確認 〔確認対象〕 ・全銀行の決済用デジタル通貨残高値

実施概要																																														
<p>実施イメージ</p>	<table border="1"> <thead> <tr> <th>#</th> <th>項目</th> <th>説明</th> </tr> </thead> <tbody> <tr><td>1</td><td>取引日時</td><td>YYYY-MM-DDThh:mm:ss.SSSZ</td></tr> <tr><td>2</td><td>取引ID</td><td>16桁の一意な文字列</td></tr> <tr><td>3</td><td>仕向銀行名</td><td>仕向銀行名</td></tr> <tr><td>4</td><td>操作種別</td><td>“送金”, “入金”</td></tr> <tr><td>5</td><td>被仕向銀行名</td><td>被仕向銀行名</td></tr> <tr><td>6</td><td>金額</td><td>送金金額</td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>#</th> <th>項目</th> <th>説明</th> </tr> </thead> <tbody> <tr><td>1</td><td>取引日時</td><td>YYYY-MM-DDThh:mm:ss.SSSZ *当該取引に紐づくP2P送金PF.取引日時とはずれる</td></tr> <tr><td>2</td><td>取引ID</td><td>16桁の一意な文字列 *当該取引に紐づくP2P送金PF.取引IDと同一</td></tr> <tr><td>3</td><td>仕向銀行名</td><td>仕向銀行名もしくは“全銀ネット（発行の場合）”</td></tr> <tr><td>4</td><td>操作種別</td><td>“発行”, “回収”, “送金”, “入金”</td></tr> <tr><td>5</td><td>被仕向銀行名</td><td>被仕向銀行名もしくは“全銀ネット（回収の場合）”</td></tr> <tr><td>6</td><td>金額</td><td>決済用デジタル通貨移転金額</td></tr> <tr><td>7</td><td>手数料</td><td>決済用デジタル通貨移転に関わる手数料 *発行, 回収は0固定</td></tr> </tbody> </table>	#	項目	説明	1	取引日時	YYYY-MM-DDThh:mm:ss.SSSZ	2	取引ID	16桁の一意な文字列	3	仕向銀行名	仕向銀行名	4	操作種別	“送金”, “入金”	5	被仕向銀行名	被仕向銀行名	6	金額	送金金額	#	項目	説明	1	取引日時	YYYY-MM-DDThh:mm:ss.SSSZ *当該取引に紐づくP2P送金PF.取引日時とはずれる	2	取引ID	16桁の一意な文字列 *当該取引に紐づくP2P送金PF.取引IDと同一	3	仕向銀行名	仕向銀行名もしくは“全銀ネット（発行の場合）”	4	操作種別	“発行”, “回収”, “送金”, “入金”	5	被仕向銀行名	被仕向銀行名もしくは“全銀ネット（回収の場合）”	6	金額	決済用デジタル通貨移転金額	7	手数料	決済用デジタル通貨移転に関わる手数料 *発行, 回収は0固定
#	項目	説明																																												
1	取引日時	YYYY-MM-DDThh:mm:ss.SSSZ																																												
2	取引ID	16桁の一意な文字列																																												
3	仕向銀行名	仕向銀行名																																												
4	操作種別	“送金”, “入金”																																												
5	被仕向銀行名	被仕向銀行名																																												
6	金額	送金金額																																												
#	項目	説明																																												
1	取引日時	YYYY-MM-DDThh:mm:ss.SSSZ *当該取引に紐づくP2P送金PF.取引日時とはずれる																																												
2	取引ID	16桁の一意な文字列 *当該取引に紐づくP2P送金PF.取引IDと同一																																												
3	仕向銀行名	仕向銀行名もしくは“全銀ネット（発行の場合）”																																												
4	操作種別	“発行”, “回収”, “送金”, “入金”																																												
5	被仕向銀行名	被仕向銀行名もしくは“全銀ネット（回収の場合）”																																												
6	金額	決済用デジタル通貨移転金額																																												
7	手数料	決済用デジタル通貨移転に関わる手数料 *発行, 回収は0固定																																												
<p>実施者</p> <p>確認対象</p> <p>タイミング</p>	<p>全銀ネット・富士通：全参加銀行分を日次で実施</p> <p>参加銀行：自行分を任意のタイミングで実施</p>																																													

また、RTGSの検証においては、全銀ネット、参加銀行9行、富士通が並行して検証を実施するため、参加銀行9行のアカウントに加え、以下のとおり仮想銀行アカウントを用意した。

表 3.4-5 インターバンク送金の発生方法

方法	内容
仮想銀行の設置	<ul style="list-style-type: none"> ・実証実験用の仮想銀行（大手町銀行、汐留銀行）を準備 ・各参加銀行の参加者アカウントを当該参加銀行と大手町銀行に半数ずつ紐づけることで、各参加銀行と仮想銀行間でインターバンク送金が可能 ・全銀ネット、富士通の参加者アカウントは大手町銀行および汐留銀行に半数ずつ紐づけ

3.5 機能検証実施結果

機能検証期間中、P2P送金PFを含め、一度もシステム停止することなく安定稼動した。
 また、新銀行間決済PFの動作確認における予定した項目は全て消化し問題は検出されなかった。
 以下に新銀行間決済PFの機能検証項目・結果を示す。

表 3.5-1 新銀行間決済 PF の動作確認結果

#	機能分類	確認項目	確認結果	
			(○：結果 OK, ×：結果 NG, -：判定対象外)	
1	銀行間決済	インナーバンク送金を実行	銀行間決済が実行されなかった。	○
2		インターバンク送金を実行	銀行間決済が正しく実行された。	○
3	決済用デジタル通貨 発行・回収	決済用デジタル通貨発行	指定の銀行に決済用デジタル通貨が正しく発行できた。	○
4		決済用デジタル通貨回収	指定の銀行から決済用デジタル通貨が正しく回収できた。	○
5		決済用デジタル通貨回収 (異常系)	指定の銀行から残高を超えた決済用デジタル通貨が回収できなかった。	○
6	決済リスク 回避方式	残高アラート	決済用デジタル通貨残高が残高アラート値を下回った場合、アラート通知が正しく機能した。	○
7		取引停止閾値	決済用デジタル通貨残高が取引停止閾値を下回った場合、P2P 送金が利用不可となった。	○

RTGS の検証においても、予定した項目は全て消化し、新銀行間決済 PF に関する問題は検出されなかった。以下に RTGS の検証結果を示す。

表 3.5-2 日次の RTGS 検証結果 (12/3 ~ 12/27)

【凡例】 ○：結果 OK, ×：結果 NG, -：判定対象外

検証観点	12/3 (月)	12/4 (火)	12/5 (水)	12/6 (木)	12/7 (金)	12/8 (土)	12/9 (日)	12/10 (月)	12/11 (火)	12/12 (水)	12/13 (木)	12/14 (金)
決済用デジタル通貨 残高チェック	○	○	○	○	○	○	○	○	○	○	○	○
取引履歴 チェック	○	○	○	○	○	○	○	○	○	○	○	○

検証観点	12/15 (土)	12/16 (日)	12/17 (月)	12/18 (火)	12/19 (水)	12/20 (木)	12/21 (金)	12/22 (土)	12/23 (日)	12/24 (月)	12/25 (火)	12/26 (水)	12/27 (木)
決済用デジタル通貨 残高チェック	○	○	○	○	○	○	○	○	○	○	○	○	○
取引履歴 チェック	○	○	○	○	○	○	○	○	○	○	○	○	○

機能検証においては、検証終了後に「機能面」、「使い勝手/デザイン面」等、参加銀行よりフィードバックを受領した。フィードバックは本実証実験の主スコープである新銀行間決済 PF だけでなく、P2P 送金を含めた一連のフローに対しての改善余地も探るため、P2P 送金 PF も対象とし、広く意見を収集した。

新銀行間決済 PF に関する主なフィードバックとしては、セキュリティを考慮した認証方式への改善、使い勝手の改善、エラーメッセージの拡充等が挙げられた。また、P2P 送金 PF との機能分担の是非についても、意見が寄せられた。これらフィードバックに対する対応策の検討は今後の課題である。

3.6 非機能検証実施内容

IPA (情報処理推進機構)が公開する非機能要求グレードを踏まえて、検証カテゴリを「可用性」、「性能・拡張性」、「運用・保守性」、「移行性」、「セキュリティ」および「システム環境・エコロジー」の6つと設定した。

