特別寄稿

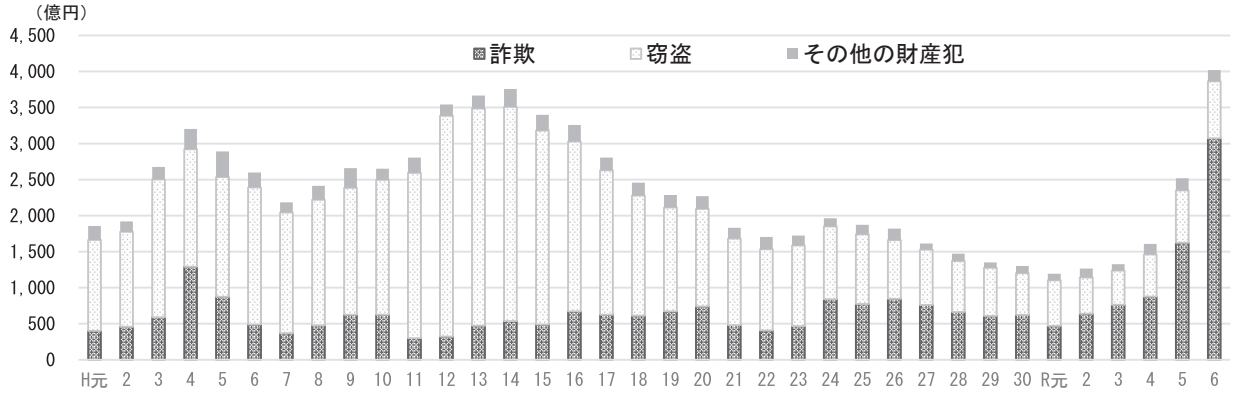
金融庁における金融犯罪対策に関する最近の取組みと留意点

金融庁　総合政策局　リスク分析総括課　金融犯罪対策室長　**齋藤　豊**

【はじめに】

24 年における刑法上の財産犯の被害額は 4,000 億円を超える中、特に詐欺被害が急増しており、同年中の詐欺の被害額は 3,000 億円を上回った。そして、詐欺の手法も従来の対面型から、インターネットやSNS、携帯電話などをはじめとする非対面型に中心が移りつつあり、最近、特に詐欺の中でも被害額が増加しているのが特殊詐欺・SNS 型投資詐欺・SNS 型ロマンス詐欺の三類型である。

（図 1. 財産犯の被害額の推移）



（出所　警察庁）

それぞれについて簡単に説明すると、まず特殊詐欺は、家族等を名乗って電話をかけ、資金が必要になったなどの理由で振り込ませる「オレオレ詐欺」や役所の職員等を名乗って「税金が戻ってきます」と言って手数料等の名目で振り込ませる「還付金詐欺」、利用してもいない出会い系サイト等の利用料を請求する「架空料金請求詐欺」など、色々なパターンがある。これらを一言で言えば、非対面で連絡を取り、振込などによって金銭等をだまし取る詐欺、ということになる。特殊詐欺では、従来から 70 歳以上の高齢者が被害者となるケースが多かった。

次に SNS 型投資詐欺は、「投資のプロがアドバイスします」「絶対に儲かる非公開の投資案件があります」など SNS 上に偽の広告を出すなどして、架空の投資話に投資させて金銭等をだまし取る詐欺のことである。

最後に SNS 型ロマンス詐欺は、SNS のメッセンジャーなどを使って、何度もやりとりをしていく中

で、相手に恋愛感情を芽生えさせたところで、「あなたに会いたい」「会いに行くためには交通費が必要」などの名目で振り込ませて金銭等をだまし取る詐欺のことである。

こうしたSNS型投資詐欺やSNS型ロマンス詐欺は、特殊詐欺とは傾向が異なり、被害者が40歳～60歳に多い特徴がある。特にSNS型投資詐欺では20歳～30歳の被害者も少なからず存在している。もはや、詐欺被害は高齢者だけの問題ではなくなりつつある。

またSNS型投資詐欺やSNS型ロマンス詐欺では、もう一つの特徴として、被害者が詐欺師のことを信じ切っている、あるいは薄々は疑問に思いながらもだまされている事実を受け入れがたいために、周囲にも相談することなく、銀行員や警察官などが説得しても耳を貸さない、という難しさがある。このため、特殊詐欺と比べても事案の発覚が遅れ、被害が高額化しやすい傾向がある。

