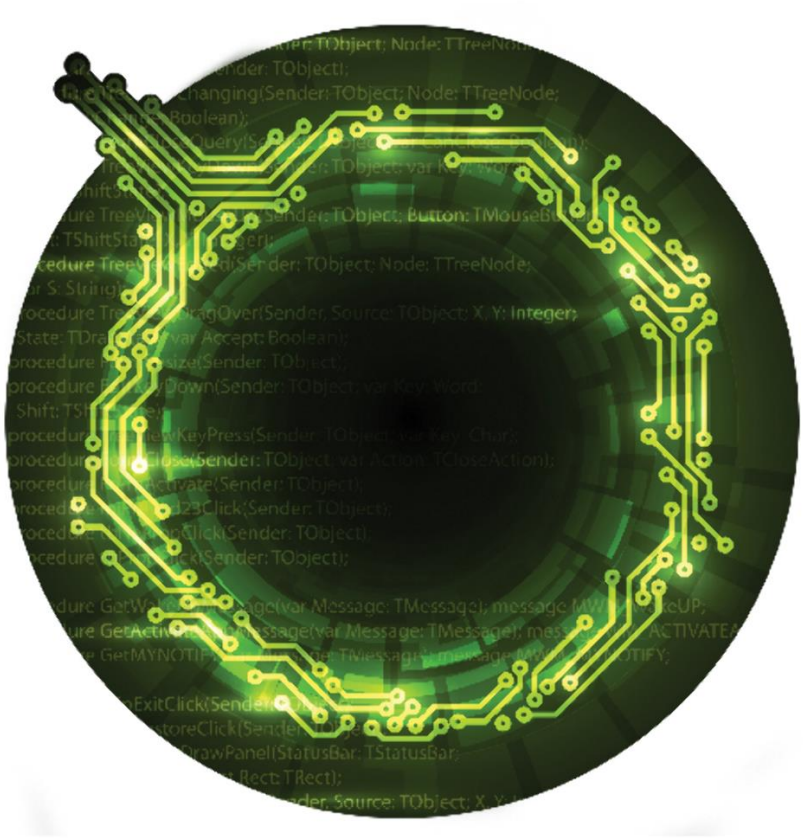

# ブロックチェーン技術を活用した本人確認（KYC）高度化プラットフォーム構築の実証に係る報告書


**ブロックチェーン研究会**

株式会社みずほフィナンシャルグループ

株式会社三井住友フィナンシャルグループ

株式会社三菱 UFJ フィナンシャル・グループ

デロイト トーマツ グループ



2018 年 7 月 13 日

## 1. ブロックチェーン研究会の概要

### (1) 研究会設立の背景と目的

昨今、金融業界においては、金融と IT の融合による技術革新である FinTech の発展が著しく、これによる既存金融サービスの代替、これまでにない革新的な金融サービスの台頭が見受けられる。中でも、ビットコイン等の仮想通貨に用いられるブロックチェーン技術は、取引における「改ざん耐性」「高可用性」等の特性から、送金・決済・証券取引等に係る業務との親和性が高く、今後の金融分野への活用が強く期待されている。

このブロックチェーン技術においては、金融業界を中心に実証実験を始めとした技術研究が盛んであり、当該技術の実用化及びデファクトスタンダードの獲得に向けた競争がグローバル下で激化しており、特に、欧米金融機関において強い積極性が見られる。

この様な状況の中、ブロックチェーン技術を日本が今後も継続的に成長するための 1 つの技術的な要素として捉え、国内金融機関がその技術の礎を築くことに貢献すると共に、欧米金融機関に比肩する水準まで技術レベルを高めていくことを当研究会における最終目標に据え、2015 年 12 月に金融システムに対するブロックチェーン技術の活用可能範囲の特定及び、実用化に向けた方向性を定めることを目的とした、ブロックチェーン研究会を設立した。

### (2) 研究会の位置づけ

ブロックチェーン研究会には、株式会社みずほフィナンシャルグループ、株式会社三井住友フィナンシャルグループ、株式会社三菱 UFJ フィナンシャル・グループ、デロイト トーマツ グループが参画し、ブロックチェーン技術の研究を推進している。

当研究会では、ブロックチェーン技術を適用しうる銀行業務を選定しプロトタイプを作成した上で、動作確認／稼働検証、評価を行う。これにより、ブロックチェーン技術が有用であることが立証されれば、将来的な実用化に向けた正式な仕様に発展させていくことも視野に入れる。

プロトタイプの作成においては、特定のブロックチェーン事業者の技術に依拠するのではなく、当研究会において抽出した要件を基にブロックチェーン事業者を複数社より選定し、技術協力を得て実施するものとしている。

なお、当研究会の基本スタンスとしては、ブロックチェーン技術の研究により実用化の方向性を定めることで、国内金融業界の発展に寄与することを目指すものである。

### (3) 今回のテーマ

ブロックチェーン研究会は、2016 年 11 月に報告書をまとめた「国内の銀行間振込業務におけるブロックチェーン技術の実証」[1]に続く、新たな研究「本人確認（KYC：Know Your Customer）高度化プラットフォームにおけるブロックチェーン技術の適用に関する実証」を 2017 年 7 月から 2018 年 3 月にかけて実施した。

