

平成18年8月

お客さま各位

## スパイウェアにご注意ください

平素は「山梨中銀ダイレクト」をご利用いただき、誠にありがとうございます。

他の金融機関において、「スパイウェア」と呼ばれるソフトによりパソコンからIDやパスワードを不正に取得し、お客さまの預金口座から身に覚えのない振込が行われるという事件が発生しております。

当行のお客さまの口座に対しましては、不正操作や被害等の報告はされておませんが、「山梨中銀ダイレクト」をご利用のお客さまにおかれましては、被害に遭われないよう以下の点にご注意くださいますようお願い申し上げます。

### 1. スパイウェアとは

スパイウェアは、パソコンに入力したパスワード等の情報を、お客さまが気づかないうちに、インターネット経由で他に送信してしまうソフトです。

### 2. 被害に遭わないために

- (1) 不特定多数の方が使用するパソコンで「山梨中銀ダイレクト」をご利用なされないようご注意ください。
- (2) ログインパスワードの入力には、「ソフトウェアキーボード」のご利用をお勧めしております。
- (3) お心当たりのない電子メールの開封やフリーソフトのダウンロード等にはご注意ください。
- (4) 電子メールの案内による不審なサイトへのアクセスは、なされないようご注意ください。
  - \* 当行の電子メールでは、サイト等へのリンクは行っておりません。
  - \* 当行の電子メールでは、ID・パスワードの入力を求めることありません。
- (5) お心当たりのないCD-ROM等を不用意にパソコンに装着なされないようご注意ください。

\* 当行では、ソフトウェアをCD-ROMで送付することは行っておりません。

- (6) OS、ブラウザは、最新の修正プログラムを適用のうえご利用してください。
- (7) スパイウェア対応のウイルス対策ソフト等のご利用をお勧めします。
- (8) ファイル交換ソフトのご利用にはご注意ください。
- (9) 無線LANによる「山梨中銀ダイレクト」のご利用にはご注意ください。
- (10) パスワードについては次の点にご注意ください

- ・他人にパスワードを知らせないこと。
- ・電話番号等の類推されやすいパスワードを使用しないこと。
- ・パスワードを他のパスワードと共用しないこと。
- ・パスワードをパソコン内に保存しないこと。

\* 当行では、IDやパスワードをお客さまにお伺いすることはありません。

- ( 1 1 ) ログイン後は、ログイン履歴をご確認ください。  
「山梨中銀ダイレクト」のメニュー画面には、「ご利用履歴」として、お客さまが過去にログインされた日時が表示されます。  
お心当たりのない履歴がありましたら、下記当行ダイレクトマーケティングセンターまでお問い合わせください。
- ( 1 2 ) お振込の受付につきましては、お客さまあてに電子メールを送信しております。お心当たりのないお取引通知を受信されましたら、下記当行ダイレクトマーケティングセンターまでお問い合わせください。

以上

< 本件に関するお問い合わせ先 >

**山梨中銀ダイレクトマーケティングセンター**

フリーダイヤル：0120-201862（照会コード：2）

（受付時間）月曜日～金曜日 9：00～17：00（銀行休業日は除きます。）