2016 年 9 月
日本銀行決済機構局

第 1 回 FinTech フォーラム（8 月 23 日）議事概要

（エグゼクティブ・サマリー）

日本銀行は、8 月 23 日に「第 1 回 FinTech フォーラム」を開催しました。

今回のフォーラムでは、生体認証システムのセキュリティ評価とブロックチェーン技術の安全性について活発な議論を行いました（参加企業・団体一覧は別紙参照）。

生体認証の技術面では、人工物を利用した所謂「なりすまし」のリスクに対応するため、多様なセンサーを搭載するスマートフォンを活用した複数の認証を組み合せるアイディアが報告されました。また、身体的特徴である生体情報の漏えいリスクに対応し、暗号化した状態での生体情報登録や照合等の処理を行う取組みも紹介されました。セキュリティ面では、評価の尺度・手法の標準化が確立されておらず、複数システムの横並びでの評価や脆弱性であるか否かの判断が難しい領域がある点や、国際標準化に向けた取組みが進められていることが報告されました。

ブロックチェーン技術については、セキュリティ上の課題が整理されたほか、秘密鍵を紛失した場合の対処として、秘密鍵を複数持つ技術の紹介がありました。また、貿易金融やサプライチェーンへの活用の動きが紹介されました。特に、証券決済において、関係者が約定内容や決済状況をブロックチェーン上に登録することを通じて、情報を共有する仕組みが紹介され、ブロックチェーンを「情報の伝達」に利用するという可能性の広がりが感じられました。

もっとも、ブロックチェーンの安全性を検証して実運用に移すには、なお多くの課題が残されており、スピード感をもった対応が必要との考察も示されました。特に、金融サービスへの活用に当たっては、ブロックチェーンが参加者間相互のパブリック型での情報共有が前提とされる中、必要な情報を必要な参加者だけに閲覧可能となるよう、情報の秘匿性を適切に確保する技術が必要との声が多数聞かれました。また、The DAO 事件[1]については、問題への対応がパブリック型のブロックチェーン全体の信頼性の問題に繋がり得る点が指摘されました。

[1] The DAO とは、ブロックチェーンプラットフォームであるイーサリウムのネットワーク上に組成された事業ファンド。本年 6 月、プログラムの脆弱性を狙って不正送金が繰り返され、約 50 億円が詐取された。その対応としてハードフォーク（ブロックチェーンを不正以前に巻き戻すこと）が行われたが、反対運動が起こるなど、非中央集権的な枠組みの下でのコンセンサス形成に課題があることが浮き彫りとなった。

１．日本銀行総裁　黒田東彦による挨拶（和文、英文）

２．プレゼンテーションと質疑
～FinTech における生体認証技術の可能性と留意点～

○　各社からのプレゼンテーションに続き、ディスカッションが行われた。

（１）「生体認証システムのセキュリティ評価と国際標準化― FinTech における活用を展望して―」（日本銀行：宇根）

（説明の概要）

わが国における金融サービスでは、ATM における本人確認の手段として静脈のパターンを用いた方式が採用されるなど、生体認証システムの活用が広がってきている。こうした本人認証のシステムでは「なりすまし」への対策が必須であり、とりわけ生体認証システムにおいては個人の生体特徴を再現する「人工物」を使用した攻撃に留意する必要がある。実際、複数の市販の製品・システムにおいて人工物による攻撃が可能となるケースが報告されている。

こうしたなか、わが国では産官連携プロジェクトとして、生体認証システムの評価・認証の実現を目指した活動が始まっている。本プロジェクトでは、人工物等を用いた攻撃への対策や評価尺度等の国際標準化が検討されており、2016 年度中には静脈パターンを用いたシステムの評価が試行される見通し。生体認証システムの評価・認証制度を活用し、FinTech 等におけるセキュリティ・ガバナンスや顧客の安心感の向上につなげていくことが期待される。

＜ディスカッションにおける主な意見等＞

（生体認証システムのセキュリティ評価手法）

- 人工物等を用いた攻撃として、入国審査における指紋による本人確認において人工指を用いて不正に入国しようとした事例等が現実に報告されている。生体認証システムのセキュリティ評価手法の確立が喫緊の課題である。
- 生体認証システムのセキュリティは、想定されるアプリケーションや攻撃者に基づいて評価されるものである。しかしながら、現時点では、人工物を用

