GMO トラスト・ログイン

第４回

生体認証と次世代の認証方式 FIDO

前回は「ワンタイムパスワード」メソッドについて解説しました。
今回は「生体認証」と次世代の認証方式として期待されている「FIDO」について解説いたします。

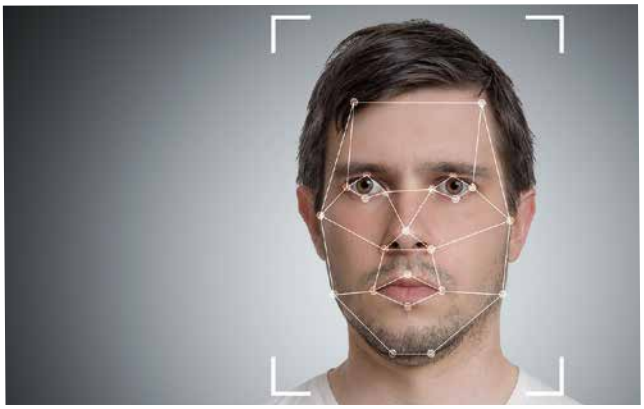
生体認証とは

生体認証とは人の身体的特徴または行動的特徴を使用して認証を行う多要素認証における一つの認証要素です。バイオメトリクス認証とも呼ばれています。生体認証ではどの身体的特徴を使用するか、行動的特徴を使用するかによってさまざまな認証メソッドが存在します。
生体認証を行うには必ず生体情報を読み取るためのリーダーまたはセンサーと呼ばれるデバイスが必要となります。このセンサーデバイスにて指紋情報や静脈情報などをスキャンします。また、顔をカメラで撮影します。また、行動的特徴を使う生体認証では筆跡や声紋を用いて認証します。

生体認証の主なメソッド

認証メソッド	特 徴
指紋認証	指紋情報を使用して認証する。センサーデバイスは様々なタイプがあり指をガラス面に乗せて下部よりセンサーで読み取る、指をボタンにタッチするだけ、指をスワイプして読み取る方法などがある。怪我などで認証できなくなる場合がある。
網膜認証	目の網膜の毛細血管のパターンを認識して認証する。目をセンサーに近接させて網膜情報を撮影する。
虹彩認証	目の虹彩パターンを認識して認証する。網膜と比べて虹彩は目の表面にあるため網膜認証と比べると比較的撮影が容易に行えるためセンサーが小型化できる。
静脈認証	指や手のひらの静脈のパターンを認識して認証する。静脈は加齢による経年変化があっても不変と言われている。
顔認証	顔を識別して認証する。カメラが主なセンサーとなるため容易に実装することができる。加齢や眼鏡の有無によって認識率が低下することがある。
声紋認証	声を識別して認証する。マイクがセンサーとなる。健康状態によって認識率が低下することがある。
掌形認証	手のひらの幅や、指の長さなどを用いて認証する方法。
筆跡認証	サインをする時の軌跡・速度・筆圧の変化などの癖を利用する方法。

生体認証の特徴



生体認証の特徴として個人の生体情報を使用するため記憶や所有と異なり必ず本人が常に身に着けていることであるため、パスワードのように忘れたり、ワンタイムパスワードのようにデバイスを紛失するといったリスクがありません。また、盗まれたり複製されたりといったリスクも低いものとなります。非常に強力な本人確認方法の一つであると言うことができます。
生体認証では本人であるにもかかわらず本人ではないと誤認識してしまうことがあります。これは「本人拒否率」と呼ばれています。また、身体的な欠損や経年変化により認証できなくなることがあります。
生体認証ではセンサーデバイスによっては導入時の初期費用が高額になる場合があります。高額なセンサーデバイスを使用するときは複数の人が共用で利用する場合や、建物への入館時などに利用される場合があります。
一般的にはセンサーデバイスは統一する必要がありますが、指紋認証では異なるセンサーデバイスを利用しても共通に利用できる場合があります。

生体認証の特徴

メリット	デメリット
紛失の心配なし	導入費用高価
忘れる心配なし	認証センサーデバイスの統一
漏洩リスク低い	健康状態による誤認識
複製リスク低い	老齢化による誤認識
認証時の操作が容易	身体的欠損による使用不可

次世代の認証方式「FIDO」とは

「FIDO」とは次世代認証方式を策定するのを目的に設立された FIDO アライアンス（Fast IDentity Online Alliance）という業界団体によって規格化されているパスワードに代わる新しい認証メソッドです。FIDO アライアンスは 2012 年に PayPal など 6 社によって設立されました。日本では 2015 年に NTT ドコモがボードメンバーとして加盟しています。現在は Web 技術の標準化団体 W3C(World Wide Web Consortium) が FIDO を採用したことで今後の Web 技術の標準化の中に FIDO が Web 認証技術として取り込まれていくことで次世代の認証方式として期待されています。

