あなたも狙われている！

●インターネットバンキングを狙った不正送金が急増しています！

警察庁の発表[1]によれば、インターネットバンキング利用者の情報を盗み取り、利用者の口座から不正送金する事案の被害が急増しています。

平成 24 年には 64 件、約 4,800 万円だった被害額が、平成 25 年には 1,315 件、約 14 億 600 万円の被害に達しており、前年比 29 倍になっています。

●不正送金の手口

同種の詐欺事件の手口としては「フィッシング（phishing）」という方法を用いるものがよく知られています。これは金融機関を騙った巧妙な電子メールにより金融機関の HP そっくりなページに誘導し、ID・パスワードや乱数表などの情報を盗み取るものです。

これに加え、最近、利用者のパソコンをウイルスやマルウエア（スパイウエアなど）に感染させて、それらの情報を盗み取る手口も多発しています。

平成 25 年には後者の手口によって、多くの金融機関で被害が発生しました。これらの手口の急速な巧妙化を背景に不正送金被害が増加しており、注意が必要です。

不正送金防止、2 つの鉄則！

第一の鉄則：乱数表等（第二認証情報）の入力は慎重に！

【ポイント】

絶対に乱数表に記載された全ての乱数を同時に入力してはいけません。また、乱数の一部だけ入力させたり、それを複数回繰り返したりする巧妙な手口もあります。銀行のサイトで偽画面の具体例を掲載して注意を呼びかけていることがあります。そのような注意喚起も活用・参照して、乱数表等の入力は慎重に行いましょう。

【説明】

インターネットバンキングでは、利用者と銀行が直接対面せずに取引することから、本人による利用であることを、様々な方法（「認証方式」）で確認しています。

例えば、ID と固定パスワード（第一認証情報）による認証に加え、資金移動等のタイミングで乱数表等の第二認証情報の入力を求める方式がしばしば見られます。

	ア	イ	ウ	エ
1	23	78	92	91
2	61	49	83	11
3	12	33	10	27
4	85	56	08	69

乱数表の例

[1] http://www.npa.go.jp/cyber/pdf/H260131_banking.pdf

乱数表を用いた認証（注 1）で大事なことは、乱数表を他人に知られないようにしっかりと保管することです。

しかし、乱数表そのものの保管だけでは十分ではありません。パソコンで入力する際の情報管理にも注意が必要です。昨今の情報を盗み取る手口においては、利用者を巧みに偽画面へ誘導した後、乱数表に記載された数字を入力させて詐取する実例があります。乱数表の情報が第三者に盗まれてしまうと、利用者本人になりすました第三者に不正送金されてしまう危険があります。平成 25 年には、そのような手口で多数の被害が発生しました。

第二の鉄則：インターネット利用機器を最新の状態に保とう！

ニセの画面表示などで、あなたの口座情報を盗もうとする手口に対抗するには、インターネット利用をしている機器のソフトウェアやアプリを最新の状態に保つことが重要です。

以下の鉄則を参考に利用している機器を最新な状態に保ち、被害にあわないようにしましょう。

- **アプリのこまめなアップデートで常に最新状態に！**
  - インストールされているアプリのアップデートは、更新案内に従い出来るだけできるだけ早く行い、最新の状態を保ちましょう。
- **セキュリティソフトを利用！ 検知用データは常に最新に！！**
  - 検知用データは、アップデートを自動更新にするなどして、常に最新の状態にしましょう。
- **基本ソフト（OS）のアップデートも忘れずに！！！**
  - アップデートの自動更新を有効に設定しておくことがお勧めです。常に最新の状態に保ちましょう。
- **アプリは正規アプリマーケットからインストールしましょう！**
  - 金融機関とは関係のない、第三者が作成したアプリなどは十分に注意して安易なインストールを避ける（特に無料アプリ）ようにしましょう。
  - Android 端末の場合、設定の中の「セキュリティ」の「不明な提供元 - Play ストア以外で購入したアプリケーションのインストールを許可する」を有効にしないようにしましょう。