

【 重要なお知らせ 】

平成 27 年 12 月 29 日

お客様 各位

釧路信用組合

インターネットバンキング不正送金被害にご注意ください

拝啓 時下ますますご清栄のこととお喜び申し上げます。

平素は、弊組合インターネットバンキングサービスをご利用いただき、誠にありがとうございます。

さて最近、全国の金融機関にて新種のウィルスによる攻撃が多発し、不正取引（パソコンをウィルス感染させ、ログイン I D やパスワードなどを詐取した不正送金）による大口の被害が発生しています。警視庁からは利便性を重視するあまり、インターネットバンキングの安全性を脅かすことがないよう万全の体制が求められております。

お客様におかれましては、被害に遭われませんようセキュリティ強化対策として、次葉のセキュリティ対策を実施およびご検討いただきますようお願いいたします。

また、不正送金防止のため、弊組合では基本的には、当日扱い振込は避けることを推奨致しますが、ワンタイムパスワード導入のお客様につきましては、お客様よりのご希望により当日扱い振込に対応致します。なお、ワンタイムパスワード未導入のお客様につきましては、当日扱い振込を禁止させていただきますのでご了承、ご協力くださいますようお願い申し上げます。

敬具

インターネットバンキングのセキュリティ強化対策としまして、次の対応のご検討をお願いします。

1. パソコンの基本ソフト（OS）やブラウザにつきましては、NTTデータAnserBizSOLが認めたバージョン内（※1）にて最新状態に更新してください。

※1：確認先 <http://www.dokodemobank.ne.jp/co/anserbizsol/environment/index.asp>

2. パソコンにセキュリティ対策ソフトを導入するとともに、最新の状態に更新してください。

なお、当組合では不正送金対策ソフト「PhisWall（フィッシュウォール）プレミアム」を無料提供しておりますので導入を検討願います。

他行のインターネットバンキングを利用しているなど、同じソフトを既に導入済みのお客様につきましては、改めて導入する必要はございません。

くわしくは、弊組合ホームページ上のインターネットバンキング内、「不正送金対策ソフトPhisWall（フィッシュウォール）プレミアム」をご参照ください。

3. 取引の申請者と承認者とで異なるパソコンを利用することを推奨します。
4. ログインパスワード、承認パスワードは類推されやすい文字を避け、定期的に変更するようお願いします。

パスワードの変更方法は、インターネットバンキングご利用ガイドの利用者管理から利用者情報の変更を参照してください。

5. ご利用限度額は必要な範囲内で設定願います。

変更は、別途「釧路しんくみ法人向けインターネットバンキングサービス利用申込書」に必要項目、変更内容をご記入のうえ、提出願います。

6. 不審なログイン履歴がないか確認を行うよう願います。

弊組合のインターネットバンキングトップページにて、過去3回のログイン履歴が表示されますので不審なログインが無いことをご確認ください。（インターネットバンキングご利用ガイドP28を参照してください。）

7. メール受信による取引の確認を行ってください。

お取引の受付確認、処理結果等のご通知を電子メールで案内しますので、メールは利用有無に関係なく定期的にご確認いただきますようお願いします。

8. 電子証明方式のご利用を推奨しますのでご検討願います。

弊組合の電子証明方式は、認証局より発行される電子証明書をお客様のパソコンに格納し、次回以降サービスにログインする際には、電子証明書が格納してあるパソコンからでしかログインを出来なくする仕組みで、不正送金防止には一定の効果があると言われています。

無料提供しておりますのでご活用のご検討をお願いします。お申し込みは電話にて受付しております。

ただし、複数ユーザがおられるお客様は全てのユーザが電子証明を取得する必要があり、1年ごとに証明書の更新が必要となります。

また、一人のユーザが複数のパソコンからログインすることができなくなります。

なお、警察庁の情報によりますと、新型ウィルスに感染した場合、電子証明書が機能しなくなる事例があるようですのでご注意ください。

9. ワンタイムパスワード（ソフトウェアトークン）のご利用を推奨しますのでご検討願います。

弊組合のワンタイムパスワードはソフトウェアトークン方式によるもののため、スマートフォンもしくは携帯電話等の別媒体が必要となりますので、お客様におかれましては、対応運用に関しましては、十分検討いただきますようお願い申し上げます。

くわしくは、当組合ホームページ上のインターネットバンキング内「ワンタイムパスワード 導入のお知らせ」をご参照ください。

10. ウィルスに感染する恐れがありますので不審なメールを開いたり、不審な入力画面を使用しないようご注意ください。

以上