「取引モニタリングの検知能力強化に向けた横断的レビューにかかる調査業務」報告書

金融庁
Financial Services Agency

目次

1. 調査の背景、目的、概要

金融業界全体での取引モニタリングの検知能力の底上げを図ることを目的とし、共通テストシナリオを用いて取引モニタリングの検知能力を横断的に調査

調査の背景／目的／概要

■ 調査の背景

- マネー・ローンダリングや特殊詐欺等の手口は巧妙化・多様化しており、特殊詐欺等の金融犯罪被害は極めて憂慮すべき状況
- **預金取扱金融機関における取引モニタリングの検知能力強化が急務**

■ 調査の目的

- テストシナリオ毎のアラート検出指標の傾向等から取引モニタリングシステムの**検知能力強化の方向性を見出し、金融業界全体での検知能力の底上げを図ること**

■ 調査の概要

- 8つの預金取扱金融機関※1を対象とし、**マネー・ローンダリングや特殊詐欺等の金融犯罪に係る取引に対する検知能力を共通テストシナリオにて横断的に調査**
- 取引モニタリングシステムによるシステム検知及び机上検証を通してアラート検出指標を調査

※1全国展開金融機関6先、地域金融機関2先

調査のスコープ

■ 調査のスコープ

- 金融庁 疑わしい取引の参考事例　預金取扱金融機関（2025年8月改正前）、警察庁の各種公表資料等を踏まえて、マネー・ローンダリングや特殊詐欺等の金融犯罪に関する共通テストシナリオを101件策定
- 調査対象領域は、取引モニタリングシステムで通常カバーしている業務およびチャネルとした
- テストシナリオのうち、通常取引モニタリングシステムに投入されない取引や店頭や窓口での確認が必要であり、取引行動としてデータ化が難しい取引は調査対象外とした
- **特殊詐欺等の金融犯罪については、検知のリアルタイム性（リアルタイム、準リアルタイム、バッチ検知）※2も調査**

※2リアルタイム性の定義
- リアルタイム検知：取引発生時に即座にアラートが発生
- 準リアルタイム検知：一定時間に発生した取引に対し、1日以内にアラートが発生
- バッチ検知：前日分の取引に対してアラートが発生

2. アラート検出結果及び傾向

全国展開金融機関のアラート検出指標が相対的に高い傾向を示しており、地域金融機関は相対的に低いことが確認された

調査の要旨

■ **全体傾向**

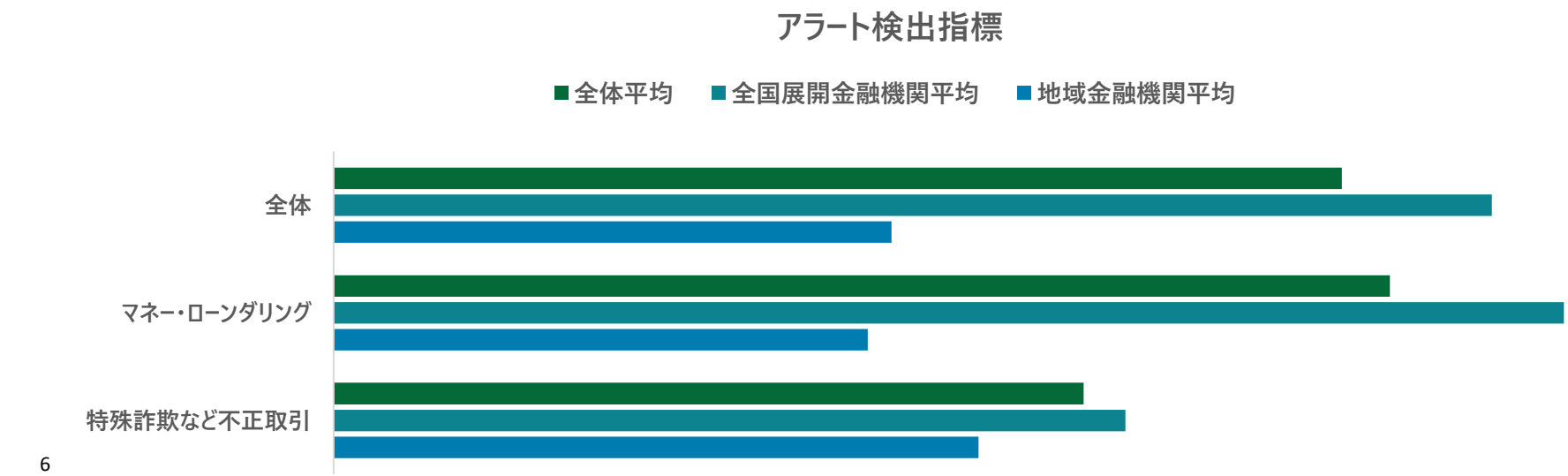
- 全国展開金融機関ほど検出指標が高く、**地域金融機関は相対的に低い傾向**であった

