近未来金融システム創造プログラム第９回講義レポート

第９回目となる本日は、newmo 株式会社 CTO の曾川景介氏を迎え、「金融と技術（各論Ｉ）技術は金融をどう変えてきたか」という題目で講義が行われた。前半では、WebPay、LINE Pay、メルペイ、メルコインの立ち上げに関わってきた経験を出発点に、技術が金融サービスの作り方をどう変えてきたのか、決済を支える認証・認可と本人確認の課題、セキュリティインシデントから得られる教訓、さらに金融とモビリティに共通する事業基盤やビジネスが成り立つ構造、それを定める規制、問題が起きた場合の責任といった課題についてお話しいただいた。

開発者向け決済から生活者の決済へ

インターネット上で商品やサービスを提供し、料金を受け取るには、決済の仕組みが必要となる。しかし、サービスを開発するたびに課金機能を実装することは、開発者にとって負担であった。この負担を減らすために開発したのが、開発者向けの決済サービス「WebPay」である。API を通じて、数行のコードでサービスに決済機能を組み込めるようにした。当時のシリコンバレーでも、オンライン決済の導入を支援する Stripe や、金融機関の口座情報を集約する家計簿サービスの Mint など、金融機能を使いやすくするサービスが登場していた。

WebPay では、少ないコードで決済を組み込める一方、その裏側では、金融の仕組みや決済ゲートウェイとの接続、情報の保護、継続的な運用が必要となる。開発者による利用を支える SDK（ソフトウェア開発キット）やドキュメントの整備も、その一部である。とりわけ重要だったのが、クレジットカード番号を別の情報に置き換えるトークン化である。カード情報の保護に関する国際的なセキュリティ基準である PCI DSS などが整備されても、実装や運用を担う人間の不備をなくすことは難しい。そこで、加盟店に本物のカード番号を知らせずに決済できる仕組みが生まれた。加盟店のシステムが攻撃を受けても、カード番号の漏洩リスクを抑えられる。Apple Pay が店頭でカード番号の代替情報をやり取りする仕組みも、この流れの中にある。

金融サービスの変化は、技術の進歩だけでなく、制度の整備やスマートフォンの普及とも結びついている。2010 年の資金決済法施行による資金移動業などの制度整備は、銀行以外の事業者による決済・送金サービスの展開を支えた。同時に、人々がスマートフォンを通じて日常的にアプリを使うようになり、金融機能を別のサービスの中に組み込む動きが広がった。WebPay の LINE への売却後は、開発者向けに決済機能を提供する取り組みから、生活者が日常的に使う LINE アプリに決済や送金を組み込む「LINE Pay」の開発へと展開した。アプリ内で決済や送金を行うには、利用者、決済サービス、加盟店をつなぐだけでなく、銀行口座から資金を入れる仕組みや本人確認の手続きを整える必要があった。

しかし、LINE Pay は当初、十分な利用につながらなかった。当時の米国では、家賃などを支払う際に小切手を書いて郵送するという慣習があり、それに伴う不便さがあった一方、日本では既に銀行振込が発達していた。そのため、利用者がまだ少なかった LINE Pay では、個人間送金のニーズが十分に顕在化していなかった。さらに、LINE Pay を使える場所が少なく、アプリでお金を扱う習慣も定着していなかったことから、加盟店の拡大とともに、実際に使ってもらうための働きかけが必要となった。例えば、後発のスマートフォン決済サービスである PayPay は、大規模な還元キャンペーンで利用を促しながら、使える場所を広げていった。LINE Pay もアカウント数や使える場所を増やしていたが、利用者の状況を調べると、場所や習慣よりも根本的な問題が見えてきた。当時、LINE のアクティブユーザーは若者が中心であり、LINE Pay への入金以前に、銀行口座に置く十分なお金を持たない利用者も多かった。決済の利便性を高めるだけでは対応できない、利用者の資金不足への対応が次の課題となった。

利用者の資金不足とメルペイ・メルコイン

利用者の資金不足への対応として、個人間でモノを売買するメルカリの仕組みと、金融サービスを結びつける発想が生まれた。メルカリには、手元のモノを売って売上金を得て、それを次の買い物に使うという資金の循環がある。ただし、この循環だけでは、モノかお金のどちらかを持っていなければ利用できないという制約が残る。そこで必要となったのが、利用者に後払いなどを可能にする与信を提供し、買い物に使える資金を補うことであった。

