Classi

ウマい パスワードのつくりかた

ウマいパスワードの条件

- **覚えやすい**
- **複雑**
- **使いまわしていない**

ウマいパスワード（ここでは安全で忘れないパスワードのことを指します）の条件は、覚えやすく･複雑で･他のサイトで使いまわしていないことです。しかし、この条件を全て満たすのは難しいと思いませんか？
Classi のパスワードは半角英字・数字・記号を混ぜた 8 文字以上でつけていただくことがルールになっていますが、これは最低限のルールです。
実は、ウマいパスワードは、コツさえわかってしまえばとても簡単に作ることができます。Classi 以外のサイトでも応用できますし、今後皆さんがインターネットを使う中できっと役に立つはずです。ぜひ、この機会に実践してみてください。

シェフのおすすめ! ウマいパスワードのレシピ

① 材料 既に覚えている情報を使う

好きな歌の歌詞
ローマ字に変換する ↓
sukinautanokashi
これだけで16文字

例えば…自由に考えてみよう！
好きなセリフ basukegashitaidesu
語呂合わせ hitoyohitoyonihitomigoro
※長過ぎるときには子音だけ抜き出す→htyhtynhtmgr

パスワードは覚えやすいことが重要なので、材料には自分の既に知っている情報を利用します。おすすめは、**自分の好きな日本語の歌の歌詞の一部を使う**ことです。
誰にでも好きで覚えている歌はあると思います、それをローマ字にしてパスワードの材料にすることで、簡単に長くて覚えやすいパスワードになります。
もちろん、自分が忘れにくい情報であれば歌詞でなくても、**好きな映画や漫画のセリフ、語呂合わせ**など何でもかまいません。
ここでのポイントは、**日本語を材料にする**ことです（理由については後述の「パスワードの破り方？」をご覧ください）

② スパイス 区切りに数字を混ぜる

○ sukina1utano2kashi3
△ sukinautanokashi123

次にパスワードの複雑さを高めるために、スパイスとして数字を混ぜていきます。自分が覚えやすい数字で構いません。
ここでのポイントは、最後に付け足すのではなく**文章の区切りで数字を混ぜ込む**ことです。

③ 仕上げ サイトを示す識別子をつける

sukina1utano2kashi3#cl ←Classi用
sukina1utano2kashi3#tw ←Twitter用
sukina1utano2kashi3#tt ←TikTok用
…など
！＃＄％＆…など使う記号を一つ決める

最後に、他のサイトで全く同じパスワードを使いまわさなくて良いように、**記号とそのサイトを示す識別子をつけます**。
記号はなんでも構いませんし識別子の文字数も自由です、左の例を参考にしてください。このように、自分の中でルールを決めて識別子をつけることで、無理のない範囲で、サイトごとに別々のパスワードを使うことができるようになります。

マズいパスワードの例

✕ **yuka1109**

名前と誕生日の組み合わせ
親しい人間なら誰でも知っている

✕ **p@ssw0rd**

単語ひとつだけ
ハッカーが使っているパスワード集（辞書）に載っている事が多い

✕ **keyakizaka46**

好きな芸能人の名前
SNS などから容易に類推ができる

マズいパスワードはなにがいけないの？

ここまでウマいパスワードの作り方を解説してきましたが、そもそもなぜウマいパスワードを使わないといけないのでしょうか？
簡単に言ってしまうと、**悪意のある第三者にあなたの個人情報が盗み見られてしまう可能性があるから**です。例えば Classi であればポートフォリオやテストの点数、先生や友達とのやりとりなんかもあるかもしれません。
他サービスの事例では、**盗まれた情報を元に脅迫され、金銭を要求**されたなんて事件も報告されています。
もちろん、Classi では皆さんの大切な情報を守るために日々努力していますが、車の事故が安全装置だけでは防げないように、Classi を使う皆さんにも安全に十分配慮して使って頂く必要があります。
自分自身やお友達の大切な情報を守るために、ご協力をお願いします。

パスワードの破り方？

パスワードを守るためには、パスワードに対する攻撃手法を知ることが必要です。ハッカーはどのようなやり方でパスワードを破っているのでしょうか？実はいくつか方法があります。

Classi ではこれらの攻撃が容易に行えないように対策を実施しています

総当たり攻撃（ブルートフォース攻撃）

すべての文字列の組み合わせを試す

全ての文字列の組み合わせを試すのが総当たり攻撃です。
たとえばパスワードが 4 桁の数字だとすると 0000～9999 まで 1 万回試すことができれば必ず破れる計算になります。
現実的に攻撃を成功させるにはかなり時間がかかるので、**桁数の大きいパスワードをつければほぼ防ぐことが出来ます。**

リスト型攻撃（アカウントリスト/パスワードリスト攻撃）

名前やIDとパスワードの流出リストを使う

他のサイトで**流出した ID とパスワードの組み合わせを入手**して、順番に試していく攻撃をリスト型攻撃と呼びます。
攻撃者からすると総当たりよりも効率的に攻撃ができるため、被害が増加しています。
他のサイトと全く同じ ID とパスワードを使っていなければ防ぐことができます。

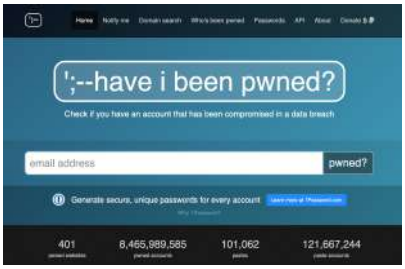
辞書攻撃（ディクショナリアタック）

パスワードでよく使われる単語を使って試す

パスワードでよく使われる単語の一覧（辞書と呼ばれます）は、実は簡単にインターネットからダウンロードできます。この**辞書に載っている単語を順番に試していく**攻撃を辞書攻撃と呼びます。
対策は、**辞書に載っている単語をそのままパスワードに使わないこと**です。
日本語の単語は、比較的辞書への掲載数が少ないことから、前ページのパスワードの材料には日本語をおすすめしています。

私、漏えいしてる？

自分の使っているパスワードが、ハッカーの使っているパスワードリストや辞書に登録されているかを調べる方法があります。
流出した情報を収集し検索できるようにした「Have I Been Pwned?(私、漏えいしてる？)」というサイトです。



https://haveibeenpwned.com/

上のメニューから「Passwords」を選び、自分が普段使っているパスワードを入力して「pwned?」をクリックします。

赤い「pwned!」というページが表示されたら、そのパスワードは漏えいリストに載っているということなので、変更したほうが良いと言えるでしょう。
このサイトは、実績もありセキュリティ業界において評価が高いですが、Classi 外のサービスなので､その点を理解して利用してください。

出典：内閣サイバーセキュリティセンター「インターネットの安心・安全ハンドブック」
https://www.nisc.go.jp/security-site/handbook/