■ **マネー・ローンダリングシナリオ**

- 取引行動と取引環境データ（地理情報、アクセス情報、デバイス情報等）や顧客プロファイリングを組み合わせた**多層的なルール検知の導入・運用は限定的**であった
- **暗号資産交換業者/オンラインカジノに関するルール検知が限定的**である金融機関も確認された

■ **特殊詐欺等の不正取引シナリオ**

- 特殊詐欺等の金融犯罪のモニタリングについては一定の対策が進んでいるものの、**一部の金融機関においては、検知ルールが網羅的でない**ことが確認された
- **全国展開金融機関を中心にリアルタイム検知システム及び準リアルタイムのシステム導入や計画が進行**している一方で、**一部の全国展開金融機関及び地域金融機関においては、未導入**であることが確認された



マネー・ローンダリングシナリオにおいては、アクセス・取引行動（個人）及び顧客プロファイリング・取引行動（個人・法人）の検知が限定的であり、特殊詐欺等の金融犯罪シナリオのアラート検出指標はマネー・ローンダリングシナリオに比べ相対的に低い傾向であることが見受けられた

アラート検出指標の結果：シナリオ分類別の検知傾向

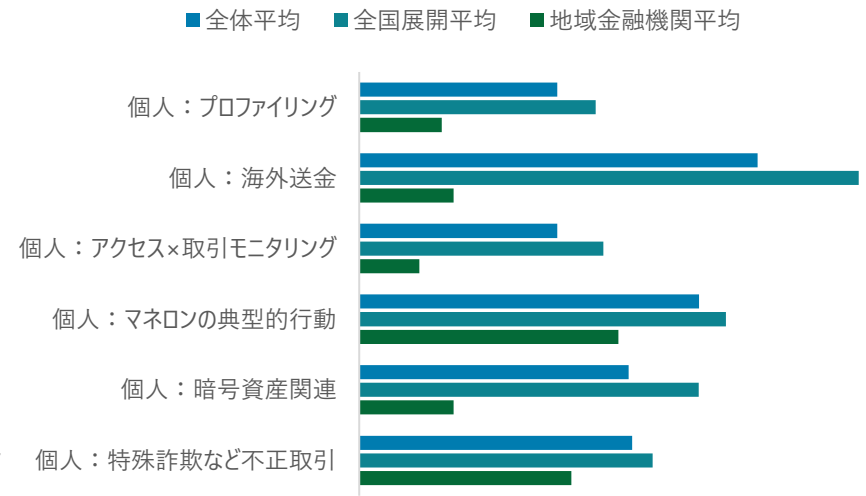
■ 個人シナリオ

- マネー・ローンダリングシナリオについては、**取引行動と取引環境データの組み合わせ、取引行動と顧客プロファイリングの組み合わせに係るアラート検出指標が低い傾向**にあることが確認された。また、シナリオ分類別の比較についても、全国展開金融機関と比較して**地域金融機関の指標は低い傾向**にあることが見受けられた
- 特殊詐欺等の金融犯罪シナリオについても、**地域金融機関はアラート検出指標が相対的に低い傾向**にあることが見受けられた