24年は、こうした特殊詐欺・SNS型投資詐欺・SNS型ロマンス詐欺の被害が急増し、被害額はこれら三つの類型の合計で2,000億円にも及び、単年としては過去最大の被害総額となった[1]。こうした被害の増加を背景として、24年6月には、政府全体で「国民を詐欺から守るための総合対策」を策定、そして25年4月には「総合対策2.0」に改訂を行い、様々な被害の未然防止・拡大防止に向けた対策を講じてきた[2]。

（図2. 特殊詐欺等への対策（金融関連））

「国民を詐欺から守るための総合対策（24年6月）」 金融関連の主な取組

- ✓ 金融庁の相談体制の強化・整備
- ✓ 無登録事業者による広告掲載が違法な金融商品取引業に該当し得ることの明確化
- ✓ 事業者団体等による偽広告等への適切な対応の推進
- ✓ **金融機関における検知能力の強化・口座不正利用の防止措置・警察への情報共有の推進**
- ✓ **業界横断的な広報活動の推進**

「国民を詐欺から守るための総合対策2.0（25年4月）」 金融関連の主な取組

Ⅰ 金融機関において**インターネットバンキング**の申込みがあった際の審査の強化や注意喚起、初期利用限度額の適切な設定、利用限度額引上げ時の確認の徹底を依頼

Ⅱ **預金取扱金融機関間で情報を共有**しつつ、不正取引を検知し速やかに口座凍結を行うことが可能となる枠組みを創設

Ⅲ 金融機関・警察で**「架空名義口座」**を管理し、犯罪者の手に渡らせ、その利用状況を把握することで、被疑者の検挙、収益の剥奪が可能（警察庁）

詐欺への対策は大きく三つに分けられる。一つ目は被害者がどうすれば被害に遭わずに済むのか、という「被害に遭わせないための対策」である。二つ目は犯罪者がどのようにすれば犯行を行うことができなくなるのか、という「犯罪者のツールを奪うための対策」である。そして三つ目は金融機関だけでなく、利用者側にも詐欺に対する意識と注意を払ってもらって、社会全体で詐欺にだまされる人を減らしていく、あるいは金融機関が取り組んでいる対策を知ってもらって、利用者にも協力を求めていく、という「利用者向けの周知・広報の強化」である。この三つの対策のうち、どれをやればいいか、というものではなく、特効薬がない以上は、いずれもしっかり取り組んでいくことで、どこかで被害発生・被害拡大を食い止めることができれば、と考えている。本稿では、このうち、特に金融庁として足下で力を

[1] https://www.npa.go.jp/publications/statistics/sousa/sagi.html
[2] https://www.kantei.go.jp/jp/singi/hanzai/index.html

入れて取り組んでいるいくつかの施策について説明をしていく。

詐欺対策について具体的に論じる前に、まず導入的な話として詐欺等の被害金、犯罪資金がどのように流れているのかについて説明する。大別すれば、被害者自身がATM等から出金して、「受け子」と呼ばれる犯罪者に手渡しするパターンや、被害者が犯罪者側の口座に窓口・インターネットバンキング・ATMから振り込むパターンが存在する。中でもインターネットバンキング経由の振込が足下で急速に増加をしていて、全体の大半を占めるまでになっている。

こうした犯罪者側の口座、すなわち不正利用口座から、資金が移転するのもまたいくつかのパターンがある。一つ目は暗号資産を購入して、プライベートなウォレットに暗号資産を移し、規制の緩い海外に持ち出して現金化するパターンである。この場合、暗号資産は価格が変動するリスクがあることから、犯罪者がそのまま持ち続けることはなく、売却して現金化するか、あるいは価格変動リスクのないステーブルコインに転換して保有することが一般的である。

二つ目が更に他の不正利用口座に送金するパターンである。一口に不正利用口座といっても様々な用途がある。例えば、被害者からの申し出によって凍結されるリスクの高い被害金の受け皿口座は、比較的容易に調達が可能な個人口座が使われる一方で、多額の入出金が可能で金融機関も凍結に及び腰な法人口座はそれらからの資金集約用、といった用途が一般的である。