「本人確認」は、マネー・ローンダリング対策（AML：Anti-Money Laundering）やテロ資金供与対策（CFT：Combating the Financing of Terrorism）、経済制裁対応に関係するものとして国際的に規制が強化されている。国内においても個人を対象とするものを含め、厳格化が進められており、それに伴い金融機関の事務処理が増えることが想定される。そこで、金融機関が共通利用できるインフラを整備することなどによって、本人確認の効率化と高度化を進めることが期待される。

こうした背景に鑑み、本研究会では「改ざん耐性」「高可用性」等の特性から、本人確認の効率化への親和性が高いと期待されているブロックチェーン技術を活用した「本人確認（KYC）高度化プラットフォーム構築」を新たな研究テーマとし、その技術を用いた本人確認システムのプロトタイプの作成と、仕様の決定を目指すこととした。効果検証においては、要件の充足性（機能実現性・性能・セキュリティ 等）、コスト低減効果等を検証観点に据え、ブロックチェーン技術を用いた新たなシステムの有用性を本研究会で評価した。

[1] ブロックチェーン研究会による「国内の銀行間振込業務におけるブロックチェーン技術の実証実験に係る報告書」について（2016 年 11 月 30 日発表）
https://www2.deloitte.com/jp/ja/pages/about-deloitte/articles/news-releases/nr20161130.html

## 2. 実証実験の評価と考察

### (1) 概要

現状、各金融機関で行っている経済制裁対象者リスト等への照合作業等を新たに設立する共同運営機関（以降、コンソーシアム）で行うとともに、取引を行なおうとする顧客の意思表明の下、当該顧客の本人確認を既に実施した他の金融機関に本人確認済みの顧客である旨を確認すること等により、本人確認等の事務手続きを簡素化する仕組みを設けることを想定した。

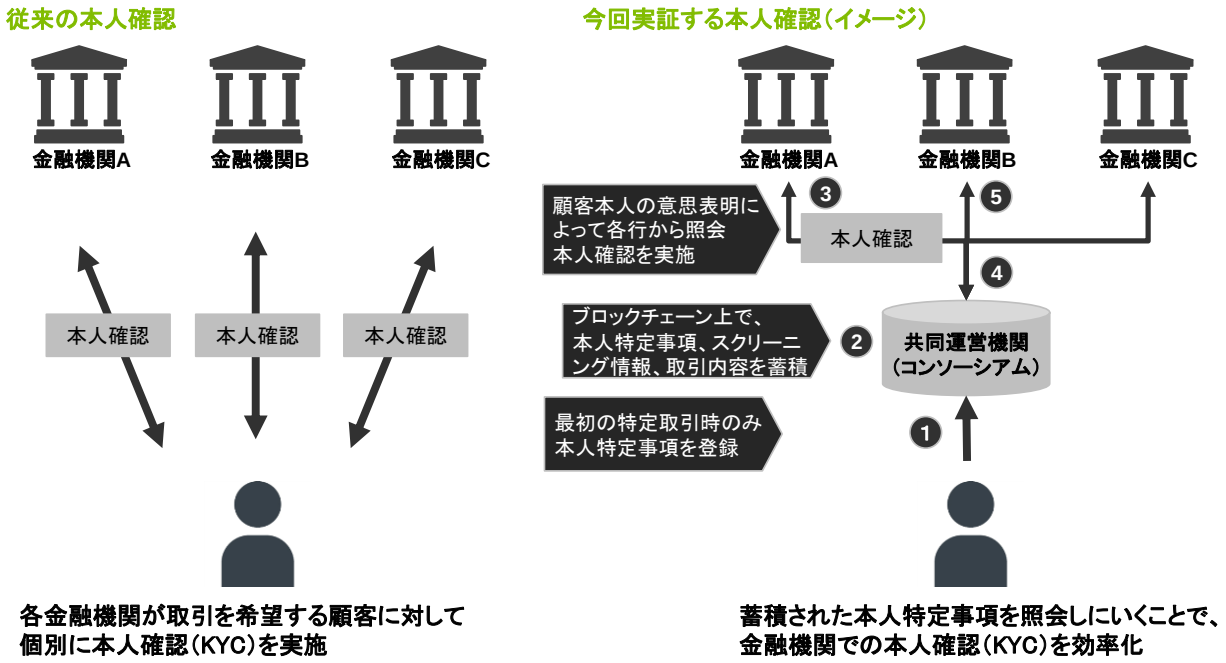


図 1　実証で行う本人確認（KYC）の仕組みの模式図

### (2) 具体的な仕組み

顧客がコンソーシアムに参加する金融機関と新規に取引を行う場合を想定したものを示す。コンソーシアムに参加する金融機関と既に取引を行っている既存顧客の取扱いについては今後の検討課題とした。

