インターネットバンキングへの攻撃手口と考えられる対応策

平成26年 8月20日

一般社団法人全国銀行協会

企画部　大坂元一

一般社団法人 全国銀行協会

目次

インターネットバンキングとは

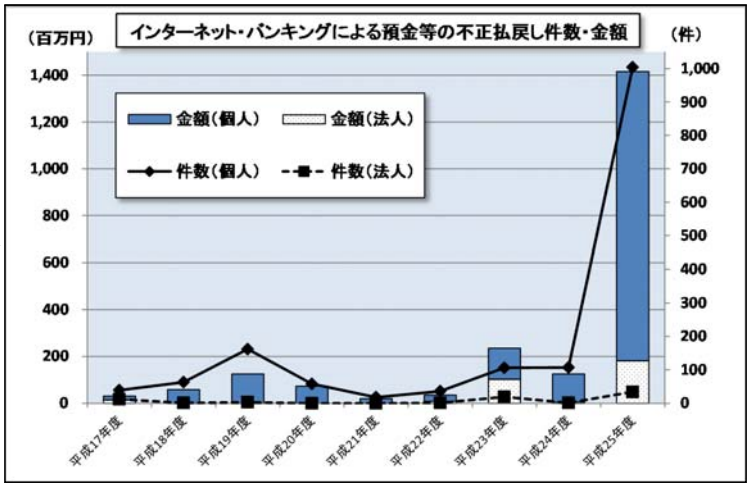
- インターネットを経由して銀行預金の残高、取引明細の確認や、振込みなどの取引が可能
- 法人のお客さま向けには、海外送金や売掛金消し込みなどのサービスも存在
- パソコンからだけではなく、スマートフォンなどからも利用可能

業態	インターネットバンキング・サービス契約口座		
	有効回答金融機関数	契約口座数	1金融機関当たり
都市銀行	5	39,166,497	7,833,299
信託銀行	3	575,000	191,667
地方銀行	61	7,349,007	120,476
第二地方銀行	38	1,098,976	28,920
信用金庫	253	1,158,662	4,580
信用組合	28	24,215	865
労働金庫	11	369,230	33,566
その他	9	16,071,517	1,785,724
合計	408	65,813,104	161,307

（注）金融情報システムセンター「平成26年版金融情報システム白書」より抜粋

インターネットバンキングにおける不正送金とは

- 銀行のホームページを偽装したニセのサイトや、マルウェアなどのウィルスに感染した顧客のパソコン経由で、
- インターネットバンキングのIDやパスワードなどの認証情報が窃取され、預金が不正に送金されるなどしてしまう

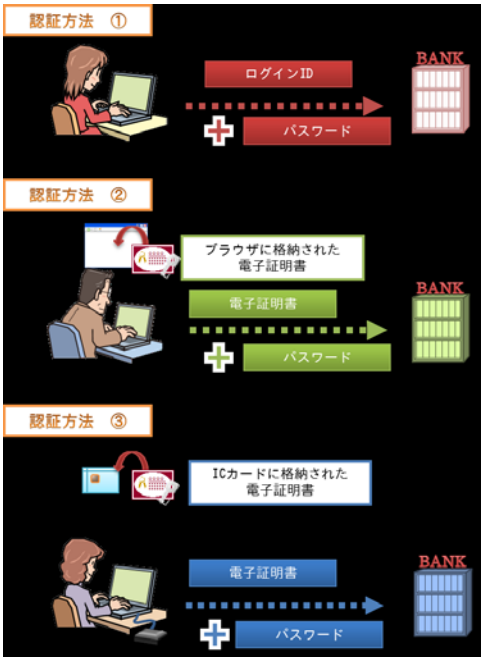


（注）上図は、全国銀行協会「盗難通帳、インターネット・バンキング、盗難・偽造キャッシュカードによる預金等の不正な払戻し件数・金額等に 関するアンケート結果および口座不正利用に関するアンケート結果について（平成26年5月発表）」（対象：全銀協正会員・準会員190行）をもとに作成

法人向けインターネットバンキングにおける認証方法

主な認証方法

- ログインIDとパスワード（固定／可変（乱数表やワンタイムパスワードなど））に基づく認証
- 電子証明書（パソコンのブラウザに格納）とパスワードに基づく認証
- 電子証明書（ ICカード等に格納）とパスワード基づく認証



