# パスワードの安全性

情報政策グループ　技術職員　山田　純一

コンピュータの初期設定にあるアカウントのパスワード設定は，コンピュータのセキュリティ対策で最初に行う対策の 1 つであり，設定の際は安全なパスワードを設定する必要がある。コンピュータを利用する方は，既に一般常識であるかもしれないが，パスワードの安全性について再確認して欲しい。

キーワード：セキュリティ，パスワード

## 1．はじめに

近年，コンピュータウイルスや情報漏洩，不正侵入などのニュースが数多く飛び交っている。コンピュータの利用者は，コンピュータウイルス対策ソフトウェアの導入，OS やプログラムの脆弱性対応，不審な Web サイトは閲覧しないなど，コンピュータのセキュリティ対策を講じていると思われる。

しかし，その一方で，パスワードのメモをパソコンに付箋で貼り付けたり，机上に誰でも見える形でメモを置いたりしている例が少なからず見受けられる。


図 1　付箋で貼り付けた例


図 2　机上に置いた例

今回この記事では，パスワードの安全性について再確認して貰うほか，パスワードが簡単だと，どれだけ早く解析されるかを実験した。

## 2．パスワード解析

安全でないパスワードは，大抵の場合，以下の 6 つのどれかが含まれている。

① ユーザ名とパスワードが同じ
② 名前や誕生日など，推測しやすいものを含む
③ 辞書に記載されている単語
④ 文字数の短いパスワード
⑤ 数字または文字のみで作られたもの

この条件に 1 つでも当てはまる利用者は，パスワードがいつ破られてもおかしくないため，すぐにパスワードを変更する必要がある。

また，米国のスプラッシュデータ社の発表によると，2011 年と 2012 年において，設定すべきではないパスワードが公表されている。まとめると，表 1 のようになる。

表 1　設定すべきではないパスワード TOP25

| 2011 年 | | 2012 年 | |
|---|---|---|---|
| 1 | password | 1 | password |
| 2 | 123456 | 2 | 123456 |
| 3 | 12345678 | 3 | 12345678 |
| 4 | qwerty | 4 | abc123 |
| 5 | abc123 | 5 | qwerty |
| 6 | monkey | 6 | monkey |
| 7 | 1234567 | 7 | letmein |
| 8 | letmein | 8 | dragon |
| 9 | trustno1 | 9 | 111111 |
| 10 | dragon | 10 | baseball |

| | | | |
|---|---|---|---|
| 11 | baseball | 11 | iloveyou |
| 12 | 111111 | 12 | trustno1 |
| 13 | iloveyou | 13 | 1234567 |
| 14 | master | 14 | sunshine |
| 15 | sunshine | 15 | master |
| 16 | ashley | 16 | 123123 |
| 17 | bailey | 17 | welcome |
| 18 | passw0rd | 18 | shadow |
| 19 | shadow | 19 | ashley |
| 20 | 123123 | 20 | football |
| 21 | 654321 | 21 | jesus |
| 22 | superman | 22 | michael |
| 23 | qazwax | 23 | ninja |
| 24 | michael | 24 | mustang |
| 25 | football | 25 | password1 |

どれだけ危険かと言うと，パスワード解析ツールを用いて，実際に解析を行った。解析は，自分で構築したサーバにユーザを 25 個作成し，表 1 のパスワードをそれぞれ設定した。サーバは，スペックの低い機器を使用したが，24 個のパスワードについては，わずか数秒で解析が完了した。残る 1 つも 30 分以内に解析が完了した。

これ以外にも管理者のパスワード解析を行った。もちろん，表中のパスワードではなく，単語を含んだ 8 文字のパスワードを設定していた。かなり時間はかかったが，3 日で解析が完了した。この解析結果から，パスワードは長いと覚えにくいから短くする，忘れないように単語で作ってしまうと破られる可能性が非常に高いことが分かる。

