法人ＩＢ不正送金被害に関するＱ＆Ａ

Q1. インターネットバンキングでどのような被害が発生しているのですか？

Ａ．幸い当金庫の共同ＩＢシステムを利用している信用金庫の被害報告は受けておりませんが、銀行を中心にコンピュータウイルスに感染したパソコン（ＰＣ）での法人インターネットバンキング（法人ＩＢ）の都度振込において、不正送金されるという被害が発生しています。
最近では、新潟日報で報道されましたように県内金融機関でも被害が発生しております。

Q2. 不正送金による被害金額は信用金庫で補償してもらえるのですか？

Ａ．当金庫の法人ＩＢの被害補償は、**平成 27 年 3 月 1 日より**補償要件を満たしている場合に上限 1,000 万円まで補償いたします。主な補償要件は次のとおりですが、お客さまの取組み等によっては補償対象外となりますので、不正送金被害を受けないように適正にコンピュータウイルス対策、ＩＤ・パスワード等の漏洩・詐取等のセキュリティ対策を講じていただきますようお願いいたします。
詳しくは、当金庫ホームページ「お知らせ」に掲載している「法人ＩＢ(WEB-FB)の不正送金に対する被害補償について」をご参照ください。

➢お客さまが不正利用に気づかれてから直ちに当金庫へ通知が行われていること。
※不正取引発生日の翌日から 30 日以内
➢お客さまが当金庫の調査に対し書面による十分な説明・提出を行い、これらの内容に不自然な点が認められないこと。
➢捜査機関(警察)に被害届を提出し、捜査に協力していること。
➢当金庫に被害状況を説明のうえ当金庫の調査に協力し、不正送金等が行われた時点において適正にセキュリティ対策を講じていたことを当金庫に示していること。

Q3. 法人IBの不正取引の手口はどんな特徴があるのですか？

Ａ．被害のあった銀行の発表や各種報道などから、最近の犯罪手口は主に次の３通りあるとみられています。

①偽の画面を表示しパスワードを詐取する手口です。（ＭＩＴＢ攻撃）
振込用の確認パスワードを入力する偽の画面を表示することにより利用者にパスワードを入力させ詐取し、その詐取したパスワードを用いて不正送金を行う手口です。

《MITB(Man In The Browser)攻撃とわれている手口》
ウイルスがブラウザを乗っ取り、自由に画面表示を変えたり、入力データの盗聴、送信データの改ざんなどを行う攻撃。

②電子証明書が入ったＰＣを遠隔操作により不正送金する手口です。
電子証明書方式では、電子証明書が入ったパソコン以外では、ＩＢの取引ができませんが、犯人は電子証明書が入ったパソコン自体を遠隔操作して不正送金を行う手口です。

③電子証明書をエクスポートして詐取する手口です。
ブラウザの電子証明書のエクスポート機能（バックアップ機能）を用いて電子証明書を詐取し、犯罪者のパソコン等に電子証明書をインポート（リストア）することにより不正送金を行う手口です。

※当金庫の法人IBでは、電子証明書のエクスポート(バックアップ)をできない設定に一律実施しております。
※ブラウザ： インターネットサイトを閲覧するソフトをいう。
代表的なブラウザは、IE(インターネット・エクスプローラ)。

Q4. 偽の画面ってどんな画面ですか？

A．一例ですが、下記のようにログイン後に不正な偽の画面を表示させ、都度振込送信確認番号（10 桁）を入力させようとする事象が確認されております。

《不正画面のメッセージの例》
「あなたのコンピュータをシステムが認識できませんでした。」というメッセージを表示後、下図のような不正画面が表示される。

インターネット・サービスプロバイダーが行った最近の変更、
または、あなたが行ったソフトウェアの更新による可能性があります。
引続きバンキングサービスを利用するには、表からコードを入力してください。

	1	2	3	4	5	6	7	8	9	10	
確認番号				●			●	●	●		

※振込確認時の画面または都度振込送信確認番号（10 桁）の変更画面以外から入力を求めることは絶対にありませんので、**このような画面が表示されても入力することなく**当金庫・ＩＢ担当までご連絡ください。

Q5. 信金さんでは何か対策を講じているのですか？

A．当金庫では、次の対策を講じています。

①お客様のパソコンにコンピュータウイルスが感染することによる不正送金被害が多発しているので、先ずは、ＩＢ契約者に注意喚起メールを一斉送信し、また当金庫ホームページにもお客様への注意喚起文書を掲載することにより、お客様への対策をお願いしています。