いた攻撃にかかるセキュリティの評価尺度が標準化されておらず、横並びでの評価が難しいのが実情。

（生体認証システムのセキュリティ評価にかかる国際標準化）

- 金融サービスにかかる技術の国際標準化を担う ISO/TC68（国内審議団体の事務局は日本銀行金融研究所）は、生体認証技術を所掌する ISO/IEC JTC1/SC37 および汎業界的な情報セキュリティ技術を所掌する ISO/IEC JTC1/SC27 との間でリエゾン関係を構築しており、生体認証システムのセキュリティ等に関して必要に応じて連携を図っている。現在、SC37 では人工物を提示する攻撃に対する安全性の評価方法、評価尺度等にかかる国際標準案（ISO/IEC 30107 シリーズ）が、SC27 では人工物の提示を検知・排除するためのセキュリティ要件等にかかる国際標準案（ISO/IEC 19989）が審議されている。

（生体認証システムの脆弱性対応）

- 各種ソフトウェア製品等の脆弱性については、IPA（独立行政法人情報処理推進機構）を届出窓口とした脆弱性関連情報届出制度が運用されており、必要に応じて脆弱性の是正を促すという仕組みが整備されている。しかしながら、生体認証システムについては、何らかの欠陥が見つかり届出があったとしても、それが「脆弱性」であるか否かの判断が難しいと聞いている。その背景として、標準的なセキュリティの評価手法が確立されていないという事情があるとみられる。

（２）「FinTech における生体認証とセキュリティについて」（Liquid Japan：佐藤氏）

（説明の概要）

生体認証が、これまでのパスワード等を用いた認証方式で想定されるリスクの低減に資すると期待されている。こうしたなか、当社では、独自の検索エンジンを開発し、指紋のみで決済を可能とするプラットフォームを開発した。本システムは、認証時における ID の提示を不要とし、ユーザーが 1 億あっても数秒で処理が可能である。また、セキュリティ

の観点からも、既存の認証プロトコルより高い安全性を実現すべく、独自の認証プロトコルを開発・採用している。

本システムはホテルのチェックインシステム等に導入されているほか、経済産業省による「おもてなしプラットフォーム」に採用されており、現在、関東近郊の観光地において実証実験を行っているところである。今後、本システムの利便性とセキュリティを活かし、さまざまなアプリケーションでの活用を展望しているところである。

＜ディスカッションにおける主な意見等＞

（多要素の認証）

- 指紋認証については、センサー面に残留した情報から人工指を作製して「なりすまし」を行うというリスクが指摘されている。こうしたリスクに対しては、認証時に生体検知を行うといった対策も考えられるが、当面の対策として、認証を行う指の数を 2 本から 3 本に増やすことでセキュリティを高める予定である。
- 本システムで採用されている 1 対 N 識別方式では、一般に、1 対 1 方式より誤検知率が高くなることが知られている。このため、1 対 N での指紋識別結果をそのまま本人認証に用いることには、相応のリスクが伴うことは認識しておくべきではないか。

（指紋以外の認証手段）

- 指紋を用いた生体認証方式には、清潔感や登録抵抗感の面で敬遠する向きもあるが、現在展開のシステムでは、最も高速に実装可能であった指紋を採用している。今後は静脈認証や虹彩認証についても展開していきたい。

（生体情報の漏えいリスクへの対応）

- 既存の認証プロトコル（FIDO）では想定されていなかった端末のハッキングや通信データの盗聴をも脅威として想定し、当社では、FIDO より安全性の高いシステム構築を行うことができたと考えている。
- 既存システムと比較した場合、生体認証システムではなりすまし等のリスクとリスクが顕在化した場合のインパクトが格段に低くなるという説明であったが、インパクトの尺度などについては議論の余地がある。

（３）「生体認証：FinTech における資産保全」（日本電気：坂本氏）

（説明の概要）

当社は、1971 年に指紋認証研究を開始。これまで、指紋のほか、静脈、顔、DNA、音声、掌紋、虹彩等の様々な認証技術の開発に取り組んできた。指紋認証は、2013 年、iPhone に指紋認証センサーが搭載されたことを契機に認知度が向上し、普及のスピードが加速してきた。

当社では、①出入国審査システム、②チケット本人確認システム（顔認証による効率的な本人確認と転売防止）、③国民 ID システム（指紋・虹彩・顔認証による二重申請の防止）等で生体認証技術を活用している。

所謂「なりすまし」の事例にみられるように、生体認証による取引は必ずしも安全とは限らない。今後は、多様なセンサーを搭載するスマートフォンを活用した認証などが考えられるほか、評価基準の標準化や、生体認証システムのリスクを定量的に評価・管理することが重要になると考えている。

