インターネットバンキングご利用のお客さまへ　金融犯罪被害に遭わないために

１．被害に遭わないために（事前の対策）

インターネットバンキング（東和銀行ダイレクトサービス）のご利用に際しては、必ずウイルス対策などを行ってください。

（１）パソコン等を使用しないときは電源を切ってください。

インターネットバンキングで使用するパソコンや無線ＬＡＮ等を長時間使用しないときは、電源を切る、ネットワークを遮断する等により外部からの不正操作を防止してください。

（２）ウイルス対策ソフトを導入してください。

不正被害を防ぐにはウイルスの感染を防ぐことが不可欠です。ウイルス対策ソフトを導入し、最新の状態で利用してください。

・ 定期的にウイルスチェックを行い、不正なソフトウェアを発見した場合は、直ちに削除してください。

※ *当行では、無料のパソコンセキュリティサービス「SaAT Netizen」を提供しております。*

（３）ＯＳ、ブラウザやお使いのソフト（アプリ）は最新の状態となるよう更新してください。

・ サポートが終了したＯＳ等（例：Windows XP）は使用しないでください。

（４）ウェブサイトの閲覧、電子メールの受信、ソフト（アプリ）の導入には十分にご注意してください。

・ スパイウェア等の侵入を防ぐためにも、フリーソフト等を安易にダウンロードしないでください。

・ ファイル交換ソフトを使用しないでください。

・ 心当たりの無い発信元からのメール、添付ファイルを開かないでください。

※ 送信元に実在する企業、金融機関等を装った事例も発生していますので、ご注意ください。

・ 不審なＷｅｂサイト、当行ホームページを装った偽サイトにアクセスしないでください。

（５）お使いの「パスワード」は定期的に変更してください。

パスワードは、他人から推測されにくい内容を設定のうえ、厳重に管理してください。

・ 名前、電話番号、生年月日、自動車ナンバー、同一数字等の連想される内容はお止めください。

・ パスワードをパソコン、スマートフォンやクラウドサービスのファイル、画像（写真）やメール等に保存しないでください。

・ パスワードは、他人に絶対に教えないでください。また、パスワードの入力を求めるメールを受信しても無視してください。

※ 当行行員であっても、お客さまにパスワードをお尋ねすることはありません。

（６）「ソフトウェアキーボード」のご利用をお勧めします。

ソフトウェアキーボードによるログインパスワード入力機能をご利用いただけます。パソコンの画面上に表示されたキーボードをマウスでクリックするソフトウェアキーボードを利用することで、キー操作の不正読み取りの抑止効果がありますので、ぜひご活用ください。

（７）個人のお客さまは「ワンタイムパスワード（ソフトウェアトークン方式）」、法人のお客さまは「電子証明書」による本人認証方式を利用してください。

※ 法人のお客さまは「ワンタイムパスワード（ハードウェアトークン方式)」による本人認証を全てのお客さまにご利用いただいております。

※ 意図せず「ワンタイムパスワード（ソフトウェアトークン方式)」、「電子証明書」が消失した場合には、ウイルス感染の可能性があります。「ワンタイムパスワード」、「電子証明書」の再発行を依頼する前にウイルス対策ソフトにより、端末がウイルスに感染していないことを必ずご確認ください。

（8）インターネットカフェ等の不特定多数の方が利用するパソコンや公衆Ｗｉ－Ｆｉを使用してインターネットバンキングを利用しないでください。

（9）メールアドレスに不審なメールアドレスが登録されていないかご確認ください。

(10) ログイン時に通常と異なる偽画面やポップアップ画面が表示された場合、「パスワード」等を入力しないでください。

・ 当行のインターネットバンキングでは、ログイン時に「パスワード」等のお取引に必要な情報を入力いただくことはありません。

※ これらの画面は、正常な画面に見えるよう巧妙に偽装されておりますのでご注意ください。

２．被害を抑えこむために（不正取引の早期発見）

（1）**ご利用状況を定期的に確認してください。**

口座残高や入出金状況、インターネットバンキングのアクセス状況には、常に注意してください。

なお、ご自分の口座に身に覚えのない取引がある、メニューのご利用履歴に表示される「ログイン日時」に覚えが無い等、異常を感じた場合は直ちにお取引店にご連絡ください。

（2）**メールアドレスを登録してください。**

お使いのメールアドレスをご登録いただきますようお願いいたします。

お振込み等の都度、受付結果をお知らせしますので、携帯電話アドレス等、日頃ご利用されており、メールの到着が直ちに判るものを登録いただくと、万が一、不正取引があっても早期の発見につながります。

※ 本サービスのご利用にフリーメールアドレス（無料でメールアカウントを取得できるアドレス）のご登録は避けてください。

（3）**振込のご利用限度額の引き下げをご検討ください。**

振込・振替限度額は「適切な金額」としてください。

お振込み等の一日当たりの限度額（振込・振替限度額）は、お客さまの操作で引き下げができる仕組みとなっております。安全のためにも、ご利用目的に合わせて「適切な金額」への見直しをお願いします。

３．被害に遭われた場合

万一、お取引などで被害に遭われた場合は、至急警察へ被害届をご提出になり、同時に当行のお取引店へご連絡ください。

以上