IT時事ネタキーワード「これが気になる！」（第152回）

パスワード変更をユーザーに要求しない新ガイダンスを米国政府機関が発表

2024.11.19

パスワードといえば、パソコンやスマホでネット上のサービスなどにアクセスするために欠かせない認証システムの一部だ。パスワードは、今までその取り扱いが長らく議論され、一般的に「パスワードは8文字以上」「他人に推測されにくい文字列」「大文字小文字に数字や記号を混ぜる」などの他、「定期的に変更する」べき、と言われてきた。

米国立標準技術研究所（NIST）が、新しいガイダンス「SP800-63B」を発表

ところが米国政府機関のNIST（米国立標準技術研究所）による「電子認証に関するガイドライン」の2024年8月の公開草案において、「パスワードを定期的に変更することをユーザーに要求“してはならない”」としたとのニュースが流れ、話題となった。

ちなみにNIST「SP800-63B」の「3.1.1 Passwords」の「3.1.1.2 Password Verifiers」の「6」に、「パスワードの定期的な変更を要求すべきではない」ことと「流出時には速やかに変更する」と書かれている。

とはいえ、長年「パスワードは定期的に変更すべき」が常識、にわかには受け入れにくい気持ちも大きい……。例えば、筆者が使っているネット銀行は、ログイン時に「パスワードが長い間変更されてない」というメッセージとともに、変更画面への案内がパスワード変更の完了まで表示されることがあった。いまだにパスワード設定画面には「パスワードの定期的な変更をおすすめします」と書かれている。

2024年5月リニューアルの総務省「国民のためのサイバーセキュリティサイト」の「安全なパスワードの設定・管理」には、パスワードの重要性を再認識して、適切なパスワード管理を心がけることを示唆するとともに、アカウントを不正に利用されないようにするため、「推測されにくい安全なパスワードを作成し、他人の目に触れないよう適切な方法で保管することが大切」と案内している。そして、この「安全なパスワードの設定・管理」を読んでいたら、ここにもパスワードの「定期的な変更は不要」という記述があり驚いた。「これまでは、パスワードの定期的な変更が推奨されていましたが、2017年に米国国立標準技術研究所（NIST）からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところです」とある。

さらに2023年1月の内閣サイバーセキュリティセンター「インターネットの安全・安心ハンドブック」にも同様の記述がある。というわけで、NISTのガイドラインに基づく「パスワードの定期的な変更は不要」と、政府のサイトで2年近く記述されているものの、ほぼ浸透していない。筆者も上記のニュースで知った次第だ。さらにはNISTが2017年つまり7年も前からパスワードの定期変更不要の方向を示して事実にも驚いた。

頻繁な変更がかえって脆弱なパスワードの使用につながる？… 続きを読む