本非機能検証において、本検証が実証実験という位置づけから「運用・保守性」および「システム環境・エコロジー」については今後の検討項目として整理し、「移行性」については新規システムを想定するため検討対象外とした。また、「拡張性」についても、現時点では将来的な取引件数の見積りが困難なことから、検討対象外とした。

したがって、本検証においては、検討対象として「可用性」、「性能」および「セキュリティ」の3点にフォーカスするものとする

3.6.1 可用性

可用性においては、本実証実験で構築したシステムが業務継続性を有しているかを評価した。

(1) 検証スコープ

本実証実験においては災対環境を具備していないため、実証実験環境のみで検証できる範囲とした。実証実験環境においては、新銀行間決済 PF 内の全機能ブロック毎に冗長化構成を設けているため、各機能ブロックを対象に単一障害時および複数障害時に対する検証をスコープとした。

(2) 評価項目

可用性検証における評価項目は以下のとおり。

表 3.6-1 可用性検証の評価項目一覧

#	評価項目	確認内容
1	業務サーバの単一障害時の業務継続確認	業務サーバを1台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
2	DBサーバの単一障害時の業務継続確認	DBサーバを1台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
3	EP/CPサーバの単一障害時の業務継続確認	EP/CPサーバを1台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。

#	評価項目	確認内容
4	CA サーバの単一障害時の業務継続確認	CA サーバを 1 台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
5	Ordering Service サーバの単一障害時の業務継続確認	Ordering Service サーバを 1 台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
6	Kafka サーバの単一障害時の業務継続確認	Kafka サーバを 1 台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
7	Zookeeper サーバの単一障害時の業務継続確認	Zookeeper サーバを 1 台停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
8	全種類のサーバの同時障害時の業務継続確認	全種類のサーバを 1 台ずつ停止させた後、銀行間決済を実行し、正常に処理完了することを確認する。
9	銀行間決済処理シーケンスにおける障害発生時の挙動確認（机上評価）	銀行間決済処理シーケンス上の処理単位に障害発生した場合の挙動・問題がある場合のリカバリ策を整理する。
10	縮退運転時のスループット性能測定（参考値測定）	全種類のサーバを 1 台ずつ停止させた状態でのスループット性能測定を実施し、劣化度合いを確認する。

3.6.2 性能

性能においては、Hyperledger Fabric および今回設計した構成が、新銀行間決済 PF にて求められるスループット性能要求（ピーク時：1,000 tps）を満たすことができるかを中心に評価した。

（1）検証スコープ

性能評価においては、新銀行間決済 PF の純粋な性能を測定することを目的とし、P2P 送金 PF、外部ネットワークはスコープ外として性能評価を実施した。本実証実験での利用において P2P 送金 PF は最小スペック・構成としており、P2P 送金 PF を介したスループット性能測定においては P2P 送金 PF がボトルネックとなり新銀行間決済 PF に適切な負荷をかけることができないこともスコープ外とした一因である。

(2) 評価項目

性能検証における評価項目は以下のとおり。

表 3.6-2 性能検証の評価項目一覧

#	評価項目	確認内容
1	スループット性能測定※ (目標 : 1,000 tps)	負荷クライアントより多重取引を実行し、新銀行間決済 PF が目標 1,000tps を発揮可能か確認する。
2	スループット性能測定 (限界性能)	負荷クライアントより多重取引を実行し、新銀行間決済 PF (実証実験システムの構成、スペックが前提) の限界スループット性能を測定する。
3	取引停止閾値確認	決済用デジタル通貨残高が取引停止閾値付近の銀行に対して、銀行間決済を複数同時実行し、取引停止閾値検知までの挙動を確認する。
4	高負荷時の参照系レスポンス測定	取引履歴が大量に蓄積した場合の決済用デジタル通貨残高取得レスポンスの遅延度合を測定する。

※性能検証においては、スループット性能測定と併せて、新銀行間決済 PF におけるレスポンス性能の測定についても実施した。具体的には、参照系の処理について、残高取得処理が 1 秒未満で完了するかどうか検証を行ったほか、更新系の処理について、銀行間決済処理が 2 秒未満で完了するかどうか検証を行った。

3.6.3 セキュリティ

新銀行間決済 PF は、厳格な価値移転記録、履歴管理が求められる。本検証においては、「耐改ざん性」に着目し、机上・実機での改ざん検証をとおして、新銀行間決済 PF において当該性質が有益たるかどうかを評価した。

(1) 検証スコープ

本実証実験においては、ブロックチェーン環境に対する耐改ざん性を評価した。その他のセキュリティ評価については、本検証での確認観点とはしていないが、一般的なセキュリティ対策は以下のとおり実施済みである。

表 3.6-3 実施済みの一般的なセキュリティ対策

#	セキュリティリスク	セキュリティ対策		導入箇所
1	通信傍受	通信暗号化	TLS	Web ブラウザ - 新銀行間決済 PF 間
2			IPSec-VPN	P2P 送金 PF - 新銀行間決済 PF 間
3			SSL-VPN	SSH クライアント - 新銀行間決済 PF 間
4	不正アクセス	アクセス制御	Firewall (FW)	Firewall
5		不正侵入検知 (IDS) / 防止 (IPS)	IDS/IPS サービス (Trend Micro Deep Security as a Service)	全てのサーバ
6	アプリ脆弱性	WAF	WAF ソフトウェア (Mod Security)	業務サーバ
7	アプリ不正利用	認証	ID/パスワード認証	業務サーバ (Web ブラウザからのリクエスト)
8			ID/パスワード認証	業務サーバ (P2P 送金 PF からのリクエスト)

*図内数字は、上表の#に紐づいている

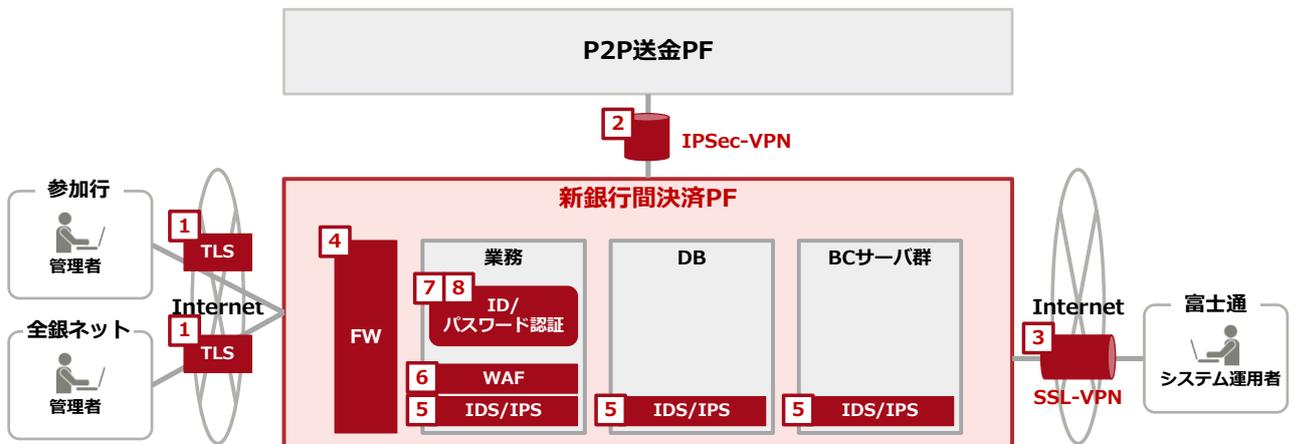


図 3.6-1 セキュリティ対策イメージ

(2) 評価項目

セキュリティに関する評価項目は以下のとおり。

なお、ここでの「改ざん」は、正当な処理フローを通さずに World State を直接更新されることと定義するものである。

表 3.6-3 セキュリティ検証の評価項目一覧

#	評価項目	確認内容
1	改ざん条件・対策の整理 (机上評価)	改ざんが成立する条件およびその条件に対する対策を整理する。
2	改ざん検知の挙動確認	World State を直接更新した後、改ざんが検知可能か確認する。
3	改ざん復旧の挙動確認	World State を直接更新した後、改ざんが復旧可能か確認する。

