opentext™

パスワードレス認証方式の概要

opentext™

目次

opentext™

「2024 年はパスワードレスソリューションの本格的な動きが見られる年になり、パスワードレスソリューションに対する需要はこれまで以上に速いペースで伸びていくでしょう」[1]

概要

認証とは、内部ユーザーと外部ユーザー双方のデジタル識別情報を検証することです。認証は組織のセキュリティに不可欠な要素です。今日では、事実上すべての情報がデジタルで作成され、デジタルで保存されています。そして、デジタルの環境は広範囲に分散していると同時に、緊密につながっています。そのため、悪意を持つ外部ユーザーから組織を保護するためのパスワードレステクノロジーの必要性が、かつてないほど高まっています。

パスワードレス認証では、セキュリティを強化できるだけでなく、資格情報を記憶したり、小さなタッチスクリーンに入力したりする負担が軽減されるため、認証プロセスを簡素化できます。指紋認証や顔認証などを利用することで、認証プロセスははるかに簡単になります。

過去 10 年間、パスワードレステクノロジーが求められてきたのは、二要素認証を義務付ける政府の規制に準拠するためでした。多くの組織がリスクベースの多要素認証の実装を進めている現在、パスワードレステクノロジーの必要性は拡大の一途を続けています。ユーザー名とパスワードを用いた従来の方式に代わるものとして、生体認証技術やパスキー技術の人気がますます高まっています。本書は、強力な認証方式の有効活用を求めている組織に有益な情報を提供することを目的としています。

1 Beta News、『Securing the world of tomorrow: Anticipating the IT security topics of 2024 and beyond』、2024 年

opentext™

パスワードレスフットプリントの拡大

パスワードが事実上の標準ビジネス資格情報となっているのは、パスワードの作成と利用が非常に簡単だからです。しかし、ハッキング、ソーシャルエンジニアリング、その他の戦略によって、推測したり盗んだりすることも簡単です。また、強度が弱いパスワードが使われたり、同じパスワードが複数のアカウントで再利用されることもよくあります。文字ベースの資格情報は、マルウェア、特にフィッシング攻撃の主要な標的になっています。

資格情報の侵害は、ほとんどのデータ侵害の基盤となっています。完璧に安全な認証方式はありませんが、パスワードレス認証の資格情報のフィッシングははるかに困難で、従来のパスワードよりも大幅に改善された認証方式と言えます。

パスワードレス認証は、セキュリティの面で優れているだけでなく、便利さや柔軟性の面でも優れています。さまざまなアカウントの複数のパスワードを覚えて管理する必要がなくなります。その代わりに、指紋やセキュリティキーなどの単一の認証要素を使用して、識別情報を検証できます。シングルサインオンを採用すれば、アクセスをさらに効率化できます。

また、従来の認証方式と比べて、パスワードレス認証のほうが通常、速くてシンプルです。認証方式によっては、ユーザーは1回タップまたはクリックするだけで、システム、サービス、デバイス、およびその他のリソースにアクセスできます。

認証方式の評価

認証方式または認証デバイスを選択する際の基準を以下に紹介します。組織にはそれぞれ独自の環境と優先事項があるため、本書は、単に記載内容に従って選択することを指示するものではなく、意思決定者またはインフルエンサーが参考に使用するものとして想定されています。

ユーザー要件

オフィス環境のセキュリティを確保することは比較的容易ですが、業務の全部または一部をリモートで行うことが世界的なトレンドとなっています[2]。このようなリモート環境では、機密情報へのアクセスを容易できるようにし、なおかつセキュリティを確保することが課題となることがよくあります。使用可能なデバイスの種類や、ユーザーはリモートオフィスにいるのか、さまざまな状況が考えられる現場にいるのか、移動中なのかといったことを検討する必要があります。

