F－CSNET NEWS

Fukuoka small and medium sized enterprises Cyber security Support NETwork

第８号

平成２９年８月
【作成】福岡県警察本部
サイバー犯罪対策課

インターネットバンキングを悪用した、不正送金事犯の手口と対策！

パソコンをウイルスに感染させる手口

（手口①）
ウイルスが、偽の「暗証番号等の入力画面（ポップアップ画面）」を表示させ、利用者にID・パスワード・第２暗証番号（※注１）を入力させ盗み取る

（手口②）
ウイルスが、利用者のログインを検知し、自動的に犯罪者が用意した口座に送金

Ａさん

迷惑メール等でパソコンが感染し、気付かないまま金融機関のHPを閲覧

Ａさんの口座
Ｂさんの口座

銀行Ａ

送金

犯罪者が用意した口座

銀行Ｂ

金融機関などを装ったメールで偽サイトへ誘導させる手口

Ｂさん

金融機関を装ったメールで、偽サイトと気づかず接続し
ＩＤ・パスワード
第２暗証番号（※注１）
等を入力

犯罪者

不正に得た
ＩＤ・パスワード
第２暗証番号（※注１）
等で、Ｂさんの口座に不正アクセス

※注１
第２暗証番号とは金融機関が利用者に事前に渡しているカード等で、指定した番号を入力させるようになっているものです。

他人事ではありません！福岡県内の状況は・・

福岡県警察サイバーマスコット「サイビー」

昨年（平成28年）中は、県内で法人・個人を合わせて３１件の被害が発生しています。法人被害の特徴として電子証明書（※注２）を利用していなかったものが複数認められました。

※注２
電子証明書とは、金融機関が発行する電子証明書を利用者のパソコンにインストールすることにより、同パソコン以外からはログインができなくなる仕組みのことです。詳細は各金融機関にお問い合わせください。

※注３
ワンタイムパスワードとは、一定時間ごとに変更され、一度しか使えないパスワードのことです。
スマートフォンアプリやカード型の専用端末等を用いる方法があります。

不正送金事犯への対策

- ウイルス対策ソフトや、パソコンのOSやインストールされている各ソフトは、常に最新の状態に更新しましょう。
- 被害防止には電子証明書を必ず取り入れるほか、専用端末等を使ったワンタイムパスワード（※３）を利用しましょう。

総合的なセキュリティ対策

- 自社に適した情報セキュリティポリシー（社内のルール）を策定しましょう。
- 万が一に備えた社内の緊急時連絡体制の整備をしましょう。連絡体制がうまく機能するか、被害等の発生を想定した模擬訓練を定期的に行うと理想的です。

サイバーセキュリティの基本講座①（パスワード管理について）

パスワードは、大切なパソコンやスマートフォンを家にたとえると、玄関の鍵のようなものです。パスワードを人に教えることは「合鍵を渡すこと」パスワードの漏えいは「鍵を失くすこと」と同じですよ。**注意して管理しましょう！**