＜ディスカッションにおける主な意見等＞

（多要素による認証）

- 身体の一部を使って認証する際、その一部が欠損した場合には、多要素の認証が有効。当社では顔・指紋・静脈等、それぞれで類似度を出し、特徴量として捉えることで、パターン認識的技術を用いて認証操作を行っている。身体情報の一部が欠損しても認証できるという技術は、社会的包摂（social inclusion）の観点からも有用だが、英国政府が国民 ID での指紋・虹彩登録を断念した事例もあることから、システム構築にかかる費用とのバランスを考え、慎重に議論する必要がある。

（利便性とセキュリティのバランス）

- スマートフォンの普及等により、消費者がより簡便なログインを求める時代だが、生体認証の利便性とセキュリティのバランスに関する評価は難しい。NIST（米国国立標準技術研究所）がユーザビリティのレポートを公表してはいるが、本人認証の手段を統一的に扱うことができるモデルはまだ存在せず、議論が必要なところである。

（リスクに対する頑健性）

- 顔・指紋・虹彩といった認証要素の「なりすまし」リスクに対する頑健さは開発ベンダーの多寡に依存すると思われる。指紋・静脈・顔認証については、研究者が世界的に多く、リスクも十分研究されている一方、目新しくあまり利用されていない技術は、リスクも伴う。
- 身体的特徴である生体情報は、パスワードのように変更が容易でないことから、漏えいによるリスクが高いとの指摘もあるが、キャンセラブル・バイオメトリクスと呼ばれる技術などによって対策を講じることができる。同技術は、一般的に、生体情報そのものではなく、生体情報を暗号化した状態で登録・照合などの処理を行うため、仮に、当該データが漏えいした場合には当該データを破棄し、元の生体情報を別の鍵で暗号化したデータを再登録することが可能である。

（海外における事例）

- 海外の金融分野における生体認証の普及・導入はまだこれからと推察される。その一方で、たとえばフランスでは、金融サービスに生体認証を利用することが法律で禁じられているとも聞いており、国によってさまざまな状況があると認識している。例えば、アフリカや南米ではモバイルバンキングが普及しているが、リアル店舗が強盗に襲われるリスクが背景にあるといわれており、生体認証の利用も先行する可能性があるように思われる。

３．プレゼンテーションと質疑
～金融分野におけるブロックチェーン技術の実装事例とその安全対策～

○　各社からのプレゼンテーションに続き、参加者との質疑応答が行われた。

（１）「ブロックチェーンの安全性とセキュリティ」（コンセンサス・ベイス：志茂氏）

（説明の概要）

ブロックチェーンの安全性は、設計や実装の手法に依存すると考えている。すなわち、①パブリック型なのか、プライベート型なのか、②コンセンサス・アルゴリズムに何を採用するのか、③ノードをどのように管理するのか、といった設計手法により、必要となるセキュリティ対策が全く異なる。

現状、金融機関が検討対象としているのは、ほとんどがプライベート型であり、従来のセキュリティ対策で対処可能である。他方、パブリック型は、不特定の者からの攻撃、ネットワークの不安定性等、安全対策面での課題が多い。安全なソフトウェアの配付、および、ネットワークのガバナンスを有効に機能させること（例えばフォーク（分岐）への対処方針を分散型合意とするのか等）が必要である。また、採掘報酬やシェアを適切に設計することも重要である。

現状実施されている実証実験をみると、技術の理解や活用方法の検討に主眼が置かれているが、セキュリティを検証して実運用に移すには、場合によっては数年かかる可能性があり、スピード感をもった対応が必要である。また、セキュリティを左右する「ガバナンス」、「経済合理性」の分野で、知見を持つ人材の育成も求められる。

＜ディスカッションにおける主な意見等＞

（ブロックチェーンの実運用に向けて）

- ブロックチェーンに関して、実証実験から運用に移行するという話が国内外で出てきているが、金融機関が実際に運用するに際しては、ソフトウェアの安定性等、未だ課題が多いと認識している。特に、パブリック型ブロックチェーンに関しては、安定的な運用には稼働開始から数年を要するとも指摘されている。

