

フィッシング詐欺被害にご注意ください

最近、銀行を装った偽の SMS や電子メールを送るなどしてインターネットバンキングのログイン画面を精巧に模倣した偽のホームページに誘導し、インターネットバンキングにおける ID やパスワード、合言葉などの認証情報を入力させて盗み取り、**口座から預金が不正に送金される被害が多発**しております。

この SMS および電子メールは偽のウェブサイトへ誘導し、お客さまの口座情報や個人情報を不正に入手するためのもので、リンク先のサイトは極めて精巧に金融機関サイトを模倣しています。

- 不審な SMS やメールは開封しない
- SMS やメールに記載された URL に安易にアクセスしない
- URL へアクセスする前に正しいホームページの URL であるかを確認する

もし不審なメールや電話や訪問を受けた場合は、最寄りの警察や下記フリーダイヤルにご相談ください。

«お問い合わせ先»

株式会社佐賀銀行 業務統括部 金融犯罪対策室

TEL 0120-504-200

<https://www.sagabank.co.jp/>

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!

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

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!

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

R 355さん 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