KPMG

KPMG グローバル金融犯罪実態調査

特殊詐欺の戦略的な対策

[日本語抄訳版]

2025年8月

はじめに

特殊詐欺*1は、国境を越えて行われる行為であり、あらゆる国や地域に被害が及びます。世界経済が各国の経済を結び、国境を越えた情報・資金のやり取りが容易にできるようになったことで、1件の特殊詐欺の影響が複数の国の複数の金融機関に及ぶ可能性もあります。世界の詐欺被害額は毎年数十億ドルに上ると推定されています。

特殊詐欺犯は、人を騙して犯罪者・犯罪組織の口座に資金を振り込ませます。銀行、業者、政府機関などの信頼できる組織になりすまし、資金を振り込むように仕向けるのが特殊詐欺の典型的な手口です。被害者は正規の取引をしていると信じ込まされますが、実際の振込先は犯罪者・犯罪組織の口座です。

複雑なグローバル社会構造において、銀行などの金融機関は、顧客の資金の「門番」と見なされることが多くあります。しかし特殊詐欺に関しては、政府、規制当局、通信会社、テクノロジー・SNS関連会社、暗号資産交換業者、法執行機関などの組織のほか、顧客自身も門番の役割を果たさなくてはなりません。

KPMGのグローバル金融犯罪実態調査では、昨今の詐欺の実態や顧客保護につながるベストプラクティスを把握するため、世界5大陸16ヵ国において48の銀行等を調査対象とし、不正・詐欺対策の専門家へのインタビューを通じて情報を収集しました。幅広い見解が得られるよう、グローバル展開する大手銀行や、デジタル・ネオバンク、相互組合・住宅金融組合などに回答を求めました。

本調査で得られた知見が、分野を問わずあらゆる組織で詐欺対策戦略の見直しや強化に向けた取組みを促し、さらには世界的な不正防止の取組みにどう貢献できるかを模索する足がかりとなれば幸いです。

Martin Dougall

KPMGオーストラリア
グローバル・フォレンジックネットワーク＆ソリューション部門統括
フォレンジック担当パートナー

KPMGの特殊詐欺に関するグローバル金融詐欺調査の対象地域

EMEA	31社
ドイツ	1
ギリシャ	3
イタリア	1
オランダ	3
ノルウェー	3
ポルトガル	2
スペイン	2
南アフリカ	3
スウェーデン	3
スイス	1
トルコ	2
英国	7

APAC	9社
オーストラリア	5
シンガポール	4

米州	8社
カナダ	5
米国	3

5大陸

16ヵ国

48社

*1 日本の警察統計等においては「特殊詐欺」にはSNS型投資詐欺やロマンス詐欺といった類型は含まれませんが、本サーベイにおいてはこれらを含めた概念として「金融犯罪」と総称して使用しています。

目次

調査結果

重要トピック

詐欺の傾向

特殊詐欺の世界共通の傾向として、被害件数ではネットショッピング詐欺が、被害額では投資詐欺がトップです。

戦略、政策、ガバナンス

専門チーム・委員会が、組織の詐欺対策を定期的に（場合によっては毎日）見直しています。見直しにあたっては、世界中から集めた知見や、実態・傾向分析の結果、顧客の声も取り入れます。

詐欺対策

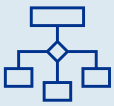
取引の一時停止・謝絶が最も効果的な防止策との回答でした。支払先の確認はあまり効果的ではないものの、基本的な詐欺対策として最低限実施すべきとの見方があります。

詐欺の検知

法執行機関、同業者団体、業界団体などとの情報共有が、最も効果的な詐欺検知方法との回答でした。

検知後の対応

調査対象のうち45％が、繰り返し詐欺被害を訴える顧客とは取引を中止すると回答しましたが、これは上級委員会の判断のもと実施される最終手段であり、たいていは顧客が不正の共犯者である場合を対象とします。



テクノロジー

回答者のおよそ5分の2の銀行では、多数のデータソースを単一のシステムに統合するオーケストレーション・レイヤを備える技術スタックを保有しておらず、これを詐欺対策の優先課題と考えています。

顧客からのクレーム

回答者の60％が、詐欺に関するクレームが増加したと回答しています。最も多いクレームの内容は、被害相当額の返金の可否・金額への不満、取引上の追加の手間や制限に対する苛立ち、対応のスピード、顧客保護のための対策不足でした。

顧客教育

教育を複数のプラットフォーム上で継続的に実施する必要性を、多くの回答者が認めています。詐欺に関する啓発運動の効果は、長く続かないとの意見もありました。

調査結果

1. 詐欺の傾向

本調査により、世界の銀行が昨今直面する詐欺の全体像が明らかになりました。新たな手口の詐欺が必ずしも多数を占めるわけではなく、世界各地の銀行で見られた特殊詐欺には共通のパターンや傾向が見られることがわかっています。

ネットショッピング詐欺

ネットショッピングサイトを悪用して顧客を騙し、架空の物品購入取引に対し支払いを行わせる詐欺です。安価で販売量の多い商品を対象とするケースが一般的ですが、一部の銀行からは自動車に関連した高額の事案も報告されています。また、大規模なエンターテインメントイベントの開催時期に急増する傾向があります。チケットの需要が高まるタイミングで、偽のチケットをネット販売する詐欺が発生するのです。

投資詐欺

投資詐欺には、投資対象資産が実在しない虚偽の投資を持ちかける詐欺と、正規の投資機会ではあるものの投資資金を投資に回さず詐欺犯が持ち逃げする詐欺とがあります。高い投資収益が約束されることが多く、全財産を費やすケースも見られるなど多額の資金を伴うことが多いため、被害額も膨らむ傾向にあります。以下は、昨今見られる投資詐欺の例です。

- **社債取引詐欺：**著名な企業の社債の取引や長期の預託金に見せかけます。
- **ボイラールーム詐欺：**高圧的な販売手法を用いて、顧客に有価証券を水増し価格で購入させます。
- **暗号資産詐欺：**詐欺犯が偽の暗号資産や、取引所、ウェブサイト、あるいはアプリを作成して顧客を偽の投資に勧誘し、資金を騙し取ります。

巧妙なりすまし詐欺

なりすまし詐欺の手口は進化し続けており、ますます巧妙化しています。詐欺犯はSNS、電子メール、電話を通じたやりとりで被害者を騙し、機密情報の提供や送金を促します。正規の文書に名前やメールアドレスを微調整するなどの細工を施す手口が多く見られます。

- **CEO詐欺：**CEOなどの上級幹部になりすまして従業員、顧客、あるいはベンダーを騙し、送金や機密情報の提供を促します。通常電子メールを通じて行われ、しばしば切迫感が演出されます。最近の例では、拡張AIを利用してSNS上の職務経歴情報の更新を追跡し、若手スタッフや新入社員を特定して標的とする詐欺行為が見られます。CEO詐欺は他の詐欺に比べて発生頻度は低いものの、多くの事案が多大な金銭被害や風評被害につながっています。
- **銀行員を騙る詐欺：**銀行員を装って、

自身が管理する口座に送金するよう仕向ける手口です。「ヘルプデスク詐欺」とも呼ばれるこの詐欺の手口は巧妙さを増しており、他の部門に電話を転送するふりをする、または偽の問合せ番号を提供するなどして被害者を騙すケースが多く見られます。銀行の犯罪対策チームを装った詐欺犯が顧客に指示して行わせた送金取引を、本物の銀行の金融犯罪対策チームが検知し、顧客に通知した事案も複数報告されています。

- **企業を狙ったなりすまし：**企業の人事やIT部門を標的にした詐欺で、被害者にQRコードまたはリンクを送り、それを通じて企業の資金や個人情報へのアクセスを獲得します。
- **当局関係者を騙る詐欺：**政府関係者や警察官などになりすます手口です。北欧では、被害者が当局関係者を装った人物と対面するという事案が度々発生しており、懸念が強まっています。
- **サポート詐欺：**ITまたはPOS関連のテクニカルサポート窓口になりすまし、被害者のパソコンや個人情報にアクセスします。リモートアクセス詐欺とも呼ばれています。
- **会計士を騙るなりすまし詐欺：**会計士を装い、偽の税務申告サービスや金融アドバイスを提供します。
- **〇〇ッシング：**信頼のおける企業や家族へのなりすまし行為で、電子メール（フィッシング）、QRコード（クイッシング）、SMS（スミッシング）、または電話（ビッシング）が使用されます。いずれの〇〇ッシングも、個人情報やワンタイムパスワードの入手、あるいはマルウェアのダウンロード、送金などを行わせることを目的とした詐欺行為です。

ロマンス詐欺

特殊詐欺の一種で、出会い系サイト、アプリ、SNS上で偽のプロフィールを使用して、被害者をオンラインの恋愛関係に誘い込む手口です。

他人の写真を無断で使い、被害者から離れた場所で暮らす魅力的でもっともらしい人物像を創り出している。

チャット、電子メール、電話などで数ヵ月やりとりして被害者の信頼を得ます。

最終的には、個人的な問題や家族の緊急事態をでっち上げるか、被害者に直接会いに行きたいという口実で金銭を要求します。ロマンス詐欺は、金銭被害に加え、深刻な心理的・精神的被害も伴います。

