金融関連サービスの連携における本人確認の在り方

資金移動業者や証券会社のサービスを通じた銀行口座からの不正出金が相次いでおり、当事者以外のサービス提供者や銀行にとって、本人確認を中心とした様々な機能・手続き等を見直す必要性が高まっている。

本人確認の構成

本人確認は主に「身元確認」と「当人認証」から成る。前者は申告された氏名・住所等の属性情報が正しいことを身分証明書等により確かめること、後者は利用者が申告済の当人であることを認証要素（知識・所持・生体）により確かめることである。いずれも目的に応じ適切な度合いで行う必要がある。

サービス連携における本人確認

昨今、銀行口座保有者が決済サービスを利用しているか否かに関わらず、銀行口座から決済サービスへの不正出金が多発した。これらの要因としては主に「サービス口座開設時の身元確認の非実施」「サービス口座と銀行口座の紐づけ時の当人認証の弱さ」の2つがあった。サービス事業者はサービス口座開設時に適切な身元確認を、銀行は銀行口座とサービス口座を紐づける際に適切な当人認証を行うべきだったのであり、いずれか一方の責任ではない。

上記はあくまで不正事例の1つの形態について、既存の本人確認（例えば、銀行口座開設時に適切な本人確認がなされている等）を省いて、要因のみを取り上げたものである。より一般的に、サービス連携として適切な状態を構築・維持するために、金融機関や他事業者がそれぞれに行うべき対策を挙げると主に次の3つとなる。

1) 身元確認と当人認証について、連携相手任せにせず、少なくとも自社側の範疇において適切な度合いとなるよう実施する。
2) 自社の各種サービスの機能追加や、昨今の不正手口等を踏まえ、各種サービスにおける身元確認や当人認証の度合いを見直す（連携対象のサービスに限らず）。
3) 連携相手に対し、自社の顧客の安心・安全に見合った度合いで身元確認と当人認証を実施していることを照会する。

特に見落とされがちなのが2）である。例えば「Webやスマートフォンアプリ等から利用者の登録電話番号を変更することができる強固でない当人認証を用いたサービス」と「登録された電話番号へのコールバックを当人認証に用いている決済サービス」があると、犯罪者はスマフォアプリ経由で（正規の利用者になりすまして）電話番号を自分のものに書き換えた上で、決済サービスを不正利用することができてしまう。

このように、（郵送・電話等のアナログなチャネルを含む、広義の）サービスにおいて、身元確認や当人認証の度合いが弱ければ、影響が波及する（自社・他社の）サービスの不正につながりかねない、ということに留意すべきである。

本人確認の度合い

各サービスにおいて適切な本人確認の度合いは、「当該サービスのリスク」と「影響が波及するサービスのリスク」の双方を踏まえた上で決定することになる。上に挙げた登録電話番号の例で言えば、前者は主に個人情報の漏洩リスク等であり、裁判例等を踏まえても甚大とまでは考え難い。一方、後者は不正決済のリスクであり、金額次第では甚大なものとなり得る。登録電話番号の変更時の当人認証を決済時と全く同じにするか否かは、具体的な犯罪手口がどの程度成立しやすいか、利便性の低

野村総合研究所　金融イノベーション研究部　©2020 Nomura Research Institute, Ltd. All rights reserved.

NOTE

1) IDの安心な利用環境の整備に取り組む米団体。
2) 電話番号を宛先にメッセージを送付するSMS（ショートメッセージサービス）は、なりすまし等もできなくはない、決して強固とはいえないものだが、不正行為における手間の増加や難度の上昇につながるため、不正の抑制が見込める。
3) APIで広く採用されている標準規格であるOpenID ConnectやFinancial-grade API（FAPI：金融データをサードパーティーに安全に流通させるためのもの）の拡張であり、「どの事業者が確認したか」「いつ確認したか」といったデータ項目と、それらの値（事業者名やタイムスタンプ等）を合わせて電文に含める際の、具体的な仕様。この仕様に則ることにより、金融機関と他の事業者が、精緻な本人確認を行うための様々な情報を遺漏なく安全に連携することが容易となる。

