特集

真のサイバーセキュリティーを構築せよ！

Interview

不正アクセスを防ぐには業態横断での情報共有が必須

犯人は同一端末からさまざまなサービスへの不正アクセスを繰り返している

カウリス　代表
島津　敦好

不正ログイン検知サービスを手掛けるカウリスは、金融機関のインターネットバンキングなどのログイン情報をモニタリングして、不正利用の分析を行うフィンテックベンチャーだ。不正利用に使われた端末情報を把握し、提携を結ぶ企業や金融機関などがその情報を共有することで、二次被害を防ぐ取り組みを進めている。「手口が巧妙化しており、業態を横断した情報共有が必要」と強調する島津敦好社長に、いま求められる不正対策について聞いた。（編集部）

偽造免許証による「合成ＩＤ詐欺」

――最近の不正ログイン事案には、どのような特徴があるか

当社では、金融機関や証券会社、クレジットカード会社、暗号資産交換業者、通信キャリアなどに、不正なアクセスを検知・共有するサービスを提供している。ログインしているスマートフォンのＯＳやブラウザのバージョン、設定言語などをモニタリングすることで、普段と異なる不正な使われ方を検知している。現在、金融機関を中心に、35社にサービスを提供しており、二次被害を防ぐために不正利用情報を提携事業者間で共有している。

最近の不正事案の特徴は、従来あった銀行口座情報を何らかの手段で窃取して出金するといった単純な手口でなく、偽造し

た公的証明書を使い、複数の業態をまたいで出金するなど、手口が巧妙化していることだ。例えば、複数のサービスをまたいで情報を不正入手・活用する犯行があった。犯罪者はまず、証券口座ＩＤとパスワードを何らかの手段で入手して不正ログインし、利用者の氏名と勤務先を入手した。次にその氏名を使って偽造運転免許証が作られ、そこでは犯人の顔写真と空き家の住所が使われる。そして、その偽造免許証で銀行口座を開設し、証券口座から出金する銀行口座を当該口座に変更して、証券口座にある有価証券を現金化していた。

実在する情報と犯人の情報とを交ぜたなりすましは、米国でSynthetic Identity Fraud（シンセティック・アイデンティティー・フロード＝合成ＩＤ詐欺）と呼ばれ、近年増加している。最近の偽造運転免許証はかなり精巧で、かつ安価で作成されており、外国人在留カードの偽造も増えている。

これらを使って開設された銀行口座は、不特定多数の犯罪者に使われ、複数の国・都道府県からアクセスされるケースもある。そのため口座開設時の本人確認と合わせて、利用者の端末傾向、属性情報の継続的なモニタリングが有効だ。金融庁の「疑わしい取引の参考事例」にあるとおり、ブラウザの言語設定、ＩＰアドレスから得られるロケーション、端末情報などからリスクの高い口座が捕捉されるケースもある。

ｅ－ＫＹＣ（オンラインでの本人確認）では、運転免許証の顔写真と申込者の顔の一致を確認するが、その運転免許証が真正か否かは確かめようがない。昨年には、偽造の公的証明書を使って、複数社に対して数十件の口座開設やクレジットカード入会を試みた端末を捕捉した。マイナンバーカードのＩＣチップに格納されている利用者証明用電子証明書を使った公的個人認証サービスを使えば、ログイン者が利用者本人だと認証できるが、マイナカード普及率は２０２２年２月１日時点で41・８％で、すべての国民が取得するにはまだ時間がかかるだろう。

電力会社と連携し顧客管理を効率化

――不正口座を排除していくにはどうすればよいか

不正に作られた銀行口座は悪用された後、さらに闇サイトなどを通じて転売されることが多い。誰が使っているか分からない口座は非常に多く存在しており、金融機関が継続的顧客管理を徹底することで犯罪に使われている口座を凍結していかなければならないが、これは容易ではない。なぜなら、金融機関は継続的顧客管理として、顧客の登録住所にはがきなどを郵送し、顧客情報の更新や取引目的の確認を依頼しているが、すでに住所が変更になっていて顧客に届かないケースが一定割合あるからだ。00年以前の銀行口座開設では、多くの金融機関で顧客から携帯電話番号やＥメールアドレスを取得しておらず、自宅の固定電話番号と住所しか把握していないケースが多い。そのためハガキ郵送による顧客情報更新しか手段がないのが現状だ。