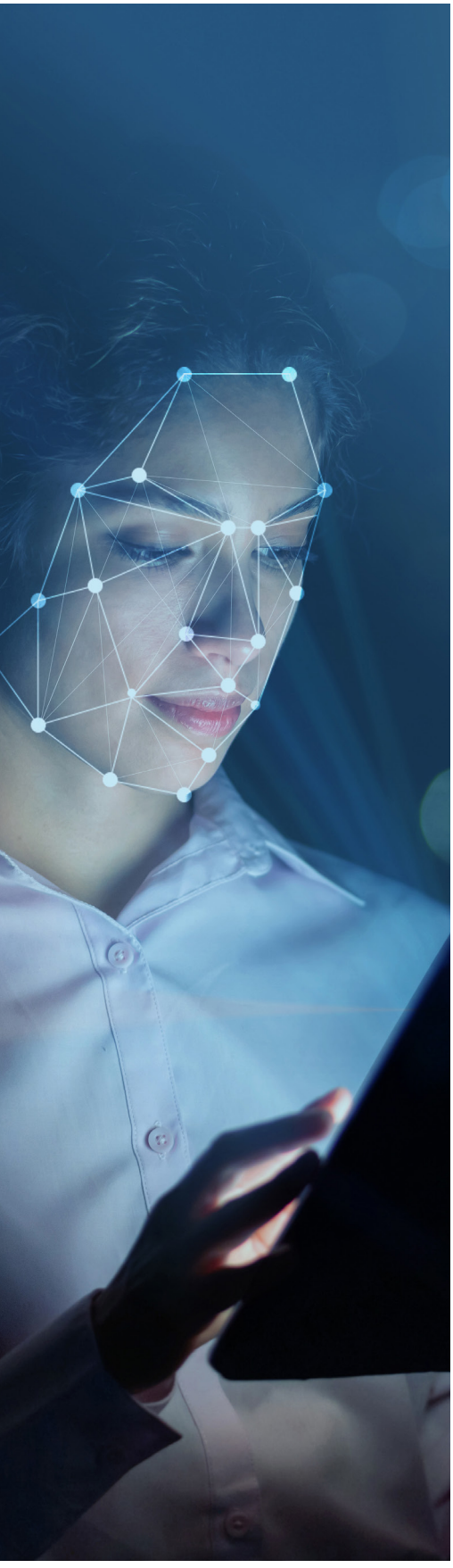
投資とコスト

コスト計算の際には、ライセンス料のほか、配送料、取扱手数料、ベンダーサポート料などが頭に浮かびますが、他の要因のほうが高くつくこともあります。

一般的なコストのポイントは次のとおりです。

- **導入コスト**
  物理デバイスの設定とユーザーへの配布、ユーザーに対する物理デバイスの使い方のトレーニングなどのコストです。通常、ハードトークンのような物理的な方式の場合、特にユーザーが地理的に分散している組織では、導入と物流のコストが高くつきます。

2 Werc、『Adapting to the New World of Work: Remote Work Trends Across Global Reasons』、2023年



- **メンテナンス**
  管理者が物理的に割り当てる必要があるデバイスは、導入時、交換時、トラブルシューティング実施時のいずれの際にもコストがかかるうえ、拡張性もあまり高くありません。にもかかわらず、組織によっては、セキュリティ要件も物理的な要件も満たしているという理由で、このようなハイタッチデバイスを選択しています。理想としては、リスクの高い環境にいるユーザーには特定の認証タイプを用意し、それ以外のユーザーには別の認証タイプを用意します。一元的な管理ポイントを確立してテンプレートとポリシーをトップダウンで管理し、セルフサービスを実装してユーザーが自分のアカウントを管理できるようにすれば、メンテナンスのコストを削減できます。
- **ソフトコスト**
  数値化は難しいものの、ソフトコストは現実に存在します。ソフトコストは、認証の信頼性の低さや煩雑さによる生産性低下などの指標で測定されます。組織によって環境はそれぞれ異なるため、どのビジネスプロセスが重要なのか、そしてそのプロセスへのアクセスが複雑なためにどれだけの価値が失われているのかを見極める必要があります。B2C 取引の場合、よくある資格情報の問題は、利用者が何回かアクセスを試みても成功しないために、処理や取引を打ち切ってしまうことです。

ユーザーの受け入れと潜在的な抵抗

新しい認証方式の採用に対する抵抗には、2 つのレベルがあります。

1. 経営陣 / 出資者レベルでは、パスワードレス方式がもたらすメリット (セキュリティや利便性の向上など) が認識されていないことがよくあります。
2. ユーザーレベルでは、変化への恐れや、新しいものに対する躊躇が見られるのが一般的です。新しいパスワードレスオプションでは、従来の資格情報の認証に比べて時間がかかるのではないかと心配する人もいます。

最も一般的で、挽回するのが最も難しいミスは、従業員の業務を遅らせたり、顧客を遠ざけたりするような方法を取り入れることです。導入に失敗しないための賢明な安全策は、新しいテクノロジーが少なくとも以前のテクノロジーと同等以上に便利であることを保証することです。