1. 顧客は特定取引[2]を実施する前に、コンソーシアムの Web 登録フォームから必要な本人特定事項の登録申請[3]を実施。
2. コンソーシアムは、経済制裁対象者リスト等のフィルタリング/スクリーニング[4]を実施。該当がない場合、該当無（以下、フィルタリング/スクリーニング情報）をブロックチェーン上に記録。
3. 当該顧客が金融機関 A において特定取引を実施しようとする際は、顧客からの意思表明[5]によって、コンソーシアムから金融機関 A に当該顧客の本人特定事項とフィルタリング/スクリーニング情報を引渡し。金融機関 A が当該顧客の本人確認を実施するとともに、上記情報を参考に取引可否を判断[6]（顧客の本人確認時にブロックチェーン上の記録に誤りがあることが判明した場合には、コンソーシアムで顧客に差し戻しを行い再度1の手続きを実施）。
4. 金融機関 A は、口座開設などの特定取引を実施した場合には、コンソーシアムを介して、ブロックチェーン上の顧客情報に実施した取引内容を記録。
5. 当該顧客が金融機関 B において特定取引を実施しようとする際は、顧客からの意思表明によって、コンソーシアムから金融機関 B に当該顧客の本人特定事項とフィルタリング/スクリーニング情報を引渡し。金融機関 B

[2] 本実証実験における特定取引は、口座開設時を想定。
[3] 実証実験では個人顧客に限定し、本人特定事項ならびに本人確認に伴う付属情報、確認書類画像（運転免許証）の登録を想定。
[4] 本実証実験においては、以下の定義を用いる。フィルタリング=顧客より受け渡された本人特定事項と制裁者等リスト（財務省リストに記載されている項目をもとに、将来拡張されることを前提にテストデータを作成）を照合し、「該当しない」（リストにヒットしないことであり、調査・判断は含まない）」または「それ以外」を抽出。スクリーニング=蓄積された本人特定事項とリストを照合し「該当しない（フィルタリングと同様）」または「それ以外」を抽出。その後各行の判断により、ホワイトまたはブラックを判定する。
[5] 本人確認情報登録完了の証左として取得したデジタル証明書を顧客が提示することを想定
[6] 金融機関 A が独自に追加収集した情報も含め判断。

は、コンソーシアムを介して当該顧客が金融機関 A で本人確認済みであることを確認[7]し、当該確認をもって金融機関 B での本人確認とすることも可能とする（各金融機関の判断）（なお、その際、金融機関 B は、当該顧客が同様の取引を様々な金融機関で実施していないかなど、ブロックチェーン上に記録された当該顧客の取引履歴を参照し、なりすましのおそれがないかどうかを検証）。

### (3) 構築した実験環境

利用者（個人顧客）の本人特定事項の登録、コンソーシアムによる登録内容照合・管理、金融機関による登録情報の照会、口座開設情報の登録/照会機能をブロックチェーン技術で実装し検証（一部は机上検証）した。本実証実験では Hyperledger Fabric[8]の利用を前提とし、全銀協ブロックチェーン連携プラットフォーム上に環境を構築した。

