

平成 26 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 I D 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頂きますようお願い申し上げます。

● I D や暗証番号（パスワード）は厳重に管理してください。

I D 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、ログインパスワードが数字のみの場合は、セキュリティを高めるために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。
- ・ログインパスワードは、定期的に変更（月 1 回程度）してください。
- ・I D 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 evitando、ソフトウェアキーボードをご利用ください。

● 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。

● **ワンタイムパスワード（ソフトウェアトークン）を利用して下さい。**

パスワードの盗難・詐取等による犯罪被害防止に有効な対策として、ワンタイムパスワード（ソフトウェアトークン）がご利用いただけます。

ワンタイムパスワード（ソフトウェアトークン）は、ログイン時に30秒毎に更新されるパスワードを入力することから、セキュリティがより強化されます。

書面による手続きはご不要で、手数料は無料でご利用いただけます。

ご利用はこちら http://www.shinkin.co.jp/aoshin/07_ib/data/20140612_02.pdf（PDF形式：330kb）から「ワンタイムパスワード（ソフトウェアトークン）ご利用までの流れ」をご覧ください。

● **不特定多数の人が操作できるパソコンでインターネットバンキングを利用しないでください。**

図書館やインターネットカフェ等、不特定多数の利用者が操作できるパソコンでは、ウイルス感染等によりIDやパスワードが漏洩する危険性がありますので、ご利用はお控えください。

● **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。

● **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。

● **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