

VDI マメ知識

＼覚えていませんか？／

パスワード変更の方法



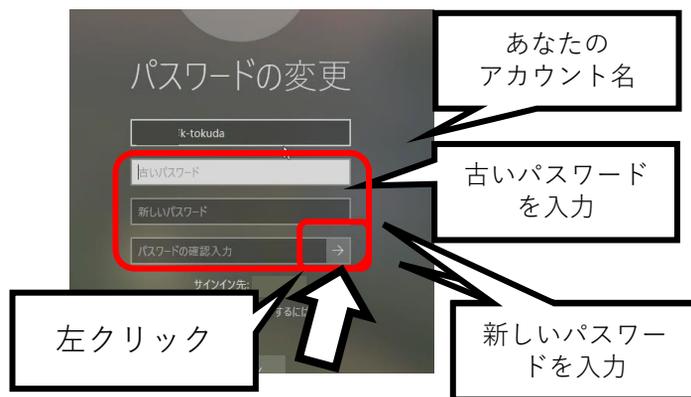
1 VDI画面上部にマウスカーソルを移動し、バーを表示



2 「パスワードの変更」を選択



3 「パスワードの変更」を選択



 安全なパスワードとは

完了！



- ① 名前などの個人情報からは推測できないこと
- ② 英単語などをそのまま使用していないこと
- ③ アルファベットと数字が混在していること
- ④ 適切な長さの文字列であること
- ⑤ 類推しやすい並び方やその安易な組合せにしないこと

サービスごとに
パスワードを
変える！

パスワードこぼなし



パスワード解析には、総当たり攻撃という方法があるんだよ。理論的にありうるパターンを全て入力して解析をする暗号解読をするんだ。

先週の半沢直樹でも使われてたやつだ！！



そうだね。ただ、半沢直のパスワードは「zansin」の6桁で英語のみで弱いんだ。Twitterでも突っ込まれていたよ。



2008年に情報処理推進機構（IPA）から出されたデータでは、英字（大文字、小文字区別）+ 数字 + 記号の種類を使った6桁のパスワードは約54日で解析され、8桁のものは約1千年で解析されると計算されたんだよ。

なら、8桁なら安心なんだね！



実はそうとも言えないんだ。



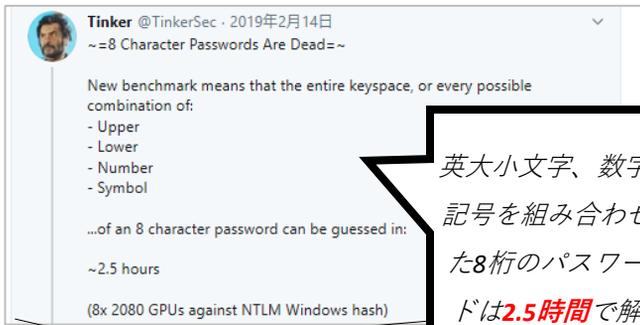
8桁のパスワード解析スピードは？

2014年の調査によれば、GPUを使えば20日程度

>8桁英大小文字、数字、記号(96文字種)を総当たりでパスワード解析した時の、全パターンの解析日数(理論値)を比較してみます。GPUを利用した場合は20日程度で終了してしまうのに対し、CPUを利用した場合には2年半程度の時間が必要になります。

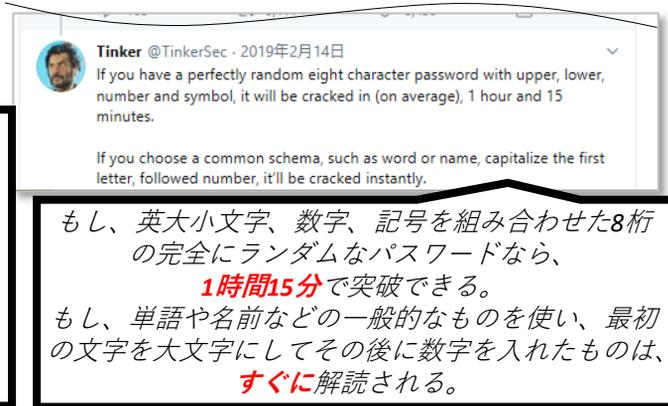
『dit セキュリティレポート 第1回：そのパスワードで大丈夫？～GPGPUによる高速パスワード解析 パスワード解析と解析マシン』
https://www.dit.co.jp/report/security_report/forensic_center/20140901.html

2019年のハッカーの発言によれば、わずか2時間半。



Tinker氏のTwitter
<https://twitter.com/tinkersec/status/1096046635593928704>

英大小文字、数字、記号を組み合わせた8桁のパスワードは2.5時間で解析できる。



もし、英大小文字、数字、記号を組み合わせた8桁の完全にランダムなパスワードなら、1時間15分で突破できる。もし、単語や名前などの一般的なものを使い、最初の文字を大文字にしてその後に数字を入れたものは、すぐに解読される。



じゃあパスワードは定期的に変えないと・・・。



昔はそうだったけど、最近はそんなことないと言われるようになってきたんだよ。



パスワードは定期的に変更する必要はない

定期的な変更によるパスワード強度が弱まるのが問題視されることになりました。

>むしろ定期的な変更をすることで、パスワードの作り方がパターン化し簡単なものになることや、使い回しをするようになることの方が問題となります。

>これまでは、パスワードの定期的な変更が推奨されていましたが、2017年に、米国国立標準技術研究所 (NIST) からガイドラインとして、サービスを提供する側がパスワードの定期的な変更を要求すべきではない旨が示されたところ。また、日本においても、内閣サイバーセキュリティセンター (NISC) から、パスワードを定期変更する必要はなく、流出時に速やかに変更する旨が示されています。



なるほどー！

『総務省 安心してインターネットを使うために国民のための情報セキュリティサイト』
https://www.soumu.go.jp/main_sosiki/joho_js/usi/security/business/staff/01.html