特集

金融犯罪・マネロンを防げ

日進月歩の勢いで巧妙化する金融オンライン犯罪

不正検知プラットフォームで犯罪集団のログイン、マネロンを阻止

近年、フィッシングサイトでID・パスワードを詐取し、銀行口座から預金を盗み出すといった手口が急増している。また、闇サイトなどを通じて口座売買が安易に行われているほか、ツイッターなどを通じた口座の不正開設が増加しており、こうした不正口座を用いたマネー・ローンダリングが広がっている。犯罪集団はセキュリティー対策が弱い金融機関を集中的に狙う。独自で対策を講じることに限界がある金融機関は、外部のセキュリティーベンダーと連携する必要があるだろう。

カウリス
代表　島津　敦好

日本を標的にする犯罪集団の実態

当社カウリスは、不正ログインの検知サービスを提供しており、現在、銀行を中心に証券会社、クレジットカード会社、暗号資産交換業者、通信キャリアなど20社に利用いただいている。

近年、犯罪者がフィッシングサイトを立ち上げ、SMS（携帯電話のショートメール）の一斉配信などによってフィッシングサイトに誘導して、金融機関の口座利用者のID・パスワード（PW）を詐取し、口座から預金を盗み出すといった手口が急増している。2020年にはインターネットに接続されるパソコン・スマートフォンが570億台になると想定されており、オンラインサービスに使われるID・PWが膨大になるため、これを詐取して悪用する「なりすまし」犯罪が確実に増えるだろうと予測されていた。実際、19年に国内金融機関で起きた不正送金は約30億円、クレジットカードの不正利用に至っては236億円に上っている。

昨今のインターネットバンキングを見ると、スマホからのアクセスがパソコンの約2倍にまで増えている。それにもかかわらず、金融機関のセキュリティー対策はいまなおパソコンが中心で、スマホ向けの対策

は遅れている。早急に追加の認証機能を導入するなど、スマホ向けのセキュリティーを強化する必要がある。

当社は、金融機関の口座利用者が自宅のパソコンやスマホなど、どの端末からインターネットバンキングにログインしているかをデータ化し、すべての提携金融機関で共有している。提供している検知サービスの特徴の一つが、当社が発行する端末識別子を利用することで、不正なログインか否かを検知する仕組みだ。具体的には、利用者ごとに、普段ログインしているスマホのOS、ブラウザのバージョン、設定言語、キーボード配列（日本語・英語・絵文字）といった情報を約150項目収集し、本人特定に利用している。その上で、利用者の普段の利用の特徴をもとに、5段階でリスクレベルを設けている。

具体的な不正検知の事例を挙げよう。昨年、ある金融機関でフィッシング被害が多発した際に不正ログインした端末を解析したところ、アクセスしている携帯のOS、かつブラウザの解像度に不自然な点が確認された。この組み合わせはネットバンキング利用者全体のうち相当少ない割合にもかかわらず、不正送金とみられるログイン端末の半数以上がこの組み合わせだった。そのため、金融機関にその組み合わせでのログインがあればブロックし、ログインさせないようにしてもらった。すると、不正アクセスがピタリと止まり、その金融機関のフィッシングサイトさえもなくなった。

他方、この金融機関への不正アクセスができなくなったことで、今度は別の金融機関のフィッシングサイトが一気に立ち上がるようになった。犯罪集団は、防止策が講じられたことが分かると、すぐに別の金融機関を狙う。実際、不正ログインに使われた端末をブラックリスト化して、提携するほかの金融機関と共有すると、同じ端末でアクセスされているケースが非常に多く確認される。

当社のサービスでは、不正なログインを検知すると金融機関に対して0・2秒で通知する。リスクレベルのうち、ハイリスクの「レベル5」に該当すれば、金融機関はその時点でこのログインを遮断する。それ以外にも、「疑わしい取引」に定められているような、日本と国交がない国や地域からのIPアドレスでのログインを遮断したり、金融機関ごとに細かく検知・遮断規則を設けたりしている。

不正ログインを解析すると、口座名義は日本人にもかかわらず、アクセスしてくるスマホ端末のキーボード設定が、一般的な「日本語・英語・絵文字」ではなく、アジア圏の外国語の配列になっているものも散見される。こうした端末もブラックリスト化し、提携する金融機関への不正アクセスを防いでいるが、日本の反社会的勢力だけでなく、さまざまな国の金融犯罪グループが日本の金融機関を標的にしてアクセスしていると想定される。

