「FinTech」時代に資産を守るセキュリティ技術

ヤフー株式会社 ヤフオク!カンパニー
ヤフオク！サービス推進本部 事業戦略部 参謀室
大神　渉　氏

FinTech は、資産のあり方や金融機関の関係性を大きく変容させる可能性を秘めている。また、FinTech におけるセキュリティは、個人の資産を守ることにつながっていくだろう。

そこで今回は、FinTech のコアとなる技術領域やそれを支えるセキュリティについて紹介しながら、変貌するセキュリティのありかたや今後の展望について考えていきたい。

■FinTech とは

FinTech とは「技術（tech）」であるが、「金融（機関）が関われば FinTech」という風潮もあり、革新的な技術であるはずの FinTech がバスワード化しつつある。

FinTech には、革新的な技術がコア部分にあり、その外側に、利便性や基盤整備など、その使用・運用のための関連技術を含んだ「広義の FinTech」があると考えている。コア部分の FinTech は、個人財務管理（PFM）、投資支援（ロボ・アドバイザー）、オンライン融資、クラウドファンディング、経営・業務支援、決済・送金、暗号通貨という 7 分野に分けられる。これらから FinTech の技術的役割を考えてみると、「これまでの金融機関とユーザーの間で実現できなかった新しいお金の流れや関係性を実現する技術」、すなわち、効率化とその還元、お金の価値の最適化・創造、運用スキルの改良、多対多の関係、金融機関の代替／省略といったものがあるといえる。

FinTech における個別の技術は、今までになかったものだけでなく、その組み合わせと活用方法が我々の身近な領域で課題を解決しているものも多い。FinTech によって新たな関係性や価値が生まれた結果、経済活動にも変化が生まれており、広義の FinTech も含め、今後さらに、技術による資産の拡大が注目されていくだろう。

■FinTech のセキュリティ

FinTech におけるセキュリティとは、ユーザーの安心・安全を守る技術領域である。FinTech には既に、公開鍵暗号方式や P2P、取引における異常検知などが存在するものの、なりすまし防止やユーザー認証、ユーザー素性の確認に関する対策は十分でない。

たとえば、脆弱なパスワードが使われることによるなりすまし被害の可能性や、暗号通貨がマネーロンダリングや犯罪資金に流用される可能性に対して、パスワード以外の認証方法や、ユーザーの素性をどう確認するか、といったことが大きな課題となっている。

FinTech のセキュリティには、意図しない取引をさせないことや、実世界における本人確認情報の活用などが求められるのである。

■強固な認証、自然な認証体験

認証には、「記憶」（本人のみが記憶するデータ）、「所持」（本人のみが所持している物）、「生体情報」（本人の特徴を表すデータ）の 3 要素がある。このうち「記憶」要素にあたるパスワードは、セキュリティ的に大きな課題として捉えられている。オンラインでの脱パスワードを目指すための手法としては、FIDO（Fast IDentity Online；ファイドと読む）が注目されている。FIDO は「所持」要素と「生体情報」要素を主要なターゲットとしたオンライン認証を可能にする、セキュアな通信仕様である。FIDO の取組みは世界各国の有名企業が参画し、標準化への取組みが進んでいる。

FinTech では、ユーザー認証だけでなく、その後の取引認証も非常に重要だ。取引認証において、その取引内容（トランザクション）に対してユーザーが真に同意したかどうかの確認については、バックエンド（サーバー側）のセキュリティだけではなく、フロントエンド（UI 側）で適切な実装をしたうえで取引がユーザーが意図したものであることを担保するという工夫も可能である。

また、認証については、入力の煩雑さや困難さなどからユーザーがサービスから離脱してしまう、といったユーザビリティ面での課題もある。ユーザーの心地よさやサービス提供側に求められる責任など多くの要素を熟慮しながら、バランスを探っていく必要がある。

こうした課題に対しては、センサ類の無線化や IoT の普及など、ユーザーの今いる状況を知る手段が増えているため、ユーザーの今の状況に合わせてセキュリティレベルを変えた認証を施す、といったことも可能になってきている。このレベル感を合わせていくためにも、ユーザーとの対話が今後ますます重要になるだろう。

■オンラインでの本人確認

本人確認には、ふるまいは善良だが犯罪などに加担するユーザーがいるかもしれない、という懸念を払拭する役割も求められている。米国などでは、Know Your Customer ルール、すなわち、資金の使い道の履歴なども含め、きちんと顧客情報を把握することが法的に定められている。日本では犯罪収益移転防止法などが関連するところである。

本人確認の確度の担保はオンラインでは難しく、FinTech においては、たとえば確認した本人がアカウントを乗っ取られてしまうこと（なりすまし）や、確認した情報を本人自体が換金・転用することで、資産が奪われたり、犯罪口座になったりする懸念がある。

そうした課題の解決策として、実世界の銀行窓口を活用することが考えられる。全国の窓口で対面による本人確認をし、その結果を、その後のオンラインの認証に利用するというものだ。この方法であれば本人性を担保したサービス提供が可能となる。こうした仕組みと FIDO といった標準技術を組み合わせることで、更にセキュアな FinTech を実現できるのではないだろうか。