

ID・パスワードの

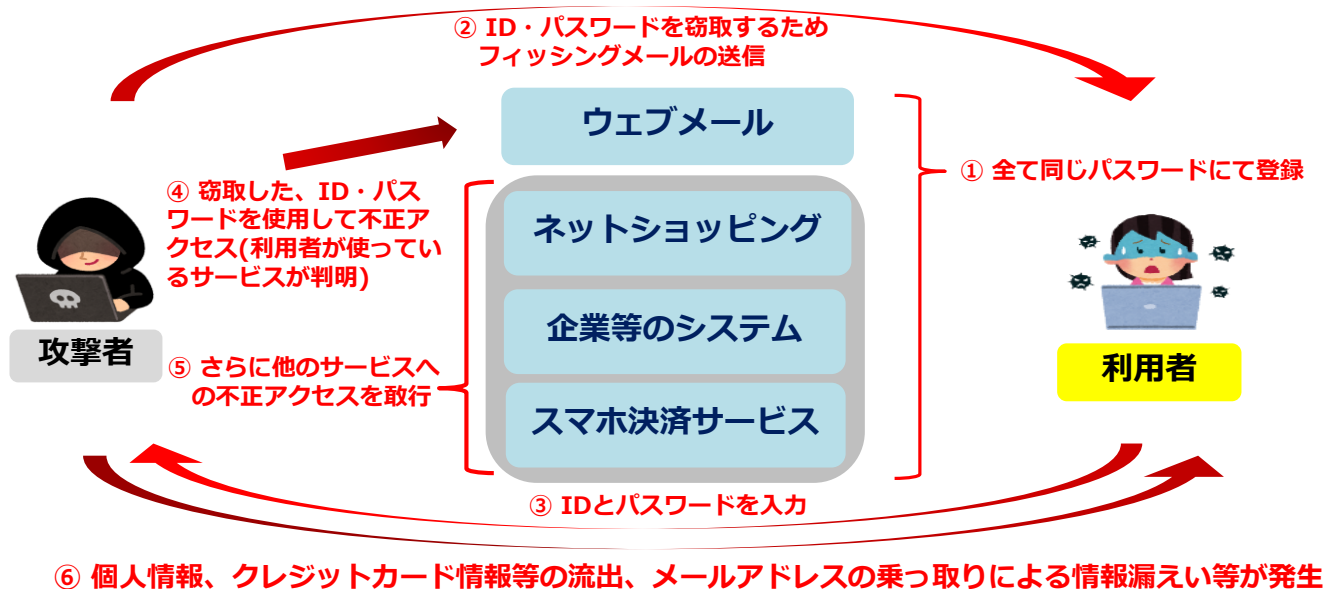
使い回しは危険です！

フィッシングによるID・パスワードの流出

フィッシング対策協議会の調査により、インターネット上の何らかの個人認証を行うサービスのうち、76.9%が「IDとパスワード」のみの認証しか行っていないことが判明しました。

(2019年7月現在)

同じIDとパスワードを複数のサービスで使用すると、いずれかが不正アクセス被害を受けた場合、他のサービスでも被害を受けるリスクがあります。



対策

1. ID・パスワードを把握し、整理する

- (1) 使用しているID・パスワードを全て書き出す
- (2) 書き出した内容を、ネットバンキング、クレジットカード情報が含まれるもの、WEBメール、全く使っていないサービスなど用途に合わせて分類する。
- (3) 全く使っていない、今後使用する予定がないウェブサービスは退会する。

2. パスワードの作成、保管

パスワードの文字列は、大小英文字、数字、記号を組み合わせ、氏名、生年月日、連続した文字列、キーボードの文字列の順番は使わない。

パソコン内には保存せず、メモ帳やパスワード管理ソフトを使い保管する。

3. 個人利用と企業等で使用しているID・パスワードは必ず分ける。

各サービス毎にパスワードが違う場合は、一つが不正アクセス被害を受けても連鎖的な被害を抑える事になりますので、**パスワードは個別に設定する対策が有効です。**

ここを
チェック

インターネット取引におけるID・パスワードの使い回しによる不正使用被害にご注意ください
<https://www.j-credit.or.jp/customer/attention/unauthorized.html>

被害を受けたらまずは警察へご相談ください



茨城県警察サイバー攻撃特別捜査隊
TEL：029-301-0110（内線5691）

