平成 19 年 6 月 12 日

各　　位

株式会社 三井住友銀行

フィッシング詐欺対策の強化について
～より安心してご利用いただく為のネットセキュリティ強化～

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、フィッシング詐欺に対して今回、新たに２つ対策を追加し、セキュリティ強化を図ります。

１．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

お客さまへの詐欺対策の提供に留まらず、弊行がフィッシング詐欺時に作成される弊行のホームページに見せかけた偽の Web サイト(フィッシングサイト)を、迅速に閉鎖させる為に、今回、ＲＳＡセキュリティ社が提供する、各国のインターネットサービスプロバイダとの協力によってフィッシングサイトを閉鎖するサービス「RSA FraudAction サービス」を採用しました。※１

これにより、国内外のフィッシングサイトを対象に、２４時間、３６５日体制で、フィッシングサイトに対してしかるべき対応を講じることが可能となります。

２．EV SSL サーバ証明書※２の導入

Windows Vista ™の Internet Explorer7 等（※３）で弊行のインターネットサービスをご利用のお客さまに、現在閲覧している Web ページが三井住友銀行の正当なサイトかどうかを、より視覚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」を導入します。

具体的には、Windows Vista ™ の IE7 であれば、お客さまに新しくソフトのインストール等の手間を掛けることなく、ブラウザのアドレスバーが緑に変わったり、サイト運営者名などが表示される為、フィッシングサイトとの判別が視覚的に簡単に行うことが出来るようになります(※４)。導入は、個人向けインターネットサービスより順次行ってまいります。

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 130 カ国、34,000 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。

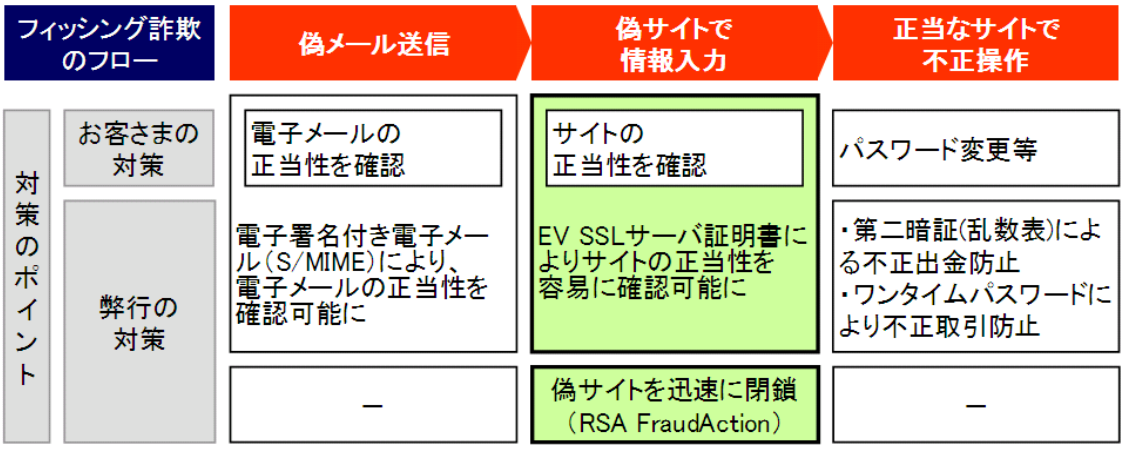
※２　今まで認証局によって個別に制定していたサーバ証明書の発行基準を全世界標準の厳格な発行基準に統一し、サイト運営組織の実在性の信頼度を高めた新規格の電子証明書。

※３　Windows XP SP2 の Internet Explorer7 でも証明書の更新を行うことで利用可能。

※４　EV SSL サーバ証明書の場合、確認方法は以下のようになります。

確認ポイント	現状のサーバ証明書	EV SSL サーバ証明書
正当な電子証明書か	ブラウザの警告が出ないこと	アドレスバーが緑であること
暗号化通信をしているか	鍵マークがあること	
三井住友銀行の電子証明書か	鍵マークをダブルクリックし電子証明書の詳細を確認し、発行先が三井住友銀行のドメイン(***.smbc.co.jp)であること	アドレスバーの右に表示される企業名が三井住友銀行であること
正しい認証局が発行しているか	電子証明書の詳細で発行者がベリサインであること	

参考１：フィッシング詐欺と対策



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　(One's ダイレクト実施当初から)

One's 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～)

One's 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。
また、法人向けインターネット窓口「ValueDoor」では、管理者さまにて利用者さまのValueDoorIDのパスワードに有効期限を設定することができる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。
※法人のお客さま向け「やさしいセキュリティ教室(法人編)」も H18/12 より提供しております。

○ 暗証入力時に新型ソフトウェアキーボードを実装　(H17/11～)

One's ダイレクト、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～)

One's 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。
また、国際CMS（弊行海外拠点用法人向けインターネットサービス※）においても承認用パスワードとして本方式を採用しております。（※SMAR&TS:H15/8～）

○ 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。

○ 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。