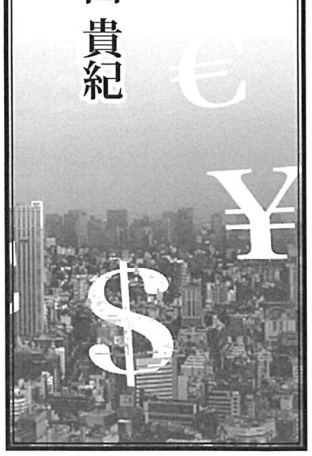
3 サービス理解度の隙を狙った金融犯罪

株式会社ACSiON 代表取締役　安田 貴紀



一　金融犯罪による被害と継続的な対応

警察庁と金融庁の発表によると、2023年上半期のフィッシング詐欺などの手口によるインターネットバンキングでの不正送金被害件数は2322件、被害額はおよそ30億円に上り、過去最悪のペースで増加している。また、口座売買や詐欺に関するニュースが毎日のようにメディアで取りあげられ、実際にフィッシング詐欺のメールやSMSを受信したことがあるという方も周りに増えている。金融犯罪が日常生活の身近で起きていることを実感するようになった。

多くの業界の方々との意見交換を通じて、年々、金融犯罪対策に関する意識は高まっていることを感じる一方、目先の金融犯罪被害を防ぐのみの対策が最優先課題となっている現場担当者も少なくない。その場合、目先の金融犯罪被害への場当たり的な対応はできても、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等予算やリソース面での課題に追われて、多様な金融犯罪事案への継続的な対応が後手になる。金融犯罪による被害を防ぐためには、何らかの対策を導入しただけで完了するのではなく、そこからが始まりで全体としてPDCAを回していくことが重要である。

また、実際の金融犯罪被害が出る前に、自社がどのような被害を受けるかを事前にどこまで想定できているだろうか。金融犯罪による被害とは、攻撃者にとって最終的に金銭的な価値にできるものとなる。他方、自社またはお客様が金融犯罪による被害として失うものは金銭、モノ、情報そして信頼など企業自体の資産に大きく影響を及ぼす。

二　自社サービスを理解することの重要性

金融犯罪対策を行うためには、攻撃者が、いつ、誰に対して、どんな手口で自社サービスへの金融犯罪を仕掛けてくるのかを知らなくてはならない。仮に、普段自分がよく利用するサービスに対し、攻撃者になったつもりで金融犯罪を仕掛けることを想像してみよう。そのサービスの魅力や特徴がわかっていると、初めの申込みの段階と2回目以降の利用の段階とどちらが仕掛けやすいか、誰をターゲットにしやすいか、何の情報を詐取できそうか、少し想像すると何となく思い浮かんだのではないだろうか。より細分化していけばもっと詳細な犯罪手口の想定が可能だろう。一方で、金融犯罪対策担当者に自社サービスについて同じ質問をすると、先入観にとらわれて過去に自らが対応を経験した金融犯罪手口やガイドライン等に記載された内容以外は、あまり思い浮かんでこないことが多い。目

の前で起きている事象にだけ対応しているあまり、自社サービスの商品性など全容を理解できていないこともある。

実際、攻撃者は銀行を騙ったフィッシングサイトで情報を詐取し、インターネットバンキングで不正送金の振込みを実行する。その際、真の目的はわからないものの、攻撃者がとった詳しい犯行手口を様々な角度から検証し、一つひとつの痕跡を見つけ出すことで、犯行手口だけでなく、犯行理由なども含めて自分たちなりに考察することができる。犯行現場において攻撃者が残していった証拠を採取・調査し、犯行状況を明らかにする鑑識のような作業であることから、私はこの綿密な調査を「鑑識」とよんでいる。不正利用を未然に防止するためには、こうした考察を踏まえ、自社サービスの全容を理解したうえで仮説を立てる力を付ける必要がある。仮説を立てて検証し、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である。

三　攻撃者は、サービス内容を深く研究している

攻撃者は、口座名義人がすぐに不正利用に気づいたり、残高の確認をされるのを防ぐために、周到に準備をしている。気づくのを遅らせるために振り込み実行時のメールが届かないようにメールアドレスを変更したり、ログイン時のＩＤやパスワードを変更するなど、これらは不正送金を実行するための準備の手口だ。こうした手口を実行するうえで、必要な情報を違和感なく詐取するために、精巧なフィッシングサイトを用意している。また、パスワードの要件など、精巧なチェックの仕組みを用意し、エラーを出して再度の入力を促し確実に情報を詐取しようとする。そして詐取した情報を使って無駄のない操作で不正送金を実行する。これらは攻撃者がサービスの全容を深く理解している証拠である。

また、各社においてマネロン対策における預金取引モニタリングが強化されてきていることから、攻撃者の手口もより巧妙になっている。例えば、確実に不正な引出しを実行できるように口座が使えるか事前にキャッシュカードでの入出金動作の確認をＡＴＭで行う手口がある。しかし、最近では初めての預金取引で金融犯罪を実行しているように思える事案がある。攻撃者は「口座の取引明細に表示される預金取引による動作確認」を行わず、残高照会などの「口座の取引明細に表示されない操作で動作確認」を行っているのである。停止されている口座の場合は、エラーメッセージが表示されるため、それを動作確認の方法としている。これらはサービスごとの作りで異なるが、攻撃者は、事前の調査を惜しまず研究熱心であることに留意しておくことも重要である。

むすびに

社内の金融犯罪対策担当者とそれを利用する顧客の立場では、商品性やサービス内容の認識度の深さに差が生まれることがある。攻撃者はその隙を狙い、さらに金融犯罪対策を各社が行っていることを前提に研究して仕掛けてくる。金融犯罪対策の高度化を進めるために、担当者は、自社のサービスを深く理解し、どのような手口で攻撃される危険性があるのかを把握し、それを上回る事前の対策をすることが必要である。さらに、その攻撃者の振る舞いを検知できる汎用性の高いシステムを加えておくことで不正利用に対して柔軟な対応が可能となる。

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。２０１９年７月の株式会社ＡＣＳｉＯＮ（アクシオン）の設立立上げから現職。ＡＣＳｉＯＮにて本人確認（ｅＫＹＣ）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。