添付資料

【今月の呼びかけ】

「 パスワード　ぼくだけ知ってる　たからもの ※1 」

※1　第6回IPA情報セキュリティ標語・ポスターコンクール(2010年度実施)標語部門
大賞 坂井 敏法 さん(新潟県　新潟市立万代長嶺小学校)

今年 4 月から 5 月にかけて、1 億件を超える ID やパスワードを含むアカウント情報漏えい事件などが発生しました。該当するサービスの利用者は、漏えいしたアカウント情報を不正に使用される“なりすまし”（不正アクセス）を防ぐため、パスワードの変更といった対処が求められています。

今までも“なりすまし”の被害は発生していましたが、今回は漏えいした情報の量が多いため、ID やパスワードを他のサービスでも使い回ししていた利用者の情報が含まれている可能性も高く、その場合、それらのサービスにおいても“なりすまし”をされ、被害が拡大する可能性があります。

大手のウェブメールサービスのアカウント情報を盗もうとするフィッシング※2 の手口も横行しており、ID やパスワードを使い回ししていると、同様に被害拡大の原因となり得ます。

オンラインサービスでは、“なりすまし”をされた場合、金銭的な被害等を受ける危険があり、これを防ぐためには、パスワードの作成や管理に十分な注意が必要です。オンラインサービスで利用する ID やパスワードは、それを悪用しようとしている者に常に狙われていることを意識し、適切に管理してください。

※2　フィッシング（Phishing）：正規のウェブサービスや金融機関など実在する会社を装ったメールを利用して偽のウェブページに誘導し、それを見た利用者の ID やパスワードなどを詐取しようとする行為のこと。

（1）ID やパスワードを使い回すことの危険性

近年は数多くのオンラインサービスが存在しており、利用者は各サービスについてそれぞれ ID やパスワードを登録、管理することになります。この際、覚えきれないといった理由で、同じ ID やパスワードを登録する“使い回し”が行われがちですが、使い回しをすると、そのうち一つのサービスでアカウント情報が漏えいした場合、連鎖的になりすまし被害が拡大する恐れがあります。

