適切なパスワードを付ける

リスト型攻撃の流行

流出したパスワードのリストを用い、別のサイトでログインできるか順番に試す攻撃方法を「リスト型攻撃」と呼びます。

同じパスワードを複数のサイトで使い回していた場合は、複数サイトでアカウントハッキングを受ける危険性があります。
また、ハッキングされたサイトより、メールアドレス・氏名・住所・カード番号などの個人情報が攻撃者の手に渡る可能性があります。

更に、収集されたメールアドレス宛にフィッシングサイトが送られてくるなど、繰り返し攻撃を受ける可能性もあります。

適切なパスワードを付ける

このようなリスト型攻撃に対処する為には、サイトごとに異なるパスワードを設定することが重要です。

一般には、英数字や記号を組み合わせたランダムなパスワードを設定することが良いとされています。
しかし、ランダムなパスワードをいくつも記憶するのは難しく、簡単なパスワードを使い回した結果、被害を受けるケースが多くなっています。
この場合は、後述する「パスワード管理ソフト」を利用し、適切に管理されることをお勧めします。

また、最近ではパスワードに長い文字数が設定できるサイトが増えています。
「ランダムで複雑なパスワード」を覚えるのが難しい場合は、「パスフレーズ」を設定されることをお勧めします。
「パスフレーズ」とは、自分の覚えやすい単語をいくつか組み合わせて、文章のようにしたパスワードです。パスワードに記号が使える場合は、一部の文字を記号に置き換えたパスワードに変更すると、より強固なパスワードとなります。
パスフレーズの一部をサイトごとに変えることにより、使い回しをしなくても覚えやすいパスワードになります。

NetStable での検知

NetStable では、初期設定のパスワードのまま運用している通信を検知するシグネチャがあります。※一部抜粋

- 2000385 Default Basic Pass 1
- 2000386 Default Basic Pass 2
- 2000387 Default Basic Pass 3
- 2000388 Default Basic Pass 4
  機器の認証画面において、デフォルトパスワードでログインしようとする通信を検出するシグネチャです。

- 2000590 Global Telnet Password Request 1
- 2000591 Global Telnet Password Request 2
  Telnet サーバに向けて簡単なユーザ名・パスワードでログインしようとするときの通信を検出するシグネチャです。

パスワードの管理方法

1.「パスフレーズ」を利用する
パスワードを自分で覚えて管理する場合は、上記のようなパスフレーズを利用したパスワードにされることをお勧めします。
ポイントとして、「覚えやすくて長い文章」「サイトごとに一部を変える」「同じパスワードを使い回さない」ことを意識してください。

2.「パスワード管理ソフト」や「パスワード保存用アプリ」を利用する
このようなソフトを利用する場合は、「パスワード作成機能」を活用し、英数字と記号を組み合わせたランダムなパスワードを利用してください。
パスワード管理ソフトを起動するためのパスワードや、パスワードデータの保存先の安全性、クラウドサービスの場合は、信頼性等を考慮し、利用するかどうかを検討してください。

まとめ

- パスワードの使い回しはリスト型攻撃の影響を受ける
- ランダムで複雑なパスワード以外にも、「パスフレーズ」を設定する方法もある
- 必要に応じて、パスワードを管理するソフトを活用する