コンセプトペーパー
「次世代金融におけるデータ利活用とプライバシーの両立」

あらまし

金融のデジタル化が進む中で、「インスタントペイメントによる即時化・自動化」や「マイクロペイメント」「決済のアンバンドリング」といったイノベーションが中長期に進行することが期待されている。また、ホールセール・クロスボーダーの決済インフラ、中央銀行デジタル通貨（CBDC）、民間のデジタル通貨、セキュリティトークンといった分野で、ブロックチェーン技術の社会実装も進んでいる。

これからの次世代金融において、様々なビジネスロジックを通じたデータ利活用を行っていく上では、社会が安心してデジタル技術を受容していくべく、プライバシーが保護される必要がある。
我々は、次世代の金融インフラにおけるプライバシーは、ユーザーのニーズに応え、データ利活用などを通じてさらなる付加価値をもたらすことによって競争優位を築いていく上での重要な肝となっていくと考える。

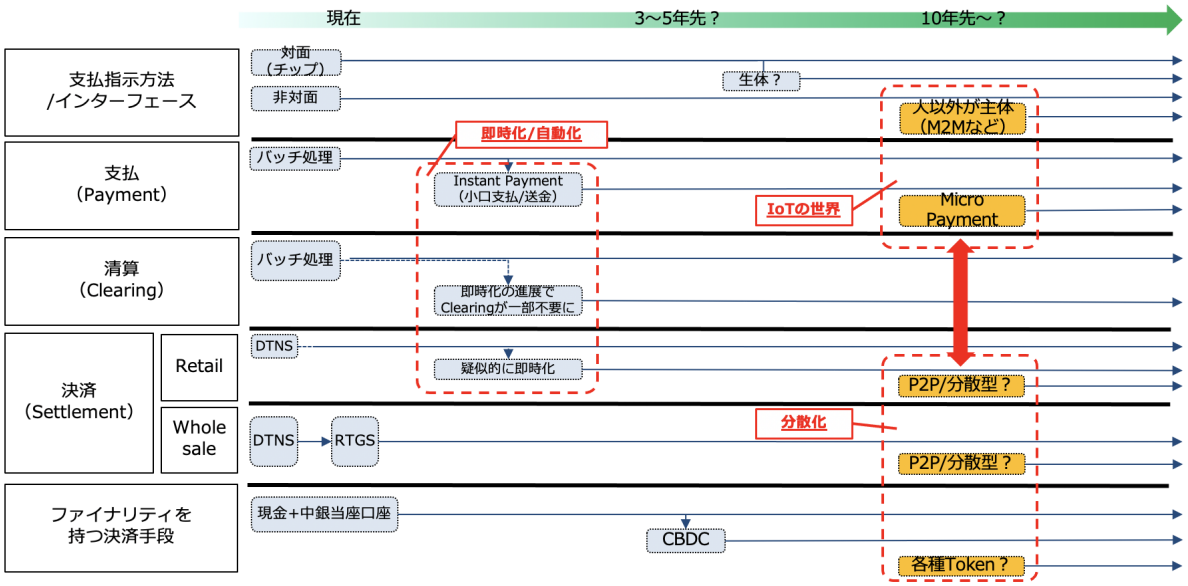
そのとき、秘匿化技術は、ビジネスを飛躍させるためにデータ利活用と「セキュリティやプライバシー」を両立させる上で、有効な手段となる。LayerXは、データ利活用とプライバシー保護を両立するべく、状態データを秘匿化したまま様々なビジネスロジックを実行可能とする秘匿化ソリューション「Anonify」の研究開発を進めている。

本稿では、データ利活用とプライバシー保護の両立にむけたユースケース仮説として、「取引トラッキング」「決済データ秘匿化とAML（アンチ・マネーロンダリング）」「複数社から持ち寄った決済履歴データの利活用」および「プログラマブル・ペイメント」という、4つのコンセプトを提案する。

1.イントロダクション

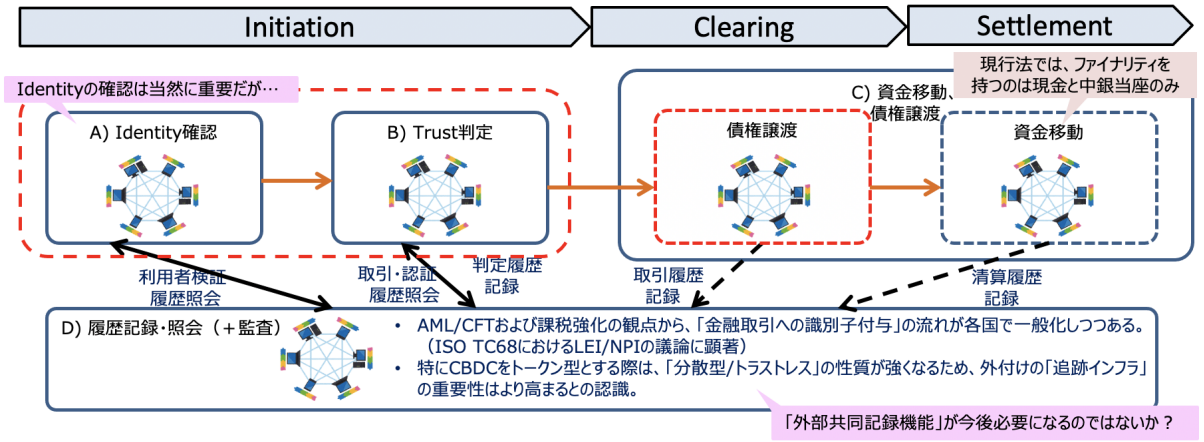
1.1.想定する決済領域の中長期変化

JCBでは、決済領域の中長期ロードマップにおける＜漸進的イノベーション＞として、「ペイメント分野におけるインスタントペイメントが進展する」「即時化の進展に伴うクリアリングが一部不要になる」などといった「即時化/自動化」を想定している。
これに加えて、＜抜本的イノベーション＞として、IoT技術やブロックチェーン上のスマートコントラクトが引き金となって、ヒト以外が主体のM2M取引のユースケースが登場することや、マイクロペイメントの手段が必要となることが考えられる。

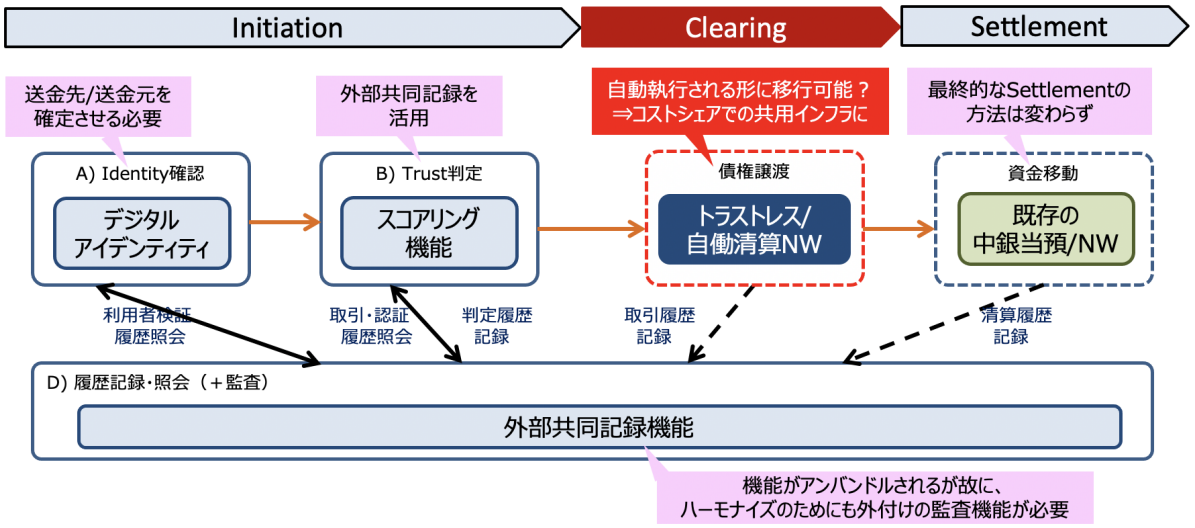


1.2.決済に関する機能のアンバンドリングに対する見立て

これら領域の変化の状況に加えて、決済に関する機能のアンバンドリングも進むと考えられる。例えばクレジットカード事業者は以下のうちSettlement以外の機能を一体のサービスとして提供していたが、今後は異なる主体がそれぞれの領域の機能を提供しつつ、連携する形になるのではないかと想定している。そのような1社に閉じないオープンなモデルにおいて必要となるのが、異なる機能提供者を跨ぐ形で処理が行われていることを「記録・照会」できることに加えて、外部(オーソリティを想定)から監査を行う「監査性」および外に向かって証明する「公証性」を備える基盤である。