（パブリック型ブロックチェーンのコンセンサス・アルゴリズムの優劣）

- パブリック型ブロックチェーンで採用され得るコンセンサス・アルゴリズムにも多様な形態があるが、どのコンセンサス、実装方式の信頼性・セキュリティが高いかという点については、ベストなものが一つ存在するというよりも、要件に依存すると考える。コンセンサス方式として Proof of Work と Proof of Stake が一般的だが、マイナーを多く集められる場合は前者、コインを巧く分配できる場合は後者がよい。実装方式としては、（網羅的に調べているわけではなく断言はできないが）やはり実績があり普及しているビットコイン、イーサリウム等がある程度、安全ではないだろうか。

（プライベート型ブロックチェーンに対する捉え方）

- パブリック型ブロックチェーンのビットコインがある程度続いている背景として、コミュニティにおける経済合理性の設計に成功していることが指摘できる。他方、プライベート型ブロックチェーンの場合、前提となるインセンティブ設計を省き、技術のみを利用しようという発想であり、フィージビリティについては議論が必要と考える。そもそも、パブリック型とプライベート型では、ブロックチェーンの目的が全く異なる。プライベート型では、（鍵管理等の扱いは加わるが）アクセス制限をどこまでするかといった、従来型のシステムと同じセキュリティ対策が必要となり、技術的には「分散データベース」に近いと言える。

（２）「ブロックチェーンにおける識別子と鍵管理」（Orb / 慶應義塾大学：斉藤氏）

（説明の概要）

ビットコインでは、資産の移転先として相手の公開鍵を指定する。そのため、当該公開鍵に対応する秘密鍵を紛失した場合には、公開鍵に紐付けられた資産を利用できなくなるというリスクがある。当社では、こうしたリスクへの対策として、資産の移転先として指定される利用者の識別子（宛先）という概念を新たに設け、識別子と公開鍵との紐付けは別途ブロックチェーン上で管理する仕組みを開発・実装した。これにより、秘密鍵を紛失した場合でも、新しい鍵ペアを作成し、対応付けを更新することで問題を解決することができ、特許を取得している。

同プラットフォーム（Orb 1）では、識別子と公開鍵との紐付けを管理する「スーパーピア」が必要となるという課題がある。事業への応用を想定した場合、スーパーピアの存在は大きな課題ではないと考えているが、識別子と公開鍵との紐付けに別の鍵ペアを活用することで自律分散的に識別子を生成する仕組みも考案している。この仕組みでも、スーパーピアが存在しないことで生じる「スクワッティング[2]」の課題は残存するが、ビットコインでもス

[2] 識別子にニーズのない者等が当該識別子を予め大量に確保すること。ビットコインにおけるスクワッティングの問題点は、主に識別子の衝突（別の二人が偶然同じ識別子を使用出来る状態）の発生確率が高まることである。

クワッティングは報告されておらず現実に起こる可能性は低いと考えている。

また、こうした考え方はビットコインとは異なるデータ構造を用いるブロックチェーンにも適用可能であると考えている。

＜ディスカッションにおける主な意見等＞

（スーパーピアについて）

- Orb 1 にはスーパーピアが存在するため、一見プライベート・ブロックチェーンに近いようにみえるが、一般ユーザーが参加出来ることを念頭に置き、パブリック・ブロックチェーンに近いものになるよう設計されている。
- Orb 社が現在開発中の新しいプラットフォームでは、実用性を重視し、Orb 1 と同じくスーパーピアが存在する従来の分散型データベースに近いものになっていると聞くが、やはりオープンでパブリックなものに社会的な意義があるという思いはある。

（データ構造について）

- UTXO[3]と状態遷移記述のブロックチェーンの比較において、状態遷移記述の方が応用しやすさのうえでは優れているが、一方で記述の正当性を検証しにくいという課題がある。図示した時に明快にロジックが分かるという UTXO の特長はもっと評価されるべきであり、UTXO の仕組みを用いてかつスマートコントラクト実装可能なブロックチェーンの開発がもっと盛り上がってほしいと考えている。

（３）「金融分野へのブロックチェーン利活用に際する実装課題と安全対策」（カレンシーポート：杉井氏）

（説明の概要）

システム構成にブロックチェーンを活用する際、パブリック、コンソーシアム、ハイブリッドの 3 つのパターンが想定可能だが、どのパターンを用いるにしても、取引事実の存在証明等のパブリック性をシステムの中に組み込

[3] 未使用トランザクションアウトプット（Unspent transaction output）。過去に行われた取引の出力のうち、まだ別の取引の原資として使用されていないものを言う。同じアドレスに紐付けられている UTXO の合計を仮想的にそのアドレスの口座残高として捉えることから、転じて一般にそうしたデータ管理方法も UTXO と呼ばれることが多い。