不正送金に見る季節性や時間帯の特徴

日本の金融機関を標的とする犯罪者の行動には、「季節性」があることが分かっている。年末年始とゴールデンウィーク、お盆休み、シルバーウィークなど、大型連休が多いときに不正ログインが集中している。休暇中の不正送金は利用者や銀行に気付かれづらく、気付いて銀行が対応しようにも連休中は人手が足りず、調査や対応が進まないことを、犯罪集団は分かっているからだ。

事前にID・PWをフィッシングでたくさん盗んでおいて、連休中に不正ログインすることを繰り返している。今年も6月にフィッシングが多かったが、実際に不正送金が多く起きたのは8月のお盆休みだ。

当社では、月間1億3000万件のログインをチェックしており、そのうち犯罪者からの不正ログインと思われる件数は年間平均でおよそ0・3％。だが、大型連休がある1月、4月、8月、9月、12月は、この数字が0・7％に上がる。また、今年は新型コロナウイルス感染拡大の影響から、3月以降に金融機関職員の在宅勤務が増え、

出社が手薄になったため、例年よりも不正ログインが増えている。金融機関は今後、リモートワークであっても不正取引をモニタリングできるように体制を整備しておく必要がある。

不正送金が行われる時間帯は主に深夜だ。犯罪者は1、2回ログインできるか確かめた後、23時台に送金限度額いっぱいまで不正送金することが多い。1日の送金限度額は0時でリセットされるため、日付をまたいでもう1回ログインして、再度、限度額まで不正送金している。こうした犯罪がわずか1時間以内に行われている。

不正口座の利用・開設にツイッターを利用

不正送金に使われた端末が次にどこの金融機関にログインしているのかを追跡すると、犯罪者は同じ端末でさまざまな金融機関に不正ログインし、資金をローンダリングしていることが分かる。こうしたマネロンで使われる口座は、不正に売買されたり、不正に開設されたりしたものだ。

不正の一例を挙げると、日本国内居住者の銀行口座なのに、1週間で世界10カ国のIPアドレスからログインしているケースがあった。通常このような利用はあり得ず、解析すると1口座を犯罪集団の複数人が悪用するトンネル口座になっていた。金融機関がその口座利用者に連絡したところ、お金に困って闇サイトを通じて口座を転売したという。闇サイトには、「ネットバンキング機能がなければ口座買取できません」と注意書きがある。普段はATMしか利用していない人でも、口座を転売する前には必ずネットバンキングに申し込む。

口座の転売価格は、以前は大手行が高く、地方銀行は安かったが、最近は地方銀行の値段が上がってきている。大手行と比較して疑わしい取引のモニタリングが厳しくされていないので、犯罪者にとって検知されにくい口座とみられており、そのため値段が高くなってきたようだ。さらに新手の手段として、口座を転売ではなく「貸し借り」する巧妙な手口もある。ツイッターなどで「2週間だけ使いませんか」と呼び掛け、この期間だけマネロンに利用して、返してもらう。銀行が入出金の履歴をモニタリングする中で、一定期間だけ不自然な振り込みがあっても、給与振り込みがあり、家賃の支払いも行っているため、通常の生活口座として判断されやすい。

犯罪者は闇サイトでの転売を通じて口座を不正に取得するだけではなく、偽造運転免許証などを使った不正な口座開設も行っている。その手口は、ICチップまで入っている精巧な偽造免許を作り、空き家を住所としてネット完結の口座開設を申し込む。空き家のポストに「不在通知書」が投函されるので、その伝票と偽造免許を持って、郵便局に受け取りに行くというものだ。偽造免許を1枚作ると、銀行だけではなく、クレジットカードや消費者金融なども申し込みがなされ、すべての金融機関で不正利用が行われる。

偽造免許の販売サイトは取り締まりを受けても、定期的に新たに立ち上がっている。偽造免許の販売価格は一昨年ごろまで6～7万円が相場だったが、技術が進歩し、現在は2万5000円で販売するサイトもある。最近は、こうしたサイトをわざわざ作ってSEO対策をして検索上位に上げるようなことはせず、ツイッターなどで「明日までに偽造免許を作ります」と手軽に勧誘する動きもある。

