

CyberCrime Control Project

平成 25 年第 2 号

広島県警察本部
サイバー犯罪対策課
082-228-0110

～ 最近の企業に関するサイバー犯罪（銀行不正送金） ～

社長！大変です。隣の「△▽製作所」が取引に使っていたインターネットバンキング口座から、現金 1,000 万円が他人の口座へ送金されたそうで、社長は金策に走り回っているそうです。



口座から金が消えた？△▽社長 資金繰りが厳しいと言っていたが、大丈夫かな。



それが、△▽社長しか知らないはずの銀行口座の ID とパスワードを使って、何者かが、全く他人の口座へ送金した記録が残っていました。その後、ATM から現金が引き出されています。



おいおい、被害金は返ってくるんだろうな。



△▽社長の話では、個人の口座被害は保証されるようですが、企業の口座は保証の対象ではないとのことでした。
うちの会社も〇×銀行のインターネットバンキングを使っているけど大丈夫ですか？



全国で 4 億 1,600 万円の被害が発生しています！

(平成 25 年 8 月 8 日現在)

➤ インターネットバンキングとは

従来の電話回線を使ったファームバンキングシステムとは違い、一般のインターネット回線と Windows パソコン等のウェブブラウザを使い各種の銀行取引を行えるシステムで、ほとんどの金融機関がこのシステムを導入しており、全国で 7,000 万以上の口座があるとされています。

非常に便利な反面、常時インターネットに接続し、ウイルスなどの脅威にさらされているパソコン上でシステムを動かすことから、セキュリティ対策には細心の注意が必要となります。

➤ 被害状況

平成 23 年には全国で 165 件の発生で 3 億 800 万円の被害

平成24年は、全国で64件、4,800万円の被害

欧米では2ヶ月で約2,000億円の被害

平成25年は、全国で455件、4億1,600万円の被害（8月8日現在）

➤ 犯行手口

- 何らかの形でパソコンがウイルスに感染
 - ・ ウイルスを添付したメールを開く（実行する）
 - ・ ウイルスを感染させるサイトに接続などが、感染源ではないかと推測されています。
- 感染したウイルスが、パソコンの通信傍受を開始
 - 特定の銀行への接続と判ると
 - ・ IDとパスワードを盗聴
 - ・ IDとパスワードを入力させる画面を表示し、情報を窃取（右図）
- 犯人のパソコンへ情報を送信
- 犯人の指令でウイルスは自身を消去
- 被害者口座から不正に他の口座へ送金し、ATMから現金を引き出す。



パスワード要求画面

➤ 被害の防止策

- 銀行が提供する「ワンタイムパスワード生成器（右図）」や「乱数表」を使用する。
注：ワンタイムパスワード生成器等でも完全に防御できない場合があります。
- ウイルス対策ソフトを常に最新の状態に保つ。
- WindowsなどのパソコンOSを常に最新の状態に保つ。（アップデート）
- Adobeアクロバットリーダーなどのソフトを常に最新の状態に保つ。
- 不審なメールを開かない、怪しいサイトにアクセスしない。
- 被害を知ったら直ちに警察や銀行へ届け出る。
早期届け出により犯人口座を凍結し、被害を防げる可能性もあります。



ワンタイムパスワード生成器

