パスワードの管理について

著者：関 勝寿　公開日：2017 年 5 月 9 日　ソース：https://sekika.github.io/2017/05/09/Password/

複雑なパスワードをいくつも覚えることは難しいため、良くないと分かっていても、とても覚えやすい単純なパスワードを使っていたり、多くのサイトで同じパスワードを使いまわしたりしている人が多いであろう。この記事ではパスワード管理方法のヒントを記す。

2026 年 4 月 18 日：パスキーについて追記した。パスキーが使えるサービスでは、なるべくパスキーを使いましょう。

1. パスワード設定の原則

パスワード設定方法には 2 つの原則がある。

1.1. 原則 1: 複雑なパスワードを使う

「複雑なパスワード」といってもいろいろなレベルがあり、特に多くの人が使っている「極めて単純なパスワード」は使うべきではない。使用してはいけないパスワード、トップ 50 によれば、2010 年の Gawker 社の事件で盗まれたパスワードを解析したところ、トップ 5 はこのようなパスワードだった。

```
123456
pasword
12345678
lifehack
qwerty
```

その先にも、単純なパスワードが続いている。アカウントを盗もうとする攻撃者は、攻撃の成功率を高めるために、このような「よく使われるパスワード」を使ってサイトへの侵入を試みるため、単純なパスワードを使っていると破られる危険性が高まる。

「単語や人の名前などを使った覚えやすいパスワード」は、「攻撃者にとっては推測して当てやすいパスワード」となるため、攻撃に対して弱いパスワードとなる。攻撃を成功しにくくするためには「複雑な覚えにくいパスワード」すなわち攻撃に対して「強い」パスワードを設定することとなる。なるべく文字数は長く、アルファベット（小文字、大文字）、数字、記号など、使う文字の種類は増やす方が攻撃は成功しにくいため、より強いパスワードとなる。

「5 万語の語彙の辞書（広辞苑など）をランダムに開いて 3 つの語を選んで繋げる」（オフライン攻撃想定の「暗号の鍵」の場合は 5 つの語を選んでつなぐ）というセキュリティ研究者の提案もある。

1.2. 原則 2: 同じパスワードを使いまわさない

この原則の目的は、パスワードリスト攻撃を防ぐことにある。あるサイトに登録したパスワードがなんらかの理由で漏洩して、ユーザー名とパスワードのリストが出回ることがある。そのときに、複数のサイトに同じパスワードが設定されていると「あるサイトから漏えいしたパスワード」が、他のサイトでも使われることでログインに成功して被害が広がってしまう。パスワードの漏えいは必ずしも漏えいしたという事実がわかるとは限らないので、「漏えいしたことがわかってからパスワードを変えればいい」とするのは不十分である。

2. パスワードの管理方法

このように「強いパスワード」を「サイトごとにばらばらに」設定すると、人間の記憶力ではそのパスワードは覚えられないので、パスワードを管理するための補助手段が必要となる。そのための 3 つの方法を記す[1]。記載する順番としては、誰でも簡単に実行できる方法から、より IT に詳しい人向けの方法へと進めていくため、適宜「自分にとって便利である」と思われる方法を選択し、さらに自分なりの工夫を加えると良いであろう。

また、ここに書かれているような方法でパスワードを管理していても、たとえばフィッシングにかかればパスワードが盗まれてしまう。ここに書かれていることはセキュリティ対策の「すべて」ではない。

2.1.(1) 紙のメモ

「パスワードは紙に書いてはいけない」と、昔はよく言われていた。その紙を他の人から見えるところに置いておけば、簡単にパスワードを盗まれてしまうためである。一方で、紙に書いた情報は離れた場所にいる攻撃者からネットワーク経由で盗まれる心配はないという点においては、ファイルで保存する方法と比べて優れている。この方法の安全性を高めるためには、「他人から見られにくい場所に紙を保管する」だけでなく「もし見られてしまってもパスワードを容易に推測できないようにする」といった対策が望ましい。そのためには、紙に記載したパスワードから本物のパスワードへの変換規則を作り、それを記憶する。たとえば、yaQ のような決められた文字を末尾に追加する、といったような変換規則が考えられる[2]。すなわち、紙には

```
○×銀行
ID seki
パスワード xTL2WLGz0P
```

