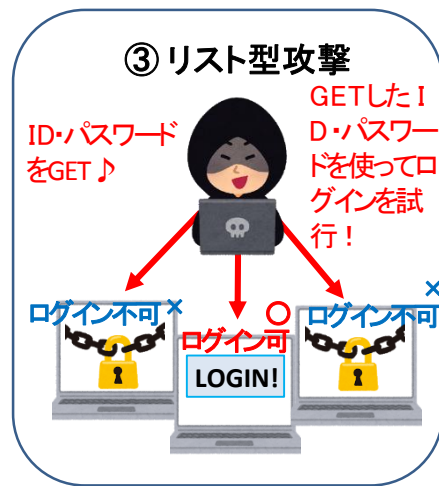
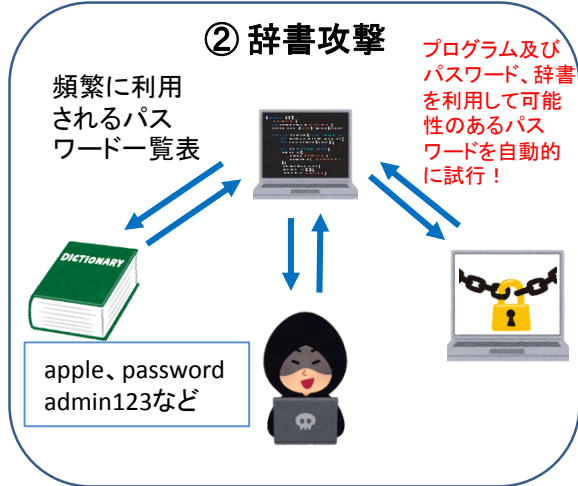


お使いのパスワード Safety or danger 自信を持って安全だと言えますか？

犯人は、あらゆる手口で銀行口座やネットバンキングのID・パスワードを盗み取り、不正送金や不正アクセスなどを敢行しています。



- ① 総当たり型攻撃 → 文字の組み合わせを全て試す
- ② 辞書攻撃 → パスワードによく使われる文字列を手当たり次第試す
- ③ リスト型攻撃 → ウェブサービス等の保管情報が漏えいしたものが悪用される

これらの攻撃を防ぐためには
“作業に膨大な時間をかけさせる”
ということが重要になります。

- × ログイン用パスワードに数字10桁のみを使用した場合 → 100億通り
- 英大小文字+数字+代表的な記号(26個と仮定)を含めた10桁の場合 → 約2785京97兆6009億通りの組み合わせ

機械入力でも
事実上突破不可能



パスワードの安全性を高めるためのポイント

1. パスワードの文字列を長めに設定する(10桁以上を推奨)
2. インターネットサービスで利用できる文字種(大小文字、数字、記号)を組み合わせる
3. 推測されやすい単語、生年月日等の単純な文字の並びの設定は避ける
4. パスワードの使い回しをしない