前払金詐欺

実在しないサービスや商品に対して前払金を支払わせる詐欺で、以下の手口が見られます。

- **偽の旅行会社**が、安いプランを宣伝

して前払金を要求した上、パスポート情報などの機密情報を盗みます。

- **宝くじ詐欺**は、当選金の受け取りにかかる手数料という名目で金銭を騙し取る行為です。
- **求人詐欺**は、内定者に対し前払金の支払あるいは機微情報の提供を要求する行為です。

ビジネスメール詐欺

BEC詐欺とも呼ばれ、ソーシャルエンジニアリングやサイバー侵入を通じて正規のビジネスメールアカウントを乗っ取り、不正に送金する行為をいいます。不正送金と悟られないよう、実際の仕入先の請求書を偽装するのが特徴です。本調査では、デジタルテクノロジーには頼らず、被害者を騙して情報を書き換えさせる、または送金先を変更させようとするケースが増加しているとの回答もありました。

複数の手口のハイブリッド詐欺

複数の不正・詐欺手口を組み合わせたもので、以下はその例です。

- **ロマンス・ベイティング：**ロマンス詐欺の被害者は、やりとりが進むにつれて投資に勧誘され、要求される金額は徐々に大きくなります。投資が相当額に達したところで、資金を持ち逃げされます。この行為は、「豚殺し」または「豚の屠殺」とも呼ばれます。
- **資金回収詐欺：**被害者が詐欺に遭ったことに気づき、弁護士事務所などに資金回収を依頼すると、前払金の支払を求められます。実際はこの弁護士事務所も詐欺犯であり、被害者はさらなる金銭被害を受けることになります。

ディープフェイク

ディープフェイクとは、テクノロジーを利用して、本物と見分けがつかない偽の動画や音声、発言を生成する技術です。本調査では、特殊詐欺においてディープフェイクと生成AIはまだ広く利用されてはいないとのコンセンサスが得られた一方で、将来の潜在的なリスクとして認識されていることも明らかになりました。

多数の銀行が、ディープフェイクやAIを利用した詐欺の件数は僅少と回答しています。現状はまだ、成功した詐欺行為の多くが、シンプルかつテクノロジーに頼らない方法で行われているのです。

以下は、銀行が遭遇したディープフェイクの事例です。

- 生成AIを使用した、本人確認や身元確認に使用されるパスポートなどの書類の偽造
- 生成AIを使用した、もっともらしい詐欺メールやメッセージの生成。多言語に翻訳し世界中のターゲットに送信された例もある
- ディープフェイクで生成した架空の人物を利用したロマンス詐欺
- 生成AIを使用した、不正行為のための偽銀行サイトの作成

本調査の回答者によると、ディープフェイクによる犯罪は、銀行よりも顧客を直接の標的とするケースが多いようです。たとえば、有名人や著名人のディープフェイクを利用したSNS上の投資詐欺がその一例です。

ディープフェイクやAIの利用は現時点では比較的珍しい手口であり、銀行は検知するのが困難であることを認識しています。

そのため、一部の銀行では、検知機能の整備に向けて外部ソフトウェアへの投資を進めています。

使用頻度はまだ低い手口ですが、将来的には増加することが予想されるため、銀行ではこの潜在リスクを認識し、今後の進展を注意深く監視しています。ある銀行では、著名な顧客のなりすましのリスクに注目し、顧客への質問を通じて本人確認を行うための研修を従業員に受講させる計画を進めています。

詐欺の標的

本調査により、最も狙われやすいのは個人および法人顧客の口座であり、特に個人顧客が最も被害に遭っていることが明らかになりました。

また、詐欺の手口により標的の年齢層が異なるものの、高齢の顧客が狙われるケースが多いとの回答が大多数の回答者から寄せられました。

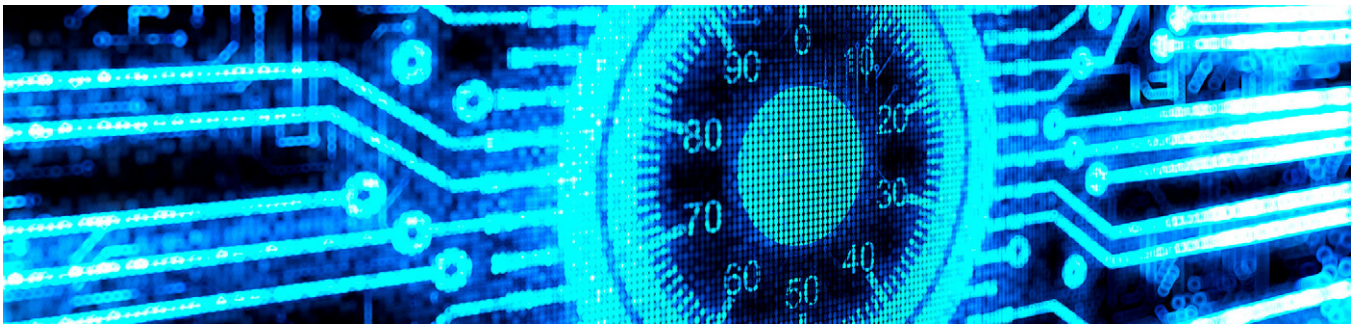
投資・サポート詐欺では高齢者層がターゲットにされており、最大の被害を受けていると見られる。一方で、若い世代はネットショッピング詐欺や暗号資産詐欺の標的にされる傾向がある。

詐欺行為が行われるチャネルとして、ネットバンキングやモバイルバンキングを中心とするデジタルプラットフォームがほとんどという回答が多く見られました。

自己名義口座間の資金移動

顧客が、異なる銀行の自らが保有する口座間で資金を移動する行為を言います。資金移動元の銀行では、詐欺などの不正取引を目的とした資金移動を特定できるかどうか不安を持っています。

2. ガバナンス



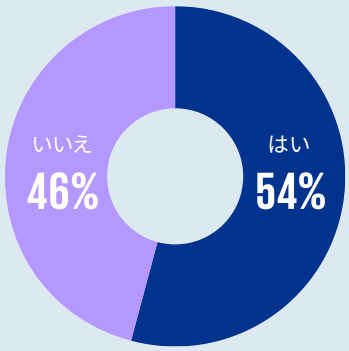
詐欺対策の戦略

本調査では、詐欺対策のための全体戦略や全体方針の規定・適用に関して、業界の見解が分かれていることが示されました。

調査に参加した銀行の半数強が、詐欺対策方針を既に整備しているか、整備を進めており、取締役会による承認や、監督責任を軸とする明確なガバナンス体制の構築に向けて取り組んでいます。

一方、残りの46％の銀行は、包括的な不正防止フレームワークを通じた取組みを行っており、詐欺対策戦略を不正防止活動に組み込むことで一貫した対応をとっています。

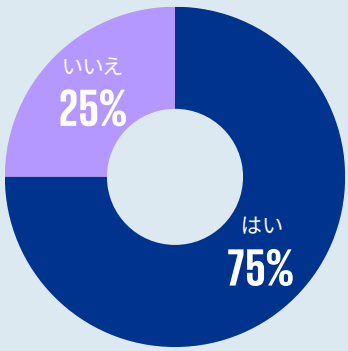
不正防止のための指針とは別に、詐欺対策に特化した全社的な方針を整備していますか？



リスク評価

特殊詐欺に特化したリスク評価を実施しているかどうかを尋ねる質問に対し、大部分の回答者は、実施しているものの、商品リスクまたは不正リスク評価の一環で行う場合もあると回答しました。

特殊詐欺を抑制するための統制の有効性を評価するリスク評価を実施したことがありますか？



適応性

特殊詐欺対策の戦略とアプローチを、新たな詐欺の手口や新しい金融商品・提供チャネルにどのように対応させているかを尋ねたところ、以下の共通のテーマが浮かび上がりました。

- **定期レビュー**（29％）：詐欺対策の定期レビュー（日次、週次、または月次）を行い、世界で蓄積される知見や顧客からのフィードバックを取り入れています。
- **協力・情報共有**（38％）：多くの銀行が、新たな詐欺の手口に関する情報を社内だけでなく、業界団体、法執行機関、他の銀行とも共有することの重要性を指摘しています。
- **データドリブン型のアプローチ**（15％）：銀行は、新たな詐欺の傾向の迅速な把握と対策のためにデータアナリティクスや機械学習といったテクノロジーを使用しているとした回答者も多く見られました。
- **専門チーム・委員会**（19％）：多くの銀行が不正リスク専門委員会や専門チームを有しており、定期的に協議の場を持ち、直近の詐欺事案の評価や対応戦略の立案・実行を行っています。

そのほか、以下の方法も挙げられました。

- **根本原因分析：**回答した銀行の多くが、詐欺がどのように発生するかを理解し、適切な対策を検討するための分析を標準手続として実施しています。
- **シナリオベース戦略：**一部の銀行では、臨機応変にシナリオベースの戦略を採用しており、定期的に戦略を評価・更新することで、新しい詐欺の手口への対応を図っています。

