

平成 29 年 3 月 31 日

ネットバンキングご契約者様

君津信用組合

不正送金に遭わないためのセキュリティ対策について

平素はきみしんインターネット・モバイルバンキング、法人インターネットバンキングをご利用頂きまして誠にありがとうございます。

この度、欧州の犯罪者グループのサーバに国内金融機関のインターネットバンキング利用者情報（ID、パスワード等）が保管されていたとの報道がございました。

本件は利用者の PC がキーロガー（※1）と呼ばれるタイプのウィルスに感染したことで、情報が盗取されたものと想定されております。

ネットバンキングご契約者様におかれましては、最新の状態に更新したウィルス対策ソフトによるチェック、およびパスワードの変更等のセキュリティ対策により不正送金の被害に遭わないようご注意ください。（※2）

ログインパスワード、確認用パスワード、ログイン ID の変更はインターネットバンキングの画面上で変更可能です。

本件の詳細につきましては、下記「一般社団法人 JPCERT コーディネーションセンター」のホームページをご覧ください。

<https://www.jpCERT.or.jp/press/2017/20170323-avalanche.html>

当組合では不正送金対策としてワンタイムパスワードとセキュリティ対策ソフト「[PhishWall（フィッシュウォール）プレミアム](#)」を導入しておりますのでご利用を推奨します。

※1 キーロガーとは

PC 利用者がキーボードから入力した情報をすべて記録し、ある程度まとまったところで外部のサーバに勝手に記録を送信する悪意のあるソフトウェア。

PC の画面では伏せ字で表示されたパスワード等も入力したまま記録されるので、ID やパスワードの盗取に悪用されるもの。

※2

その他のインターネットバンキングのセキュリティ対策は下記をご覧ください。

[インターネットバンキングを利用した不正出金にご注意ください](#)

お問い合わせ先

君津信用組合事務部

電話 0438-20-1122（平日 9 時～17 時）