AI 不正取引検知サービス：AI ゼロフラウド事例

auじぶん銀行株式会社 様

大規模フィッシング被害の教訓を活かし、早期AI不正取引検知システムを導入

金融犯罪被害の急増が社会問題となっている。警察庁の公表※によると、2025 年の詐欺被害額は約 4,029 億円と前年比で 31.1% 増加、インターネットバンキング不正送金被害額も約 104 億円と初めて 100 億円の大台を突破した。特に見逃せないのは、その約 9 割がフィッシングを起点としている点だ。

金融犯罪の被害は、銀行からの送金によって犯罪者に資金を詐取されるケースが大部分を占めるため、金融機関にとって対策が喫緊の経営課題となっている。金融機関は高度な社会インフラであり、安心安全なサービスを提供することが求められているためである。

※ 令和 7 年におけるサイバー空間をめぐる脅威の情勢等について」| 令和 8 年 3 月警察庁サイバー警察局
https://www.npa.go.jp/bureau/cyber/pdf/R07_cyber_jousei.pdf

スマートデバイスの体験とセキュリティ対策

au じぶん銀行は「デジタルを駆使する。お客さま視点で考える。そして、期待を超える金融へ。」というパーパスを軸に、「未来まで明るく。」というブランドメッセージを掲げ、顧客に寄り添った金融サービスを展開している。口座数は 714 万、預金残高は 5.5 兆円（2026 年 1 月 1 日時点）、住宅ローンやカード融資などの各種サービスも拡大し、顧客満足度を維持しながら着実に事業基盤を伸ばしてきた、インターネット専業の銀行だ。

一方で、オンラインサービスは、認証・送金・通知といったデジタル導線が攻撃者に狙われやすい。特にフィッシングや認証情報の窃取を起点とした不正送金に加えて、騙された本人が送金する SNS 型投資詐欺やロマンス詐欺は正規の操作として成立してしまうため、防御は容易ではない。だからこそ、利便性と安全性を両立させるためのセキュリティや不正対策は、サービスの後付けではなく、顧客体験の一部として設計される必要がある。

今回は、au じぶん銀行でセキュリティ対策の中核を担い、金融犯罪対策やアンチマネーロンダリング対策を推進している執行役員 チーフコンプライアンスオフィサー 兼 チーフリスクオフィサー 兼 リスク管理本部長の光末 史郎氏に話を聞いた。

チーフコンプライアンスオフィサー 兼 チーフリスクオフィサー
兼 リスク管理本部長 光末 史郎氏

大規模化・巧妙化する攻撃と運用負荷の増大

インターネットバンキング不正送金をめぐる環境変化を語るうえで、フィッシングの質の高度化・巧妙化は見逃せない。かつてのフィッシングメールは、不自然な日本語や誤字脱字が目立ち、顧客への注意喚起による一定の抑止が機能していた。しかし生成 AI の登場以降、2023 年ごろからは、メール文面から不自然な日本語が消え、遷移先サイトの完成度が上がり、従来のフィッシングメールの見抜き方が通用しなくなった。

フィッシング手口が洗練されるほど、認証情報の詐取件数が増え、それを起点としたなりすましによる不正送金も連鎖的に増加する。このため、金融機関側のモニタリングや調査の負荷は急激に膨らむ。

同時に、「疑わしい取引をどれだけ止めるか」という従来の課題に加え、「止め過ぎによる顧客体験の毀損」の回避も両立する必要に迫られる。不正を防ぐほどに正規ユーザーの体験を損なうリスクが高まり、両者のトレードオフがよりシビアになっている。実際に、au じぶん銀行も、2023 年には大規模なフィッシングの標的にされたことで、運用負荷と顧客体験の両立という難題に直面することになった。

振込保留と誤検知数を重視する理由

店舗がないネット銀行にとってコールセンターは、お客さまと直接つながる大切なチャネルだ。疑わしい振込を一時的に止める「振込保留」が増えれば、顧客体験への悪影響だけでなく、コールセンターへの問い合わせが増加し、現場の負荷も跳ね上がる。