また、「Clearing」「Settlement」が旧来の中央集権的なものであり続ける/自律・分散・トラストレスなもの（トラストレスな決済ネットワークの可能性としては「Payment・Clearingといった川上」を想定）へと移行していくかに拘らず、（既にそうした移行は進んでいるという認識ではあるが）下記のように機能がアンバンドルされた構造になっていくと想定している。



1.3.金融領域におけるブロックチェーン応用

一方で、分散台帳技術としてのブロックチェーンの応用が、金融領域においても進んでいる。新たな金融インフラを実現するテクノロジーとして、ホールセール・クロスボーダーの決済インフラ、中央銀行デジタル通貨（CBDC）、民間のデジタル通貨、セキュリティトークンなど活用例は幅広い。海外では徐々に研究・実証実験のフェーズを終えて本番稼働するプロジェクトも増えてきており、国内でも同様の動きが起こると思われる。[1]

1.4.ブロックチェーンの社会実装を進める上で大きな壁となる「秘匿性」

ブロックチェーンを活用し、つながるユーザーが増えるにつれ、機密性の高いまたはプライバシー情報をいかに第三者が閲覧できない状態にするか（秘匿化）が今後の技術的な焦点になる。多くの金融システムは金融機関や企業の機密性の高い情報を扱うため、ブロックチェーンで全参加者に共有することはできない。一方で、共有を避けていてはブロックチェーンの利点がなくなってしまう。

消費者のプライバシーに関する意識が高まりつつある中、決済データが多くの金融機関や企業に連携されることに心理的に抵抗を感じるユーザーも増える。例えば、欧州中央銀行（ECB）が行ったデジタルユーロのパブリックコンサルテーションにおいても、プライバシーを求める声が41%と最多であった[2]。特に、社会的公益へのデジタル技術活用を巡っては、「監視社会化」との懸念[3]がつきものであることから、データ利活用とプライバシー保護の両立をはかることが重要である。

---

[1] ブロックチェーン活用、「隠す」技術で攻める　LayerX中村龍矢執行役員（https://financial.nikkei.com/article/DGXZQOGD188UI0Y1A210C2000000）, 最終アクセス日：2021年6月19日

[2] 「ECB digital euro consultation ends with record level of public feedback」https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210113~ec9929f446.en.html, 最終アクセス日：2021年6月19日

[3] 「世界」2021年4月号（岩波書店刊）　P94中扉

1.5.データ利活用とプライバシー保護の両立をいかに実現するか

マネーロンダリングやテロリストなどに資金が流れることを防ぐための各種ルールを強制するには、決済実行時に何らかの判定ロジックを実行したり、疑わしい決済を追跡したりすることが必要だ。[4]また、決済データをファイナンスや与信などでビジネスに活かす時にも、決済データに対して複雑な処理を行う必要がある。こうした様々なビジネスロジックを通じたデータ利活用を、プライバシー保護と両立するには、どういった技術的手段があるだろうか。

単純な秘匿化技術として、暗号学的なアプローチ（例：ゼロ知識証明）を挙げることができる。これは、トランザクションが引き起こす状態遷移から秘匿すべき情報を解釈することを不可能とすることによって、単純な送金額や送金者の秘匿化を（部分的に）実現するものだ。シンプルな送金だけであれば、暗号学的なアプローチで足りる一方、データ利活用をはかるべく、例えばAML/CFT（マネー・ロンダリング及びテロ資金供与対策）の各種ルールを強制したり、決済に際して判定ロジックを実行したりといった場合には、処理の柔軟性が十分ではないといった障壁につきあたる。また、ゼロ知識証明を生成するためには計算リソースがかなり必要となることも問題になる。このように、データ利活用とあいまって複雑で柔軟な処理を必要とする金融のユースケースにおいては、処理の柔軟性および計算リソースの面でネックとなるため、ゼロ知識証明のように暗号学的アプローチを用いた単純な秘匿化技術が直接解決策になることはない。

また、エンタープライズ向けブロックチェーンのプライバシー強化技術を用いることも考えられるが、CordaやHyperledger FabricおよびQuorumといった代表的なエンタープライズ向けブロックチェーンのプライバシー強化技術は、トランザクションデータに対してアクセスできるノードを制限する技術であるため、実現できるプライバシー保護レベルに限界がある（例：当技術はトランザクションの検証とプライバシーを両立しているのではなく、トランザクションデータにアクセスできるユーザーやノードを制限する技術であるため、トランザクションを共有するユーザーグループの中でのお互いに対してや、コンセンサスノードに対して対コンセンサスノードの匿名性・秘匿性を担保できない。詳細はLayerXのレポート[5]を参照されたい）。そのため、エンタープライズブロックチェーンにおいてプライバシー保護するためには、デフォルトで備わっているプライバシー強化技術だけでなく、アドオンでプライバシー強化技術も利用することが重要となる。

このように、複雑で柔軟な処理を必要とする金融取引において、単純な秘匿化技術では「処理の柔軟性」の面で不十分であり、エンタープライズ向けブロックチェーン のプライバシー強化技術では秘匿性の担保において限界がある。そこで、これらと異なるアプローチによる技術開発が活発になっている。有望な解の一つがTrusted Execution Environment (TEE) と呼ばれる技術である。これは、プロセッサのセキュリティー機能であり、特定のアプリケーションが他のソフトウエアから隔離保護された領域で実行されることを保証するものだ。TEEを用いる秘匿化アプローチでは、柔軟な処理を記述可能であることに加えて、計算リソースの消費も実用面でボトルネックとならない。そのため、LayerXでは、アドオンで利用可能なセキュリティ・プライバシー保護技術「Anonify」の開発を、TEEを用いて進めている。

---

[4] ブロックチェーン活用、「隠す」技術で攻める　LayerX中村龍矢執行役員（https://financial.nikkei.com/article/DGXZQOGD188UI0Y1A210C2000000）, 最終アクセス日：2021年6月19日

[5] 「エンタープライズ向けブロックチェーン基盤比較レポート[プライバシー編]を公開 -独自のフレームワーク「LEAF」に基づき分析-」（https://layerx.co.jp/labs/insights/leaf_privacy/）, 最終アクセス日：2021年6月19日

手法	概要	処理の柔軟性 データ利活用	複数者間での秘匿性 プライバシー保護
ゼロ知識証明 （暗号学的アプローチ）	ビジネスロジックの完全性を暗号学的に保証	▲	○
エンタープライズブロックチェーン	共有するノードを限定することで秘匿化を実現する	○	▲
TEE	ハードウェアレベルの機能でビジネスロジックの完全性を保証	○	○

1.6.LayerXの秘匿化ソリューション「Anonify」

「Anonify」は、Trusted Execution Environment (TEE) を用いた秘匿化・プライバシー保護技術（特許取得済）である。TEE技術の利用例としては、Visaの研究開発部門（Visa Research）も、個人の機密データについて、TEE内で処理した上で、演算結果を受け取るシステムについて論文として発表している[6]。他の秘匿化技術と比較すると、様々なアプリケーション（金融、産業、行政）における匿名化・秘匿化を実現可能なことが特徴だ。

Anonifyの詳細については、「暗号と情報セキュリティシンポジウム（SCIS2021）」にて発表した論文「Anonify: プライバシーを保護した検証可能な状態遷移モジュール」[7]を参照されたいが、本ペーパーでは例え話を用いて、Anonifyが実現する世界観・概念を説明する。

