平成２６年４月

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、全国的にインターネットバンキングを利用した犯罪が発生しております。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、以下の点にご注意願います。

１．当行および警察等からお客さまへインターネットバンキングのＩＤやパスワード、暗証番号等を問い合わせすることは、電話・電子メール・訪問等いかなる方法でもございません。そのような問い合わせがあった場合は絶対に教えず、直ちにお取引店へご連絡ください。
２．当行では、福島銀行メールマガジンサービス、インターネットバンキングご利用結果の通知およびお客さまから電子メールでお問い合わせいただいたご質問に対する回答以外に電子メールを送付することはございません。上記以外で当行を騙った電子メールが届いた場合は、直ちにお取引店へご連絡ください。
３．不審なメール（知らない先からのメール）の開封は絶対にしないでください。
心あたりのないメールに記載されているＵＲＬ（アドレス）をクリックしたり、添付されているファイルを開封することは絶対に行わないでください。また、そのような電子メールに記載されたＵＲＬ（アドレス）も絶対にクリックしないでください。

【利用環境等についてのお願い】

①セキュリティ対策ソフトをご利用ください
ご利用になるパソコンには、市販のウィルス対策ソフトを導入するなど、セキュリティを高めてお使いください。また、セキュリティ対策ソフトは常に最新の状態に更新してお使いください。

②ＯＳ・ブラウザは最新の状態でお使い下さい
ＯＳやブラウザは、最新の修正プログラムを適用してください。

③インターネットバンキングを使用するパソコンを制限してください。
インターネットカフェ等不特定多数の方が使用するパソコンでは、インターネットバンキングのご利用をしないようお願いします。

④ファイル交換ソフトを利用するパソコンでの使用を制限してください。
インターネットバンキングで利用するパソコンがウィルスに感染することや設定を誤ること等により、ファイル交換ソフト（Winny 等）を介してＩＤやパスワード等の重要な情報が流出する危険性があります。インターネットバンキングのご利用につきましては、ファイル交換ソフトをインストールしていないパソコンでご利用ください。

【IDやパスワード等の厳重な管理のお願い】

①パスワードの定期的な変更
ＩＤ、パスワードや暗証番号等は、生年月日等の類推しやすいものを避けるとともに、定期的に変更することをおすすめします。

②ソフトウェアキーボードを利用してください
ソフトウェアキーボードとは、パソコン本体のキーボードではなく、パソコンの画面上に表示されたキーボードをマウス等でクリックすることで暗証番号等の入力を行う機能です。キーボードの操作履歴がパソコン本体に残らず、パソコン本体のキーボードの操作履歴を盗み取り、インターネットを介して第三者へ送信するタイプのスパイウェアに効果があります。

③ＩＤ・パスワードの管理

ハードディスクにＩＤ・パスワードを保存している場合、ウィルスなどへの感染により保存したデータが外部へ漏れる可能性がありますので、ハードディスクへの保存はお控えください。

【不正利用の被害防止について】

①ログイン管理

インターネットバンキングの利用画面では、直前のご利用３回分のログイン日時が表示されますので、身に覚えのないものがないか必ずご確認ください。

②残高管理

口座の取引明細や残高情報はこまめにご確認いただくようお願いいたします。

③アドレスバーの確認

アドレスバーにあるフィッシュウォールやＥＶＳＳＬ証明書を確認することにより、閲覧しているサイトが当行の正当なサイトがどうか簡単に判別できます。

フィッシュウォールとは、Web サイトのブラウザのアドレスバーに緑色の信号表示がされることにより、真正なサイトであることが一目で確認できる、フィッシング詐欺対策のソフト

です。**ご使用されるパソコンにお客さまご自身で当行のホームページから無料でダウンロードしていただくことによりご利用いただけます。**

ＥＶＳＳＬ証明書とは、画面上部のアドレスバーが緑色で表示されるとともに、ウェブサイトを運営する組織名とＳＳＬサーバー証明書を発行した認証局名が表示されることにより、真正なサイトであることが一目で確認することができる機能です。

④取引通知のためのメールアドレス登録

お振込や暗証番号の変更等のお取引につきましては、お取引内容をお届けの電子メールへ通知いたします。電子メールのアドレスが誤っている場合やご登録がない場合、お届けのアドレスを変更された場合は電子メールが届きませんので、**必ず受信可能な電子メールアドレスをご登録ください**。ご利用の身に覚えがないにも関わらず電子メールが届いた場合は、直ちにお取引店へご連絡ください。

【万が一に備えご検討下さい】

①「電子証明書」と「可変式パスワード」の併用

平成 26 年 7 月より「可変式パスワード」を導入予定です。

②都度振込の当日扱いサービスの停止

当日扱いの振込・振替を停止することにより、不正利用があった場合に前日に利用結果の通知メールが到着しますので被害が事前に防止できます。

③振込・振替の利用限度額の引下げ

振込・振替の利用限度額を事前に引下げることにより、万が一被害に合われた場合の被害額を抑えることができます。（注.書面で届出いただいた限度額の範囲内での引下げは、お取引画面上で変更可能です。）

《本件に関するお問い合わせ先》
福島銀行　法人インターネットバンキングサポートセンター
0120-55-2940
（平日　９：００～１８：００）