

不正アクセスによる被害が多発しています。

！ 至急、セキュリティ対策を実施してください ！

拝啓 時下ますますご清栄のこととお慶び申し上げます。

平素は格別のご高配を賜り、厚く御礼申し上げます。

さて、現在、お客さまのパソコンをウィルス感染させてインターネットバンキングの ID や暗証番号等を不正に取得するとともに、お客さまが気づかれぬうちにお口座から不正に預金を引き出す被害が全国の金融機関で発生しております。

お客さまにおかれましては、不正な引き出しを確認された際には早急に当金庫へご連絡いただくとともに、このようなウィルス感染や不正な引き出しの被害発生等を防ぎ、サービスをより安全にご利用いただくため、下記の点にご注意いただきますようお願い申し上げます。

敬具

記

1. 「ID/パスワード方式」から「電子証明書方式」にお切替え願います。

不正送金被害に遭われる方の多くが、「ID/パスワード方式」をご利用になられています。

お客さまの大切な資産を守るためにも、ぜひとも「電子証明書方式」にお切替え願います。

(1) 「電子証明書方式」とは

利用者 1 人につき 1 枚発行される電子式の証明書をパソコンにインストールすることで、インターネットバンキングを利用するパソコンを 1 台に限定する方式です。「電子証明書方式」を利用いただくことで第三者による“なりすまし”のリスクが軽減されますので、セキュリティ面での強化を図ることができます。

<ID/パスワード方式の場合>

 会社のパソコン  自宅のパソコン  ネットカフェのパソコン

IBを利用するパソコンを特定しないため、第三者にパスワード情報を盗まれる危険性があります。

<電子証明書方式の場合>

 会社のパソコン  自宅のパソコン  ネットカフェのパソコン

IBを利用できるパソコンを特定することで、リスク軽減につなげます。

(2) 切替方法について

「ビジネス Web 電子証明書発行（兼再発行）依頼書」にご記入・ご捺印のうえ、お申し込みください。

(3) 「電子証明書方式」にかかる料金について

「電子証明書方式」へのお切替えにかかる手数料は発生いたしません。また、「電子証明書方式」にお切替えいただいた以降の月間手数料も変更ございません。

(4) 「電子証明書方式」をご利用いただけるパソコンについて

次の URL より動作確認済環境をご確認願います。

<https://www.shinkin.co.jp/info/houjincl/kankyo.html>

2. ワンタイムパスワードを登録願います。

ワンタイムパスワードとは、30秒毎に都度生成される1度きりのパスワードのことです。インターネットバンキング「お客様カード」と一緒に送付いたします「ハードウェアトークン」をビジネス Web に登録いただくことでご利用いただけます。

なお、ワンタイムパスワードのご登録をもってビジネス Web でのお振込・お振替が可能となりますので、必ず登録いただきますようお願いいたします。

3. PhishWall (フィッシュウォール) プレミアム【無料】をご利用ください。

パソコンに MITB (マン・イン・ザ・ブラウザ) 攻撃対策機能を持つ不正送金対策ソフトを入れていただきますと、ビジネス Web を安心・安全にご利用いただけます。

インストール方法につきましては、次の URL よりご確認願います。

https://www.securebrain.co.jp/products/phishwall/install_other.html

4. セキュリティ対策ソフトをご利用ください。

セキュリティ対策ソフトは常に最新の状態に更新願います。併せて、定期的にセキュリティ対策ソフトによるウイルスチェックを実施願います。

5. OS やブラウザは、動作確認済環境にあるものをご利用ください。

次の URL より動作確認済環境をご確認願います。

<https://www.shinkin.co.jp/info/houjincl/kankyo.html>

6. ウィルス感染を防ぐため、身に覚えのないメールは開かないようにしてください。

また、不審なホームページにアクセスしないでください。

7. 前回のログイン時間をご確認願います。

身に覚えのないログイン時間である場合は、早急に当金庫へご連絡ください。

8. 取引限度額は必要最低限に設定願います。

その他の注意事項につきましては、以下のページをご参照願います。

インターネットバンキングを安全にご利用いただくために

https://www.shinkin.co.jp/info/security_01/index.html

以上