平成 30 年 1 月

お客様各位

株式会社福島銀行

コンピューターウィルス「DreamBot」にご注意ください

近年、コンピューターウィルス「DreamBot（ドリームボット)」に感染したパソコン等によるインターネットバンキングの不正送金被害が全国的に広がっています。

１．感染被害例

（１）パソコン等に入力・保存したログインＩＤ、パスワード情報等が窃取される。

（２）インターネットバンキングにログインした際、暗証番号、ワンタイムパスワードを不正に求める偽画面が表示される

（３）パソコン等が乗っ取られ、悪意ある第三者によりお客様の預金口座から不正に送金される。

２．感染防止対策

（１）身に覚えのないメールの添付ファイルを開封しないでください。

（２）身に覚えのないメールに記載されているリンクＵＲＬをクリックしないでください。

３．　セキュリティ対策

（１）インターネットを利用するパソコン等には必ずウィルス対策ソフトを導入し、常に最新の状態にして利用してください。

（２）当行が推奨しているセキュリティ対策ソフト「Phish Wall プレミアム」と「SaATNetizen」の両方をご利用ください。当行ホームページより無料ダウンロードできます。

（３）お客様のパソコンがコンピューターウィルス DreamBot に感染していないかをご確認ください。「日本サイバー犯罪対策センター（JC3)」のホームページにて DreamBot・Gozi 感染チェックサイトが試験運用されていますのでご活用ください。

【日本サイバー犯罪対策センターのホームページ】

https://www.jc3.or.jp/info/dgcheck.html

以 上

＜本件に関するお問い合わせ先＞

インターネットバンキングサポートセンター

０１２０－５５－２９４０（平日：　９：００～１８：００）