顧客への返金

87%の銀行が、詐欺被害相当額の返金に関するガイダンスを方針や基準に盛り込んでいることがわかりました。

また、返金の有無および金額（全額か一部か）を決定する方法について尋ねると、2つのテーマが浮かび上がりました。

- ほとんどの銀行が返金に関し一貫したアプローチを採用しており、善意を示しつつ規制要件も考慮するための全社的な枠組みと意思決定ツリーを整備しています。
- 回答したグローバル銀行のうち、特殊詐欺における被害相当額の返金に関し世界共通の指針を整備しているのはわずか23%で、規制環境の課題と多様化を浮き彫りにする調査結果となりました。

返金の有無や金額を事案ごとに判断している銀行のうち、ある銀行は、少額の返金については現場チームに委ね、多額の返金については委員会の承認を得ることとしている。

法令遵守

回答した銀行の一部は、法規制に基づき返金を実施しています。該当する法規制として挙げられたものには、英国の条件付被害返金モデル規定（CRM Code）や、オランダの銀行窓口詐欺（なりすまし）における損失補償基準（Criteria for awarding compensation for loss arising from bank help desk scams（‘spoofing’））などの自主的な取り決めがありました。

事案ごとの検討

その他の銀行は、十分な注意喚起がなされていたか、被害者が狙われやすい立場にあったか、初めて受けた被害であったか、顧客の言動がどうであったか、運用上の不備が無かったかなどの基準をもとに各事案を個別に検討する柔軟な対応がとられていました。

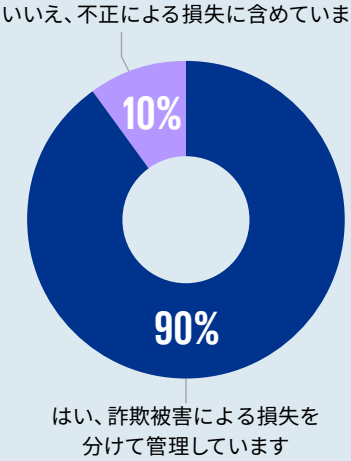
経営報告

調査対象の銀行の圧倒的多数（90%）が、顧客の詐欺被害による損失を不正全般による損失とは分けて管理することの重要性を認識しています。

これは多くの銀行で、報告書の項目を分ける、または委員会の協議の中で重要議題として取り上げているなどの形で示されます。

上記90%の回答者の大部分が、詐欺損失を経営情報の一部として、不正全般の損失と分けて個別に報告していますが、残りの10%は、経営報告において詐欺被害による損失を個別に報告していません。

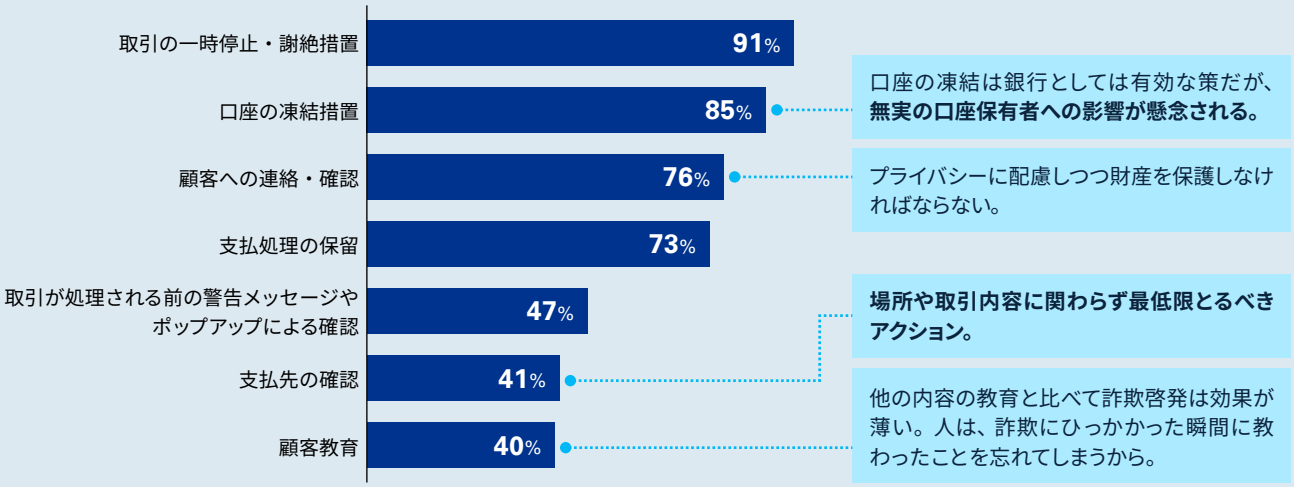
詐欺被害による損失を不正による損失とは分けて管理していますか？



3. 詐欺対策

詐欺対策は、個人・組織を詐欺から保護するための戦略と統制からなります。本調査では、詐欺予防策を講じている銀行の回答者に対し、各予防策の有効性を評価するよう求めました。

詐欺対策の内容



取引の一時停止・謝絶措置

銀行は疑わしい行為の調査を進めながら、取引を一時停止することで、不正が疑われる行為にストップをかけ、該当口座の全取引を制限することができます。

回答者の大多数にあたる91％が、有効な詐欺のリスク低減策として取引の一時停止・謝絶措置を選びました。銀行は、資金の送金元、送金先、顧客との取引期間などの調査に基づくリスクスコアや、不正の兆候を考慮の上、取引を制限します。

有効な策ではあるものの、昨今、マネーミュール用の口座はすぐに解約されるため、抑制効果は高くない。

口座の凍結

銀行が疑わしい行為を理由に口座利用を制限すると、その口座の保有者は制限が解除されるまでの間、資金の引き出し、送金などの取引を行うことができません。

問題が確認された口座を即座に凍結できるよう、常時モニタリングしている。

回答した銀行の85％が口座の凍結を有効な策と回答するも、無実の口座保有者にも支障が及ぶことを懸念しています。一方で、マネーミュール口座（不正に入手した資金の送金や洗浄に使用される口座）の場合は、凍結することで詐欺犯の頼みの綱である金融ネットワークを混乱させ、不正資金を移動させるための重要な経路を遮断できるため、優れた方法との回答でした。多くの銀行では、日次の監視体制を整備しており、既知のマネーミュール口座については業界データベースとも照らし合わせながら確認するプロセスを取り入れています。

顧客への連絡・確認

銀行が電話、電子メール、あるいはSMSを通じて顧客本人と連絡をとり、取引の確認や潜在的なリスクの説明を行います。これは、顧客を巻き込んだ直接的な不正防止策の1つです。

プライバシーに配慮しつつ財産を保護しなければならない。

回答者の76％が、疑わしい取引について顧客に連絡し確認を取ることは有効と回答しています。大部分の銀行が、アプリ内のメッセージのほか、電話で本人に直接連絡しています。従業員と顧客との効果的な会話により、疑わしい取引が実行される潜在的なリスクを理解させることができるため、顧客への直接の連絡は重要と認識されています。

支払処理の保留

取引の正当性を検証する時間を確保するために、支払プロセスを意図的に遅らせ、詐欺行為の成功率を下げます。

回答者の73％が、特定の条件に該当する支払手続きを遅らせるのは、顧客への問合せ・調査への対応の時間が必要な場合に有効な手段としています。そのような取引を一旦保留とするのでなく、即座に拒否する方針に変更した銀行もあります。支払の保留期間は通常2～72時間程度とされ、ハイリスクな取引の審査時間の確保に役立っているとのことです。

うまくやれば非常に有効だが、大変手間がかかる。

警告メッセージやポップアップによる確認

ネットバンキングやモバイルバンキング上での取引の際に、警告メッセージを表示し、取引実行前に取引の正当性を確認するよう促します。

大量のメッセージに嫌気が差している。

この手段を有効な詐欺対策だと考えている回答者はわずか47％でした。多くの顧客がよくある警告メッセージに慣れきっており、その効果が薄れていると説明しています。

効果的な対策は、リアルタイムのリスクスコアリングに基づく警告メッセージを、支払手続の中で特に重要な瞬間に絞って表示することや、顧客への直接連絡であるとの回答でした。

状況に合ったメッセージを、適時に、適切な顧客に送る必要がある。

支払先の確認

顧客が提供する支払先情報が、銀行のシステムに登録される情報と一致していることを確認します。これにより、支払におけるミスや不正取引を防止し、正しい支払先への送金を確実にします。

場所や取引内容に関わらず、最低限とるべきアクション。

支払先の確認を有効と回答したのはわずか41％でした。その多くが、一定の安心感や顧客体験の向上につながるほか、顧客の単純なミスを発見しやすくなると述べています。一方で、詐欺犯の多くは質問を上手くかわし、被害者には問合せを無視するよう指示することから、詐欺対策の効果は限定的であるとの回答も多く見られました。こういった見解はあるものの、稚拙な詐欺の撃退にはつながるため、このプロセスを導入している銀行ではあえて撤廃はしないとのことです。