3.7 非機能検証実施結果

予定した検証項目は全て消化し、複数の問題を検出した。「可用性」「性能」「セキュリティ」ごとに実施結果を示す。

3.7.1 可用性

単一障害時および全種類のサーバの縮退運転時に業務継続可能であることが確認できた。一方で、縮退運転時に縮退割合以上の大幅な性能劣化が発生することを確認した。

表 3.7-1 可用性検証の評価結果一覧

#	評価項目	確認結果 (○：結果 OK, ×：結果 NG, -：判定対象外)
1	業務サーバの単一障害時の業務継続確認	業務サーバの単一障害時においても業務継続可能であることを確認した。 ○
2	DB サーバの単一障害時の業務継続確認	DB サーバの単一障害時においても業務継続可能であることを確認した。 ○
3	EP/CP サーバの単一障害時の業務継続確認	EP/CP サーバの単一障害時においても業務継続可能であることを確認した。 ○
4	CA サーバの単一障害時の業務継続確認	CA サーバの単一障害時においても業務継続可能であることを確認した。 ○

#	評価項目	確認結果	
		(○ : 結果 OK, × : 結果 NG, - : 判定対象外)	
5	Ordering Service サーバの単一障害時の業務継続確認	Ordering Service サーバの単一障害時においても業務継続可能であることを確認した。	○
6	Kafka サーバの単一障害時の業務継続確認	Kafka サーバの単一障害時においても業務継続可能であることを確認した。	○
7	Zookeeper サーバの単一障害時の業務継続確認	Zookeeper サーバの単一障害時においても業務継続可能であることを確認した。	○
8	全種類のサーバの同時障害時の業務継続確認	全種類のサーバを1台ずつ停止させた同時障害時においても業務継続可能であることを確認した。	○
9	銀行間決済処理シーケンスにおける障害発生時の挙動確認 (机上整理)	銀行間決済のいずれの処理タイミングでシステム障害発生した場合においても、リカバリ不能となるケースは存在しないことを確認した。 詳細は「表 3.7-2 障害発生タイミングに対する挙動・リカバリ整理」「図 3.7-1 銀行間決済処理シーケンスにおける障害発生時の挙動確認」を参照。	-
10	縮退運転時のスループット性能測定 (参考値測定)	通常時と比較し、縮退運転時は約 62%の性能劣化が生じることを確認した。(通常時 : 746 tps → 縮退運転時 : 284 tps) 詳細は「表 3.7-3 縮退運転時のスループット性能測定結果」を参照。	-

表 3.7-2 障害発生タイミングに対する挙動・リカバリ整理

サーバ	#	単一障害発生 タイミング	問題 有無	挙動		リカバリ	
				取引不整合 発生有無	リカバリ 可否		
業務	①	Tx 実行準備	無	有	可	P2P 送金 PF の業務サーバがエラーを検知し、エラーメッセージを出力する。 P2P 送金 PF の処理は成立済みであるが、新銀行間決済 PF の処理は実行されないため、PF 間での不整合が生じる。	新銀行間決済 PF の銀行間決済処理を手動実行し、取引不整合を解消する。 (SE 作業)
	②	Tx 実行	無	無	-	P2P 送金 PF の業務サーバがエラーを検知しエラーメッセージを出力する。	-
	③	完了通知	無	無	-	新銀行間決済 PF の処理も実行されるため、PF 間での不整合は生じない。	-
DB	①	DB 参照	無	無	-	新銀行間決済 PF の業務サーバがエラーを検知し、セカンダリ DB サーバより必要情報を取得する。	-
EP/CP	①	残高取得	無	無	-	新銀行間決済 PF の業務サーバがエラーを検知し、正常稼働中の EP/CP サーバより残高を取得する。	-
	②	プロポーザル	無	無	-	新銀行間決済 PF の業務サーバがエラーを検知し、正常稼働中の EP/CP サーバにプロポーザルし、Tx は成功する。	-
	③	ブロック登録	無	無	-	新銀行間決済 PF の業務サーバがブロックコミットのタイムアウトを検知する。 正常稼働中の EP/CP サーバは Tx に成功し、P2P 送金 PF と新銀行間決済 PF 間で不整合は生じない。(障害発生の EP/CP サーバは起動後に自動復旧する)	-
Ordering Service	①	Tx 受付	無	無	-	新銀行間決済 PF の業務サーバがエラーを検知し、正常稼働中の Ordering Service サーバに対し、Tx をブロードキャストするため、Tx は成功する。	-
	②	ブロック生成	無	有	可	Tx が実行されず、取引の不整合が生じる。	新銀行間決済 PF の銀行間決済処理を手動実行し、取引不整合を解消する。 (SE 作業)
Kafka	①	Tx 整列	無	無	-	新銀行間決済 PF の Ordering Service サーバがエラーを検知し、レプリカサーバへ切り替えを行う。	-

原因調査の結果、Hyperledger Fabric は停止済み（縮退対象）のサーバに対しても、毎回通信を発生させており、タイムアウトまで待ち受けていることが判明した。

なお、現時点の最新バージョン 1.4 においても、本件の改善につながる機能エンハンスは公式ドキュメント上、見受けられない。

一方、停止ノードに対してもリクエストを送信する仕様については、ノード復活時にシームレスな業務復帰を望める効果もあり、一概に問題視するものでもなく運用設計と含めて今後考慮すべき事項に当たるものとする。

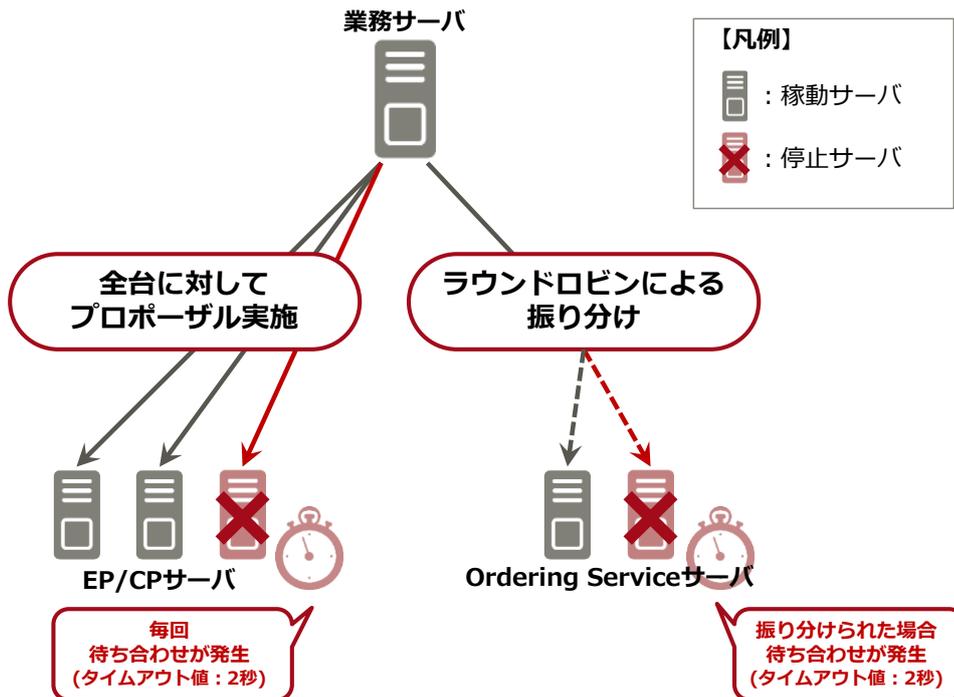


図 3.7-2 縮退運転時の Hyperledger Fabric の挙動イメージ

3.7.2 性能

目標とするスループット性能（ピーク時：1,000 tps）が発揮できることを確認した。一方で、1日当たりの取引数が膨大となった場合に残高取得のレスポンス劣化に関する課題を検出した。

表 3.7-4 性能検証の評価結果一覧

#	評価項目	確認結果 (○：結果 OK, ×：結果 NG, -：判定対象外)	
		1	スループット性能測定※ (目標：1,000 tps)
2	スループット性能測定 (限界性能)	1,099 tps を記録した。 (業務サーバ：6 台、多重度：3,000)	○
3	取引停止閾値確認	決済用デジタル通貨残高を 1,001,000 円としたうえで、500 円送金を集中的に 5 件実施。その結果、先方 3 件が成功、後方 2 件が失敗し、決済用デジタル通貨残高が 999,500 円となったことを確認。 確認の前提として、ブロックチェーンの技術特性（非同期バッチ処理）上、取引処理中の停止閾値検知においては取引中の未確定値を取得してしまう可能性があり、処理が集中する状態においては設定閾値を下回って停止する可能性があることを想定していたが、本検証で、想定どおり取引集中時の検知ラグの顕在化を確認。	○
4	高負荷時の参照系レスポンス測定	約 6 万件の取引明細増加ごとに決済用デジタル通貨残高照会レスポンスが約 850ms 遅延することを確認。 詳細は「表 3.7-5 取引件数と残高照会レスポンスの関係性」を参照。	-

