日経 XTREND
クロストレンド

NTTドコモが運営する電子マネーサービス「ドコモ口座」などを経由し、提携先の銀行の預金残高が不正に引き出される金融事故が発生して以降、金融サービスのセキュリティーがいっそう注目されている。キャッシュレスがより浸透している中国では、金融事故に対してどういった対策が取られているのか。システム、ユーザー体験、そして設計思想を通じて中国フィンテックサービスのセキュリティー対策を追った。

中国でキャッシュレス決済がはやった理由として「お札（現金）が信用されていなかったから」という意見を聞くことが間々ある。確かに中国では偽札が多く、銀行のみならず商店ですら紙幣鑑別機を備えていることが一般的だ。対して日本の商店では紙幣鑑別機を見かけることは稀（まれ）であるが（最近の自動釣り銭機能付きレジスターなど紙幣鑑別を行う事例もある）、これは紙幣の信用を高めるために極めて高いコスト（偽造防止のための高度な印刷技術や金融機関での管理体制など）をかけているからだ。

日本における紙幣や印鑑（実印）のように「絶対安全である」と皆が信じることで、それをアンカー（基点）に信頼性を担保する仕組みを「トラストモデル」という。中国は偽札が横行するばかりでなく、歴史的に王朝の永続性にも乏しく、トラストモデルとの相性が悪かった。そうした経緯から家族以外の他人を信用せず、自分自身で安全を確保するという考え方が中国では一般的だ。これが後の「ゼロトラスト（信頼しない）」指向につながる。

従来型のトラストモデルには 2 つの問題がある。1 つは、いったん信頼性が揺らぎ始めると修復するのが難しく、システムが一気に崩壊してしまう可能性が高まることだ。

諫山創氏による著名な漫画作品『進撃の巨人』は、巨人から守るために作られた高い城壁の内側で 100 年間維持されてきた生活圏が、城壁が破壊されることにより一瞬にして崩壊するストーリーが描かれている。インターネットの普及と職業ハッカーの登場により脅威のレベルが一気に増したことで、これまで完璧に築き上げてきた日本の金融ネットワークの安全神話が大きく揺らいでいる現状は、まさに巨人に攻め込まれる前夜と言えるかもしれない。

もう 1 つの問題は、トラストモデルを守るために外部との連携に厳しい制約を置くこととなり、イノベーションの妨げとなってしまうことだ。

銀行のシステムの一部を他者が利用できるように開放する「銀行 API（アプリケーション・プログラミング・インターフェース）」も、トラストモデルの内側にプレーヤーを引き込むことになるため厳格な審査があり、現状では個人やスタートアップ企業がこれを利用することができない。

また、企業における社内システムを物理的なオフィスからのアクセスに限定しがちなこともトラストモデルの 1 つと言える。その結果、社内にいる人は無制限に信用してしまう（LAN ケーブルに細工した攻撃者を受け入れてしまう）一方で、テレワークをしようとした社員は物理的に社外にいるため、重要な社内システムから締め出されてしまう。これもトラストモデルの弊害の 1 つである。

■中国流「ゼロトラスト」設計が高度なフィンテックサービスを実現した

中国で始まったゼロトラストの設計思想は、中国企業のアリババ集団や騰訊控股（テンセント）だけでなく、米グーグルや米アマゾン・ドット・コム、米アップルに代表される米情報技術（IT）大手にも採用されている。

またインターネットの通信を暗号化する SSL/TLS 通信（https で始まる URL）は、10 年前にはショッピングサイトの決済画面でクレジットカード番号を伝達するときに主に使われる規格でしかなかった。それが、Wi-Fi（無線 LAN）の盗聴やネットワーク機器への攻撃などに備えて中間者を信用してはいけないという考えが広まるにつれて、暗号化は常時、かつ全区間で行われることが今日の常識となった。

「Suica（スイカ）」や「楽天 Edy」など日本で幅広く利用されている電子マネーで使われている規格「FeliCa（フェリカ）」は、金銭価値情報をカードに持たせるためにフェリカネットワークス（東京・品川）という会社を基点としたトラストモデルを構築している。安全を保つトラストが単一である以上、カードが偽造・変造されたらシステムの安全性は崩壊を免れない。

