解説

「パスワードの定期変更は不要」の波紋
―パスワードの現状とその誤解―

神戸大学大学院工学研究科教授　森井　昌克

1．はじめに

今年の3月に，総務省が「パスワードの定期変更は不要」との発表を行った。現在でも，多くの銀行や証券会社，それにネット通販等，特に資金の移動や重要な個人情報に絡むサイトへのアクセスにはパスワードが用いられ，それを三か月毎等，定期的に変更するように要求される。セキュリティに厳しい学校等でも，成績等を管理する教務システムへのアクセスにもパスワードが用いられ，その定期変更が求められている。直感的には定期変更することによって，パスワードの安全性が増すと考えられる。にもかかわらず，なぜパスワードの定期変更が勧められないのか。本稿ではパスワードの安全性とは何か，安全に運用するためには何が本質なのかについて解説する。

2．パスワードの本質

パスワードとは何か。英語の意味としては「合言葉」と訳されるが，特にパソコンおよびネット関連で使われる用語の意味としては，「IDで識別される利用者が，そのIDを有する本人であることを保証するための文字列」となっている。銀行等のATM（現金自動預け払い機）で用いられる暗証番号と混同される場合も多い。

パスワードと呼ばれる符合が使われてから半世紀，「パスワードは終わった！」と言われてからも四半世紀近くが経とうとしている。それでも今，パスワードが使われている。なぜパスワードが使われるのか。その理由はただ一つ，それが有する安全性と，その運用に関する費用（手間）を考え合わせたコストが最良との理由からである。ただし，どのようなセキュリティシステムでも，その安全性を保証するための仮定がある。すべてのセキュリティシステムにおいて無条件の絶対的安全性は存在しない。パスワードも然りである。パスワードでの安全性の仮定は，いくつかあるものの，その第一は利用者の高いセキュリティ意識である。利用者のパスワードの管理が最良である場合，パスワードは有効に作用する。しかし，今，そのパスワードを取り巻く状況が大きく変わってしまった。利用者の高い意識が期待されないのである。パスワードが利用され始めた当時，パソコンやネットへ接続する人は一部であり，かつ高いセキュリティ意識を有していた。しかし現在はすべての人が利用するといっても過言ではないほど，パスワードは一般化している。特にスマートフォンの普及によって，社会生活におけるすべてのサービスがネット化し，そのサービスを受けるための認証システムとしてもパスワードの利用が不可欠となっているのである。

誰でもがパスワードを利用することになって，全体的にはセキュリティ意識が極めて低くなったことが，パスワードの安全性自体の仮定を崩す結果となったのである。パスワードの安全性を保障する仮定の第一は，利用するパスワードを本人しか知り得ないということである。通常，サービス側でもパスワードを保存しない。パスワードを登録する際にハッシュ化した値のみを保存し，パスワードは廃棄するためである。この知り得ないという意味は，他者に推測されないという意味も含んでいる。したがって，8文字，あるいは12文字以上の英数大文字小文字，それに記号まで加えた無意味な文字列，通常はそれらの個々の文字種を

無意味に並べ替えた文字列，つまりランダムな文字列が推奨される。このパスワードは通常，他人に知られることがないようにとの制約から記憶することが求められる。このことが安全性の強度に大きく影響するのである。つまり，セキュリティ意識が低い場合，他人に推測され難いという抽象的な目標よりも，記憶するという具体的な目標が優先されて，無意味ではなく，自分にとっては意味のあるパスワードを付けてしまうことになってしまうのである。つまり自分や身近な人の住所や電話番号，それに生年月日に関係する英数字，あるいは自分自身が覚えやすい英単語が選択されることとなる。

3．パスワードの定期変更

この他人に推測され難い，無意味でランダムな文字列をパスワードとして採用すべきという最も基本的な注意事項であるが，セキュリティ意識の低い一般の人にとっては必ずしも容易ではない。

IPAの調査でもわかるように，一般の人にとって一番の不安はパスワードを忘れてしまうことなのである。これが推測され難い無意味な，そしてランダムな文字列を使うことへの阻害要因になっている。

当初，このパスワードの他人による推測を防ぐために，そしてパスワードへの注意喚起，パスワードの設定を意識させることを目的に，パスワードを定期的に更新することが推奨され，実際に，特に高いセキュリティが求められる銀行や証券会社，それにネット通販等，資産や取引に関わるサイトへアクセスする際の認証に用いられるパスワードには定期更新が強く求められた。

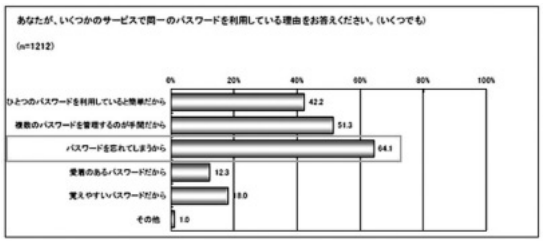

図１　同一のパスワードを使う理由
引用：IPAプレス発表パスワードリスト攻撃による
不正ログイン防止に向けた呼びかけ

パスワードの定期変更が推奨される最も大きな理由は，かつてアメリカ国立標準技術研究所（NIST）がパスワードの定期変更を推奨していたためである。NISTとはアメリカの技術や産業の規格や利用について，その要件等を定める機関であり，そこで決められたことは米国での利用基準となっている。日本政府でも，それに準じて，例えば総務省ではパスワードの利用に関し，「パスワードの定期変更」を推奨していたのである。もちろん，それだけではなく，第一にパスワードへの関心を高めるため，第二には，もしそのパスワードが洩れていた，あるいは推測されていたとしても，利用期間における制限から限定的な被害に収まるだろうという期待からである。