三つ目が海外送金等を取扱っている資金移動業者を経由して、他の不正利用口座に送金される、あるいは暗号資産購入代金の送金を行うパターンである。

これらの資金の流れの中で、犯罪者に不正に利用される口座には大きく二つの種類があり、一つ目は偽造身分証により開設される口座である。これは、後ほど改めて説明するが、本人確認資料のICチップ情報を読み取ることにより今後は防止できると考える。

二つ目は正規の身分証により開設されるものの、それが犯罪者に違法に売却・貸与される口座である。こうした口座譲渡を目的とした開設への対策としては、これも後ほど詳述するが、現在、全国銀行協会において検討が進められている不正利用口座の名義人情報の共有や、使いまわしされている電話番号やメールアドレスではないか検知することが有効である。

また、口座譲渡が行われたことを適時に検知するためには、利用する端末の変更などアクセス環境の変化や、電話番号・メールアドレスなど顧客情報の変更、そして、振込限度額の高額な変更に着目することが有効である。

最終的に、譲渡された口座を不正取引に使用する際には、犯罪者はその口座が使えるかどうか動作確認をする特有の挙動（予兆取引）があるため、それらを検知することも有効である。例えば、試しに少額を入金して、それがすぐに出金できるかどうか確認することで、口座が凍結されていないか確認するような手口も出てきており、こうした挙動を検知することも有効である。

このように、不正取引が行われるまでの各段階で様々な対策が考えられることから、可能な限り多くの対策を講じることで、少しでも多くの不正取引をどこかで止めることが重要と考えている。

【本人確認の厳格化】

25年6月に犯罪収益移転防止法施行規則が改正され、非対面取引については、本人確認方法が運転免許証等を撮影・送信する方式（e-KYC）が廃止となり、ICチップ情報の読取方式に一本化されることとなった[3]。本物と見分けのつかない精巧な偽造身分証が出回っていることが対策の背景にあるが、非対面取引だけでなく、対面取引についても25年12月よりパブリックコメントに付されているように同様の方向で検討がなされており、遅かれ早かれ対応が必要になる。

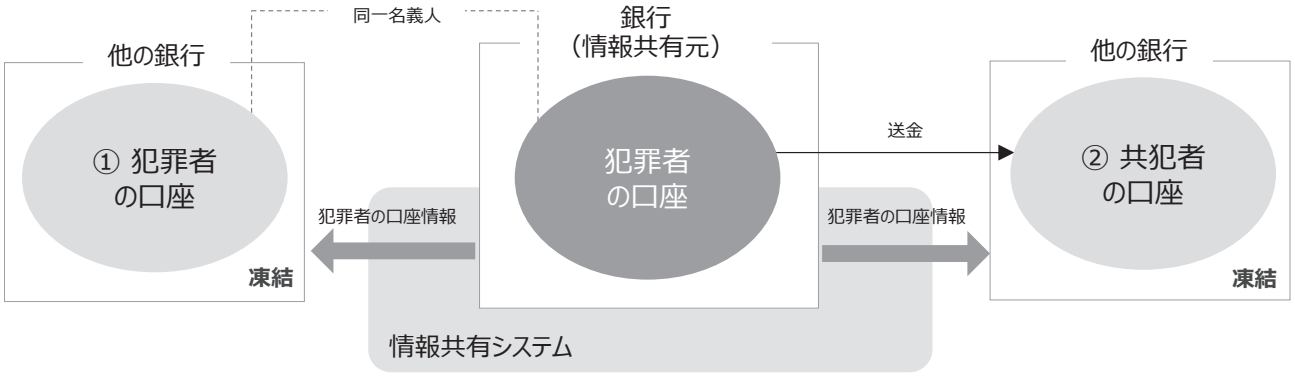
ICチップ情報の読取方式を全面的に導入した金融機関からは、偽造身分証による口座開設はなく

