

金融情報システムセンター（FISC）エグゼクティブセミナー

伊藤長官 講演原稿

（令和8年9月1日（火） 13:00～14:00）

本日は、金融のデジタル化や決済インフラの高度化をめぐる最近の動向について、ご説明させていただきます。

具体的には、

- ・ 第一に、ブロックチェーン技術を活用した決済高度化に向けた取組みと、その社会実装を後押しする「決済高度化プロジェクト（Payment Innovation Project（PIP））」、
 - ・ 第二に、我が国の次世代決済インフラの構築に向けた全銀ネットの新システムの検討状況、
 - ・ 第三に、フロンティアAIの進展を踏まえた金融分野におけるサイバーセキュリティ上の課題と対応
- について、ご紹介いたします。

1. PIPの趣旨及び取組みについて

＜決済高度化に向けた取組み＞

- ブロックチェーン技術を活用した新たな決済手段は、単に送金を「早く」「安く」するだけではなく、スマートコントラクト等と組み合わせることで、商流・物流と決済を連動させ、取引全体を効率化していく可能性を持っています。
- 本日は、まず、国内外でのブロックチェーン技術を活用した決済高度化に向けた取組みをご説明した上で、今後のAI時代を見据えて、金融システム全体のインフラをどのようにトランスフォームしていくのかについて、ご説明します。

＜ステーブルコインとトークン化預金の比較＞（１ページ目）

- デジタル社会における新しい決済手段である、ステーブルコインとトークン化預金についてご説明します。両者はいずれもブロックチェーン技術を用いる点で共通しますが、法的性質、発行主体、価値の裏付け、利用上の留意点は大きく異なります。
- 具体的に、ステーブルコインは、法定通貨を対価としてブロックチェーン上に発行されるトークンです。日本では、資金移動業者、信託銀行、信託会社などが発行主体となり得ます。価値の裏付けは、預金や国債などの安全資産を中心とした準備資産です。一般に、幅広い利用者の間で転々流通する場合には、マネー・ローンダリングやテロ資金供与対策をどのように実効的に確保するかが重要となります。また、預金ではないため、預金保険の対象外であり、利息を付与することはできないのが特徴です。
- これに対し、トークン化預金は、預金残高のデータをブロックチェーン上で管理するものです。発行主体は銀行に限定されており、価値の裏付けは銀行の預金です。移転の際には預金としての制約を伴いますが、既存の運用に準じた本人確認や取引モニタリングなど、マネー・ローンダリングやテロ資金供与対策について、一定の水準が確保されやすいという特徴があります。また、預金保険の対象となり、利息を付与することも可能です。

＜ステーブルコインとトークン化預金の国際的な動向＞（２ページ目）

- 次に、国内外におけるステーブルコインの制度整備、及びステーブルコインやトークン化預金を活用した取組みについてご紹介します。

- 日本では、世界に先駆けてステーブルコインの制度整備を進めてまいりました。昨年10月には国内で初めての円建てステーブルコインとしてJPYCの提供が開始され、本年6月には新たに、SBI新生信託銀行によるJPYSCの提供が開始されました。さらに、3メガバンクが共同でステーブルコインを発行し、実取引の開始を目指すことを発表しております。
- また、ステーブルコインに限らず、トークン化預金の発行を検討する金融機関も増えています。GMOあおぞらネット銀行で発行が開始され、ゆうちょ銀行でも発行に向けた検討が進められているほか、北國銀行による地域通貨「トチカ」など、発行例も既に見られます。
- 海外でも、制度整備と実証の双方が進展しています。
- ステーブルコインについて、米国では昨年7月に連邦レベルの包括的な規制枠組みとなるGENIUS法が成立し、現在、世界のステーブルコイン取引の約9割をドル建てのUSDTやUSDCが占めています。EUでも規制枠組みが整備され、ユーロ建てを含む発行例も登場しています。
- トークン化預金についても、JPモルガンによる機関投資家向けの取組みや、BIS主導のProject Agoraなど、クロスボーダー決済や銀行間決済の高度化を目指す取組みが相次いでいます。