顧客教育

銀行では、顧客自身が不正行為に気づき、回避し、報告するよう促しています。

本調査において顧客教育に対する見解はまちまちで、有効性の評価は困難との見方が目立ちました。支払手続中にリアルタイムのメッセージを表示するなど、手続中の複数のポイントで重要な瞬間に教育的情報を表示する方法（警告メッセージやポップアップなどで）が最も有効との回答でした。

詐欺啓発は効果が薄い。
人は、詐欺に引っ掛かった瞬間に教わったことを忘れてしまうから。

その他の取組み

新しい支払先の追加、住所の変更などを一定時間経過後に反映するなど、追加的な統制措置も整備している。反映までの時間は12時間で、詐欺犯の動きを大幅に遅らせるだけでなく、手続に一定時間がかかるので口座ごと乗っ取られるリスクを回避できる。

詐欺への関与を強要されている従業員を特定するための分析手続を導入済み。

預金口座のロック解除後、24時間はアクセスできないシステムを導入。

オーストラリアの大手2行は、暗号資産政策を強化している。一方は暗号資産の購入を月1万豪ドルに制限、もう一方は特定のハイリスクプラットフォームへの支払依頼を受け付けない方針としている。

銀行の問合せ窓口になりすました偽の銀行サイトや電話番号を削除。

狙われやすい顧客

81％もの回答者が、詐欺リスクが高い顧客の特定に取り組んでいると回答しました。英国の金融行為規制機構などの規制当局の定義を判断基準としている銀行もあります。年齢、健康状態、経済力などの従来の判断基準だけでなく、病気、死別、高価な買い物といった顧客の置かれる状況が、狙われやすさを左右することは既知の事実です。

狙われやすい顧客を保護するため、以下を含む取組みが実施されています。

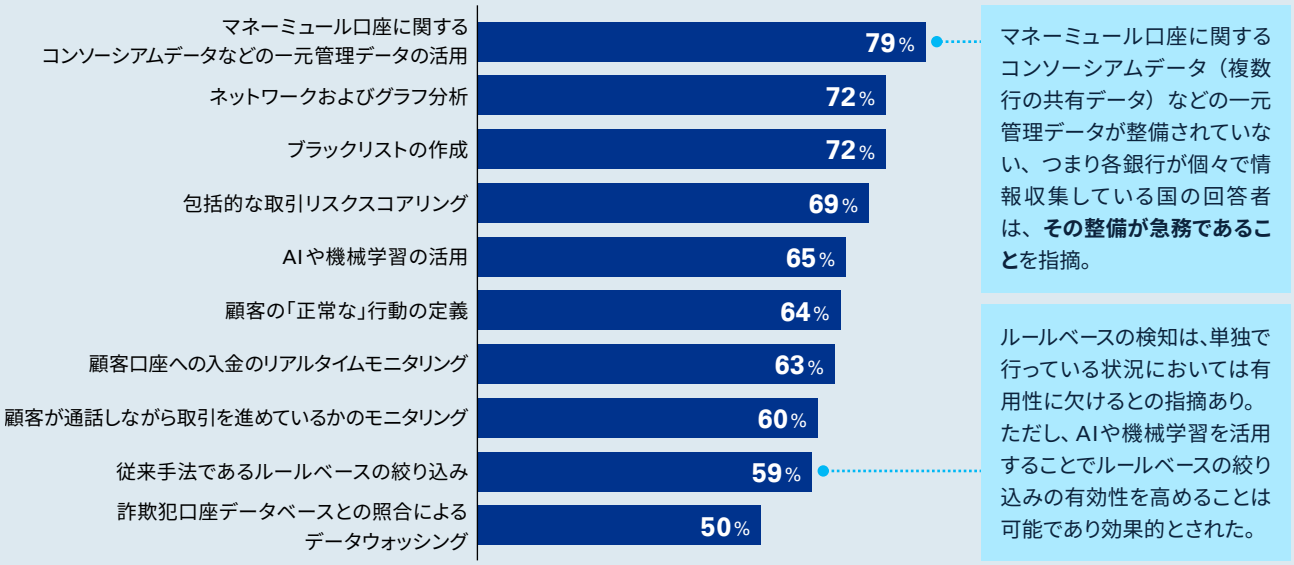
- モニタリング方法のカスタマイズ（特定の顧客セグメントの送金上限額を引き下げるなど）
- 機械学習を使用した狙われやすい顧客の特定（不正の可能性とそれによる影響の評価など）
- コアバンキングシステム内での直近の詐欺被害者の特定
- 従業員向け研修のカスタマイズ
- 追加的な取引承認プロセスの導入（支店での手続を条件とするなど）
- 対象を絞った教育の実施（特定の顧客層に向けた説明会の開催、顧客への対面でのリスクの説明など）

専門チームを置き、モニタリング活動を通じて狙われやすい顧客をいち早く認識し、必要に応じて顧客に直接コンタクトしている。顧客が家庭内暴力や虐待を受けている可能性がある場合に警告する仕組みも整備済み。

4. 詐欺の検知

詐欺は、不正行為を特定するための戦略およびプロセスを通じて検知します。本調査では、回答者が所属する銀行において、詐欺検知のための手段が整備されている場合に、その有効性を評価するよう求めました。

詐欺検知手法



マネーミュール口座に関するコンソーシアムデータ（複数行の共有データ）などの一元管理データが整備されていない、つまり各銀行が個々で情報収集している国の回答者は、**その整備が急務であること**を指摘。

ルールベースの検知は、単独で行っている状況においては有用性に欠けるとの指摘あり。ただし、AIや機械学習を活用することでルールベースの絞り込みの有効性を高めることは可能であり効果的とされた。

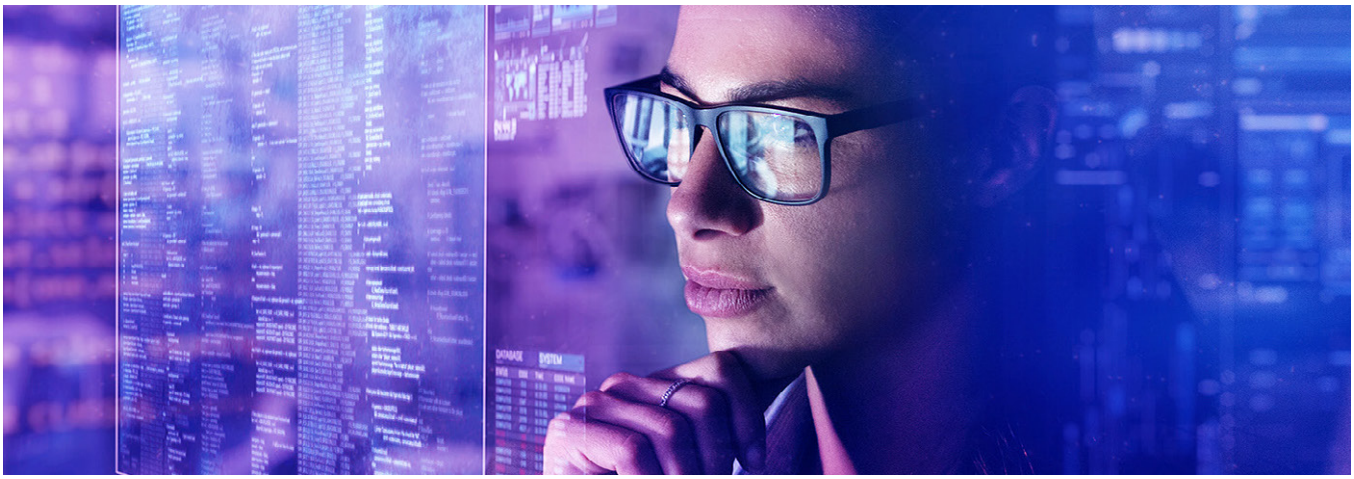
データ分析と共有

銀行や他の金融機関が保有する顧客データを分析することで、不正行為の可能性がある取引を検知することができます。組織内での分析により検知された疑わしい個人や取引に関するデータを他の銀行や規制当局と共有することで、こういった個人や取引に対する理解を深めることも可能です。

- **コンソーシアムデータ**とは、異なる銀行間で共有される、個人や取引に関する情報です。不正行為のパターンや関与者の特定の手がかりとなる情報を豊富に含み、詐欺の検知の可能性を高めてくれます。

データ共有を実施していない、つまり個々で情報収集している銀行の回答者は、そういった体制の整備が急務であり、その整備や監督の責任は行政にあると回答しています。コンソーシアムあるいは警察などの行政機関で一元管理されるデータへのアクセスを持つ回答者は、そういったデータが詐欺の防止に有効であるとしています。

