複雑さより長さが大事!?

パスワード設定の新常識

Jugemu Jugemu Gokō-no
Surikire Kaijarisuigyo-no
Suigyōmatsu Unraimatsu
Fūraimatsu ……

増井技術士事務所 代表
技術士（情報工学部門）
増井　敏克

インターネット上のサービスや、パソコン・スマートフォンのログインなどでパスワードを設定する機会は多くあります。どのようなパスワードを設定し、どのように運用すればよいのか、トレンドを踏まえて解説します。

従来のパスワード設定の問題点

パスワードに設定する値として、アルファベットの大文字、小文字、数字、記号を組み合わせたものを求められたり、「○文字以上」などと文字数の制限が設けられていることが多くあります。

また、毎月のように変更を求められ、新しいパスワードを考えたり覚えたりすることに悩んでいる人も多いでしょう。

使っているサービスが1つや2つであればそれほど問題にはなりませんが、インターネット上には多くのサービスがあり、1人で10個や20個、人によっては100個以上のパスワードを管理しなくてはならないこともあります。

このような状況で頻繁な変更を求められると、覚えておくのは現実的ではなく、複数のサービスで同じパスワードを使い回す人が多いものです。また、毎月変更を求められるサービスでは、4月に「xxxxx04」、5月に「xxxxx05」、6月に「xxxxx06」のように末尾だけを変えている人もいます。

こうしたパスワードの運用について、「あまりよくないのではないか」と問題意識を感じている人は少なくないでしょう。では、どうすればよいのでしょうか？

パスワードはどのようにして漏洩・悪用されるのか

そもそも、パスワードの変更が求められる理由として、設定したパスワードが漏洩し、悪用されることが挙げられます。

漏洩や悪用が発生する原因を、「攻撃者」「提供者」「利用者」という3つの視点から考えます。

①　攻撃者がパスワードを盗む

第三者にパスワードを知られる理由として、攻撃者によるパスワードの探索があります。このときの手法には、「総当たり攻撃」「辞書攻撃」「リバースブルートフォース攻撃」などがあります。

「総当たり攻撃」は、連番などを順に試す攻撃です。4桁の数字のような単純なパスワードであれば、「0000」「0001」……と繰り返し、「9999」まで1万個を試せば必ず見つけられます。

「辞書攻撃」は、辞書に載っているような単語や、一般によく使われているパスワードを順に試す攻撃です。よく使われているパスワードとしては、「password」や「qwerty」（キーボードの左上から右に順に押したもの）、「123456」などが知られています。

「総当たり攻撃」や、単純な「辞書攻撃」への対策は比較的容易で、パスワードを3回間違えたときに、そのIDをロックするなどの方法がよく使われます。

このような対策が使えないのが「リバースブルートフォース攻撃」です。これはパスワードを固定し、IDを変える攻撃です。

たとえば、「0000」というパスワードに対してIDを変えながら試すと、単純なパスワードを設定しているIDにログインできます。この場合、IDが毎回変わるため、「パスワードを3回間違えるとロックする」といった対策は使えません。

そのため、これらの攻撃に対しては「単純なパスワードを設定しない」ことが重要です。

②　提供者からパスワードが流出する

第三者にパスワードを知られる

表　パスワード設定における文字の組合せ

文字数	文字の種類	パターン数
4	数字のみ（10種類）	10^4=10,000通り
4	大文字・小文字・数字（62種類）	62^4=14,776,336通り
8	大文字・小文字・数字（62種類）	62^8=218,340,105,584,896通り
12	小文字のみ（26種類）	26^{12}=95,428,956,661,682,176通り

原因として、情報漏洩もあります。サービスを提供する事業者の誤操作や誤設定、誤送信などによって、事業者が保有する情報が外部に漏洩してしまう場合です。

また、事業者が使っているプログラムに脆弱性（セキュリティ上の不具合）があり、第三者がそれを狙って攻撃することで、事業者が保有するパスワード等の情報が漏れてしまう場合もあります。

③　利用者自身によるパスワードの漏洩

利用者自身がパスワードを漏洩してしまう例としては、フィッシング詐欺があります。攻撃者から送られてきたメールに記載されたリンクをクリックするなどの方法で偽サイトに誘導され、そこでIDとパスワードを入力してしまうと、その値が漏れてしまいます。

パスワードを書いたメモを捨ててしまう、管理者を装った電話に答えてしまう、電車内など外出先での会話から推測されてしまう、といった事案も発生しています。

このような提供者や利用者からの漏洩では、複雑なパスワードを設定していても意味がありません。「パスワードを使い回さない」ことと、「不審なログインがあったときにパスワードを変更する」ことが求められます。

パスワード設定の新常識

単純なパスワードを設定しないということは、逆に考えると「長く複雑なパスワードを設定する」ということです。

「長く」というのは文字数、「複雑」というのは「大文字、小文字、数字、記号のすべてを使う」ということです。

たとえば、4桁の数字であれば「0000」から「9999」までを調べれば突破できますが、8桁で大文字、小文字、数字、記号をすべて使うと、調べる数が大幅に増加します。もっとも、文字数が多ければ、文字の種類はそれほど重要ではありません。

上表のように文字数を増やすだけでパターン数は大幅に増加するため、小文字だけでも文字数を増やせば十分です。総当たり攻撃にかかる時間が現実的でなくなるため、**「可能な限り長いパスワードを設定すること」**が有効です。

