インターネットバンキングをお申込みのお客様へ

～ご預金を守るための大切な確認とお願い～

1．ご導入にあたって

□ OSやソフトウェアは最新の状態ですか？

脆弱性が残された状態でコンピューターを利用していると、不正アクセスに利用されたり、ウイルスに感染したりする危険性があります。

脆弱性を塞ぐには、OS やソフトウェアのアップデートが必要となります。たとえば、Windows の場合には、サービスパックやWindows Update によって、それまでに発見された脆弱性を塞ぐことができます。ただし、一度脆弱性を塞いでも、また新たな脆弱性が発見される可能性があるため、常に OS やソフトウェアの更新情報を収集して、できる限り迅速にアップデートを行ってください。

□ ウイルス対策ソフトは導入していますか？

ウイルス対策ソフトは、一般的にコンピューターの電源がオンであるときには常に起動した状態になり、外部から受け取ったり送ったりするデータを常時監視することで、インターネットや LAN、記憶媒体などからコンピューターがウイルスに感染することを防ぎます。

ただし、ウイルス対策ソフトは、これまでに発見されたウイルスに対応するウイルス検知用データからウイルスを見つけ出す仕組みになっているため、新しいウイルスは検知できないことがあります。そのため、ウイルス検知用データはいつでも最新のものに更新しておかなければなりません。

2．安全にご利用いただくために

【WEBバンキングをご利用のお客様】

□ **ワンタイムパスワードの利用登録が必要となります。**

当金庫のシステムとお客さまがダウンロードしたソフトウェアトークン（パスワード生成アプリケーション）または専用端末のハードウェアトークンが 30 秒毎に同じタイミングでお客さま固有のパスワードを更新し、この間だけ有効な双方のパスワードを照合することにより、ログイン時および資金移動等の取引時の認証を行います。一度認証に成功したパスワードは、その時点で利用できなくなりますので、万がースパイウェア等によって入力したパスワードを盗まれてしまった場合でも、悪用されるリスクが極小化されます。

なお、携帯電話単独での WEB バンキングのご利用はできません。

※ハードウェアトークンにつきましては、故障を除く再発行時には再発行手数料 1,000 円（税別）がかかります。

【WEB-FBをご利用のお客様】

□ **電子証明書の取得が必要となります。**

電子証明書によるログインでは、電子証明書をインストールしたコンピューターからのみパスワードを入力してログインでき、電子証明書がインストールされていないコンピューターからはログインできなくなります。そのため、万が一フィッシングやスパイウェアにより ID やパスワードが漏洩したとしてもログインできないため、成りすましによる不正利用を防ぐことができセキュリティが格段に向上します。

□ **ワンタイムパスワードの利用登録が必要となります。**

当金庫のシステムとお客さまがダウンロードしたソフトウェアトークン（パスワード生成アプリケーション）または専用端末のハードウェアトークンが 30 秒毎に同じタイミングでお客さま固有のパスワードを更新し、この間だけ有効な双方のパスワードを照合することにより、承認・登録等の取引時の認証を行います。一度認証に成功したパスワードは、その時点で利用できなくなりますので、万が一スパイウェア等によって入力したパスワードを盗まれてしまった場合でも、悪用されるリスクが極小化されます。

※ハードウェアトークンにつきましては、紛失・破損による再発行時には再発行手数料 1,000 円（税別）がかかります。

3. より安全にご利用いただくために

□ Rapport（ラポート）をご利用ください（無料でご利用いただけます）。

Rapport（ラポート）は、インターネットバンキング専用ウイルス対策ソフトで、

(1) インターネットバンキングを狙ったウイルスを検知・駆除します。

(2) インターネットバンキングで使用する通信情報の改ざんを防ぎます。

(3) インストールするだけで、自動的に機能します。また、他のウイルス対策ソフトとの併用ができます。

ただし、ウイルス対策ソフトにより、インストールや利用する際に特別な操作が必要な場合もあります。

※「Rapport」は、IBM 社が提供する無料セキュリティソフトで、当金庫のホームページよりダウンロードできます。

4. 当金庫の補償制度について

□ 万が一被害が発生した場合、個人のお客さまについては「預金者保護法」に準じた対応を行う方針が業界より示されており、金融機関側に過失がない場合でも、お客さまご自身の責任によらない被害は、基本的に金融機関が補償を行うこととなっております。

しかしながら、法人のお客さまの被害補償については、法整備がなされていないことから各金融機関に対応が委ねられている状況です。

当庫においては法人のお客さまに対する補償制度の整備が必要と考え、平成 27 年 4 月 1 日から「インターネットバンキング不正利用被害補償制度」を新設しております。

５．ご導入後の管理

□　ログインパスワードの管理について

パスワードは、他人に推測されにくく、ツールなどで割り出しにくいものを使ってください。

（1） 名前などの個人情報からは推測できないこと。

（2） 英単語などをそのまま使用していないこと。

（3） 類推しやすい並び方やその安易な組み合わせにしないこと。

（4） 同一のパスワードを長期間使い続けることは避け、こまめにパスワードを変更すること。

（5）Word 文書やメモ帳、メールソフト内のメール等で ID、パスワードを記載したファイルをパソコン内に保存しないこと。

（6）Web メールやクラウドサービス等に ID、パスワードを記載したファイルを保存しないこと。

□　前回のログイン日時をご確認ください。

身に覚えのないログイン日時が表示された場合は、すぐに帯広信用金庫事務部システム担当（0155-67-5084）までご連絡ください。

□　取引限度額は必要最小限に設定してください。

通常ご利用されるお取引金額の範囲内で取引限度額を設定してください。

□　帯広信用金庫のホームページを「お気に入り」「ブックマーク」に登録してください。

当金庫のホームページを「お気に入り」「ブックマーク」に登録し、ご利用の際はそこからアクセスしてください。

当金庫のホームページアドレスは以下の通りです。

http://www.shinkin.co.jp/obishin/index.html

□　不審なホームページにはアクセスしないでください。また、身に覚えのないメールは開かないでください。

ウイルスは悪性のホームページなどで配布されていたり、メールに添付されていたりなど、さまざまな経路でコンピューターに侵入してきます。悪性ホームページに接続する可能性のある迷惑メールや掲示板内などのリンクに注意する、不審なメールの添付ファイルを開かないなどの対策が必要です。

□ インターネットバンキングご利用時にいつもと違う画面が表示されたら、いったん入力を中止し、すぐに帯広信用金庫事務部システム担当（0155-67-5084）までご連絡ください。

インターネットバンキングにログインする際に、お客様のコンピューターに感染したウィルスが不正な入力画面を表示し、お客様の情報を入力させようとする事象を確認しております。

【WEBバンキングをご利用のお客様】

ログインする際に「資金移動用パスワード」を入力いただくことはありません。また、いずれの場合でも「資金移動用パスワード」のうち、3桁以上の数字を入力いただくことはありませんので、絶対に入力しないでください。

【WEB-FBをご利用のお客様】

ログイン直後等に「各種パスワード」を入力いただくことはありませんので、絶対に入力しないでください。

「あなたのコンピューターをシステムが認識できませんでした。」というメッセージ等で始まる不正な画面で各種パスワードの入力を要求された場合、絶対に各種パスワードを入力しないでください。

（平成 29 年 9 月 25 日現在）