

## 5) セキュリティについて

**Q.** インターネットバンキングのセキュリティはどうなっていますか？

**A.** 当組合のセキュリティに対する取り組みについては、下記の通りになっています。

- i. 128 ビット SSL 暗号化通信方式を採用。
  - インターネット上で情報が暗号化され、お客さまの大切な情報が盗まれたり、書き換えられたりされないよう情報の保護が行われます。
- ii. EV SSL 証明書。
  - 当組合のインターネットバンキングのページを表示した際に、アドレスバー（画面上部 http://～と表示されている部分）が緑色に変わることによって正式なページであることが確認できます。これにより不正利用を目的とした利用者が作成した偽のログインページを判別することが出来ます。
- iii. 厳重な本人確認。
  - お客さま以外の第三者による不正利用を防ぐため、お客さまを特定するログイン ID、パスワード、確認パスワードで本人確認を行っております。
- iv. ご確認メール送信による取引確認。
  - お客さまのお取引確認のメールを、ご登録いただいたメールアドレスへ送信します。取引にお心当たりがない場合は、まずパスワードを変更していただき、当組合お取引店の窓口か渉外担当にご連絡ください。
- v. 前回のログイン時間表示による利用確認。
  - ログイン後の画面へ、お客さまがご利用になられた最新 3 回のログイン日時を表示しています。ご利用履歴にお心当たりがない場合は、まずパスワードを変更していただき、当組合お取引店の窓口か渉外担当にご連絡ください。
- vi. 自動ログアウト。
  - ログインしたまま一定時間操作が行われない場合、自動的にログアウトされる仕組みになっています。ご利用の途中で離席される場合は、必ずログアウトを行ってください。
- vii. ソフトウェアキーボード。
  - インターネットバンキングの画面上のボタンをマウスでクリックして文字を入力するソフトウェアキーボードをお使い頂くことにより、不正なプログラムによるパスワードの不正取得を防止することが出来ます。

- viii. 電子証明書（もしくは「クライアント証明書」）。
- 電子的に作られたお客さまを識別するための身分証明書のようなもので、セキュリティ対策の一つです。インターネットバンキング利用時に利用する端末に発行（保存）した「電子証明書」を提示することにより、他のパソコンによる操作を排除することができるので、セキュリティが保持され、お客様の重要な取引情報等を保守するために重要なものになります
- ix. ワンタイムパスワード。
- ログイン時の認証に使う一度だけ有効な使い捨てパスワードのことを言います。取得するには、お客さまのスマートフォンまたは携帯電話のワンタイムパスワードアプリに表示されるパスワードにて取得します、表示後 1 分間隔で更新します。そのため、一度利用したパスワードは、使用することが出来ませんので、インターネット上でパスワードを盗まれても利用される事は無く、非常に高いセキュリティを保つことができます。
- x. 無料のセキュリティ対策ソフト「PhishWall プレミアム」の提供。
- このセキュリティ対策ソフトをお客さまのブラウザに導入することにより、フィッシング等による不正送金の防止策となります。当組合 HP のトップページに表示されております。

以上