まなければブロックチェーンのメリットを十分に活かすことはできない。また、ブロックチェーンは既存のデータベース全てを置き換える技術ではないので、両者のそれぞれ良い部分を活かしたシステム構成とするべきである。

ブロックチェーンは構成要素が多岐に亘るため、セキュリティについても複数のレイヤーで対応する「多層防御」とする必要がある。①ネットワークレベルでは従前同様、統一されたアクセス基準を用いることが重要。②ノードレベルでは、要件ごとに細かなアクセス権限を設定することが有効。③ロジックレベルでは、ドキュメントの閲覧制御技術（ドキュメントの暗号化や分散ストレージでの保管等）が必要。④トランザクションレベルでは、取引権限の制御に用いるマルチシグネチャ、取引送信者の秘匿に用いるリング署名、取引詳細の秘匿に用いる秘匿トランザクション等の技術が有効である。

また、⑤鍵管理は従来型のハードウェア・セキュリティ・モジュールが有効。さらに、⑥KYC や AML 対策が必須となる金融分野では、非中央集権主義を標榜するビットコイン等では通常用いられない、第三者によるタイムスタンプや公開鍵暗号基盤（PKI）を用いた認証が必要である。

ブロックチェーン技術を応用したスマートコントラクトでは、「コードは法だ」という極端な主張があるものの、The DAO 事件で判明した通り、完備なコードは不可能なほか、パブリック型では仕様改定する際の合意形成も困難。今後は、事故を防止する技術的な対策が必要であるが、「開発者の信用や稼働実績」といった従来型の安全確保が有効な面もある。

＜ディスカッションにおける主な意見等＞

（セキュリティの実装状況）

- 紹介したセキュリティのうち、ドキュメントの閲覧制御については、分散ストレージと併用し基礎レベルの実証実験が既に行われている。分散ストレージの非情報化処理については理論段階のものを含むが、特に実用性が高いと感じている。トランザクションレベルでは、マルチシグネチャは既に実装が行われているが、リング署名、秘匿トランザクション技術は、イーサリウム系の実装をベースにしたものの場合、内部構造に手を加える必要があり、まだ仮説の段階に過ぎない。

（ブロックチェーンと AI）

- ブロックチェーンと人工知能（AI）に関する議論として、AI 自体のバージョン管理にブロックチェーンが活かせるのではないか。即ち、AI では制御出来ない自身のバージョン情報を人間側で管理する際にブロックチェーンを用いることもあり得ると思う。
- 機械学習により帰納的に何かをアウトプットする場合、一般的に学習データがあるものについては結果を保証できるものの、そうでない場合は結果を保証することが難しい。想定外の事象が発生し、機械が制御できなくなった場合、リカバリーとして人間に制御権を引き継ぐ必要が出てくるが、その際、人間が制御し易い形で渡すようにする必要がある。
- 仮に、機械学習が未知のことを検知することが難しいとすると、AI によって完備度の高いコードを作るという話には限界があるように感じる。他方で「コードは法だ」という主張に関する議論のポイントの一つは、リアルな世界の契約も実際のところ完全ではなく、不完全な部分をヒト同士の対話で解決している一方で、コードで完結する世界にはそうした解決手段が無いという点である。

（ブロックチェーンとタイムスタンプ）

- ブロックチェーン上のトランザクションにタイムスタンプを付与するというのは難しい。元々トランザクションの順序性は保証するが時間の厳密性は持たないというのがブロックチェーンの本質であるからだ。そのため、ブロックチェーンの外にトランザクションの時間を担保する仕掛けを設けないとうまく機能しないと思われる。また、従来のタイムスタンプサービスのように信頼できる第三者機関を前提とするのであれば、ブロックチェーンの設計の在り方自体にも影響を与えるのではないか。
- ビットコインは P2P を前提として始まっており、中央集権的なノードを排除して設計されているので、タイムスタンプも信頼できる第三者によるものではなく「紳士協定」によるものが使われている。但し、ビジネス上の要請から、ブロックチェーン上のトランザクションに対し、TSA など信頼できる第三者により署名の施されたタイムスタンプシステムが必要になると考えられる。こうした実装がなされたブロックチェーンシステムの例はまだないと思うが、例えばビットコインを例にとれば約 10 分間にブロックとして承認される数多のトランザクションに施されている各タイムスタンプを互いに比較すれば、大きなズレは発生しないとも考えられ、そのズレをどの程度許容するかといった点が論点になるように思う。