次に、使い回しにより発生しうる被害拡大の一例を説明します（図 1-1 参照）。

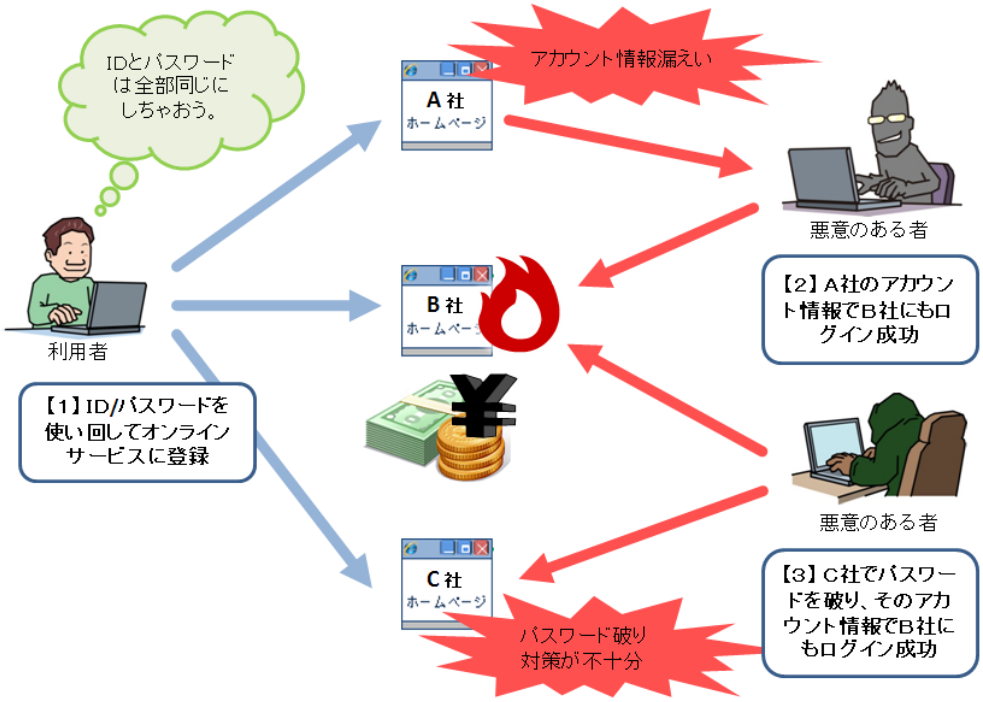

図 1-1：ID やパスワード使い回しによる危険性

【1】ID やパスワードを使い回してオンラインサービスに登録

複数のサービス（図では A、B、C 社）の利用者が、パスワード管理を簡略化するために、各社にログインするための ID やパスワードを全て同じにしていたとします。

【2】A 社のアカウント情報で B 社にもログイン成功

A 社で情報漏えい事件が発生してパスワード情報が流出してしまい、悪意ある者が、流出した情報を元に B 社のウェブサイトへのログインを試行すると、B 社でもログインに成功してしまうケースです。

【3】C 社でパスワードを破り、そのアカウント情報で B 社にもログイン成功

悪意ある者が、パスワードを破ろうとする総当たり攻撃※3 や辞書攻撃※4 への対策が不十分な C 社のウェブサイトで、ID やパスワードを入手します。その情報をもとに、B 社のウェブサイトでログイン試行すると、B 社でもログインに成功してしまうケースです。

※3　何らかの規則にしたがって文字の組み合わせを総当たりで試行する、いわゆる力ずくの攻撃方法。

※4　辞書にある単語などを組み合わせながら試行する攻撃方法。

パスワードの使い回しをしないことは、“なりすまし”の**被害を拡大させない**ための重要なポイントの一つです。

根本的に“なりすまし”の**被害に遭わない**ためには、ID やパスワードを扱う上での基本的な対策が必要です。

（2）なりすまし対策の基本

“なりすまし”対策の基本は、**パスワードの強化・保管・利用**の 3 点に集約できます（図 1-2 参照）。この 3 点のうち、1 点でもおろそかにしてはいけません。

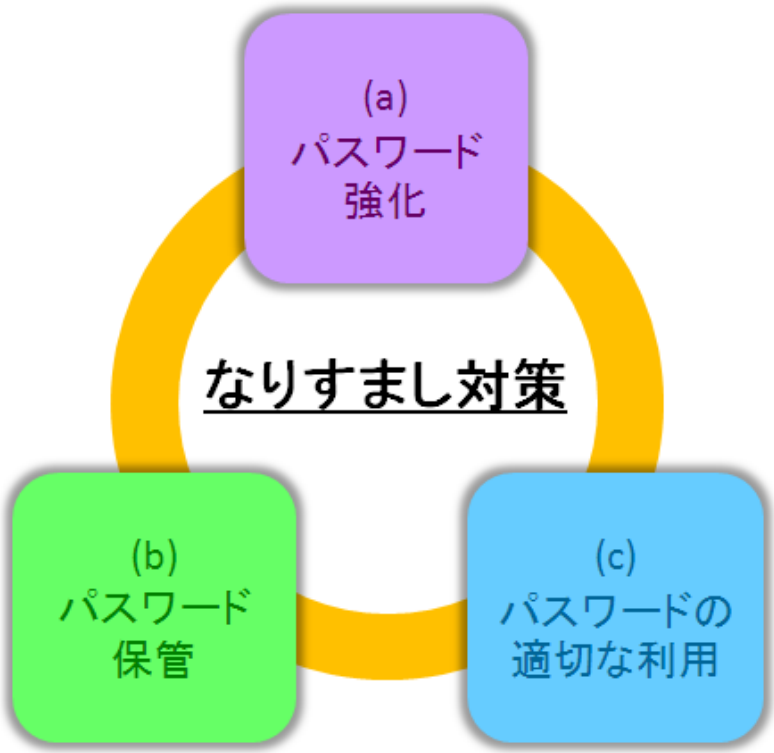

図 1-2：なりすまし対策

以下のポイントを参考に、ID やパスワードの管理を適切に実施してください。

（a）パスワードを強化する

破られやすいパスワードを使用していると、総当たり攻撃や辞書攻撃を受けることによりパスワードを破られる危険性が高くなります。次の条件を満たすよう、破られにくいパスワードを使用し

