特集

総仕上げのマネロン対策

疑わしい取引検知のカギは顧客行動の「不自然さ」の把握

あえて攻撃者の立場になって不正利用の手口を考えることが重要

金融機関における「疑わしい取引」が後を絶たない。金融犯罪対策担当者がこれらを早期に発見し、被害を極小化するためには、攻撃者の立場で「仮説を立てること」が重要だ。また、疑わしい取引を検証して、細部に現れる攻撃者の「不自然さ」を捉えることもカギとなる。金融機関の経営者は、実効性ある金融犯罪対策のためシステムと人材面の充実を図る必要がある。

アクシオン
代表　安田　貴紀

SNSで容易に見つかる「口座売買サイト」

現代の日本社会は、金融サービスの利用者が金融犯罪に巻き込まれやすい状況にある。インターネット上では普通に不正口座作成のための勧誘行為が行われ、口座売買といった不正取引のサイトも存在するなど、金融犯罪が身近にある大きな社会課題であることは間違いない。

例えば、銀行口座の売買については、全国銀行協会のホームページで「インターネットやダイレクトメールで銀行の口座の売買を持ちかけ、報酬と引き換えに連絡してきた者へ口座情報の提供をする」など、具体的な犯罪手口の例が示されている。また、SNSを介して「口座買い取りサイト」に容易にたどり着くことができる。サイトには銀行口座の開設申し込みに誘導するリンクが設定され、口座の買い取り価格も掲示されている。

口座売買は犯罪であり、売る側も罪に問われる。一見して怪しく見えない巧妙なサイトがインターネットの検索ですぐに表示されてしまうことを考えると、多くの人々がまったく意図せず、口座売買に関わってしまうリスクにさらされているといえる。

一方、金融機関の金融犯罪対策担当者にとって、こうしたネ

ット上の情報には「疑わしい取引の検知」に役立つ情報が多くある。例えば、口座売買のサイトでは、「1日の振込限度額200万円以上」「入出金200万円」などの文言が掲載されている。これらは、オンラインで犯罪を行う「攻撃者」が求める銀行口座の条件といえるだろう。担当者はこうした情報を上手に生かして、金融犯罪対策における不正検知のための施策を考えるのも一つの方法である。

攻撃者の立場で不正利用を考える

金融サービスにおいて、攻撃者による不正利用と思われる「疑わしい取引」は後を絶たない。例えば、架空名義による銀行や証券の不正口座開設、クレジットカードのなりすまし入会、第三者による不正入会といった取引は年々、巧妙化している。金融犯罪対策担当者がこれらを早期に発見し、被害を極小化するためには、「仮説を立てること」が必要である。

そのためには自社サービスに限らず、まずは自分がよく利用しているサービスで不正利用を考えてみるのがよいだろう。攻撃者がどのように不正利用を仕掛けるのか、どのタイミングで何を詐取するのか、サービスを利用している誰をだますのか――これらを「攻撃者の立場で」想像するとよい。金融犯罪対策担当者の立場で考えると、先入観にとらわれて、過去に経験したこと以外、あまり思い浮かんでこないことがあるためだ。また、目の前で起きている事案にだけ対応するあまり、自社サービスの全容を把握できなくなってしまうケースもある。

実際の攻撃者は手口を教えてはくれない。攻撃をした真の目的も分からない。金融犯罪対策担当者は、実際に起きた出来事について、さまざまな角度から調査して、一つひとつの痕跡を見つけ出していくことになる。その際、仮説を立てて検証し、以後、攻撃者によるアタックの兆候をいかに早期に捉えることができるかがポイントとなる。

疑わしい取引検知のカギは、細部に表れる攻撃者の「不自然さ」を捉えることである。何が不自然なのかは自社サービスの内容によるが、不自然さを見極めるための手触り感を持っておく必要がある。そのためには、前述したように、いかに先入観を取り除いて攻撃者の考えを想像できるかが肝要となる。

実は、不自然さを見極める能力は、ある程度のトレーニングで身に付けられる。例えば、普段から自分自身や周りの同僚、友人の行動を冷静に捉えることで、そのコツをつかむことができる。

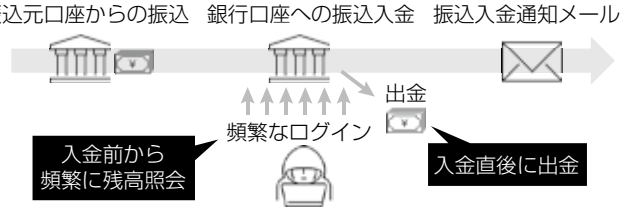
不正利用が疑われる不自然な行動パターン

銀行口座のモニタリングにおける不自然さの事例を二つ紹介したい。

近年、多くの金融機関では、預金者に対して給与等が振り込まれるとメールで通知してくれるサービスを導入している。こうしたサービスにおいて、顧客行動パターンは、メールを受信

〔図表〕　インターネットバンキング利用時における不自然さ

- インターネットバンキングで残高照会の連打
- メール通知前にもかかわず、頻繁にログインを繰り返す



（出所）　筆者作成

した後から出金や残高照会を行うのが一般的だ。一方、口座が不正利用されている場合、攻撃者は被害者から振り込まれるタイミングを事前に把握しているため、実際に入金される前からインターネットバンキングにログインし、残高照会を頻繁（連打）に行う様子が見られる（図表）。メールの通知に関係なくお金を引き出そうとしているわけだ。このように一般的な顧客の行動と比較することで、「残高照会をするタイミングや頻度」において、攻撃者の不自然さが見えてくる。

