

株式会社 京都銀行

京都市下京区扇丸通松原上る
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！ フィッシングサイト閉鎖サービス「RSA FraudAction®」を導入

京都銀行（頭取 柏原 康夫）では、近年増加傾向にあるフィッシング詐欺対策を強化するため、フィッシングサイト閉鎖サービス「RSA FraudAction®（アルエスエー フロードアクション）」を導入いたします。

当行では、京銀ダイレクトバンキングのインターネットバンキングについては、ご利用時の暗証番号や乱数表、ワンタイムパスワードサービス等による本人認証方式の実施、京銀インターネット EB サービスについては、不正なアクセスの防止を目的とする電子証明である「クライアント証明書方式」を導入する等、これまで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まいりました。

フィッシング詐欺は、金融機関の偽サイトに顧客を誘導し、インターネットバンキングで使用する ID やパスワードを不正に取得し金融犯罪に悪用するものですが、今回「RSA FraudAction®」を導入することにより、世界各国で立ち上げられるフィッシングサイトを早期に閉鎖すべく対応することが可能になります。

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

「RSA FraudAction®（アルエスエー フロードアクション）」

株式会社 NTT データが RSA セキュリティ株式会社と連携して提供

2. サービスの内容

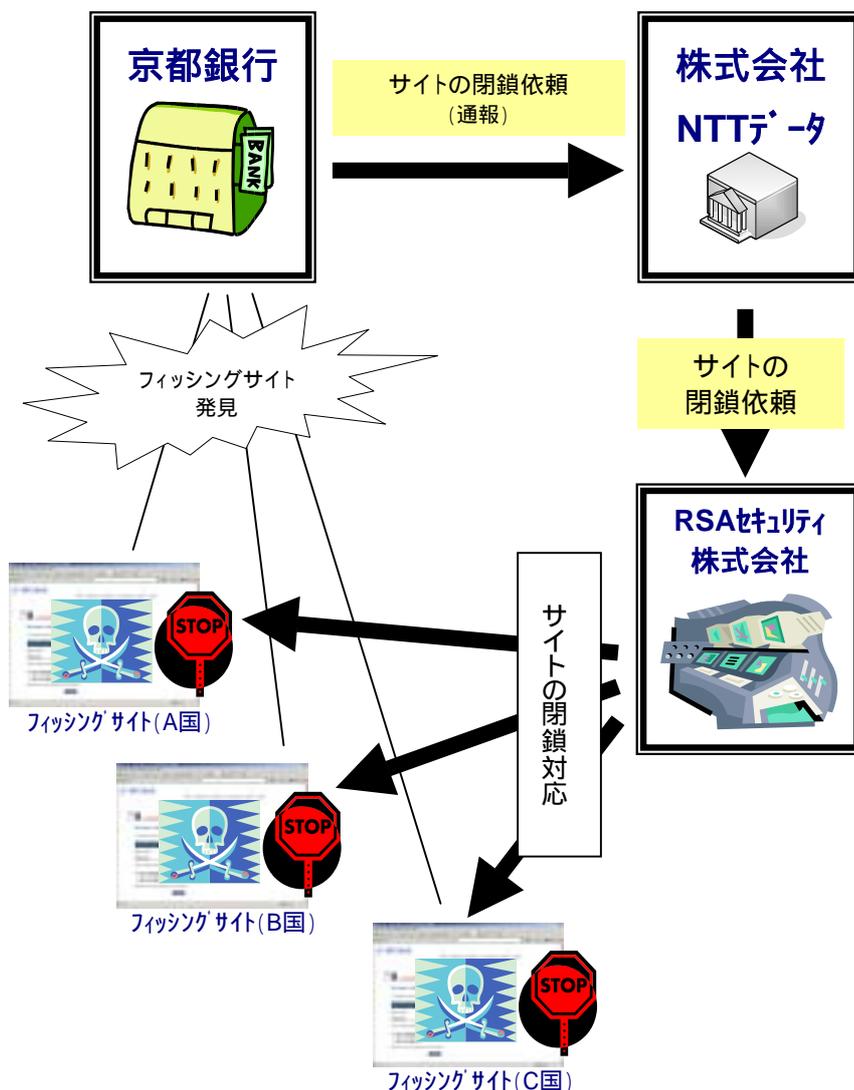
当行が株式会社 NTT データを通じて RSA セキュリティ株式会社にフィッシングサイトの閉鎖依頼を行うことで、インターネットサービスプロバイダとの協力によりフィッシングサイトの早期閉鎖を実施できます。

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。

3. サービス開始日

平成 20 年 5 月 1 日（木）

4. 「フロードアクションサービス」の仕組み



<ご参考> 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) 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パソコンのインターネットバンキングの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。

(2) クライアント証明書方式

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京銀インターネットEBサービスの利用を可能にするもので、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。

以上