<PIPの設置>（3ページ目）

- そこで重要となるのが、「具体的に何に使うのか」、すなわちユースケースの創出です。新しい技術を使ったサービスを検討

する際には、どのような法令が適用されるのか等、事業を進める上での課題となることがあります。

- 金融庁では、制度整備を行った上で、社会実装の動きを後押しすることが重要と考えており、これまでも、新たな事業を検討する民間事業者の創意工夫の支援に取り組んできました。
- 昨年11月、「F i n t e c h実証実験ハブ」内に「決済高度化プロジェクト」、通称P I P（ピップ）を設置しました。この枠組みでは、必要に応じて関係省庁とも連携しながら、関係法令の解釈やコンプライアンス、監督上の論点等を整理し、実証実験が円滑に進むよう支援を行っております。
- 現在、P I Pでは、既にステーブルコイン、トークン化預金、金融資産のトークン化に関する3件の実証実験を支援しており、ここからは、それぞれの取組み内容についてご紹介します。

<P I P 1号案件>（4ページ目）

- まずは、昨年11月7日に初めて支援を決定した、円建てステーブルコインの共同発行及びそれを活用したクロスボーダー決済に関する実証実験についてご紹介します。
- 国際送金については、従来から、処理に時間やコストがかかるとの指摘があります。ステーブルコインを活用することで、こうした課題に対応することが期待されています。
- 本実験では、大手商社などからステーブルコインの注文を受けたメガバンク3行等が共同で信託銀行を通じて円建てのステーブルコインを発行し、そのステーブルコインを海外拠点への

資金移動などに利用することで、クロスボーダー決済の高度化・効率化に活用できるかを実証します。

- なお、先ほども触れましたが、本年6月10日には、本年度中に本件のステーブルコインを用いた実取引の開始を目指すこと、および、本件のステーブルコインに関する運営方法やガバナンスのあり方、将来的に参加を検討し得る金融機関・関係者との連携のあり方などについて検討を進める協議会を設置すること、が公表され、取組みを加速させております。

＜PIP2号案件＞（5ページ目）

- 続いて、2号案件として、本年2月13日に支援を決定した「オンチェーンでの証券決済に向けた取組み」についてご紹介します。
- ブロックチェーンを用いた金融資産のトークン化について、国内では、不動産証券化商品や社債等で活用が進んできましたが、国債や証券等の伝統的資産は、振替機関による権利者管理とそれを前提とした市場インフラが確立しており、振替口座を用いたオンチェーン取引は実現しておりませんでした。
- 他方、海外においては、様々な伝統的資産のトークン化の取組みが著しく進展しており、海外投資家を含む幅広い投資家層を呼び込み、国際競争力を高める観点から、オンチェーンでの証券決済を実現する期待が高まっています。
- 本実験では、国債等の債券、投資信託、株式等の有価証券を対象に、証券会社間取引において振替口座簿の記録とブロックチェーン上のデータを同期させる仕組みを実証します。

- スライド中央の＜イメージ＞を用いてご説明すると、売り手となる証券会社Aから買い手となる証券会社Bへの証券の移転を、証券決済用のブロックチェーン上で行うと同時に、振替口座簿の記録を更新し、法律上の権利を移転させます。
- また、証券会社Bから証券会社Aへの購入代金の支払いには、資金決済用のブロックチェーン上でステーブルコイン等のデジタルマネーを用いることで、振替有価証券の権利移転と資金決済を同時に実行する、D v Pを実現します。

＜PIP3号案件＞（6ページ目）

- 次に、3号案件として、本年4月3日に支援を決定した「トークン化預金を複数の銀行間で移転する仕組みの構築に向けた取り組み」についてご紹介します。
- 今後、多数の銀行等がトークン化預金を導入した場合、異なる銀行の顧客間でトークン化預金の移転を行う場合には、既存の送金・振込と同様に、銀行間をつなぐ資金移転の仕組みが必要になります。
- スライド内の＜イメージ＞を用いてご説明すると、既存の銀行送金では、顧客Aから顧客Bへの送金は、全銀システムによる振込情報の連携に基づいて各銀行が口座の引落とし・入金処理を行い、その結果生じる銀行間の資金決済を、日銀ネット上の日銀当座預金の振替により、最終的に完了させる仕組みとなっています。
- これに対し、本実験では主に2つの方式で実証を行っています。1つ目は、銀行同士が相互で相手方の銀行にトークン化預金