このように構築したサーバで解析を行ったが，Web サイトを利用して確認することも可能である。今回は「How Secure Is my pass」と「Microsoft パスワードチェック」を利用して解析を行ってみた。まず，最も設定すべきではないパスワードである「password」を入力すると，すぐに警告が出る。


図 3　How Secure Is my pass での解析 1

パスワードの強度も低いとの判定が出た。

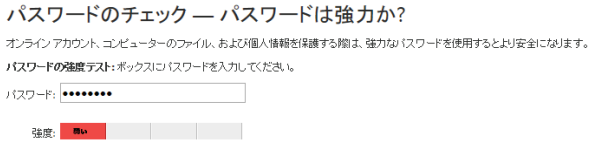


図 4　Microsoft パスワードチェッカーでの解析 1

少し文字を変更して，Passw0rd，Pa55w0rd、Pa55w0rds にしたが，いずれもパスワードの強度は低く，Pa55w0rds では約 39 日間で破られるとの予測が出た。


図 5　How Secure Is my pass での解析 2

続いて文字列を長くして，Pa55w0rds12 にしてみた。Microsoft パスワードチェッカーでは，強度が強いとの判定が出たが，How Secure Is my pass では，注意が出た。

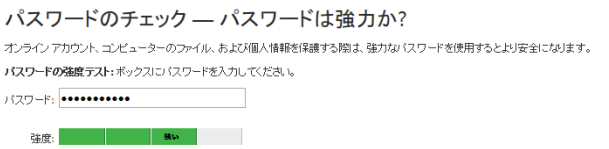


図 6　Microsoft パスワードチェッカーでの解析 2


図 7　How Secure Is my pass での解析 3

文字列の中に記号を入れて，Pa55w0rds*12 にしてみた。パスワードの強度は強いとの判定で，解析も 344×1000 年かかるとの予測判定が出た。

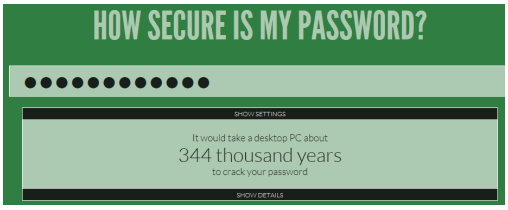


図 8　How Secure Is my pass での解析 4

最後に Microsoft パスワードチェッカーにおいて，とても強いとの判定になるようなパスワードを考えてみたところ，かなり長いパスワード列が必要になった。How Secure Is my pass でも解析までに果てしなく時間がかかるとの予測が出た。

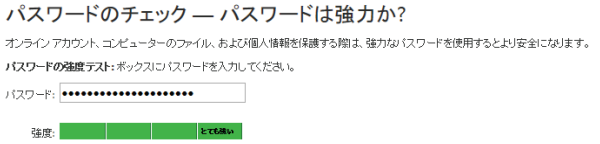


図 9　Microsoft パスワードチェッカーでの解析 3


図 10　How Secure Is my pass での解析 5

## 3．安全なパスワードとは

ここまでは，単語を含んだパスワード，設定すべきではないパスワードがどれだけ簡単に解析されるかを説明してきた。逆に安全なパスワードはどのようなパスワードであるかを説明する。

一般的に安全性の高いパスワードは，以下のものを含んでいる。

① ユーザ名とパスワードは同一のものにしない
② 名前や誕生日など，容易に推測できるものを使用しない
③ 辞書に記載されている単語を使用しない
④ 8 文字以上のパスワードを使用する
⑤ 文字，数字，記号をランダムに含める

よくパスワードは 8 文字以上と言われるが，独立行政法人情報処理推進機構が 2008 年にまとめた「コンピュータウイルス・不正アクセスの届出状況[9 月分および第 3 四半期]について」の中にパスワードについて記載した項目がある。その項目から，使用できる文字数と入力桁数によるパスワードの最大解読時間の表を以下に抜粋した。