たとえば、現在ワンタイム PIN (OTP) を採用している場合、PIN 入力よりもアウトオブバンド (OOB) プッシュのほうが多くの人に好まれるため、ユーザーは OOB プッシュを自然に受け入れるはずです。OTP オプションよりも指紋スキャナーを使用する方を好む人もいます。これは携帯電話でよく使われ、ラップトップへの採用も増えています。

認証方式を別のものに取り替えるのではなく、別のものを追加する方が安全です。既存の認証方式を廃止して、新しい方式を導入するのであれば、十分な準備期間を設けて、しばらくは既存の方式と新しい方式を並行して使用できるようにし、廃止は段階的に行うと効果的です。この準備期間中に、エンロールメントや認証に関する報告を参考にしながら、採用率を常時モニタリングすることが大切です。

リカバリおよびその他のサポート

資格情報が原因で、認証されたユーザーが業務を妨げられたり、ユーザーによる利用ができなくなったりする事態があってはなりません。PIN のリセット、更新された証明書の取得、検証済みデバイスの交換など、もしもの場合にユーザーが対応できるプロセスを用意する必要があります。また、例外的な事態が発生したときのために、別の認証方式を利用できるようにしておくのが理想です。

opentext™

セキュリティ

使いやすさだけでなく、フィッシング、マルウェア、ソーシャルエンジニアリングなどの脅威を防ぐ機能の点でも、認証方式を評価する必要があります。認証方式によっては、適切なレベルで識別情報の検証を行うために、低リスクのリソースには適しているが高リスクのリソースには適していないと考えられる場合があります。

セキュリティチームは、さまざまな状況で各種の認証方式を継続的に評価する必要があります。認証方式が不適切に実装された場合、セキュリティが損なわれます。実際の運用が、管理のセキュリティや、ガバナンスの継続や、強制的適用を危うくする弱点になることがあります。例外的なケースを考慮に入れながら、運用を検証し、定期的に見直すことが重要です。

認証タイプと考慮事項

パスワードレス認証市場の収益は 2024 年には 200 億ドルを超え、5 年以内には倍増すると予測されています[3]。こうした需要によって急速に変化が進むことになるため、認証方式に関する包括的なガイドはすぐに時代遅れになってしまいます。本書は、網羅的なリストではなく、さらなるリサーチの土台となることを目的としています。

ユーザーベースで認証が必要とされる状況はさまざまであり、使用するデバイスも異なるものであるかもしれないことを忘れないでください。無理なく提供できるオプションが多いほど、ユーザーが各自に最適なオプションを使える可能性が高くなります。

ますます巧妙化する攻撃から身を守るため、リスクとユーザー行動を継続的に評価して必要な認証を判断する方式に移行する組織が増えています。セッション中に何度も本人確認を行う必要があるかもしれないユーザーからすると、パッシブ認証やフリクションレスに近い認証方式をより多く利用できる環境であればあるほど、利便性が高まります。パッシブ認証オプションでは、セキュリティインフラストラクチャでユーザーのものとされる識別情報の再検証が行われ、ユーザーの作業を中断させることはありません。

従来のユーザー名 / パスワード方式

ユーザーは、デジタルデバイスやサービスを初めて使ったときから、ユーザー名とパスワードで本人確認をするように教えられています。ユーザー名とパスワードを用いる方式は、シンプルで使い慣れている人が非常に多いため、これからもしばらくは認証方式の主力であり続けるでしょう。

この従来の資格情報が支持されている最も強力な理由の 1 つが、事実上すべてのプラットフォーム、アプリケーション、サービスでデフォルトでサポートされていることです。そのおかげで、専用のハードウェアやソフトウェア、インフラストラクチャに投資する必要がないため、初期投資要件が大幅に軽減されます。通常、このデフォルトのインフラストラクチャは非常に拡張性が高く、大規模な組織や大手企業にとっては安全な選択肢です。

3 Statista、『Passwordless authentication market revenue worldwide from 2021 to 2030』、2024年

opentext™

ハードトークン

ハードトークンを使用した認証では、時間ベースの PIN を表示できるハードウェアデバイスが使用されます。ユーザーは、ハードトークンが割り当てられた後、ログイン時に表示される時間ベースの PIN を使用して認証チャレンジに応答します。