当時のメルカリでは、クレジットカード、コンビニ払い、売上金を使う利用者が、それぞれ約３分の１を占めていた。一般的な電子商取引に比べてカードの利用割合が低く、コンビニ払いや売上金で買い物をする利用者にも、決済手段と与信を提供する必要があった。この課題に対応するサービスとして始まったのが「メルペイ」である。売上金を活用した決済に加え、与信によって買い物に使える資金を補うことで、利用者の購買力を支える役割も担った。

暗号資産のサービスを手がける「メルコイン」も、メルカリでの売買に金融機能を組み込む発想から生まれた。暗号資産のサービスは、現金を暗号資産に換えて投資するものとして捉えられやすい。一方、メルコインの構想には、モノを売った代金をビットコインで受け取り、ビットコインで買い物をするという使い方も含まれていた。もともと決済手段として作られたビットコインを、単純な投資だけでなく、モノとお金の循環の中で利用できるようにする取り組みである。その事業化にあたっては、暗号資産の流出事件などを背景とする規制上の課題に対応し、暗号資産交換業の登録を得るなど、事業に必要な準備を進めた。

金融サービスの出発点は、必ずしも金融そのものにあるわけではない。WebPay は課金機能を実装する開発者の負担、メルペイは買い物をする利用者の資金不足という、既存の

サービスに関わる課題から生まれた。API を通じて金融機能を提供する場合も、本業のサービスに組み込む場合も、ユーザー体験や利用者が抱える課題を捉え、そこに必要な機能を加えていくことが重要になる。こうした金融サービスの変化には、AI が担う役割も関わってくる。判断の支援、不正や誤操作の検知、利用者に代わる操作の実行などが、その主な役割として挙げられる。特に代理実行では、AI に操作する権限を与えるため、その範囲の設計が問われる。安易に権限を渡せば、社内の情報が持ち出されたり、利用者の財産が意図しない形で使われたりするおそれがある。そのため、何を任せ、どこまでの操作を認めるかを定める必要がある。

決済における本人確認・認証・認可

アプリやサービスに決済などの金融機能を簡単に組み込めるようになった一方、その安全性を確保することは容易ではない。プログラミング言語や開発手法が変化しても、不正行為は時代を問わず存在してきた。セキュリティは、特定の技術への対策にとどまらず、人がサービスを利用する限り向き合い続ける課題である。大手コンビニチェーンのスマートフォン決済サービスの不正利用問題では、外部 ID との連携やパスワード再設定など、アカウントを保護する仕組みの脆弱性が問題となった。ここで問われるのは、認証・認可の設計だけでなく、安全性を十分に確認したうえでサービスを公開するという経営判断のあり方である。また、発覚後の記者会見では、二段階認証という言葉が一人歩きし、技術的な論点が十分に共有されない状況も生じた。この事例は、事後的な対策だけでは間に合わない場合があることを示しており、公開前の安全性の確認と、それを支える経営の理解が必要となる。

銀行口座と連携して入金や支払いを行う通信キャリアの提供した資金移動サービスの不正利用問題では、サービスのアカウントと銀行口座の名義人が同一人物かを確認することが課題となった。当時、決済サービスの本人確認には、銀行口座に依拠する方法が広く使われていた。銀行が既に行った本人確認を資金移動サービス側でも利用する仕組みであり、サービスの利用者と銀行口座の名義人が同一人物であることが前提となる。オンラインで手続きを完結できるこの方法は、決済サービスの普及に大きな役割を果たした。しかし、口座番号と 4 桁の暗証番号による認証が通っても、決済サービスのアカウントと銀行口座が同じ本人のものだとは限らない。ドコモ口座の不正利用問題では、この確認が不十分なまま連携できたことが課題となった。攻撃者のアカウントに他人の銀行口座が紐づけられれば、不正な資金移動につながる。メルペイではアカウントと銀行口座の名義の一致を確認していたが、その対策を個社にとどめず、業界の標準として共有することも課題であった。

決済の裏側では、承認、残高の記録、資金の移動、照合などの処理が行われる。その際には、認証によって操作している人がアカウントの正当な利用者かを確かめ、認可によって、その人に特定の加盟店へ一定の金額を支払う権限があるかを判断する。この意味で、

決済を支える中心的な機能は認証と認可である。利用者を認証し、与えられた権限の範囲で操作を認めるという構造は、Google などのアカウントを使って別のサービスにログインし、情報の取得や操作を許可する仕組みとも共通している。ただし、認証・認可とは別に、申告された人物が本人であることを確かめる「本人確認」も重要となる。

