フィッシング詐欺対策で見直されるユーザー認証

フィッシング詐欺を抑止するインターネットサービスでのユーザー認証を技術的観点からまとめる。FIDO認証と生体認証の組み合わせは有効かつ利便性が高く、活用が期待される一方で、デバイス紛失などによるアカウントリカバリに関する課題がある。これに対処するためのスムーズかつ確実な運用が求められる。

増加するフィッシング詐欺被害

金融業を中心にフィッシング詐欺の被害が後を絶たない。2019年の報告件数は約1,800件（被害額は約25億円）、翌20年の報告件数は約4倍となり、フィッシング詐欺目的の不正サイトの報告件数とブランド名を悪用された企業数も増加傾向にある[1)]。

フィッシング詐欺とは、正規サービスからの連絡を装って不正アプリの取得や偽サイトへ利用者を誘導し、ユーザーの個人情報や認証情報を入力させて詐取、正規サービスの不正利用により、オンラインで金券購入・口座取引をするなどして金品を奪う行為だ。

フィッシングで使われる“なりすましメール”は、具体的には、メール配送のプロトコルとメールのデータ形式のうち、システム利用する送信元の情報とメーラーで表示する差出人の情報を、送信者が任意に設定できる仕組みを悪用している。近年の巧妙化したフィッシングは、メールのみならず、Smishing（SMS[2)]）、Vishing（IP電話[3)]）、Quishing（QRコード[4)]）等の悪用の手段がある。また、全く別の手法によりアクセス先を偽サイトにすげ替えるPharming[5)]が知られている。

ユーザー認証vsフィッシング詐欺

拡大するフィッシング被害に対してユーザーの認証手段という観点から、その対策について取り上げたい。

認証に使う秘密の情報が、アクセス者とシステム間でそのまま送信されるケースでは、二要素認証であっても突破されることがある。偽サイトで奪取した認証情報を裏で正規サイトに入力し、正規サービスからユーザーに届いた正規のワンタイムパスワードの入力や、ログイン承認のプッシュ通知の押下を促されれば突破される。また、デバイスOS側では、SMSに届いた正規のワンタイムパスワードとユーザーのアクセス先のサービスの紐付けを確認する仕組みも検討されているが、ユーザーがワンタイムパスワードを偽サイトに手入力するケースでは効果はない。

FIDO認証（所持認証）×生体認証の仕組み

こうした不正を防止する観点から、フィッシングを抑止する組合せによる認証が注目されている。

認証は、一般に「知識認証[6)]」、「所持認証[7)]」、「生体認証[8)]」の3つに分類され、このうちの2つを組み合わせた二要素認証で、突破の難易度を高めるという考え方がある。

なかでも最近、注目されるのは、所持認証にFIDO認証[9)]を採用し、生体認証にデバイスの機能を組み合わせた認証である。デバイスの機能には、AppleのTouch ID、Face ID、Androidの顔認証や指紋認証、MicrosoftのWindows Helloなどがある。

この組合せは、秘密鍵と公開鍵を作成し、デバイス側とサービス側で共通の秘密をもたない状態で認証が進む[10)]。仕組みはこうだ。

まず、事前にサービスで利用設定をする。対応関係にある電子証明書を作成してデバイス側とサービス側で保存する。また、デバイス側で、サービスを特定する情報と、ユーザーを特定する情報を保存する。

