

窃取した ID やパスワード等による不正アクセス・不正取引が発生しております

大和証券を装ったフィッシングメールでは、「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**したうえで、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。

また、マルウェア（ウイルス）等により、パソコンやスマートフォンからログイン ID、パスワード等を抜き取られる可能性も指摘されています。

第三者がそのような手口によりお客様のオンライントレードに不正にログインし、お客様の資産を利用して、有価証券等の売買等を行った事例も確認されました。

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や、身に覚えのないログイン・取引があった場合は、直ちにログインパスワードを変更してください。

また、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。

安心してお取引いただくため、セキュリティ対策等のご対応をお願いいたします。

- **身に覚えのない電子メール、SMS（ショートメッセージ）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。**
- お気に入り（ブックマーク）機能をご利用ください。
 - オンライントレードをご利用される場合は、メールのリンクからではなく、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）機能からアクセスすることを推奨いたします。
- OS やブラウザは常に最新の状態にアップデートしてください。
 - パソコンやスマートフォンの OS やブラウザをアップデートしないまま利用し続けることは危険です。OS やブラウザは常に最新の状態に更新してください。自動更新を設定すると便利です。また、ウイルス対策ソフトの導入及び更新もお願いいたします。
- オンライントレードの「ログイン追加認証」をご利用ください。
 - ログインパスワードに加えて、メールに送信されるワンタイムパスワードを入力することでログインできるようになる仕組みです。
 - 「ログイン追加認証」を利用いただくためには、事前にメールサービスの「情報用メール」のメールアドレスのご登録が必要です。
- 心当たりのないメール通知を受信された場合、直ちにご連絡ください。

- 弊社では、お客さまの身に覚えがないログイン・取引が行なわれた場合に、お客さまにすぐにお気づきいただけるよう、ログインやお取引などの操作が行なわれた場合の操作通知をメールでお届けしております。
- 万が一、心当たりのないメール通知を受信された場合、直ちに大和証券のお取引店またはコンタクトセンターまでお問い合わせください。

詳細につきましては、「[お客さまにお願いしたいセキュリティ対策](#)」をご参照ください。

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

なお、ログイン追加認証の設定方法等は以下をご参照ください。

【重要】 [オンライントレードのセキュリティ強化について \(2025 年 5 月 11 日実施 \(予定\)\)](#)

[| 大和証券 \(daiwa.jp\)](#)

■フィッシングメールの例① ※似たような様々な件名および本文で送信されています。

(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/>

(以下略)

■フィッシングメールの例② ※似たような様々な件名および本文で送信されています。

(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すようお願い申し上げます。

（以下略）

以上