平成２８年７月１４日

ほうわ法人向け／ほうわ個人向け
インターネットバンキングサービスをご利用のお客さまへ

株式会社　豊 和 銀 行

インターネットバンキングサービスの不正利用にご注意ください。

最近、フィッシング詐欺やウィルス感染によって、お客さまの ID・パスワード等が悪意ある第三者に盗み取られ、不正アクセスされる事例が全国で多く発生しており、警察庁によると平成 27 年中のインターネットバンキングに係る不正送金被害額は約 30 億 7,300 万円と、被害金額ベースで過去最悪となりました。

また、当行が定めている被害補償制度におきましては、一定の補償限度額がございますとともに、お客さまのセキュリティの状況に応じて補償減額あるいは補償できない場合がございますので、お客さまには当行が提供しておりますセキュリティ対策をご導入いただくことに加え、以下の点に十分ご注意いただくようお願い申し上げます。

記

１．心あたりのない電子メールを不用意に開封したり、不審なサイトにアクセスしないでください。

業務連絡や金融機関などを装い、偽りの情報を記載した電子メールを送りつけ、添付ファイルを開くことによりウィルスに感染したり、電子メールに貼られている URL をクリックすることにより、本物と酷似した WEB サイト（フィッシングサイト）へ誘導し、ID・パスワードを盗取される事件が発生しています。（改ざんされた WEB サイトを閲覧するだけで、ウィルスに感染してしまう例も確認されています。）

２．当行が提供・推奨するセキュリティ対策をご利用ください。

当行が提供するセキュリティ対策は以下をご確認ください。

◆ 法人向けインターネットバンキングのセキュリティ対策は**こちら**
◆ 個人向けインターネットバンキングのセキュリティ対策は**こちら**

３．ウィルス対策ソフトを導入してください。（当行はご提供しておりません。）

ご利用のパソコンへのウィルス等の感染を防ぐため、ウィルス対策ソフトを導入してください。また、ご利用にあたってはウィルス対策ソフトを常に最新の定義ファイルに更新し、定期的にウィルスチェックを実施してください。

４．OS・ブラウザ等パソコンにインストールされている各種ソフトウェアを常に最新の状態に更新して使用してください。

パソコンを動かすための基本ソフトであるＯＳ（オペレーティングシステム）やインターネット閲覧ソフトであるＩＥ等ブラウザ、インターネット上の動画の再生に必要な Adobe Flash Player、PDF ファイルを閲覧するために必要な Adobe Reader および各種ソフトウェアの動作に必要な Java などのソフトウェアについて、脆弱性に対処するための修正プログラム（セキュリティパッチ）を適用してください。

５．ID やパスワード等のアカウント情報を、ご利用のパソコン、スマートフォンおよびクラウドサービス等には絶対に保存しないでください。

ご利用のパソコンがウィルスに感染すると、クラウド上に保存しているアカウント情報が不正取得されるおそれがあります。

６．ファイル交換・共有ソフトのご利用にご注意ください。

インターネットバンキングを利用するパソコンでは、ファイル交換ソフト（Winny、Share、LimeWire、Win MX など）を利用しないでください。

７．フィッシング詐欺に遭わないために、当行インターネットバンキングのログイン画面が真正かどうか慎重に確認してください。

インターネットバンキングをご利用の際はログイン画面 URL を確認してください。なお、パソコンでご利用の場合は、当行が無償で提供する「PhishWall プレミアム」により真正なログイン画面かどうかをご確認いただけます。

◆セキュリティ対策「PhishWall プレミアム」は**こちら**

◆当行インターネットバンキングＵＲＬ◆
（個人）https://www.parasol.anser.ne.jp/ib/index.do?PT=BS&CCT0080=0590
（法人）https://www.bizsol.anser.ne.jp/0590c/rblgi01/I1RBLGI01-S01.do

ただし、真正な URL でログインした場合でも通常と異なる操作手順を求められたり、少しでも不審な点を感じられた際には、直ちに操作を中止し、末尾のお問合せ先までご連絡ください。

８．フリーメールアドレスを登録するのは避けてください。

フリーメールアドレス（無料でアカウントを取得できるアドレス）は、第三者に悪用される可能性があります。

９．振込結果確認の送信先にはお取引に利用するパソコンとは別の機器を指定してください。

メール通知パスワードや振込結果確認を受信するメールアドレスには、携帯電話会社の提供するメール（キャリアメール）アドレスなど、お取引に利用するパソコンとは異なる機器のメールアドレスを登録されることを強くお勧めします。

１０．キーボード入力補助（オートコンプリート）機能は解除して使用してください。

インターネットバンキングに利用するパソコンでは、入力しようとする内容を過去の入力履歴から予測表示する入力補助（オートコンプリート）機能を解除してご使用ください。

１１．不特定多数が利用するパソコンでインターネットバンキングのご使用は避けてください。

インターネットカフェやホテルなど不特定多数が利用する共用のパソコンでのインターネットバンキングのご使用は避けてください。

１２．公衆 Wi-Fi を利用してインターネットバンキングのご使用は避けてください。

公衆 Wi-Fi スポットでは暗号化が施されていない、または暗号化強度が弱い可能性があります。

１３．電子メールや電話等で ID・パスワード等を回答しないでください。

当行行員や、銀行協会職員が電子メールや電話等で ID・パスワード等をお尋ねすることは絶対にありません。

１４．ID やパスワード等は決して第三者に知らせないでください。

ID・パスワード等は慎重に管理し、お客さま以外の第三者には決して教えないでください。

１５．パスワードは定期的に変更するとともに、第三者から推測されやすいものに設定しないでください。

パスワードには他人から推測されやすい、生年月日、自宅住所・地番、電話番号、勤務先の電話番号、自動車のナンバー等の番号のご使用は避けてください。また、推測されやすい番号はすみやかに変更してください。

１６．パスワードを他のサービスの暗証番号として使用することは避けてください。

インターネットバンキングのパスワードに、その他の各種サービスの暗証番号と同じものを用いないでください。

１７．定期的に預金残高や取引履歴を確認してください。

不正な取引を早期に発見するため、定期的に預金残高や取引履歴を確認してください。

１８．振込限度額は必要な範囲で可能な限り低く設定してください。

不正送金の被害を極力抑えるため、振込や電子マネー購入等のための即時振込の取引限度額は、必要な範囲でできる限り低く設定してください。

＜ 本件に関するお問い合わせ先 ＞

◆ 豊和銀行インターネットバンキング係　０１２０－０８０－８４８
◆ 受付時間　銀行営業日の午前９時から午後５時まで

以　　上