（注）右図は、独立行政法人情報処理推進機構「2014年8月の呼びかけ」（平成26年8月1日）より抜粋

犯罪者の主な手口・・・①（個人向け／法人向けIB）

フィッシング

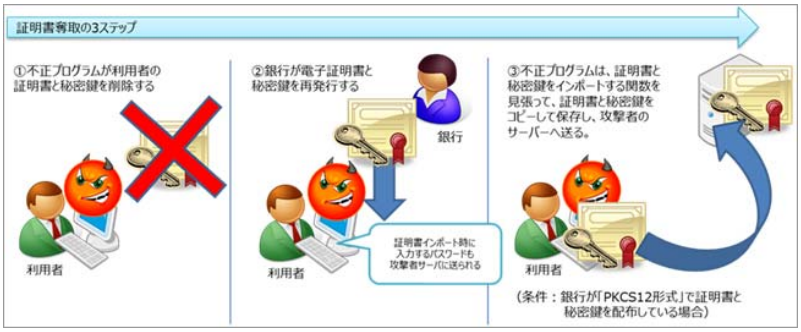
- 犯人は、銀行を装った偽のメールを送りつける
- 偽のホームページに利用者を誘導し、IDやパスワード（、乱数表の情報）などの認証情報を入力させて、これらを盗む

ウィルス／スパイウェア／マルウェア感染

- 犯人は、スパイウェアを添付したメールを送りつけたり、ホームページの脆弱な部分を改ざんして、ウィルスを忍び込ませておく
- メールやホームページを見た利用者のパソコンが、ウィルスに感染。IDやパスワードなどの認証情報の入力を促す、偽の画面を表示させて、これらを盗む
- ウィルスの中には、利用者がインターネットバンキングにアクセスする挙動を監視しており、正規のログインページ上に偽のポップアップ画面を表示して、IDやパスワードなどの入力を促すタイプも存在

犯罪者の主な手口・・・②
（法人向けIB）

- スパイウェアによる電子証明書の窃取
  - 【方法1】利用者のパソコンのブラウザ内の電子証明書と秘密鍵をすべてエクスポートし、ファイルに保存。攻撃者サーバへ送信する
  - 【方法2】利用者のパソコンのブラウザ内の電子証明書と秘密鍵をいったん削除ないし破壊。銀行から電子証明書が再発行されたタイミングで盗取ないしコピーを保存。攻撃者サーバへ送信する



（注）上図は、トレンドマイクロ社　セキュリティブログ（平成26年7月10日）より抜粋

不正送金被害に遭う原因

- 不正送金被害は、インターネットバンキング利用時のセキュリティ対策の不十分さを原因として、発生することが多い

⇒ セキュリティ対策を**複数組み合わせて採用・実施**することにより、**被害に遭遇する可能性を低減**させることが重要

⇒ フィッシングサイトや偽の画面への入力を未然に防ぐため、**取引銀行の注意喚起を確認**し、犯罪の手口を知っておくことが重要

銀行が提供している・今後提供する予定のセキュリティ対策（例示）

- 電子証明書のセキュリティ強化策
  - 電子証明書をICカード等、パソコンとは別の媒体・機器への格納
- ワンタイムパスワードや、パソコンのブラウザとは別の携帯電話等の機器を用いる取引認証
  - ハードウェアトークン、ソフトウェアトークン、電子メール通知
- セキュリティ対策ソフトの提供
- トランザクション認証
- リスクベース認証の導入・強化
- 不正なログイン・取引等の検知　　など

被害に遭わないために・・・①
－必ず実施していただきたい対応策－

- 端末（パソコンなど）のセキュリティ対策
  - 銀行が導入しているセキュリティ対策を着実に実施する
  - OSやウェブブラウザ等の各種ソフトを最新の状態に更新する（特に、ウェブブラウザ（Internet Explorer）、Adobe 、Java）
  - メーカーのサポート期限が経過したソフトは利用しない
  - （銀行が提供している、または市販の）セキュリティ対策ソフトを導入するとともに、最新の状態に更新する
  - パスワードを定期的に変更する
  - 銀行が指定した手順以外での電子証明書の利用は行わない
- 利用時の対策
  - 誰でも利用できるパソコン（例、インターネットカフェなど）では、インターネットバンキングの取引を行わない

