2024 年 11 月８日
日本銀行決済機構局

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第 10 回会合の議事概要

１．開催要領

（日時）2024 年９月 11 日（水）14 時 00 分～16 時 00 分
（形式）対面形式およびＷｅｂ会議形式
（参加者）別紙のとおり

２．プレゼンテーション

ＰａｙＰａｙ株式会社よりプレゼンテーションが行われた。概要は以下のとおり。

コード決済事業における不正検知の現状（ＰａｙＰａｙ株式会社）
―― プレゼンテーション資料は別添１を参照。

ＰａｙＰａｙのサービス概要を紹介した上で、コード決済事業において発生しうる犯罪手口を挙げる。その後、犯罪や不正利用を防止するための不正検知に関連する参考情報として、行政からの要請、代表的な不正検知の対策、不正検知の実施方式のあり方等を紹介し、ディスカッションへと繋げたい。

当社は、コンビニ等の店舗での対面決済、ＥＣサイト等でのオンライン決済、ＰａｙＰａｙユーザー同士の個人間送金、公共料金や税金の支払い等で利用可能な決済サービスを提供している。本人確認済みユーザーがチャージできる残高であるＰａｙＰａｙマネー（資金移動業として発行）や、必ずしも本人確認をせずともチャージできる残高であるＰａｙＰａｙマネーライト（前払式支払手段として発行）といった残高の種類に応じて、個人間送金額の上限や利用可能な決済サービスに差がある。サービス内の残高、チャージ額、決済額、個人間送金額等に設定された上限は、不正利用の発生状況やリスクに応じて見直すことも可能となっている。

次に、コード決済事業にて発生しうる犯罪手口の代表例として、①偽造書類等を用いたなりすましによる不正な本人確認の実施、②アカウント乗っ取り等による不正利用、③詐欺行為による資金詐取、④マネー・ローンダリング（以下、マネロン）を挙げる。これらの犯罪手口に対して、ユーザーへの注意喚起や不正検知の体制構築等を行っており、不正利用が発覚した場合には、当該アカウントの停止等を含め、必要な措置を講じている。

続いて、不正検知に関連する参考情報を紹介する。

第一に、令和６年（２０２４年）８月に金融庁および警察庁が「法人口座を含む預貯金口座の不正利用等防止に向けた対策の一層の強化について」[1]を公表し、関係する業界団体へ対応を要請した。これにより、預貯金口座を保有する金融機関に対して、犯罪手口に着目した検知シナリオ・閾値の充実・精緻化や、不正検知及びその後の顧客への確認、出金停止・凍結・解約等の措置の迅速化などが要請された。

第二に、不正検知において必要な対策として代表的なものを５点挙げる。１点目は「データベース（以下、ＤＢ）の整備」。顧客データ、取引データ、ＩＰアドレス等のアクセス環境情報のＤＢを整備・活用することが重要と考える。２点目は「シナリオ・閾値等の設計」。当該ＤＢを用いたリアルタイム／事後での不正検知において、不正・詐欺・マネロン等の犯罪行為を検知するシナリオ・閾値設定が必要である。また、新たな犯罪手口に対しては、迅速に対応できる柔軟な体制が必要である。３点目は「不正検知時／検知後のオペレーション」。不正利用の調査手順、疑わしい取引の届出要否判断基準、取引制限・解除基準の整備、緊急性の高いケースに対して 24 時間／365 日対応できる体制構築等が必要である。４点目は「結果分析」。不正検知の有効性の検証、顧客および捜査機関から寄せられる犯罪手口の分析、当該分析を元にした対策の改善等が必要である。５点目は「顧客等への対応」。顧客からの問い合わせ、被害発生時の補償対応、捜査機関からの照会対応等が必要と考える。これらの対策を講じた上で、トップマネジメントによるコミットメント、部門の壁を越えた協力体制、不正対策の現場でのＰＤＣＡによる改善活動等を中心に組織体制を整えることも重要である。

