



個人

# 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. 基本ソフト(OS)やWebブラウザ等を最新版に更新してください。
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. ソフトウェアトークンによる「ワンタイムパスワード」をご利用ください。(固定パスワードによる認証に加え、パスワード生成ソフトウェアにて、一定時間毎に生成された1回限りの使い捨て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。)
6. ご利用限度額を必要な範囲内で、可能な限り低く設定してください。
7. 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。

インターネットバンキング操作についてのお問合せ

インターネットバンキングヘルプデスク

[0120-959-211] 平日9時～22時(土・日・祝 12月31日～1月3日休止)



"最も相談しやすい地元のしんきん"を目指しています。

杜の都信用金庫

MORI NO MIYAKO  
SHINKIN BANK