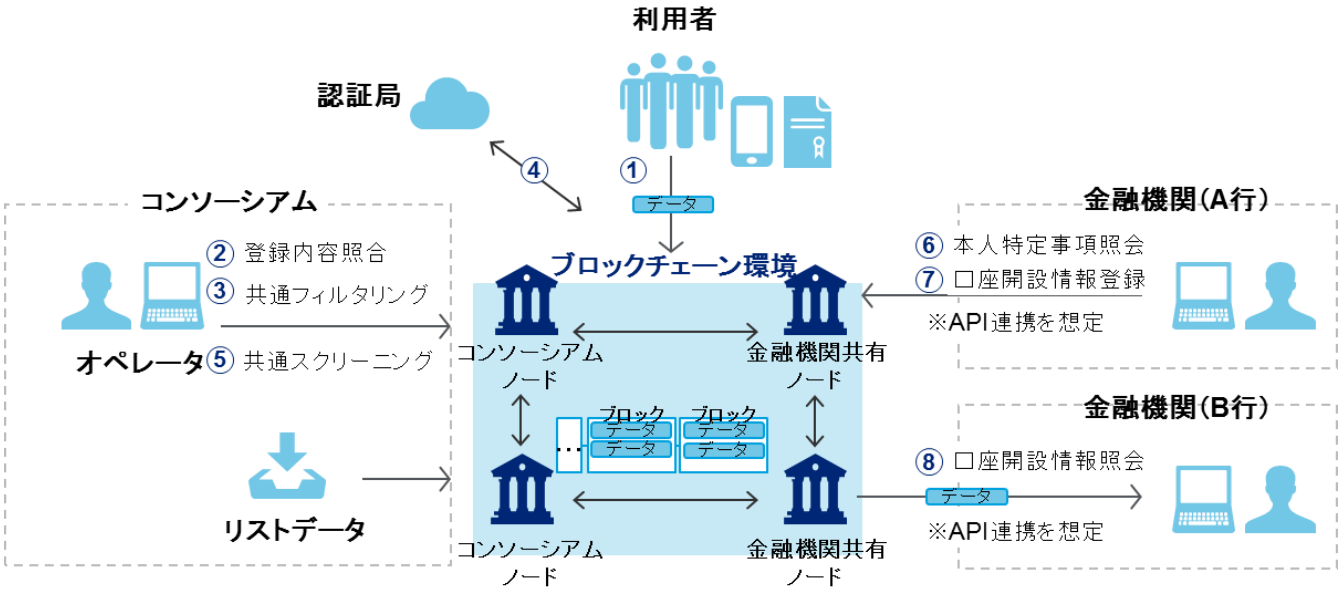


図 2　構築した実験環境イメージ

表 1　実験環境に実装した主要機能の概要

| 機能 | 説明 |
|---|---|
| ① 本人特定事項登録 | ・利用者は、Web 登録フォームで本人特定事項を入力し、ブロックチェーン環境へ送信 |
| ② 登録内容照合 | ・コンソーシアムは、ブロックチェーン環境へ登録されたデータを参照し、登録内容に関する不備等をチェックする |
| ③ 共通フィルタリング | ・リストデータ（実証実験では財務省リストで実施）でフィルタリング処理し、「該当無し」「その他（完全一致/部分一致）」の判定および補足コメントをブロックチェーン環境へ保存 |
| ④ デジタル証明書発行 | ・認証局からデジタル証明書を取得し利用者へ通知 |
| ⑤ 共通スクリーニング | ・リストデータが更新されると登録されている全件に対して、スクリーニング処理を行い、結果（フィルタリング同）をブロックチェーン環境へ保存 |
| ⑥ 本人特定事項照会 | ・口座開設申込みを受けた金融機関（A 行）は、利用者の本人特定事項をブロックチェーン環境へ照会 |
| ⑦ 口座開設情報登録 | ・金融機関（A 行）は、独自フィルタリング／スクリーニング処理の結果、口座を開設した場合はその旨の情報を登録（結果、開設不可となった場合は他行に参照できない形式で登録） |

[7] 金融機関 B がコンソーシアムを介して顧客の口座開設状況を確認する際、開設済の金融機関（ここでは金融機関 A）の名称を把握できるか否かについては今後検討。（本実証実験では匿名（金融機関 X の様な表記）で実施した）

[8] Hyperledger Fabric は ブロックチェーン フレームワーク インプリメンテーションで、The Linux Foundation がホストする Hyperledger のプロジェクトの 1 つです。

| 機能 | 説明 |
|---|---|
| ⑧ 口座開設情報照会 | ・ 金融機関（B 行）は、他行で口座開設されている情報を確認し、独自フィルタリング／スクリーニングを銀行判断で一部省略し、口座開設事務を実施する |

(4) **実証実験の参加者**

実証実験の検証スコープや要件はプロジェクトオーナ、メンバ（3 メガバンク/地銀/証券会社/デロイト）が検討・決定し、これに基づき日立/全銀協がシステム構築を行う。オブザーバは論点等の意見・助言を実施した。

**プロジェクトオーナ（ブロックチェーン研究会）**

- 株式会社みずほフィナンシャルグループ
- 株式会社三井住友フィナンシャルグループ
- 株式会社三菱 UFJ フィナンシャル・グループ
- デロイト トーマツ グループ

**プロジェクトメンバ** ※五十音順

- SMBC日興証券株式会社
- 大和証券株式会社
- 株式会社千葉銀行
- 野村證券株式会社
- 株式会社福岡銀行
- みずほ証券株式会社
- 三菱UFJモルガン・スタンレー証券株式会社

**機能・環境提供**

- 日立製作所グループ
- 一般社団法人全国銀行協会[9]

**オブザーバ**

- 金融庁
- 日本銀行

(5) **検証結果・考察**

Ⅰ) **業務面**

**<u>法的位置づけの考え方</u>**

業務観点では KYC のコアプロセスである「本人特定事項の収集」「本人確認」を軸に有効性と利便性に鑑みて、コンソーシアムが果たす役割（責任）を法的位置づけと紐づけて優先して整理を行った。

| | 本人特定事項の収集 | 本人確認（本人特定事項の確認） | リスト照合 | 取引方針の策定 | 記録保存 | 継続的な顧客管理 |
|---|---|---|---|---|---|---|
| 主な業務内容 | ➢本人特定事項と証跡書類の入手（対面・非対面） | ➢本人特定事項の確認（対面）<br>➢上記事項＋本人限定受取郵便の送付・受領確認（非対面） | ➢リストとの照合（システム検知）<br>➢照合結果の判定（目検による判定） | ➢AMLリスク評価（未実施事業者含む）<br>➢取引可否判断（総合判断）<br>➢リスク軽減措置導入（必要に応じて） | ➢本人特定事項や担当者、確認方法、記録作成者等の記録<br>➢7年間の保管 | ➢本人特定事項変更およびリスト更新時の悉皆スクリーニング<br>➢取引モニタリング、リスク評価見直し（定期・都度）、他 |

図 3　一般的な本人確認（KYC）業務フロー

[9]全銀協ブロックチェーン連携プラットフォーム環境を提供

基本的な考え方として、本人確認（実在性と同一性の確認）の有効性が、現状水準、または当局目線を充足する水準以上に担保されること、利用者（顧客、事業者）にとっての利便性に考慮する必要があることを前提とした。