とりわけ、大規模なフィッシング被害が発生し、振込保留が急増した場合の影響は深刻だ。コールセンターの電話が繋がらなくなり、電話が繋がらない状況が続けば、「送金を不当に止められ、かつ問い合わせもできない」という不満が顕在化し、SNS などで一気に拡散される。これはオペレーションの問題にとどまらず、ブランド毀損に直結するレピュテーションリスクであり、最も避けるべき事態である。

このため、振込保留は必要最小限に抑える必要がある。同時に重要になるのが「誤検知」数の抑制だ。誤検知とは、正しい送金を銀行が不正と判断することだが、正規の送金を不正と判断して停止した場合、顧客に不利益が生じる可能性がある。

振込保留や誤検知はいずれも、顧客体験と運用現場の双方に負担をかける。だからこそ、不正取引対策は検知率を高めるだけでは不十分であり、振込保留と誤検知の二つをいかに抑え込むかを重視するのだ。

“止める”と“回す”を両立するための選択

au じぶん銀行では当初、不正取引の検知を従来の主流であったルールベースで開始する想定だった。しかし、生成 AI の普及により攻撃者側の手口高度化が加速し、ルールの裏を突くスピードが飛躍的に高まっている。こうした環境変化とラックからの助言を踏まえ、AI による不正取引検知を本格検討することにした。

ラックの AI 不正取引検知システム「AI ゼロフラウド」は、高い検知精度で振込保留と誤検知の抑制が期待できる点が評価された。実際、au じぶん銀行の取引データを用いた PoC で、想定通りの成果を確認している。さらに、採用の決め手となったのは技術面だけではない。ラックの金融犯罪対策センター（Financial Crime Control Center：以下、FC3）には銀行実務に精通した人材が多く、検知ロジックだけでなく、導入後の業務フローや運用負荷まで見据えた具体的な議論が可能だった点も大きい。

PoC の段階で、ルールベースと比較して振込保留や誤検知を大幅に抑制できることが確認できたので、AI 検知のみにすることも検討したが、最終的にはルールと AI の両立を図る方針となった。背景にあるのは、攻撃手法の急変への対応力である。攻撃側の手法が変わり被害が急増した場合、ルールベースであれば担当者が取引内容を確認・分析することで、すぐにルールを変更できる。しかし、AI のみで不正検知を行う場合、ルールベースに比べて再学習と検証に時間を要してしまうため、即応性では不利な場面もある。

ただし、AI とルールベースの “ 二段構え ” は、AI の検知精度の高さとルールベースの柔軟なルール運用という利点がある一方で、要件定義は複雑化する。先行事例が無い中で最適な組み合わせを見出すには、技術と業務の双方を理解したうえでの試行錯誤が不可欠であり、au じぶん銀行とラックが一体となって設計と運用を磨き上げていく必要があった。

スピードだけでは終わらない、二段構えで実現した不正検知

こうした背景がある中で、驚くべきは、意思決定から開発に至るまでのスピードだ。2023 年夏に AI による不正取引検知の検討を開始し、同年 10 月から約半年間の PoC を行った。2024 年夏に開発を決定・着手している。不正対策の領域では、検討開始から実装までに数年を要することも珍しくないため、かなりスピーディーに進んだといえる。

本来、PoC には実際の取引データが必要になる。その準備だけでもマスキングを含め 2 ～ 3 か月を要することが多い。さらに AI に学習させるためのデータの整備、PoC 評価、予算化と進むと、開発着手までに 2 年前後かかるケースもある。しかし、au じぶん銀行は、2023 年の大量のフィッシングの標的となったことへの危機感が経営層まで共有され、PoC から予算化、開発までの意思決定が一気通貫で進んだ。

