

サイバーセキュリティ パートナーシップだより



令和元年8月 山口県警察本部生活環境課

不正ログイン対策① ～ 二段階認証の活用 ～

インターネット上で利用している各種サービス（アカウント）は、IDとパスワードを用いた認証方法が多く採用されていますが、IDとパスワードが流出した場合、第三者からの不正ログインを防ぐことができません。

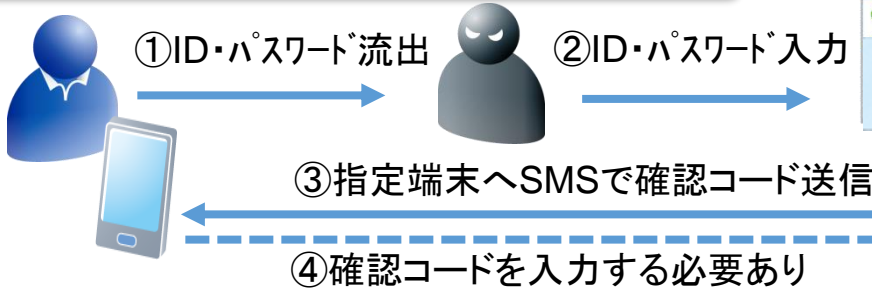
しかし、従来のパスワードに異なる認証方法を追加（二段階認証）すれば、IDとパスワードが流出しても不正ログインを防ぐことができます。

IDとパスワードのみによる認証



IDとパスワードがあれば、誰でもログインが可能

二段階認証（例）



確認コードを受け取るため、指定端末が必要であり、第三者のログインが困難

- 広く利用されているサービス（アカウント）のほとんどは、既存の認証方法から二段階認証に変更することが簡単に可能です。
(iPhone、Google (Gmail)、Amazon、Yahoo! Japan、facebook など)
 - 二段階認証を許可された端末は、2回目以降の二段階認証は不要です。
 - 認証方法は、主に次の3種類に分けられます。
 - 知識認証 ～ パスワード、PINコード
 - 生体認証 ～ 指紋、顔、静脈、虹彩
 - 所有物認証 ～ ICカード、キャッシュカード、トークン など
 - 異なる複数の認証方法が、不正ログイン防止に非常に効果的です。
- ※ 上の例では、ログインにパスワード（知識）と端末（所有物）が必要です。

**被害防止のために
十分なセキュリティ対策を！**

サイバー犯罪相談窓口
TEL 083-922-8983
cyber.soudan@police.pref.yamaguchi.lg.jp