第三に、金融機関同士の連携を含めた不正検知の実施方法のパターンを４つ検討し、各パターンの評価を行ったことについて紹介する。「パターンＡ　各金融機関」は、従来通り金融機関が各自で不正検知を実施するもの。そのため、金融機関を跨いだ情報共有は行われない。「パターンＢ　システム共同化」は、不正検知の機能を持つ共同機関を設立し、それぞれの金融機関から顧客データや取引データを共同機関へ共有し、共同機関の不正検知の機能の判断に基づき、共有元の金融機関に対して必要に応じてアラートを出し、最終的に各金融機関において不正利用か否かを判断するもの。共同機関では各金融機関から共有されたデータを分別管理し、金融機関を跨いだ共有はされないものとした。「パターンＣ　システム＆データ共同化」は、パターンＢにおいてデータを分別管理せずに統合した場合のもの。「パターンＤ　不正情報共同化」は、パターンＡと同様に金融機関が各自で不正検知を実施するが、不正利用者に関する情報等（以下、不正情報）について、不正検知に役立つ情報に限定して、共同機関を介して共有ができるもの。

以上のパターン分けにおいて、①ＤＢ整備、②シナリオ設定（不正検知の

[1] https://www.fsa.go.jp/news/r6/ginkou/20240823/20240823.html　参照。

機能）、③調査・判断等、④分析結果、⑤顧客等対応の５つの観点から各参加者より意見やコメントがあれば伺いたい。

３．質疑応答とグループディスカッション

参加者による質疑応答とグループディスカッションが行われ、その後、各グループ代表者からの発表が行われた。モデレータは、株式会社イオン銀行が担当した。概要は以下のとおり。

【不正発生の傾向】

（日本銀行）コード決済事業等における残高や決済の上限額と、不正発生率に相関関係はあるのだろうか。例えば、上限額が一定の閾値を超えると不正が増加する等のご知見があれば伺いたい。

（参加者）不正が増加する閾値は状況により異なるため一概に申し上げることは難しいが、不正が起こりうる仕組みが存在し、且つ取扱える上限額が高いと、悪意者にとって不正を働くインセンティブが生じるため、上限額が高ければ高いほど不正発生リスクも高まると考えられる。

（参加者）コード決済事業においては、本人確認済みのユーザーか否かによっての不正率に差があるか。

（参加者）大きな偏りがあるとまでは言えないが、本人確認未済のユーザーの方が不正率は高い傾向にあると分析している。

【加盟店の審査・管理】

（日本銀行）加盟店が不正に加担した架空決済によるポイント詐取の犯罪手口もあり、加盟店の審査・管理も重要と理解した。このように加盟店が不正に加担した犯罪の被害は、どの程度の規模で生じているか。また、ＣＢＤＣの普及を考えた場合、利用できる場所を増やすためには小規模な事業者を含めて加盟店を開拓することが必要となる可能性があるが、特に数の多い小規模な加盟店に関しての審査・管理における留意点があれば伺いたい。

（参加者）まず、被害状況について、加盟店が不正に加担した犯罪の被害規模については差し控えるが、アカウントの乗っ取りやＳＮＳ型投資詐欺・ロマンス詐欺等による被害の方が規模は大きいと認識している。架空決済によるポイント詐取については、通常時は不正を行った場合の経済的なメリットが少ないものの、ポイント増加キャンペーン等を実施した際には不正を行った場合の経済的なメリットが大きくなるため、不正行為が増加する傾向がある。次に、加盟店の審査・管理についてだが、これは、非常に難

しい課題と認識している。特に小規模な事業者の場合は、審査にかかる時間とコスト等に対して費用対効果のバランスを取ることは難しい。そうした中でも、適正な審査・管理を効率的に実施し、不正が起こるリスクを低減していくために、審査・管理のプロセスを改善していくことが重要だろう。