その推進力となったのが、責任者である光末氏の存在だ。過去の教訓を踏まえ、事前に論点整理と合意形成を進めていたことに加え、開発の進捗や他行動向、脅威の変化を継続的に経営層へインプットし続けた。大規模攻撃の記憶は時間とともに風化し、「そこまでやる必要があるのか」「段階的に縮小できないか」という声が上がりがちな中で、リスクと投資対効果を経営判断の言葉に翻訳し続けたことが、スピードと継続性の両立につながっている。

もっとも、この取り組みは速いだけではない。リリースは二段階で設計されており、2025 年 5 月にルールベースを先行リリースし、同年 12 月にルールと AI を組み合わせた正式版へ移行した。即応性の高いルールで早期にリスクを抑えつつ、検知精度の高い AI を段階的に組み込むことで、スピードと確実性を両立させた。さらに興味深いのは、想定外の効果である。AI ゼロフラウドは振込保留と誤検知の抑制に加え、SNS 型投資詐欺や ロマンス詐欺、さらには不正口座の兆候まで検知した。不正送金対策にとどまらず、金融犯罪全体を俯瞰する検知基盤として機能し始めたのだ。

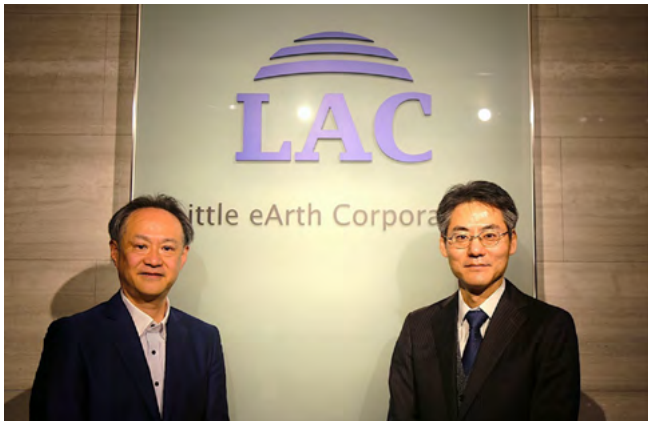
社会の公器となったネット銀行による官民・業界連携

金融犯罪対策は、一社単独の努力だけで完結しない。むしろ、どれだけ高度な対策を講じても、自社だけで守る前提では限界がある。2023 年の大規模フィッシング被害を経て明らかになったのは、複数の手段を組み合わせる必要性だ。

犯行グループは金融機関だけでなく、通信事業者や各種プラットフォームを横断して攻撃を仕掛けるため、官民、業界横断の連携が効果を発揮する。

金融庁、警察庁・警視庁、各地の警察、KDDI グループとの情報連携に加え、金融 ISAC や JC3 など業界団体とも情報共有や共同の枠組みを強化し、兆候の早期把握と封じ込めのスピードを上げていくことが重要となっている。金融犯罪対策は非競争領域と位置づけられるため、脅威の前では競合である他行と協力することが前提となる。ネット銀行はもはや、インターネットサービスの一つではなく、すでに社会のインフラの一部であるという自覚が、この連携の土台にある。

金融犯罪対策は、技術進歩が著しい分野だ。AI の悪用により攻撃手法は急速に進化しており、FIDO/ パスキーなどの認証強化に加え、AI を活用した不正取引検知の高度化、行動バイオメトリクスの活用といった選択肢も現実味を帯びている。金融庁も監督指針の改定や要請文を相次いで発出しているが、金融機関もリソースに限りがある以上、自社の金融犯罪対策を適切に評価し、優先順位をつけて投資していく視点が欠かせない。FC3 は、国内外の最先端の技術や対策の事例を踏まえ、au じぶん銀行の金融犯罪対策の高度化の支援をこれからも続けていく。



右から、au じぶん銀行 光末 史郎氏、ラック FC3 エバンジェリスト 小森 美武

［お問い合わせ］
株式会社ラック
サービス紹介ページ　https://www.lac.co.jp/solution_product/zerofraud.html