下や運用負荷の増加がどの程度か、といったことを考慮した上で判断することとなる。

もちろん、すべてのサービスにおいて厳しい度合いの本人確認が求められるわけではなく、例えばホームページ等における一般的な情報公開のような、当該サービスのリスクが低く、また波及先もないといったものを、本人確認なしで行うこともあるように、あくまでリスクに応じて調整するものである。

本人確認の度合いの検討・評価等にあたっては、その度合いの段階を区切った「保証レベル」という概念が有用と考えられる。

図表では例として米国立標準技術研究所（NIST）の定めたものを挙げたが、保証レベルを何段階にするか、どのような内容にするかは様々である。外部機関等から公開された定義に対し、例えば端末側に秘密鍵を保持する新しい認証技術（FIDO）の採否によりレベルを細かく刻むといったようなカスタイマイズを加えてもよい。

図表　本人確認の度合いに関わる保証レベル

身元確認の保証レベル（IAL）

IAL1	本人が実在する人物かどうかの確認を実施しない
IAL2	本人確認書類による身元確認をリモートまたは対面で実施
IAL3	対面での物理的な存在確認と専門性を持つ人による本人確認書類の検証を実施

当人認証の保証レベル（AAL）

AAL1	1要素による認証を実施する
AAL2	2つの独立した要素の組み合わせによる認証を実施する
AAL3	2要素かつハードウェア暗号鍵を使用した認証デバイスを使用する

アカウント連携の保証レベル（FAL）

FAL1	アカウントのプロバイダによる署名付きアサーションによる認証連携
FAL2	アカウントのプロバイダによる、署名付きかつ暗号化されたアサーションによる認証連携
FAL3	上記に加え、アサーションと紐づけられた秘密鍵を本人が保有していることを証明できる認証連携

（注）IAL：Identity Assurance Level、AAL：Authenticator Assurance Level、FAL：Federation Assurance Level　2017年6月に発表されたSP800-63-3の第3版で定義された。これらの概念は米国政府機関やその接続企業等を中心に採用されている
（出所）米国立標準技術研究所（NIST）の電子的な本人確認に関わるガイドライン「SP800-63-3」を基にNRIセキュアテクノロジーズ作成

いずれにせよ、サービスを連携させる事業者間や社内のサービス担当者間で共通の尺度を持つことは、円滑かつ遺漏ない認識合わせに有用である。

例えば事業者間でアカウントを連携させる場合は、これらの保証レベルを活用して、以下のような考え方で事業者間のアカウントをひも付けるのが良いと考えられる。

- 最善策：一方（例えば銀行口座のアカウント）と他方（例えば決済サービス口座のアカウント）で最低限の身元確認の保証レベル（IAL）を決める（例えばIAL2以上とする）。双方で身元確認情報が一致した際にアカウントをひも付ける
- 次善の策：一方は強固な身元確認（例えばIAL2）を、他方は、不正なアカウントの作成を抑制する対策（例えばSMS送達確認等[1)]）をそれぞれ実施。身元確認ができたことをもってアカウントをひも付ける

厳しい保証レベルが要求される場合は、さらに「どの事業者が、どのようなフレームワークに基づき、何の情報（根拠）を使って、いつ身元確認をしたか」といった保証プロセスの内容を事業者間でやり取りすることも望まれる。米OpenIDFoundation[2)]は、事業者間でこれらの情報をやり取りする際の電文に関する仕様を検討しているが、いずれはこのような類の仕様[3)]が金融関連サービスに関わる事業者や他の事業者にも広く普及することにより、利用者が安心できるサービス連携環境が整うことが期待される。

Writer's Profile

太田 海 Kai Ota
NRIセキュアテクノロジーズ
上級セキュリティコンサルタント
専門はIT/セキュリティに関するリスク管理
focus@nri.co.jp