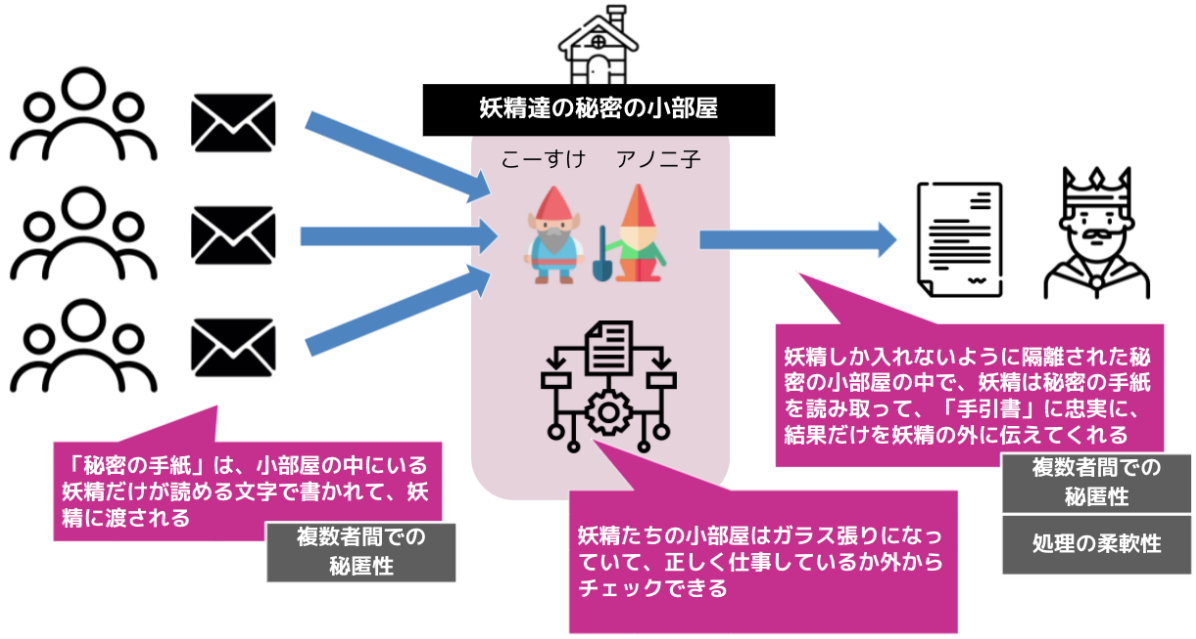
1.6.1.Anonifyが実現する世界観　～ (1) 王様と妖精達のものがたり ～

ある国の王様は、最近講じた政策に民衆の支持が過半を得ているか気になっているものの、民衆は正直に伝えるのを嫌がっていた。そこで困った王様は、「秘密の小部屋に住んでいる妖精たち」に助けを求めた。民衆の書いた「秘密の手紙」は、妖精だけが読むことができる文字で書かれている（＝秘匿化）。そして妖精たちは、民衆の声をもとに政策の支持率を集計する手順が記された「手引書」に忠実に従って、集計を行う（＝処理の柔軟性）。王様は、妖精たちの助けを借りて、民衆の不支持に気付き、自身の政策を改めたという。

---

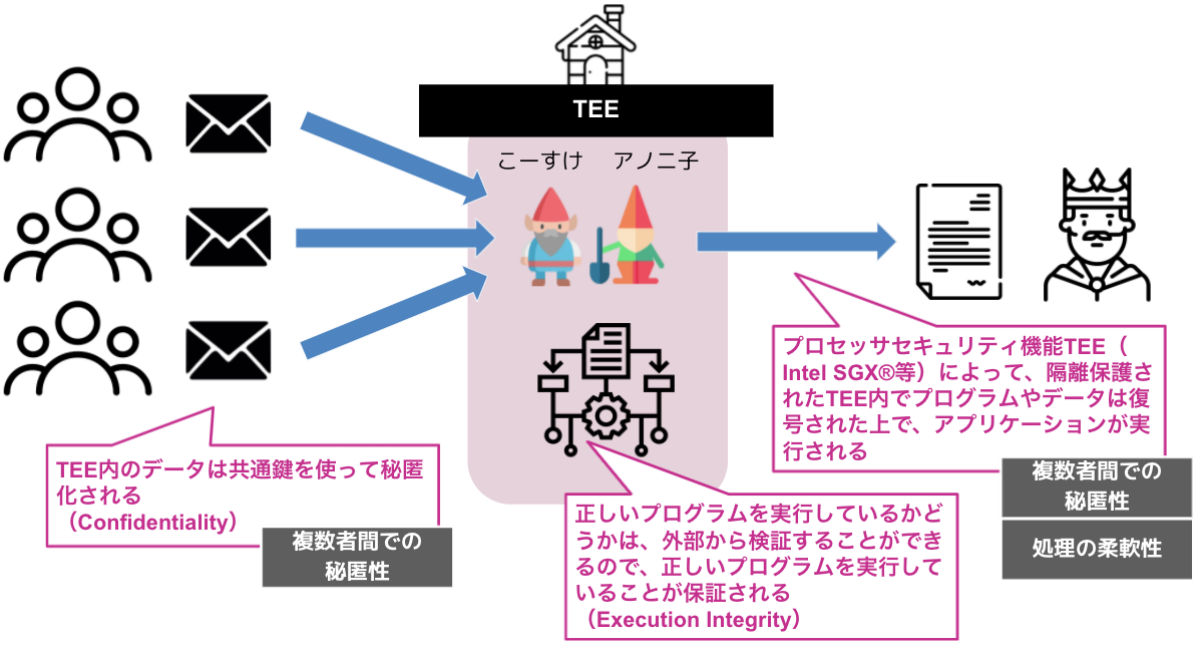
[6] LucidiTEE: A TEE-Blockchain System for Policy-Compliant Multiparty Computation with Fairness（https://eprint.iacr.org/2019/178.pdf）, 最終アクセス日：2021年6月19日

[7] 「Anonify: プライバシーを保護した検証可能な状態遷移モジュール」（https://layerx.co.jp/wp-content/uploads/2021/02/anonify-scis2021.pdf）, 最終アクセス日：2021年6月19日



1.6.2.Anonifyが実現する世界観　～ (2) 技術的な解説 ～

上述の「妖精達の秘密の小部屋」が、プロセッサのセキュリティ機能によって、隔離保護されたTEEである。TEE内のデータは共通鍵を使って暗号化される。そしてTEE内でプログラムやデータを復号した上で、アプリケーションが実行され、結果だけが出力される。このとき、TEEにはOSすらアクセスすることができないため、システム管理者すら元データにアクセスすることは不可能であり、データの秘匿性が担保される、という仕組みだ。



1.6.3.Anonifyによる秘匿化の価値

Anonifyで暗号化されて管理されたデータは、たとえ内部犯であっても、平文にアクセスすることはできない。そのため、「外部からの攻撃・ハッキングのリスク」「従業員や業務委託先の内部犯行のリスク」および「運営者がデータを閲覧できることに対するユーザーの懸念」を大きく低減することができる。これは、自社のデータを扱う際のセキュリティ・プライバシーを担保する上で有用であるばかりでなく、他社とのデータ連携・共有を通じた利活用を行う際にも有効である。例えば、複数社から持ち寄ったデータの名寄せをTEE内で行うことによって、プライバシー・セキュリティを担保しながら名寄せ（同一ユーザーの情報を1つのデータとして統合）した上で、統計分析処理の結果のみを出力するケースを考えることができる。

2.ユースケース仮説

本稿では、データ利活用とプライバシー保護の両立をはかる必要のあるユースケース仮説として、「取引トラッキング」「決済データ秘匿化とAML」「複数社から持ち寄った決済履歴データの利活用」および「プログラマブルペイメント」という4つを以降の節で紹介する。

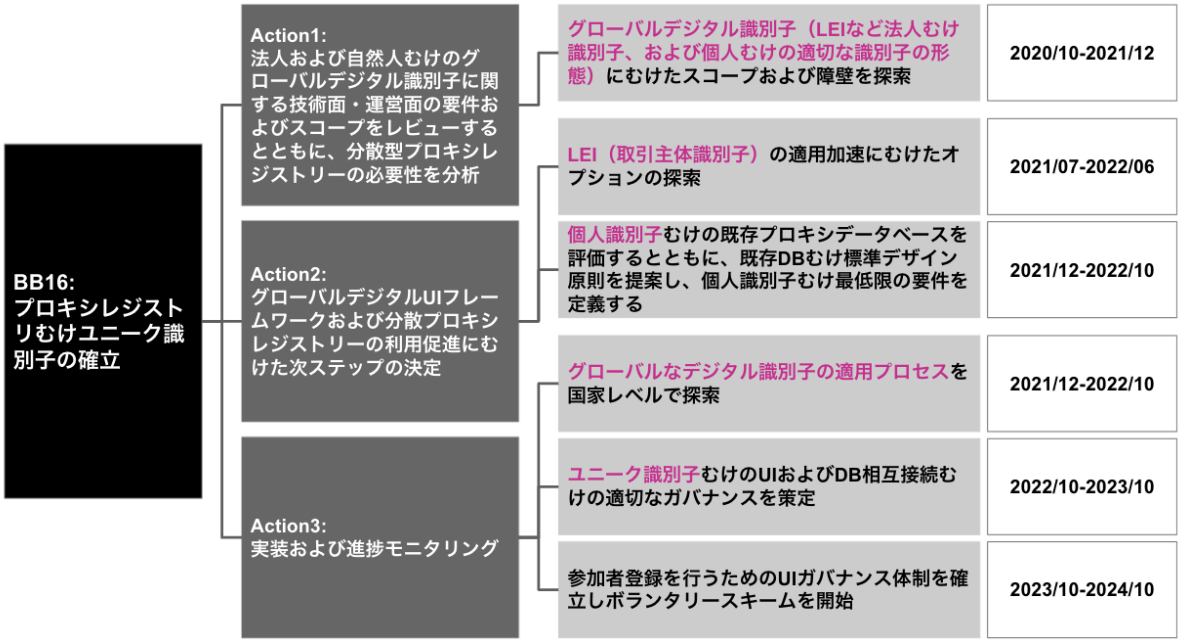
	データ利活用	プライバシー 保護
取引トラッキング	• 決済データへの識別子付与を通じた、トラッキングや監査レポート	• 疑わしい対象取引以外は秘匿したまま、特定の取引IDや法人・個人識別子に基づいて取引をトラッキング • 当局に個別取引の内容を見られないまま、監査レポートのみを提出
決済データ秘匿化とAML	• 疑わしい取引を業者間で共有することによって、個別業者のAML効率向上・不正検知負担軽減	• 警察捜査の一次情報となる個別の情報を明かすことなく、取引OK・NGの結果のみを返す
複数社から持ち寄った決済履歴データの利活用	• 決済履歴を法人・個人の識別子をキーとして購買履歴と紐付けることによって、顧客の好みを理解し、パーソナライズドオファーを提供	• 個々の決済データと購買データを秘匿したまま、識別子をもとに同一ユーザーの情報を１つのデータとして名寄せ・統合
プログラマブルペイメント	• 顧客の自動車などから収集した情報をもとに、安全運転スコアなどの計算結果を取得し、それに応じた保険料を算出	• 位置情報などを秘匿化したまま、安全運転スコアなどの計算処理を実施

