マネーローンダリング対策実務３級試験　最新情報

「マネー・ローンダリング等対策の取組と課題」の概要

2025／10（再掲載）

今般、金融庁では、マネー・ローンダリング・テロ資金供与対策について、2023 事務年度の金融庁所管事業者の対応状況や金融庁の取組等を「マネー・ローンダリング等対策の取組と課題（2024 年６月）」として取りまとめ、公表した。本レポートは、「第１章日本政府におけるマネロン等対策の取組」「第２章ＦＡＴＦ第４次対日相互審査での指摘対応を含めた基礎的な態勢の整備」「第３章 ＦＡＴＦ第５次対日相互審査を見据えた実効性向上に向けた取組」「第４章 金融サービスの不正利用対策」から構成されている。とりわけ、特殊詐欺事案等の急増とこれらにおける金融サービスの不正利用対策は目下の最重要課題であることから、本稿では、第４章を下記転載（一部抜粋）する。なお、全体の内容については、下記を参照のこと。

https://www.fsa.go.jp/news/r5/amlcft/20240628/20240628.html

【第４章　金融サービスの不正利用対策】

近年、インターネットバンキングに係る不正送金事犯及び特殊詐欺事案や預貯金口座不正利用事案等は著しく増加傾向にある。これら金融サービスの不正利用等から得た被害金等は、多数の口座から集約用口座に資金移転される、オンラインカジノ等を経由した資金移転が行われる、暗号資産に変換されるなど、資金の行方を不透明なものとする事例が多く確認されており、金融犯罪の複雑化・巧妙化がより一層進みつつある。

金融庁は、我が国の金融サービスにおいて、不正な口座開設・売買・譲渡やこれらを悪用した資金移動等を阻止することは、利用者保護の観点に加え、マネロン等の前提犯罪の削減や抑止等に向けた取組の一環として極めて重要と認識しており、引き続き金融業界と連携して様々な取組を行っていく。

１．インターネットバンキング不正送金対策強化

（１）フィッシング対策

わが国のインターネットバンキングに係る不正送金事犯については、昨年に引続き増加傾向にあり、各金融機関等によるフィッシング対策の高度化が喫緊の課題となっている。

フィッシングの特徴としては、常に他金融機関等比で脆弱な金融機関等に標的が移ることや、金融機関側が対策を講ずるたびに新たなフィッシング手口による攻撃が行われることにある。そのため、絶えずフィッシング対策の情報収集を行い、フィッシングの最新の手口や他の金融機関等のフィッシング対策の取組状況等を把握する必要がある。以下、金

融庁がモニタリングにより把握した各金融機関等のフィッシング対策の取組状況を列挙する。各金融機関等は、これに限らず他の金融機関等や業界団体と連携し、日々対策を高度化していくことが求められる。

・普段と異なる利用環境からのアクセスを適時・適切に捕捉するシステムを導入し、リアルタイムでのログイン謝絶や送金保留を実施
・不正送金事犯で使用された ＩＰアドレスや端末情報をブラックリスト化し、リスト登録先からのログインを自動謝絶
・モアタイム中（夜間）の振込上限額の変更依頼や新規振込先への送金依頼 を自動保留し、即時での反映は行わず、翌営業日以降に反映

（２） 暗号資産交換業者宛ての不正送金対策

昨今、インターネットバンキングによる不正送金事犯や特殊詐欺事案において、暗号資産交換業者が所有する預貯金口座を利用した不正送金被害が多発している。こうした状況を踏まえて、2024 年２月、金融庁と警察庁は連名で、全銀協を始めとする関連業界団体等へ利用者保護等のためのリスクベースによる更なる対策の強化等を要請している。本要請においては下記２点の対策が参考事例として挙げられているが、各金融機関等はこれに限らず他の金融機関等や業界団体等と連携し、対策を不断に高度化していくことが期待される。

対策事例の１点目は、振込名義変更（異名義）による暗号資産交換業者への送金 停止等である。金融庁にてモニタリングを行った金融機関では、既にインターネットバンキングにおける振込名義変更による暗号資産交換業者への送金をシステムで検知し、自動で事前停止しているなどの取組が多く見受けられた。対策事例の２点目は、暗号資産交換業者への不正な送金への監視強化である。前述したフィッシング対策や、後述する口座の不正利用対策の内容の中には、暗号資 産交換業者宛ての不正送金の監視にも有益となる取組が含まれている。また、下記のような暗号資産交換業者に特化した検知の仕組みや不正利用実態の調査・分析などが含まれる。

・暗号資産交換業者宛ての送金の中でも、特にリスクが高いと判断された取引やその取引に関連した個人及び法人に対する深堀調査、必要に応じてインターネットバンキングの利用制限を実施
・ネットワーク分析を行い、不正利用の疑いが強い口座名義人に関連する個人・法人を特定して、組織的犯罪集団の疑いがあるケースとして深堀調査を実施

２．預貯金口座の不正利用対策等

（１）預貯金口座の不正利用の特徴と対策

近年、特殊詐欺の被害やフィッシング被害が増加しており預貯金口座の不正利 用件数も増加傾向にある。金融庁は、口座の不正利用対策に関して金融機関等に対する継続的なモニタリングを行っており、以下の傾向を把握した。

・非対面にて開設された口座は対面で開設された口座よりも不正利用されやすい。

・新規に開設された口座（開設後約１年未満の口座）は既存の口座よりも不正利用されやすい。

以下では、口座の不正利用対策として先進的な取組を紹介する。なお、こうした先進的な取組を行っている金融機関等の多くにおいて口座の自主凍結の件数が、警察等からの凍結要請の件数を上回っていた。