NISTでは最近になって，パスワードの定期変更を推奨することはなくなり，それどころか，昨年の６月には，「一般には，パスワードの定期変更を求めてはいけない」という，今までと真逆の推奨が提示された。それにともなって今年の３月には，総務省が「パスワードの定期変更は不要」との発表を行った。なぜパスワードの定期変更が勧められないのか。

パスワードの定期変更の目的はパスワードが推測される可能性を低減させるため，そして万が一に，パスワードが洩れたとしても，その被害を最小化するためであった。しかし，先に説明したようにパスワードの安全性は，もともと他人に推測されない無意味でランダムなパスワードに設定していることを仮定していたのである。しかるにパスワードの定期変更を強いることによって，この仮定が崩れる傾向が判明したのである。つまり定期変更する際にも，変更前のパスワードと，変更後のパスワードは当然，無相関，つまり改めて無意味でランダムな文字列をパスワードとして設定しなければならない。ところが頻繁な変更を強いるがゆえに，そして多数のパスワードを扱う必要から，それぞれ定期変更を強いられることで手間が倍増し，安易な変更になる場合が多いのである。例えば，先のパスワードを規則的に変更する

ために，末尾の番号を１加えたり，他のサービスのパスワードを順々に使いまわしたりすることが判明したのである。言わば，パスワードの本質において，枝葉を気にするあまり，本質を見失っていたのである。

４．パスワードの誤解とパスワードリスト攻撃への対処

現在，パスワードにとって最大の脅威は「パスワードリスト攻撃」である。パスワードリスト攻撃では，一つのサイトで漏えいしたID（アカウント名）とパスワードを，他のサイトに適用し，アクセスを試みる。これに対する対策は，利用する複数のパスワードをそれぞれまったく異なったパスワードにすることであるが，これを実際に実現することは容易ではない。現在ではパスワード管理ツール（ソフト）があり，特にスマートフォンではその利用が推奨されているが，その適用と操作の面倒さゆえに，普及しているとは言い難い。特に以前からパスワードについては以下の３点を厳守することが言われていた。

(1) パスワードは定期的に更新すること

(2) パスワードは紙に書いてはいけない（覚えること）

(3) できるだけ長いパスワードをつけること

しかし，この３点を文字通り，厳守することは必ずしもパスワードにおいて，他人に類推されないという本質を満たさないのである。(1) については先に述べた。(2) については紙に書くのが不都合ではなく，その紙に書いたパスワードが容易に他人の目に触れることが問題なのである。したがって，会社や学校ではなく，自宅においては，メモ帳に記述し，自分だけが手に取ることができる場所に保管すればまったく問題ないのである。また日頃持ち歩く，手帳やスマートフォンであっても，パスワードが記述する場所がわからなければ問題はない。ただし，決して「何々に対するパスワードはxx」と書いてはならない。さりげなく，パスワードだけノートの片隅に書いておくのである。(3) に対しても，一見，長いパスワードは安全である，つまり推測され難いと思われがちであるが，長いパスワードであればあるほど，意味のある文字列を採用することが常であり，たとえば小説や歌詞の一節となって，ある程度の個人情報や嗜好が判明すれば容易に類推されることも少なくない。

このように常識と思われている，安全なパスワードの作成や運用が，実はパスワードの本質を阻害する結果となっている。確かに，一部の比較的セキュリティ意識の高い利用者の限られたサービスにおいて，少数のパスワードを運用していた時代では常識として通用していた。しかし，時代が変わり，セキュリティ意識を求めることができず，強制的な方法以外では指示や推奨に従うことのない利用者が大部分となり，必ずしも常識が通用しなくなったのである。正確には文字通りの常識に拘るがあまり，本質が犯される結果となった。

５．むすび

認証システムであるパスワードを含めて，サイバーセキュリティの基本は想定される脅威から，利用者である自分自身を守ることである。オールマイティのセキュリティ対策はありえない。以前はパスワードの定期変更が，パスワードの強度化や，その漏えいに対して一定の効果が期待された。それはスマートフォン登場以前であり，利用するネットサービスも少なく，管理するパスワードの数が少ない場合であった。しかもパソコンを使うという一定の知識，特にネットリテラシーと呼ばれるネットの使い方，パスワードの使い方にほんの少しでも注意を向けられる人が大半であった。以前と比べて数多くのネットサービスを利用し，しかも誰でもがパスワードを使っている。サイバーセキュリティの根本的な常識が変わったのではなく，パスワードやサイバーセキュリティを取り巻く状況が変わったのである。