インターネットバンキングにおける MITB （Man-in-the-Browser）攻撃

に対する注意喚起について

記

１．最新状態のウイルス対策ソフトの利用

メールで感染を広げるコンピュータウィルスが流行っているため、ウイルス対策ソフトやＯＳ・ブラウザを最新状態にし、定期的なスキャンを実施願います。

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。

添付ファイルの開封、URL のクリックを実施した場合、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。

当信組では、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 入力が要された場合は、取引は継続せず当信組までご連絡下さい。

２．PhishWall プレミアムのインストールの徹底

PhishWall プレミアムはＩＢ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がございますので、必ずPhishWall プレミアムのインストールを実施してください。

※PhishWall プレミアムは当組合ホームページより無料でダウンロードできます。

【MITB 攻撃による不正送金被害の一例】

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。

②Emotet 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、ＩＢにアクセスすることで不正プログラムが実行される。

③Zloader の不正プログラムにより、利用顧客（エンドユーザ）がＩＢ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ＩＢへアクセスし、不正送金が実行される。

以上