

2025年3月25日 更新
2025年3月12日
大和証券株式会社

大和証券をかたるフィッシングメールにご注意ください

大和証券を装ったフィッシングメールが発生しております。

大和証券を装った偽の電子メールが発生しております。偽のメールでは、「以下の URL をクリックして、セキュリティ更新を行ってください。」などとして、**偽のサイトの URL (当社と関係ないアドレスの場合と、「daiwa.jp/…」と表示されているが実は偽装の場合があります)**を表示し、**これをクリックさせてフィッシングサイトへ誘導し**、ログイン ID、ログインパスワード及び取引パスワードといった認証情報などを入力させようとしています。

身に覚えのないメールのリンクはクリックせず、またクリックしてしまった場合でも開いた画面に認証情報などを入力しないよう、ご注意ください。

万が一、偽のログイン画面に情報を入力してしまった場合は、速やかにログインパスワードを変更してください。

また、身に覚えのない取引があった場合には、直ちにお取扱いの**本・支店**☒、またはコンタクトセンター (0120-010101) までご連絡をお願いします。

ブラウザから当社の取引サイトをご利用される場合は、当社公式 URL (https://www.daiwa.jp/) を「お気に入り登録 (ブックマーク)」し、お気に入り (ブックマーク) 機能からのアクセスを推奨いたします。

不審な電子メール・SMS 等にご注意ください | 大和証券 (daiwa.jp)

■3/24 に確認された偽メールの例

(件名)

【重要なお知らせ】大和証券の安全な取引環境維持のための更新

(本文)

※本メールは重要なお知らせのため、メールによるお知らせを希望しないとご登録されたお客さまへも配信しております。

平素は大和証券をご利用いただきありがとうございます。

当社では、お客さまの大切な預金とお客さま情報をサイバー攻撃等の犯罪行為から守るため、定期的な安全更新を実施しております。

今回のセキュリティ強化では、お客さまの個人情報保護のための新しい暗号化技術を導入し、ログイン認証システムをより安全なものに更新いたしました。これにより、不正アクセスやデータ漏洩のリスクを大幅に低減することが可能となりました。

また、当社のセキュリティ専門チームが24時間体制でシステムを監視し、お客さまの資産を守るための対策を講じております。

▼以下の URL をクリックして、セキュリティ更新を行ってください。

[https\[://\]www.daiwa\[.\]jp/service/security/update/](https://www.daiwa[.]jp/service/security/update/)

(以下略)

■3/11 に確認された偽メールの例

(件名) 【重要】大和証券口座の確認のお願い

(本文)

いつも大和証券をご利用いただきまして誠にありがとうございます。

弊社では、お客様の資産並びに個人情報の保護を最重要課題と位置づけ、さらなるセキュリティ強化に努めております。その一環として、万一にも不審な取引の兆候が認められた場合、迅速かつ的確な対応が必要であると判断いたしました。つきましては、誠に恐縮ではございますが、下記 URL よりログインいただき、速やかにお客様ご自身の口座状況をご確認の上、所定の手続きを実施くださいますようお願い申し上げます。

【重要：アカウント確認のご案内】

[https\[://\]bienqui\[.\]com/*****](https://bienqui[.]com/*****) (偽サイトの URL)

なお、上記手続き完了後は従来通りのお取引が可能となりますが、確認が1営業日以内に完了されなかった場合、上記 URL は自動的に無効となります。あらかじめご了承くださいませようお願い申し上げます。

(以下略)

以上