【各グループ代表者からの発表】

（参加者）金融犯罪対策と取引の安全性の観点から取引内容に懸念があると判断した場合は、ＣＢＤＣの送金、店頭やＥＣ等での決済を保留し、懸念がないことを確認してから実行する仕組みも必要と考える。

（参加者）どのような犯罪手口を対象に不正検知システムを構築するかは議論の必要がある。また、個人情報保護の観点からＣＢＤＣではユーザーの個人情報を匿名もしくは仮名で管理するとした場合においても、不正検知の機能が有効になるような考慮は必要だろう。

（参加者）不正検知のために個人情報も含めて関係者間で共有すると想定した場合、ユーザーから事前に個人情報の共有に関して許諾を得る必要があるだろう。ただし、許諾を得たからといって、全関係者間で全ての情報を共有しても良いわけではなく、どのようなエンティティであれば情報を共有することができ、どのような情報がマスキングされるべきか等についての議論が必要だろう。また、不正情報の共有は、早期に対策を行う観点から、可能な限りリアルタイムな情報共有が求められるだろう。そうした観点では、「パターンＤ　不正情報共同化」のように各金融機関が不正者と判断した情報について共同機関を介して共有する場合はどうしてもタイムラグが生じる。他方で、「パターンＣ　システム＆データ共同化」のように各金融機関から共有されたデータを共同機関のＤＢに統合している場合はリアルタイムに金融機関を跨いだ情報共有がされているため、情報共有の早さの点では優れている。「パターンＢ　システム共同化」については、システム自体は共同化されるため一定のコスト削減効果はあるものの、共同機関のＤＢでは各金融機関から共有されたデータを分別管理しており、そうした中で金融機関を跨いだ情報共有をどのように行うかについて各金融機関と検討・調整することは簡単ではないだろう。以上の点を踏まえると、各金融機関に求められる個別対応は抑制しつつ、不正に対して素早く的確な対応の実現が見込める「パターンＣ　システム＆データ共同化」が、不正検知の観点のみからは比較的優れているのではないだろうか。

（参加者）ＣＢＤＣが広く国民に使われることを踏まえると、各金融機関が不正検知を個別に行うのではなく、「パターンＢ　システム共同化」や「パターンＣ　システム＆データ共同化」のように共同で行うことのメリットは大きいだろう。ただし、共同機関で不正を検知しユーザーのアカウント

を停止する等の対応を考慮した場合、当該ユーザーへの説明責任はアカウントを管理している各金融機関に帰属すると考えられるため、アカウント停止等の判断は各金融機関が負うことになるだろう。また、共同機関において不正検知後に各金融機関に連携した場合、取引保留、アカウント停止等の対応をリアルタイムで行うことは難しい可能性もあるため、対応のリアルタイム性を求めるのであれば、「パターンＡ　各金融機関」のように各金融機関が一気通貫で不正検知からユーザーへの対応を行う必要性も考えられるだろう。「パターンＤ　不正情報の共同化」は、不正検知の観点からは理想的な取り組みの一つと考えるが、個人情報保護の観点で議論が必要であるのに加え、不正と判断されてアカウント停止等になったユーザーが再びＣＢＤＣと関わりを持つことができるのか等について金融包摂やユーザビリティの観点から考えるべき論点があるだろう。

