

JFマリンネットバンクのセキュリティ対策強化の実施について

安全のため、限度額はお客さまの利用目的に合わせて「適切な金額」を設定してください。

1日あたりの振込・振替上限額と限度額変更日

ワンタイムパスワード	上限額	限度額引き上げ・引き下げ変更日	
		引き上げ	引き下げ
利用あり	500万円	受付日の5日後に引き上げられます。	操作完了後、即時に変更されます。
利用なし	50万円		

1日あたりの税金・各種料金の払込み限度額

収納先	1日あたりの払込限度額	限度額引き上げ・引き下げ変更日	
		引き上げ	引き下げ
民間収納機関	20万円	受付日の5日後に引き上げられます。	操作完了後、即時に変更されます。
国・地方公共団体	限度額なし	—	—

(補足) 限度額引き上げの変更日

24:00	24:00	24:00	24:00	24:00	24:00
1日目 (受付日)	2日目	3日目	4日目	5日目	6日目以降
即時に変更されない					引上げ※

※ 受付日から、午前0時を5回経過したタイミングで変更されます。利用可能時間における引き上げ後の限度額でお取引いただけます。金曜日の0:00～23:59:59までに限度額を変更された場合、水曜日に反映されます。

※ その他、事前周知された特定日・時間帯に休止になる場合がございます。詳細はJFマリンバンクホームページ等をご確認ください。

JFマリンバンクを装ったフィッシングメールにご注意ください！

偽メールに気をつけてください



ポイント

操作を焦らされていませんか？

メールの件名や内容で慌てず、まずは公式サイトからログインし、あわせて身に覚えのない取引がないか確認しましょう。

- <メールの件名> ※他業態等で実際に確認されたもの
- ・【xxネットバンク】利用停止のお知らせ
 - ・【xxネットバンク】緊急停止のご案内
 - ・【xxネットバンク】お客さま情報等の確認について
 - ・【xx組合】振込(出金)、ATMのご利用利用停止のお知らせ
 - ・【緊急】xxネットバンク お取引を保留(必ずご確認ください)



偽サイトに気をつけてください



ポイント

フィッシングメールなどに記載されているURLにはアクセスしない!

偽サイトにはID・口座番号・パスワード等は絶対に入力しないでください。

<要注意>

特にワンタイムパスワードを漏洩すると、犯人側で送金が可能となり、**貯金残高の全額を不正送金されるリスクがあります。**



フィッシングメールの被害に遭った場合は最寄りの店舗へご相談を！
(被害に遭われたと思ったら…緊急停止を実施してください。)

偽のセキュリティ警告（サポート詐欺）にご注意！！

サポート詐欺のリスクがありますので、気をつけてください！！

～サポート詐欺の手口～

サポート詐欺手口の流れ～その①～

- PC等の画面に「ウイルスに感染しました」等の**偽のセキュリティ警告**が表示されます
- 偽の警告画面は**偽のサポート窓口へ電話するように誘導**します



サポート詐欺手口の流れ～その②～

- 偽のサポート窓口へ電話すると、犯人が**PC等を遠隔操作できるように誘導**します
- JFマリンネットバンクの**ID・パスワードワンタイムパスワード**を聞き出すことも！！



サポート詐欺手口の流れ～その③～

- 犯人は、PC等からウイルス除去をしたように見せかけ、**サポート代金の振込を要求**します
- 犯人は、お客さまから聞き出したJFマリンネットバンクのパスワード等を使い、**お客さまの口座から犯人の口座へ不正送金**します



お客さまへのお願い～被害防止のために～

- 警告画面に表示される電話番号には連絡しない！
- JFマリンネットバンクのID、パスワード等を伝えない！
- 「おかしい」と感じたらパソコンの操作を中止すること！
- 不正送金被害に遭った場合は最寄りの店舗へご相談を！
（被害に遭われたと思ったら…緊急停止を実施してください。）

