仙台銀行

平成 29 年 3 月 29 日

お客さま　各位

仙台市青葉区一番町二丁目１番１号
株式会社　仙　台　銀　行

「DreamBot（ドリームボット）」ウイルス感染による被害にご注意ください

パソコンのウイルス感染によるインターネットバンキングの不正送金被害が、全国的に拡大しておりますが、今般、インターネットバンキングの不正送金対策として導入している「ワンタイムパスワード」を偽画面から入力させて、利用者の預金を自動的に別口座に送金する新型ウイルス「DreamBot(ドリームボット)」による被害が国内で確認されました。

身に覚えのないメールは、安易に開封したり、添付ファイルを開かないとともに、普段と違う画面にてワンタイムパスワードを要求された場合は、入力することのないよう、十分にご注意ください。

記

１．感染経路について

(1) ウイルス付きメール添付ファイルを開封する。

(2) メール本文中に記載されているリンクの URL をクリックする。

※お客さまのパソコンがこのウイルスに感染していないかを確認するためには、「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へ＞

https://www.jc3.or.jp/topics/dreambot.html 別ウィンドウが開きます。

２．セキュリティ対策について

(1) インターネットを利用するパソコンには必ずウイルス対策ソフトを導入し、常に最新の状態に更新して使用して下さい。さらに、パソコンがウイルスに感染していないか定期的にウイルスチェックを行ってください。

(2) セキュリティ対策ソフト「PhishWall プレミアム」を利用してください。
お客さまへ、MITB 攻撃※を検知・無効化する機能が搭載されている「PhishWall プレミアム」のご利用を強く推奨します。無料でご利用いただけますので、是非ダウンロードしてご利用ください。くわしくはこちらをご覧ください。

※MITB 攻撃とは、悪意のあるものがお客さまのパソコンにウイルスを侵入させ、不正な画面（ポップアップ画面）を表示し、ログイン ID やパスワード等のお客さま情報を盗み取る攻撃のことです。

以　上

【本件に関する問合せ先】
≪インターネットバンキングに関する事項≫
サポートセンター　　℡　0120-8661-39
（受付時間）　月～金曜日　9：00～17：00　（土・日・祝日を除く）

じもとホールディングス