

【重要】 詐欺電話に注意してください

三菱 UFJ 銀行（以下「当行」といいます。）または電手・でんさいコールセンターを騙って悪意ある第三者から、「更新手続きが済んでいないため、一時的に取引を制限させていただきます」などと不安を煽り、言葉巧みに、お客さまのメールアドレスやパスワードを聞き出したり、アプリのインストールを促そうとする不審な電話（自動音声含む）が確認されています。そのような電話があった場合は、**すぐに電話を切り、誘導された操作を絶対に行わないようご注意ください。**

<確認されている事例>

■ 不審な電話

- 「こちらは三菱 UFJ 銀行 電手・でんさいコールセンターです。経理担当は 1 を、経理担当以外は 2 を選択押してください」となどの自動音声の電話がかかってくる。
- 当行または電手・でんさいコールセンターを騙る人物から、以下のような電話がかかってくる。
 - ・「証明書の手続きがまだ完了していません」
 - ・「セキュリティの強化・更新が終わっていないため更新が必要」
 - ・「FAX を利用できなくなるため、レポート（ウイルス対策ソフト）を利用する必要がある」
 - ・「インターネットバンキングがウイルス被害にあっている。ウイルス対策ソフトを導入する必要がある」

■ 詐欺サイトへの誘導・操作指示、遠隔操作アプリの意図しないダウンロード

- メールアドレスや電話番号を聞き出す（しつこく聞き出すケースもあります）
 - ➡ **メールアドレスや電話番号を教えると、不審な URL 付き E メールやショートメールが送られてきます。**
絶対に教えないでください
- 聞き出したメールアドレスや電話番号宛に、URL 付き E メールやショートメールが送られてきて、その URL にアクセスするよう求められる。
 - ➡ **URL をクリックすると、遠隔操作アプリや画面共有アプリのインストールが意図せず行われます。インストールするとお客さまのパソコンが犯人に遠隔操作されます。（閲覧されることで口座情報などを見られる可能性もあります）**
絶対に URL をクリックしないでください
- 表示された画面に従って、ログインパスワード、確認番号などのお客さま情報を入力するよう求められる。
 - ➡ **入力すると騙し取られた認証情報等をもとに、犯人に不正なアクセス・取引を実行されてしまいます。**
絶対に入力したり、犯人に教えたりしないでください

当行から上記のようなご案内（電話、E メールやショートメール）は絶対にいたしません。万が一、このような連絡があった場合には、電話、E メールやショートメールのリンク先にお取引に必要な情報（お客さま番号、ユーザ ID、パスワード、確認番号等）を絶対に回答しないようお願いいたします。

<改めてのお願い>

全国的に、金融機関や国内外の大手企業を騙った不審な電話、偽 E メール、偽ショートメッセージが確認されています。お客さまの大切な資産を守るためにも、不審な電話には従わず、電手決済サービスをご利用いただく際は、BizSTATION 認証をご利用のお客さまは当行ホームページから、DenPASS 認証をご利用のお客さまは予めお気に入り登録いただいた電手 WEB システム専用 URL (※) から、それぞれログインいただくようお願いいたします。

※DenPASS 認証 URL・・・ <https://bizstn.bk.mufg.jp/dente/> (お気に入り登録のうえご利用ください。)

- 【1】 不審な電話はすぐに電話を切る
- 【2】 不審な人物にメールアドレスや電話番号、パスワードなどは絶対に教えない (不審な画面に入力しない)
- 【3】 不審な URL はクリックしない

少しでも「おかしい」と感じたら、電話を切り、操作を中断し、速やかに電手・でんさいコールセンターへご連絡ください。必要に応じ、貴社のセキュリティ担当、警察への連絡をご検討ください。

お問い合わせ先

三菱UFJ銀行

0120-103-172 (銀行営業日 9:00~17:00※)

電手・でんさいコールセンター

フリーダイヤルがご利用いただけない場合は 03-5730-1963 (通話料有料)

※ 自動音声メッセージが流れますので、電手決済サービス「1」を押してください。

ご照会内容によっては、翌営業日のご回答となることがございます。恐れ入りますが、予めご了承ください。

※ご参考

- 三菱 UFJ 銀行の法人向けインターネットバンキング (BizSTATION) からのご案内もご参考ください。

(<https://www.bk.mufg.jp/houjin/mufgbiz/index.html>)

- 警視庁の注意喚起もご参考ください。

(<https://www.npa.go.jp/bureau/cyber/koho/caution.html>)