パスワードは定期的に変更してはいけない！？

5 月下旬、米国国立標準技術研究所（NIST）が新しく発行する『電子認証に関するガイドライン』で、定期的なパスワード変更を推奨しないことを決定した、というニュースが飛び込んできた。NIST のガイドラインは、米国の政府機関がセキュリティ対策を実施する際の指針となる文書として知られている。

かねてよりパスワードの定期変更は、特別の理由がない限りユーザにパスワード変更を求めるべきではないという意見が専門家の間では増えてきていた。そうしたなか、2016 年 6 月、NIST の傘下部門である CSD（Computer Security Division）がドラフトとして発行した文書において、パスワードの定期変更を否定する内容が記述されており、これまでの論争に終止符を打つのではないかと注目されていた。

現在では、多くの人が複数のパスワードを抱えている。NIST がパスワードの定期変更を推奨しないことを決めた背景には、ユーザはパスワード変更時に新しいパスワードを適当に決める傾向がある、ということである。例えば、米国ノースカロライナ大学の調査によると、ユーザは定期的にパスワード変更を求められると、多くの場合、新しくパスワードを作るのではなく、前回と似たパスワードを設定する傾向がある、という結果が示された[1]。つまり、いずれ数カ月後には変更を求められるのであれば、「Password1」のように末尾に数字を追加するなど、規則性が容易に推測できる変更が多くなるということである。

上記ノースカロライナ大学における研究では、単純なパスワードによる認証の放棄と、より長い「パスフレーズ」の採用を求めていた。それがここにきて現実味を帯びてきつつあるということであろう。また、NIST では、最低 64 文字のパスフレーズを推奨するほか、ウェブサイトなどで「パスワードが長期間変更されていません」などの警告を定期的に表示することも止めるように勧告するという。

現在、パスワードはほとんどが半角英数字で作成されているが、コンピュータの性能向上もあり、パスワードを解読することは比較的容易になってきた。他方で、漢字やひらがなどを使う日本語のような 2 バイト文字を解読することは、クラッキングソフト開発を含めた需給関係などもあり、ハードルは高いとされる。

NIST では、さらに秘密の質問も使用するべきでないとしている。今後の認証システムにさまざまな影響を与えることになろう。

（撞球者）

1 Zhang, Yinqian, Fabian Monrose and Michael K. Reiter, “The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis,” ACM CCS October 4-8, 2010