表 2　使用できる文字数と入力桁数によるパスワードの最大解読時間

| 使用する文字の種類 | 使用できる文字数 | 最大解読時間 | | | |
|---|---|---|---|---|---|
| | | 入力桁数 | | | |
| | | 4 桁 | 6 桁 | 8 桁 | 10 桁 |
| 英字（大文字，小文字区別無） | 26 | 約 3 秒 | 約 37 分 | 約 17 日 | 約 32 年 |
| 英字（大文字，小文字区別有）＋数字 | 62 | 約 2 分 | 約 5 日 | 約 50 年 | 約 20 万年 |
| 英字（大文字，小文字区別有）＋数字＋記号 | 93 | 約 9 分 | 約 54 日 | 約 1 千年 | 約 1 千万年 |

※すべての組み合わせを試すために必要な時間を計算。記号は 31 文字使用できるものとした。

使用パソコン OS：Windows Vista Business 32bit 版、プロセッサ：Intel Core 2 Duo T7200 2.00GHz、メモリ：3GB

独立行政法人情報処理推進機構では，英字（大文字，小文字区別有）と数字の組み合わせで 8 桁のパスワードを作成した場合，解読には最大で約 50 年（全ての組み合わせを試算した場合）かかるため，この組み合わせでパスワードを作成すれば，パスワードの強度は十分だとある。

しかし，2008 年の時点なので，現在では 8 文字では強度が弱く，解析も 3 日間で解析されると

の予測が出た。

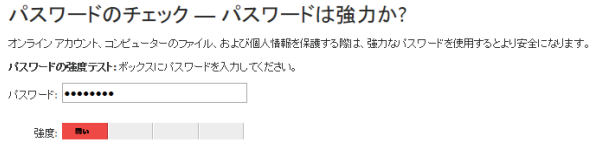


図 11 Microsoft パスワードチェッカーでの解析 4

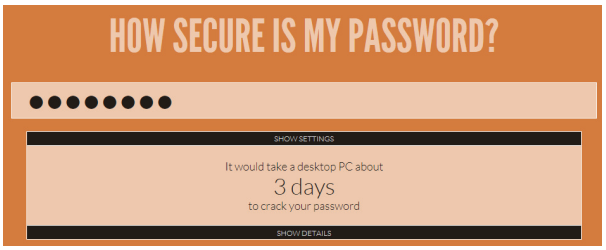


図 12　How Secure Is my pass での解析 6

この 2 つの解析結果から，パスワードの強度が強く，かつ解析までに時間がかかるパスワードの長さは，最低 12 文字以上であると推測した。ただし，前述したように，ユーザ名とパスワードは同一にしない，容易に推測できない文字，数字，記号をランダムに含んだものが前提である。

しかし，セキュリティの高いパスワードに設定してもパスワードを付箋で貼り付ける，机上に置くなどの行為があると意味がない。パスワードを人目に付くところには置かないことが重要である。

また，当たり前だがパスワードを人に教えないこと，パスワードを打つところを人に見られないようにすることもパスワードを守る上で大事である。

## ６．まとめ

この記事により，パスワードの安全性について再認識して貰えれば幸いである。現在は，シングルサインオン（ユーザ ID，パスワードを一元化することで，一度の認証により複数のリソースを使用できること）も使われる時代であり，パスワードの管理は非常に重要である。

また，パスワードの安全性も数年後には最低 12 文字以上でも危なくなる時代が来るものと思われ，その時に応じた長さにしていかなければならない。

## 参考文献・資料

1) SplashData, Inc. When "Most Popular" Isn't A Good Thing: Worst Passwords of the Year – And How to Fix Them
http://splashdata.com/splashid/worst-passwords/

2) SplashData, Inc. Worst Passwords of 2012 — and How to Fix Them
http://splashdata.com/press/PR121023.htm

3) How Secure Is my pass
http://howsecureismypassword.net/

4) Microsoft パスワードチェッカー
https://www.microsoft.com/ja-jp/security/pc-security/password-checker.aspx

5) 独立行政法人情報処理推進機構　第 08-23-133 号コンピュータウイルス・不正アクセスの届出状況[9 月分および第 3 四半期]について
http://www.ipa.go.jp/security/txt/2008/10outline.html