※なお、スループット性能の検証と併せて実施したレスポンス性能の測定においては、目標としていたレスポンス性能（残高取得処理（参照系）：1 秒未満、銀行間決済処理（更新系）：2 秒未満）が発揮できることを確認した。

表 3.7-5 取引件数と残高照会レスポンスの関係性

#	取引件数（件）		残高照会レスポンス（ms）	
	測定値	（増加分）	測定値	（増加分）
1	0	-	43	-
2	62,590	（ + 62,590）	884	（ + 841）
3	118,522	（ + 55,932）	1,724	（ + 840）
4	178,189	（ + 59,667）	2,618	（ + 894）

◆ 検出課題②

#4 の評価において、決済用デジタル通貨残高照会時、取引履歴からの算出対象が大幅に増加した場合、レスポンス遅延が大幅に発生する事象を検出した。本課題は、GUI による残高照会のレスポンス遅延に留まらず、銀行間決済のレスポンス・スループット性能にも影響するものである。

銀行間決済の前処理として、「送金額に対して残高が不足していないかどうか」をチェックする必要があるが、その際最新残高を取得（計算）する必要がある、取得時点で大量の未集計取引履歴が存在している場合に#4 で検出した処理時間が追加的に発生してしまうことになる。考える。（スループット性能検証においては大量の未集計取引履歴が蓄積している状況ではなく、当該問題は顕在化しなかった）

3.7.3 セキュリティ

複数のネットワークセキュリティを突破されなければ改ざんできないこと、および、仮に改ざんされた場合においても、非改ざんノードで合意形成ポリシーを満たせる状態（本実証実験においては、非改ざんノードが 2 台以上）であれば、不整合を発生させることなく、業務用途において、Hyperledger Fabric の耐改ざん性が有効に機能することを確認した。

表 3.7-6 セキュリティ検証の評価結果一覧

#	評価項目	確認結果 (○：結果 OK, ×：結果 NG, -：判定対象外)	
1	改ざん条件・対策の整理 (机上評価)	改ざん条件・対策の整理を実施。	-
2	改ざん検知の挙動確認	非改ざんノードで合意形成ポリシーを満たせる状態であれば、問題ないことを確認。	○
3	改ざん復旧の挙動確認		○

(1) 改ざん条件・対策の整理

改ざんの実現には、World State にアクセスできることが必要である。

これを防止するために本実証実験システムにおいては、複数のネットワークセキュリティ「SSL-VPN 認証」「SSH 接続認証/EP/CP ログイン認証」を設けており、セキュリティ強度としては十分である。

しかし、これらセキュリティを有効に働かせるためには、証明書/ログイン情報の適切な管理が必要である。改ざんに必要な条件は以下のとおり。

表 3.7-7 改ざんの必要条件

#	条件
①	SSL-VPN 証明書を入手し、新銀行間決済 PF との SSL-VPN を確立
②	SSH 証明書および EP/CP ログイン情報（アクセス権限含む）を入手し、EP/CP へ SSH 接続
③	ブロックチェーン/World State (levelDB) へアクセスし、直接更新

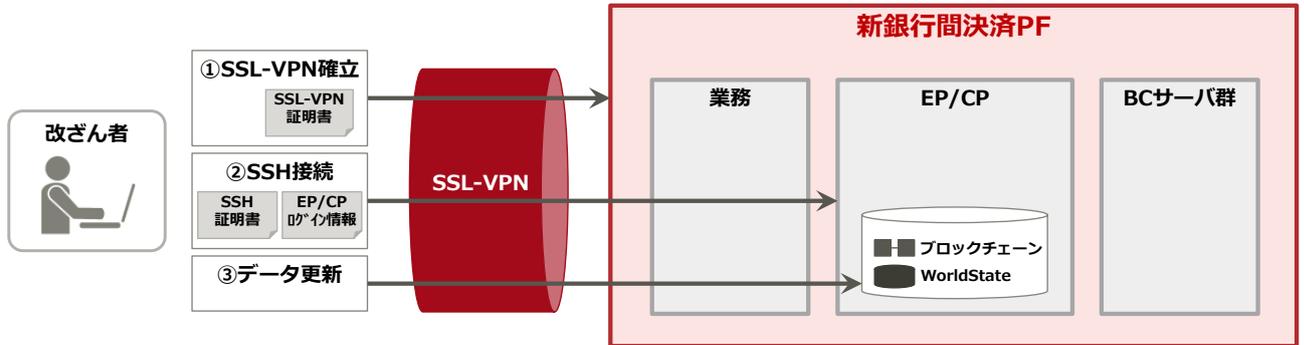


図 3.7-3 改ざんイメージ

(2) 改ざん後の挙動確認

改ざんされた場合を想定し、改ざん値の利用阻止および検知の有無、改ざんの復旧が可能かどうかを実機により確認した。その結果は以下のとおり。

改ざん値利用阻止/改ざん検知可否

改ざん台数	参照処理*1		更新処理*2		改ざん復旧可否
	利用阻止	検知	利用阻止	検知	
1台	○	○	○	○	○
2台	×	○	○	○	×
3台	×	×	×	×	×

*1: 参照系処理においては、アプリ仕様により「プロポーザルした全ノードから得られた値が合意形成ポリシーを満たしているかどうか」をチェックしている
 *2: 更新系処理においては、Hyperledger Fabric仕様により「プロポーザルした全ノードから得られた処理結果が同一の値になっているかどうか」をチェックしている

図 3.7-4 改ざん後の挙動確認結果

3.8 机上検討実施内容・実施結果

本実証実験においては、決済用デジタル通貨を用いた銀行間資金決済（RTGS）に係る機能面・非機能面の検証を行うほか、運用面の観点について机上検討を実施した。本検討を進めるに当たっては、全銀ネットと富士通による検討の論点抽出とディスカッションを経たうえで、全銀ネットブロックチェーン実証実験タスクフォースにおける意見照会を行い、理事行の意見を検討結果に反映させた。

3.8.1 机上検討の実施目的

新銀行間決済 PF に関して、本実証実験における機能面・非機能面の検証において不足する、運用面の検討について机上実施を行うものである。なお、今回の机上検討の粒度については、全体把握のための概要整理に留めるものとし、具体詳細検討は来年度以降の積み残し課題として整理を行うものとした。

3.8.2 机上検討の実施事項

タスクフォースにおいて、以下 3 点について机上検討を実施した。

(1) 決済用デジタル通貨の価値の裏付け方法の検討

本実証実験の検証スコープは新銀行間決済 PF であり、P2P 送金 PF ならびに、決済用デジタル通貨の価値の裏付けを制御するシステムは対象外としている（図 3.8-1 参照）。一方で、銀行間決済専用のデジタル通貨である決済用デジタル通貨は、当該価値が保全されることを前提として、資金清算機関である全銀ネットから加盟銀行に対して発行されるものであり、この特性（決済用デジタル通貨の授受をもって銀行間決済が完了）を踏まえた「価値の裏付け方法」の検討が必要となる。具体的には、現時点で考えられる価値の裏付け方法を選択肢として洗い出し、決済用デジタル通貨の特性等を踏まえ、それぞれの方法のメリット・デメリット等の整理を行うものとした。

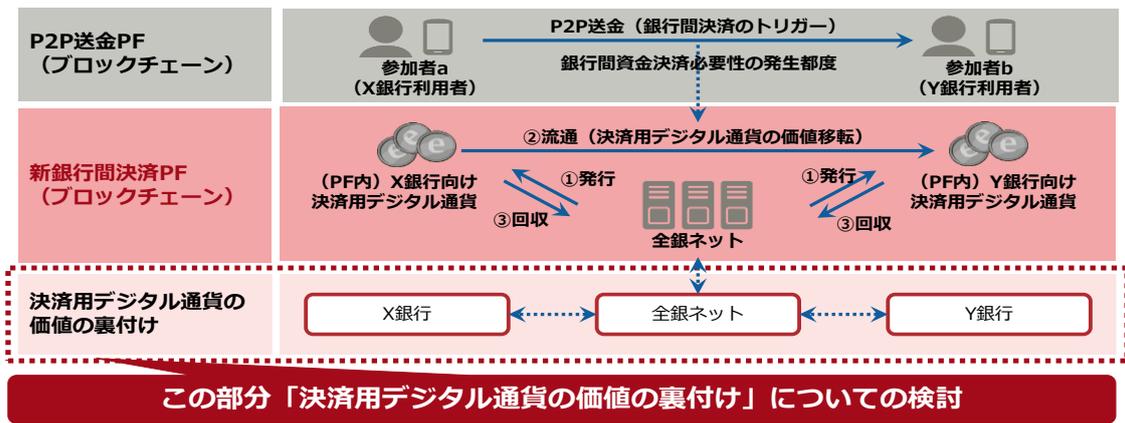


図 3.8-1 決済用デジタル通貨の価値の裏付け方法の検討イメージ

(2) 業務プロセスの概要整理

決済用デジタル通貨運用のサイクルに沿って、基本的な業務プロセスの整理を実施する。具体的には、実証実験のスキームにおける基本的な業務フロー（決済用デジタル通貨の発行・流通・回収）を前提とし、正常系の業務プロセスを想定するものとした。なお、想定する業務プロセスの対象となる資金移動サービスは P2P 送金 PF とし、決済用デジタル通貨の価値の保全は、日銀当預残高を用いることで、前提の仮置きを行った。