（参加者）不正検知システムを共同化し、共同機関が共同システムを運営した場合において、運営上の課題は複数考えられる。課題の１点目は、大手の金融機関へ運営上の負担が集中することにより不公平が生じうる点。具体的には、取引量が多い大手の金融機関が、不正利用に関する情報やその対策、システム開発に関するノウハウの一方的な提供側になる可能性に加え、仮にユーザー数に応じてシステム開発コストを負担することになれば、コスト負担においても大きな割合を大手の金融機関が負う可能性がある。２点目は、大手の金融機関と同じ水準の不正検知の機能は、小規模な金融機関にとっては、過剰な機能となりうる点。不正検知のために共同システムが要求する情報（例えば、ＩＰアドレス等の情報）を各金融機関において予め取得する必要があるが、仮にそうした機能が金融機関のシステム内になければ、当該機能を開発する必要が生じる。こうした場合、主に小規模な金融機関では、事業規模に対してシステム開発コストが見合わないことも考えられる。結果として、適切な情報を共同機関に提供できず、適切な不正検知ができないことに繋がる。また、仮にシステム開発が可能としても、小規模な金融機関の事業においては、必ずしも大手の金融機関が求める不正検知の水準に追従する必要性があるとは限らないため、共同システムを利用する金融機関間での意見調整は簡単ではないだろう。３点目は、ＡＩにおいても似たような課題があるが、各金融機関において不正な取引と判断した根拠について説明責任が果たせるのかという点。共同システムが不正の可能性が高いと判断したことのみを根拠に不正利用口座として凍結等を行った場合、訴訟等において各金融機関が不正と判断したことに対する説明責任を果たしたと評価されるかは判然としない。各金融機関は、自らの事業におけるリスクや個別の取引状況等を考慮した上で、不正と判断した根拠の説明責任を果たせるような何らかの仕組みを考慮する必要があると思われる。理想的には不正検知システムを全て共同化して、どの金融機関においても共通の対策がなされているために、犯罪者が狙う金融機関を変更しても同じ犯罪はできないという状況をめざすべきであるものの、これまで挙げた課題を踏まえると、実現するのは簡単ではないだ

ろう。

４．次回予定

次回の会合は 11 月 14 日（木）に開催予定。

以　上

別紙

ＣＢＤＣフォーラム ＷＧ３
「ＫＹＣとユーザー認証・認可」
第 10 回会合参加者

（参加者）※五十音・アルファベット順
株式会社イオン銀行
セコム株式会社
ソニー株式会社
大日本印刷株式会社
株式会社千葉銀行
日本電気株式会社
日本マイクロソフト株式会社
日立チャネルソリューションズ株式会社
フェリカネットワークス株式会社
株式会社ふくおかフィナンシャルグループ
株式会社マネーフォワード
株式会社みずほ銀行
株式会社三井住友銀行
株式会社三菱ＵＦＪ銀行
株式会社ゆうちょ銀行
株式会社りそなホールディングス
ＮＲＩセキュアテクノロジーズ株式会社
株式会社ＮＴＴドコモ
ＰａｙＰａｙ株式会社