そのバリエーションとして、OATH (オープン認証) ベースのハードウェアトークンでは、HOTP (HMAC-based One-time Password：HMAC ベースのワンタイムパスワード) や TOTP (Time-based One-Time Password：時間ベースのワンタイムパスワード) などのオープンスタンダードを使用して PIN やコードを生成します。OATH ベースのハードウェアトークンは、オープンスタンダードであるため、一般的に従来のトークンより使いやすいと考えられています。また、OATH 規格によって、これらのトークンの汎用性が高くなり、互換性のあるサービスやシステムの範囲が広がっています。

ハードウェアトークンの使用は、かつては二要素認証の主力方式でしたが、現在でははるかに特殊化されています。ハードトークンは強力なセキュリティを提供しますが、使い勝手の悪さとオーバーヘッドコストが原因で使用が限られています。

- エンロールメントは手作業でのプロセスとなり、管理者が手動でデバイスをユーザーに割り当ててからユーザーに送付する必要があります。
- トークンにサポートやトラブルシューティングが必要な場合は、ユーザーがデバイスを IT 部門に送り返さなければならないことがあります。

ハードトークンが普及したときに比べて、現在では多要素認証の使用がはるかに浸透しているため、コストと管理オーバーヘッドを制御するため、組織全体に他の認証タイプも導入する必要があるかもしれません。

opentext™

リモート環境では、アクセスを容易にできるようにし、なおかつセキュリティを確保することが固有の課題となることがよくあります。

モバイル SMS：ワンタイム PIN

現在、SMS (Short Message Service) のワンタイム PIN (OTP) は、最もよく使われている二要素認証タイプです。ほとんどの社会人がスマートフォンを所有し、日常的に SMS を利用することが多いため、シンプルで身近なアクションとして普及しています。人が常にスマートフォンを携帯しているという事実をうまく利用する形となっています。

SMS ベースの OTP セキュリティモデルには、次の 3 つの基礎があります。

- 所有者の識別情報は、電話番号に関連付けられている特定の SIM (Subscriber Identity Module) カードまたは内蔵の eSIM にその情報が割り当てられたときに検証されます。
- OTP は、最初にユーザー資格情報を入力したときとは別の経路で受け取ります。したがって、資格情報がハッキングやフィッシングの対象となっても、SMS PIN のセキュリティに影響はありません。
- OTP は一般的に 4 ～ 6 桁の長さで、ほとんどの場合、時間ベースのワンタイム PIN (TOTP) です。PIN は有効期限が切れると、本人確認に使用できなくなります。

モバイル SMS ベースの OTP は強力なセキュリティを提供しますが、脆弱性も存在します。SMS メッセージの傍受によって OTP が漏洩する可能性があるため、中間者攻撃が脅威となります。SIM スワッピングもリスクであり、ソーシャルエンジニアリングの被害を受ける可能性もあります。

モバイルアプリへのアウトオブバンドプッシュ

アウトオブバンドプッシュモバイルアプリ認証は、SMS と異なり、電話番号ではなく特定のモバイルアプリが主要アイデンティティプロバイダー (IdP) に関連付けられます。これらのアウトオブバンドモバイルアプリは SMS と同様に、通常はアウトオブバンドプッシュ通知を受信したときにワンタイム PIN や承認オプションをプッシュします。

この通知は暗号化プロトコルを使用して送信されるため、この方式のほうがセキュリティレベルが高くなります。さらに、ほとんどの場合、PIN を入力するよりもプッシュ通知を承認するほうが速くて便利です。

ただし、この方式には、攻撃に対する耐性がありません。通知の暗号化によってメッセージは保護されますが、ユーザーのデバイスが侵害を受けたり盗まれたりした場合、攻撃者が不正な認証を試みて承認できてしまう可能性があります。さらに、ユーザーが正当性をあまり検証せずにリクエストを承認してしまう可能性もあります。

近接型カード (プロキシミティカード)

プロキシミティカードは、一般に近接型カードまたはキーカードと呼ばれ、アンテナから近距離でカードリーダーに無線でデータを送信することで機能します。データは、リーダーによってコード (通常は PIN) として読み取られ、認証システムに送信されて検証されます。カード内部に埋め込まれたチップにより、必要に応じて簡単に再プログラム (有効化、無効化、変更) することができます。

