

【重要】ご注意ください！

インターネットバンキングの不正送金が多発しています！

最近、複数の金融機関において、インターネットバンキングの不正送金被害が多発しております。インターネットバンキングのパスワードやIDの管理には充分にご注意ください。

早急に以下のような被害防止対策を実施いただき安全にご利用くださいますようお願い申し上げます。

【被害防止対策】

1. ワンタイムパスワードのご利用

ワンタイムパスワードは、資金移動等の重要な取引を実行する際に入力する、1分毎に変化するその時限りのパスワードです。(ワンタイムパスワードは、無料をご利用いただけます。)

ワンタイムパスワードをご利用されていないお客さまは、早急に当組合に利用の申込みをご依頼ください。

2. クライアント証明書のご利用（ビジネスネットバンキングご利用者のみ）

法人・個人事業主のお客さまは、クライアント証明書(無料)を特定のパソコンに導入していただくことにより、そのパソコン以外からのインターネットバンキングの利用はできなくなります。

クライアント証明書をご利用されていないお客さまは、早急に当組合に利用の申込みをご依頼ください。

3. フィッシング対策ソフトのご利用

当組合では、フィッシング対策としてホームページ上に無償でフィッシング対策ソフト「PhishWall」を提供していますので、ご使用のパソコンにインストールしてください。

4. パソコンやスマートフォン、セキュリティソフトのアップデートを行ってください！

アップデートを実施することで、セキュリティを含めた機能の改善が図られます。可能な限り最新バージョンをご利用ください。

5. 各種認証はパソコン・スマートフォン内に保存しないでください！

各種認証（ログインID、ログインパスワード、確認用パスワード）を、パソコンやスマートフォン等の「メモ帳」等に保存している場合、盗取されるリスクが高まります。電子機器に保存せず、ご自身で厳重に管理くださいますようお願いいたします。

6. 各種認証は定期的な更新を行ってください！

特にログインパスワードや確認用パスワードについては定期的（毎月）更新し、同じパスワードを使いまわすことのないようご注意ください。

7. 不審なメールやメッセージは開封しないでください！

コンピュータウィルスに感染しないために、身に覚えのない不審なメールやメッセージを発見した場合は、開封したり添付ファイルを開いたりしないでください。

8. 取引履歴等を定期的にご確認ください！

不審なログイン履歴や、身に覚えのない取引履歴・予約取引、取引通知がないか定期的(朝・昼・晩など)に確認してください。

※上記対策は合わせて実施することで効果が高まりますので、未実施の対策がありましたら、実施いただくようお願いいたします。