（事務局）
日本銀行

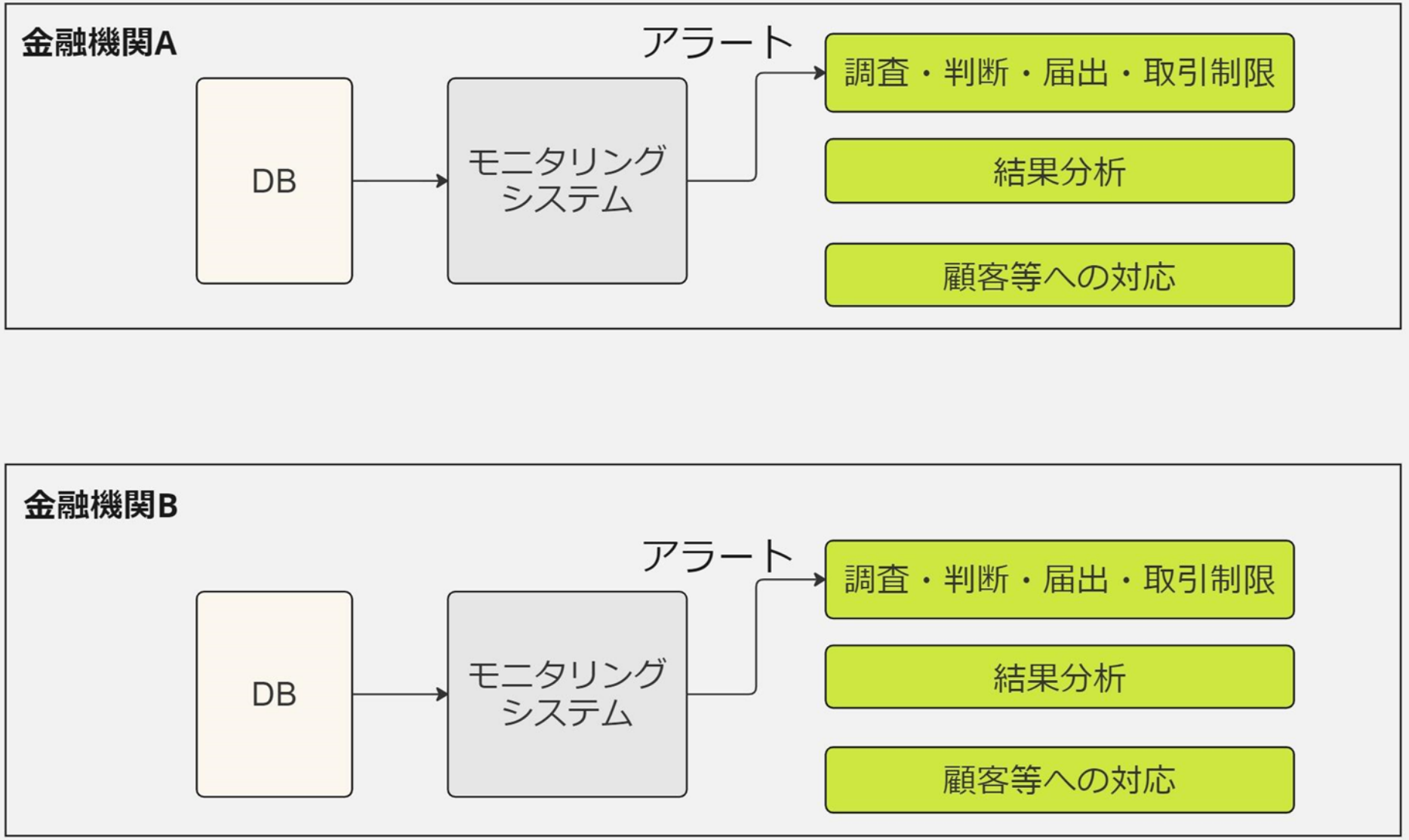
不正検知において必要な対策

項目	必要な要素
①DBの整備	● 以下を含むDBの整備、活用 　○ 顧客データ（KYC情報） 　○ 取引データ（日時、金額） 　○ IPアドレス、ブラウザ言語、タイムゾーン、デバイス情報等アクセス環境情報
②シナリオ・閾値等の設計	● リアルタイム検知、事後検知の機能 ● リスク（不正・詐欺・マネロン等）に対応したシナリオ・閾値設定 　○ 新たな手口に対する迅速な変更対応 　○ 定期的な見直し
③検知時/検知後のオペレーション（調査・判断・届出・取引制限等）	● 調査手順、疑わしい取引の届出要否判断基準、取引制限・解除基準等の整備 ● 緊急性の高いケースに対して、24時間/365日対応できる体制
④結果分析	● 有効性の検証（シナリオ毎の疑わしい取引の届出率分析等） ● 顧客申告/捜査機関からの寄せられる不正手口分析 ● 分析結果を元にした対策の改善
⑤顧客等への対応	● 顧客からの問い合わせ、被害発生時の補償対応等 ● 捜査機関等からの照会対応