属性変更手続きのタイミングでも、不自然さを見ることができる。預金者が転居や機種変更に伴って電話番号の変更手続きを行うことは、よくある行動である。一方で、口座開設時に申請した電話番号を、キャッシュカード受領直後に別の番号に変更して利用開始することは、めったにない行動だ。キャッシュカードの所有者を本来の預金者から攻撃者に変え、元の所有者へ銀行からの電話をつながらなくするために行われている可能性があり、口座売買の疑いがある。

このように「手続きが行われるタイミング」に着目すると、不自然さが見えてくる。自社サービスにおいて不正対策のカギとなる攻撃者の不自然さが顕在化する場所と、それがどのような内容なのかをあらためて考える必要がある。

なお、疑わしい取引とみられる行動があるか否かは、サービスの内容や顧客ごとの取引内容、頻度、属性等によっても異なる。「特定の取引が何回以上あれば、一律で疑わしい取引である」とは断定できない。

ただし、金融庁が公表する「疑わしい取引の参考事例」には、預金取扱金融機関だけでなく保険会社や金融商品取引業者など、各業態で発生している不正の手口などが記載されており、疑わしい取引に該当する水準が確認できる。他業態のさまざまな事例は、不自然さを見極める際の「手触り感」を持つ上で参考となる。記載内容によっては、他業態の事例の方が役立つものも多い。担当者はあらためて確認するのがよいだろう。

犯罪の未然防止にはシステムと人材が必須

金融犯罪の未然防止に向けた施策は年々、具体的になり、その実効性が重視されるようになっている。実効性を向上させていくには、まずはすぐにできることから開始し、常にＰＤＣＡを回していくことが重要だ。攻撃手口など犯罪を取り巻く環境が大きく変化した際には、これまで確立していた対策を速やかに見直すことが求められる。

攻撃者の手口の変化は速く、時には「顧客になりすましてコールセンターに電話をかけてくる」といった大胆な行動を仕掛けてくる。従来の対策の延長線上で未然に防止できないことが増えていけば、後手の対応に終始してしまう。そうなれば人海戦術や属人的なオペレーションに陥ってしまい、結果として、人件費の増加や予期せぬ追加費用の発生等の課題に追われることになる。

こうした犯罪手口の変化に対しては、柔軟に対応できる汎用性の高いシステムを備えておくことが重要だ。金融犯罪の未然防止を強く念頭に置いた実効性のあるシステム準備が、いざという時に大きな効果を発揮するだろう。

人材育成も課題であり、これには「知識」と「スキル」の観点がある。知識の中にも二つの側面があり、規制や事務といった「管理面」と、システムの「技術面」の両方を理解する必要がある。知識はあればあるほど、より具体的かつ効果的なア

イディアを描くことができるため、積極的に情報をインプットしていくことが重要だ。

他方、スキルとしては、コミュニケーション力や社内調整力、仮説力、プレゼンテーションスキル、分かりやすい資料の作成力――といった能力が業務推進の上で大切である。起きている事象を正しく把握し、その状況を経営層や他部署に説明し、関係者を取りまとめて被害を極小化し、未然防止に向けた不正対策を推進する、一連の業務推進が求められるからだ。このスキルを高めるためにも、外部の講演やセミナー等に積極的に参加し、分かりやすい事象の伝え方などを常に情報収集しておくことが大切である。

経営層のコミットや社会貢献意識が重要

金融犯罪対策には、もう一つ大切なことがある。それは金融犯罪対策担当者を含めた金融機関職員一人ひとりの「社会的使命への志」や「社会に役立った」という充足感の醸成である。

対策内容の重点を、被害発生後の対応から被害発生前の未然防止対策にシフトすると、当然ながら不正利用の被害を防げる確率が高まってくる。実際に顧客から被害防止のお礼の電話などを受けることもある。こうした反応があれば、担当者には「社会に役立った」という充足感が生まれる。担当者のやる気が向上し、より志を持って業務に臨んでもらえるようになると、現場には組織としての一体感が生まれ、業務最適化の実現にもつながる。

金融犯罪対策は一度行えば終わりではなく、継続してやり続けていかなければならない。社会的責任を担う企業としては、金融犯罪に対する経営層の認識を高め、全社的に取り組めるような組織体制を構築していくことが望ましい。そのためには金融犯罪の未然防止事例を含めて自社で起きている金融犯罪の状況を、常に経営層に対して情報提供することが担当者に求められる。たとえ未然防止できていても「攻撃がある」ということは、攻撃者に狙われており、注意が必要ということである。

他の企業や他の業界で起きている事案についても、自社で起こる可能性を検証し、それを経営層と共有することで、いつ・どのような事象が発生しても、経営層が迅速に意思決定できるような基盤を整えておきたい。大きな事案が起きた時には、経営層と金融犯罪対策の担当者が密に連携することになる。その時のためのコミュニケーションや知識、認識の共有を日々培っておく必要がある。それが一番大事な局面において強みとなる。

攻撃者は、自社の最も脆弱な部分を狙ってくるため、対策に必要な技術だけではなく、商品性やリスク管理などを含めてさまざまな角度から検討する必要がある。つまり金融機関は、商品・サービスの企画段階から、あらかじめ想定されるリスクを考慮して「金融犯罪対策を織り込んだ商品・サービス」を作らないといけない環境になりつつある。経営層は、いま金融犯罪対策の現場で起きていることをあらためて把握し、リーダーシップを発揮することで、社員の意識改革と企業文化の醸成にもつなげることができるだろう。

やすだ よしき
セブン銀行での商品開発と金融犯罪対策およびサイバーセキュリティー対策（ＣＳＩＲＴ＝Computer Security Incident Response Team）での対応を行った実務経験を有している。19年ＡＣＳｉＯＮ（アクシオン）設立から現職として、本人確認（ｅ－ＫＹＣ）事業、不正検知事業、コンサルティング事業などに従事。フィッシング対策協議会運営委員。