ご留意事項

■パソコン・スマートフォン等の管理について

・サービスのご利用は、契約者自身が管理するパソコンやスマートフォン等から行ってください。不特定多数の方が利用する機器からのご利用は、お止めください。パスワード等が盗用され、被害に遭う恐れがあります。

・サービスの利用中に、パソコンやスマートフォン等の前から離れる場合は、必ず「ログアウト」を行ってください。

・パソコン等の操作時
ブラウザの「戻る」「進む」「×」は使用しないでください。
入力項目の移動は「マウスの左クリック」または「Tab」キーで行い、「Enter」キーは使用しないでください。
ダブルクリックは行わないでください。ログインボタンをダブルクリックすると二重ログインエラーになりますので、ご注意ください。このような場合、５分程お待ちのうえ再度ログインしてください。

・スマートフォン等の操作時
スマートフォン等の「電源OFF」や「クリア」、「戻る」等の機能は使用しないでください。
途中で処理が中断することがありますので、その際は再ログインしてください。なお、二重ログインとなる場合もありますので、その際には５分程度お待ちのうえ再度ログインしてください。

■フィッシング詐欺（パスワード等の詐取）にご注意ください！

・フィッシング詐欺とは、銀行等の企業を装って電子メールを送りつけ、実在する企業の偽ホームページに誘導しＩＤやパスワード等を入力させるなどして、不正に個人情報を盗み取る行為をいいます。

・当行が、インターネットバンキングサービスのＩＤやパスワード、キャッシュカードの暗証番号、クレジットカード番号等について、電子メールで入力を求めたり、電話でお伺いしたりすることはありません。
送信元として当行の名称（ドメイン名）（@yamanashibank.co.jp）や類似した名称が使われている電子メールを受信され、その内容がＩＤ、パスワード、暗証番号、クレジット番号等の入力を求めるものであった場合は、決して入力されないようご注意ください。

・フィッシング詐欺の一般的な手口は以下のとおりです。

（１）実在の金融機関やクレジットカード会社、ショッピングサイトなどを装った電子メールを送付する。

（２）電子メールにリンクを貼り付けて、その金融機関やショッピングサイトにそっくりな「罠のサイト」に呼び込む。（添付ファイルで入力を促すものもあります。）

（３）電子メールを受取った方が、詐称された企業の何らかの会員（金融機関の場合は、インターネットバンキング、キャッシュカード、クレジットカードなど）であった場合、ID・パスワード、暗証番号やクレジットカード番号等の個人情報を入力してしまうケースがあり、これにより個人情報が詐取される。

（４）詐取した個人情報により、インターネットバンキング、キャッシュカードやクレジットカードの不正使用が行われる。

■振り込め詐欺（特殊詐欺）にご注意ください！

電話を利用して、親族・警察官・弁護士等を装い、交通事故の示談金等の名目で現金を預金口座等に振り込ませ、だまし取る事件が多発しております。
高額の現金を「振り込め」という要求に対しては、電話の相手が本人であることを必ず確認するなど落ち着いて行動し、安易な振込を行わないようにしてください。
なお、不審と思われる場合には、最寄の警察署にご相談ください。

■スパイウェアにご注意ください！

他の金融機関において、「スパイウェア」と呼ばれるソフト等によりお客さまのパソコンからパスワード等が不正に取得され、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。

下記事項にご留意のうえ「山梨中銀ダイレクト」をご利用くださいますようお願い申しあげます。

（１）スパイウェアとは

スパイウェアは、パソコンに保存されている個人情報や入力したキーワード等を、お客さまが気づかないうちに収集し、インターネット経由で送信してしまうソフトです。

（２）お心当たりのない電子メールや不審なフリーソフトにご注意ください

スパイウェアは、電子メールやフリーソフトをダウンロードした時に、気づかないままパソコンにインストールされてしまいます。

お心当たりのないメールを安易に開いたり、不審なサイトへのアクセスや不審なソフトのダウンロードを行わないよう、十分ご注意ください。

（３）ウイルス対策ソフト等をご利用ください

スパイウェア対応のウイルス対策ソフト等をご利用いただき、アップデート（更新）のうえご確認および駆除していただきますよう、お願い申しあげます。

※スパイウェアの詳細や対策方法は、専門のサイト等でご確認ください。また、OS、ブラウザ等も更新プログラムを適用のうえご利用してください。

（４）ログイン後は、メニュー画面に表示されるログイン履歴をご参照ください

山梨中銀ダイレクトのメニュー画面には、「ログイン履歴」として、お客さまがログインされた日時が表示されます。

お心当たりのないご利用履歴がありましたら、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。

（５）お取引結果メールを常に閲覧可能な状態にしておいてください

山梨中銀ダイレクトによるお取引結果は、ご登録いただいたEメールアドレスに都度お送りしております。

お心当たりのないお取引通知を受信されましたら、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。

（６）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」をご利用なさらないようご注意してください

不特定多数の方が利用するパソコンには、スパイウェアがインストールされている可能性がありますので、「山梨中銀ダイレクト」のご利用は避けてください。

（７）ファイル交換ソフトの利用には、十分ご注意ください

（８）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。
・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。
・パスワードは定期的に変更されることをおすすめします。
・警察や当行がパスワードをお客さまに照会することはありません。