誰が不正検知を実施するか　各金融機関or共同化

パターンA

各金融機関が個別に対応

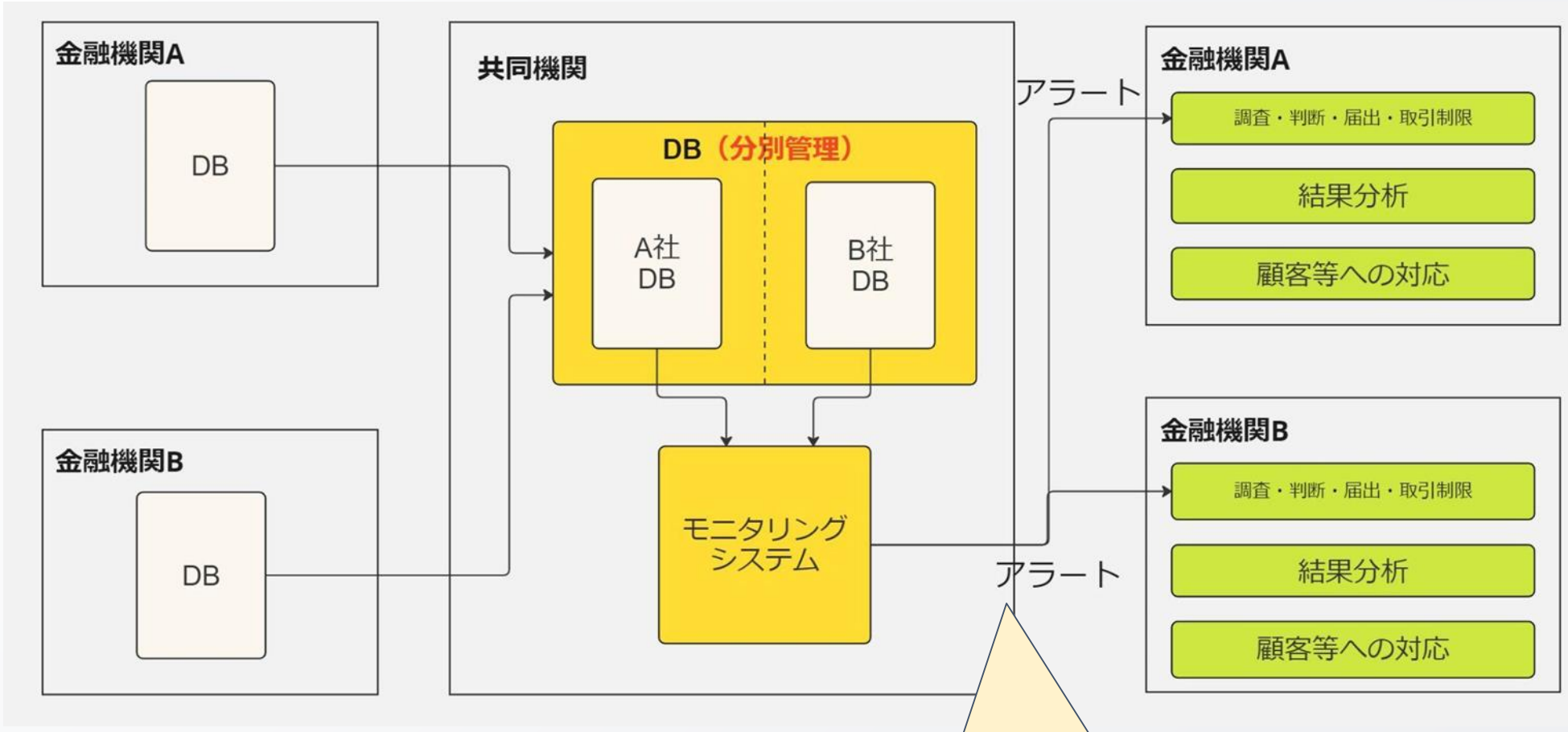


誰が不正検知を実施するか　各金融機関or共同化

パターンB

システム共同化

・検知機能のみ共同可
・データは分別管理



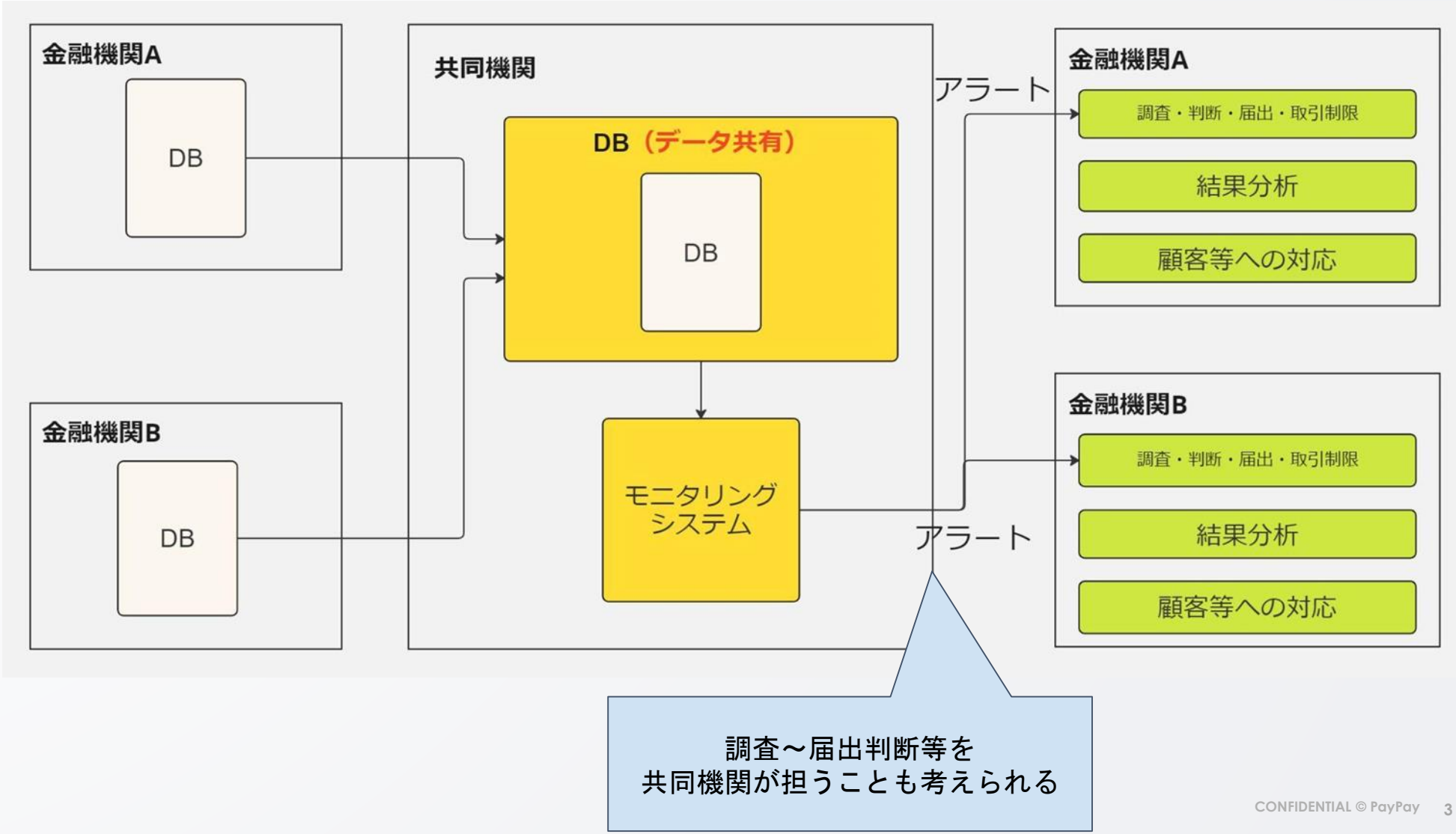
調査～届出判断等を
共同機関が担うことも考えられる

誰が不正検知を実施するか　各金融機関or共同化

パターンC

システム&データ共同化

検知機能およびデータを共同化



誰が不正検知を実施するか　各金融機関or共同化

パターンD

不正情報共同化

システムの共同化等は行わず、不正者に関する情報のみを共有