【重要】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・モバイルバンキングおよび＜りょうしん＞ビジネスバンキングをより安全にご利用いただくため、次のセキュリティ対策を行っていただきますようお願いします。

○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。

○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わないようにご注意ください。

○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。

○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。

○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。

○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わないでください。

○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

お客様の 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、http://www.ryousin.shinkumi.jp/phishwall.htmlにてご確認下さい。

・「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います。

○<りょうしん>インターネット・モバイルバンキングについて

・「メール通知パスワード」の利用（ワンタイムパスワードとの併用不可）

ログインする都度､あらかじめ指定されたメールアドレスにランダムに作成した可変パスワードを記載したメールが送信され､そのパスワードを入力することでご本人さまの確認を行います。

○<りょうしん>ビジネスバンキングについて

取引データ作成者と承認者の権限を分けてご利用ください。(権限機能にて設定可能です。)また、電子証明書もご利用ください。

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