2.1.ユースケース①取引トラッキング

2.1.1.重要度が増す「外部共同記録機能」：識別子を用いたトラッキングの一般化

まず、1.2節で触れた、”異なる機能提供者を跨ぐ形で処理が行われていることを「記録・照会」でき、外部(オーソリティを想定)から「監査」を実施できる基盤”をめぐるトピックについて紹介したい。

FSB（金融安定理事会）のロードマップ[8]において、法人や個人の識別子の利用が語られるようになっている。2022-2023年には、法人・個人の金融取引に識別子をつけることによって、データの真正性・秘匿性を担保しつつ、モニタリングや監査/レポーティングが楽にできるようになると見られる。OTC（Over The Counter）取引などの用途で先行する LEI（Legal Entity Identifier：取引主体識別子）に遅れる形にはなるが、2024年頃にはNPI（Natural Persons Identifier：自然人に紐づく識別子）も各国で当たり前のように利活用されるようになっているだろう。



出典：https://www.fsb.org/wp-content/uploads/P131020-1.pdf

LEIについては、McKinseyが、世界中の取引主体を一意に識別するために金融安定理事会によって設置された国際的中央運営機関であるGLEIF（Global Legal Entity Identifier Foundation）との共著として発表したLEIユースケースホワイトペーパー[9]の中で、「取引相手の識別におけるトランザクション・オペレーション面をスムーズにする他、特定取引における法人のバックグラウンド情報へのアクセス・追跡可能性を向上」できるとした上で、「信用状の処理を高速化する他、電子インボイスネットワークにおける売り手の識別、借り手のKYCデューデリや情報トレーサビリティに有用」としている。

LEIのユースケースでも触れられている追跡可能性（トレーサビリティ）については、銀行間の国際金融取引に利用される国際金融決済システム（SWIFT）でも類似の仕組みがある。SWIFT gpiのTracker[10]では、Trackerを使うことによって、銀行はgpi送金の状態をリアルタイムで追跡することが可能になっている。具体的には、送金を一意に特定するユニークなリファレンス番号（Unique end-to-end transaction reference：UETR）がSWIFTを利用した全ての送金に必須となり、その結果全ての送金メッセージは迅速・効率的 に追跡できるようになるというものだ。

[8] Enhancing Cross-border Payments - Stage 3 roadmap（https://www.fsb.org/wp-content/uploads/P131020-1.pdf）, 最終アクセス日：2021年6月19日
[9] McKinsey & Company and GLEIF White Paper: Creating Business Value with the LEI（https://www.gleif.org/en/lei-solutions/mckinsey-company-and-gleif-creating-business-value-with-the-lei）, 最終アクセス日：2021年6月19日
[10] The Basic Tracker（https://www.swift.com/ja/node/234706）, 最終アクセス日：2021年6月19日

2.1.2.海外におけるトラッキング/トレースの動向

この他、海外では米国および中国において、トラッキング/トレースが一般的になる方向にある。米国では、国立標準技術研究所（NIST）が財務省・国防総省と協働でブロックチェーンを用いたペイメントのトラッキングについて、暗号化機能の課題特定などを目的とした実証実験を、このほど発表した[11]。これは、連邦準備銀行からの助成金を対象としたトラッキングである。信用状（L/C）を表象するブロックチェーンベースのトークンおよび銀行口座と紐づいたウォレットを用いて、助成金支払いをトラッキングするものだ。トークンは受領者識別子や金額・日付など表象し、換金可能で受領者のレポーティングやモニタリング要件の緩和につながるとしている。同様に、中国でも、法定通貨の電子化と並行して、政府補助金/助成金を想定してトラッキングを可能にしようというコンセプトを打ち出している模様である[12]。

中国人民銀行は、デジタル人民元の開発を進行中であるが、「コントローラブルな匿名性」[13]がデジタル人民元のデザインの中核であり、完全なる匿名性はオプションに無いことを表明している。決済手段としてだけでない監視ツールとしての用途にも言及しているほか、AMLや脱税目的での利用可能なデザインは受け入れられないことから「コントローラブルな匿名性」は国際的なコンセンサスである、という見方も示している。

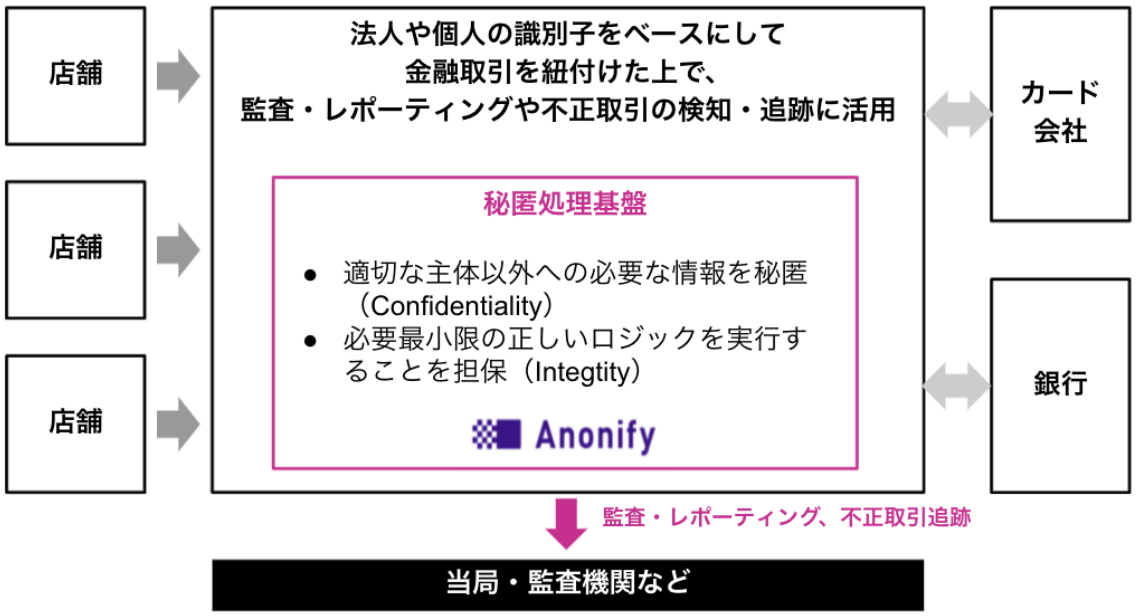
なお、中銀デジタル通貨については本稿のトピックではないが、国際決済銀行（BIS）も、CBDCの特性として、中央銀行によるコントローラビリティに言及している点にも注目している[14][15]。こうした動向を踏まえ、先んじて民間主導の仕組みを用意できると有益ではないかと考えている。

2.1.3.決済データへの識別子付与を通じたトラッキング

決済のアンバンドリングが進む中で、異なる機能提供者をまたぐ形で処理が行われていることを「記録・照会」でき、外部オーソリティが「監査」できる「履歴の外部共同記録機能」を想定してみたい。民間の決済インフラの決済データに、法人や個人の識別子を紐付けることによって、当局がトラッキング可能になると考えている（次章で述べるように、銀行などの既存プレイヤーにとって、履歴情報の提供メリットとして、AML業務の負担低減への応用可能性も想定できる）。

