「バイオメトリクス認証への過信は禁物」――経産省情報セキュリティ政策室が警鐘

「運用によっては，単なるパスワード認証よりもセキュリティ・レベルが下がる恐れがある。ユーザーは十分注意する必要がある」――。経済産業省（経産省）商務情報政策局情報経済課情報セキュリティ政策室の久米孝課長補佐は 4 月 12 日，IT Pro の取材に対して，バイオメトリクス認証を過信することの危険性を警告した。

バイオメトリクス認証とは，指紋や声紋，筆跡（サイン），顔，虹彩といった，人間の特徴を示す生体情報を使って，ユーザー個人を特定し認証する技術あるいはシステムのこと。

以下，同氏の発言内容をまとめた。

運用次第では“危ない”バイオメトリクス認証

ベンダーの宣伝やメディアの報道を見ると，「バイオメトリクス認証ならば安全」といった表現が目立つ。確かに，バイオメトリクス認証技術自体は有用である。運用次第で，物理的なアクセス（施設などへの入退室）や，ネットワークへのアクセスに関するセキュリティを高められる。

しかし同時に，単なるパスワード認証よりも低いセキュリティ・レベルになる恐れもある。具体的には，バイオメトリクス認証のバックアップとして，パスワード認証を使用している場合である。実際，そのような運用は多いと考えられる。

バックアップ用のパスワードが“落とし穴”

指紋認証を例にとると，いつもは正常にアクセスできる正規ユーザーであっても，指にけがをした場合などは，認証に失敗する可能性がある。そのとき，ユーザーがアクセスできない“まま”ならば問題はない。

つまり，失敗した場合には，管理者に依頼しない限りアクセスできない運用ならば，バイオメトリクス認証によるセキュリティ・レベルを維持できているといえる。

問題は，バックアップにパスワード認証を用意している場合だ。認証に失敗しても，ユーザー自身がパスワードを入力すればアクセスできる運用である。この運用では，バイオメトリクス認証とパスワード認証のどちらでもアクセスできることになる。

つまり，セキュリティ・レベルはより低い方，すなわちパスワード認証と同じになる。さらに悪いことに，パスワード認証だけを使用する場合よりもセキュリティ・レベルが低くなる恐れさえある。この場合のパスワードは，ユーザーの意識では「バックアップ」だからだ。

ただでさえ，ユーザーは覚えるべきパスワードの数が多い。それに加えて，めったに使わないバックアップ用ともなれば，ユーザーは安易なパスワード（例えば，自分の生年月日など）を設定しがちだ。そのパスワードが破られてしまえば，強固なバイオメトリクス認証を破られたのと同様にアクセスされるにもかかわらずである。

高まるのはセキュリティではなく利便性

　バイオメトリクスとパスワードのどちらでもアクセスできるようにしておけば，利便性は向上する。しかし，パスワード認証よりもセキュリティ・レベルが高まることはない。もしそのような運用方法を勧めておいて，利便性ではなくセキュリティが高まるというベンダーがあれば，それは明らかに虚偽を言っている。

　バイオメトリクス認証というと，「何万回に１回しか誤認しない」といった認識率がとかく話題になる。それも大事だが，「認証に失敗したときにどうするか」といった運用の方が実際には重要だ。そのことを十分認識した上で利用しなければならない。

　もちろん，運用の重要性はバイオメトリクス認証に限らない。他のセキュリティ製品でも同じだ。製品に使用されている技術がいくら優れていても，運用がおろそかでは何の意味もない。「この製品を導入しているから安心だ」と思うことで，その製品がない場合よりもセキュリティ・レベルが低下する恐れすらある。

（勝村　幸博＝IT Pro 編集）

２００２年４月１５日付　日経 IT Pro

オリジナルは
http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20020412/1/
をご参照下さい。