（４）「ブロックチェーン導入における課題とその対応について」（NTT データ：赤羽氏）

（説明の概要）

ブロックチェーンは、いくつかの技術の組み合わせでできており、その導入に当たっては、技術毎に安全面・運用面の検証が必要である。中でも①P2P ネットワーク、②偽造防止・暗号化、③コンセンサス・アルゴリズム、④スマートコントラクトは、ブロックチェーン特有の安全対策が必要である。

安全面では、安全性の定義が定まっておらず、その結果十分な安全性の検証がなされていないことが課題となっている。また、The DAO 事件のように、ブロックチェーン基盤だけでなく、その上で実行されるプログラムの安全性を担保する手段についても十分な検証が必要である。

運用面では、The DAO 事件のように、ブロックチェーンに誤った情報が書き込まれた際の対応の検討や、P2P ネットワークに分断が発生した際の運行基準などのルール作りが必要である。また、コンソーシアム型とパブリック型で運用の考え方が大きく変わる点には留意が必要である。

当社は、ブロックチェーンには検証すべき項目が数多く残されてはいるが、大変魅力溢れる技術であると評価しており、貿易金融や証券取引分野でブロックチェーン活用に向けた取組みを行っている。ブロックチェーンの導入においては、安全面での理論と実装のギャップをしっかりと認識することが重要となる。ブロックチェーンはシステムの一部のパーツでしかなく、従来のシステムで使っていた安全対策をしっかりと行っていく必要がある。

＜ディスカッションにおける主な意見等＞

（The DAO 事件のハードフォーク問題）

- The DAO のようなケースでは、何らかの原因で正しくない情報が書き込まれた場合、その対応について事後的にユーザー間の合意をとるのでは間に合わないため、予め何らかの運用ルールを作っておくべきである。また、コンソーシアム型であれば、予め運営主体を構成するメンバーによってルールを決め、明示しておくべきである。
- コンソーシアム型のブロックチェーンであれば、バージョン管理までコントラクトに設計しておけば、誤った情報が書き込まれたとしてもコントロール

可能だと思う。実際、実証実験において、バージョン管理をするコントラクトを設定し、そこから最新バージョンのコントラクトを問い合わせ、コンソーシアム内でバージョンの変更をアナウンスすることで機能することを確認している。

- The DAO 事件で判ったことは、枠組みのごく一部で起こった盗難事案への対応が、パブリック型のブロックチェーン全体の信頼性の問題に繋がったということ。例えば、一部の日本円が盗難されたとしても、日本円のシステムの根幹を揺るがすような事態には至らない。ブロックチェーンによって、本来は何を達成したかったのかというレベルに立ち返って考えるべきである。

（ブロックチェーンにおける秘匿情報の取扱い）

- 貿易金融やシンジケートローンの分野は非常に煩雑な事務を伴うため、ブロックチェーン化による事務効率化には期待が寄せられている。もっとも、ブロックチェーンでは、取引の偽造・改ざんを防止するための暗号化は行われているが、取り扱うデータそのものは暗号化されていない。そのため、ブロックチェーンで契約情報等の機密情報を扱う場合には、情報の秘匿化が課題となる。この点、当社では、貿易金融の信用状（L/C）発行に係るブロックチェーンの実証実験を行っているが、その第 2 フェーズで情報の秘匿化も含めて実験を行う予定である。

（量子コンピュータと暗号技術）

- 暗号技術を利用したシステム一般の問題として、量子コンピュータが登場すると電子署名の有効性が失われるという問題がある。セキュリティ界隈では取組みが始まっているが、ブロックチェーンについても、長期的に運用される前提であるため、検討を行う必要がある。英国の Post Quantum などの動きを取り込んでいく必要があろう。米国立標準技術研究所（NIST）では耐量子コンピュータ暗号の標準化プロセスを始めており、こうした動きも参考になると思われる。

（５）「Hyperledger Project のセキュリティと方向性」（日本 IBM：高木氏）

（説明の概要）

当社は、業界横断でブロックチェーンのオープンスタンダードを検討する Hyperledger Project に参加し、「Hyperledger Fabric」と呼ばれるブロックチェーン基盤を開発中。Hyperledger Fabric は、参加者を限定するプライベー