【関連記事】

- ドコモ口座問題、銀行から漂う「人ごと感」の根深さ
- キャッシュレス不正を防ぐ　個人情報入力、細心の注意
- 銀行と事業者、連携に穴　ゆらぐネット金融の安全

一方、QR コードはカメラやコピー機があれば極めて容易に複製可能であり、これ単体に信用の基盤を置いていない。中国におけるスマートフォン決済サービスの 2 強である「支付宝（アリペイ）」と「微信支付（ウィーチャットペイ）」 は、 QR コードを読み取る

端末に置かれた秘密鍵、位置情報、電話番号、顧客と加盟店の挙動など多くの要素を用いて決済の承認判断を行っている。単一のトラストに依拠したモデルではないのだ。

こうしたゼロトラストの設計思想が、スタートアップ企業による決済端末やオンラインサービスへの参入を容易にした。その結果、ゲームセンターからシェア自転車まで、あらゆる場面で QR コード決済が利用できるようになったのだ。単一トラストモデルを取る FeliCa をベースにした電子マネーが、今もレジや自販機など限られた場所での利用にとどまっており、また信用供与のコストが高いことから決済手数料も中国に比べて高いという状況に置かれているのとは、対照的だ。

そして今回のドコモ口座を利用した不正引き出し事件である。何者かがドコモ口座に他人の地方銀行の口座を登録して口座内の残高を詐取した。この銀行口座登録には、地方銀行が共同出資して NTT データに委託し運営されている地銀ネットワークサービス（東京・中央）が提供するサービスが利用されている。このサービスを基点としたトラストモデルを NTT ドコモが全面的に信用したことにより、口座が不正にひも付いてしまったと言えるわけで、まさにゼロトラストの考えが欠如していたと言わざるを得ない。

■それでも「事故は起こるもの」と想定せよ

もっとも、仮にゼロトラストの設計思想を貫いたとしても、個々の不備を糸口に攻撃を仕掛ける金融犯罪を完全に防ぐことはできない。とりわけイノベーションを担うプレーヤーが多くなればなるほどシステムの「穴」を完璧に塞ぐのは難しくなるし、完璧を求めようとすればするほど、今度はイノベーションのほうが停滞してしまう。そこでアリペイやウィーチャットペイは、ゼロトラストの設計思想を貫きつつも、「事故は起こるもの」と覚悟を決め、いかに当事者に負担をかけず、被害が広がらないよう迅速に解決できるかに力を入れている。

今回のドコモ口座を利用した不正引き出し事件では、被害者はネットバンキングや通帳記入をたまたま行ったことで、異変に気づいた。また NTT ドコモや銀行に被害を訴えても当初の反応が鈍かった。両者ともに金融犯罪を受け付ける専門の窓口はなく、被害者への対応は後手に回った。

アリペイやウィーチャットペイを用いて銀行の口座を利用した場合、アリペイやウィーチャットペイから通知が届くだけでなく、銀行からもショートメッセージサービス（SMS）やプッシュ通知、対話アプリのメッセージなど複数の手段で利用が通知される。犯罪

者がこうした通知のすべてを止めることは困難であり、犯罪の抑止効果が認められている。またアプリ上には、「不審な取引を通報」「安全センター」などのリンクが目立つ場所に用意されており、ワンタッチで専門部署からのサポートを受けられるようになっている。

被害の迅速な回復にも力を入れている。アリペイでは人工知能（AI）による被害の自動査定プログラムを導入しており、カスタマーセンターに連絡してから最短 5 秒で被害額が補てんされる。ウィーチャットペイでは金融被害に気づいたときに攻撃者にパスワードを変えられてしまうなどスマホの制御が奪われている可能性を考慮し、「友達に凍結を手伝ってもらう」機能が用意されている。また過去のパターンと比べて決済額が大きいなどの疑わしい取引をしようとした場合、取引そのものを保留したり、追加の本人確認を要求されたりすることもある。

日本の金融システムは、「システムは完璧であり、システム起因での犯罪は起きないもの」との前提ですべてが設計されている。このため、例えば銀行には、利用者が金融犯罪の発生を連絡するための電話番号や専用の問い合わせフォームは用意されていないことが一般的だ。しかし、インターネットを経由して世界中から攻撃されるリスクや、「モアタイムシステム」など 24 時間の接続が当たり前となり営業時間外であってもセキュリティーへの一次対応が必要となった今では、中国同様、ゼロトラストの設計思想へと転換し、万一の際の通報フローの整備を取り入れ、「事故は起こるもの」との意識を持つことが重要なのではないだろうか。

（インターネットプラス研究所所長　澤田翔）

［日経クロストレンド　2020 年 9 月 25 日の記事を再構成］