- **ネットワークおよびグラフ分析**は、犯罪に関与する個人や組織を紐づけます。複数の回答者が、不正資金の運び屋（「ミュール」）が関与する不正の全貌を掴むのに特に有用、と回答しました。また、調査チーム間の協力・情報共有により、個人や組織の紐づけがうまくいく可能性がさらに高まると考えています。
- **ブラックリストの作成**とはコアバンキングシステムに登録される既知の不正行為者のリストで、不正を犯した人物や組織が追加されていきます。
銀行では、行政機関やコンソーシアムなどの外部の情報源から情報を受け取ることができる場合に、有効な手段であると考えています。一部の銀行では、投資詐欺を防ぐ目的で自国の金融当局から提供されたリストを利用しています。顧客が友人や家族に代わって決済を行ったケースなどで、ホワイトリストが有用であったとの回答もありました。



- **包括的な取引リスクスコアリング**は、位置情報、取引パターン、取引額などの予め設定された基準に基づき行われます。
  機械学習や行動的生体認証などの他の手段と組み合わせた場合に有用な方法、との声が聞かれました。
- **データウォッシング**とは、銀行等で継続的に行う、顧客取引データを詐欺犯口座のデータベースと照合する作業をいいます。
  回答者の50％が、組織内外のブラックリストを使用した、既知の詐欺犯口座との照合によるデータウォッシングが有効な手段であると感じています。ただし、不正ネットワーク内の関係を特定するのには効果的ではあるものの、不正履歴がないマネーミュール口座が絡む場合には十分な結果が得られません。 大部分の回答者が、業界内の協力関係の強化により、データウォッシングの有効性が高まるとの見解を示しました。

ネットワーク内の関係を特定する場合に特に効果的。

AIおよび機械学習

詐欺を検知する可能性を高めるために、AIや機械学習を他の手法と組み合わせて使用するケースが増えています。

AIや機械学習を有効と評価した回答者は、ルールベースの絞り込みの有効性を高めるためにAIや機械学習を取り入れたと説明しています。

顧客の行動のモニタリング

口座や取引を介した不正の疑いのある行為を検知するため、コアバンキングシステムには、顧客の行動を予防的にモニタリングする先進的な機能が備わっています。

回答者の半数以上（64％）が、**顧客の取引実績を分析して「正常な」行動パターンを定義する**ことが、異常な取引の検知に有効であると述べています。また、誤検知（不正取引として誤って検知された正規の取引）を減らす上でも効果的な方法との見解も見られました。

回答者の63％が、顧客口座への**入金取引をリアルタイムかつ予防的にモニタリングする**方法を有効と評価しています。マネーミュールの兆候ともいえる異常な活動や不正な預金を検知するためのモニタリングを実施しています。どの程度有効かについては、各銀行等における運用の成熟度に依存します。

一部の銀行では、顧客がネットバンキングやモバイルバンキングを利用しながら**第三者とやりとりしているかどうかをモニタリングしています。**このモニタリングを実施している銀行の60％が、これを効果的な詐欺対策と考えています。本調査を実施した時点では、多くの銀行がこのテクノロジーの導入を進めている最中にあったため、その有効性については回答を控えました。

最後に、**従来手法であるルールベースのアプローチ**は、回答者の59％が有効と評価しました。規定の条件によって、位置情報、取引パターン、取引額などの属性に基づき検知する手法ですが、一部の銀行では、入金および出金取引の双方にこの手法を採用しています。また、この手法は単独では効果がなく、複数の方法を組み合わせた分析が必要とのコメントもありました。

他の手法と組み合わせて使用する場合のみ有効。

5. 不正対応

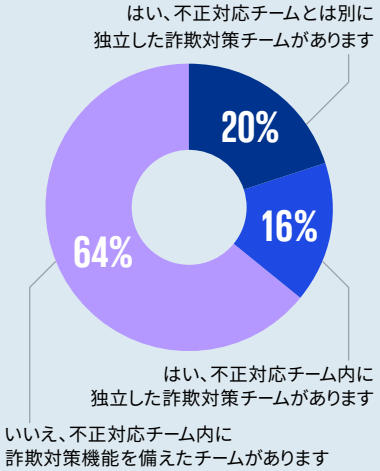
本調査では、不正対応チームの構成と責務に加え、詐欺に関するアラートが発出された際の調査や解決の方法について尋ねました。

詐欺対策チームの構成

大半の銀行で、不正対応チーム内に詐欺対策機能を備えるチーム体制をとっているとの回答でした。詐欺専門の独立したチームを持つのではなく、不正防止・不正対応という大きな枠の中に詐欺対策も含めるアプローチです。

一方、一部の銀行では、特定の部門から詐欺対策機能を切り出し、デジタル決済やネットバンキングなどの領域に対応させる体制をとっています。

不正対応チームとは別に、独立した詐欺対策チームがありますか？



詐欺対策チームの責務

専門の詐欺対策チームあるいは不正対応チーム内に詐欺対策機能を備える銀行において、当該組織の責務は以下を含みます。

- **事案管理：**詐欺事案のレビュー、規制基準遵守のための対応、複雑な状況下での顧客対応方法の決定を行います。
- **調査：**アラートが発出された取引やマネーミュール口座と疑われる口座の調査を行います。
- **顧客対応：**一部の銀行には、「呪縛解除」チームがあります。このチームは、詐欺で使われる巧妙な手口、すなわち「呪縛」を顧客に理解させ、それを解くサポートを提供する組織です。この組織が、被害者の対応窓口の機能を兼ねる場合もあります。
- **資産の追跡：**顧客の資金を追跡し、回収します。
- **返金請求：**詐欺被害の返金について決定します。複雑なケースは上層の意思決定組織に持ち込まれます。
- **詐欺の実態の把握：**将来的な詐欺の防止のために、詐欺の実態や新たな手口を調査し、顧客に対し啓発や注意喚起を目的とした資料を配信します。

不正対策研修

本調査では、特殊詐欺に関するアラートへの対応のため、金融機関がさまざまな研修プログラムを採用していることが示されました。

- **各種業務に関する研修：**一部の銀行では、ディシジョンツリーに基づいた研修を整備し、詐欺被害者の可能性がある顧客への対応に特化した研修コースを用意しています。
- **顧客対応およびソフトスキル：**複雑な事案を評価する力や、潜在的なリスクに関して顧客を納得させる説得力を身につけるため、効果的な聴き取りの方法や判断力に関する研修に加え、憤慨した顧客や自己防衛に走る顧客にうまく対応するための研修も担当者に受講させます。
- **詐欺の手口：**事案の対応に当たる従業員が顧客に正しい情報を伝えられるよう、現在使用される詐欺の手口に関する研修の受講を徹底します。

顧客体験は重要であり、顧客が負った心の傷を乗り越えるためのサポートも顧客体験の一環。詐欺対策担当者は、不正行為を見抜く能力だけでなく被害者への共感も示さなければならない。

不正対策に関する判断の自動化

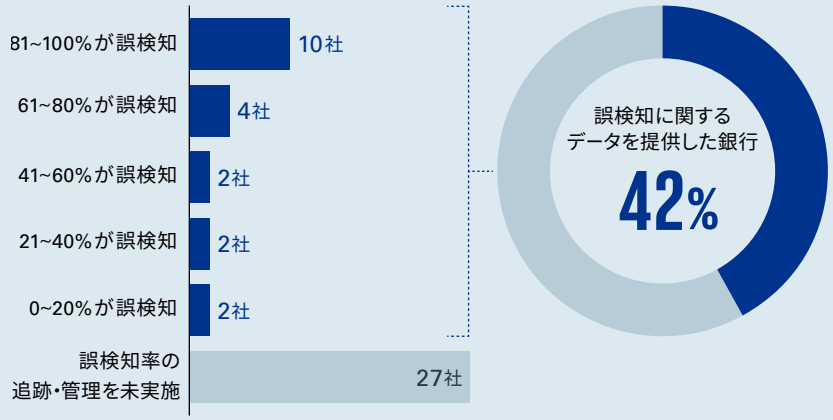
回答した銀行の半数強（56％）が、取引の保留や口座の凍結を自動的に決定するための条件を設定しています。一方、被害相当額の返金に関しては、自動的な判断は行わないことを原則としています。

問題の性質によっては、人による判断が必要。

誤検知

誤検知とは、正規の取引が誤って不正取引として検知されることをいいます。誤検知に関するデータを提供した銀行は回答者全体のわずか42％でしかなかったものの、これらの銀行の誤検知率はかなり高く、特殊詐欺による取引を検知することの難しさを示しています。取引を行う当事者は当然顧客本人であることから、他の類いの不正に使用される端末の確認は何の役にも立ちません。また、詐欺犯は銀行の統制措置を熟知しており、支払額を検知システムに引っ掛からない水準に変更するでしょう。

詐欺に関する警告のうち誤検知の比率はどの程度ですか？



既知の詐欺行為に対する注意義務

財務的安全性が刻々と変化する中、顧客資産の保護が顧客の自己決定権に影響を及ぼすケースが増えています。詐欺の可能性があると警告された取引を顧客が強行しようとする場合にどのような対応をとるか、という質問からは、顧客との関係性を維持しながらリスクを軽減するための戦略の数々が浮かび上がりました。