被害に遭わないために・・・②
－できる限り実施していただきたい対応策－

- 端末（パソコンなど）のセキュリティ対策
  - パソコンの利用目的を、インターネットバンキング取引に限定する
  - パソコンや無線LANのルータ等について、未利用時は可能な限り電源を切断する
  - 取引の申請者と承認者とで異なるパソコンを利用する
  - 振込等の限度額を必要な範囲内でできる限り低く設定する
  - 不審なログイン履歴や身に覚えのない取引履歴、取引通知メールがないかどうかを定期的に確認する

- 利用時の対策
  - 取引銀行のホームページを「お気に入り」に登録しておき、そこからアクセスする
  - 銀行から電子メールを受信したときは、送信元のアドレスを確認する

被害に遭ったと思ったら

- インターネットの接続を止め、速やかに取引銀行に連絡する
- ファイルやメールの削除は行わない
- 最寄りの警察に通報し、事情を説明する
  （※）都道府県警察本部のサイバー犯罪担当課 または 所轄警察署
- 後日の取引銀行からの調査依頼や、警察の捜査に協力する

個人のお客さまに対する不正送金被害の補償
－預金等の不正払戻しに関する全銀協申し合わせ－

- 「預金者保護法」（※）の考え方を踏まえた、全国銀行協会の申し合わせ（平成20年2月19 日）

  （※）偽造カード及び盗難カード等を用いて行われる不正な機械式預貯金払戻し等からの預貯金者の保護等に関する法律。平成18年2月施行。

- 銀行が無過失でも、**被害者(個人のお客さま)に過失がない場合、原則として銀行が被害額を補償**

〔被害補償の条件〕
〇被害者が個人のお客さまであること（法人については次頁を参照）
〇被害に遭ったことを警察および銀行へ迅速に届け出ること

〔補償されない場合や補償額が減額される場合〕
〇パスワード等の管理に過失（他人に教えたなど）があった場合
〇親族による引き出しの場合
〇被害発生から30日以上経って銀行へ通知した場合　　など

法人のお客さまに対する不正送金被害の補償
－補償の考え方に関する全銀協申し合わせ－

- 全国銀行協会の申し合わせ「法人向けインターネット・バンキングにおける預金等の不正な払戻しに関する補償の考え方」（平成26年7月17日）
- 銀行と被害者(＝法人のお客さま)の双方が、一般的に必要とされるセキュリティ対策を行っていても、なお発生した不正な払戻しについて、個別銀行がその経営判断として、補償することを検討

〔被害補償検討に当たっての留意事項〕
〇法人のお客さま側に、セキュリティ対策の不作為をはじめとする一定の事象が発生している場合、銀行は補償を減額または補償をしないという判断をすることがあり得る。
〇法人のお客さまの属性（例：大、中小、零細企業、等）や、セキュリティ対策への対応力（例：当該法人がIT業種など）に応じて、「補償の対象先」（＝補償するか否か）や、（補償金額の）「上限」を個別銀行が個別の事象に応じて判断する。

ご参考

金融犯罪の未然防止策
〔銀行における口座不正利用防止への取組み①〕

１．不審な口座開設の排除・口座売買の防止（本人確認等の徹底）

- 口座開設時の本人確認や、開設目的の確認を厳格に実施
- 正当な必要性がある場合を除き、同一名義人の口座開設数を抑制するなど、不審な口座開設を排除

（参考）架空名義口座の開設防止　…　口座開設時における本人特定事項の確認の強化

- マネー・ローンダリング防止のため、口座開設時に本人特定事項の確認を実施
- 平成15年1月、**「本人確認法」**（現在の「犯罪収益移転防止法」）施行

口座開設時の公的書類（免許証、パスポートなど）による本人確認を法律で義務付け

※平成19年1月の本人確認法改正により、ＡＴＭでの現金振込みが10万円以下に制限された。

ご参考

金融犯罪の未然防止策
〔銀行における口座不正利用防止への取組み②、③〕

２．不正利用口座の凍結

- 警察（や被害者等）から通報あれば振込先口座の入出金停止（口座凍結）

銀行は、約款（普通預金規定）にもとづき、次のようなケースでは**口座を凍結**（入出金停止や強制解約）

※ ① 架空・借名口座であるとわかったとき
② 不正に譲渡されたとき
③ 法令や公序良俗に反する行為に使用されたとき

３．凍結口座名義人リストの運用

- 過去に、振り込め詐欺やインターネットバンキングにおける不正送金に利用された口座の名義人情報を警察庁がリスト化

⇒ 全銀協等を通じて各銀行に提供

- 各銀行では、口座開設時等のチェックに活用