[3] https://www.npa.go.jp/sosikihanzai/jafic/hourei/hotop.htm

なったといった話も聞く。対策の効果は大きいことから、金融庁としても、施行期日である 27 年 4 月を待つことなく早めの対応を金融機関には要請している。

【金融機関間での不正口座情報の共有】

（図 3. 金融機関間での不正口座情報の共有イメージ）



金融機関間での不正口座情報の共有の仕組みがどのようなものかを単純化して示したのがこの図である。まず、中央にある銀行が取引をモニタリングしている中で不審な動きをする口座を検知し、自主的に口座を凍結する。この凍結した口座の情報を他行にも共有する仕組みなのだが、まず中央の凍結口座から送金が行われている右側の銀行の口座は、詐欺等の被害金が流れている先であり、共犯者の可能性が高い、ということでこの口座も凍結する。また、左側の銀行の口座は、資金の流れがなくても中央の口座と同一名義人の口座であり、同じ犯罪者の可能性が高い、ということでこれも凍結する。

こうした形で、一つの凍結口座を起点として、関連する他の口座も凍結し、犯罪者が悪用する口座を潰していくこと、口座の中に残っている残高を被害者の被害回復に充てていくことがその狙いである。

もちろん課題もいくつもある。個人情報保護法上の問題、守秘義務や訴訟リスクとの関係、情報共有を行うシステムの要件・コストなど様々な論点について全国銀行協会の下でこれまで整理してきた[4]。いくつかの金融機関で試行的に情報共有しつつ、実際に口座を凍結するための具体的な業務フロー・業務プロセスや情報共有を行うために必要なシステム機能の検討を進めてきたところであり、システム供用開始に向けて着実に準備を進めていく。まずは、銀行を対象に供用を開始するが、いずれは協同組織金融機関にも対象を広げていく前提である。

【インターネットバンキングの対策強化】

特殊詐欺等では、被害金の受け皿として口座が犯罪者に広く用いられている実態も踏まえ、24 年 8 月には金融庁と警察庁の連名で口座不正利用対策の強化に関する要請文を全ての預金取扱金融機関を対象として発出した[5]。

そして、今や特殊詐欺等において、被害者が被害金を振り込まされる多くがインターネットバンキングによる振り込みであって、もはや ATM や窓口での振り込みの方が少数派になりつつある。また、最近の事例では、インターネットバンキングの利用申請から、限度額の引上げ、多額の送金までの一連の手続きを多くのケースで被害者がだまされて自身の手で行っている。本人自らがやっているわけなのだから、生体認証をはじめとする厳格な本人認証だけ

[4] https://www.zenginkyo.or.jp/news/2025/n033101/
[5] https://www.fsa.go.jp/news/r6/ginkou/20240823/20240823.html

では被害は止められない。

こうした状況も踏まえて、25 年 9 月には新たにインターネットバンキングの強化策を追加する形で要請文を発出した[6]。具体的にはインターネットバンキングの利用開始時における顧客への注意喚起・確認や利用開始後の取引のモニタリング、初期利用限度額が過度に高額とならないような適切な額での設定、顧客が利用限度額を引き上げようとした場合の確認や引き上げ後の取引モニタリングなどを求めている。

犯罪者からすれば対策の弱い金融機関ほど使い勝手が良く、インターネットや金融機関間のネットワークを通じて全国どこからでもアクセス可能である以上、口座の不正利用はどの金融機関でも起きうることであり、これらの要請内容は規模・立地によらず対策が必要である。そして、システム上の対応が必要であり、実施までに時間を要する対策もあることから、計画的・着実に取り組んでいく必要がある。このため金融庁が要請した内容を各金融機関がどの程度実施しているか、アンケートを発出して継続的にフォローアップすることとしている。

このアンケートでは、各質問項目において難易度の高い対策から、低い対策まで様々並んでいるが、いずれも国内の金融機関のどこかで実際に実施されている対策である。少なくとも、どの金融機関でも難易度の低い対策はとり急ぎ対応してもらいたいが、それに甘んじることなく、ぜひ難易度の高い対策も目指していただきたい。そして、言わずもがなではあるが、一定以上の顧客基盤を有する金融機関では、何か起きた場合の影響度を踏まえれば難易度の高い対策も最初から求められる。

