Press Release

Date 平成 22 年 4 月 1 日

株式会社 京都銀行
京都市下京区烏丸通松原上る
郵便番号600-8652

インターネットバンキングの

フィッシング詐欺対策を強化！

― 「検知サービス」導入にて常時フィッシングサイトの発生を監視 ―

京都銀行（頭取 柏原 康夫）では、近年増加傾向にあるインターネット取引のフィッシング対策を継続して強化しておりますが、４月１日より「検知サービス」を導入し、フィッシングサイトの発生を常時（２４時間）監視いたします。

これにより、早期にフィッシングサイトを検知・閉鎖することが可能となり、お客様をフィッシング詐欺から守ることがより強化されます。

フィッシング詐欺は、金融機関の偽サイトにお客様を誘導し、インターネットバンキングで使用するＩＤやパスワード等を不正に取得し金融犯罪に悪用するものです。

現在導入しております「フィッシングサイト閉鎖サービス」では、ご利用者からのご連絡やお問い合わせによりフィッシングサイトを発見し、迅速に閉鎖を行うことでフィッシング被害の拡大を防止するというものでしたが、「検知サービス」を導入することにより、フィッシングサイトをより早く発見することが可能となります。

当行では、今後とも多様化するお客様のニーズにお応えするために、安全性と利便性を兼ね備えた質の高いサービスを提供してまいります。

記

１．サービスの名称

「検知サービス」　　※株式会社 NTT データが RSA セキュリティ会社と連携して提供

２．サービスの内容

RSA セキュリティ株式会社が運営するオンライン不正対策指令センタ（AFCC）により２４時間・３６５日フィッシングサイトの発生を監視し、当行を装ったフィッシングサイトが検知された場合はいち早く当行に連絡されます。当行は連絡のあったフィッシングサイトを即時確認の上、株式会社 NTT データを通じて RSA セキュリティ株式会社に当該サイトの閉鎖依頼を行い、フィッシングサイトを早期に閉鎖いたします。

３．サービス開始日

平成２２年４月１日（木）

４．当行のインターネットバンキングの主なセキュリティ対策

導入時期	内容	詳細
平成 18 年 1 月	クライアント 証明書方式	京銀インターネットＥＢサービスの利用を、あらかじめ取得したクライアント証明書（電子証明書）が格納されたパソコン端末でのみ可能にするもので、ＩＤやパスワードの情報を外部のものが不正に入手してもサービスが利用できず、本人認証を行う上での極めて有効な手段となります。
平成 19 年 5 月	ワンタイム パスワードサービス	お客様の携帯電話の画面上に表示された、一度限りのパスワードを京銀ダイレクトバンキング（インターネットバンキング）のログイン画面に入力し本人認証を行うというもので、第三者による不正取引を防止する極めて有効な手段となります。
平成 20 年 4 月	ＥＶ　ＳＳＬ証明書	実在する運営者の正当なサイトであることを証明する規格で、正当なサイトの場合はアドレスバーを「緑色」で表示する機能があり、アドレスバーを確認することにより、接続しているサイトが正当なものかどうかを見分けることができます。
平成 20 年 5 月	フィッシングサイト 閉鎖サービス	万一、当行を装ったフィッシングサイトが発見された場合、当行が株式会社ＮＴＴデータを通じて、ＲＳＡセキュリティ株式会社に当該サイトの閉鎖依頼を行うことで、インターネットサービスプロバイダとの協力により当該サイトを早期に閉鎖することができます。 世界各国で立ち上げられるフィッシングサイトも対象とし、２４時間・３６５日の対応が可能です。
平成 21 年 8 月	フィッシング対策ソフト 「フィッシュカット」	当行のホームページとして閲覧しているサイトが当行の正規のサイトであるか、当行を装った偽サイトであるかが、ツールバー上の表示によって容易に判別できるようになります。また、「フィッシュカット」には、偽サイトと判別したサイトへ、お客さまが誤まって重要情報（ログインＩＤなど）を送信しようとした場合に、送信を強制的に中止する機能を備えています。

以　上