ただし、同じ文字の繰返しや辞書にある単語、「qwertyuiop」のようなパスワードでは辞書攻撃によって突破されてしまいます。このため、ある程度は複雑な値を設定しなければなりません。

そして、**「パスワードの使い回しをしないこと」**が重要です。あるサービスでパスワードが流出すると、同じパスワードを設定している他のサービスにもログインされてしまうためです。

このとき、まったく同じパスワードでなくても、末尾にサービス名をつけたようなパスワード（xxxx_yahoo、xxxx_line、xxxx_facebook…）では、攻撃者によって推測される可能性があります。

パスワードの適切な管理方法

パスワードの設定だけでなく、運用についても常識は変わってきています。

現在もパスワードを定期的に変更するように求めるサービスがありますが、上記のように末尾の数字だけを変えるような運用をしている人が多いものです。

そこで、NIST（米国国立標準技術研究所）による『SP800-63』という文書では、パスワードの定期変更を要求すべきでないことが記載されています。また、日本のNISC（内閣サイバーセキュリティセンター）や総務省もパスワードの定期変更を推奨しなくなりました。

現在は、長く複雑なパスワードを設定し、使い回さないようにして、不審なログインがあったときに変える運用が適切だとされています。ただし、このような運用では、パスワードを覚えておくことが現実的ではなくなります。

手帳など肌身離さず持っておくものに書いておく方法や、表計算ソフト等で管理する方法もありますが、**「パスワード管理ソフトを**

使う」方法が推奨されています。

最新のiOS（Apple社開発のOS）などのApple製品には、「パスワード」という管理アプリが標準で搭載されています。また、『1Password』や『LastPass』といった個別のアプリを使う方法もあります。Google ChromeなどのWebブラウザが標準で備える、パスワードの自動保存機能を使う方法もあるでしょう。

これらを利用すると、長く複雑なパスワードでも自分で覚えておく必要はなく、使い回さない運用を手軽に実現できます。

さらに、パスワードを入力する欄に自動入力してくれる機能を備えたソフトでは、アクセスしたWebサイトのドメインに合わせてパスワードを入力してくれるため、フィッシング詐欺など異なるドメインのサイトにアクセスしたときに誤って入力してしまうことを防げます。

ただし、注意しなければならない点もあります。パスワード管理ソフトが導入されたパソコンやスマートフォンを他人に使わせない、ということです。

他人と共用するパソコンにパスワードを保存してしまうと、他の人がそのままログインできることがあります。このため、自分しか使わないパソコンやスマートフォンでの使用にとどめ、離席中などに他人が使うことがないように、離席するときはコンピュータをロックすることを推奨します。

なお、過去にパスワード管理ソフトの脆弱性から、パスワードが漏洩した可能性があることがニュースになりました。パスワード管理ソフトも絶対に安全だとはいえません。セキュリティを考える際はリスクを踏まえ、個々人が判断する必要があります。

たとえば、次のようなリスクを想定し、管理するパスワードの数や個人の環境（自宅でしか使わない、持ち運んで使うなど）を考慮したうえで、パスワード管理ソフトを選択してください。

- **パスワード管理ソフトを使わずに単純なパスワードを設定したり、使い回しをするリスク**
- **パスワード管理ソフトから情報が漏洩するリスク**
- **手帳などに書いたパスワードを紛失したり他人に見られたりするリスク**
- **表計算ソフト等で管理したファイルが誰かに閲覧されるリスク**

外部ネットワークへの接続について

パスワードを管理するとき、外部ネットワークへの接続に不安を感じる人もいるかもしれません。

先述のパスワード管理ソフトを使う場合、ネットワークに接続していることが前提となります（接続していないと、「アクセスしたWebサイトのドメインに合わせたパスワードを入力してくれる」といった機能が使えないため）。

また、パソコンは一般的にネットワークに接続していると思いますので、外部ネットワークへの接続を避けるのは現実的ではないと感じます。Excelファイルなどにパスワードを設定する方法もありますが、そもそもパソコンのなかのファイルが見られているような状況が発生すること自体が問題なので、そうならないような対策を実施すべきです。外部ネットワークでの管理を過剰に不安がる必要はありません。

安全性を高めるために追加で実施したい対策

ここまで解説した対策は、個々人が実施するだけでなく、組織としてパスワードの重要性や安全な管理方法について従業員に教育し、意識を高めることが大切です。それに加えて、以下のような対策を実施するとよいでしょう。

2段階認証や2要素認証の設定

情報漏洩やフィッシング詐欺などでパスワードが知られると、長く複雑なパスワードを設定して使い回していなくても、第三者にログインされる可能性があります。これを防ぐため、2段階認証や2要素認証が設定可能なサービスでは必ず設定しておきます。

ログイン履歴の確認

不審なログインがないか履歴を定期的に確認することも重要です。ログイン時やログイン失敗時にメールで通知してくれるサービスもありますが、それ以外でもログイン後の画面でログイン履歴を確認できることが多いものです。

パスキーの使用

生体情報（顔・指紋認証等）やパターン認証によりログインできるパスキーに対応したサービスも増えています。これらを導入するのも1つの選択肢です。

以上を参考に、パスワードのトレンドを知り、セキュリティへの意識を高めましょう。

ますい　としかつ　増井技術士事務所代表。技術士（情報工学部門）をはじめ数多くの資格を保有。ITに関するコンサルティング、ソフトウェアの開発、執筆活動等を行なう。