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やスマートフォ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．ワンタイムパスワードをご利用願います。
　ワンタイムパスワードとは、３０秒毎に都度生成される１度限りのパスワードのことです。スマートフォンにソフトウェアトークン（アプリ）をインストールし、パーソナル Web に登録いただくことでご利用いただけます。詳細は次の URL をご確認願います。
　https://www.shinkin.co.jp/hiratuka/personal/info/pdf/otp_howto.pdf

２．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、パーソナル Web を安心・安全にご利用いただけます。
　https://www.securebrain.co.jp/products/phishwall/install_other.html

３．利用者番号や暗証番号（パスワード）は厳重に管理願います。
　利用者番号や暗証番号（パスワード）はパソコンやスマートフォンに保存・記録せず、厳重に管理願います。また、暗証番号（パスワード）は定期的に変更することをおすすめします。

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ィ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/kojin/kankyo_02.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