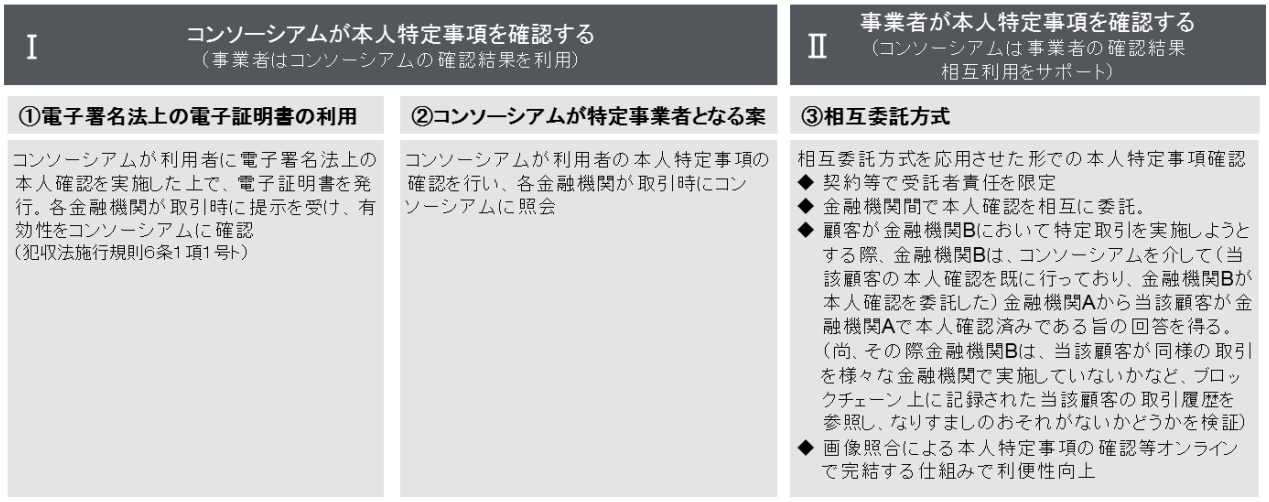


図 4　法的位置づけの取り得るパターン

**<u>法的位置づけに関する考察</u>**

「①電子署名法上の電子証明書の利用」については、電子署名法上、電子証明書の発行機関は、その発行に際して、（ア）顧客から本人確認書類の提示を受ける方法（対面）、（イ）顧客宅に本人限定受取郵便を送付し、顧客からその返送を受ける方法、（ウ）公的個人認証による方法のいずれかで顧客の本人確認を行う必要がある。（ア）・（イ）では本人確認がオンラインで完結しない等、利用者利便性に課題があると認識した。一方、利便性の高い仕組みとして、公的個人認証の活用について検討を深める必要があると認識した。

「②コンソーシアムが特定事業者となる案」は、そもそも本人確認は犯罪収益移転防止法に基づき「特定事業者」が本人確認を実施する必要があるため、顧客との間で特定取引を行なうわけではないコンソーシアムが当該法が定める「特定事業者」として本人確認を実施する選択肢は、困難であると認識した。

「③相互委託方式」については、本人確認を他の金融機関に委託することに抵抗がある先もあるとの意見があった。これについては、図4で記した金融機関 A が顧客の本人確認が完了した後、ブロックチェーン上に当該顧客の本人確認書類の画像を登録し、金融機関 B が当該顧客と特定取引を行なう際に、金融機関 A への本人確認の委託に加え、任意に自らもブロックチェーン上に登録された当該顧客の本人確認書類に不審な点がないか検証を行う仕組みとすることで対応することが考えられるとの意見があった。

一方、金融機関間の委託内容（契約形態・義務等）の明確化等については、今後、検討を深めていく必要があると認識した。

なお、「③相互委託方式」の適法性に関して、犯罪収益移転防止法施行令13条では、「特定事業者 B が特定事業者 A に委託して顧客と特定取引を行なう場合、A が過去の取引の際に当該顧客の本人確認を実施しており、本人確認記録を保存していれば、再度の本人確認は不要（本人確認済みの確認で足る）である」旨規定されている。この点に関して、当該規定の「委託」には、契約締結権までを委託せず、本人確認手続きのみを委託することも含まれるとの解釈を今般、当局から得ており、法令上も問題ないと考えられる。

### Ⅱ) システム面

システム面では、今回の実証実験において検証できた範囲は限られているものの、現段階で致命的な欠陥は確認されず、本人確認（KYC）高度化プラットフォームの実運用への適用可能性があるものと考えられる。

**<u>機能観点</u>**

機能面では今回要件として定義したレベルの簡易的[10]な本人確認（KYC）高度化プラットフォームに対しては、ブロックチェーン技術が十分に適用可能であることが検証された。ユーザ利便性を考慮した複数の要件（ユーザビリティ改善、異例ケースへの対応等）を基に段階的にプロトタイプや仕様の改善を図り、一定の効果があ

[10] 一部限定的・条件付で構築した環境、ならびに業務面もフィルタリング対象を制裁者等リスト（財務省リストに記載されている項目をもとに、将来拡張されることを前提にテストデータを作成）等、簡易的な水準での実験結果であることの意