口座を開設し、顧客間の資金移転と銀行間の資金移転を同時に実施する方式です。2つ目は、顧客間でのトークン化預金の移転と銀行間でのステーブルコインの移転を連動させる方式です。

- いずれの方式でも、オンチェーンでの顧客間の取引に応じて、その銀行間決済もオンチェーンで完結させることで、決済リスクや業務負荷等を低減し、顧客利便性を向上することを目指しています。
- なお、日本銀行は日銀当座預金のトークン化及びその活用に向けたサンドボックスプロジェクトを行う予定となっており、相互の実験の状況に関する情報や知見の共有などを通じて、連携してまいります。

＜ブロックチェーン技術の活用可能性＞（7ページ目）

- いずれの実験も前例のない取組みであり、技術的な実現可能性や利用者の利便性、事業者目線での実用性、そして法令遵守やリスク管理など、様々な面をひとつひとつ確認することが必要ですが、そうした積み上げなくしては、新たなサービスを具体化することはできません。こうした取組みをしっかりと後押ししたいと考えています。
- その際、金融分野はもちろん、社会全体としての意義も大切にしたいと思います。ブロックチェーン技術の活用のメリットは、金融に限るものではありません。ブロックチェーン技術は、（１）改ざんされにくい形で記録が残せる、（２）関係者が参照できる、（３）スマートコントラクトと呼ばれるプログラムによる自動的な処理との接続に親和性が高い、といった特徴があります。

- 例えば、貿易に携わる様々な事業者の間では、貨物の輸送・通関の状況等をブロックチェーン上で管理・共有する取組みが進んでいます。これをステーブルコイン等による代金決済とブロックチェーン上で連動させることで、貨物の発送・受渡しにあわせて代金決済を連動させることが可能になると指摘されています。単に貿易に伴う決済を効率化するにとどまらず、貿易取引に関する業務プロセス全体の効率化・高度化につながる可能性があります。
- 同様に、例えば中小企業の受発注に関する情報を、ブロックチェーン上で管理・共有し、物品等の受け渡しと代金支払いを連動させることで、入金・支払いの消込などの事務負担・コストの低減につなげるアイデアも指摘されています。人手不足に悩む中小企業にとって、業務効率化は喫緊の課題です。
- このように、ブロックチェーンのプログラマビリティは、決済そのものの付加価値を超えて、様々なビジネスの生産性向上につながることを期待されます。
- また、A I エージェントが人間に代わって自動で商品の購入などを行う、エージェントック・コマースが現実味を帯びてくるなかで、即時化された決済とスマートコントラクトを組み合わせることで、商取引と決済が一体として自動的に実行される世界が到来する可能性もあります。

＜金融システムを支えるインフラへの投資＞（８ページ目）

- 本年７月２１日に公表された「成長投資を促進するための金融戦略」では、政府が目指す「強い経済」を実現するための成長投資を支える重要な要素として、金融システムを支えるインフラ

への投資の促進、が挙げられております。

- この中で、金融庁は、ブロックチェーン技術を基盤とする「オンチェーン金融」の推進と、既存の金融インフラである「オフチェーン金融」とのベストミックスを目指し、「A I時代を見据えたオンチェーン金融イニシアティブ」を立ち上げることとしております。
- こうした将来像を踏まえつつ、関係省庁や日本銀行をはじめとする関係機関と連携し、日本の金融システムを支えるインフラを着実にアップグレードするなど、引き続き、国際的な動向や技術の進展も踏まえながら、日本にふさわしい形での健全な金融の発展を後押ししてまいります。

2. 全銀ネットの新システム (9 ページ目)

