パスワードは不要になるのか？

WebAuthn (Web Authentication)

・W3C(ワールド・ワイド・ウェブ・コンソーシアム) による標準の Web API
・ウェブサイトやデバイス間などで安全に認証する新方式を ユーザーに提供
・FIDO アライアンスと共同で開発され、ユーザーは、簡単にログインが可能
・生体認証を簡単に利用でき、生体情報がネットワーク上を流れない

認証器

・指紋・虹彩などの生体特徴を持つ機器
・セキュリティチップが組み込まれた USB キー
・Android などの端末を利用して認証できる仕組み

かつては重要な業務アプリやクラウドサービスが多くなるほど、定期的に変更すべきパスワードの管理がとても大変でした。
2018 年 3 月､総務省は､国民のための情報セキュリティサイトを改訂し､パスワードの「定期的な変更は不要」と明記して、やっと私たちは沢山のパスワードの変更管理から解放されそうです。これは、2017 年の NIST(米国国立標準技術研究所) の発表したガイドラインにも､「パスワードの定期的な変更を要求すべきではない」とあるように、世界的な常識が変わってきているという証拠です。
但し、こうした傾向は定期的にアプリ側から変更を促され、そのたびに違うパスワードを覚えなければならず、パスワードの作り方がパターン化したり、使いまわしてしまうために更に危険が増すという問題に対処するもので、パスワード自体は、かえって長く複雑な設定を求められるようになってしまいました。背景には、パスワードリスト攻撃やブルートフォース攻撃などのパスワード解読率が上がっていることも原因です。
そして、ネットを使用したアプリではパスワードだけでなく、2 要素認証を求められるなど、一般に生活している IT リテラシーの低い人にとっては、ログイン方法がかえって複雑になってしまい面倒な手続きでハードルが高くなって、利便性が低下し始めていることも事実です。
一方、パスワードが不要な認証方式にもいろいろな手法があり、すでに実施され始めました。
たとえば、FIDO（ファイド）は、パスワードに代わる認証技術で、W3C(ワールド・ワイド・ウェブ・コンソーシアム) によるブラウザ経由でパスワードなしの認証を可能にする WebAuthn（Web Authentication ）という API の標準の仕組みの元になっています。これは、クレデンシャルとなる秘密鍵は認証器に保存されているため、ユーザはパスワードを暗記する必要がなくなり、ネットワーク経路上にパスワードが流れることがないので認証プロセスがより安全になるというメリットがあり、各メジャーなブラウザもすでにサポートしてきています。
ただし、認証器の代表が Android デバイスなどの生体認証や PIN などなので、スマートフォンを落としたら、買い物もできないし仕事もできないという時代になってきてしまいそうです。
この流れに乗って、今後はやはり人間にチップを埋め込むインプラントがトレンドになっていくのでしょうか？