その本人性をオンラインで確かめるための仕組みも変化している。身分証の画像を撮影して送る方法に加え、マイナンバーカードを用いた公的個人認証も普及してきた。当初はカードの普及が進まなかったが、ポイント付与などのインセンティブを通じて、本人確認手段を広く行き渡らせる取り組みが進められた。こうした取り組みを通じて、マイナンバーカードによる本人確認手段が広く行き渡るようになった。一方、国による情報の把握にはプライバシー上の論点もあり、基盤の整備によってすべての課題が解決するわけではない。また、サービスの安全性を保つには、本人確認に加え、外部からの監視や監査も必要となる。

セキュリティインシデントとサプライチェーンリスク

金融サービスは複数のシステムを組み合わせて成り立つため、自社が安全でも接続先から被害が波及することがある。メルカリでの情報流出も、利用していた外部の開発ツールへの侵害を足がかりとする、サプライチェーン攻撃によるものだった。

この事例では、テストや配備に使う開発環境から認証情報が不正に取得され、ソースコード管理システムに保存されていた個人情報へのアクセスにつながった。外部の開発ツールを通じた侵入への対策に加え、秘密情報や個人情報をソースコードとともに保存しないという、社内の情報管理を徹底する必要性も明らかになった。認証情報の無効化と更新、調査、利用者への連絡を進めた後も、再発防止と継続的な改善が求められた。当時は異常の兆候から不正アクセスの把握までに約 1 週間を要したが、AI によって攻撃が高速化すれば、調査や対策、公表を準備する時間もさらに限られる。

現代の開発は多くの外部ライブラリやツールに依存し、AI を使う場合もその依存関係を把握できるとは限らない。データの保存場所を管理するとともに、侵害が起きても情報が漏れないよう、安全上の制約を開発作業に組み込む必要がある。端末や開発環境が既に侵害されている可能性も踏まえ、AI を動かす環境や、外部から取り込むものにも注意を払う必要がある。

こうしたセキュリティ上の課題は、開発環境に限らない。データを暗号化して身代金を要求するランサムウェアなど、組織全体の業務に影響する攻撃もあるため、セキュリティ対策を専任担当者だけに任せることはできない。他社の事故から学び、個社の知見を標準化やガイドラインに反映することも、業界の安全性を高めるうえで重要である。

金融とモビリティ

金融もモビリティも、利用者から見えない事業基盤に支えられている。金融では銀行や

加盟店、サポート、運用が決済を支えるように、移動では車両や乗務員、営業所、配車がサービスを支える。タクシー事業と自動運転開発に取り組む newmo は、タクシー会社の買収と運営改善から基盤を整えている。ドライバー不足と市場縮小に直面するタクシー事業では、担い手を確保できなければ、提供できる移動サービスも限られる。自動運転は、この担い手不足に技術で対応する取り組みである。

ハードウェアの低価格化や論文・データセットの公開により、自動運転の開発環境も変わった。人が細かなルールを書く方法から、データでニューラルネットワークを学習させる方法へと開発が進む中、技術に加え、データを継続的に集める事業構造が重要になっている。newmo の構想は、英国の自動運転開発企業 Wayve のように走行画像から学習する AI モデルと、米国の自動運転サービス企業 Waymo のように技術開発から車両の運行まで自ら担う垂直統合のビジネスモデルを組み合わせるものである。商用車両から得たデータを学習と評価に使い、社会実装までの全てのサイクルを自ら回すことに、タクシーの事業基盤を持つ意味がある。

ただし、このように技術と事業基盤を整えても、社会への導入には規制や現場で働く人の立場を踏まえた事業運営が必要となる。金融は人の財産、モビリティは人の命に関わるため、新しい技術を導入する事業者には、事故や問題が起きた際の責任を引き受けることが求められる。一方、規制によって既存事業者が保護される中で、利用者の課題が解決されずに残る場合もある。新たに参入する事業者の役割は、規制を無視することではなく、その目的を理解し、責任を担いながら課題の解決を進めることにある。

自動運転の社会実装には、車両の運行を支える設備も欠かせない。自動運転には車両の充電や運行を支える拠点が必要となるが、電力を大量に確保できる場所は限られており、ピーク電力を抑える運用も課題である。モデルの開発だけでなく、エネルギーの確保と日々の運営を支える基盤まで整えることが、継続的なサービス提供につながる。

