平成 21 年 6 月 18 日

各位

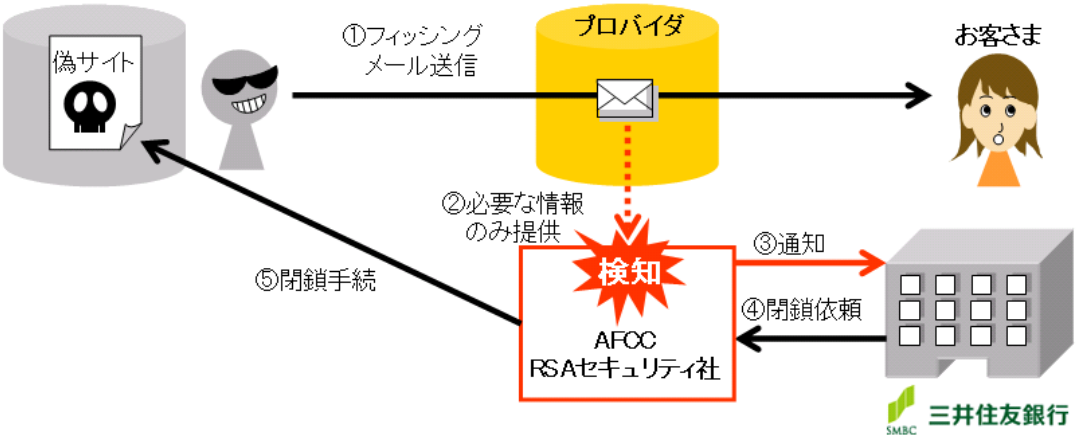
株式会社三井住友銀行

フィッシング詐欺サイト早期閉鎖サービスのレベルアップについて
～「検知サービス」オプションを追加導入し、より迅速な対応が可能に～

株式会社三井住友銀行（頭取：奥 正之）は、弊行インターネットサービスをより安心してご利用いただけるよう、平成19年7月より導入しているフィッシング詐欺サイト早期閉鎖サービス「RSA FraudActionサービス※１」に新機能である「検知サービス」オプションを追加導入し、セキュリティ強化を図ります。

従来、フィッシング詐欺サイトは、お客さまからのご連絡やお問い合わせ等によって初めて検知されることも少なくありませんでした。今般追加導入する「検知サービス」オプションは、サービス提供会社であるRSAセキュリティ株式会社経由で同社の「オンライン不正対策指令センター（AFCC）」がインターネットサービスプロバイダをはじめとする検知パートナーの協力のもと、24時間365日体制で自ら怪しいサイトを抽出して契約企業に通知するものであり、現状通り、お客さまに特段のご準備やご負担をおかけすることなく、フィッシング詐欺サイトを閉鎖するまでの時間を従来より大幅に短縮することが可能となります。

＜検知サービスのイメージ＞

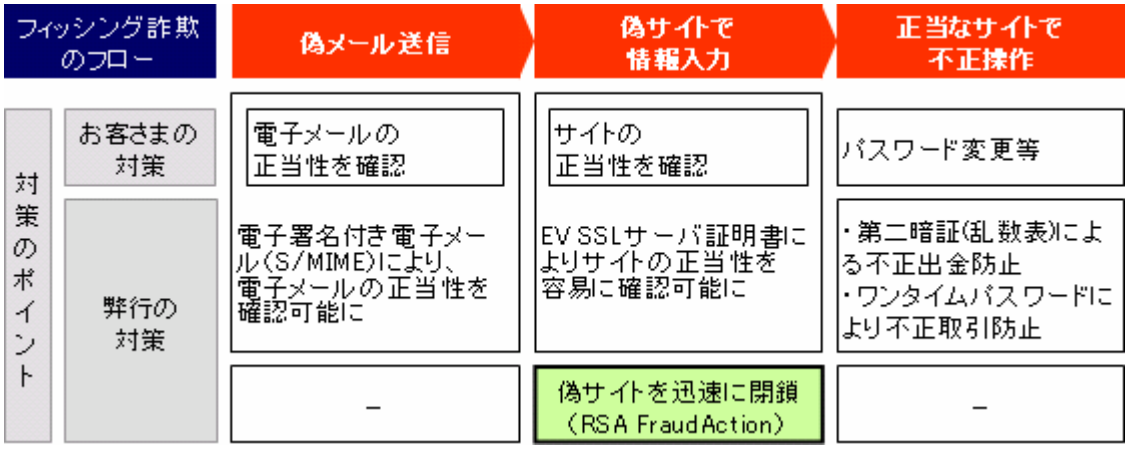


三井住友銀行では、これまでもネット犯罪に対して様々なセキュリティ対策を実施してまいりましたが、今後とも安心して銀行をご利用いただくために、有効な対策、サービスを検討してまいります。

以　上

※1　RSA セキュリティ株式会社は RSA, The Security Division of EMC の日本法人です。RSA は「情報を中心とするセキュリティ(Information-Centric Security)」のエキスパートとして、ライフサイクルを通して情報を保護する多様なソリューションを展開しています。RSA FraudAction は、オンライン不正対策指令センター(AFCC)が 24 時間、365 日体制でフィッシングサイトのシャットダウンを実施するサービスで、複数の言語を駆使し、各国の法律・規制にも精通しており、既に 140 カ国、150,000 サイトをシャットダウンした実績があります。また、シャットダウンに要する時間は殆どのケースで 5 時間以内です。