そこで当社は電力会社と提携し、銀行保有の顧客情報と電力会社の設備情報を照会するサービスを提供している。電力会社の設備情報の照会については、19年に規制サンドボックスで認定を受けて事業化しており、過去に複数の銀行・クレジットカード会社での不正口座開設・不正入会防止で実証している。今後は、継続的顧客管理に適したサービスを構想している。

資金移動業者で不正利用情報を共有

――キャッシュレス推進協議会が22年度中に運用を開始する「不正利用関連情報確認データベース（CLUE）」にカウリスが技術協力するが、どのような取り組みか

近年、スマホのキャッシュレス決済サービスの普及に伴い、不正アクセスは銀行口座やクレジットカードのほかに、○○ペイなど資金移動業者の決済サービスでも見られるようになっている。そこでキャッシュレス推進協議会が主体となり、キャッシュレス決済事業者間で不正利用の情報を迅速に共有する仕組みを構築することにした。

かねて当社サービスにより、端末情報を共有することで、疑わしい取引を企業・業界横断で検知している。今回のCLUEプロジェクトでも、不正利用に使われた情報を共有することは、決済事業者内での被害抑制に大きく寄与するだろう。各事業者はCLUEに不正利用に関連する情報のみを、適切にハッシュ化（不可逆変換）した上で登録する。照合する事業者は自社サービスで不正利用の可能性があるかどうかのみを確認でき、他の目的では利用できない仕組みとする。

当初はNTTドコモやKDDI、コモニー、ファミマデジタルワン、LINEペイ、楽天ペイメントなどのメンバーでスタートするが、将来的に金融機関やクレジットカード会社など他業態からの参画も予定している。

――不正アクセス検知で課題はあるか

スマホの基本ソフト（OS）の設定において、セキュリティーとプライバシーが相反する事態が生じつつある。ウェブ広告においては、インターネットの閲覧ソフト（ブラウザ）のクッキー情報を元に消費者の趣味嗜好に沿ったリターゲティング広告が打てるようになっているが、プライバシー保護の観点から消費者が自身の情報の提供を抑制する意識が高まっている。そこでアップルは、利用者のプライバシー保護のため、21年9月にアップデートしたiPhoneの「iOS15」でプライバシー保護機能を強化できるようにした。利用者が「プライベートリレー」という機能をオンに設定すると、「サファリ」ブラウザで閲覧した場合、IPアドレスが匿名化され、ウェブ閲覧履歴が非公開となる。

そのため金融機関では、利用者が「新宿区」でログインしたことを従前は把握できていたが、設定によっては「国」や「都道府県」までしか分からなくなってしまう。日本ではスマホにおいてiPhoneのシェアが約7割と海外より高いため、今後iOS15に更新し、プライベートリレー機能をオンに設定する人が増えると、不正アクセス検知の観点からは利用状況把握や閲覧追跡が難しくなる。

当社はこの設定をした端末からアクセスがあった場合、リアルタイムで金融機関に伝えている。一部の金融機関では、その端末から高額な入出金があった場合、モニタリングを強化するケースもあり、該当端末でのログインを認めない方向で検討している事業者もある。

グーグルもプライバシー機能強化を計画しており、プライバシーとセキュリティーがトレードオフする状況となっている。プライバシー保護は重要だが、犯罪抑止の観点から政府や関係省庁と連携し、業態を横断して対策を考えていきたい。

（聞き手・本誌　加藤精一郎）

しまづ　あつよし
京都大学卒業後、ドリコム入社。複数社を経て、15年にカウリス創業。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、フィンテック協会理事。