

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に

最近、フィッシング詐欺やスパイウェア等により、お客様の暗証番号（パスワード）などを不正に取得し、お客様になりすまして、預金口座から不正に資金を引き出す被害が一部の金融機関で発生しております。

当金庫においては、このような不正取引による被害は発生しておりませんが、今後とも安全にインターネットバンキングサービスをご利用いただくため、以下の点にご注意いただきますようお願いいたします。

- **利用番号・お客様IDや暗証番号（パスワード）は厳重に管理してください。**
 - ・ 暗証番号（パスワード）は第三者に教えないでください。警察官や当金庫の職員であっても、お客様に暗証番号（パスワード）をおたずねすることはございません。
 - ・ 暗証番号（パスワード）は推測しづらいものを利用してください。
 - ・ 暗証番号（パスワード）は定期的に変更してください。
 - ・ 利用者番号・お客様IDや暗証番号（パスワード）をメモ等に残したり、パソコン内に電子ファイルで保存しますと、盗まれるおそれがありますのでご注意ください。

- **フィッシング詐欺にご注意ください。**
 - ・ 当金庫はメールにてお客様の暗証番号（パスワード）などの問合せはいたしません。身に覚えのないメールは開かないようご注意ください。
 - ・ 利用者番号・お客様IDや暗証番号（パスワード）を入力するページは、ウィンドウに鍵マークを表示しております。鍵のマークをダブルクリックし、証明書の発行先が以下のとおりになっていることをご確認ください。
個人インターネットバンキング：www.shinkinbanking.com
法人インターネットバンキング：www.shinkin-webfb-osaka.jp

- **スパイウェアやウィルスにご注意ください。**
 - ・ OSやブラウザは、適宜、最新版にアップデートしてください。
 - ・ セキュリティ対策ソフトのご利用を推奨します。
 - ・ 身に覚えのないメールは開かないでください。
 - ・ インターネットカフェなど、不特定多数の方が利用できるパソコンでの本サービスのご利用はお控えいただくことを推奨します。
 - ・ 不審なホームページを開いたり、フリーソフト等をインストールされる際はご注意ください。
 - ・ 身に覚えのないCD-ROMが送られてきた場合は、CD-ROMをパソコンで読み込まないようご注意ください。

- **不正利用を早期発見するために**
 - ・ Eメールアドレスの登録を推奨します。
 - ・ ログオン時には、ログオン履歴をご確認いただく他、定期的に残高照会、取引履歴照会、入出金明細照会を行い、不正利用・不正引き出しの有無をご確認ください。