サイバーニュース

2023年5月
第 12 号

石川県警察サイバー犯罪対策イメージキャラクター「サイビット」

そのパスワード（＊＊＊＊＊）、安全ですか？

パスワードを突破する目的で

- ○　総当たり攻撃（全ての文字列を試す）
- ○　リスト型攻撃（流出しているパスワードを使う）
- ○　辞書攻撃（パスワードによく使われる文字列を試す）

などの攻撃があります。

総当たり攻撃対策 ➡ 桁数及び文字種を多くする

総当たり攻撃にとって、探り当てるまでに膨大な時間がかかるようにすることが１番の対策です。

数字だけだと10桁あっても100億通りしかなく、機械にかかれば一瞬で解読可能です。数字＋英字の大文字＋英字の小文字＋記号をうまく組み合わせて桁数を10桁以上にすることで、機械で総当たり攻撃されても解読困難になります。

リスト型攻撃対策 ➡ 全て別の、不規則なものにする

同じパスワードを使用していると、１つのパスワードが流出しただけで、利用している全てのサイトで不正アクセスされる可能性があります。

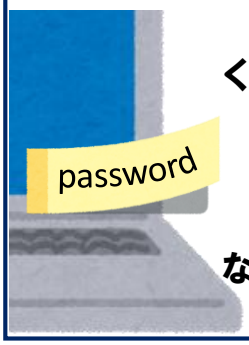
また、後ろの文字を１文字変えるだけだったり、サイト名＋同じ文字列を加えるだけ（例：shop9sPe!、bank9sPe!、sns9sPe!）だったり、規則性があるものは危険です。

全て別々の、規則性のないパスワードを使用しましょう。

辞書攻撃対策 ➡ 意味の無い、複雑なものにする

「password」や「sakura」などの意味のある単語や、キーボードを並び順に押すだけの「123456」や「1qaz2wsx」などの簡単なパスワードは危険です。

意味のある単語は避けて、複雑なパスワードを使用しましょう



付せんに書いてＰＣに貼っておく、デスクトップにメモを保存しておくなど、パスワードを使用する場所に保管しておくことは危険です！

パスワードは

- ○　**ノートに書いて安全に保管する**
- ○　**パスワード管理アプリ※を利用する**

などして保管するようにしましょう！

※利用するパスワード管理アプリの安全性については、十分検討しましょう。

Twitter
@IP_cybertaisaku

石川県警察本部生活安全部サイバー犯罪対策課
076－225－0110
cyber@police.pref.ishikawa.lg.jp

Instagram
IP_cybertaisaku