パスキー（Passkey）

（パスワードからパスキーの時代へ）

JJ1SXA/池

各種サービスやシステムを利用する際にはパスワードを設定することが一般的ですが、問題点も挙げられています、そんな中、パスワードを使用しないパスワードレス認証が注目されつつあり、特に注目を集めているものが「パスキー（Passkey）」だそうです。

パスキーとは、パスワードレス認証基準を普及させる団体である「FIDO Alliance（ファイド アライアンス）によって策定された、新しいパスワードレス認証方法を指し、正式名称は「マルチデバイス対応FIDO認証資格情報（Multi-device FIDO credential）」です。

FIDO-ファイド）は「Fast Identity Online」の略で、従来のパスワードに代わる認証手段として期待される認証技術の一つだ。

パスキーは指紋認証や顔認証といった生体認証を利用することから、安全性と利便性を両立する認証方式なので。従来のパスワードを用いた認証方法に比べて、フィッシング攻撃に対する高い耐性を実現できるようです。

マイクロソフトや、グーグル、アップルも積極的に採用しており、今後は、ログイン方法の主流になる可能性が高いようです。

パスキーの特徴は本人確認をする「カギ」をパソコン内に保存すること、「カギ」は資格情報（秘密鍵）とも呼ばれ、それを使ってログインする際は「Windows Hello（生体認証やPin入力）」による本人確認が要求される、このため、OSとブラウザー（ネットサービス）でログイン方法が共通になる。

パスキー自体は「FIDO（ファイド）」と呼ばれる標準規格に沿った技術で、カギはスマホやセキュリティキーに保存できる、その場合は紛失、盗難に気をつけなければいけない。

パスキーが安全な理由は、ユーザーの目に触れない固有のカギを安全に管理しているからだ、実際には、ペアのRSA暗号カギを使って、水面下で認証手続きが行われている。

パスキーを有効にすると、秘密鍵と公開鍵が作られ、パソコンでは秘密鍵でコードを暗号化、サーバーでは公開鍵でコードを暗号化、パスキーでログインするときの流れは、パソン側からログインを要求すると、サーバーからコードが送信され、パソン内で本人確認をしてコードを暗号化してサーバーニ送信、これをサーバーで復号して検証する、パソコン内のカギはWindows Helloによって安全に管理され、ユーザーの目に触れないので漏れる心配が無い。

「Windows Hello」は、PIN、顔認識、または指紋を使って Windowsデバイスにすばやくアクセスできる、よりプライベートで安全な方法だ。

ちなみに、私のデスクトップパソコンは、Win7から、段階的にバージョンアップしたWin10マシン、顔認識、指紋認識など、それ何？だ、高齢マシンは、高齢使用者とどちらが先にパタンかと言ったところ（hi）

（2023年12月記）