- **取引の拒否：** 回答した銀行の51％は、ブラックリストに登録されている支払先への支払である場合など、詐欺に関連している可能性が高い取引の場合に、当該取引を拒否すると回答しています。
- **説明と同意：** 一部の銀行では、詐欺のリスクが検知された顧客から明示的な承諾を得るプロセスを踏んでいます。口頭または書面での確認を含み、支店にて対面で得る場合と承諾書への署名の形をとる場合とがありますが、いずれの場合も、顧客が説明を受けたリスクを理解していることと、取引による財務的影響に関して銀行の責任を追及しない意思を表明するものです。
  このプロセスにより、顧客が危険性を十分に認識していること、銀行側がデューデリジェンスを通じてアドバイザーとしての役割を果たしたことが確認されます。
- **追加の手間・制限：** 一部の銀行では、顧客が特殊詐欺について考え直す時間を確保しようと、追加の手間や制限を課して、手続を一時停止させます。たとえば、踏み込んだ質問を投げかけ再検討を促す、支店への来店を求める、信頼できる家族の意見を求めるようアドバイスする、などの方法があります。
- **リスクプロファイルとリスクに応じた対応：** 銀行は、検知された詐欺や不正のリスクの高さに応じてしばしば対応を調整します。たとえば、リスクが比較的低いとされる小規模な取引の場合は、顧客を教育した後に処理を進める場合がある一方で、リスクや金額が大きい取引は拒否に至る可能性が高くなります。
- **法執行機関への持ち込み：** 一部の国・地域では、詐欺行為が明白でありながら顧客の説得に至っていない事案は司法機関に持ち込むこととしています。たとえば英国では、銀行・警察間の連携により「銀行行動規範（Banking Protocol）」と呼ばれる対応措置を講じます。この規範のもと、支店の従業員は、詐欺被害の兆候を検知するスキルを身につけるための研修を受講し、検知した場合には警察の緊急サービスに通報します。警察は支店を訪れ、詐欺容疑を調査するとともに、容疑者が現場にいる場合は取り押さえます。
- **顧客による選択を優先：** 高リスク取引と区分されていても顧客が実行を希望すればそれを進める方針としている銀行では、風評リスクや法的リスクに加え、最終的な意思決定権は顧客にある点をその根拠として挙げました。

常習的な被害者に対する注意義務

たびたび詐欺被害を受ける常習的な被害者が顧客にいる場合、銀行側では当該顧客との取引関係を継続するか、リスクや対応費用の増大を受け取引関係を断つかという重要な決断を迫られます。

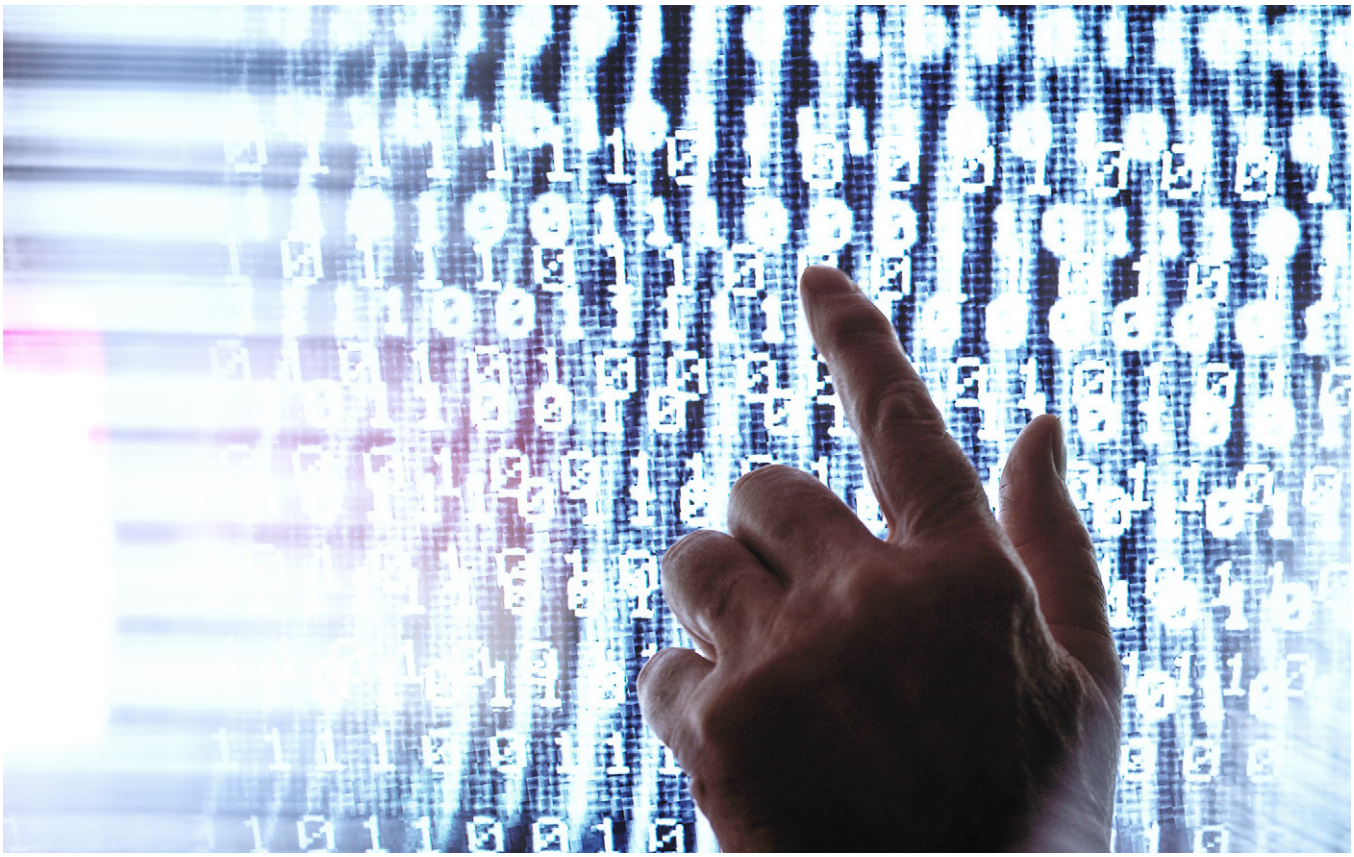
本調査では、回答した銀行のほとんどが、完全な取引の中止よりも保護策を講じることを選択すると回答しました。取引関係を解消することはせず、ハイリスク口座に指定する、モニタリングを強化するなどして、不正行為の予防を図るアプローチです。顧客と金融機関の双方をさらなる詐欺被害から守るために、追加の手間や制限を課すことも多くあります。

口座は閉鎖しないまま、ネットバンキングへのアクセスや国際取引を制限するなどの措置を講じるのです。この方法により、顧客に寄り添って基本的な金融サービスを引き続き提供しながら、詐欺被害のリスクを低減できたとのことです。この意思決定に大きな影響を与えるのが、金融包摂の問題です。

回答した銀行の45％が、最終手段として顧客との取引の中止も検討すると回答しているものの、実行されることはあまりありません。通常、経営幹部層が事案ごとの状況に基づき、決断を下します。取引の中止との決断に至るのは、顧客が不正行為の共犯者である可能性（「ファーストパーティー詐欺（当事者による詐欺）」と呼ばれる）がある場合など、想定されるリスクが高く口座を継続する価値がないことが示された場合です。大抵の銀行は金融サービスを拒否することに対し慎重であり、顧客が故意に不正行為に関与したことが発覚した場合のみに、取引関係を断つ選択肢を検討します。

6. 知見の提供

回答した銀行の大多数が、詐欺や不正の撲滅を目指すコンソーシアムデータを使った取組みの一環として、特殊詐欺に関する情報を何らかの形で他行と共有しています。



以下は、その取組みに携わる組織と情報提供の方法の例です。

- **法執行機関とのパートナーシップ：** シンガポール警察の詐欺対策司令部（Anti-Scam Command）や、英国の国家犯罪対策庁（National Crime Agency）の一組織である国家経済犯罪センター（National Economic Crime Centre）など、一部の国には金融犯罪専門の部隊があります。
- **業界団体：** 英国のUKファイナンス（UK Finance）、北欧金融業界のコンピュータ緊急対応チーム、カナダ銀行協会（Canadian Bankers Association）、オランダ銀行協会（Nederlandse Vereniging van Banken）、米国銀行協会（American Bankers Association）、オーストラリア銀行協会（Australian Bankers Association）などがあります。
- **民間組織によるパートナーシップ：** 世界の金融セクターでは、多数のパートナー組織がコンソーシアム内で情報共有を行っています。
- **非営利組織：** 英国の詐欺防止サービス（Cifas）、オーストラリア金融犯罪情報交換所（AFCX）、南アフリカ銀行リスク情報センター（SABRIC）などがあります。

銀行による情報提供の程度にはばらつきがあり、プライバシー保護、GDPRなどのデータプライバシー関連規制、各国の中央銀行の方針などにより情報共有が制限されているとの回答もありました。詐欺は国境を越えて行われる犯罪行為であることから、こういった情報の制限を緩和することは今後の優先課題と考えられています。

