平成 26 年 6 月 2 日

トマト銀行

インターネットバンキングの不正利用による不正送金被害にご注意ください！

現在全国的に、インターネットバンキングにおける不正アクセス被害が多発しており、法人のインターネットバンキングも標的となっております。

ご利用のパソコンがウィルスなどに感染することにより、被害に遭う恐れがありますので十分にご注意ください。

インターネットバンキングの不正利用を防止するため、以下の点をご注意ください。

1. 不審な E メールや添付ファイルを不用意に開いたり、不審なサイト等へのアクセスや、フリーソフトのインストールによりウィルスに感染しないようご注意ください。OS、ブラウザ、セキュリティ対策ソフト等インストールされている各種ソフトウェアは、常に最新の状態に更新してご使用ください。
2. ご利用のパソコンへのウイルス等の感染を防ぐため、セキュリティ対策ソフトを導入いただき、常に最新の状態に更新し、定期的にウイルスチェックと駆除を行ってください。
3. 当社がご提供・推奨しているセキュリティを積極的にご利用ください。

個人のセキュリティ（ワンタイムパスワードなど）
（http://www.tomatobank.co.jp/banking/s_info/security.html）

法人のセキュリティ（電子証明書など）
（http://www.tomatobank.co.jp/bizdirect/login/security.html）

4. 第三者に悪用される可能性があるため、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）を登録することは避けてください。
5. お取引きの安全のため、メール通知パスワードや取引通知等の重要なお知らせが届くメールアドレスは、携帯電話会社の提供するメールアドレスを登録いただくことを強くお勧めします。
6. インターネットバンキングを利用するパソコンは、過去の入力履歴から、次の入力内容をあらかじめ表示するキーボード入力補助（オートコンプリート）機能を解除してご使用ください。
7. 不特定多数の方が使用するインターネットカフェ等でのパソコンのご使用は避けてください。
8. 当社からＥメールや電話等で会員番号やパスワード等をお聞きすることや入力を依頼することはございません。不審な点がございましたら当行までご連絡ください。
9. パスワード等は決して第三者に知らせないでください。また、第三者が指定するパスワード等は使用しないでください。
10. 生年月日、自宅や勤務先の住所・地番・電話番号、同一数字や連番等の推測されやすいパスワードの使用を避け、定期的に変更してください。
11. キャッシュカード等他のサービスや携帯電話等当行以外の取引で使用しているパスワードの使用は避けてください。
12. パスワードをメモに残しておくことや、パソコン内に保存することは避けてください。
13. 不正利用早期発見のため、定期的に、過去のログイン日時、取引履歴、預金残高をご確認ください。身に覚えのない不審なお取引に気づかれた場合は、お客さまサポートセンター（0120-992-996）までご連絡ください。

不正利用により多額の被害に遭わないよう、振込等のご利用限度額は必要な範囲でできるだけ低く設定することをお勧めします。

以上