こうしたカードは非常にシンプルで迅速に使用できるため、次の用途によく使用されます。

- **物理アクセス制御：**建物の入退室管理、制限区域、駐車場
- **論理アクセス制御：**コンピューターネットワーク、安全なアプリケーション
- **キャッシュレス決済：**公共交通機関、自動販売機、カフェテリア
- **ロイヤルティプログラム：**会員 ID、ポイント追跡
- **勤怠管理：**従業員の出退勤、労働時間の追跡

近接型カードは高速でシンプルですが、セキュリティには限界があります。送信データが暗号化されていないため、傍受されて複製される可能性があります。また、盗難の可能性もあり、現在の所有者が承認されたユーザーかどうかを検証する手段がありません。

このため、近接型カードは通常、決済システムや物理アクセス制御ポイントに使用されます。さらに高レベルのセキュリティが必要な場合は、一般に生体認証や PIN などの別の方式が追加されます。

スマートカード

スマートカードには、機密データを暗号化して暗号化操作を実行するセキュアなマイクロチップが搭載されているため、近接型カードとは異なり、改ざんやマルウェア攻撃に対する高い耐性があります。これらのチップのストレージサイズや処理性能はさまざまですが、セキュア情報 (通常は証明書) が必ず含まれています。

スマートカードはリーダーに挿入することで起動します。このときに証明書が検証され、多くの場合、サインインのもう 1 つの要素として PIN が使用されます。セキュリティレベルの高いこのカードの欠点は、高価な管理システムが必要になることです。

指紋認証

指紋認証は、最もよく使われているパスワードレス認証タイプになっています。スマートフォンや安全なモバイルアプリのロック解除を目的として導入されていることがよくあります。指紋認証はスピードと利便性に優れているため、OTP や顔認証よりも普及しています。

指紋などの生体認証は、次の理由で多くの組織にとって魅力的です。

- ユーザーが複数の資格情報を覚えたり、それらの資格情報を忘れた場合にその問題を解決する操作を行ったりする作業負荷が解消されます。
- ユーザーユニークであり、偽造が困難です。
- 通常パスワードを入力するよりも速いため、よりスムーズなユーザーエクスペリエンスが得られます。

過去にハッカーが指紋認証を突破した事例があるため、セキュリティニーズを満たせるかどうかを判断するには注意が必要です。すべてのスマートフォンリーダーが同じテクノロジー (静電容量式、光学式、超音波式) を使用しているわけではないことに注意が必要です。特にモバイル BYOD の場合、指紋の使用を多要素認証に限定する必要があります。

指紋認証には多くの利点がありますが、モバイル端末を除く利用では、コストと導入時の物流の問題に直面します。指紋認証をラップトップやタブレットに拡張することは、さらに困難です。現在、市場規模が 35 億ドルを超えて成長しているため [4]、指紋リーダーの搭載はラップトップを含む電子デバイスで一般的になりつつあります。つまり、指紋認証を採用するには、新しいハードウェアデバイス (ラップトップまたは FIDO リーダー) の購入が必要になります。

顔認証

ビジネスの世界において、顔認証を用いたパスワードレス認証はまだ初期段階にあります。適切なセンサーセットを搭載したハードウェアに依存している点を別にしても、プライバシーの懸念があるため、いまだに使用範囲が限定されています。ラップトップ / デスクトップでの顔認証はやっと広がり始めたばかりです。一方、モバイルデバイスでは、顔認証がはるかに普及しています。両者の主な違いの 1 つは、ラップトップ / デスクトップが企業所有であることが多いのに対し、スマートフォンは通常ユーザー個人が所有している点です。そのため、プライバシーの懸念がなく、ユーザーは自分のデバイスに自分の顔を登録することに抵抗がありません。

スマートフォンユーザーは、次のようなシーンで顔認証の利用をする機会が増えています。

- **スマートフォンのロック解除**：顔認証の最も一般的な使用法です。
- **モバイルマネー取引**：一部の銀行アプリや決済アプリは顔認証に対応しています。
- **アプリ認証**：代替ログイン方式として顔認証を使えるアプリが増えています。

企業での採用は徐々に増加しており、次のような用途が最も一般的です。

- **アクセス制御**：建物への入退室管理、制限区域、機密データへの従業員のアクセスを安全に許可します。
- **勤怠管理**：時間追跡と出退勤管理を自動化します。
- **不正防止**：国の識別情報データベースに対するユーザー検証と認証を行うことで、システムや財務データへの不正アクセスを防止します。