(3) 機能要件の概要整理

想定された基本的な業務プロセスを前提として機能要件の整理を実施する。具体的には、想定業務プロセスで必要となる業務タスクの洗い出しを実施し、それぞれのタスクについて新銀行間決済 PF への機能実装の対象（システム化対象）とするかどうかについて整理を行う。

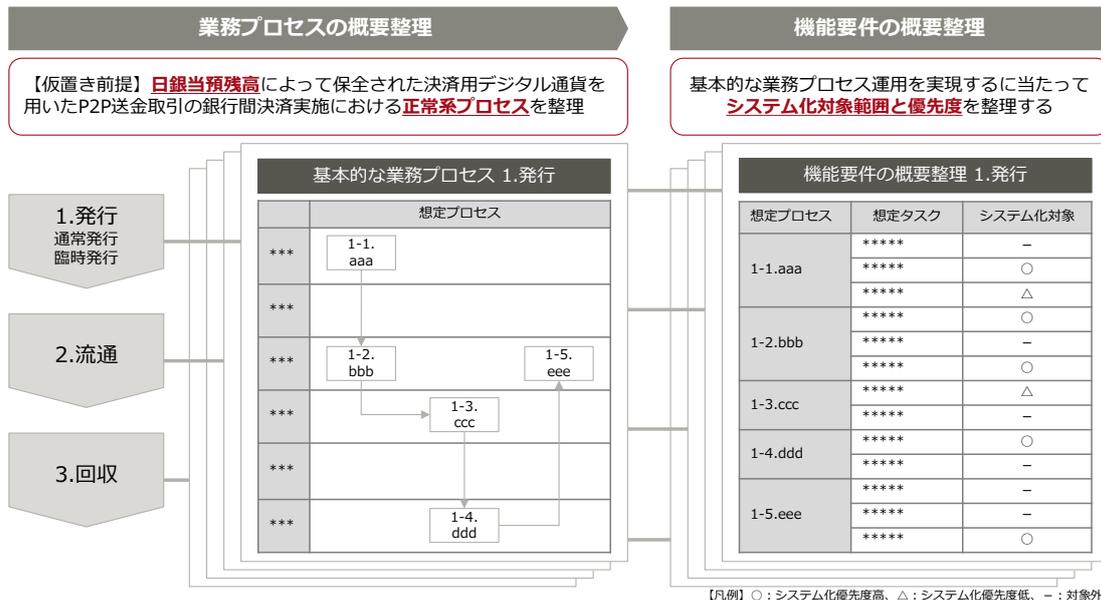


図 3.8-2 基本的な業務プロセス／機能要件の概要整理イメージ

3.8.3 机上検討の実施結果

(1) 決済用デジタル通貨の価値の裏付け方法の検討結果

以下のとおり、現時点で考えられる価値の裏付け方法を選択肢として洗い出し、決済用デジタル通貨の特性等を踏まえ、それぞれの方法のメリット・デメリット等の整理を実施した。ただし、実際に決済用デジタル通貨を発行するに当たっては、以下の整理に加え、資金決済に係る現行の関係制度等に照らした検討を行う必要がある。

表 3.8-1 「価値の裏付け方法」の選択肢/メリット・デメリット整理

項	裏付け方法	方法の概要	メリット	デメリット
1	日本銀行当座預金口座残高	各行が、全銀ネットの日銀当預口座に対して、決済用デジタル通貨発行額の残高振替を実施する方法	<ul style="list-style-type: none"> これまでの現金担保の仕組みと同様の運用が可能のため、システム改修・構築および運用設計が小規模（もしくは不要）となると考えられる。 	<ul style="list-style-type: none"> 日銀当預を保有していない法人の直接接続ができない。
2	仕向超過額管理制度における各行差入担保	仕向超過額管理制度にもとづき設定した限度額内で決済用デジタル通貨を発行する方法	<ul style="list-style-type: none"> 現状の仕向超過額管理制度を利用し運用するため、全銀ネットがコントロール可能な範囲が比較的広い。 	<ul style="list-style-type: none"> 現状の仕向超過額管理に係るシステムと連動させる必要があり、相応のシステム改修が必要となる可能性がある。
3	決済銀行の普通預金残高	全銀ネットが開設している（ある特定の決済銀行の）普通預金口座に対して、各行が決済用デジタル通貨発行額の振込を実施する方法	<ul style="list-style-type: none"> 既存の仕組み（全銀システムを利用した振込）で運用が可能のため、システム改修・構築および運用設計が小規模（もしくは不要）となると考えられる。 日銀当預を保有していない法人においても決済用デジタル通貨発行額の残高振替が可能。 	<ul style="list-style-type: none"> 口座開設先の銀行のシステム・事務体制に依存することとなり、当該銀行に対する各種リスク管理が必要となる。 決済用デジタル通貨発行額分の資金が口座開設先の銀行に保有されるため、当該銀行破綻時に、当該資金が全額保全されないおそれがある。
4	信託	特定の信託銀行等、外部機関へ資金を積み立てる方法	<ul style="list-style-type: none"> 制度設計によっては、柔軟な運用が可能となる。 日銀当預を保有していない法人においても決済用デジタル通貨発行額の残高振替が可能。 	<ul style="list-style-type: none"> 新たな枠組みおよび制度の設計、外部機関を利用するメリットの整理、外部機関との調整等が必要となる。

(2) 業務プロセスの概要整理結果

決済用デジタル通貨の運用に係る基本的な業務フロー（決済用デジタル通貨の発行・流通・回収）を前提とし、正常系の業務プロセスをフロー図に落とし込むことで想定を行った。なお、想定する業務プロセスの対象となる資金移動サービスはP2P送金PFとし、決済用デジタル通貨の価値の裏付けは、日本銀行当座預金残高を用いることで、前提の仮置きを行っている。

◆ 決済用デジタル通貨の発行

決済用デジタル通貨の発行における現実的な運用として、前営業日までに各加盟行から発行額の決定ならびに当該申請が実施され、全銀ネットが申請内容を確認したうえで発行オペレーションを実施する日跨ぎの運用とした。またプロセスの想定に当たって、定常業務として日次実施が想定される「通常発行」と、決済用デジタル通貨の不足時等に日中都度実施される「臨時発行」のプロセスを区別して整理した。