---

[11] CFO Office of the Future（https://www.nsf.gov/oirm/bocomm/meetings/fall_2018/15_CFO_Office_of_the_Future_Presentation.pdf）, 最終アクセス日：2021年6月19日
[12] The Goldman Sachs Group, Inc. "Reinventing the Yuan for the Digital Age", p26（https://www.coindeskjapan.com/88816/）, 最終アクセス日：2021年6月19日
[13] PBoC official says 'completely anonymous CBDC is not an option'（https://www.theblockcrypto.com/linked/98925/pboc-anonymous-cbdc-not-option）, 最終アクセス日：2021年6月19日
[14] How CBDCs Give ‘Absolute Control’ to Central Banks（https://www.coindesk.com/podcasts/coindesk-podcast-network/cbdcs-give-central-banks-absolute-control）, 最終アクセス日：2021年6月19日
[15] Central Bank Digital Currencies will grant authorities “absolute control” over money（https://goldandsilveruk.co.uk/central-bank-digital-currencies-will-grant-authorities-absolute-control-over-money/）, 最終アクセス日：2021年6月19日

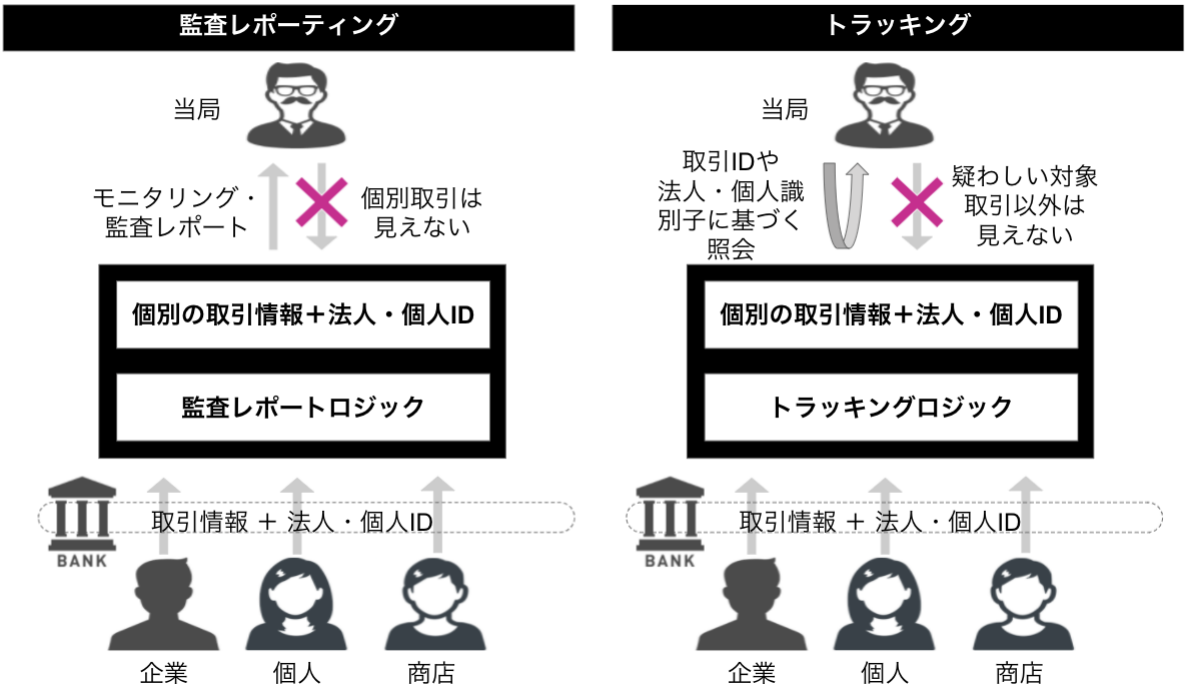


このときに重要なのが、プライバシー保護とデータトラッキングの折り合いだ。当局によるトラッキングを行うことは、プライバシー保護と対立するものとして考えるのではなく、プライバシー保護とデータトラッキングに折り合いをつけるための工夫を行うことが必要である（参考文献[16]）。そのため、プライバシーとトラッキングを両立すべく、適切な主体以外への必要な情報を秘匿することを要件としたい。

2.1.4.取引を追跡可能とする上で必要なプライバシーとの両立

前述の「決済データへの識別子付与を通じたトラッキング」基盤において重要なのが、データの真正性・秘匿性を担保しつつ、監査レポートロジックやトラッキングロジックを実行できることだ。前者の「監査」においては、当局に個別取引の内容を見られないまま、監査レポートの結果のみが当局にわたるようにすべきだ。一方、後者の「トラッキング」においては、疑わしい対象取引以外は秘匿化されたまま、特定の取引IDや法人・個人識別子に基づき照会できることが必要である。

[16] 宮下紘『プライバシーという権利』（岩波書店刊）



2.1.5.履歴の蓄積・参照・追跡に必要となる機能

上記を踏まえ、「履歴の蓄積・参照・追跡に必要となる機能」を考えてみる。単純な履歴の蓄積・参照に加えて、情報開示請求などをうけて、修正・削除（論理削除）の対応と、それが虚偽だった場合に（論理削除した履歴の）復旧を可能にしたいというニーズは履歴の基本的な管理機能として出てこよう。これに加えて、当局むけ監査レポートの作成機能や、特定の当局に対してのみ取引や法人・個人の識別子に基づく履歴を開示する追跡機能が考えられる。

2.2.ユースケース②決済データ秘匿化とAML

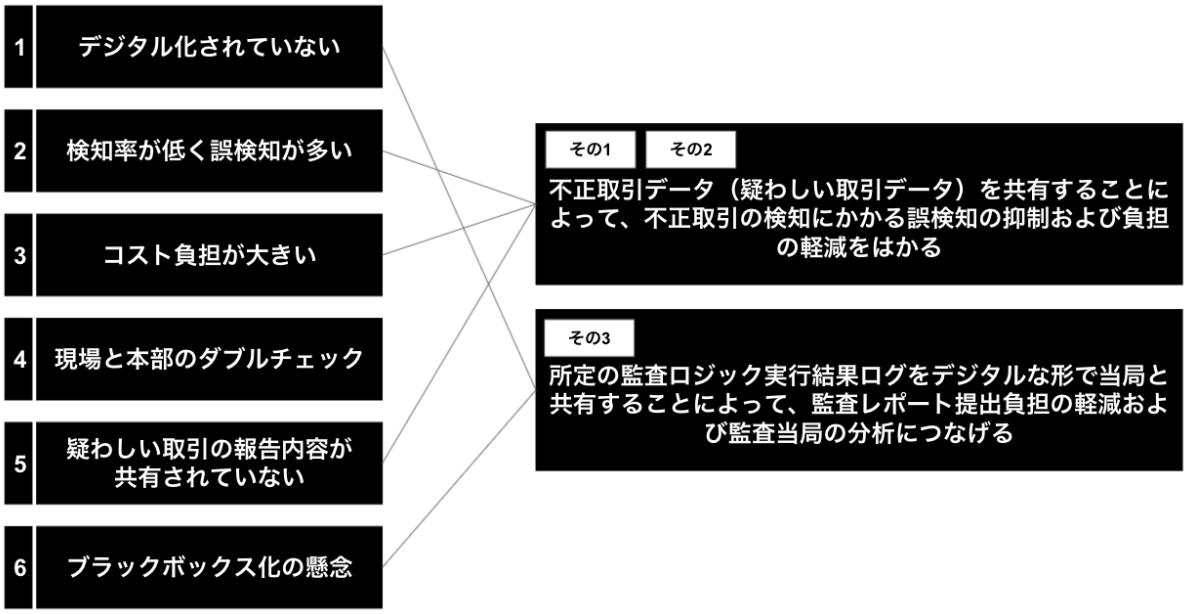
2.2.1.既存のAMLプロセス・ソリューションが抱える課題

現行のAMLプロセスは、検知率が低く、規制が重くなる中にあってコスト面で維持不可能なものになりつつある。中でも、金融機関は、疑わしい取引の届出をしたことを他者に漏らしてはならないため、金融機関どうしでの情報共有が進まず、各金融機関の業務に大きな負担を強いることになっている。