4 Markets and Markets、『Fingerprint Sensors Market Size, Industry Report, Trends, Growth Drivers, Opportunities, 2030』

チャレンジレスポンス / ナレッジベース認証

チャレンジレスポンス方式 (ナレッジベースとも呼ばれる) ログインは、最も需要の大きい非暗号化バックアップ認証方式の 1 つです。この方式は、メインの認証方式を使用できない可能性のあるユーザーにとって便利な代替手段となります。この方式は、事前にユーザーが秘密の質問と回答のペアを登録してからでないと機能しない点に注意してください。

チャレンジレスポンス方式によるログインが許可されているユーザーには、事前に登録したいくつかの質問 (「チャレンジ」) が提示され、正しい回答 (「レスポンス」) を入力する必要があります。この方式は、複数の正答が必要であるため、ユーザー ID/ パスワード方式よりも安全であると考えられています。ただし、他のテキストベースのプロセスと同様に、チャレンジレスポンス方式でも傍受や覗き見の被害を受ける可能性があります。

ジオフェンシング (パッシブ)

ここまで説明してきた認証タイプは、ある程度のユーザーへの負担があります。つまり、ユーザーが本人確認を行うためにアクションを実行する必要があります。生体認証のオプションは負担が少ないものの、セッション中に継続的に認証がアクティブになるような強固なセキュリティを必要とする状況では、ユーザーの作業を中断させることになります。パッシブ認証の場合、一切の操作なしにユーザーの識別情報を検証できるというメリットがあります。

ジオフェンシングとは、認証対象の本人確認を行うデータポイントとして、位置情報テクノロジーを使用する方式です。たとえば、従業員がオフィスまたは企業敷地内でイントラネットの認証をするときに、ジオフェンシングテクノロジーを使用することで、従業員が実際にそこにいることの確認ができます。

さまざまな位置情報テクノロジーがありますが、最も使用されているのは、衛星ベースのナビゲーションシステムであるグローバルポジショニングシステム (GPS) です。スマートフォンには一般的に GPS 受信機が搭載されており、収集した座標をモバイルアプリでキャプチャして位置を検証できます。

パッシブ認証タイプであるジオフェンシングは、多要素認証の第 2 要素に適しています。ただし、ユーザーが認証可能な「許可された」ロケーションを決めて設定を行うのに時間がかかる場合があります。それでも、モバイルユーザーにとって、ジオフェンシングは適切な認証強度を設定するのに有効です。

Bluetooth (パッシブ)

Bluetooth テクノロジーもジオフェンシングと同様の使い方をすることができますが、この場合は地理的な境界ではなくデバイスへの近接を感知します。ユーザーは、ラップトップとスマートフォンをペアリングするなど、Bluetooth 対応デバイスを登録します。スマートフォンが Bluetooth の通信範囲外にあるか無効になっている場合、ラップトップの認証エージェントが認証インフラストラクチャに警告を出します。たとえば、ユーザーが Bluetooth 対応ワークステーションを離れてオフィスを出た場合、ユーザーのスマートフォンが通信範囲外になるとワークステーションが自動的にロックされます。

音声認証

音声認証は、個人に固有である声の特徴に基づいて識別情報を検証する方法です。これは生体認証の 1 つであり、他の生体認証と同様のメリットがあります。他の生体認証方式と同様、音声認証はパスワードよりも高度なセキュリティを提供します。音声はユーザーが忘れてしまうものが何もなく、フィッシングにも耐性があります。

顔認証と同様に、音声認証は、何かの表面に触れる必要がないという点で指紋認証より優れています。ただし、前述の他の 2 つの生体認証方式とは異なり、音声認識では、失敗した場合の代替認証オプションを用意しておくことが重要です。背後の雑音が混じるか、風邪やアレルギーなどの健康状態によって、ユーザーの声が一時的に変わる可能性があります。

AI を使用して偽の声紋を作成できることも、音声認識システムの制限です。組織で音声認証を使用している場合は、追加でナレッジベースなどの他の方式を使用する必要があるかもしれません。他の生体認証方式と同様に、音声認証にもプライバシーの懸念があり、セキュアなストレージと倫理的な使用が求められます。

標準化された認証インターフェイス

認証方式自体のほかに、堅牢でユーザーフレンドリーなパスワードレス環境を実現するための実用的なアプローチを提供する認証インターフェイスと標準規格を、以下に紹介します。これらは、幅広いユーザー要件と状況の下でさまざまなアプリケーションを保護できる、コスト効率の高いフレームワークを実現するための最良の手段です。

