サイバーだより

栃木県警察本部
サイバー犯罪対策課
令和６年11月

多要素認証だけでは守れない！フィッシング攻撃の対策

多要素認証とは？

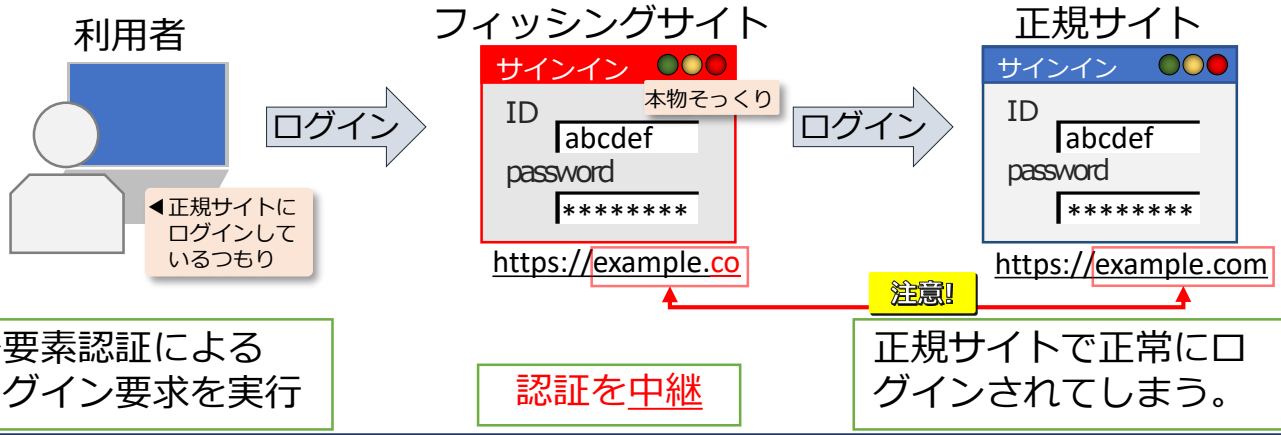
認証の３要素「知識情報」「所持情報」「生体情報」のうち２つ以上を組み合わせる認証方法のこと

- 知識情報：・パスワード ・ＰＩＮコード 等
- 所持情報：ワンタイムパスワード 等
- 生体情報：・指紋認証 ・静脈認証 等

2つ以上の要素を組み合わせる認証方法　セキュリティ高

多要素認証を突破するフィッシング攻撃

フィッシングサイトが利用者と正規サイトの間に割り込み、データを中継することで多要素認証をしていても不正ログインされてしまう。



利用者がとれる対策

フィッシングメールなどに添付のURLはタップしない。

フィッシングメールは、正規サービスのメールを元にして作られています。
メールに添付のURLについては、自分が要求したものでなければ押さないでください。

ログイン画面が同じに見えてもURLが正規サイトのものかを確認する。

フィッシングサイトは、正規サイトと同じデータを使用しているため、見た目では区別できません。上図のようにURLを確認することで見破ることができます。

パスワードレス認証を活用する。

最初からパスワードを使わなければ漏えいすることはありません。オーセンティケーター（サービスへのログインに使用するアプリ）によるセキュリティの強化をしましょう。

栃木県警察
Tochigi Police

栃木県警察ＨＰ(サイバーだより)
https://www.pref.tochigi.lg.jp/keisatu/n14/seikatu/cyber_cyber_dayori.html