る事を UAT（実機検証）を通じて確認した。今後実用化に向けてユーザ利便性の向上に対する継続的な取り組みが必要であると考えられる。

**非機能観点**

性能においては、共通スクリーニング相当のバッチ処理性能評価を実施し、本人情報登録や口座開設におけるブロックチェーン情報参照等のオンライン処理への影響を考慮の上、共通スクリーニングのバッチ処理運用時間を工夫することで、今回要件とした範囲（1,000 金融機関、約 1,000 万件/年（3 万件/日））に対して、適用可能性があることを確認した。

実用化に向けてはスループットの観点で、大容量データや暗号化情報をスクリーニング処理する際に発生する性能劣化に対し、画像分離やスケールアウト/スケールアップ構成の検討が必要である事、また機器保守性の観点で、安定稼働・性能値モニタリング等のための機能が Hyperledger Fabric 標準にはないため、OSS[11]との連携や Hyperledger Fabric コミュニティの議論を踏まえた検討が必要である事を確認した。これらに対しては、今後も継続的に検討を進めていくことが必要と考えられる。

[11] Open Source Software : ソフトウェアのソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェア

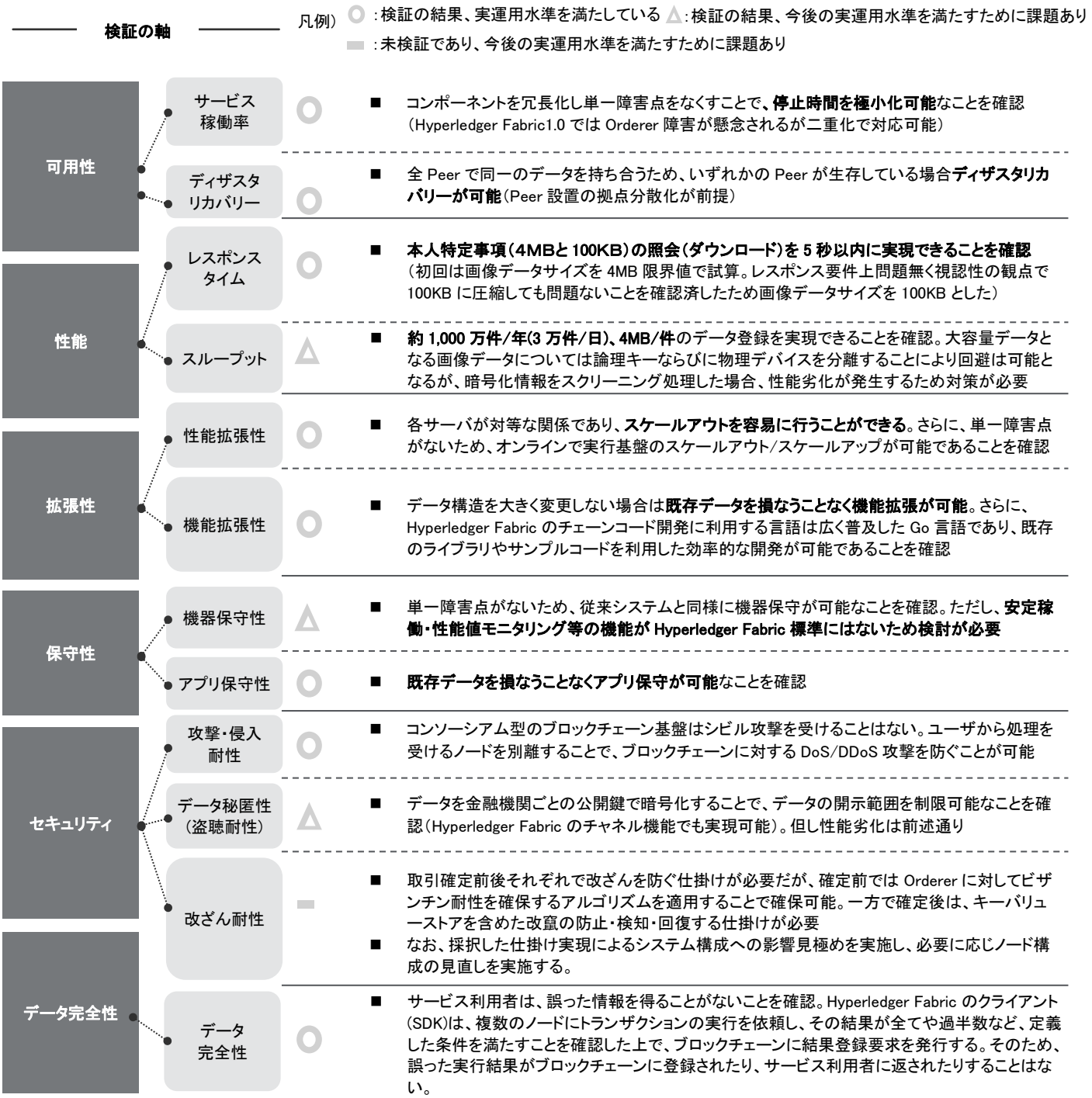


図 5　非機能要件の検証軸と検証結果概要

**コスト観点**

現状の本人確認業務に費やす業務量とコンソーシアムが構築された際の業務量の比較から、期待されるコスト削減額、また実験環境の実用化を想定した際のシステム構築導入費用と、期待されるコスト削減費用を比較しその度合を検証する想定であるが、現時点ではコンソーシアムが担う業務内容が明確には定まっておらず、付随して必要となるブロックチェーン機能を特定できないことから、今回の実証実験では一次的な試算を実施するにとどめた。また、記録表の保管を共通化（コンソーシアム保管）した場合には一定のコスト削減効果がある事を共有した。