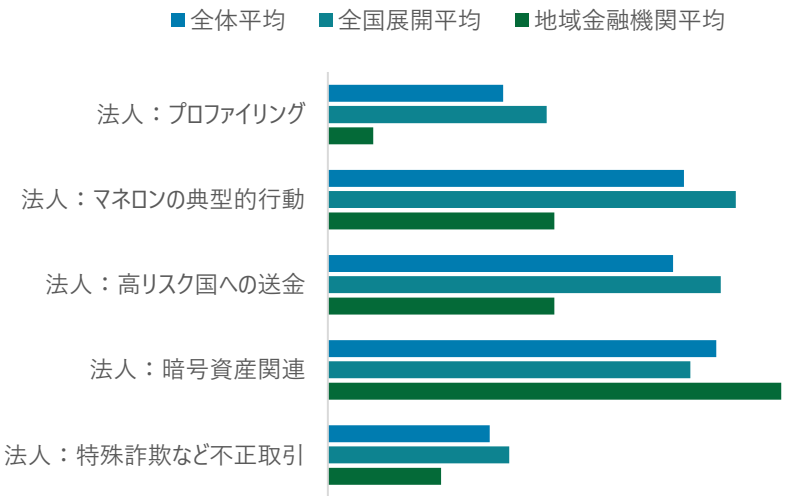
■ 法人シナリオ

- マネー・ローンダリングシナリオについては、プロファイリングに係るシナリオのアラート検出指標が低い傾向であり、ヒストリカルプロファイリング（取引履歴との乖離）への対応は確認されたが、**顧客プロファイリングに基づくルール検知は限定的**と見受けられた
- 特殊詐欺等の金融犯罪シナリオについては、**マネー・ローンダリングシナリオと比較してアラート検出指標が低い傾向**であると見受けられた

個人シナリオ：アラート検出指標



法人シナリオ：アラート検出指標



リアルタイム検知システムの導入及びAI活用については、全国展開金融機関を中心に実施していることが確認された

テスト参加先におけるリアルタイム検知システム及びAI活用の事例

- 特殊詐欺等の金融犯罪対策に資するリアルタイム検知システムの導入状況については、**全国展開する金融機関を中心に、リアルタイムまたは準リアルタイムの検知システムが導入済み、もしくは導入予定**であることが確認された
- 一方、地域金融機関を中心とする一部のテスト参加先においては、リアルタイムまたは準リアルタイムの検知システムは未導入であることが確認された。このような金融機関においては、**即時性の高い取引モニタリング態勢を構築することが期待される**
- また、一部のテスト参加先では、マネー・ローンダリング、特殊詐欺等の金融犯罪対策として、**AIを活用した取組**も確認された

リアルタイム検知システムの事例

■ **インターネットバンキングにおけるリアルタイム検知システムの導入**

- アクセス、デバイス情報と取引行動データを組み合わせて、リスク判定して検知するシステムを導入している

■ **取引種類を限定したリアルタイム検知システムの導入**

- 取引種類を限定して、不正リスクの高い取引を検知するリアルタイム検知システムを導入済、あるいは、導入予定である

■ **取引種類を限定した準リアルタイム検知システムの導入**

- 取引種類を限定して、日次で複数回バッチ処理を実施することにより、不正リスクの高い取引を検知する準リアルタイム検知システムを導入済、あるいは、導入予定である

各金融機関は自らの業務・サービス内容や金融犯罪の発生状況等に応じて、計画的かつ実効的に即時性の高い取引モニタリング態勢を構築することが期待される

AI活用の事例

■ **取引モニタリングシステムにおけるAI実装**

- 取引モニタリングシステムにAIを実装し、取引の疑わしさを算出して一定スコア以上となった場合にアラート発生させる仕組みを導入している

■ **不正口座と類似した口座を抽出するAI**

- 不正口座の取引行動や属性などを学習データとして、不正リスクが高い口座を抽出するAIを構築し、取引モニタリング等に活用している

■ **分析ツールやAIを活用した多層検知**

- 分析ツールやBIツールによる分析、AIを活用した検知ルールおよびスコアリングモデルを構築し、潜在的な不正口座・取引の抽出と事後検知の強化に取り組んでおり、取引モニタリングシステム単体に依存しない多層的な検知を実施している