RADIUS

RADIUS (Remote Authentication Dial-In User Service) は、リモートダイヤルインユーザーの認証を目的に開発されましたが、現在では OpenID Connect や SAML などの最新のプロトコルを直接サポートしていない Web および内部のアプリケーションやサービスのための一般的な統合ポイントとなっています。

認証管理ベンダーが RADIUS を利用して、自社がサポートしていない認証タイプとの互換性を提供していることがよくあります。RADIUS は、識別情報を検証するための一元化されたゲートキーパーとして機能させることができますが (認証管理を一元化している組織にとって重要)、認可に関する情報を含めることもできます。

FIDO アライアンス

FIDO アライアンスは、オンライン認証におけるパスワードへの依存度を下げるために結成された、オープンな業界団体です。その戦略は、強力な認証のための標準を開発し、促進することです。同団体には、Google®、Microsoft®、Apple®、Samsung® など、250 社の主要ベンダーがサポートおよび協力しています。FIDO アライアンスの推定によれば、現在使用されている FIDO 対応デバイスは 40 億台に上ります。

FIDO Universal 2nd-Factor (U2F)

U2F は、二要素認証 (2FA) に対応するため、外部ハードウェアセキュリティキーをサポートするように設計されています。これらのキー (通常は USB または NFC ベース) には、オンラインサービスごとに固有の暗号キーが格納されます。ログイン時、従来の資格情報を入力した後、セキュリティキーにタッチして 2FA プロセスを完了すると、アクセスが許可されます。

2018 年、FIDO アライアンスは、Client to Authenticator Protocol (CTAP) で U2F ユースケースを更新し、パスワードレス認証シナリオを直接サポートするようになりました。この新しいプロトコルでは、生体認証やセキュリティキーだけで、パスワードをまったく使用せずに Web サイトやアプリにログインできます。CTAP のほうが U2F よりセキュリティが強化されているものの、どちらのプロトコルも十分に高度なセキュリティを提供します。

FIDO Universal Authentication Framework (UAF) および FIDO2

UAF は、パスワードレス認証を実現する FIDO エコシステムをサポートするために設計されました。生体認証 (指紋、顔認証)、PIN、セキュリティキーなど、FIDO デバイスに組み込まれているセキュリティ機能を活用して、従来のパスワードを使わずにオンラインサービスの認証を行うことに重点を置いています。全体として、FIDO UAF はパスワードレス認証の導入において重要な役割を果たし、さらに高度な FIDO2 テクノロジーへの道を拓きました。

UAF は、現在でも安全なログインの有効なオプションであり、古いシステムとの互換性が懸念される場合には特に便利ですが、FIDO2 はさらに拡張され、トランザクションの署名とアサーションの検証に対応しています。UAF はブラウザーベースのプロトコルを使用していますが、FIDO2 はプラットフォーム固有の API を使用してセキュリティを強化しています。そのため、FIDO2 は現在、幅広い機能とセキュリティの強化により新しい実装でよく採用されるアプローチとなっています。

まとめ

入念な計画、経営陣への早期の働きかけ、段階的な導入を行うことで、パスワードレス認証は、組織内のセキュリティと効率を高めると同時に、利用者とのデジタルエンゲージメントを強化するのに役立つようになります。

パスワードは本質的にハッキング、フィッシング、ブルートフォース攻撃に対して脆弱なため、パスワードレス認証を採用すると、機密情報や規制情報の保護において大きな前進をもたらします。100% 安全な認証はありませんが、生体認証や暗号化キーは従来の資格情報よりもはるかに安全であるだけでなく、シンプルでスピーディーです。全体として、パスワードレス認証の導入によって、ユーザーが ID や複雑なパスワードの組み合わせを記憶したり管理したりする手間がなくなります。本書を参照することで、新しいパスワードレス環境への移行や、既存のパスワード環境のセキュリティ強化につながれば幸いです。

OpenText の認証ソリューションの詳細については、YouTube の NetIQ Unplugged チャンネルをご覧ください。

OpenText について

「The Information Company」を掲げる OpenText は、市場をリードする情報管理ソリューションを通じて、お客様がオンプレミスでもクラウドでもインサイトを獲得できるようにします。OpenText (NASDAQ：OTEX、TSX：OTEX) の詳細については、opentext.com をご確認ください。

SNS 情報：

- OpenText の CEO、Mark Barrenechea のブログ
- X (旧 Twitter) | LinkedIn