通常発行

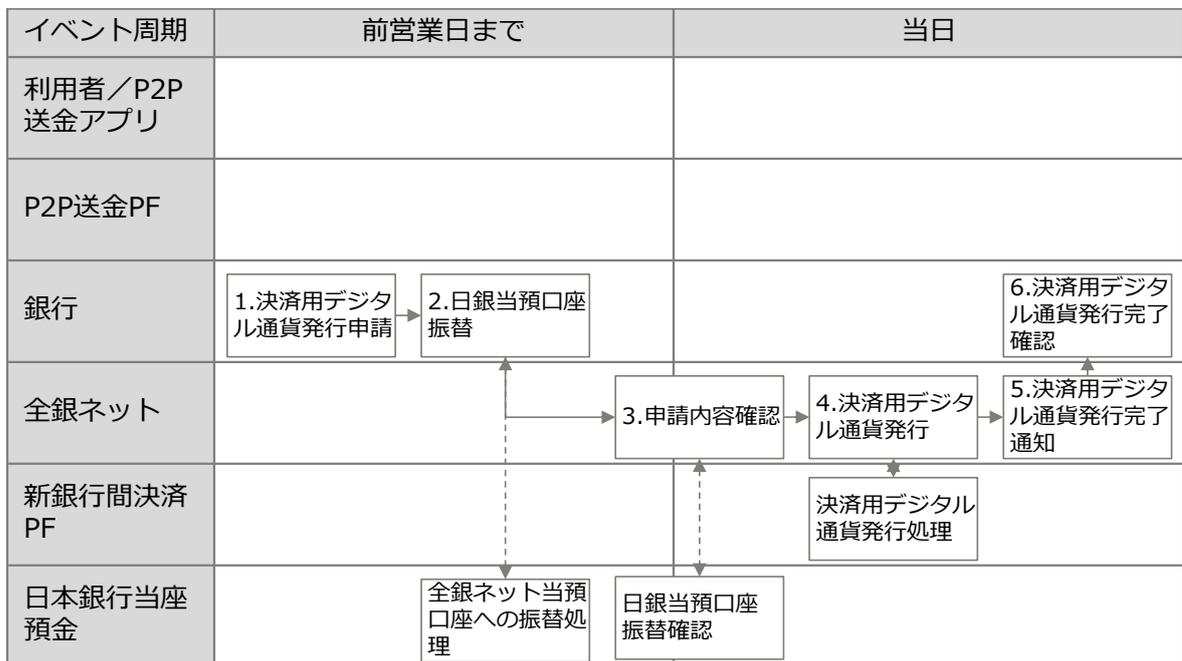


図 3.8-3 「決済用デジタル通貨の通常発行」業務プロセス

表 3.8-2 「決済用デジタル通貨の通常発行」業務プロセス主体と概要

分類	#	プロセス	主体	プロセスの概要
通常発行	1	決済用デジタル通貨発行申請	銀行	翌日以降の決済用デジタル通貨発行の申請を行う
	2	日銀当預口座振替	銀行	決済用デジタル通貨の発行額にもとづき、全銀ネットの日銀当預口座へ振替を行う
	3	申請内容確認	全銀ネット	当該銀行からの申請内容と全銀ネットの日銀当預口座への振替を確認する
	4	決済用デジタル通貨発行	全銀ネット	当該銀行へ決済用デジタル通貨の発行指図を行う (新銀行間決済 PF 上で発行処理が行われる)
	5	決済用デジタル通貨発行完了通知	全銀ネット	当該銀行へ決済用デジタル通貨発行の完了を通知する
	6	決済用デジタル通貨発行完了確認	銀行	決済用デジタル通貨が発行されたことを確認する

臨時発行

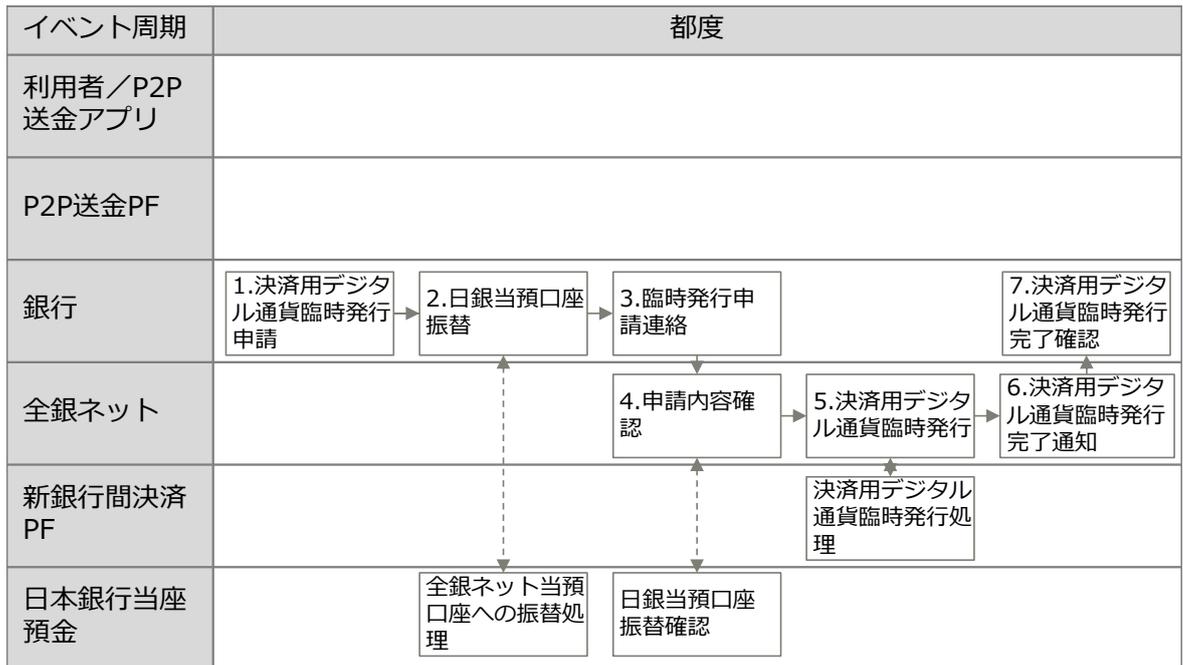


図 3.8-4 「決済用デジタル通貨の臨時発行」業務プロセス

表 3.8-3 「決済用デジタル通貨の臨時発行」業務プロセス主体と概要

分類	#	プロセス	主体	プロセスの概要
臨時発行	1	決済用デジタル通貨臨時発行申請	銀行	決済用デジタル通貨の臨時発行の申請を行う
	2	日銀当預口座振替	銀行	決済用デジタル通貨の臨時発行額にもとづき、全銀ネットの日銀当預口座へ振替を行う
	3	臨時発行申請連絡	銀行	全銀ネットへ決済用デジタル通貨の臨時発行の申請に係る連絡を行う
	4	申請内容確認	全銀ネット	当該銀行からの申請内容と全銀ネットの日銀当預口座への振替を確認する
	5	決済用デジタル通貨臨時発行	全銀ネット	当該銀行へ決済用デジタル通貨の発行指図を行う（新銀行間決済PF上で発行処理が行われる）
	6	決済用デジタル通貨臨時発行完了通知	全銀ネット	当該銀行へ決済用デジタル通貨臨時発行の完了を通知する
	7	決済用デジタル通貨臨時発行完了確認	銀行	決済用デジタル通貨が臨時発行されたことを確認する

◆ 決済用デジタル通貨の流通

決済用デジタル通貨の流通プロセスの想定に当たっては、P2P送金ならびに決済用デジタル通貨の決済が問題なく行われた場合を想定した。



図 3.8-5 「決済用デジタル通貨の流通」業務プロセス

表 3.8-4 「決済用デジタル通貨の流通」業務プロセス主体と概要

分類	#	プロセス	主体	プロセスの概要
流通	1	P2P 送金指図	P2P 送金 PF (利用者)	P2P 送金アプリにより、受取人への P2P 送金指図を行う
	2	P2P 送金処理	P2P 送金 PF	送金依頼人から受取人への P2P 送金処理が行われる
			P2P 送金 PF (利用者)	P2P 送金アプリにより、受取人への送金が完了したことを確認する
	3	決済用デジタル通貨決済指図	P2P 送金 PF	P2P 送金 PF から新銀行間決済 PF に対し決済用デジタル通貨決済指図が行われる
4	決済用デジタル通貨決済処理	新銀行間決済 PF	決済用デジタル通貨決済の処理が行われる	
			新銀行間決済 PF から P2P 送金 PF に対し決済用デジタル通貨決済完了の通知が行われる	

◆ 決済用デジタル通貨の回収

決済用デジタル通貨の回収における現実的な運用として、前営業日までに各加盟行から回収額ならびに当該申請が実施され、全銀ネットが申請内容を確認したうえで回収オペレーションを実施する日跨ぎの運用とした。

