

金融犯罪者は なりすましが得意だから



従来の
パスワード
対策では
危険です!!

フィッシングに耐性のある「多要素認証」が効く!

昨今、証券口座への不正アクセスが発生しています。その手口は、メールやSMSなどで実在する金融機関のウェブサイトを装い、フィッシングサイトへ誘導するものです。誘導先のサイトでIDやパスワードなどを入力してしまうと、これらの情報が盗み取られ、証券口座に不正アクセスされるおそれがあります。他にも金融犯罪者があなたのスマホやパソコンなどをマルウェアに感染させ、リアルタイムでそれらの端末を監視するとともに操作し、個人情報などを窃取するなどの犯罪がひろがっています。

パスワードを入力する必要がない、
安全性の高い仕組みでなりすましを防ぐ!



パスキーによる認証

パスワードの代わりに生体認証(指紋認証や顔認証)、PINコードなどを使ってログインする、より安全で簡単な次世代認証方式です。パスワードを覚える手間もなくセキュリティと利便性を両立できます。



PKI(公開鍵基盤)による認証

公開鍵と秘密鍵のキーペアからなる技術で、信頼できる第三者(認証局)を通じて、本人であることを電子的に証明する仕組みです。マイナンバーカードを認証に利用することもできます。



メールやSMSに届くワンタイムパスワードを利用した多要素認証は、リアルタイムフィッシングに脆弱なほか、中間者攻撃、マルウェアによる窃取等により突破される場合があります。

リアルタイムフィッシングとは…金融犯罪者が利用者から入力された認証情報を即座に盗み取り、リアルタイムに正規サイトへ不正ログインする手口

パスキーやPKIには以下のメリットがあります。

メリット
01

パスワードレスでより安全

端末に保存された秘密鍵や電子証明書を使用し認証するため、パスワードの入力が不要

メリット
02

フィッシングサイトをブロック

端末側で本物サイトを確認するため、人間に代わってフィッシングサイトをブロック

秘密鍵や電子証明書とは…いずれも数千桁のランダムな数値で複製や口伝が困難なもの

金融機関から強力な認証方式が提供されている場合は積極的に利用しましょう。

つまり!

もしもフィッシングサイトに誘導されても、パスキー・PKI認証があなたを守る!



フィッシングメール・
SMSを送付



受け取ったメール等
から偽サイトを
クリックしてログイン



偽サイトを
ブロックするため
ログインできない



そもそも攻撃者が
盗もうにも盗むべき
「パスワード」が
存在しない

大切な資産は、奪わせない。

金融庁
Financial Services Agency



警察庁
National Police Agency

JBA 一般社団法人
全国銀行協会

Face to Face 一般社団法人
全国信用金庫協会

信用組合 一般社団法人
全国信用組合中央協会

ろうきん 一般社団法人
全国労働金庫協会

JSDA 日本証券業協会
Japan Securities Dealers Association