のように書いておき、xTL2WLGz0P に決められた文字 yaQ を追加して xTL2WLGz0PyaQ というパスワードとする。この「yaQ」という文字は他のサイトにも共通のものとしておけば、この程度の長さであれば記憶可能である（ただし、長期的に使わないと忘れてしまうことがあるので、忘れにくいように自分なりの工夫をすると良い）。このようにすれば、たとえば家族がその紙を見てこっそりとログインを試みても[3]成功しない。

紙の保管で大変なのは紛失対策である。大きめのノートに記して決められた場所に保管する、持ち歩かない（持ち歩くと紛失の危険性が高くなる）、あるいはコピーして 2 箇所以上に保管する、といった対策が考えられる。

2.2.(2) パスワード付き電子ファイル

パスワードなどのアカウント情報をパソコンやスマホなどに電子的に記録することで、たとえばマルウェアに感染してその情報を盗み取られるという危険性が生じる。その対策をする必要があるという前提で、アカウント情報をどのように電子的に記録するのかを考える。

アカウント情報が書かれているファイルを「そのまま読める状態で」保存しておくことはリスクが高く、ファイルを暗号化して、解読用のパスワードを入力しなければ読むことができないようにすることが望ましい。IPA が例示する方法の中にもこの方法が書かれている。「パスワード付き電子ファイル」を作るためには、パスワード付き圧縮ファイルを使う方法や、GPG のような暗号化のためのソフトウェアを使う方法、暗号化ディスクイメージファイルを作成する方法などがある。なお、暗号化したファイルを総当たり攻撃で解読されないためには、ファイル暗号化のパスワードには十分な強さのものを使用する必要がある。「パスワード」という言葉は「単語」の長さをイメージするので、もっと長い「パスフレーズ」を使うように推奨されることもある。

2.3.(3) ハッシュ関数

「記憶した共通のマスターパスワード」と「サイト固有の情報」から、決められたハッシュ関数でパスワードを生成する、という方法である。これは (2) と似て非なるものである[4]。SuperGenPass は、「サイト固有の情報」を、公開された情報である「サイトのドメイン名」として[5]、JavaScript やブックマークレットを使って使いやすくしたものである。Mobile 版を試してみると、使い方が分かる。また、シード文字列（マスターパスワード + サイト固有の情報）を強化するために自分だけがわかるなぞなぞを使う EpisoPass というシステムもある。

この方法を実現する自作のパスワード生成プログラム を公開する。サイト固有の情報（パスワードの種）を 1 つのファイルとして管理し、パソコンに保存されたパスワードの種と、毎回打ち込むマスターパスワードからパスワードを生成する[6]。モバイルからのアクセスのために HTML ファイルを生成することもできる。

3. 二要素認証

いずれの方法でパスワードを管理したとしても、さらに安全性を高めるためには、パスワード以外の認証方法を併用することが有効である。ここでは、多要素認証の 1 つである携帯・スマホなどによる二要素認証について記す。これは、本人しか知らない「パスワード」に加えて、本人しか持っていないもの（携帯・スマホなど）を持っているかどうかによって認証をする、というものである。

たとえば、携帯の番号を登録しておいて、パスワードを入力すると、携帯・スマホにテキストメッセージ (SMS) で確認コード（ワンタイムパスワード）が送られてきて、その番号を入力してはじめてログインできる。その番号はそのとき 1 回限りのものなので、そのときに携帯・スマホを「持っている」人でないとログインできない、というしかけである。二要素認証には、主として

・携帯・スマホへの SMS や音声通話を使うもの
・確認コード（ワンタイムパスワード）表示専用の小型端末（トークン）を使うもの
・モバイルアプリを使うもの（Google 認証システムの仕組み参照）

がある。ここで、たとえばモバイルアプリで二要素認証を設定すると、そのモバイルアプリが使えなくなったとき（スマホの紛失など）にログインできなくなるので、SMS でも二要素認証ができるようにする、バックアップコードを印刷する、などといった対策が必要となる。スマホを紛失しても同じ電話番号で新しいスマホを取得すれば、登録しておいた電話番号宛の SMS を受け取ることは可能となる。

なお、二要素認証で登録した電話番号を解約したり変更したりするとログインができなくなるので、注意が必要である。どのサービスにどの電話番号を登録したのかというリストを作っておくと良いであろう。

