インターネットバンキングご利用のお客様へ

＜重要なお知らせ＞

複数の金融機関のインターネットバンキング取引において、「ログインＩＤ・口座番号・暗証番号」等の重要情報をスパイウェア（※）等により盗み取られたため、第三者により身に覚えの無い取引（不正取引）が行われる被害が発生しています。

※　スパイウェアとは
本人に気付かれず、インターネット経由でパソコンの情報を外部から盗み出すソフトです。
電子メール等の形でパソコンに侵入し、パスワード等の個人情報を第三者に転送してしまうプログラムです。
無料で入手できる画像等のフリーソフトをダウンロードする際にインストールされる場合があります。
なお、ウィルスのような感染力、自己増殖力は無く、基本的に他人に迷惑をかけるものではありません。

当行では、インターネットバンキングのご利用にあたり、以下のセキュリティ強化の仕組みを用意しておりますので、是非ご活用ください。

＜セキュリティ強化の仕組み＞

・　「ソフトウェアキーボード」
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。
ログインＩＤ、ログインパスワード入力時に「ソフトウェアキーボードを開く」をクリックしますと、通常のキーボードとは別にソフトウェアキーボードが画面表示されます。
このキーボードをマウスでクリックし、ログインパスワードを入力することができます。

・　「ｎＰｒｏｔｅｃｔＮｅｔｉｚｅｎ」
スパイウェア、フィッシング等への対策ツールです。
「ｎＰｒｏｔｅｃｔＮｅｔｉｚｅｎ」のアイコンをクリックし、内容をご確認、ご了承いただいた後、インストールのうえご利用できます。
ｎＰｒｏｔｅｃｔＮｅｔｉｚｅｎについてはこちらをご確認下さい
↓
(http://www.towabank.co.jp/whatsnew/20060922nprotect.pdf)

また、被害にあわないため、以下の事項にご注意ください。

＜ご注意ください＞

・　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。
・　心当たりの無い発信元からのメールを不用意に開かないでください。
・　不審なＷｅｂサイトにアクセスしないでください。
・　ＯＳやブラウザには、適宜、最新の修正プログラムを適用してください。
・　スパイウェア対応のアンチウィルスソフトをご利用いただき、定義ファイルを最新状態に保ってください。
・　ＩＤ、パスワード等を記録したファイルをパソコン内に保存しないでください。
・　ファイル交換ソフトを使用しないでください。
・　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で利用しないでください。
・　ログイン画面に表示される、ご利用履歴に不審なものがないか確認してください。
・　パスワードは定期的に変更することをお勧めいたします。

万一、不審な取引をご確認された場合

・　東和銀行ダイレクトサービスセンターにご連絡いただくとともに、最寄の警察にもご相談いただきますようお願いいたします。

―――お問い合わせは―――

東和銀行ダイレクトサービスセンター

0120 ０１２０－４６９－１０８

受付時間/平日 9:00～17:00（ただし、銀行休業日を除く）

E-mail　direct@towabank.co.jp

以　上