巧妙化・多様化する特殊詐欺等の手口を踏まえて、人間によるルール設定だけではなく、AIを活用した金融犯罪パターンの抽出及び検知業務の効率化を継続的に検討していくことが期待される

3. 発見事項及び高度化の方向性

テスト参加先にて確認された発見事項は以下のとおりであり、各金融機関においても今後の高度化に向けた参考材料とすることが期待される

発見事項及び高度化に向けた方向性：マネー・ローンダリングシナリオ（1/2）

テスト参加先分類	発見事項	想定される高度化に向けた方向性
テスト参加先共通	■**取引データと顧客プロファイリングの組み合わせ** ➢ 顧客プロファイル（属性と実態の乖離）、ピアプロファイリング（同集団からの乖離）に関するシナリオ検知が限定的	➢ 継続的な顧客管理による顧客情報の最新化の取り組みを踏まえて、顧客プロファイル・ピアプロファイリングの乖離を検知するルールを整備することが考えられる
テスト参加先共通	■**取引データと取引環境データの組み合わせ** ➢ 住所変更などのイベント、アクセス元/デバイス、地理情報、時間帯/ATMと取引行動を組み合わせるルールが限定的	➢ イベント×地理×チャネル、デバイス×時間帯×取引の複合的な要素にて疑わしさを判断するルールを整備することが考えられる

テスト参加先にて確認された発見事項は以下のとおりであり、各金融機関においても今後の高度化に向けた参考材料とすることが期待される

発見事項及び高度化に向けた方向性：マネー・ローンダリングシナリオ（2/2）

テスト参加先分類	発見事項	想定される高度化に向けた方向性
一部のテスト参加先	■**新興リスクへの対応** ➢ 暗号資産交換業者/オンラインカジノ関連のシナリオに関するルール検知が限定的	➢ 暗号資産交換業者のリスト運用、高額/多頻度検知、オンラインカジノが疑われる決済代行疑い先の特徴抽出とルール整備を実施することが考えられる
地域金融機関	■**個人の海外入出金** ➢ 個人の海外送金、入金関連シナリオに関するルール検知が限定的	➢ 個人の海外入出金関連シナリオについて、検知ルールの新規作成、拡充、及び、敷居値の見直しをすることも一案として考えられる

テスト参加先にて確認された発見事項は以下のとおりであり、各金融機関においても今後の高度化に向けた参考材料とすることが期待される

発見事項及び高度化に向けた方向性：特殊詐欺等の金融犯罪検知シナリオ

テスト参加先分類	発見事項	想定される高度化に向けた方向性
テスト参加先共通	■**特殊詐欺等の被害者行動に関する検知** ➢ 詐欺被害者の行動に関する検知が限定的	➢ 特殊詐欺などの被害者にみられる取引行動について、犯罪類型別にルール整備することが考えられる
地域金融機関	■**特殊詐欺等の金融犯罪に係る検知ルールが限定的** ➢ 全国展開金融機関に比べて、地域金融機関における特殊詐欺等の金融犯罪に係る検知ルールが限定的	➢ 犯罪者、被害者の両視点に立ち、犯罪類型別にみられる取引行動へ対応した検知ルールを整備、運用することが考えられる
一部のテスト参加先（特に地域金融機関が顕著）	■**リアルタイム検知システムの未導入** ➢ リアルタイム検知システムが未実装であるテスト参加先が確認された	➢ 即時性の高い取引モニタリング態勢の構築を計画的かつ実効的に推進することが考えられる