このように金融庁としての期待と意図があえて透けて見える質問項目・アンケート構成にしたのは、「犯罪者は対策の弱い金融機関に流れる」という厳然とした事実がある以上、そこから目を背けることなく、他の金融機関と比べて自分たちはどうなのか、この程度の対策で大丈夫なのかを冷静に自問自答していただきたいという思いが背景にある。そして、検討中のまま進展がなく、立ち止まっている金融機関があるとすれば、なぜ対策が進まないのかを経営陣自らよく振り返っていただきたい。経営課題としての優先順位や顧客の安心・安全に対する感度の問題なのか、人員・コストの配分の問題なのか、「他行が被害に遭っても自分たちだけは大丈夫なはず」という楽観的観測なのか、いずれにせよ、往々にしてその原因は経営陣自身にあることが多いように感じている。

【業界横断的な広報】

これまで、主要行・地銀・信金・信組・労金など各業態がそれぞれ別々に実施していた広報を一本にとりまとめ、そこに金融庁・警察庁も参画する形で官民一体での広報を昨年から開始している。昨年は、マネロン対策の一環で顧客情報の最新化のために顧客に送付しているハガキやインターネットでの回答率を高めるために、落語仕立ての広告を様々なメディアで配信した。

そして、足下では、詐欺被害金の受け皿として、売買・貸出された口座が悪用されており、口座が数万円程度でインターネット・SNS 上で取引されていることもあって、小遣い稼ぎの感覚で軽い気持ちで口座売買・貸出に応じる者がいる。特に最近では、銀行口座と暗号資産や資金移動のアカウントをセットで高額で買い取るケースも確認されている。もちろん、口座売買・貸出はれっきとした犯罪であるが、摘発されたケースでは、犯罪であることの認識が薄い者も少なからずいることから、「口座売買・貸出は犯罪である」ことをまずは利用者にしっかりと知らしめる必要がある。それにとどまらず、そうした行為を発見した場合には、警察への通報や新規口座開設の拒否など金融機関としても厳しく対処していく方針を明確に理解させることが重要である。こうした警鐘を鳴らすことが、軽い気持ちで口座売買・貸出に手を染めようとしている者を思い止まらせることにもつながると考えている。若年層を含めて広くメッセージが届くよう、デジタル媒体を中心にこうした内容を利用者に訴えかけるショートドラマ仕立ての広告を 25 年 12 月より開始している[7]。

[6] https://www.fsa.go.jp/news/r7/sonota/20250912/20250912.html
[7] https://www.fsa.go.jp/news/r7/ginkou/20251128/20251128.html

【金融機関と警察との連携強化】

24年8月に発出した口座不正利用対策の要請文の中でも対応を求めていた「都道府県警察との連携」に関して、ほとんどの地域において、金融機関と警察との連携協定が締結された。

その中では警察に被害届が出された振込先の口座、すなわち詐欺被害金の受け皿口座の情報を迅速に金融機関に共有するための取組み、埼玉県が発祥のためその名がついた「埼玉モデル」が各地で広がりを見せつつある。また、全国展開している大手銀行・ネット銀行では取引モニタリングで不審な取引を積極的に検知している先も多く、こうした検知した取引を警察に提供することで、潜在的な被害者への注意喚起や捜査への活用を目指す動きが広がっている。

【オンラインカジノへの対応】

オンラインカジノは当然のことながら我が国において日本人が利用することは賭博・違法行為であり、これまでにもスポーツ選手や芸能人の摘発が頻繁に報道されてきたように、国内で社会問題化している。警察庁が公表している調査結果でも若年層を中心に一定数のユーザーがいるとみられており、そのうち半数近くは違法性の認識を持っていないとされている[8]。

特殊詐欺等では、だます側の「犯罪者」とだまされる側の「被害者」の両方が存在し、「被害者」をこれ以上生んではいけない、被害を食い止めなければならない、という理屈はよく理解いただけると思う。他方で、オンラインカジノでは、違法な賭博を取り仕切る胴元や賭け金の送金に関与する者は当然のことながら、賭博に手を出すユーザーも含めて全員が「犯罪者」であり「被害者」が存在しないため、特殊詐欺等と同列で対策の必要性を論じることに違和感がある、という声も聞かれる。