1	デジタル化されていない	• 入り口からして「顧客から徴求した本人確認書類や、担当者が対面確認で得た情報を収集・蓄積してインプット」となっており貧相な現状
2	検知率が低く誤検知が多い	• シカゴ大学のレポートの推計によれば、ロンダリングされた資金のうち、うまく捕捉されたのはわずか0.2%である。（出所：Bank4.0）
3	コスト負担が大きい	• 法令や指針、条例に準じた新たな対応が継続的に求められており、結果としてコストの増大も招いており、規制がさらに重くなる中で維持不可能に
4	現場と本部のダブルチェック	• 窓口担当者にとってAMLは数十ある確認観点（個人情報など）の一部 • 本部側で「リスト照合・目検」や「全顧客の継続的顧客管理」など体制を敷いている分の負担も大きい
5	疑わしい取引の報告内容が共有されていない	• **届出をしたことを他人に漏らしてはならないことになっている**
6	ブラックボックス化の懸念	• ベンダーソリューションは必要以上に複雑・独自のアルゴリズムを採用しているため、監査や利害関係者へ有効な説明ができない場合がある

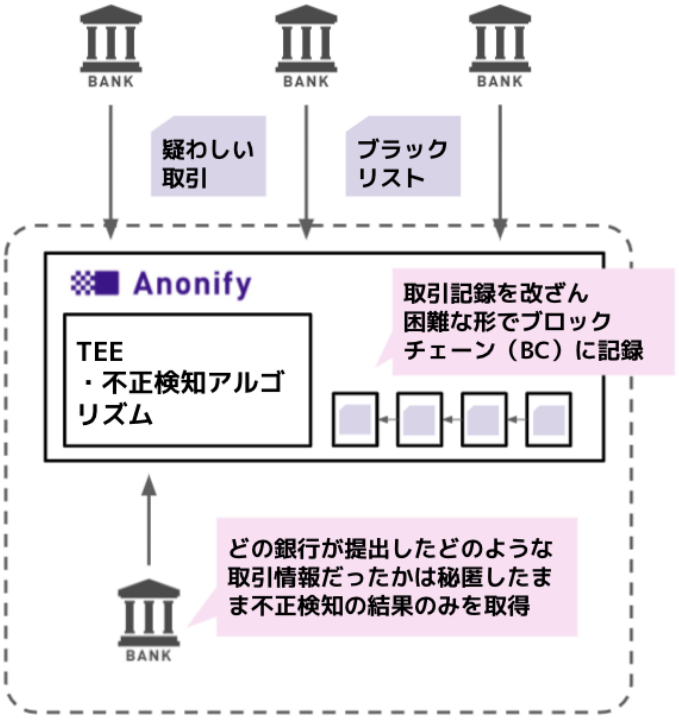
2.2.2.AMLプロセス・ソリューションが抱える課題の解決方向性

そこで、不正取引データ（疑わしい取引データ）の共有を図ることによって、金融機関の不正検知負担を軽減することができないだろうか。また、所定の監査ロジック実行ログを当局と共有することで、金融機関および当局の監査負担を軽減することが考えられる。
このとき、情報共有のプラットフォームとしては、共同運用形態の外部機関によって運営されることによって、金融インフラの一部として銀行・証券など業界横断のプラットフォームを実現することを想定する。現在、個別金融機関がそれぞれソリューションを導入しているのに対して、これは社会インフラ・公共財としてのシステムを提供する位置付けに近い。



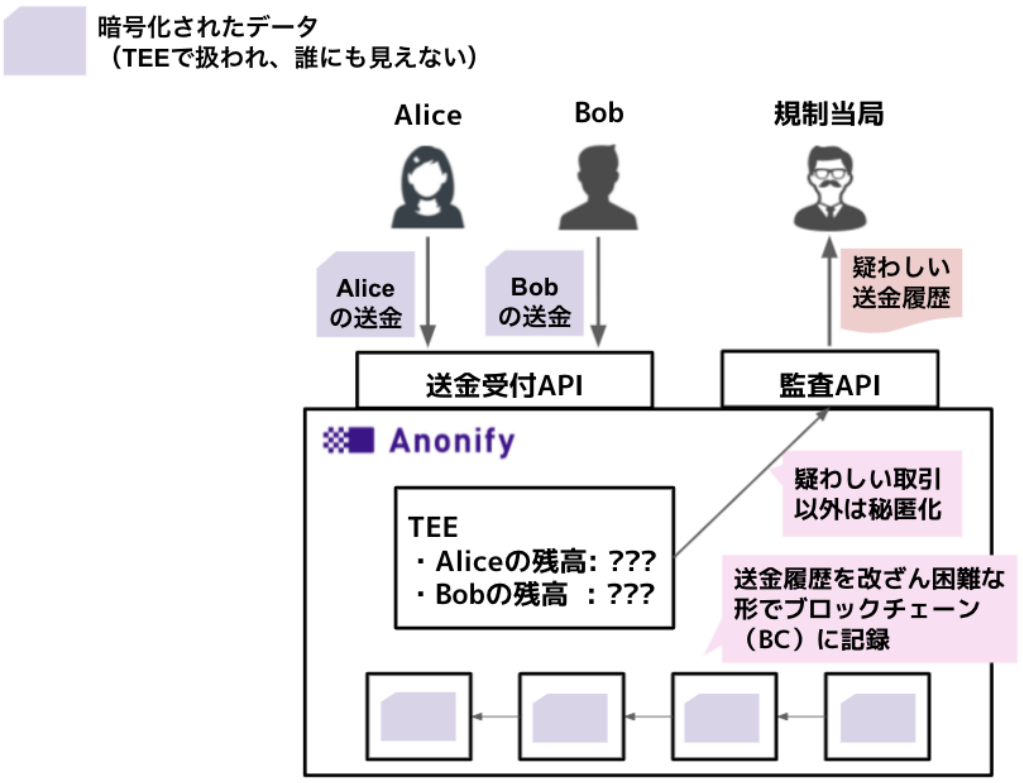
2.2.3.疑わしい取引の銀行間共有

AML業務において、金融機関同士で共有できずそれゆえに検知率があがらない（取りこぼしがある）ことを課題として設定する。その解決策として、ブラックリスト/疑わしい取引を業者間で共有することによって、個別金融機関のAMLに役立てられないだろうか。
その実装方法としては、いくつか考えることができる。まず一つは、特定条件満たす情報がないか閲覧するというものだ。たとえば、当該の口座番号がブラックリストに掲載されているかどうかの結果のみを参照し、口座番号などを入力すると、OK/NGが返ってくるというものが考えられる。このとき、警察捜査の一次情報となる個別の情報は明かすことなく、OK/NGの結果のみを返すという仕組みが望ましい。あるいは、特定条件満たす情報があった場合にPush型で通知してもいいだろう。たとえば、口座番号がブラックリストに掲載されている取引があった場合に、その旨を銀行へ通知するというものだ。



2.2.4.当局監査対応の効率化

所定の監査ロジックを実行した結果ログをデジタルな形で当局と共有することによって、監査レポート提出負担の軽減および監査当局による分析につなげることも有効だ。



2.3.ユースケース③複数社から持ち寄った決済履歴データの利活用

2.3.1.データ利活用と消費者の視点

従来は単一組織内において、自組織にかかるデータの利活用が進められてきた。販売計画策定・人材配置計画・収益管理などといったデータの取得や連携の仕組みが整備される中で、昨今では「官＜＞民」「民＜＞民」といったように、組織を横断したデータ連携・データ利活用が検討されるようになっている。

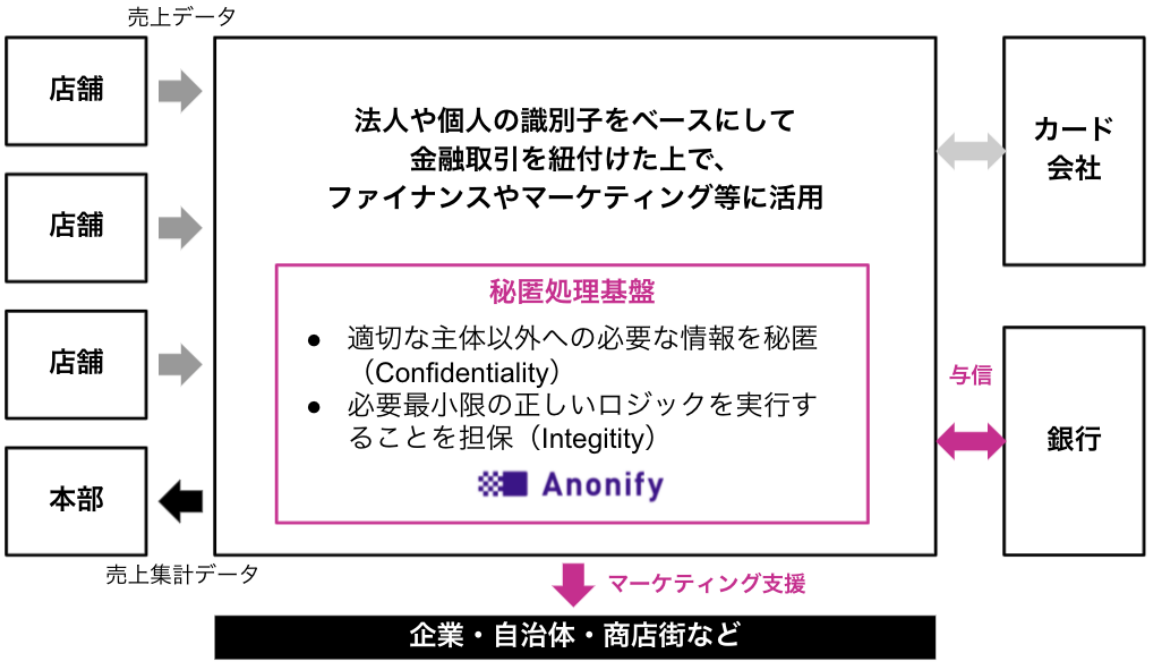
たとえば、決済において、商品の情報や購入者の属性といった具体情報を把握することができることによって、個別企業に対する融資・ファイナンスの与信材料としたり、個別店舗に対するマーケティング支援を行う上での材料としたりといったことができる。