7. ブランド保護

今日のデジタル環境では、銀行のブランドを保護する取組みが不可欠です。ブランド保護を徹底することで、顧客の信頼を確かなものにし、セキュリティ対策の強化、評判の維持にもつながります。

ダークウェブのモニタリング

本調査では、83％もの銀行が、詐欺に関する情報を得るためにダークウェブのモニタリングを実施していると回答しました。これらの銀行のサイバーセキュリティチーム（あるいは外注先）は、以下をモニタリングしています。

- **詐欺の実態・傾向：**モニタリングを行う銀行が名指しされている、またはターゲットになっていると推定できる記述など
- **顧客情報の侵害：**カード情報など
- **情報漏洩：**公表が許可されていない機密情報や個人情報の漏洩
- **評判：**その他自行に関する会話

その他の取組み

銀行ではこのほかに、以下の取組みによって詐欺や不正などの影響からブランドを守っています。

- **なりすまし対策：**銀行ではインターネット情報のモニタリングを行い、著作権侵害、ウェブサイトコードのコピー、ウェブサイトの複製、銀行またはその従業員を装った偽のウェブサイト、モバイルアプリ、SNSアカウントの有無を監視しています。銀行はまた、偽のウェブサイトの存在を示すような自行名に関連するインターネットドメインの登録がないかもモニタリングしています。
- **アルファタグ*2の保護：**アルファタグは顧客にSMSを送信する際に送信元を明確にすることができます。一部の銀行では、通信会社や世界の業界団体と連携し、アルファタグのなりすまし（正規の送信元IDから送信されたかのように見せかける行為）から保護しています。
- **テイクダウンサービス：**インターネット上から有害なコンテンツを削除するサービスで、ブランド、著作権、プライバシーの侵害を受けた銀行、企業、個人が、外部ベンダーに委託するのが一般的です。偽のマーケティングサイトやSNSのプロフィールを削除するサービスが提供されることもあります。
- **ホワイトハットハッカー：**倫理的ハッカーとも呼ばれるサイバーセキュリティの専門家で、システム、ネットワーク、アプリケーション内のセキュリティ上の欠陥を特定し、解消する専門知識を有します。システム所有者の同意のもと、セキュリティ対策の強化や潜在的リスクへの対策を講じます。
- **発信禁止番号リスト（Do Not Originate list）への登録*3：**このリストには、詐欺犯が銀行になりすますために使用する恐れのある、実在する銀行の着信専用番号も含まれています。一部の銀行では、着信専用番号をこの発信禁止番号リストに登録することで、なりすましに使用されるのを防いでいます。

*2 ［翻訳者註釈］アルファタグとはSMSメッセージでしようされる送信者を表す11桁以内の文字列（数字、文字や特殊等）で構成される固有の識別子をいう。
*3 ［翻訳者註釈］国によっては、企業が着信のみに使用する番号をリストに登録することによって、通信事業者がリストに登録された番号からの発信を制限する対策が取られている。

8. テクノロジー

詐欺の高度化が進む中で、特殊詐欺の防止、検知、対応に使用されるテクノロジーも進化しています。

オーケストレーションレイヤー

オーケストレーションレイヤーは、多数のデータソースを単一のシステムに統合するテクノロジーです。これにより、顧客情報へのアクセス性が向上し、より迅速で正確な情報に基づいた意思決定が可能になるとともに、サイバーインシデントが発生した際の調査が容易になります。

個々の取引のみではなく、顧客の活動全般を調査（360度評価）するのが、最も強力な統制手段。

回答した銀行の59％が、オーケストレーションレイヤーを備えていると回答し、複数の銀行で現在構築中あるいは導入中と回答しています。

統合の対象となるデータソースには以下を含みます。

- 取引データ
- KYC情報
- リスク格付
- 端末情報
- 行動解析データ
- 不正に関する警告

さまざまな段階における顧客の行動傾向、取引習慣、プロファイル特性を同時に評価可能。

不正行為の99％が、衝動的犯行ではないと言われる。 別の何かとつながり、組織的に仕組まれる。したがって、物事を個別に見るだけでは不十分で、取引情報と非取引情報の関係性もしっかり理解する必要がある。

次世代詐欺対策テクノロジー

回答者に対し、特殊詐欺を防ぐための次世代テクノロジーについて尋ねたところ、以下を含むさまざまなテクノロジーに関する回答が寄せられました。

- **行動解析：**主に未承認詐欺（被害者の同意なく行われる取引を通じた詐欺）の検知に使用される手法です。行動バイオメトリクスによって顧客の音声からストレスが検知され、顧客が詐欺の被害者である可能性を示した実例もありました。
- **ディープフェイクの検知：** 銀行ではさまざまなテクノロジーを駆使し、ディープフェイクによる不正の特定と防止に取り組んでいます。
- **適応性の高い自己学習型のルール設定：**継続的なモニタリングや取引データに基づき検知ルールを適応・更新することが可能なシステムは、刻々と進化する動的な検知ルールによって、新たな詐欺の手口にも素早く対応することが可能です。
- **状況に合わせカスタマイズされる警告メッセージ：**支払手続の過程で、顧客に詐欺のリスクがあることを理解してもらうため、銀行は明確で詳細の説明が必要となります。こうした取組には取引手続の前の、顧客との自動または生成AIを使ったチャットサービスを通じたコミュニケーションによる説明も想定されます。

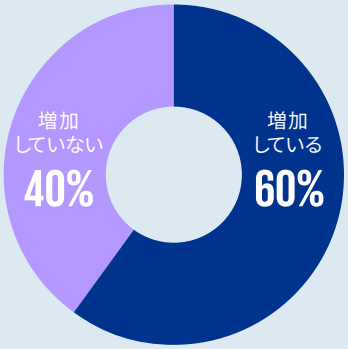
9. 顧客からのクレーム

以下は、不正や詐欺に関する顧客からのクレームに多い内容です。

- **被害相当額の返金：** 顧客が返金を受けられなかった場合、あるいは返金請求の結果に不満がある場合のクレームです。
- **追加の手間・制限：** 問題の解決や取引の実行に際し、多くの制限が課せられたことに対し苛立ちを感じた場合のクレームです。これらの制限には、手続の遅延あるいは拒否、行き過ぎたセキュリティ対策が含まれます。
- **保護：** 特殊詐欺を未然に防ぐために、銀行側でさらなる対策を講じるべきだとするクレームです。具体的には、より確実な詐欺の検知、より効果的な教育の取組み、詐欺が疑われる取引の停止などを要求してきます。
- **銀行の対応：** そのほかに、クレームを入れた時点から解決までの対応が遅かったこと、資金利用が制限されたこと、詐欺事案に関する最新情報など銀行からの情報伝達が不十分だったことなどについて、クレームを受けることがあります。

ある銀行では、犯罪者からのクレームが増加している。
犯罪者自身が支店に出向いて口座の凍結の解除を強要することも。

詐欺に関するクレームは増加していますか？



10. 顧客教育・啓発

銀行では、顧客が警戒心を高め、自分自身を守る術や怪しい要求に気づく能力を身につけてほしいとの思いで、特殊詐欺の兆候や手口に関する教育を提供しています。

本調査では、詐欺対策における顧客教育と啓発の役割についての理解を深めるため、具体的な取組みを7つ挙げ、各銀行で実施しているものを選んでもらいました。

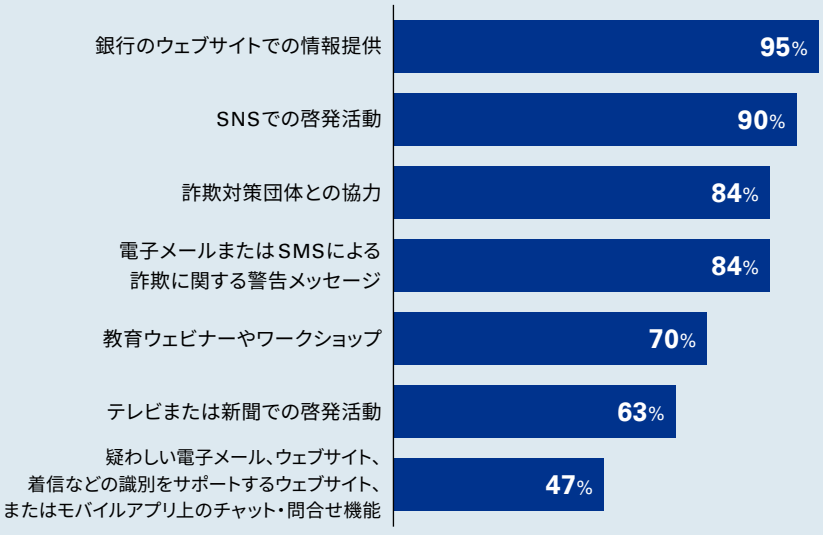
すべての回答者が、コミュニケーション戦略には、単一の取組みではなく、複数のプラットフォームをまたいだ継続的な取組みを盛り込むべきと考えています。回答者の数名は、啓発運動の効果は長く続かないと述べています。

