

平成 28 年 6 月 17 日

インターネットバンキング  
法人インターネットバンキング ご利用者様

君津信用組合

## インターネットバンキングマルウェア「Gozi」による被害にご注意ください

日頃より、インターネットバンキングをご利用いただきありがとうございます。

今般、インターネットバンキングマルウェア「Gozi」の被害拡大の注意喚起が JC3（日本サイバー犯罪対策センター）から発表されました。

Gozi は、インターネットバンキング利用者が入力した情報を盗み取る不正プログラムです。Gozi に感染した端末でインターネットバンキングを利用すると、ID・パスワードなどの情報が盗み取られ、預金口座から不正送金が行われてしまうおそれがあります。

Gozi に感染してインターネットバンキングで不正送金の被害にあわないよう、以下を参考にセキュリティ対策を実施して頂きますようお願い致します。

### 記

#### ○ 適切な対策

- ・ウイルス対策ソフトを導入し、パターンファイルを常に最新の状態に更新する。
- ・基本ソフト（OS）や、ウェブブラウザなどの各ソフトウェアを常に最新の状態に更新する。
- ・インターネットバンキングにアクセスした際に不審な入力画面等が示された場合、ID・パスワード等を入力しない。※不審な画面が表示された際は当組合へご連絡ください。
- ・意図しないログイン履歴がないか、自分の口座の入出金明細等を定期的に確認する。

上記対策に加え、当組合では「ワンタイムパスワード」と不正送金対策ソフト「PhishWall プレミアム」を無料でご提供しておりますのでご利用を推奨します。

導入方法は下記をクリックしてご覧ください。

- ・ [ワンタイムパスワードご利用手順書（インターネットバンキング編）](#)
- ・ [ワンタイムパスワードご利用手順書（法人インターネットバンキング編）](#)
- ・ [「PhishWall プレミアム」導入方法](#)

#### ○ インターネットバンキングマルウェア「Gozi」について

##### 【機能】

- ・感染した端末を使用してインターネットバンキングを利用すると、ID・パスワードな

どの情報が窃取され、銀行から不正送金が行われるおそれがあります。

- 偽のクレジットカード入力画面を表示させる機能を持っているため、クレジットカード情報が窃取され、クレジットカードが不正使用されるおそれがあります。
- キー入力操作情報を収集して送信する機能を持っているため、感染した端末からは、金融機関関連情報だけでなく、その他の重要な情報が窃取されるおそれがあります。

#### 【感染経路】

- 請求書の送付などの業務連絡を装う不審なメールが、日本語で数多く送り付けられていることが確認されており、添付されているファイルを開封すると Gozi に感染するおそれがあります。
- 改ざんされたウェブサイトを開覧するだけで、Gozi に感染してしまう例も確認されています。

#### 【別名】

「Gozi」は、「Ursnif」、「Snifula」、「Papras」などの別名で呼ばれています。

○適切な対策

○インターネットバンキングマルウェア「Gozi」について  
日本サイバー犯罪対策センターホームページより  
(<https://www.jc3.or.jp/topics/gozi.html>)

お問い合わせ先

君津信用組合 事務部

TEL0438-20-1122（平日 9:00～17:00）

以上