さらには、独立第三者機関の管理する履歴データをもとに、個人を特定しない形で、決済履歴データを公的な基礎統計データとして利用することも想定できる。例えば、「年齢が40歳代で商品xxxを好む層の消費者には、xxxといった傾向がある」「2021年4月に商品xxxを購入した人数の地域別分布」といった統計情報を把握するための利用が一案である。

このような中では、官民・民民のデータ連携・データ利活用を通じた、「他社に知られたくない」という情報管理要件と併せ、対個人との関係において「自身に関するプライバシーを保護したい」という要件を考慮する必要がある。

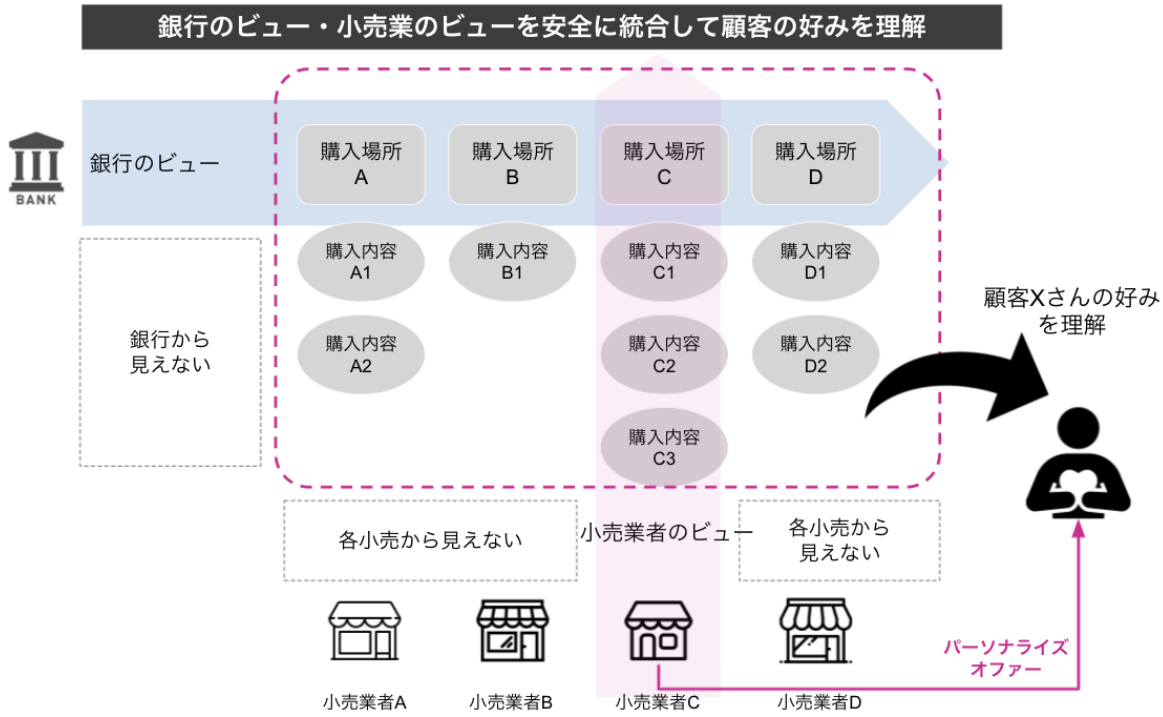
2.3.2.秘匿化された決済履歴を用いたデータ利活用基盤

決済履歴（商品や購入者の属性を含む）を法人・個人の識別子をベースにして、銀行・地域のサプライチェーンなどと紐付けることによって、決済データをAMLの他にファイナンスやマーケティングに活用することが考えられる。このとき、決済インフラ全体を秘匿化した上で、ファイナンス・マーケティングなど必要最小限のロジックを実行することを担保することができるとしたら、どうだろうか。



これに近い例としては、カナダのRoyal Bank of Canada (RBC)が、Microsoft Azure Confidential Computingを用いてデータを元にプライバシー保護しながらパーソナライズオファーを生成するVirtual Clean Room (VCR)のパイロットを実施している[17]。想定されるのは、銀行が持つ「どこで決済しているかの好み情報」と小売業者の持つ「何を購入しているかの好み情報」について、プライバシーを維持したまま組みあわせることによって、パーソナライズオファーを提供可能にするというものだ。銀行・小売業者ともに、お互いのデータは見えない（秘匿化）まま、顧客の好みを理解できる点が特徴である。

[17] RBC creates relevant personalized offers while protecting data privacy with Azure confidential computing（https://customers.microsoft.com/en-us/story/1356341973555285762-royalbankofcanada-banking-capital-markets-azure）, 最終アクセス日：2021年6月19日



2.3.3.データの利活用を柔軟に行うために

データの利活用を柔軟に行う方法としては、「本人同意を得て利活用する方法」「特定の個人を識別できないようにすることで本人同意をとらずに利活用する方法（匿名加工情報など）」の2つがある。今後のデータ利活用を展望した際、これらの方法に対して様々な意見がみられるので、紹介したい。

まず同意管理に対しては、「複雑・大量かつ修正不可な利用規約やプライヴァシーポリシーによりユーザーとの関係を規律している現状からは、ユーザーが自発的・主体的に同意できているか、自由な意思決定ができているかと問われれば、心許ないと言わざるをえない」[18]のように、ユーザーの自発性・主体性を問うものがある。また、「何でも同意を求められて“同意疲れ”になる。先のことを予想できず、わからないまま同意してしまうこともある」[19]や「特にGDPR以降、「通知と同意」の必要性は認識されたが、一方で「同意万能」のような流れも生まれてしまっており、改めて「結局、同意って何なんだろう」とその難しさを感じる」[20]といったユーザーからみた「同意疲れ」を問うものもある。

一方で匿名化については、現時点で実装されているプライバシー保護対策のほとんどが匿名加工であることを踏まえて「現時点で実装されているプライバシー保護技術は、ほとんどが匿名化であり、プライバシーの保護性は高いが、一方で統合解析の観点からはデータの質は落ちてしまう。」[21]のように、分析・解析への利用のしにくさを問う意見が見られる。

---

[18] 「同意する」とは、どういうことか？：水野祐が考える新しい社会契約〔あるいはそれに代わる何か〕Vol.4（https://wired.jp/2021/01/15/new-trust-new-social-contract-4），最終アクセス日：2021年6月19日
[19] 根づくか「情報銀行」 金融機関や流通大手が参入、情報提供でポイント還元も（https://dot.asahi.com/wa/2021010700020.html?page=3），最終アクセス日：2021年6月19日
[20] 【事務局レポート】JIPDECセミナー100回記念「デジタル社会に生きる」年末放談会「デジタル社会を進む私たちに必要な視点とは」（https://www.jipdec.or.jp/library/report/20201215_02.html），最終アクセス日：2021年6月19日
[21] プライバシー保護技術に関する動向と医療ヘルスケアデータの利活用における示唆（http://www.jpma.or.jp/opir/news/061/pdf/no61_p09.pdf）

今後のデータ利活用を想定すると、上記のアプローチに加えて、「データそのものを共有することなく、秘匿したまま処理する方法」の可能性についても、技術やUXに加えて制度面の双方からのアプローチも必要ではないだろうか。そうした多面的なアプローチを視野に入れ、今後検討していきたい。