FIDO の特徴

FIDO の特徴は認証をユーザが使用している端末のローカルで実施し、その認証結果のみを認証サーバに送信するという仕組みになっています。これには標準的な公開鍵暗号化方式が採用され端末に保持されているクライアント証明書を端末のローカルで認証できたことでロックが解除され、認証サーバから求められたチャレンジに署名してレスポンスを返して認証されます。この方法では指紋データやパスワードなどの認証情報がネットワーク上に全く流れないことを意味します。また、サーバ側にも認証情報が蓄積されていません。これにより認証情報の漏洩リスクが軽減されることになります。

FIDO対応のUSBセキュリティキー　yubico社

FIDO 1.0 バージョンでは「U2F（Universal 2nd Factor）」と「UAF(Universal Authentication Framework)」の二つの仕様が提供されています。

「U2F」では多要素認証のパスワードの次の二つ目の認証にセキュリティキーを使用して認証を行います。セキュリティキーは USB キー、USB ドングル、Bluetooth デバイス、NFC デバイスの形式で提供されています。主に USB や Bluetooth を搭載した PC での利用を想定しています。U2F のセキュリティキーのうち USB キーは非常に安価に導入が可能でまた電池を必要としていないため定期的な交換が不要です。

「UAF」は生体認証を使用します。「指紋」「顔」「虹彩」「静脈」等が使用可能です。主にモバイル端末にセンサーデバイスを搭載しモバイル端末の中で UAF による認証を可能としています。UAF に対応した認証サーバであれば認証に使用するモバイル端末がどの生体認証方式を使用していても共通で利用することが可能です。認証自体は端末内部で実施しその結果だけを認証サーバに送信されるため異なるメーカーの端末で一方は指紋認証、他方は顔認証を採用していても利用することができます。これは前段の生体認証で説明した同一メーカーのセンサーデバイスを利用しなければいけないといった生体認証のデメリットを解消することになります。また、「UAF」では認証に使用する端末の中に認証情報を持っているため生体情報で認証されたことに加えてその端末を所持しているということも併せて証明されたことになります。

FIDO 2.0 の仕様では「U2F」と「UAF」が統一されることになります。これにより生体認証とセキュリティキーでの認証が一つの認証サーバで実現することが可能となると期待されています。

生体認証の特徴

メリット	デメリット
認証情報をネットワークに送信しない	「U2F」セキュリティキー紛失リスク
「U2F」対応セキュリティキーであれば メーカー問わず使用可能	
「U2F」導入が安価	採用 Web サービスがまだ少ない
「UAF」対応の生体認証付き端末であれば 指紋認証や顔認証など問わず使用可能	

第 4 回　生体認証と次世代の認証方式 FIDO

FIDO による認証の仕組み

1 ログイン

オンラインサービスは、サービスの受け入れポリシーに適合する以前登録したデバイスでログインするように、ユーザーにチャレンジします。

2 ユーザーの承認

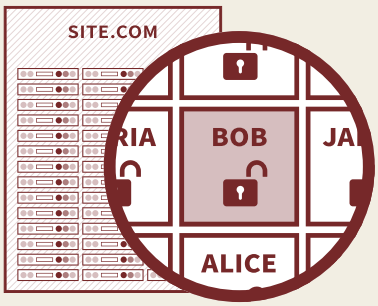
ユーザーは、登録時と同じ方法を使って、FIDO オーセンティケーターをロック解除します。

3 キーが選択される

デバイスは、サービスから提供されたユーザーのアカウント識別子を使って正しい鍵を選択し、サービスのチャレンジに署名します。

Using
PUBLIC KEY CRYPTOGRAPHY

4 ログイン完了



クライアントデバイスは、署名したチャレンジをサービスに返送します。サービスは、保管している公開鍵で確認を行い、ユーザーをログインさせます。

出典 FIDO アライアンス「FIDO の仕組み」より

徐々に普及している FIDO

すでに FIDO をサポートしている Web サービスが登場しています。Google は 2 段階認証プロセスとして FIDO U2F をサポートしています。また Google が提供するブラウザ Google Chrome では U2F の読み取りが可能となっています。Dropbox、Facebook、GitHub、Salesforce などの Web サービスが U2F をサポートしています。マイクロソフトは Windows 10 の認証オプション Windows Hello、Microsoft Edge および Microsoft Passport にて FIDO 2.0 による認証をサポートしています。
このように FIDO のサポートは今後も様々な Web サービスで広がっていくことが期待されています。

お問い合わせ
(GMOグローバルサイン株式会社)
03-6370-6540
support-jp@globalsign.com