(6) **今後の課題と論点**

抽出したブロックチェーン技術を活用した本人確認（KYC）高度化の課題に対しては、今後の論点を明らかにした上で継続的に検討を重ねていくことで、実運用への適用の方向性が精緻化されていくものと想定される。

**業務面**

a. 法的位置づけ

「本人確認の有効性」と「利用者の利便性」に鑑みてコンソーシアムの法的位置づけについて、複数の論点を認識した（法的位置づけに関する考察参照）ため、今後も継続的に検討していく必要がある。

b. 組織のあり方

コンソーシアムの担い手・組織について検討していく必要がある（ISAO[12]としての整理も視野）。また、本枠組みへの参加規約を検討していく必要がある。

**c.** 陣容・スキル

コンソーシアムの立ち位置や役割によっては AML 専門人材の登用も視野に入れる必要がある。

d. リスト照合対応

コンソーシアムが提供するサービスとしての可能性は否定しないものの、照合ロジックや判定基準は共有化に馴染まない領域であることを認識。今後、コンソーシアムがリスト照合対応を行う必要性や妥当性から検討する必要がある。

**e.** 継続的顧客管理

本人特定事項変更（住所変更等）の一括処理への関与や確認記録作成・保存への関与等を検討していく必要がある。

**システム面**

**機能観点**

f. 利用ユーザを想定したユーザビリティの改善

「住所等自動入力支援機能の充実」、「本人確認書類からの文字情報自動読み取り」や「撮影動画から公的書類の表面加工や側面情報読取り真贋確認」等、目視確認に頼らない機械認識の実現可能な技術の検討や、本人確認書類としてパスポート等運転免許証以外の取り扱い範囲を検証していく必要がある。

g. 本人個人の確認・特定のトレーサビリティの改善

本人情報の鮮度や変更イベントを含むトレーサビリティ確保の実現可否を実機確認し、他の付加価値の有無を検証する。また生体認証の組み合わせにより、同一性確認の精度（本人確認する上で必要な水準）の向上を継続的に検討していく必要がある。

h. 認証局連携、マイナンバー制度との連携

NFC 経由でのマイナンバーカード読み取り可能な既存機種(Android)を用いて、KYC コンソーシアムと

[12] ISAO とは、サイバー上の脅威に関するリスクや過去のインシデント、ベストプラクティス等を共有し連携して体制強化を目指す取り組み、あるいはかかる動きを支援する組織（ISAO）やその基準（ISAO SO）のこと。大量の個人情報を取り扱うコンソーシアムの組織形態も ISAO 基準を意識した検討が望まれる

JPKI テスト環境とを繋いだ接続実証実験を行い、今後も継続的に技術・運用上の課題を洗い出すことも考えられる。

**非機能観点**

i. データの秘匿性対策

暗号化データをブロックチェーン基盤に登録すると、データベースの高速な検索機能を利用できないことや、アプリケーション(チェーンコード)での復号処理のオーバヘッドにより、トランザクション処理性能が劣化する。これらを踏まえ、スケールアウト/スケールアップや暗号化不要なシステム設計[13]による対応を検証していく必要がある。

j. スループット性能対策

大容量データであるほどあいまい検索の性能が低下することから、地理的に分散されたノード間における合意形成の遅延時間を考慮した性能検証についても検討が必要である。

**k.** 機器保守性向上

安定稼働と性能問題検出・分析のためには、性能値や各コンポーネントのリソース使用状況などのモニタリングが必須であるが、現状の Hyperledger Fabric はそのような機能を提供していない。また、各コンポーネントは冗長構成が可能だが、Fabric-ca[14]、Peer、Orderer は、それ自身が死活監視や接続先の管理、処理振り分けのための機能を有しているわけではない。そのため、既存の OSS との連携等や Hyperledger Fabric コミュニティでの死活監視の実現方法に関する議論を踏まえた Hyperledger Fabric ネットワーク全体の運用を検討する必要がある。

**コスト観点**

**l.** 想定される新たな業務フローの明確化や、本人確認関連書類の保存・管理コスト削減など、現行業務との比較・効率化の観点から、今後も引き続き精査が必要である。また、コスト削減の観点だけでなく、情報参照に対しては、データ提供により利用料を受け取る仕組みを検討するなども考えられる。また、本スキームにおける更なるコスト削減が期待されるなら、ブロックチェーン以外の技術も視野に入れたシステム構成の検討が必要

[13] 今回の実証実験では、データの暗号化による金融機関間のデータ参照権限を制御する方式としたが、データの共有範囲を制御する方式も選択の候補。Hyperledger Fabric1.0 では、データ共有相手を限定するチャネル機能があり、Hyperledger Fabric の次期バージョンに向けては、データ共有相手を制御する方式が議論されている。また、データベース上のデータを暗号化しないことで、今後、高度な検索機能(インデックスなど)を持つデータベースが利用可能となり、性能向上が見込める。これらを踏まえ、どのような方式が望ましいかは今後の論点として検討