2.4.ユースケース④プログラマブル・ペイメント

2.4.1.「デバイスなどから得られるプライバシー情報」と「おカネにまつわるプライバシー情報」

IoT技術が進展する中で、コネクテッドデバイスから取得できる情報が増加している。それに伴い、決済・購買データといったお金に直接かかわるプライバシー情報とは別に、車両の位置データといった、直接お金に関わらない、デバイスから得られるプライバシー情報にも、注目が集まっている。例えば、コネクテッドモビリティのデータ共有において、一見匿名にみえる位置情報からも、他のデータセットを相互参照するなどを通じて、ドライバーの身元を明らかにすることが可能だ。具体的には、出発地と目的地の位置情報、その訪問頻度などから住居や勤務先を特定できる。中期的には、モノの移動をトリガーとして決済が行われるといった「プログラマブル・ペイメント」として、「モノのプライバシー」と「おカネのプライバシー」が交わっていくことが想定されることから、次世代金融をめぐるプライバシーのユースケースの締めくくりとして紹介したい。

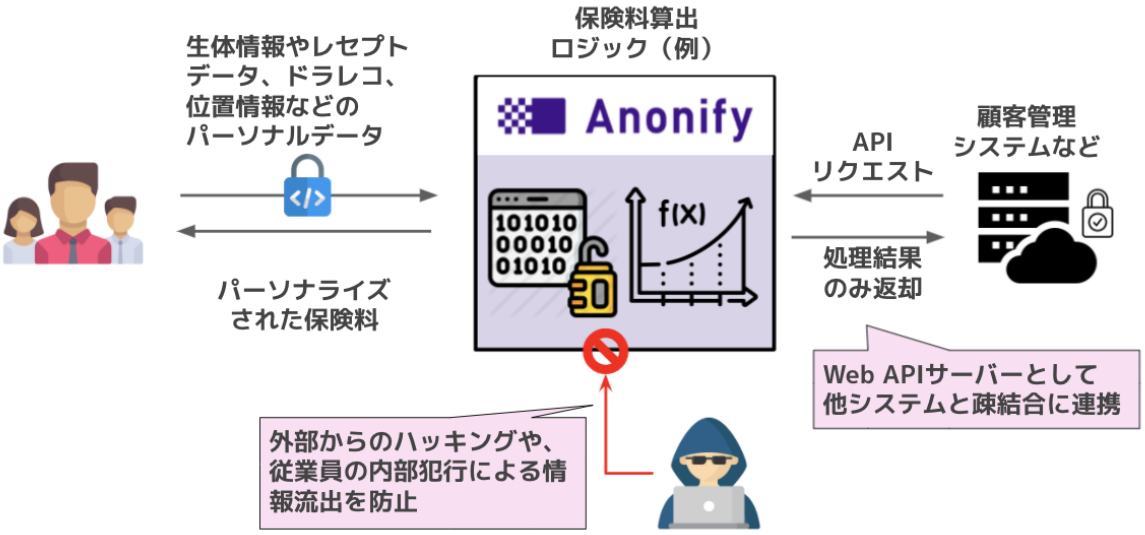
2.4.2.保険のパーソナライズ

損害保険業界において、カーナビやドライブレコーダーなどのデバイスから抽出される自動車の走行情報より運転特性を導くことによって、保険料などのサービスをパーソナライズすする保険商品の提供が盛んになっている。従来は、顧客の運転特性に関わらず画一的な自動車保険サービスを提供していたのに対して、運転走行情報、速度超過や危険挙動（急アクセル、急ブレーキ、急ハンドルなど）から安全運転度をスコア化、スコアの高さに応じて保険料割引が受けられるようになるというものだ。

こうしたパーソナライズ保険の提供に際して、さらなるパーソナライズ度合いを高める上にでは、速度情報や危険挙動だけでなく、位置情報や社内外録画情報などの活用が不可欠であることから、プライバシー/セキュリティのトレードオフが存在する。

そこで考えられるアプローチが、ユーザーのデータ（位置情報など）を秘匿化したまま、安全運転スコアなどの計算処理を実行することによって、プライバシーやセキュリティに関する懸念を最小化するというものだ。顧客の自動車やスマートフォン、カーナビなどから収集した情報を、損害保険会社が閲覧不可の状態のまま処理する。そのため、安全運転スコアなどの結果だけを取得した上で、それに応じた保険料を算出することが可能となる（保険分野の取組については、LayerXのホワイトペーパーも参照されたい[22]）。

[22] 保険業界の最新トレンドである保険料のパーソナライズ実現におけるプライバシー保護（https://www.anonify.layerx.co.jp/anonify-for-insurance）



3.まとめ

3.1.金融デジタル化で求められる「データ利活用と秘匿化の両立」

下記に挙げる3つのトレンドにより、データ利活用と秘匿化を両立させることの重要度が今後一層高まると考えられる。

まず一点目は「商流データの結びつき」だ。現状、商流データは、決済手段や決済端末ごとに分断状態にあり、これらのデータの統合・追跡が経済DXの肝となる。今後は、決済履歴が多くの金融機関や企業が共有するインフラに溜まることとなり、それは日本のCBDCの役割の可能性の一つとなるだろう。そのとき、決済インフラに乗るデータの種類が増え、データのリスク増大が課題となる。そこで決済にかかわるプライバシーを保護すべく、秘匿化したまま、決済データを紐づけて活用できることが必要となる。

次に二点目は「金融機関・企業をまたぐデータ連携」だ。現状、金融機関の顧客の決済データ等は基本的に内部に閉じている。今後は、「メインバンクが異なる企業群からなるサプライチェーンの分析」や「不正送金履歴を共有して共同でAIを学習」といった形で、金融機関同士がデータを共有するニーズが生まれる。そのときに課題となるのが、営業秘密のため共有が進まない且つデータの信頼性が低い、ということだ。そこで、データを秘匿化したまま共有し、処理結果だけ各社に共有した上でお互いにデータの正しさを証明することが有用となる。具体的には、決済データへ電子署名したり、決済台帳にブロックチェーンを採用したりといったことが考えられる。

最後に三点目は「消費者・企業のプライバシー意識の高まり」だ。現状、個人・法人の決済データは、決済手段提供者は閲覧可能となっている。今後は、ユーザーのプライバシー意識の高まりにより、全てを閲覧される決済サービスは使われなくなる可能性が高まるだろう。そのとき、不正検知/AMLやデータの与信への応用などとの両立が課題となる。そこでは、不正検知ロジックなどを暗号化したまま実行できることが必要だ。与信の判定結果のみを算出し、職員は元データを閲覧できてはならない。

これら3つのトレンドに共通して言えるのは、単なる暗号化ではなく、「秘匿化と利活用のバランス」を可能とする技術が求められているということだ。

3.2.むすび

「プライバシー」は、徐々に「守りではなく攻め」のテーマになりつつある。プライバシーという言葉は今日、リスク管理やコンプライアンスの文脈で登場し、どちらかといえばネガティブなイメージを持っている読者も多いのではなかろうか。[23]

これまでの「プライバシー」は、リスク管理やコンプライアンスの文脈で「避けて通ることができないもの」であり、リスク低減を目的として、受動的に対応するものであった。これに対して、次世代の金融インフラにおける「プライバシー」は、ユーザーのニーズに応え、データ利活用などを通じてさらなる付加価値をもたらすことによって競争優位を築いていく上での重要な肝となっていく。そのとき、秘匿化技術は、ビジネスを飛躍させるためにデータ利活用と「セキュリティやプライバシー」を両立させる上で、有効な手段となる。

Anonifyは、マネーロンダリング対策やデータの利活用に必要な柔軟なビジネスロジックを組み込むことができるものであり、LayerXが特許を取得し、社会実装に向けて準備を開始している。そしてJCB・LayerXの共同研究では、BtoB取引履歴インフラにおける秘匿化とデータ利活用を両立するためにAnonifyを活用している。

本コンセプトペーパーが、日本の次世代金融におけるデータ利活用とプライバシーの両立にむけた、議論の本格化のきっかけになれば幸いである。（了）

次世代金融におけるデータ利活用とプライバシーの両立
2021年7月

発行
- 株式会社LayerX
- 株式会社ジェーシービー

協力
- 明治大学政治経済学部教授　小早川　周司
- ナッジ株式会社 代表取締役社長　沖田　貴史
- 株式会社LayerX 執行役員 兼 LayerX Labs所長　中村　龍矢

[23] ブロックチェーン活用、「隠す」技術で攻める　LayerX中村龍矢執行役員（https://financial.nikkei.com/article/DGXZQOGD188UI0Y1A210C2000000）, 最終アクセス日：2021年6月19日