【検知及び検知後対応の即時性（リアルタイムモニタリング）】

・24 時間体制で、送金等個別取引の自動保留、自動謝絶や速やかな口座の凍結対応等を実施

【預貯金口座凍結の判断基準の精緻化・明文化】

・属人的な判断能力やノウハウに頼ることなく口座凍結の判断基準を明確に設定し、規程やマニュアル等にて明文化

【取引モニタリングシナリオや預貯金口座の凍結の判断基準の機動的な見直し】

・口座の売買・譲渡や収納代行などに見られる特有の挙動・振舞いに着目し、きめ細やかなモニタリングシナリオを設定

・不正利用の検知基準向上のため、日々の業務の中で把握した傾向等を、数日以内に既存のモニタリングシナリオや判断基準に反映

・モニタリングシナリオや判断基準の見直しを、月次以上の頻度で実施。加えて、定期的にシナリオや敷居値の有効性を検証

金融庁は、これまでのモニタリングを通じて、相対的に対策が劣る金融機関等では 口座の不正利用が増加する傾向を把握している。他方で、口座凍結に積極的に取り組む金融機関等では不正利用が抑止・減少する傾向にある。 各金融機関等は、積極的・機動的な情報交換を行うとともに、他の金融機関等の取組を参考にしつつ、自らの口座不正利用対策に劣っている点がないか、また、改善・高度化の余地がないか、感度を高く保つことが重要である。

（２）法人名義の預貯金口座の悪用への対応

法人名義の預貯金口座は、一般的に個人名義の口座と比較して、振込限度額が高額あるいは上限設定がない場合が多く、例えば、短期間で多頻度の入出金が繰り返される場合であっても、通常の商取引に係る決済・送金と不正な入出金とを明確に区別をすることは、金融機関等にとって困難な場合が多くみられる。また、金融機関等が正規に利用されている法人名義の口座を誤って口座凍結・取引停止した場合、当該法人の事業運営及び継続、資金繰り等に多大な影響を与えるおそれがあることについて、金融機関等としては、不正利用が疑われる場合であっても法人名義の口座への対応には慎重になる傾向がある。

これらの特徴を含め、詐欺等のために口座の不正利用を企図する者にとっては、法人名義の口座の買入れ・譲受けを志向するものと考えられる。各金融機関等における法人名義の口座の取引モニタリングに当たっては、インター ネットバンキングの接続場所や端末、申告された事業の特性と入出金との整合性等、通常の商取引に係る取引とは異なる取引を

検知するため、これまで以上に法人顧客について、リスクに応じた適切な顧客理解を深めることが期待される。

３．偽造本人確認書類を用いた預貯金口座開設への対応

特殊詐欺や ＳＮＳ型投資詐欺・ロマンス詐欺など預貯金口座への振込みにより他人の金銭を詐取する類いの犯罪において、架空・他人名義の口座が振込先として悪用されている例が多数みられる。 このように不正に利用される振込先口座には、本人確認書類（運転免許証等）の偽造等により不正に開設されたものもある。インターネット上には、偽造本人確認書類の販売や本人確認書類の偽造等の請負に関するウェブサイトが存在し、精巧な偽造書類を比較的容易に入手することが可能となっている。そのため、金融機関等にとって、本人確認書類の偽造等への対応を始め、不正な手段による口座開設への対策は急務である。特に、顧客と対面することなく口座開設を受け付ける場合には、本人確認書類自体の手触りや質感等を確認することができず、偽造等を看破することが困難であることから、本人特定事項の確認方法の特性に応じた対応を検討する必要がある。後述の「国民を詐欺から守るための総合対策」では、口座の不正利用防止対策の強化等として、非対面、対面ともに公的個人認証による本人確認を行うこととしている。なお、本人確認書類の偽造等を識別するために金融機関等では、以下のような対策が講じられている。

・本人確認書類の偽造に関し、手口等の特徴を分析して審査に活用
・偽造本人確認書類の識別能力を向上するためシステム化を推進
・口座開設数の増加に応じ、行内のリソース確保や業務委託先との連携を含め、適切な審査体制を整備

また、本人確認書類の偽造等に対し高い耐性を持つと考えられる本人確認方法としては、犯収法施行規則第６条第１項第１号ヘ・ト・チに規定する本人確認書類のＩＣチップに記録された情報の送信を受ける方法のほか、同号ワに規定する公的個人認証サービスを利用する方法があり、今後、一層の利用拡大が期待される。また、対面での本人確認においても、本人確認書類の提示に加え、ＩＣチップ情報の確認を行うことも偽造本人確認書類を見分ける上で効果的である。

４．国民を詐欺から守るための総合対策

一層複雑化・巧妙化する詐欺等について、その変化のスピードに立ち後れることなく対処し、国民をその被害から守るためには、官民一体となって、一層強力な対策を 迅速かつ的確に講ずることが不可欠である。 そこで、今般、「オレオレ詐欺等対策プラン」及び「ＳＮＳで実行犯を募集する手口に よる強盗や特殊詐欺事案に関する緊急対策プラン」を発展的に解消させ、特殊詐欺、ＳＮＳ型投資・ロマンス詐欺及びフィッシングを対象に、政府が総力を挙げて取り組む 施策をまとめ、2024 年６月、犯罪対策閣僚会議において、「国民を詐欺から守るための総合対策」が策定された。

以上