本人確認情報の管理と制度運用の課題

本人確認の強化が進む一方、身分証の画像などを大量に保存すれば、その情報自体が攻撃の標的となる。本人確認を行うことと、そのために使った情報を保存し続けることは分けて考える必要がある。情報そのものを開示せずに必要な条件を満たすことを証明するゼロ知識証明も、本人確認への活用が議論されている。日本では公的個人認証を使い、身分証の画像を預からずに本人確認を行える場合もある。ただし、画像を保存するかどうかには、行政による指導や制度の運用も関わる。

レンタカー事業では、免許証のコピーの保存をめぐって、国土交通省が保存までは求めていなくても、地域の運輸局から求められる場合がある。金融でも、同じ制度の下で地域によって判断が異なることがある。裁量による運用は、個別の事情に対応できる一方、共通の対策や迅速な変更を難しくする場合もある。また、事業者の規模や体制が異なるため、一律の対応を求めることにも限界がある。制度からこぼれる人や例外が必要な事情に

も配慮しながら、リスクを管理して運用することが求められる。
　金融とモビリティのいずれにおいても、技術だけでなく事業基盤を整え、責任を引き受けて課題を解決することが重要となる。

Q&A

Q1. 決済手段が増える一方、利用者から見た利便性は頭打ちになっているように感じる。各事業者が掲げる金融インフラのビジョンと、利用者が感じる利便性とのギャップについて、事業者側としてどう考えるか。
A1.
曾川（敬称略）：Pay サービスが乱立した背景には、制度の変化によって参入が可能になったことに加え、事業者側の都合もある。今振り返ると、広く使われるサービスを中心に標準化し、他のサービスとも連携できる設計を目指す余地はあった。ただし、資本力や独自の経済圏を持つ事業者は、その中でサービスを完結できるため、統一は簡単ではない。
デジタル通貨やステーブルコインには、サービス間で残高を移したり、共通して扱ったりする仕組みへの期待がある。その実現にはアカウント間の連携が必要であり、マイナンバーカードなどの共通の認証基盤を使って、同じ本人による操作かを確認する方法が考えられる。一方、利便性の捉え方は地域や利用者によって異なり、使い慣れた通信キャリアのサービスを便利に感じる人もいるため、一度に統一することは難しい。

Q2. オンラインで本人確認を行う eKYC に高い信頼が置かれているが、スマートフォンやマイナンバーカードを盗まれた場合のリスクもあるのではないか。また、自動運転が乗っ取られた場合の、人命に関わるリスクにどう向き合うか。
A2.
曾川：eKYC は万能ではないが、不正な利用を防ぐために一定の確認は必要となる。各社が独自に本人確認の仕組みを実装するより、安定した実装を備えた複数の信頼できる基盤を利用し、その安全性を高める方法が考えられる。マイナンバーカードも、署名用のパスワードを推測しやすいものにしている場合などには、リスクが残る。メルカリでは、名義の一致や配送先の住所の確認に加え、継続的な取引モニタリングを重視していた。本人確認だけに頼らず、不自然な取引を見つけて止めることも重要であり、AI を活用できる領域でもある。
自動運転やソフトウェアで制御される車両には厳格なサイバーセキュリティ対策が求められるが、基準を満たすだけで守り切れるとは限らない。車両の前に人が出てきて走行を妨害するような物理的なリスクも含め、想定される脅威をモデル化し、リスクを継続的に洗い出すことが重要である。

Q3. マイナンバーなどの情報だけでなく、周辺の情報を組み合わせて個人を特定するリス

クもある。こうした脅威は今後増していくのか。
A3.
曾川：増していくと考えられる。情報をつなぎ合わせるコストやプログラミングの負担が下がれば、以前は難しかった攻撃も実行しやすくなる。金融などの産業では従業員の身元確認も課題となり、リモートで働く人が本当に本人かを確かめる必要がある。また、社内のシステムや端末が既に侵害されている可能性も踏まえなければならない。社内や端末を無条件に信用せず、継続的に安全性を確認するゼロトラストの考え方で、リスクを評価し続ける必要がある。個人情報の保存も危険を伴うため、必要がなければ預からない判断が重要である。
赤井（敬称略）：リモートで働く従業員らしき人が本人かという問いは重要であり、AI で作られた人物などを通じた社内会議への侵入も考えられる。
金融とモビリティは、提供するサービスや業務の工程は異なるものの、厳格な規制の下で事業を営む産業として共通する構造を持つ。技術を使って産業の仕組みを変える際に検討すべき点は、バイオや製薬、農業にもある。例えば、農業が工業化し、AI で制御される完全閉鎖型植物工場では、気候変動の影響を抑えられる一方、何らかの障害によって生産が一度に止まれば、食料供給に影響が及ぶおそれもある。