平成２９年２月

お客さま　各位

兵庫県信用組合

改ざんサイトの閲覧による不正プログラムの感染にご注意ください

近時、「RIG-EK」と呼ばれる攻撃ツールが組み込まれたサイトに誘導するよう改ざんされたウェブサイトの急増が確認されています。

改ざんサイトを閲覧することで、気付かないうちに「Gozi」（※）等不正プログラムに感染し、犯罪被害に遭う恐れがあることから、以下を参考として適切な被害防止対策を実施してください。

＜被害防止対策＞

・ウイルス対策ソフトを導入し、新しい不正プログラムを検出するための定義ファイル（パターンファイル）を最新のものに更新する。

・RIG-EKなどの攻撃ツールによって脆弱性を悪用されないよう、Windows等の基本ソフト（OS）の自動更新機能等を利用し、常に最新の状態を維持する。
また、その他ウェブ閲覧と関連するウェブブラウザ等のソフトウェアについても、各セキュリティパッチを適用して最新の状態を維持する（脆弱性を解消する）。

（※）Goziの概要

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恐れがあります。 ・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恐れがあります。 ・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恐れがあります。
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感染する恐れがあります。 ・改ざんされたウェブサイトを閲覧するだけで感染する例も確認されています。
別名	・「Ursnif」、「Snifula」、「Papras」などの別名で呼ばれています。

＜参考＞

一般財団法人日本サイバー犯罪対策センター

・「RIG-EK改ざんサイト無害化の取組」
https://www.jc3.or.jp/topics/op_rigek.html

・「インターネットバンキングマルウェア『Gozi』による被害に注意」
https://www.jc3.or.jp/topics/gozi.html