- 全銀システムは、更改や機能追加を重ねながら、半世紀以上にわたり、我が国の経済活動を支える基幹的な決済インフラとして大きな役割を果たし、高い信頼性を維持してきました。
- 他方、決済を取り巻く環境は大きく変化しており、例えば、国際的にはリアルタイム決済の普及が進む中、QR コードや、トークン化預金・ステーブルコイン等の新たな決済手段との連携など、多様化する利用者ニーズに応えていくことも求められています。また、安全性の確保やマネロン対策の高度化の観点から、FATF 勧告に基づく国際標準への準拠や決済電文に含まれる情報の充実も重要となっています。
- こうした環境変化を踏まえて、利用者利便の向上に資する観点から、我が国の決済インフラを一段と高度化し、国際的な競争力を高める機会としていくことが重要です。このような問題意識の下、金融機関、有識者及び当局担当者が参加した全銀ネットの検討会において昨年より議論が行われ、本年3月19日に報告書が公表されました。
- 同報告書では、既存システムへの部分的な機能追加にとどまらず、将来のニーズに柔軟に対応できる新たな決済システムの構築に向けて、検討を進めることが盛り込まれました。
- 当該新たな決済システムのもたらす効果として、第一に、24 時間 365 日、数秒で振込を完結させるリアルタイム決済の実現、第二に、トークン化預金やステーブルコイン等のデジタル決済手段との連携や、海外の決済システムとの相互接続を視野に入れ

た拡張性の確保、第三に、マネロン対策の高度化や送金先口座の事前確認、着金確認等による安心・安全の向上、第四に、金融機関の業務効率化を通じたコストの軽減が期待されています。

- 今後、全銀ネットは、新たな決済システムについて 2027 年 3 月に構築方針を示す見込みです。構築する場合には、基本的な機能については 2030 年の稼働を目標としています。また、当面は現行の全銀システムと新たな決済システムを併存させ、安定的な移行を確保しながら、追加的な機能の充実を図るとともに、将来的な機能集約も見据えて検討が進められているところ、金融庁としても当該検討に積極的に関与してまいります。
- なお、新たな決済システムを構築する場合には、参加金融機関においても、それぞれのシステムや業務について一定の対応が必要になります。各金融機関におかれては、新たな決済システムに係る今後の検討状況や具体的な開発計画を踏まえつつ、自行のシステム開発計画等への反映について、早い段階から検討を進めていただくことを期待しています。
- 金融庁としても、全銀ネットや金融機関をはじめとする関係者と丁寧に対話しながら、利用者利便の向上に資する我が国の次世代の決済インフラが、安全かつ着実に構築されるよう、取組を後押ししてまいります。

3. フロンティア AI への対応

- 3つ目のテーマは「フロンティア AI によるサイバー脅威の変化への対応」です。

＜AI によるサイバー脅威の変化と金融分野への影響＞（10 ページ目）

- Anthropic 社の Claude や OpenAI 社の GPT シリーズをはじめとするいわゆるフロンティア AI の性能向上など、AI 技術は急速に進展しており、サイバー攻撃の「大規模化」「高速化」「高度化」が懸念されるなど、金融分野を取り巻くサイバー脅威は一層高まっています。
- 具体的には、AI の活用により、攻撃メールの作成や標的の選定、情報収集等の効率化・自動化が進み、従来よりも大規模かつ同時に攻撃が実行される可能性があるほか、AI による脆弱性分析や攻撃コード生成の高速化により、脆弱性の発見から実際の攻撃までの期間は大幅に短縮されることが懸念されます。
- 金融システムは相互接続性が高く、決済や取引がリアルタイムで処理されているため、サイバー攻撃によるシステム障害が、市場機能や金融仲介機能に波及し得るという特性があります。
- このため、金融機関においては、脆弱性情報の把握からパッチ適用までの対応や、サイバー攻撃の検知から対処までのプロセスについて、更なる高速化を図ることが重要です。
また、サイバー攻撃を完全に防ぐことは困難であるとの前提に立ち、多層防御の強化に加え、攻撃を受けた場合でも影響を最小限に抑え、重要業務の継続及び業務の早期復旧を実現するた