課題山積のセキュリティー対策

金融機関のセキュリティーホールは大きく3点ある。自行のモニタリングの成熟度、システム対応の柔軟性、そして口座連携先のセキュリティーレベル――の3点だ。

1点目の自行のモニタリング態勢については、現状でセキュリティーレベルが高いのはネット専業銀行だ。店舗がない分、オンラインに注力して取引モニタリングに人手とコストをかけている。一方、多くの地方銀行では、店舗がメインであるため、オ

ンラインに割ける投資額が少なく、その分、セキュリティーも手薄になっているようだ。さらに、コロナの影響で利用者の来店が減り、インターネットバンキングの利用が増えているにもかかわらず、モニタリングは質・量ともに不足している。地方銀行はＡＰＩによって、外部のセキュリティーベンダーと連携する必要があるだろう。

２点目のシステム対応の柔軟性としては、他行と共通のプラットフォームでインターネットバンキングを運営する金融機関の例を挙げたい。こうした金融機関では、不正ログインやマネロン防止のためにシステムを改修したり、外部のサービスを利用したくても、システムベンダーに対応してもらえないケースがある。その改修コストを自行で全額負担することが難しく、他行と調整するにしても時間がかかるためだ。さらには、従前の完全自前主義のもと、外部のサービスについて検討すらしないベンダーもいる。早急にセキュリティー機能を追加できずに、不正ログインを許すような事態があってはならないはずだ。日本を標的にする金融犯罪に対峙する上で、ベンダーはこれまでの自前主義から脱却し、外部の多様なサービスと連携するなど方針転換を図る必要があるのではないか。

３点目は、金融機関の出金先となる資金移動業等のセキュリティーレベルである。昨今、不正利用が起った通信キャリアの電子決済サービスでは、自社による厳密な本人確認プロセスがない中で、メールアドレスさえあればアカウント開設が可能となっていた。今後、金融機関として口座連携先のセキュリティーレベルを担保するガイドライン策定が求められるのではないか。

ほかにも、金融グループ内の商業銀行や信託銀行、証券会社、消費者金融でセキュリティーレベルに濃淡があることも課題といえる。親会社が非金融系のＩＴ大手では、傘下の各サービスに共通ＩＤを利用しているが、セキュリティーレベルの低い子会社が突破口となり、芋づる式にグループ内の銀行、証券が被害に遭う可能性がある。現金は○○ペイや暗号資産に転換でき、簡単にローンダリングされるため、金融サービスはできる限り銀行のセキュリティーレベルに近づけていかないと狙われてしまう。

官民一体でのトレーサビリティー強化を

18年時点で当社の提携先は約10社だったが、このとき疑わしいアクセスは全アクセスの１・９％だった。当時、暗号資産（仮想通貨）取引所の不正流出事件が騒がれたが、当社取引先の事業者でも他業態に比べて、疑わしいアクセスが目立った。ある週では10％が疑わしいアクセスだった。銀行口座から盗んだ資金を暗号資産取引所に流してローンダリングする動きも見られた。このように、その時々でセキュリティーが手薄な業態が狙われやすい。

今後は、不正資金がどのようにローンダリングされているか、金融機関や資金移動業者などが連携し、トレーサビリティーを担保していくことが重要だ。利用者から盗まれたと報告があったら、即時にその資金がどう流れていったのか、各社が相互開示できるような仕組みが求められるだろう。

キャッシュレスを推進すればするほど、資金の出所がどこなのかが重要になってくる。自行から資金が盗まれないことに注力するのは当然のことであり、さらに不正な資金が自行に環流していないかをモニタリングしていかないと、マネロンは防げない。各金融機関でホットラインを設け、官民一体で金融犯罪を食い止めていく必要がある。（談）

しまづ　あつよし
京都大学卒業後、ドリコム入社。その後、オンライン英会話学習のロゼッタストーン・ジャパンを経て、Ｃａｐｙ社で不正ログイン対策のソリューション提案に従事。15年にカウリスを創業。法人向けクラウド型不正検知サービス「フロードアラート」を開発・販売。フィッシング対策協議会運営委員。ｅメール：info@caulis.jp