# インターネットバンキングをご利用のお客様のセキュリティ対策について

最近、マスコミで報道されていますように、インターネットバンキングにおいて、不正送金被害が増加しています。ご利用のお客様におかれましては、不正送金被害に遭わないために、以下のセキュリティ対策を実施していただきますようお願いいたします。

なお、お心当たりのないお振込み等がありましたら、速やかにお取引店までにご連絡ください。

**１．インターネットバンキングをご利用のお客様は、以下の対策を実施していただきますようお願いいたします。**

（１） ウイルスの感染防止・・・パスワード等を漏えいさせないでください。

不審なサイト、メールは開かず、パソコンには必ずセキュリティソフトを導入して、ウイルス定義ファイル等を最新版へアップデートしてください。

また、パソコンがウイルスに感染していないことを定期的に確認してください。

（２） パスワードの定期的な変更・・・漏えいしたパスワードを無効化

類推され易いパスワードは使用せず、パスワードも定期的に変更してください。

また、インターネットカフェ等のパソコンで、インターネットバンキングを利用しないでください。

⇒パスワードの変更についてはこちら

⇒ログイン ID の変更についてはこちら

**２．特に法人・事業者のお客様におかれましては、上記１の対策を実施していただくとともに、以下の対策を実施していただくようお願いいたします。**

（１） インターネットバンキング専用のセキュリテイ対策ソフトの導入など、当組合が提供しているセキュリティ対策を実施してください。


⇒フィッシング対策ソフト『フィッシュウォールプレミアム』についてはこちら

（２） 不正アクセスの検知・・・不正送金を未然に察知してください。

インターネットバンキングの利用の有無に関わらず、随時、残高照会、利用履歴を確認して不審な取引が無いかを確認してください。

※取引通知メールの宛先を携帯電話等に設定し、退社後の不正アクセスについても検知できるようしてください。

⇒取引通知メールの受信先変更設定についてはこちら

※不正アクセス（ログイン）がないかを確認してください。


⇒最新 3 回のログイン履歴が表示されますので、不正なアクセスがないかを確認してください。

（３）振込上限金額は必要最低限を設定してください。

⇒上限金額の変更については、お取引店にご相談ください。

（４）メール通知パスワード・ワンタイムパスワード等の可変式パスワードを追加で利用してください。

また、メール通知パスワード・ワンタイムパスワードをされる場合、メール送信先のアドレスを携帯電話等のＰＣとは別媒体に設定してください。

⇒メール通知パスワード・ワンタイムパスワードについてはこちら

（５） ＰＣを利用していない時は、ＰＣの電源をオフにしてください。

平成２７年８月

富山県信用組合