長崎三菱信用組合

２０１８年2月26日

法人向けインターネットバンキングの不正送金にご注意ください

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おります。
お客さまにおかれましては＜りょうしん＞インターネットバンキングをより安全にご利用いただくため、以下のセキュリティ対策を行なっていただくようお願いします。

記

１．セキュリティ対策ソフトの最新化と定期的なチェック

パソコンには必ずセキュリティソフトを導入し、最新版へのアップデートをお願いします。
また、ウイルスに感染していないことを定期的に確認してください。

２．パスワード等の定期的な変更

パスワード等は、必ず定期的に更新を行なってください。また、漏えい防止のため、同一パスワードの他のサービスでの使い回しは行なわないようにご注意ください。

３．ＯＳやブラウザ等の最新化

ＯＳやブラウザ等、パソコンにインストールされている各種ソフトウェアには、適宜、最新の修正プログラムを適用してください。

４．振込限度額の確認

振込限度額は必要最低限に設定してください。

５．ソフトウェアキーボードのご利用

ＩＤ・パスワード等のウイルスによる漏えいを防止するため、入力欄への直接入力を避け、ソフトウェアキーボードを利用されることを推奨します。

６．不審なメールは絶対に開かない

ウイルスに感染する危険性があります。心あたりのないメールに記載されているＵＲＬのクリックや添付ファイルの開封などは行なわないでください。

７．推奨するセキュリティ対策（無料）

・「ＰｈｉｓｈＷａｌｌ（フィッシュウォール）プレミアム」の利用
お客さまのＰＣがＭＩＴＢ攻撃型ウイルスに感染していないかをチェックし、感染の徴候を発見した場合に、警告画面で情報の入力をブロックします。また、ウイルスを無効化する機能が搭載されています。
詳しくは「PhishWallプレミアムの説明」をご確認ください。

・「ワンタイムパスワード」の利用

最大有効期限が１分の可変パスワードです。携帯電話もしくはスマートフォンを利用してランダムに作成されたパスワードを通知します。表示されているパスワードを入力することでご本人さまの確認を行ないます。

ワンタイムパスワード詳しい説明はこちら

８．「クライアント証明書」による電子証明書ログイン方式を必須としております

ご利用者さまごとに発行した証明書により当サービスへの接続を特定し証明書がダウンロードされているパソコンからのみログインができます。許可されていないパソコンからの不正アクセスを防止する事ができます。

８．取引データ作成者と承認者の権限を分ける

取引データ作成者と承認者の権限を分けてご利用いただくことで、二重チェックが可能となります。（権限機能にて設定可能です。）

上記に関するご質問・お問い合わせや、万一不正アクセスによる被害を受けられた場合は、経営管理本部（℡095-861-4161）または最寄りのりょうしん各営業店までご連絡ください。

以上

まごころバンク りょうしん