2013 年 10 月 10 日

各　位

株式会社 り そ な 銀 行
株式会社 埼玉りそな銀行
株式会社 近 畿 大 阪 銀 行

インターネットバンキングの不正送金への対策強化について

りそなグループのりそな銀行（社長 東 和浩）、埼玉りそな銀行（社長 上條 正仁）、近畿大阪銀行（社長 中前 公志）は、増加しているインターネットバンキングの不正送金被害を軽減させることを目的に、インターネットバンキングサービス「りそなダイレクト」ならびに「近畿大阪ダイレクト」について、以下の対策を実施（強化）いたします。

１．ソフトウェアトークンを利用したワンタイムパスワードの導入

2014 年 1 月をめどに、ソフトウェアトークンを利用したワンタイムパスワードを導入いたします。ソフトウェアトークンを利用したワンタイムパスワードは、現在ご提供しているワンタイムパスワード生成器（ハードウエアトークン）の代わりに、お客さまのスマートフォンなどに専用のアプリケーションをダウンロードしてワンタイムパスワードを利用するものです。

なお、現在提供しているワンタイムパスワード生成器（ハードウェアトークン）の利用手数料（2000 円 税込）も、2013 年 10 月 15 日より、無料といたします。

２．乱数表を発行しないＷＥＢサービス提供

インターネットで残高照会・明細照会・お振替等は利用したいものの、振込はしないというお客さま向けに、「ダイレクトご利用カード」（乱数表）を発行しないサービスを 2014 年 4 月目処に開始いたします。振込機能がありませんので、不正送金等のセキュリティ面に不安をお持ちのお客さまも安心してご利用いただけます。

以　上

ご 参 考

インターネットバンキングを安全にご利用いただくために、お客さまご自身で行っていただきたい以下の対策についても各社のホームページや電子メール等で随時お知らせしています。

（１）振込限度額の適正化

振込限度額を必要最低限の金額に設定しておくことで、万一の際の被害を最小限に抑えることができる可能性があります。

（２）振込受付時（予約扱い）、振込実現時の電子メール確認

振込取引が行われると当社より『「りそなダイレクト」振込・振替受付のご案内』もしくは『「りそなダイレクト」振込・振替手続完了のご案内』という電子メールが必ず届きます。

（３）最新のウィルス対策ソフトの利用

ウィルス対策ソフトを必ずご利用いただき、かつウィルス対策ソフトは常に最新の状態に更新し、定期的にウィルスチェックを実施することでリスクを軽減できる可能性があります。

なお、既に当社ではお客さまにインターネットの各種サービスを安心してご利用いただくため、パソコンセキュリティサービス「nProtect:Netizen」を無償でご提供させていただいております。本サービスは、当社ホームページにアクセスしている間、「nProtect:Netizen」を起動すると、「nProtect:Netizen」がお客さまのパソコンを監視し、ウィルス、スパイウェアなどによる不穏な動きがあった場合、検知・駆除・遮断するものです。（本サービスは、ネットムーブ株式会社の協力を得て、ネットムーブ株式会社が提供するサービスです。）

（４）ログインした際の前回ログイン日時確認

りそなダイレクトにログインされた際は、トップページの前回ログイン日時を必ずご確認ください。

（５）残高・入出金明細の確認

口座の残高・入出金明細を定期的にチェックすることで、早期に不正送金が発見できます。

【最近の不正送金の手口】

最近発生している事例は、お客さまのパソコンをコンピューターウイルスに感染させ、インターネットバンキング（「りそなダイレクト」「近畿大阪ダイレクト」）のログインＩＤ、パスワードの入力後に、「セキュリティー強化(追加認証)のため」という理由で、ご利用カード（乱数表）の数字を「複数」同時に入力を促す「偽のポップアップ画面」を表示させ、お客さまの情報を抜き取り、不正送金をするものです。

（偽画面の特徴）

・正式な画面の上に表示される
・正式な画面と酷似している
・入力しないと画面が進まない

具体的な画面例をホームページに掲載しておりますのでご確認ください。
http://www.resona-gr.co.jp/resonabank/direct/gochui/detail/20121027.html