Ksisnet
Kyoto Small and Medium Enterprises Information Security Support Network
京都中小企業情報セキュリティ支援ネットワーク

Ｋｓｉｓｎｅｔだより

発行：京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）事務局

平成２８年
６月２７日
Ｖｏｌ．１７

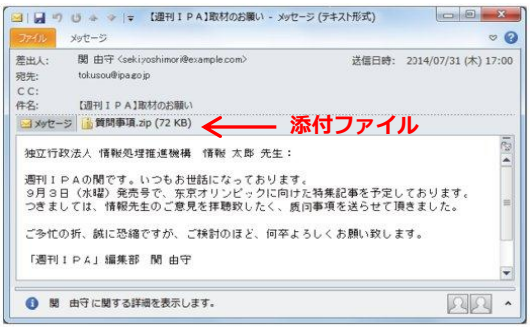
ネットバンキングを狙う不正プログラムの感染に注意!!

① ネットバンキングを狙った攻撃は、これまで正規のオンライン銀行を装う偽のサイトに誘導してIDやパスワードを盗み取る「フィッシング詐欺」が主流でしたが、最近は、「オンライン銀行詐欺ツール」を使用した攻撃が急増し、被害が相次いでいます。

② 「オンライン銀行詐欺ツール」は、正規のオンライン銀行へのアクセス時に、利用者のIDやパスワードの入力を求める偽の画面を表示させて情報を盗み取る不正プログラムです。

オンライン銀行詐欺ツールの感染ルートは主に２つ

【①標的型メール攻撃による感染】



・添付ファイルの開封
・本文中に記載のURLへのアクセス　等

【②改ざんされたウェブサイトの閲覧による感染】

・組み込まれた不正プログラムのダウンロード　等

オンライン銀行詐欺ツールの仕組み

【犯人側の動向】

○ 『オンライン銀行詐欺ツール』を利用者にメール送付するか、不特定のウェブサイトに『オンライン銀行詐欺ツール』を組み込んで利用者の感染を待つ

○ 感染した利用者がオンライン銀行の情報入力ページにアクセスすると『オンライン銀行詐欺ツール』が自動感知して利用者のパソコン画面に偽の情報入力フォームを表示させる

○ 感染した利用者が本物の情報入力フォームと思い込んで入力したID・パスワード情報を盗む

○ 盗んだ情報を利用してインターネットバンキングの不正送金を行う

【銀行情報窃取までの流れ】

上記画像は、トレンドマイクロ（株）から引用

～被害防止策①（オンライン銀行詐欺ツールの被害防止策）～

◎　ID・パスワード等を使い回さない!!
　ID・パスワード等を使い回すと全ての口座等が被害に遭う危険性があります。
　面倒でもサービス（銀行等）ごとに異なるID・パスワードを設定しましょう。

◎　通帳や利用明細のこまめなチェックを!!
　通帳や利用明細をこまめにチェックし、身に覚えのない取引がないか確認しましょう。
　不正な取引を発見した場合は、速やかにサービス管理者（銀行やクレジットカード会社）に連絡してください。

～被害防止策②（全てに共通する必須の被害防止策）～

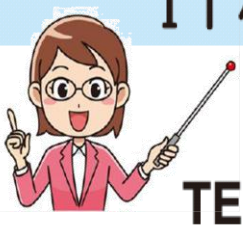
◎　送信者アドレス、添付されたファイル（拡張子が.zip・.exeなど）、添付されたURL、文面を確認し、不審なメールは開かないでください。
　最近では、犯罪者が取引を装って複数回メールをやりとりして信用させる手口が急増しています。従業員に対し繰り返し教養を行ってください。

◎　内容が改ざんされたウェブサイトは、URL等に変化がないため容易に発見できません!!
　不用意にファイルやソフトをダウンロードせず、ウイルスチェックを徹底してください。

◎　ウイルス対策ソフトやソフトウェアを最新の状態に更新してください!!
　不正なメールを自動で隔離したり、不正なウェブサイトへのアクセスをブロックする機能も充実してきています。
　更新されていなければ効果はありませんので、必ず更新してください。

お困りの時は!!

京都中小企業情報セキュリティ支援ネットワーク（Ksisnet）
ＩＴ相談窓口（公益財団法人京都産業21 お客様相談室）



相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の9：00～17：00（祝日を除く）

TEL 075-315-8660　メールアドレス okyaku@ki21.jp

公益財団法人京都産業21 お客様相談室（〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内）