TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2023年
第3号

リスト型攻撃に注意しましょう！

～ID・パスワードの使い回しは危険です～

リスト型攻撃とは？

「リスト型攻撃」とは、フィッシング等の手段で入手した第三者のIDとパスワードを用いて、ウェブサイト等に不正アクセスを試みる攻撃です。

様々なサービスで、同じIDとパスワードを使い回していると、どれか一つのサービスからその情報が漏えいしたときに、他のサービスも不正アクセスされ、「SNSアカウントの乗っ取り」、「不正送金」、「個人情報の流出、改ざん」などの被害に遭うおそれがあります。

被害防止のため、以下の対策を心掛けましょう。

被害に遭わないための対策

○　IDとパスワードは、利用サービスごとに違うものを使う

サービスごとに違うIDとパスワードを使用すると、被害を最小限に抑えられます。

○　パスワードは英数字記号を使い、長くて複雑なものにする

単語や生年月日を使ったり、短くて単純なパスワードは、簡単に推測されてしまいます。英数字記号を組み合わせた推測されにくいものを設定しましょう。

○　IDとパスワードは、適切に管理する

様々なサービスで異なるIDとパスワードを使用すると覚えきれませんが、暗号化対応の信頼できるパスワード管理アプリやパスワード管理専用ノートを作るなど、他人に知られないように管理しましょう。

○　多要素認証を利用

可能であれば、指紋認証や顔認証等の生体認証、認証アプリ等、複数の認証を設定しましょう。

○　ログイン履歴、ログイン通知メールの定期的な確認

不正なログインがないか定期的にログイン履歴、ログイン通知を確認しましょう。

○　被害に気付いたら直ちにパスワードリセット等を行う

身に覚えのないログイン通知等が届いたら直ちにパスワードを変更し、被害拡大を防ぎましょう。

不正アクセス被害を受けた場合は、警察への通報をお願いします！

【参考】
2013年8月の呼びかけ：IPA 独立行政法人 情報処理推進機構
https://www.ipa.go.jp/security/txt/2013/08outline.html
総務省：リスト型攻撃対策集について
https://www.soumu.go.jp/main_content/000265404.pdf
内閣サイバーセキュリティセンター（NISC）：インターネットの安全・安心ハンドブック第3章
https://security-portal.nisc.go.jp/guidance/pdf/handbook/handbook-03.pdf