インターネット・バンキングをご利用のお客さまのセキュリティ対策について

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。
ご利用者におかれましては、以下のセキュリティ対策を実施してください。
なお､インターネット･バンキングにログインした際に不審な入力画面等が表示された場合、ID・パスワード等の情報を入力せず、当金庫にご連絡ください。

１．インターネット・バンキングのご利用者は、以下の対策を実施してください。

インターネット・バンキングのご利用者に実施していただくセキュリティ対策	
①	インターネット・バンキングに使用するパソコン（以下、単に「パソコン」という。）に関し、基本ソフト（ＯＳ）やウェブブラウザ等、インストールされている各種ソフトウェアを最新の状態に更新する
②	パソコンにインストールされている各種ソフトウェアで､メーカーのサポート期限が経過した基本ソフトやウェブブラウザ等の使用を中止する WindowsＸＰによる使用は中止してください
③	パソコンにセキュリティ対策ソフトを導入するとともに､最新の状態に更新したうえで使用する 当金庫はインターネット･バンキング専用のウィルスに対応したセキュリティ対策ソフト「Rapport（ラポート)」を無償で提供しています
④	インターネット・バンキングに係るパスワードを定期的に変更する また、推測されやすいパスワードは使用しない ※同一の英数字や連番、生年月日、電話番号、自動車のナンバーなど
⑤	ログインパスワードは、ソフトウェアキーボードから入力する
⑥	お客様カードは厳重に保管する
⑦	入出金明細は定期的に確認する（不正利用の早期発見）
⑧	Ｅメールアドレスを登録し、取引の都度のメール受信で取引内容を確認する。
⑨	インターネットバンキングで使用する各種限度額は必要な範囲でできるだけ低く設定する
⑩	取引履歴の確認、前回ログイン日時の確認で身に覚えのない利用がないか注意する。

２．特に、法人向けインターネット・バンキングのご利用者におかれましては、上記１の対策を実施いただくとともに、以下の対策を実施してください。

法人向けインターネット・バンキングのご利用者に実施していただくセキュリティ対策	
①	電子証明書を利用する （現在、電子証明書利用先では不正送金被害は確認されていません）
②	当金庫が指定した正規の手順以外で電子証明書を利用しない
③	資金移動取引において、入力する暗証番号がその都度変更となる利用者ワンタイムパスワード機能を利用する
法人向けインターネット・バンキングのご利用者に推奨するセキュリティ対策	
①	パソコンの利用目的として、インターネット接続時の利用はインターネット・バンキングに限定する
②	パソコンや無線ＬＡＮのルータ等について、未利用時は可能な限り電源を切断する
③	取引の申請者と承認者とで異なるパソコンを利用する
④	振込・払戻し等の限度額を必要な範囲内でできるだけ低く設定する
⑤	不審なログイン履歴や身に覚えがない取引履歴、取引通知メールがないかをその都度確認する

本件に関するお問い合わせ先
甲府信用金庫　ＩＢ担当
電話番号　０５５－２３１－２８１１
受付時間　平日　午前９時～午後５時