②次の対策を講じております。
・でんさいネット利用先に導入している電子証明書について、平成 26 年 6 月 23 日（月）からエクスポート（バックアップ）をできない設定に一律変更しました。
・でんさいネットを利用しない法人ＩＢ契約者についても、電子証明書のサービスを開始しておりますので、ご利用されていないお客さまは取引店にお申込みください。

③IB不正送金事案等の発生状況により、新たにお客さまに講じていただくセキュリティ対策等があれば、当金庫ホームページ、電子メール、郵送等によりお客さまに適正な情報をお届けします。電子メールアドレス、電話番号、住所等の連絡先に変更がありましたら、直ちに設定変更または当金庫所定の手続きをしていただきますようお願いします。

Q6. 不正送金の防止として、ウイルスに感染しないためにはどうすれば良いですか？
また、IDやパスワード等を詐取されないためにはどうすれば良いですか？

A．お客様のパソコンにおいて、次の確認または実施を行ってください。
これで完全とはいえませんが、かなり高い確率で防御できるといわれています。

① ウイルス対策ソフトを必ず導入してください。
また、使用期限が過ぎていないことを確認してください。
ウイルス対策ソフトの選定にあたっては、フリーウェアのウイルス対策ソフトは避けて信頼できる市販のウイルス対策ソフトを導入してください。
不明な場合は、パソコンの購入業者に相談するといいでしょう。

② ウイルス対策ソフトのパターンファイルは常に最新の状態に更新し、定期的にウイルス検査を実施してください。
ウイルス対策ソフトの自動更新機能および自動検査機能を利用するといいでしょう。
また、不明な場合は、ウイルス対策ソフトの問合せ先にご確認ください。

③ 身に覚えのないメールは開かないでください。

④ メールの添付ファイルまたはダウンロードしたファイルを使用する前には、ウイルス対策ソフトでウイルス検査を実施してください。

⑤ 不審なホームページを開いたり、フリーソフト等をインストールすることはなるべく避けてください。この場合は、速やかにウイルス対策ソフトでウイルス検査を実施してください。

⑥ ブラウザおよびOSは、常に最新の状態に更新してください。
WindowsUpdate を自動更新する設定にするとOSは最新状態に更新されます。
WindowXPはマイクロソフト社のサポートを終了しています。当金庫インターネットバンキング推奨OSをご利用ください。（当金庫ホームページに掲載しています。）

⑦ 「あなたのコンピュータをシステムが認識できません」などと偽の画面を表示し都度振込送信確認番号（10 桁）の入力を促し詐取する被害が発生しています。振込確認時または都度振込送信確認番号（10 桁）変更画面以外の画面から入力を求めることは絶対にありませんので、このような画面が表示されても入力することなく当金庫・IB担当までご連絡ください。

Q7. 不正送金の危機を想定した場合の対策はありますか？

A．お客様のパソコンにおいて、次の取扱いを実施してください。
これで完全とはいえませんが、かなり高い確率で防御できるといわれています。

① 長期間同じログインパスワードおよび都度振込送信確認番号（10 桁）を使用せず定期的に更新してください。また、推測されやすいパスワード（生年月日、電話番号、車のナンバー等）は設定しないでください。
なお、都度振込送信確認番号（10 桁）については、都度振込処理完了の都度変更することにより、万が一、都度振込送信確認番号（10 桁）が詐取された場合でも不正送金の被害防止になります。

② 都度振込の1回の振込限度額および1日の振込累計限度額を低い金額に設定変更してください。当金庫にお届けいただいている限度額内であれば、お客様自身で自由に変更できます。都度振込を利用しない間は、千円に設定し、都度振込利用時に限度額を引き上げる取扱いも可能です。

③ 対策ではありませんが、不正取引を発見または不正取引の疑いがある場合は、すみやかに当金庫のIB担当まで連絡ください。

Q8. 個人IBも利用していますが、法人IBではないので心配ありませんか？

A．最近は、法人ＩＢによる被害がマスコミ報道されていますが、個人ＩＢにおいても被害が発生しています。コンピュータウイルスに感染しないようＱ６．の確認および対策を講じてください。
また、Q7. と同様に、①ログインパスワードは定期的に更新し推測されやすいパスワードは設定しない、②1回の振込限度額および1日の振込累計限度額を低い金額に設定変更する、③不正取引を発見または不正取引の疑いがある場合は、すみやかに当金庫のIB担当まで連絡するなどの取扱いをお願いいたします。

以 上