めのサイバーレジリエンスの確保を進める必要があります。

- Anthropic 社の Claude Mythos Preview が登場した当初は、脆弱性を発見して侵入するというリスクや脅威、すなわち A I の「攻撃面」が強調されていたように思われますが、足元では、脆弱性の発見にとどまらず、例えば、対応すべき脆弱性の優先順位付けやパッチの提案・適用も含めたサービス、すなわち「防御面」の対応も検討・提供され始めています。いわゆる、「A I 対 A I の攻防」の世界が到来しつつあります。
- 様々な最先端 A I モデルが今後も次々と開発されていくものと考えていますが、それぞれのモデルにおけるガードレール等の安全性確保のあり方やデータの取扱いについて、適切に認識した上で、目的に応じた活用をしていくことが望ましいと考えています。
- また、フロンティア A I の悪用による脅威に備え、多層防御や脆弱性管理、インシデント対応等の基本的な取組を着実に実施しつつ、サイバーレジリエンスを不断に強化していくことが重要です。

＜フロンティア A I による脅威変化を踏まえた金融機関等の短期的な対応の要請＞（11 ページ目）

- フロンティア A I の進展が金融分野にもたらす変化を踏まえると、新たな備えや経営判断が一層重要となってくることから、金融業界と政府・日本銀行等が早期に共通の理解を持ち、対応に当たることが不可欠です。

- こうした背景から、A I を活用したサイバー攻撃が常態化する状況を想定した対応策を経営主導で検討・実施していくため、
 - ・ 本年4月に「A I 脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議」を開催するとともに、
 - ・ 5月にはその作業部会を開催し、金融業界とIT企業、政府、日本銀行等の官民の連携強化を図るとともに、
 - ・ 5月22日に、短期的な対応について要請文を発出し、更なる対応をお願いしているところです。

この要請文は、短期的に脆弱性や修正プログラム（パッチ）が集中的に発見・提供される可能性に備え、金融機関等において速やかに講じるべき対応を取りまとめたものです。

- したがって、この要請文に記載された短期的な対応事項のみを実施すれば十分というものではありません。

A I 脅威に対しても基本的な対応が有効なため、金融機関においては、2024年10月公表の「金融分野におけるサイバーセキュリティに関するガイドライン」（以下「ガイドライン」という。）で示されている、ガバナンス、資産管理、脆弱性管理、インシデント対応といった基本的な取組をより迅速かつ着実に実施するとともに、レジリエンスの観点から、重要サービスの継続や復旧力の向上にも継続して取り組む必要があります。

- 「要請文の概要」について、ポイントを絞って説明します。

- まずは、フロンティアA I への対応を経営課題として扱うことです（資料①）。

サイバー攻撃によるインターネットバンキングや決済機能の停止や顧客情報の漏えいは経営に直接影響します。

このため、経営トップのリーダーシップの下、C I OやC I S Oのみならず、業務部門やリスク管理部門を含めた組織横断的な体制で対応を進める必要があります。

- そして、優先的に対応すべきサービス／I Tシステムを特定することも重要です（資料②）。

フロンティアA Iによって脆弱性が大量に発見された場合、金融機関側では速やかにパッチを適用していくことが求められます。

しかしながら、発見される脆弱性が大幅に増加した場合には、パッチ適用の負荷が著しく増加することとなり、全てのシステムを一律に防御することは困難です。

このため、優先的に対応すべきサービスやI Tシステムを予め特定し、リソースを重点的に配分するなど、リスクベースで対応することが重要です。

例えば、インターネットバンキング等の重要業務を支える外部公開I Tシステムについては最優先で対応することが考えられます。

- こうして特定した資産について、発見された脆弱性に迅速に対応するために、技術負債を解消しておくことが必要です（資料③）。

脆弱性が大量に発見された場合に重要となるのは、自らが保有しているシステムやソフトウェアの構成を正確に把握できているかという点です。

具体的には、どこにどのようなシステムが存在し、どのようなソフトウェアが稼働しているのかを把握できていなければ、脆弱性が発見された際に、その影響範囲を迅速かつ正確に特定することができません。

