平 成 ２ ６ 年 ６ 月

お 客 さ ま 各 位

青 木 信 用 金 庫

インターネットバンキングの不正利用にご注意ください

最近、お客さまのパソコンをウイルス感染させ、インターネットバンキングのＩＤや暗証番号（パスワード）などを不正に取得するとともに、お客さまに気づかれずにパソコンに侵入し、お客さまの口座から不正に預金を引き出す被害が全国の金融機関で発生しております。

お客さまにおかれましては、サービスを利用するパソコンへのウイルス感染を防止するための自衛手段を講じて頂くとともに、パソコンの利用に際しては不審な点がないかご留意いただきますようお願い申し上げます。

●　ＩＤや暗証番号（パスワード）は厳重に管理してください。

ＩＤや暗証番号（パスワード）は、本人確認するうえで非常に重要な情報です。次の点に注意して、管理していただきますようお願いいたします。

・暗証番号（パスワード）は、第三者に絶対に教えないでください。警察官や当金庫の職員であっても、お客さまに暗証番号（パスワード）をおたずねすることはございません。

・暗証番号（パスワード）は、推測しづらいものにしてください。
また、契約先（利用者）暗証番号および契約先（利用者）確認暗証番号が数字４桁のままの場合は、早急に半角英数字を組み合わせたものに変更してください。

・契約先（利用者）暗証番号および契約先（利用者）確認暗証番号は、定期的に変更（月１回程度）してください。

・ＩＤや暗証番号（パスワード）をメモ等に残したり、パソコン内に電子ファイルで保存すると、盗まれるおそれがありますのでご注意ください。

・パソコンを破棄する際は、専用ソフト等を使用してパソコン内のデータを完全に消去することをおすすめします。

・他のサイト等で使用している暗証番号（パスワード）は使用しないことをおすすめします。

・暗証番号（パスワード）の入力時には、キーボードからの直接入力は避けて、ソフトウェアキーボードをご利用ください。

● **ワンタイムパスワードをご利用ください。**

資金移動時にこれまでの利用者確認暗証番号に加えて、暗証番号がその都度変更となる利用者ワンタイムパスワードをご利用ください。
ご利用方法については下記のページをご参照ください。
（http://www.shinkin.co.jp/info/hib/oshirase/20140417_1/otp.pdf）

● **前回インターネットバンキングにログインした時間を確認してください。**

お心当たりのないログイン日時が表示されている場合は、至急お取引店までお問い合わせください。

● **パソコンのＯＳやブラウザ等を最新版にアップデートしてください。**

インターネットへの接続にあたっては、ＯＳ・ブラウザ等、お客さまが利用している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アップデート（更新）してください。

● **ウイルス対策ソフトを導入してください。**

ご利用中のパソコンへのウイルス等の感染を防ぐため、ウイルス対策ソフトを導入し、ご利用にあたっては、ウイルス対策ソフトを常に最新の状態に更新して、定期的にウイルスチェックと駆除を行ってください。

● **不審な電子メールは開かずに速やかに削除してください。**

ウイルス感染を防ぐため、心当たりのない電子メールや添付ファイルは絶対に開かないでください。
また、心当たりのない電子メールに記載されたＵＲＬは絶対に開かないで下さい。

● **振込限度額を必要最小限に設定してください。**

インターネットバンキングでは、１回および１日当たりの振込限度額を変更することができますので、ログイン後のメニューからお客さまの振込限度額をご確認いただき、ご利用に差し支えない範囲で変更してください。

● **パソコンをインターネットに接続したまま長期間放置しないでください。**

パソコンをインターネットに接続したまま長期間放置すると攻撃者による不正送金のリスクにさらす事になりますので、不必要時にはインターネットを遮断し、パソコン未使用時は電源をお切りください。

● 電子証明書をご利用ください。

「ＩＤ・パスワード方式」をご利用の場合は、不正取引の被害防止の有効な手段として、よりセキュリティの高い「電子証明書方式」のご利用をおすすめいたします。
電子証明書とは、電子的に作られた身分証明書のことで、ご利用されているパソコンに取得（インストール）していただくことで、電子証明書を取得していないパソコンからの操作ができなくなります。
万が一、暗証番号等が盗まれた場合でも不正に利用されることはきわめて困難となっております。
また、当金庫では、電子証明書が不正に犯罪者に詐取されないよう電子証明書のエクスポート機能（バックアップ機能）は無効としております。
なお、「ＩＤ・パスワード方式」から「電子証明書方式」への変更のお手続きは、お取引店までお申出ください。

● お受取人さまの事前登録をお願いいたします。

これまで発生したインターネットバンキング不正送金事件の手口の大半は、当日付で受取人を指定する都度指定振込であることから、当日付（即日扱い）でお振込みをされる場合は、可能な限り事前にお受取人さまのご登録をお願いいたします。

● 金融機関を騙る偽メールにご注意ください。

インターネットバンキングのパスワード等を盗み取ろうとする不審な電子メール等が、不特定多数の方に送信されております。
警察官や当金庫では、電子メール等でインターネットバンキングのパスワード等をお尋ねすることはございませんので、そのような照会には絶対にお答えにならないでください。
また、金融機関を不正に騙り、「入金のお知らせ」「セキュリティのお知らせ」等と称して、金融機関とはまったく関係のないサイトに誘導する電子メール等が不特定多数の方に発信されております。
このような電子メール等に記載されているリンク先をクリックしたり、添付ファイル等を開いたりすると、インターネットバンキングのパスワード等を盗み出すサイトに誘導されたり、パソコンがウイルス感染するおそれがありますので、不審なメールを受信した場合は、メールを開く、リンク先をクリックする、添付ファイルを開く等は絶対に行わないでください。

● 「管理者」と「利用者」はそれぞれ異なるパソコンをご利用ください。

データ伝送取引を行う際には、「管理者」と「利用者」がそれぞれ異なるパソコンを使用することで、セキュリティを高めることができます。

● **不正にポップアップ画面を表示させて、インターネットバンキングの情報を盗み取ろうとする犯罪にご注意ください。**

インターネットバンキングにログインした後に、情報を盗み取ろうと不正に暗証番号（パスワード）などお客さまの情報を入力させようとするポップアップ画面が表示されるという事例が国内の銀行で発生しておりますので、ご注意ください。

● **その他、注意事項につきましては、下記のページをご参照ください。**

インターネットバンキングを安全にご利用いただくために
（http://www.shinkin.co.jp/info/security_01/index.html）

【お問い合わせ先】

ご不明な点や不審な取引等がございましたら、速やかにお取引店までご連絡願います。

○　青木信用金庫　お取引店

受付時間：平　　日　９：００～１７：００

インターネットバンキングの操作に関するお問い合わせは下記までご連絡願います。

○　しんきんインターネットバンキングヘルプデスク

０１２０－７０－５８８０（フリーコール）
受付時間：平　　日　９：００～２２：００
　　土日祝日　９：００～１７：００
　　※１２月３１日～１月３日休み

以　上