4. 更なる取引モニタリングの高度化に向けた対策例

多層的な検知ルールの検討、機動的なシナリオ管理、即時性の高い取引モニタリング態勢の構築、AIの活用、そして部門横断の一体運営が今後の高度化において重要

更なる高度化に向けた取組例

■ 取引行動と取引環境データや顧客プロファイリング等を組み合わせた多層的な検知ルールの検討

- 非対面取引の拡大により金額・件数のみでは捉えにくい兆候が増えているため、取引データに取引環境データ（IPアドレス、端末情報、ブラウザ言語、タイムゾーン等）や最新の顧客情報等を組み合わせ、総合的にリスク判定する多面的検知へ高度化することも一案として考えられる。また、継続的な顧客管理に基づき、顧客情報と乖離した行動を捉えるプロファイリングのシナリオを強化することも一案として考えられる。

- アクセス関連モニタリングを担うサイバーセキュリティ対策部門と、マネー・ローンダリング対策部門、金融犯罪対策部門の密接な情報連携を強化し、三部門が一体となった取引モニタリング体制を構築していくことも一案として考えられる。

■ 特殊詐欺等の金融犯罪に係る検知ルールの機動的な管理

- 特殊詐欺等の金融犯罪対策では、新手口や発生状況に応じて敷居値や対象行動・対象顧客を機動的に更新するシナリオ管理が求められることから、検知条件の更新頻度を高めることも一案として考えられる。

■ 即時性の高い取引モニタリング態勢の構築（事後検知から未然防止へ）

- 特殊詐欺等の金融犯罪については、資金流出後の回復が困難であることから、事後届出・分析に依存せず、一般的取引との比較、顧客の過去傾向、本人確認結果との整合性等を踏まえ、一定の高リスク兆候にはアラートに加えて追加認証や取引保留など、未然防止措置を可能とする運営・システム設計と規則整備をしていくことも一案として考えられる。

■ AIや統計分析の活用

- AI・統計分析の活用は有用であるが、ルールベース検知との両輪で、アラートの優先順位付けや検知ルール構築から段階的に導入し、説明可能性の確保、定期的なモデル検証、AIリスクへの対応策を検討することも一案として考えられる。

Appendix：調査で使用したテストシナリオ

金融庁が公表している疑わしい取引の参考事例や警察庁等の不正事例を元に、マネー・ローンダリング、特殊詐欺等の金融犯罪に関するテストシナリオを策定

調査で使用したテストシナリオ分類

対象	シナリオ分類	シナリオ概要
個人	プロファイリング	個人における顧客情報（職業・年齢・収入/資産・居住地等）と取引実態の整合性、及び過去傾向からの乖離関連のシナリオ
	マネロンの典型的行動	個人口座を用いた典型的なマネロンパターン（多額の現金出金、多頻度入出金、反復取引による複雑化）のシナリオ
	アクセス×取引モニタリング	インターネット/モバイル等のアクセス情報（ログイン・端末・IP・位置等）と取引行動を組み合わせたシナリオ
	海外送金	個人口座における不自然な海外送金（高額、多頻度、高リスク国等）や、国内取引と組み合わせたシナリオ
	暗号資産関連	暗号資産交換業者への多額、多頻度な入出金に関するシナリオ
	不正取引、特殊詐欺など	特殊詐欺・フィッシング・口座乗っ取り等に伴う被害者側の送金行動、及び受け口座などに関するシナリオ
法人	プロファイリング	法人における顧客情報（業種、規模、売上）と取引実態の整合性、及び過去傾向からの逸脱などのシナリオ
	マネロンの典型的行動	法人口座を用いた典型的なマネロンパターンに関するシナリオ（多額多頻度入出金の海外送金など）
	高リスク国への送金	法人口座における高リスク国への送金などに関するシナリオ
	暗号資産関連	法人による暗号資産関連先への送金・入出金に関するシナリオ（実体不明な資金流、反復取引による複雑化の可能性）
	不正取引、特殊詐欺など	法人口座の売買や乗っ取り等の不正送金などに関するシナリオ