滋賀県警察
サイバーセキュリティ情報SHIG@
サイバー犯罪からあなたを守るセキュリティ情報をお届けします。
R４年度 No.３

「二要素認証」・「二段階認証」で不正ログイン防止対策を推進しましょう。

フィッシングにより、ID・パスワードを盗み取られるケースが多数発生しています。
特定のインターネットのサービスを利用するときに必要なID・パスワードですが、フィッシング等により盗まれたり、推測されたりして不正にログインされると、クレジットカード番号情報等の個人情報を盗み取られたり、無断で買い物をされたりする被害が発生します。
不正ログイン防止のためのシステムに、「二要素認証」と「二段階認証」があります。
二要素認証や二要素認証は、ID・パスワードによる認証を補足するもので、利用することで、不正ログインのリスクが減少します。
サービス提供会社が、これらの認証方法を導入している場合は、ぜひ利用してください。

二要素認証とは？

通常、認証は、IDとパスワードの組み合わせで行います。
そのIDとパスワードに別の「要素」を組み合わせなければ認証できない方式を、二要素認証と呼びます。
認証するための要素は大きく分けて３つあります。
①知識情報（知っているもの）・・・ワンタイムパスワードやセキュリティコード等
②所持情報（持っているもの）・・・ICカードやUSBキー等
③生体情報（本人自身に関するもの）・・・静脈パターンや指紋等
これらの要素から２つの要素を組み合わせるのが二要素認証です。
さらに、複数の要素を組み合わせる認証を多要素認証と言います。

二要素認証とは？

二要素認証に似た認証方式に「二段階認証」があります。
二段階認証とは、ID/パスワードに加えて、ワンタイムパスワードやセキュリティコード等でさらに認証を行う方式のことです。二段階認証においても、多要素にすることで安全性が高まります。

リスクベース認証とは？

リスクベース認証は、普段使っていない機器から接続があった場合に、追加で認証を求める認証方式のことです。

二要素認証の例	二段階認証の例	リスクベース認証の例
ID/パスワード（知識情報）	ID/パスワード	普段使っていない機器で接続
＋	＋ 一旦ログイン	↓
ICカード等（所持情報）	ワンタイムパスワード	ID/パスワード
OR	OR	OR
指紋等（生体情報）	セキュリティコード	ワンタイムパスワード等

➢ **二要素認証や二段階認証も万全でありません。**
ワンタイムパスワードを盗み取る手口もありますので、認証作業は慎重に実施してください。

«サイバーコネクトSHIG@»定期的にソフトウェアの脆弱性情報をチェックしましょう。

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）　県警Webページ→