ト型のブロックチェーンで、幅広いユースケースを念頭に、柔軟性の高い設計を行っている。

Hyperledger Fabric の安全性の中核を担うのはユーザー権限の管理を行うメンバーシップサービス（認証局）。参加者の ID 証明書の他に、エンドユーザー用に取引毎のワンタイム証明書 Transaction certificates（Tcert）を導入し、鍵の漏洩や紛失に伴うリスクを低減。Tcert の利用により、機密情報の秘匿化も可能となる。もっとも、検証ノードが鍵を漏洩・紛失した場合には秘匿化した機密情報が流出するなどリスクが高いため、その管理においては既存システムと同等のセキュリティ対策が必要。

Hyperledger Fabric における取引の検証アルゴリズムは、PBFT（Practical Byzantine Fault Tolerance）の課題を解決するための新たなアルゴリズムとして Next Generation Consensus を開発中。同アルゴリズムでは、検証を二段階に分け、指定されたノードのみが取引内容を含む一次検証を行い、二次検証の段階ではハッシュ化した取引の形式的な確認のみ行う。また、The DAO 事件でみられたようなスマートコントラクトの不正を検知する仕組みを整備することも検討している。

海外の銀行では、ブロックチェーンの多くの利点はコンソーシアム型にあるものの、解決すべき課題が多いとの見方から、先ずは自行内でプライベート型ブロックチェーンを導入し、徐々に他行間のコンソーシアム型に移行するアプローチをとっている。こうした段階的アプローチは有効だと考えている。Hyperledger Fabric の検証ノードは金融機関のシステムと同等の管理が必要であることから、安全性を確保しながら、徐々にブロックチェーンを育てていく必要がある。

＜ディスカッションにおける主な意見等＞

（Hyperledger Fabric のコンセンサス・アルゴリズム）

- Hyperledger Fabric は 2017 年 3 月に Ver.1 のリリースを目標としている。リリースに向けた最大の課題は、コンセンサス・アルゴリズム。これまで前提にしていた PBFT は、ユースケースによっては耐え得るものの、海外の銀行が想定するようなユースケースにおいては安全性の観点から採用できないと言われている。

- PBFT 問題を解決するために開発中の新たな仕組み「Next Generation Consensus Algorithm」は、一次検証と二次検証の部分はコンセンサスとは独立させ、一部切り出して実装していく方向もあり得る。

（Hyperledger Project へのエアバスの参加）

- 8 月 16 日、仏航空機メーカーであるエアバスが Hyperledger Project のプレミアムメンバーとして参加した。エアバスが本 Project に参加する目的はサプライチェーンマネジメントへのブロックチェーンの活用である。これまでブロックチェーンに関する取組みは金融界がリードしてきたが、今回のエアバスの参加で勢力図が変わる可能性がある。金融業界が堅牢なセキュリティレベルを求めて議論を重ねているうちに、多産業でより簡易な手法をベースとしてブロックチェーンが一気に普及してしまうかもしれない。

（６）「証券ポストトレードにおけるブロックチェーン技術の実装デモとその安全対策」（みずほ銀行：河野氏）

（説明の概要）

日本株・日本国債にかかる国内の証券決済では、約定照合の結果を決済の関係者（証券の買い手、売り手、カストディアン、証券集中振替機関＜CSD＞）の間で共有する仕組みが構築されており、このデータを基に決済指図が作成されるため、決済照合の段階で指図の不一致は発生しない。これに対して、非居住者が関係するクロスボーダーの証券決済では、約定情報を共有する仕組みが存在しないため、証券の買い手・売り手はそれぞれ決済指図を作成し、次の関係者に伝達しており、数%の割合で決済指図の不一致が発生する。このような指図の不一致は、多くのフェイルの原因となっている。

当行は、ブロックチェーン技術を用いることでフェイルを低減できないかとの問題意識の下、富士通および富士通研究所の協力を得て、実証実験を行った。具体的には、決済関係者が、約定内容や決済状況の情報をブロックチェーン上に登録することで、これらの情報を共有する仕組みを構築した。これにより、決済指図の不一致を解消しやすくできるほか、全関係者が処理ステータスをリアルタイムで把握できるようになり、決済に要する時間を短縮できることが期待できる。セキュリティ面では、個々の取引を暗号化し、暗号鍵

