

法人

インターネットバンキング ご利用のお客さまへ

昨今、フィッシング詐欺やスパイウェア等により、インターネットバンキングの不正利用被害が多発しています。お客さまにおかれましても十分ご注意ください。

《主な不正利用の例》

- 利用者に金融機関等を装ったメールを送りつけ、偽サイトへ誘導したうえ、IDやパスワードを入力させて情報を盗む。(フィッシング詐欺)
- パソコンをウイルスに感染させ、パスワードなどを盗み出し不正送金する。(スパイウェアやウイルス)

被害に遭わないため、以下の対策をお願いします。

1. OSやブラウザは、推奨環境をご参照のうえ、最新の状態でご利用ください。
2. 当金庫推奨環境のパソコンをご利用ください。また、サポート期限が終了したソフトやWebブラウザ等 (Windows XPなど) は使わないでください。
3. ウィルス対策ソフトを導入し、最新版にアップデートしてください。
4. ログインパスワードを定期的に変更してください。
5. 利用者ワンタイムパスワードをご利用ください。(資金移動時に、従来の利用者確認暗証番号に加え、入力する暗証番号が都度変更となる利用者ワンタイムパスワードをご利用いただくと、更にセキュリティが高まります。)〈利用者ワンタイムパスワードについてのお問合せ〉: 芝信用金庫インターネットバンキングヘルプデスク 0120-48-8956【音声アナウンスで【1】を押してください。】平日9時~17時(※12月31日~1月3日休止)
6. ご利用限度額を必要な範囲内で、できるだけ低く設定してください。(「しんきん法人インターネットバンキングサービス申込書」に所定のご記入が必要ですのでお取引店へお申し付けください。)
7. 管理者と利用者が異なる場合は、パソコンをそれぞれ別にされることをお勧めします。
8. 「ID・パスワード方式」をご利用いただいているお客さまは、よりセキュリティの高い「電子証明書方式」への切り替えをお勧めします。(「しんきん法人インターネットバンキングサービス申込書」に所定のご記入が必要ですのでお取引店へお申し付けください。)
9. お客様カード、ご契約者ID(利用者番号)やログインパスワードは、パソコンに保存しないで厳重に管理してください。また、不審なログイン履歴や身に覚えのない取引履歴がないか定期的に確認してください。