Cyber Security Information サイバー セキュリティ インフォメーション 2022 Vol.4

狙われやすいパスワードを設定していませんか？

SNSの投稿・プロフィールから推測できるパスワードや、簡単なパスワードを設定していると、SNSやショッピングサイトのアカウントが乗っ取られる不正アクセス被害にあう危険性が高まります。

また、パスワードを使い回していたり、流出したのに放置したりすれば、次のような攻撃を使ってパスワードが解読される危険性があります。

安全なパスワードの設定と管理のためのポイント

○パスワードの使い回しはゼッタイにダメ！
○数字と英字（大・小文字）と記号を組み合わせてケタは多く！
○多要素認証を設定しましょう！（詳しくは下の欄で！）

ちょっと豆知識　パスワードの組合せの数について
数字10個を使って4ケタのパスワードを作るときの組合せの数はわかりますか。
「10個の中から1つ選ぶ」を4回繰り返す＝10×10×10×10＝1万通り（10の4乗）になります。
数字と英字（小文字のみ）で8ケタだと、2兆8,211億990万7,456通り（36の8乗）
数字と英字（大、小文字）と記号32個で10ケタだと、なんと5,386京1,511兆4,094億9,000万通り！（94の10乗）

組合せが多いほど総当たり攻撃でも解読が大変だよね。

IDやパスワードは誰にも教えないで！

元交際者のSNSを乗っ取り、なりすまして投稿したという不正アクセス事件が起きています。

親しい間柄同士でも、SNSのID・パスワードを教えたり、お互いに共通するワードでパスワードを設定したりすると、このようなトラブルを招きかねませんので、やめましょう。

たとえ他人のID・パスワードなどを知ったとしても、勝手に他人のアカウントにログインをすると、不正アクセスの犯罪になりますので、いたずらでもログインしてはいけません。

アカウントの安全のために、多要素（たようそ）認証を使いましょう

アカウントのログイン設定で、パスワードに加えて指紋認証やアプリ認証システムを使用するように設定すると、パスワードが破られた場合の不正アクセス被害を防ぐことができます。

このように、異なる要素（本人が知っているパスワード、本人の生体情報、本人が持っている物）を二つ以上組み合わせて本人確認することを多要素認証と呼びます。

皆さんが利用しているサービスのセキュリティ設定で、多要素認証を設定することができれば、積極的に使ってアカウントを守りましょう。

北海道警察サイバーセキュリティ対策本部