4. パスキー

近年は、パスワードに代わる認証方法としてパスキーに対応するサービスも増えている。ここでいうパスキーとは、一般に、WebAuthn / FIDO2 に基づく認証資格情報を用い、利用者がパスワードを入力せずにログインできる仕組みを指す通称である。

パスキーでは、サービス側には公開鍵が登録され、対応する秘密鍵は利用者の端末側で管理される。ログイン時には、端末内の秘密鍵を利用して認証が行われ、その際に指紋認証・顔認証・PIN・画面ロック解除など、端末側の本人確認操作が求められることが多い。

この方式の重要な特徴は、認証処理が正規のサイト（オリジン）と結び付けられていることである。別ドメインの偽サイトに対して生成された認証結果を、正規サイトへの認証としてそのまま利用することはできないよう設計されている。そのため、偽サイトに認証情報を入力させて盗み取る従来型のフィッシングに対しては強い耐性を持つ。また、利用者になりすますために必要な秘密鍵をサーバー側に保存しないことから、サーバーに保存された認証情報が漏えいしても、それだけで利用者としてログインされる危険は低い。

また、利用者が秘密情報そのものを毎回入力して送信する方式ではないため、パスワードの記憶・入力・使い回しといった問題も軽減できる。サービスや端末によっては、複数端末間で認証情報を同期できるものと、特定端末のみに保存されるものとがある。

一方で、端末の故障・紛失や、端末アカウントへのログイン不能時には、認証手段の回復が必要となる。予備端末の登録、回復用メールアドレスや電話番号の最新化、バックアップコードの保管など、各サービスの復旧手段を事前に確認しておくことが重要である。

対応サービスでは、安全性と利便性の向上が期待できる認証方式として、パスキーの利用を検討する価値がある。

5. 注

[1] パスワードを管理するソフトウェアを使用する方法については除外する。その理由としては、ソフトウエアの開発元は信用できるか、開発元に悪意がなくてもソフトウェアの不具合によってパスワードが漏えいしないか、ソフトの開発が止まって突然ソフトが使えなくならないか、というような懸念もあり、自ら特定のソフトを信頼して使うのは良いとしても、他人に勧めることはできないと考えているためである。

[2] この規則に、さらに「6 文字目から読み始める（5 文字目までは無視する）」といったような規則を加えることも考えられる。ただし、あまり複雑にすると「規則を忘れてしまう」危険性も高まる。

[3] 他人のパスワードのメモを見てこっそりとログインをする行為は不正アクセス禁止法に違反する三年以下の懲役又は百万円以下の罰金の刑事罰に相当する不法行為である。

[4] サイト固有の情報を入手した攻撃者が適当なマスターパスワードを入力したときに、生成されるパスワードが正しいか間違っているかが「サイトへのログインを試行しないとわからない」という点が、この方法が (2) とは決定的に異なる点である。すなわち、(2) の方法では、パスワード付き電子ファイルが漏えいしたときに、オフラインでマスターパスワードが正しいか間違っているかがわかってしまうために総当たり攻撃が成立する。一方で、この方法ではサイトがパスワードの誤入力を許容する頻度の限界によって制限される。パスワード入力ミスを一定回数繰り返すとロックがかかるシステムも多い。したがって、短い期間に何万回も試行を繰り返すような攻撃は通常は不可能である。ただし、あるサイトのパスワードが漏えいしたときには、「正解がわかっている」ために総当たり攻撃でマスターパスワードが解析される危険性がある。

[5] 「サイト固有の情報」が公開情報となっているため、注 4 に記したように、あるサイトでパスワードが漏えいしたときに総当たり攻撃でマスターパスワードが解析される危険性がある。マスターパスワードがわかれば、他サイトのパスワードもわかる。そのため、十分に強いマスターパスワードを設定する必要があると作者は解説している。サイト固有の情報が公開されている以上は、マスターパスワードの複雑性を本質的には増強していないことになる。

[6] このプログラムでは「サイト固有の情報（パスワードの種）」が書かれているファイルが漏えいしなければ、「あるサイトのパスワード」がわかっても総当たり攻撃が成立しない。総当たり攻撃をするためには「サイト固有の情報」が書かれているファイルと「あるサイトのパスワード」の両方を不正に入手する必要がある、という点で SuperGenPass よりは安全性が高まっているはずである。ただし、このファイルが失われたらこのプログラムで管理しているすべてのサイトのパスワードが失われるため、セキュリティを確保しつつファイルを失わない様に管理をしなければならない。