他方で、こうしたオンラインカジノの送金ネットワークには、犯罪組織が加担しているケースもあり、そこで得た手数料や報酬がこれらの収益源となっている。オンラインカジノでの収益を元手に犯罪組織が拡大し、新たな犯罪とその被害者を生む。この負の連鎖は断つ必要がある。

オンラインカジノを利用する場合、様々な方法があるとされているが、海外のオンラインカジノ、つまり胴元自体は日本国内に入金用口座を持っているわけではなく、ユーザーはオンラインカジノの指示する法人・個人口座に振り込み、そこから様々な口座を転々とさせることで、警察による捜査の目をくらませようとする。こうした中で、オンラインカジノ対策に先進的な金融機関は、警察から要請されるまでもなく、取引モニタリングにより、まずオンラインカジノへの送金に関与する口座を特定し、自主的・積極的に凍結を行っている。そして、この凍結口座に送金していた者はオンラインカジノユーザーとして同様に凍結を行っている。

こうした先進的な金融機関での取組みも踏まえ、金融庁からは預金取扱金融機関・資金移動・暗号資産の三つの業態に対して、25年5月に要請文を発出した[9]。要請文では三点の対応を求めているが、最も重要なのが「オンラインカジノが違法であることの利用者向け注意喚起」である。前述のとおり、オンラインカジノユーザーの中には、犯罪という意識がない、あるいは多少は罪の意識がありつつも軽く捉えているケースも多い。こうした利用者に対して、「オンラインカジノは犯罪である」ということに加えて、「オンラインカジノの利用を確認した場合は、金融機関としても口座凍結を行う、新規口座開設を拒否するなど厳格に対処する」といったことをしっかりと伝えていくことが、対策の出発点になると考えている。

また、取引モニタリングでどうやって送金に関与している口座やオンラインカジノユーザーを特定するかであるが、実際に止めている銀行では、「多数の個人からの小口の送金があって、賭け金の入金がどのユーザーからのものかオンラインカジノ側で特定するために、振込依頼人名の前後に会員番号とおぼしき英数字が付加されている」「同一の端末から複数のユーザーのインターネットバンキングにログインが行われるという不自然な状況が生じている」など、

[8] https://www.npa.go.jp/bureau/safetylife/hoan/onlinecasino/onlinecasino.html
[9] https://www.fsa.go.jp/news/r6/sonota/20250515/20250515.html

取引の様々な特徴に着目している。こうした実務上の知見を金融機関に共有するために、金融庁では「疑わしい取引の届け出 事例集」を 25 年 8 月に更新している[10]。この更新にあたっては、オンラインカジノだけでなく、Web ブラウザを介したなりすまし、ボットによる自動入力など、非対面取引での不正利用事案を中心に全般にわたって事例を追加している。

但し、こうした着眼点はいずれも一時点のものであり、金融機関が対策を講じることで、犯罪者側も新たな手口を模索・実行する傾向がある。終わりのない戦いと言ってしまえばその通りではあるのだが、オンラインカジノだけでなく金融犯罪対策の全てに通ずる話として、犯罪者の視点でどういった行動を取るか想像力を働かせながら絶えず注意深くモニタリングすることが重要であり、もし取引の不自然さや違和感を覚えたのであれば、そのままにせず詳細な調査を行った上で、口座凍結など必要な対応を迅速に講じるべきである。

【おわりに】

特殊詐欺等の金融犯罪に接している金融機関の現場の方々の努力・苦労は私も目の当たりにしてきており、本当に頭が下がる思いである。それを承知の上で、あえて申し上げるが、犯罪者は新たな犯罪の手口・資金移転の方法を常に考えていて、それができる場所を常に探している。このような犯罪環境の変化に追随していくためには、金融機関も現状に甘んじることなく、高度化を図っていく必要がある。

更に言えば、自身の金融機関で被害が出る、不正送金に悪用される、そうしたリスクが顕在化してから後追い的に対処するのは、風評リスクや被害を受けた顧客への対応なども重なって、莫大なコストと労力が生じる。そうではなく、他の業態・他の金融機関での事例なども踏まえて、リスクの感度を高く持ち、「いずれ自分たちも狙われるかもしれない」という気持ちを持って、常に「備えておくこと」が大事である。

（以　上）

[10] https://www.fsa.go.jp/str/jirei/index.html