参考１：フィッシング詐欺と対策



※「偽サイトを迅速に閉鎖」部分が今回のレベルアップ部分

参考２：インターネットバンキングのこれまでのセキュリティ対策への取組

○ 取引の種類に応じた 3 つの暗証での認証　(SMBC ダイレクト実施当初から)

SMBC ダイレクトでは、取引のレベルに応じて、お申し込み時にお客さまが指定する第一暗証、乱数表を利用した第二暗証、乱数表の特定の一枠を指定した第三暗証を確認する認証方法を採用しております。

○ 暗証レベルの選択　(H17/10～)

SMBC ダイレクトでは、取引毎に必要な暗証レベルを設定していますが、「もっとセキュリティを高くしたい」というお客さまの要望にお応えし、取引毎に暗証レベルを引き上げる設定も可能にしました。

○ 暗証の管理に関する注意喚起機能実装　(H17/10～)

暗証を一定期間変更していないお客さまに限り、ログイン時に暗証変更に関する案内を表示したり、暗証変更の際に類推され易い暗証番号を設定しようとした場合に限り注意を促す機能を実装しております。

○ セキュリティ対策コンテンツ「やさしいセキュリティ教室」　(H17/10～)

お客さまご自身にも金融犯罪をご理解いただき、ご自身でも最低限の対策を行なえるよう、

ＡＴＭ、キャッシュカードのセキュリティに関する注意点に加え、フィッシング詐欺、スパイウェアの仕組み、対策のポイント等をわかりやすく解説しております。

○ 暗証入力時に新型ソフトウェアキーボードを実装　(H17/11～)

SMBC ダイレクト、法人向けインターネット窓口「ValueDoor」では暗証を入力する際、ソフトウェアキーボードを利用できます。キーボードの配置を都度変更する機能の他、クリックする際にキーボードの内容を非表示にするという新機能を持ち、画面情報を盗取するタイプのスパイウェアに対しても有効です。

○ ワンタイムパスワード　(H18/2～)

SMBC ダイレクトをご利用いただく際に、契約者番号、第一暗証の入力に加え、パスワード生成機の液晶部分に表示されるパスワードを入力して本人確認を行ないます。一度使ったパスワードは無効となりますので、万が一スパイウェアやフィッシング詐欺等でパスワードを盗まれてしまっても、不正にログインすることができなくなります。

○ 電子メールへの電子署名付与　(H18/5～)

弊行から「三井住友銀行」名義でお客さまのパソコン宛にお送りする電子メール全てに電子署名を付与し、①電子メールの送信者が間違いなく三井住友銀行であること②電子メールが送信途中で改ざんされていないことをお客さまがご自分のパソコンで容易に確認できるようにしました。

○ フィッシング詐欺サイトの迅速な閉鎖にむけた体制整備　(H19/7～)

フィッシング詐欺サイトを発見した際に２４時間、３６５日体制で迅速に閉鎖を実行する為に、「FraudAction サービス」を採用しました。

○ EV SSL サーバ証明書の導入　(H19/8～)

「閲覧している Web ページが三井住友銀行の正当なサイトかどうか」をより直感的かつ容易に確認いただけるよう、新規格のサーバ証明書「EV SSL サーバ証明書」を導入しました。

○ 取引受付完了のご連絡メール　(H19/12～)

SMBC ダイレクトで振込などのお取引を受け付けた際、あらかじめご登録いただいている電子メールアドレス宛にお知らせします。これにより、万が一、不正な操作が行われた場合でも、電子メールで検知することができます。

○ 自動コールバックによる本人確認システムの導入　(H20/10～)

SMBC ダイレクトの暗証カードを安全にお客さまにお届けするため、一旦暗証カードを無効の状態でお送りし、追加の本人確認として、銀行から自動でコールバックをすることで暗証カードをご利用いただける状態にする仕組みを導入しております。

○ 法人向けインターネットサービス（H15/1～）

法人向けインターネット窓口「ValueDoor」では取引のレベルやお客さまのニーズに応じて、パスワード認証方式、電子認証方式、IC カード認証方式の 3 種類の認証方法を採用しています。そのうち電子認証方式と IC カード認証方式につきましては、PKI（＝Public Key Infrastructure：公開鍵基盤と呼ばれる暗号化技術）を利用しておりますので、万が一スパイウェアやフィッシング詐欺等でパスワードを盗まれてしまっても、不正にログインすることはできません。

○パソコンバンク Web21 への「振込データ改ざん防止システム」導入（H20/7～）

お客さまの内部統制強化をサポートすべく、お客さまが三井住友銀行に送信する振込データが、お客さま企業内で改ざんされていないことを担保する仕組み「振込データ改ざん防止システム」をオプションでご用意しております。

○ 国際 CMS:SMAR&TS

弊行海外拠点（豪亜）とお取引のある法人のお客さま向けインターネットバンキング「SMAR&TS」においても、一定期間ごとの暗証番号変更誘導機能・ワンタイムパスワード・電子メールへの電子署名付与・フィッシング詐欺サイトの迅速な閉鎖に向けた体制整備・EV SSL サーバ証明書の導入を実施済です。