インターネットバンキングを安全にご利用いただくためのご注意

いつも当行のインターネットバンキングサービスをご利用いただきまして、まことにありがとうございます。

インターネットバンキングの安全性向上のために以下の点にご注意いただきますようよろしくお願いいたします。

１．利用者ＩＤ、ログインパスワードおよび取引実行パスワード（以下「パスワード等」）の取扱いについて

（１）パスワード等の設定についてのご注意

① 他人から推測されやすい番号のご使用は避けてください。

【推測されやすい番号】　生年月日、自宅の住所・地番、電話番号、勤務先の電話番号、自動車のナンバー、同一数字、連番の番号等など

② インターネットバンキング以外のサイトと共通のパスワードを使用しないでください。

③ 第三者が指定したパスワード等を使用しないでください。

（２）パスワード等の管理

① パスワード等は定期的に変更してください。

万一パスワード等が盗取された場合でも、不正操作時にパスワード等が変更されていれば被害を防ぐことができます。

② パスワード等をパソコン内での保存やメモをしてパソコンに貼りつけるなど、第三者の目にふれる方法で保管しないでください。

③ 第三者に知らせないでください。

当行行員が電子メールや電話等でＩＤ・パスワード等をお伺いすることはありません。

また、その他の金融機関職員や銀行協会職員が電子メールや電話等でお伺いすることもありませんので、不審な照会を受けた場合には回答は避け当行へお問合わせください。

④ パスワード等を不用意に入力しないでください。

パスワード等は、「操作マニュアル」でご案内している画面でのみ入力してください。

通常とは異なるパスワード等の入力を促す画面が表示された場合は、入力せず当行へお問合せください。

２．ウィルス対策を行ってください。

（１）当行が提供するインターネットバンキング専用ウィルス対策ソフト「Rapport（ラポート）」をご利用ください。

（２）利用するパソコンのソフトウェア（基本ソフト（ＯＳ）、ブラウザ、その他のソフトウェア）は常に最新の状態で利用し、サポートが終了したソフトウェアは使用しないでください。

（例：WindowsXP など）

（３）利用するパソコンにはセキュリティ対策ソフトを導入のうえ、最新のパターンファイルでご利用されていることをご確認ください。**※「Rapport（ラポート）」と併用してお使いください。**

（４）心あたりのないメールに記載されているＵＲＬのクリックや、添付ファイルの開封は絶対に行わないでください。

（５）利用するパソコンや無線ＬＡＮなどのルーター等については、サービスを利用しないときは可能な限り電源を切断してください。

３．万一の不正利用を早期発見する対策を実施してください。

（１）トップページに前回ログイン日時を表示しています。ログインの都度、不審なログイン履歴がないかご確認ください。

（２）預金残高や取引履歴は定期的に確認してください。

（３）資金移動取引等重要なお取引を受付けた際には、あらかじめご登録をいただいているお客様の電子メールアドレスに通知をいたしますのでご確認願います。また、電子メールアドレスを変更された場合は速やかに登録を変更してください。

また、フリーメールアドレス（無料でメールアカウントを取得できるアドレス）は、第三者に悪用されてしまう可能性がありますので、フリーメールアドレスを登録することはお控えください。

４．サービス管理責任者の方は以下の点にもご注意ください

（１）インターネットバンキングを利用するパソコンは利用目的を制限してください。
不審なウェブサイトや電子メールの送受信には利用しないようご注意ください。

（２）利用者ＩＤおよび利用するパソコンを厳重に管理し、担当者の異動等によるサービス利用者の変更や使用するパソコンを変更した場合は、不要になった利用者ＩＤの削除や電子証明書の削除を行ってください。

（３）利用者ごとにサービスの利用権限を設定することができます。社内の体制に応じて適切な権限設定を行ってください。
また、資金移動取引においては、申請者と承認者は別のパソコンを使用する等の措置を講じてください。

（４）資金移動取引につきまして、１日または１件あたりの利用限度額をご指定いただけますので必要最小限の金額を設定してください。

以　上

不審なメール・サイトを発見した場合や身に覚えのないお取引がある場合には、
至急下記までご連絡ください。
もみじ銀行　ＦＢセンター　０１２０－４１４－６８３
受付時間　　平日　９：００～１７：３０（ただし、銀行休業日は除きます）