

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！

— フィッシング対策ソフト「フィッシュカット」を導入 —

京都銀行（頭取 柏原 康夫）では、これまでも継続してインターネット取引のセキュリティ強化を図ってきておりますが、近年増加傾向にあるフィッシング詐欺への対策を強化するため、フィッシング対策ソフト「PHISHCUT（以下、フィッシュカット）」を導入しますのでお知らせいたします。

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。「フィッシュカット」をご利用いただくことにより、京都銀行の正規のサイトであるかを判断し、疑いのある場合は警告を表示するなど、フィッシング詐欺からお客様を守ります。

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. 導入するソフトウェア

「PHISHCUT（フィッシュカット）」 ※ NTTコムウェア株式会社が提供

2. 「フィッシュカット」の概要

「フィッシュカット」をご利用いただくことで、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。

3. ご利用方法

「フィッシュカット」のご利用は無料です。
ご利用にあたっては、お客様がご自分のパソコンに「フィッシュカット」をインストールしていただく必要があります※（すでに「フィッシュカット」を利用されている場合はインストール不要です）。なお、インストール後は特別な操作を必要とせずにご利用いただけます。

※ 対応 OS は、Microsoft Windows2000/XP/Vista、対応ブラウザは、Microsoft Internet Explorer 6/Internet Explorer 7 です。

- 1 -

4. ご利用開始日

平成21年8月17日（月）

5. 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

(1) クライアント証明書方式（平成18年1月に導入）

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。

(2) ワンタイムパスワードサービス（平成19年5月に導入）

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。

(3) EV SSL証明書（平成20年4月に導入）

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。

(4) フィッシングサイト閉鎖サービス（平成20年5月に導入）

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。

以上