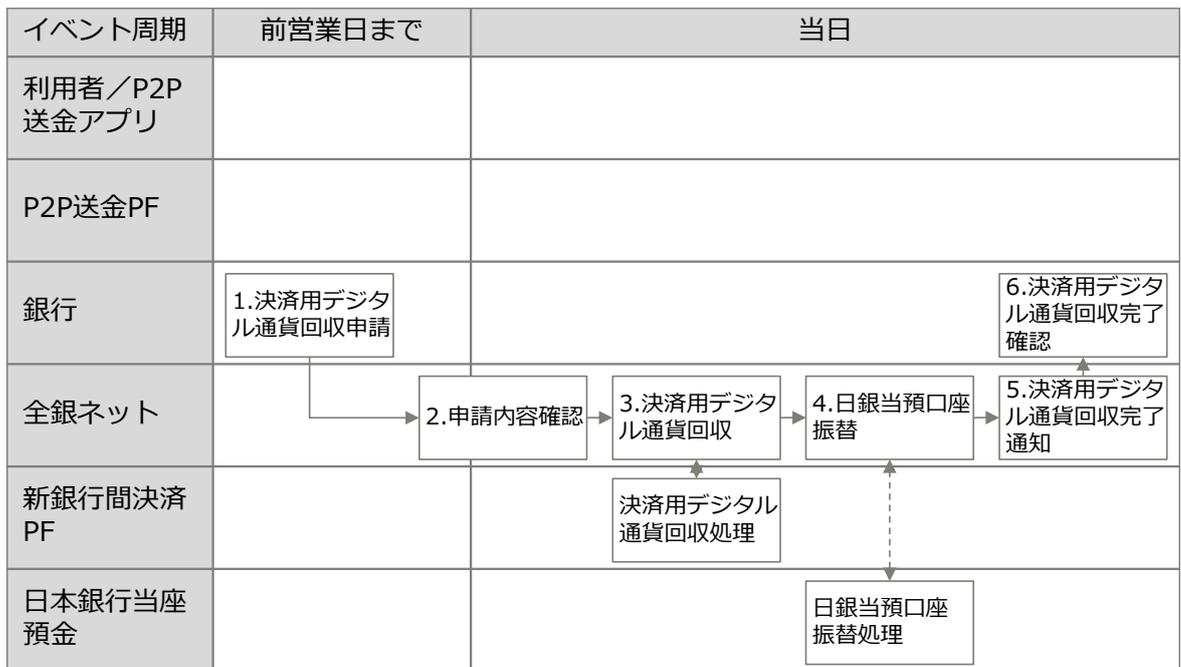


図 3.8-6 「決済用デジタル通貨の回収」プロセス

表 3.8-5 「決済用デジタル通貨の回収」業務プロセス主体と概要

分類	#	プロセス	主体	プロセスの概要
回収	1	決済用デジタル通貨回収申請	銀行	翌日以降の決済用デジタル通貨回収の申請を行う
	2	申請内容確認	全銀ネット	当該銀行からの申請内容を確認する
	3	決済用デジタル通貨回収	全銀ネット	決済用デジタル通貨回収指図を行う (新銀行間決済 PF 上で回収処理が行われる)
	4	日銀当預口座振替	全銀ネット	当該銀行の日銀当預口座へ振替を行う
	5	決済用デジタル通貨回収完了通知	全銀ネット	当該銀行へ決済用デジタル通貨回収の完了を通知する
	6	決済用デジタル通貨回収完了確認	銀行	決済用デジタル通貨が回収されたことを確認する

(3) 機能要件の概要整理結果

想定された基本的な業務プロセスを前提として機能要件の整理を実施した。具体的には、想定業務プロセスで必要となる業務タスクの洗い出しを実施し、それぞれのタスクについてシステム化の対象（新銀行間決済 PF への機能実装の対象）とするかどうかについて整理を行った。

システム化の対象整理に当たっては、それぞれのタスクに対して、システム化の対象範囲と優先度を「○（優先度高）／△（優先度低）／－（対象外）」として評価／分類を実施した。「△」は、システム化が可能ではあるものの、メール連絡等による代替が可能なものとし、「－」はすでに他のシステムに実装されている等、新銀行間決済 PF への実装が機能重複となるケース等を想定した。

◆ 決済用デジタル通貨の発行

通常発行

表 3.8-6 「決済用デジタル通貨の通常発行」のシステム化対象となる業務タスク

分類	#	プロセス	主体	プロセスの概要	業務タスク	システム化
通常発行	1	決済用デジタル通貨発行申請	銀行	翌日以降の決済用デジタル通貨発行の申請を行う	決済用デジタル通貨残高照会	○
					日銀当預口座残高確認	-
					決済用デジタル通貨発行額決定	-
					決済用デジタル通貨発行申請	△
	2	日銀当預口座振替	銀行	決済用デジタル通貨の発行額にもとづき、全銀ネットの日銀当預口座へ振替を行う	日銀当預口座振替	-
	3	申請内容確認	全銀ネット	当該銀行からの申請内容と全銀ネットの日銀当預口座への振替を確認する	決済用デジタル通貨発行申請受付	△
					決済用デジタル通貨発行申請内容確認	△
					日銀当預口座振替確認	-
	4	決済用デジタル通貨発行	全銀ネット	当該銀行へ決済用デジタル通貨の発行指図を行う (新銀行間決済 PF 上で発行処理が行われる)	決済用デジタル通貨発行オペレーション	○
	5	決済用デジタル通貨発行完了通知	全銀ネット	当該銀行へ決済用デジタル通貨発行の完了を通知する	決済用デジタル通貨発行処理完了通知	△
	6	決済用デジタル通貨発行完了確認	銀行	決済用デジタル通貨が発行されたことを確認する	決済用デジタル通貨残高照会	○
					決済用デジタル通貨履歴明細照会	○

臨時発行

表 3.8-7 「決済用デジタル通貨の臨時発行」のシステム化対象となる業務タスク

分類	#	プロセス	主体	プロセスの概要	業務タスク	システム化
臨時発行	1	決済用デジタル通貨発行申請	銀行	決済用デジタル通貨の臨時発行の申請を行う	決済用デジタル通貨残高照会	○
					日銀当預口座残高確認	-
					決済用デジタル通貨臨時発行額決定	-
					決済用デジタル通貨臨時発行申請	△

分類	#	プロセス	主体	プロセスの概要	業務タスク	システム化
	2	日銀当預口座振替	銀行	決済用デジタル通貨の臨時発行額にもとづき、全銀ネットの日銀当預口座へ振替を行う	日銀当預口座振替	-
	3	臨時発行申請連絡	銀行	全銀ネットへ決済用デジタル通貨の臨時発行の申請に係る連絡を行う	電話・メール連絡	-
	4	申請内容確認	全銀ネット	当該銀行からの申請内容と全銀ネットの日銀当預口座への振替を確認する	決済用デジタル通貨臨時発行申請受付	△
決済用デジタル通貨臨時発行申請内容確認					△	
日銀当預口座振替確認					-	
	5	決済用デジタル通貨臨時発行	全銀ネット	当該銀行へ決済用デジタル通貨の発行指図を行う (新銀行間決済 PF 上で発行処理が行われる)	決済用デジタル通貨臨時発行オペレーション	○
	6	決済用デジタル通貨臨時発行完了通知	全銀ネット	当該銀行へ決済用デジタル通貨臨時発行の完了を通知する	決済用デジタル通貨臨時発行処理完了通知	△
	7	決済用デジタル通貨臨時発行完了確認	銀行	決済用デジタル通貨が臨時発行されたことを確認する	決済用デジタル通貨残高照会	○
決済用デジタル通貨履歴明細照会					○	

◆ 決済用デジタル通貨の流通

表 3.8-8 決済用デジタル通貨流通のシステム化対象となる業務タスク

分類	#	プロセス	主体	プロセスの概要	業務タスク	システム化
流通	1	P2P 送金指図	P2P 送金 PF (利用者)	P2P 送金アプリにより、受取人へのP2P送金指図を行う	受取人指定	-
					P2P 送金金額入力	-
					P2P 送金指図	-
	2	P2P 送金処理	P2P 送金 PF	送金依頼人から受取人へのP2P送金処理を行う	P2P 送金指図受付	-
					送金依頼人アカウントから受取人アカウントへのP2P送金処理	-
			P2P 送金 PF (利用者)	P2P 送金アプリにより、受取人への送金が完了したことを確認する	アプリの残高、履歴明細の確認	-
	3	決済用デジタル通貨決済指図	P2P 送金 PF	P2P 送金 PF から新銀行間決済 PF に対し決済用デジタル通貨決済指図が行われる	決済用デジタル通貨決済指図の受領	○
	4	決済用デジタル通貨決済処理	新銀行間決済 PF	決済用デジタル通貨決済の処理が行われる	仕向銀行から被仕向銀行への決済用デジタル通貨決済処理	○
				新銀行間決済 PF から P2P 送金 PF に対し決済用デジタル通貨決済完了の通知が行われる	決済用デジタル通貨決済完了通知	○

