インターネット研究所
ハジメ・コトー Jr. 所長

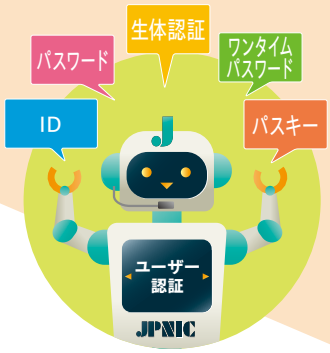
助手ロボット
JP_29 II

インターネットことはじめ

第25回

［テーマ］
ユーザー認証

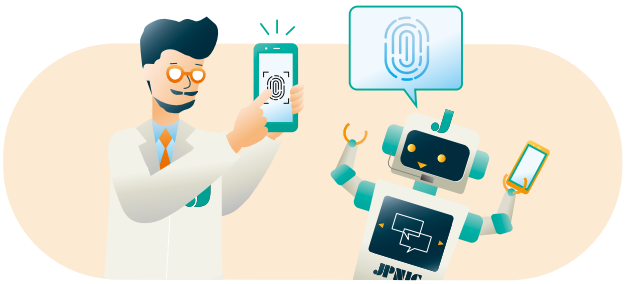
JPNIC



協力:株式会社日本レジストリサービス

ユーザー認証とは

ユーザー認証は、ユーザーがコンピュータやサービスを利用する際に「本当にそのユーザーか」を識別・確認するための、本人確認の手続きです。普段の生活ではあまり意識しませんが、スマホアプリの課金やネットショッピングの利用など、現代のオンラインサービスにおいて、必要不可欠なものの一つです。



初期のユーザー認証

コンピュータ開発当初は、そもそもコンピュータを使えるのは開発者を含めたごく少数の人間だったので、ユーザー認証の必要性はほとんど無かったと思われます。

コンピュータの利用が商用化されても、しばらくの間はバッチ処理として、大型計算機に複数のジョブをまとめて連続的に、休み無く計算させる方法が主流でした。バッチ処理では、コンピュータに処理させたジョブの量に応じて料金を計算することが一般的であったため、誰がどのくらいコンピュータを使ったかを管理する際に、ユーザー認証が必要になりました。とは言え、このぐらいであれば「このジョブはこのユーザーからの依頼」といった、人手による処理でも対応可能でした。

現代的なユーザー認証の始まり

現代的なオンラインでのユーザー認証が必要になったのは、Time Sharing Systemが開発され、1台のコンピュータを複数のユーザーが対話的に利用するようになった時です。また、研究室や部署単位で導入可能なミニコンピュータやワークステーションが開発され、組織アカウントでの共同利用が主流であった大型計算機から、ユーザーごとにアカウントを作成・管理する、個別のユーザー認証が主流になってきました。

この時点で導入されたのが、現在でも一般的な「IDとパスワード」による認証方式です。IDによってユーザーを区別し、本人しか知らないはずのパスワードを入力することによってユーザー本人である、と判断するおなじみの方法です。1961年、マサチューセッツ工科大学（MIT）のフェルナンド・コルバト氏が開発したCTSS（Compatible Time-Sharing System）での採用が嚆矢とされています。

高度化するユーザー認証

2025年時点においてもIDとパスワードによる認証は広く普及しています。ただ、この方式にはIDとパスワードがわかれば別人がそのユーザーになりすますことができるという弱点があります。

この弱点を克服するため、さまざまな認証方式が開発されました。最初に普及したのは1回ごとに使い捨てるワンタイムパスワードでした。ついで、指紋／虹彩／静脈／顔といった生体情報も利用されるようになりました。既にATMやスマートフォン、PCなどでの普及が進んでいます。これらを複数組み合わせる多要素認証も一般的となりました。

そしてここ2年ほどで普及しつつあるのが、パスキーという技術です。これは公開鍵暗号技術の応用で、サービス利用開始時にペアとなる公開鍵と秘密鍵を生成し、公開鍵をサーバに、秘密鍵をユーザーのデバイスに自動的に保存します。サービス利用時には、ユーザーが持つ秘密鍵を使ってサーバが送ってきたデータに電子署名を行い、その署名が正しいかどうかをサーバ側が確認することで、本人であることを確認します。この時秘密鍵を使うには、各デバイスに備わった生体認証やPINコードでの認証をパスする必要があります。

サービスごとに異なる鍵ペアを使うこと、秘密鍵やPINコードがネットワーク上を流れないこと、利用に際し秘密鍵の入った端末が別途必要なことなどから、パスキーはかなり安全性の高い技術となっています。また、生体認証の利用を前提とすれば、いちいちパスワードやPINコードを覚えたり入力したりする必要もありません。

実のところ、テキストベースのリモートログインを行うsshなどのプログラムでは、10年以上前から公開鍵と秘密鍵のペアを使う方法が一般化していました。ただ、鍵ペアの生成や登録などをユーザーが明示的に行う必要があり、これにはそれなりの手間がかかります。対してパスキーは鍵ペアの生成と登録が自動的に行われるのが大きな利点となります。まだ対応したサービスやデバイスは少ないですが、パスキーは今後の普及が大いに見込まれる技術です。

「インターネット歴史年表」も見てね!!
https://www.nic.ad.jp/timeline/

次回はホスティングの予定です。