[14] Hyperledger Fabric における認証局。ブロックチェーンのネットワークにおいてユーザ管理を行い、証明書の発行を行う。Fabric-CA により証明書を発行されたユーザのみがネットワークに参加しトランザクションを発行できる。

## 3. まとめ

ブロックチェーン技術を活用した本人確認（KYC）高度化プラットフォーム構築の実証を通して、ブロックチェーン技術の活用により、今回要件として定義したレベルの簡易的な本人確認は十分に適用可能であることが確認された。ただし、実用化を目指すためには利用者の需要性や利便性、法的な論点等、様々な課題が存在することも認識した。

当研究会としては、今回の実証実験で得られた示唆に基づき、本人確認業務へのブロックチェーン技術の適用性の検証と実用化に向けた方向性の検討を、上記様々な課題を踏まえ引続き進めていくかを検討する。

最後に、本資料(実験結果のサマリ)を公開することで、広く実用化に向けたコメントが寄せられること、そして、金融業界において今後も多くの実証実験が繰り返され、ブロックチェーン技術の向上に貢献することを期待する。

## Appendix（用語集）

| No. | 用語 | カテゴリー | 説明 |
|---|---|---|---|
| 1 | ブロック | ブロックチェーン（一般） | ブロックチェーンにデータを記録していく単位。複数のトランザクションが取りまとめられ、1つのブロックに格納される。ブロックに格納されたトランザクションは承認済み(覆せない)の状態となる。 |
| 2 | ブロックチェーン | ブロックチェーン（一般） | 過去から現在までのブロックが時系列でつながったもの。 |
| 3 | コンセンサスアルゴリズム | ブロックチェーン（一般） | ノードによるトランザクションの正当性検証と承認(ブロックの生成)の仕組み。ビットコインの「プルーフ・オブ・ワーク」を筆頭に様々な方式が存在する。 |
| 4 | ノード | ブロックチェーン（一般） | ブロックチェーンの P2P ネットワークに接続される(ブロックチェーンを用いたサービスを利用する)サーバなどの通信機器。 |
| 5 | シビル攻撃 | ブロックチェーン（一般） | ネットワーク内に複数のIDを持ち、異なる主体であるようにみせかけて、参加者の合意形成に不当な影響を及ぼそうとする攻撃。 |
| 6 | ビザンチン障害 | ブロックチェーン（一般） | メッセージの未達や改ざん等任意の障害のこと。たとえば、悪意のある参加者が、全体として正しい合意形成をさせないよう故意に偽の情報を伝達する場合に生じる。 |
| 7 | 台帳(Ledger) | Hyperledger Fabric（コンポーネント） | 過去のすべてのトランザクション実行結果が適用されたデータ。基本的にすべての参加者が同一の台帳を保持する。 |
| 8 | Orderer | Hyperledger Fabric（コンポーネント） | トランザクション実行順序を確定し、ブロックとしてそれらをまとめ、Peer に配信するモジュール。トランザクション実行順序の確定はいくつかの実装をプラガブルに利用でき、たとえば Kafka を利用できる。 |
| 9 | Peer | Hyperledger Fabric（コンポーネント） | トランザクションの実行(Chaincode の実行)や、台帳の管理を行うモジュール。 |
| 10 | Chaincode | Hyperledger Fabric（コンポーネント） | トランザクション処理内容が定義されたスマートコントラクトプログラム。開発者がアプリケーションに応じたロジックを Chaincode として作成する。 |
| 11 | Fabric-CA(Membership) | Hyperledger Fabric（コンポーネント） | Hyperledger Fabric における認証局。ブロックチェーンのネットワークにおいてユーザ管理を行い、証明書の発行を行う。Fabric-CA により証明書を発行されたユーザのみがネットワークに参加しトランザクションを発行できる。 |
| 12 | クライアント（SDK） | Hyperledger Fabric（コンポーネント） | ユーザからの要求を契機として、Peer へのトランザクション発行と Orderer へのトランザクション実行結果確定依頼を行うプログラム。 |
| 13 | Endorsement ポリシー | Hyperledger Fabric | どのような条件を満たしたらトランザクション実行結果を正当なものとして認めるかどうかを定義したポリシー。Peer は、ポリシーを満たすトランザクション実行結果を台帳に反映する。ポリシーは、トランザクションを実行するべき組織や実行するべき Peer の数から構成される。複数組織の複数 Peer でのトランザクション実行を必須とすることで、トランザクション実行結果の信頼性を高められる。 |
| 14 | キーバリューストア | ソフトウェア | バリューというデータ値とバリューを一意に特定できるキーをひとつとして格納されるデータベース方式。一意に特定できる性質上データ値を素早く取り出せる特徴がある |
| 15 | Kafka | ソフトウエア | 高スケーラブルな分散メッセージングシステム。Orderer におけるトランザクション実行順序確定のための実装として利用されている。OSS であり、ブロックチェーン以外でも利用されている。 |