パスワード設定と管理の常識が変わる

◆総務省が「パスワードの定期的な変更は不要」とサイトの記述を見直す

総務省は2018年3月に「国民のための情報セキュリティサイト」でパスワードの設定と変更に関する記述を見直した。総務省はこれまでインターネット上のサービスなどを利用する時に使うパスワードの「定期的な変更」を推奨していた。これを「パスワードを破られてアカウントが乗っ取られたり、サービス側から流出した事実がなければ、パスワードを変更する必要はない」としたのである。

この見直しの理由は、定期的な変更がかえって安全性を低下させるからである。たとえば、変更の度にパスワードを1文字変える、誕生日や名前を組み合わせたパスワードを作って変更の度に順番を入れ替えるなどして、設定のわずらわしさから逃げる利用者が出てくると、ツールを使ってパスワードが簡単に見破られるからだ。この危険は以前から指摘されており、17年6月に米国国立標準技術研究所が、17年12月に内閣サイバーセキュリティセンターがガイドラインやハンドブックを見直していた。今回の総務省の見直しはこれらに追随したものである。

◆見直しで変わる利用者及びサービス提供者のパスワード設定と管理の方法

今回の総務省の見直しにより、パスワード設定と管理の方法が変わってくる。まず、利用者は英数字と記号を組み合わせた12字以上の、個人情報やパスワードとして使われやすい単語以外で作ったパスワードを要求されるようになる。また、情報が漏えいした場合の深刻さに合わせて複数のパスワードを使い分けることが求められるようになる。そして、パスワードが破られたり、流出した場合や、その疑いがある場合は速やかにIDとパスワードを変更することが必要になる。

サービス提供者も安全性確保の取り組みの追加が必要になる。たとえば、①パスワードの設定や変更時に文字数のチェックとともに誕生日や名前、パスワードリストに登録された用語をチェックして警告を出す、②普段と違う端末から利用した場合や、パスワードを複数回間違えた場合に利用者に通知する、さらに、③普段と違う端末で利用する時はID、パスワードに加えて電話等で伝えるもう一つのパスワードの入力を求める二段階認証を行うなどである。　【藤井和則】