銀行での画期的な取組みについて尋ねたところ、所属行の内外での取組みに関する回答が寄せられました。以下は、その一部です。

- 中央銀行や大学との協力
- 顧客がコールセンターの応答を待つ間の、不正の実態・傾向に関する情報提供
- クリスマスやイードなどの休暇を対象とした季節の取組み
- オンライン市場でのリスクに焦点を当て、対象を絞り込んだ啓発運動
- 顧客を疲弊させないよう、取引内容に応じてポップアップを調整
- 顧客がデジタルウォレットを開設する際に、暗号資産に関するオンライン講習の受講を要請

2024年だけで、32もの啓発運動を実施。

以下の取組みのうち、実施したことのあるものはどれですか？



詐欺に関する警告メッセージと教育

詐欺に関する警告メッセージや教育活動の有効性は数値化が難しいにもかかわらず、回答した銀行の51％で、それらの有効性のモニタリングを試みていることが明らかになりました。

以下は、有効性の測定方法の例です。

- **浸透度合いの測定：**閲覧者数、視聴者数、クリック率に基づき測定
- **支払手続中に表示される警告メッセージの影響：**特定の取引に対する警告メッセージが表示された後に断念された支払の件数に基づき測定
- **事例証拠：**不正行為を回避した顧客の成功事例に基づき測定
- **詐欺事案の推移の分析：**教育実施後の詐欺事案の推移に基づき測定
- **顧客調査：**調査回答に基づき測定

11. 課題と機会

特殊詐欺リスクの管理における今後の課題と機会について尋ねたところ、課題と機会に共通のテーマが浮かび上がりました。

テーマ	課題	機会
規制	銀行は、各国・地域での急速な環境の変化に応じて事業活動を変化させていく必要があることから、急速な規制の変化への対応が大きな課題となっている。 多くの国・地域において、詐欺を取り巻く社会構造の中では、規制対応の責任は銀行に向けられることが多く、銀行以外の金融機関はさほどの責任を追及されてこなかった。	規制を厳格化する、うまく機能した規制モデルを他国にも取り入れるといった取組みにより、規制の有効性と適用性を確保することが可能。 詐欺を取り巻く社会構造におけるすべての利害関係者を対象に規制が強化され、ステークホルダー間の連携が推進されれば、あらゆる業界で特殊詐欺の検知と対処が強化されるだろう。
情報共有	データプライバシー規制は、重要な情報の共有の妨げとなることがあり、クロスボーダー取引での情報共有は特に困難である。取引のグローバル化が進み、国際犯罪組織が台頭していることから、各国の銀行と法執行機関による国を跨いだ連携が一層複雑化している。	包括的な戦略のもと、国境を越えたパートナーシップやコンソーシアムデータモデリングなどの有効な取組みを実施すれば、詐欺やマネーミュールのネットワークに対処できる可能性がある。これには、業界を超えた情報共有プロトコルや、銀行、法執行機関、通信会社、暗号資産交換業者など、詐欺を取り巻く社会構造における重要なステークホルダー同士の連携も求められる可能性がある。
テクノロジーの進化とAI	生成AIを使えば単純な本人確認手続をすり抜けることができる。生成AIの台頭により今後ますます巧妙な詐欺の手口が使われることが予想され、詐欺の検知はさらに複雑化すると見られる。	生成AIは詐欺リスクの管理に有用である。たとえば、生成AIを使用し、状況に応じてメッセージをカスタマイズすることで、顧客へ特定のリスクを警告することが可能となる。
顧客教育・啓発	顧客の間で「大量のメッセージに対する疲弊」が見られることから、銀行は新しい配信方法を検討する必要がある。	政府資金による啓発運動により、国民の詐欺に対する意識を高めるほか、顧客の批判的思考と強力な認証手段の利用を促すことで自己防衛を支援できる可能性がある。
テクノロジー・人材への投資	銀行では、進化する詐欺の技術に後れをとらないよう、新しいツールや研修への投資を継続していく必要がある。一部の国ではこれに加え、熟練した人材をめぐる競争や人材の移住が課題となっている。	銀行では、不正対策業務の統合や機械学習の活用により、不正検知プロセスを最適化できる可能性がある。
取引関係の一元管理	一部の銀行では、取引関係が複数のチャネルや商品にわたる顧客の取引を一元的に管理することが困難であり、詐欺行為を未然に特定することが難しい。	昨今、多数のデータソースを1つのオーケストレーションレイヤーに統合する動きが見られる。この環境下では、生成AIを利用することでチャネルや商品をまたいだ管理ができる。

12. お問合せ先・執筆協力者

本書の作成に携わった多くのKPMGメンバーファームのメンバーに謝意を表します。

Trygve Kringlebotn Aandstad
Director, Forensic
KPMG in Norway
E: trygve.aandstad@kpmg.no

Marilyn Abate
Partner, RC – Financial Crimes
KPMG in Canada
E: marilynabate@kpmg.ca

Steve Ackroyd
Director, Forensic I&C
KPMG in the UK
E: steve.ackroyd@kpmg.co.uk

Ignatius Adjei
Partner, FS Forensic
KPMG in the UK
E: ignatius.adjei@kpmg.co.uk

Anja Apfel
Assistant Manager -
FS Regulatory & Compliance
KPMG in Germany
E: aapfel@kpmg.com

Maria Barcenilla
Director, Forensic Technology
KPMG in Spain
E: mbarcenilla@kpmg.es

Cedric Biedermann
Director, CO Forensic CH
KPMG in Switzerland
E: cbiedermann@kpmg.com

Luca Boselli
Partner, Cyber & Tech Risk
KPMG in Italy
E: lboselli@kpmg.it

Christina Chliaoutaki
Manager, Data Analytics
KPMG in Greece
E: cchliaoutaki@kpmg.gr

Pedro Costa
Partner, Advisory
KPMG in Portugal
E: pdcosta@kpmg.com

Mikael Flod
Senior Manager, Financial Services
KPMG in Sweden
E: mikael.flod@kpmg.se

Patricia Gabriel
Associate Director, RC GRC
KPMG in South Africa
E: patricia.gabriel@kpmg.co.za

Joakim Hansson
Manager, Financial Services
KPMG in Sweden
E: joakim.hansson@kpmg.se

Christopher Jackson
Director, Forensic
KPMG in Singapore
E: christopherjackson@kpmg.com.sg

Marc Kilcher
Partner, FS GE
KPMG in Switzerland
E: mkilcher@kpmg.com

Eric Lachapelle
Partner, RC – Financial Crimes
KPMG in Canada
E: ericlachapelle@kpmg.ca

Alex Lerner
Senior Associate, Financial Services
KPMG in USA
E: alexlerner@kpmg.com

Alwyn Loh
Director, Forensic
KPMG in Singapore
E: alwynloh@kpmg.com.sg

Joao Madeira
Partner, Advisory
KPMG in Portugal
E: jmadeira@kpmg.com

Michelle van der Merwe
Senior Manager, Forensic
KPMG in South Africa
E: michelle.vandermerwe@kpmg.co.za

Javier Migoya
Director, Forensic Technology
KPMG in Spain
E: jmigoya@kpmg.es

Oytun Onder
Partner, Forensic
KPMG in Turkey
E: oonder@kpmg.com

Patrick Ozer
Partner, Forensic
KPMG in the Netherlands
E: ozer.patrick@kpmg.nl

Catherine Pihl
Manager, Forensic
KPMG in Norway
E: cathrine.pihl@kpmg.no

Timo Purkott
Partner, Forensic
KPMG in Germany
E: tpurkott@kpmg.com

Jori van Schijndel
Senior Manager, Forensic
KPMG in the Netherlands
E: vanSchijndel.Jori@kpmg.nl

Paul Stanwix
Associate Director, Forensic
KPMG in Australia
E: pstanwix@kpmg.com.au

Harriet Tennent
Director, Forensic
KPMG in Australia
E: htennent1@kpmg.com.au

Cenk Tuce
Director, Forensic
KPMG in Turkey
E: ctuce@kpmg.com

Dustin J Tupper
Managing Director, Advisory
KPMG in USA
E: dtupper@kpmg.com

Vasiliki Varzaka
Director, Deal Advisory
KPMG in Greece
E: vvarzaka@kpmg.gr

Amelia Ventura
Associate Partner, Forensic
KPMG in Italy
E: aVentura@KPMG.IT

Rohan Vinu
Manager, Forensic
KPMG in Australia
E: rvinu@kpmg.com.au

[英語オリジナル]

KPMG Global Banking Scam Survey
Strategies to manage authorised push payment fraud

発行日：2025年2月
発行所：KPMGオーストラリア

[日本語抄訳版]

発行日：2025年8月
発行所：株式会社KPMG Forensic & Risk Advisory

T: 03-3548-5773
E: FRA-Contact@jp.kpmg.com

kpmg.com/jp/fra

本冊子は、KPMGオーストラリアが2025年2月に発行した「KPMG Global Banking Scam Survey: Strategies to manage authorised push payment fraud」を、KPMGオーストラリアの許可を得て抄訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。