

金融機関等を装ったフィッシング詐欺にご注意ください！

証券会社や銀行、携帯電話会社等を装ったメールやSMS（ショートメッセージ）を送信して偽サイトに誘導し、お客さまのIDやパスワード等を盗み取る犯罪「フィッシング詐欺」が全国的に発生しています。

主な手口は、メールやSMSのリンク先をクリックしたり添付ファイルを開くと、パスワード等の重要情報を入力させる偽サイトに誘導され、入力した情報を元に悪意のある第三者がお客さまのオンラインサービスを不正利用するというものです。

万が一、不審なメールやSMS等を受信した場合はすぐに削除し、記載されたリンク先へのアクセスやパスワード等の入力には絶対にしないでください。

当社がメールやSMS、電話等でお客さまのパスワードをお尋ねすることは決してございません。

以下の状況で「パスワード」等を入力してしまった場合は、下記までご相談ください。

- ・いつもは見かけないような不審な画面等が表示され、パスワード等を入力してしまった場合
- ・いつもと違う操作に誘導され、パスワード等を入力してしまった場合
- ・不審なサイトにアクセスして、パスワード等を入力してしまった場合
- ・不審なメールやSMSのリンク等からパスワード等を入力してしまった場合

なお、当社では、京銀証券オンラインサービスについて、フィッシング耐性の高いパスキー認証を導入しておりますので、お客さまの大切なご資産を守るためにもパスキー認証のご利用を強く推奨いたします。

記

【ご連絡先：フリーダイヤル】

電話番号：0120-161-800

受付時間：平日 9：00～17：00（土・日、祝日、12/31～1/3 を除く）

【ご参考】

日本証券業協会ホームページ 「[不正アクセス等にご注意ください！](https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/index.html)」

https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/index.html

以 上