てください。

- 英字（大文字、小文字）・数字・記号など使用できる文字種全てを組み合わせる
- 8 文字以上にする
- 辞書に載っているような単語や名前（人名、地名）を避ける

（b）パスワードを適切に保管する

破られにくいパスワードを作成したあとは、その保管について以下の項目にも注意してください。

- パスワードをメモする時は、ID と別々にする

  長く複雑なパスワードを作成すると、記憶するのは大変です。この場合、紙にメモしても構いませんが、ID とパスワードは別々に保管することを勧めます。仮にパスワードが知られたとしても、どの ID に対応するパスワードなのかがわからなければ、なりすましは難しくなります。

- 定期的に棚卸しをする

  古い ID を放置していると、時間をかけてパスワードを破られる危険性が高まります。利用サービスを定期的に棚卸しして、利用しないサービスに関しては登録解除することを勧めます。

（c）パスワードを適切に利用する

サービス利用時にパスワードを入力する際にも注意が必要です。

- ネットカフェなど、不特定多数が利用するパソコンでは、ID やパスワードを入力しない

  破られにくいパスワードを設定していても、ネットカフェ内のパソコンにパスワードを盗むウイルスが仕掛けられていたら簡単に盗まれてしまいます。自分の管理下にないパソコンでは、ID やパスワードを必要とするオンラインサービスの利用は避けるようにしてください。

- ワンタイムパスワードなどのサービス（二要素認証、二段階認証等）を利用する

  オンラインバンキングやオンラインゲームなどでは、その時だけ有効なパスワードを発行する「ワンタイムパスワード」というサービスを提供していることがあります。ID やパスワードを盗むウイルスに感染していても、一度きりのパスワードのため、仮に盗まれてもその後悪用されることはありません。また、フィッシングの手口に引っ掛かり、ID やパスワードを盗まれたとしても、同様に、悪用されることはありません。ただし、ワンタイムパスワードのトークン※5 を他人に渡さない、トークンに表示されているパスワードを他人に教えない、信頼できるサイトに対してのみパスワード入力する、などの基本的対策は必須です。

  オンラインサービスによっては、ログインしたタイミングでお知らせメールを送信する機能（ログインアラート機能）を提供している場合があります。身に覚えのないログインアラートメールが届いた場合は、即座にアカウントをロックすることにより、被害を最小限に留めることができます。

  ※5　トークン（Token）：利用者の認証をより確実にするために使用する、ハードウェアまたはソフトウェアのこと。ハードウェアの場合には、ポケットに入る程度に小さなものが多く、時刻に基づくワンタイムパスワードを表示したり、暗号鍵や生体認証のための情報を格納しておくなどの機能がある。

上記のなりすまし対策を行っていても、セキュリティ対策の基本であるウイルス対策ソフトの導入は必須です。オンラインサービスへログインする時に利用者が入力した ID やパスワードを盗み取るウイルス（キーロガー）が確認されています。このようなウイルスに感染して情報を盗まれないために、ウイルス対策ソフトを導入し、ウイルス定義ファイルを最新に保つようにしてください。

さらに、OS（オペレーティングシステム）やアプリケーションソフトの脆弱性対策も必須です。

また、Internet Explorer などのブラウザには、ID やパスワードを保存する機能がありますが、保存された情報を盗むウイルスも確認されています。盗まれるリスクを減らすため、ブラウザには ID やパスワードを保存しないようにすることを勧めます。