また、不要なネットワークポートの閉鎖や未適用パッチへの対応、さらにはサポートが終了した製品の更新など、技術的負債を平時から解消しておくことも重要です。

- パッチ適用プロセスをリスクベースにすることも重要です（資料⑥）。

脆弱性が大量に発見される状況においては、全ての脆弱性に同一の優先順位で対応することは現実的ではありません。

そのため、リスクに基づく優先順位付けが重要となります。

多くの金融機関では共通脆弱性評価指標スコアや攻撃コードの有無等に基づきパッチ適用の優先順位を決定していると考えられますが、必ずしもスコアの高い脆弱性のみが攻撃対象となるものではありません。

このため、金融機関においては、発見された脆弱性が自組織のサービスやITシステムに及ぼし得る影響を適切に把握するとともに、攻撃が成立する蓋然性も踏まえ、リスクベースで優先順位付けを行い、よりリスクの高い脆弱性から迅速かつ着実に対応する必要があります。

- また、パッチ適用以外の対策も強化することが重要です（資料⑦）。

パッチ適用に要する期間の短縮が困難な場合等は、仮想パッチの適用等、複数の対策を組み合わせた多層防御の強化を図る必要があります。

また、ネットワーク分離や多要素認証の導入、端末における不正検知・対応機能の活用に加え、内部侵入後の横展開を防止するための対策等についても、可能な限り推進することが重要です。

- そして、重要なサービスの停止にも備えることも重要です（資料⑧）。

サイバー攻撃を完全に防御できない可能性があることを前提に、サービス・ITシステムの能動的な停止も選択肢の一つとして検討しておくことが必要です。

また、金融機関においては、そうした事態に備えて、サービス・ITシステムを停止する際の判断基準や手順を予め整理しておくなど、必要となる対応について早急に整理・点検するとともに、経営陣のリーダーシップの下、ITベンダーとも緊密に連携しつつ、態勢強化を加速させていくことが重要です。

- 最後に、外部との連携を維持・強化することも重要です（資料⑨）。

フロンティアAIを巡る脅威は極めて速いスピードで変化しており、一つの組織だけでその全てを把握し、対応することは困難です。

このため、金融ISACをはじめとする業界横断的な情報共有の枠組みや、監督当局や関係団体との連携を通じて、継続的に情報を収集することが重要です。

また、自らが得た知見や対応事例についても積極的に共有し、金融分野全体の防御力向上に貢献することが重要です。

<さいごに>

- フロンティアAIの登場により変化するサイバー脅威に対しても、資産管理や脆弱性管理、多層防御、インシデント発生時の備えといった基本的な取組は有効であり、従来以上のスピード感と実効性をもって実施することが重要です。

- 金融庁としても、金融機関のサイバーセキュリティ態勢の向上を図るため、検査・モニタリングのみならず、「公助」の取組を進めています。
- その一環として、2022 事務年度以降、毎年、サイバーセキュリティセルフアセスメント（CSSA）として、金融機関に自己評価の実施をお願いしています。

分析結果を金融機関に還元していますので、他の金融機関との比較を通じて、自組織の課題を把握し、必要な改善につなげて頂くとともに、金融業界全体のサイバーセキュリティが強化されることを期待しています。
- また、2016 年から、金融業界全体のインシデント対応能力の向上を図るため、金融業界横断的なサイバーセキュリティ演習（Delta Wall）を実施しています。

当該演習では業態ごとに、最新のサイバー脅威動向を反映したシナリオを用意するとともに、参加金融機関に対して演習結果の評価を還元し、改善に向けた取組につなげて頂いています。

さらに、非参加金融機関におけるインシデント対応能力の向上を図る観点から、演習結果を匿名化・一般化した上で、演習を通じて認められた課題や好事例について、業界団体を通じて還元しています。
- 今後もこうした取組を継続してまいります。

金融機関におかれても、A I を含む新たな技術の活用を進めつつ、基本的なサイバーセキュリティ対策を着実に積み重ね、金融システム全体のレジリエンス向上につなげて頂くことをお願いし、私からの説明は以上とさせていただきます。

（以上）