MITB 攻撃による不正送金犯罪にご注意ください

平素より、もおしんインターネットバンキングサービスをご利用いただき、誠にありがとうございます。
さて、昨年の 7 月以降、MITB （Man-in-the-Browser）攻撃による不正送金犯罪が増加しております。
そこで、安全にインターネットバンキングサービスをご利用いただくため、下記の内容にご注意いただき、ご対応くださいますようお願い申し上げます。

■ 最新のウイルス対策ソフトご利用のお願い

最近、メールで感染を広げるコンピュータウイルスが流行っております。ウイルス対策ソフトやOS・ブラウザを最新状態にし、定期的なスキャンの実施をお願いします。

また、例え知人からのメールであっても、身に覚えのないメールは開封せず破棄して下さい。誤って開封した場合は、添付ファイルは開封せず、記載されている URL もクリックしないで下さい。

添付ファイルを開封、または URL をクリックした場合、ウイルス感染した可能性があります。ウイルス感染すると、インターネットバンキングの操作を実施する際、偽画面が表示され、認証情報が窃取されている可能性があります。

当組合では、ワンタイムパスワード（以下、「OTP」）は振込取引等重要取引時にしか入力要求はありませんので、ログイン時など通常のタイミングと異なる箇所で OTP の入力が要された場合は、取引を継続せず当組合までご連絡下さい。

【MITB 攻撃による不正送金被害の例】

昨今、流行傾向にある MITB 攻撃による不正送金被害の一例は以下のとおりです。

① 知人、 取引企業から不審なメールが送付される。
メールの添付ファイル（Word ファイル等）を開いた際に Emotet（エモテット） と呼ばれるウイルスに感染する。

② Emotet の感染により、インターネット上から Zloader（ゼットローダー）と呼ばれる MITB を行うためのウイルスがダウンロードされる。
※ Zloader はダウンロードされただけでは動かないが、インターネットバンキングにアクセスすることで不正プログラムが実行される。

③ Zloader の不正プログラムにより、利用顧客（エンドユーザ）がインターネットバンキングにアクセスした際に偽画面が出力され、認証情報（アカウント、パスワード、ワンタイムパスワード等） をリアルタイムで詐取し、悪意のある第三者が正規画面よりインターネットバンキングへアクセスし、不正送金が実行される。
※ Emotet は、感染したパソコンのアドレス帳に登録されているメールアドレスに Emotet に感染させるためのファイルを添付してメールが送信されるため、感染したパソコンを踏み台として感染を広げていく。

■ PhishWall プレミアムのご利用のお願い

当組合は、インターネットバンキングサービスをより安心してご利用いただけるよう、不正送金、フィッシング対策ソフト「PhishWall プレミアム」をご提供しております。

PhishWall プレミアムはインターネットバンキングにアクセスするタイミングで通信が安全な状態かをチェックし、MITB 攻撃による偽画面が表示される等の問題を発見した場合、パソコンに警告メッセージを表示して不正な画面への入力を防ぐ機能を持っています。ソフトをお客様のパソコンへインストールすることにより有効となる機能であります。積極的なご利用をお願いいたします。

真岡信用組合