◆ 決済用デジタル通貨の回収

表 3.8-9 決済用デジタル通貨回収のシステム化対象となる業務タスク

分類	#	プロセス	主体	プロセスの概要	業務タスク	システム化
回収	1	決済用デジタル通貨回収申請	銀行	翌日以降の決済用デジタル通貨回収の申請を行う	決済用デジタル通貨残高照会	○
					決済用デジタル通貨回収額決定	-
					決済用デジタル通貨回収申請	△
	2	申請内容確認	全銀ネット	当該銀行からの申請内容を確認する	決済用デジタル通貨回収申請受付	△
					決済用デジタル通貨回収申請内容確認	△
	3	決済用デジタル通貨回収	全銀ネット	決済用デジタル通貨回収指図を行う (新銀行間決済 PF 上で回収処理が行われる)	決済用デジタル通貨回収オペレーション	○
	4	日銀当預口座振替	全銀ネット	当該銀行の日銀当預口座へ振替を行う	日銀当預口座振替	-
5	決済用デジタル通貨回収完了通知	全銀ネット	当該銀行へ決済用デジタル通貨回収の完了を通知する	決済用デジタル通貨回収完了通知	△	
6 7	決済用デジタル通貨回収完了確認	銀行	決済用デジタル通貨が回収されたことを確認する	決済用デジタル通貨残高照会	○	
				決済用デジタル通貨履歴明細照会	○	

4 プロジェクト活動考察

本実証実験を通じた、ブロックチェーン技術の有効性、課題、銀行間資金決済ならびに決済用デジタル通貨スキームにおける活用可能性について述べる。

4.1 ブロックチェーン技術の活用可能性

決済用デジタル通貨を用いた銀行間資金決済（RTGS）を実現していくに当たって、機能面については、ブロックチェーン技術活用は可能（正しく機能する）であることが確認できた。一方で、非機能面においては、下記に述べる有効性と課題が抽出された。

銀行間資金決済ならびに決済用デジタル通貨スキームにおけるブロックチェーン技術適用については、本実証実験結果に加えて、後述する積み残し課題を踏まえた継続的な検討を進めていく。

4.1.1 非機能面の有効性

(1) 可用性

単一障害時および全種類のサーバの縮退運転時における業務継続性を確認した。

(2) 性能

目標とするスループット性能（ピーク時：1,000tps）を達成した。

(3) セキュリティ

本業務用途において、非改ざんノードで合意形成ポリシーを満たせる状態において Hyperledger Fabric の耐改ざん性は十分に機能することを確認した。

ノードの改ざんに当たっては、ネットワークや認証等に係る複数のセキュリティを突破し、World State へ直接アクセスする必要がある。さらに、合意形成ポリシーを満たすに足るノード数を直接かつ同時に更新を行うことが必要となるため、大量のトランザクションが処理されているブロックチェーンネットワーク内において、過半数のノードを同時に改ざんすることは現実的に困難であると考えられる。

4.1.2 非機能面の課題

(1) 可用性

縮退運転時に大幅な性能劣化が発生する。当該事象は、Hyperledger Fabric の仕様にもとづくものであり、現時点の最新バージョンにおいても本件の解決はなされていないと見受けられることから、今後の継続的なモニタリングならびに、必要に応じて運用機能による停止サーバの切り離しなどの対応を行っていく必要があるものとも考える。

(2) 性能

今回採用した処理方式においては、取引数が増加した場合のレスポンスが低下する。GUI レスポンスのみならず、取引全体のレスポンス・スループット性能に影響する。

レスポンス遅延の要因は、送金額に対する残高チェックを取引都度実施しているためであり、本課題解決に当たっては、決済用デジタル通貨のリスク管理/残高管理のあり方も含めた解決策の検討が求められる。

(3) セキュリティ

上述のとおり、複数のセキュリティが突破され、合意形成ポリシーを満たすノード数が同時に改ざんされるリスクは極めて低いものの、論理的にゼロではない。さらにセキュリティの維持は、ブロックチェーンのみならず、証明書やユーザ権限等の適切な管理が必要となることから、運用面を含めた継続的な対策の実施が求められる。

5 今後に向けて

本報告書においては、実証実験の実施内容・実施結果（「3. プロジェクト活動結果報告」）およびその考察（「4. プロジェクト活動考察」）を述べてきた。本章は、それらを踏まえ今回の実証実験での「主な積み残し課題」を整理するとともに、今回の実証実験を振り返ったうえで、「今後の取組みの方向性」について言及する。

5.1 主な積み残し課題

本項は、今回の実証実験で解決することのできなかった「積み残し課題」について述べる。「積み残し課題」はその性質上、「実証実験によって明らかになった検討課題」と「実証実験のスコープ外として不足している検討課題」に分類できることから、それぞれの概要を以下のとおり整理した。

5.1.1 実証実験によって明らかになった検討課題

前述のとおり、実証実験を通じて以下の検討課題が明らかになった。

(1) 機能性

机上検討からの抽出観点および参加銀行からのフィードバックを考慮した新銀行間決済 PF に具備すべき機能の選定・実装検証。

(2) 可用性

縮退運転時の大幅な性能劣化に対する整理および運用回避。

(3) 性能

ブロックチェーン技術の採否検討も視野に入れた、処理方式の再検討を含めた残高チェックのレスポンス・スループット劣化への対応。

(4) セキュリティ

システム全体の運用面を含めた継続的なセキュリティ対策。

5.1.2 実証実験のスコープ外として不足している検討課題

前述のとおり、今回の実証実験の目的は、ブロックチェーン技術を活用した新たな銀行間決済（小口取引における RTGS）の仕組みの有効性について検証することであった。

今回の実証実験で得られた知見・経験をもとに、次年度以降の取組みにつなげていくためには、これまで本報告書で述べてきた技術面の課題のほか、以下のような検討課題が存在すると思われる。

(1) 新銀行間決済プラットフォームのユースケースに係る検討

- ・新銀行間決済プラットフォームの具体的なユースケースの検討
- ・ユースケースを踏まえた、利用者および関係者の整理

(2) 新制度／ルール面に係る検討

- ・ユースケースや利用者・関係者を踏まえた制度面の検討
- ・決済用デジタル通貨の法的位置付け（価値の裏付け方法を含む）の整理
- ・ユースケースを踏まえた、信用リスク・流動性リスク管理等の対応

(3) 機能要件／非機能要件に係る検討

- ・各種業務プロセス・リスク管理方法の具体化
- ・新銀行間決済プラットフォームで実装すべき機能要件と他のシステム（新銀行間決済プラットフォームに連携）で実装すべき機能要件の整理
- ・ユースケースを踏まえ想定される取引量やセキュリティ要件等の把握と非機能要件への落とし込み

5.2 今後の取組みの方向性

本報告書で述べてきたとおり、今回の実証実験を通じ、ブロックチェーン技術を活用した新たな銀行間決済（小口取引における RTGS の実現）の仕組みの有効性について確認できたことに加え、ブロックチェーン技術そのものの特性についても確認することができた。その一方で、前述のとおり、「ブロックチェーン実証実験タスクフォース」における議論・検討や実証実験の結果・考察から想起される「積み残し課題」があり、それらについては、次年度以降の検討課題となる。

全銀ネットは、資金決済システムを運営する国内唯一の資金清算機関として、今回の実証実験で得

られた知見・経験を、より具体化した取組みにつなげていくため、2018 年度全銀ネット有識者会議において有識者から示唆・提言があった「インターオペラビリティの確保」という点も念頭に置きながら、銀行業界の協調領域である「銀行間資金決済」の効率性向上に関する検討、次世代の資金決済システムのあり方に関する検討を持続的に進めていく必要がある。

また、その検討においては、国を挙げたキャッシュレス化の推進（2025 年までにキャッシュレス比率を 4 割とする目標が掲げられている）や、昨今の個人間送金（P2P 送金）を取り巻く状況、具体的には、足許様々なプレイヤーがサービスを提供している状況を踏まえつつ、検討を進めることも重要である。

以上を踏まえ、次年度以降の取組みの具体的な方向性として、今回の実証実験によって明らかになったブロックチェーン技術に関する課題について、技術動向をフォローするとともに、例えば、新銀行間決済プラットフォームに関する検討を進めるに当たって重要な技術の一つである API 接続等に関する調査・研究も実施しつつ、次のステップとして、第 3 次中期経営計画（2019 年度～2021 年度）における具体的課題の一つである「次世代の資金決済インフラの構築に向けた検討」の一環として、新銀行間決済プラットフォームにおけるユースケース等の検討を行うこととする。

以 上