認証は、認証を要求するサービスと、デバイス側の

NOTE

1) フィッシング対策協議会フィッシングレポート2020, 2021, https://www.antiphishing.jp/report/wg/
2) スミッシング。偽サイトや不正アプリ取得のURLをSMSで送る。仕様を悪用し、正規サービス事業者のスレッドに挿し込む事例もある。
3) ヴィッシング。IP電話の発信元情報の任意の設定を悪用した偽装。不正なURLへ誘導する効果が他よりも高いとの報告もある。
4) クィッシングなど。偽QRコードをメール添付してURLや添付ファイルをチェックするセキュリティシステムをすり抜けて受信させる。
5) ファーミング。ネットワーク情報を操作し（DNSサーバやプロキシサーバの工作、マルウエア等によるhostsファイル変更）、正規サイトのドメインを偽サイトのIPアドレスに替える。
6) パスワード、PINコードが該当。
7) ICチップ入りカード、トークン（ハードやソフト）、スマートフォンなどのデバイス（電話やSMSでワンタイムパスワード通知・ネイティブアプリのプッシュ通知）、電子証明書が該当。
8) 指紋、顔、静脈、虹彩、声紋、外耳、心臓（心電図、動き）、歩行・口の動き等が該当。
9) ファイド。標準化団体FIDO Allianceの技術モデル。
10) W3C First Public Working Draft "Web Authentication: An API for accessing Public Key Credentials Level 3", 27 April 2021
11) 総務省、マイナンバーカードの機能のスマートフォン搭載等に関する検討会（第8回）。
12) Multiple Authenticators for Reducing AccountRecovery Needs for FIDO-Enabled Consumer Accounts, June 2020

サービスを特定する情報との一致を検証した後に進む。デバイス側の電子証明書の機能解除として生体認証をし（操作者が、顔や指をかざす）、インターネット上で電子署名付きの結果のみを通信する。

認証結果は、サービスが対応関係にある電子証明書で検証し、操作者が利用設定時のユーザーであることを確認する。認証結果にユーザーを特定する情報を含むため、サイトへのユーザーIDの入力は不要になるというわけである。

マイナンバーカードで利用できる公的個人認証サービスは、所持認証に電子証明書を取り入れている点で、これと似た仕組みを持っている。知識認証（PINコード）を組み合わせているが、ICチップに顔写真のデータがあるため生体認証（顔認証）も活用できる。

さらに、現在、総務省においてマイナンバーカード機能のスマートフォンへの搭載[11]が検討されており、スマートフォン向けの電子証明書の発行によって様々な手続きがスマートフォンひとつで完結できることを目指している。スマートフォンに搭載されるセキュアエレメント（外部からの解析、読み取り、改変に対して耐性のある領域）に電子証明書を安全に格納しつつ、生体認証機能を活用することで安全性と使いやすさを両立させる方針だ。これにより、公的サービスを起点とした利用シーンの広がりが、期待される。

アカウントリカバリに関する課題

ただ、こうした認証の組み合わせは、デバイスの紛失、買い替えで認証ができなくなるという課題がある。このアカウントリカバリのベストプラクティス[12]として、次のような方策がある。

①事前に、この認証を使える複数のデバイス（PC、タブレット、専用外付けデバイス）を設定する
②ユーザー登録時の本人確認以上の厳密さで、アカウントリカバリの申請者が当該ユーザーであることを確認し、認証を再設定させる

②は、窓口への身分証の提示、SIMカードの回線契約情報の利用など、サービス提供者で独自の取り組みが求められる。フィッシング耐性の劣る、他の認証を許容しないサービス提供者は、①②の対応が必要となる。一方、フィッシング耐性の劣る認証の併用を許容するサービスでは、その認証を使った再設定を促すケースがある。

まとめ

フィッシング詐欺対策が必要な金融サービスでは、フィッシング耐性が高く、ユーザーにとって利便性の高い認証を提供することが求められている。利便性の高い手段としてスマートフォンやデバイスに搭載の生体認証を活用することが期待されるが、その場合はこれまでよりもアカウントリカバリの運用を、スムーズかつ確実な方法とする必要がある。サービス提供者はサービス内容の全体を踏まえて認証を検討する必要がある。

Writer's Profile

吉川 由希子 Yukiko Yoshikawa
NRIセキュアテクノロジーズ
シニアセキュリティコンサルタント
専門は、CIAM・認証認可
focus@nri.co.jp