を有している関係者以外は、約定内容や決済状況を閲覧できない仕組みとなっている。

なお、本実証実験では、ブロックチェーン基盤として、ビットコインの Open Assets Protocol[4]を利用している。

＜ディスカッションにおける主な意見等＞

（本デモに対する評価）

- 実証実験のブロックチェーン基盤として、皆がプライベートチェーンを評価している中で、ビットコインのパブリックチェーンを使って実現したことは素晴らしいと思う。

（ブロックチェーン基盤の選択）

- パブリック型、コンソーシアム型、プライベート型のブロックチェーンにはそれぞれ長所・短所があるほか、個々のブロックチェーン基盤にも特色がある。取引処理のファイナリティの観点からは、ビットコインではチェーンの分岐が発生する可能性があり、コンソーシアム型のコンセンサス・アルゴリズムの方が優れている。検証を行うためのインセンティブの観点からは、ビットコインでは報酬というインセンティブがプロトコルに組み込まれているのに対して、コンソーシアム型では適切なインセンティブ設計が課題とされている。ブロックチェーンをどのように利用したいかにより、重視すべき機能・性能は異なり、結果としてブロックチェーン基盤の評価や選択も異なる。
- 本実証実験では、ブロックチェーン技術を決済関係者間の情報共有手段として利用しており、証券残高の振替には、既存の振替決済制度を利用することを想定している。ブロックチェーン上で権利移転を行う場合と比べると、ファイナリティに必ずしも重点を置いているわけではない。

（取引情報の秘匿）

- Hyperledger Fabric では、取引情報を暗号化し、参加者ごとに閲覧権限を付与することができるが、検証ノードは検証用の暗号鍵を保有しており、悪意があれば全ての取引の内容を閲覧できてしまうという課題がある。本実証実験の仕組みでは、決済関係者のみが暗号鍵を保有するため、関係者のみにアクセスを制限することができる。

[4] ビットコインを送金する際の空き領域に追加情報を記載する手法。

４．ラップアップ（日本銀行：岩下）

○　日本銀行岩下 FinTech センター長は、カンファレンスにおける議論の内容について、以下のとおりラップアップを行った。

- 銀行業務は、かつては手形や小切手等の紙ベースの処理が中心であったが、50 年ほど前に、銀行本支店間のオンラインシステムや、内国為替取引を処理する全銀ネットが整備された。これらの仕組みの構築にあたって、関係者は「為替電文を用いてどのように決済を行うべきか」といった点について喧々諤々の議論を行ったと想像され、そうした議論の結果生み出されたインフラが、現在の金融システムを支えている。
- 同様に、我々は現在、次の世代のインフラを構築するという責任ある立場にあるのではないかと思う。生体認証やブロックチェーンについては、様々な活用方法が模索されているところであり、何が本筋となるかは現時点では必ずしもみえていない。言い換えれば、これらの技術は、それだけ多くの可能性を秘めている。
- 次の 50 年（ムーアの法則を踏まえるとそれよりも短いかもしれないが）を支える新しい基盤を作るための議論を、ぜひみなさんと共に進めていきたい。第 2 回以降の FinTech フォーラムについても、引続きご協力をお願いしたい。

以　　上

（別　紙）

参加企業・団体一覧（50 音順）

FinTech 協会	東京金融取引所
GMO クリックホールディングス	東京スター銀行
Liquid	東芝ソリューション
NTT データ	日本アイ・ビー・エム
NTT データジェトロニクス	日本自動認識システム協会
Orb	日本証券金融
SMBC 日興証券	日本電気
TMI 総合法律事務所	日本取引所グループ
渥美坂井法律事務所・外国法共同事業	日本ヒューレット・パッカード
阿波銀行	日本ユニシス
沖電気工業	農中信託銀行
オリックス	野村総合研究所
カレンシーポート	野村ホールディングス
金融庁	日立オムロンターミナルソリューションズ
慶応義塾大学	日立製作所
経済産業省	富士通
ゴールドマン・サックス証券	富士通エフ・アイ・ピー
国際銀行協会	富士通研究所
コンセンサス・ベイス	ブラジル銀行東京支店
島根銀行	マネーツリー
重要生活機器連携セキュリティ協議会	マネックス証券
証券保管振替機構	みずほ銀行
常陽銀行	みずほ証券
信金中央金庫	みずほフィナンシャルグループ
スイフト・ジャパン	三井物産
住信 SBI ネット銀行	三井住友銀行
セールスフォース・ドットコム	三井住友信託銀行
セコム	三菱東京 UFJ 銀行
セブン銀行	森・濱田松本法律事務所
ソラミツ	ヤフー
大和証券グループ本社	山梨中央銀行
大和ネクスト銀行	ゆうちょ銀行
多摩信用金庫	横浜銀行
デジタルガレージ	リンクパートナーズ法律事務所
電通国際情報サービス	レピダム
ドイツ証券	