平成 21 年 10 月 13 日

各　　位

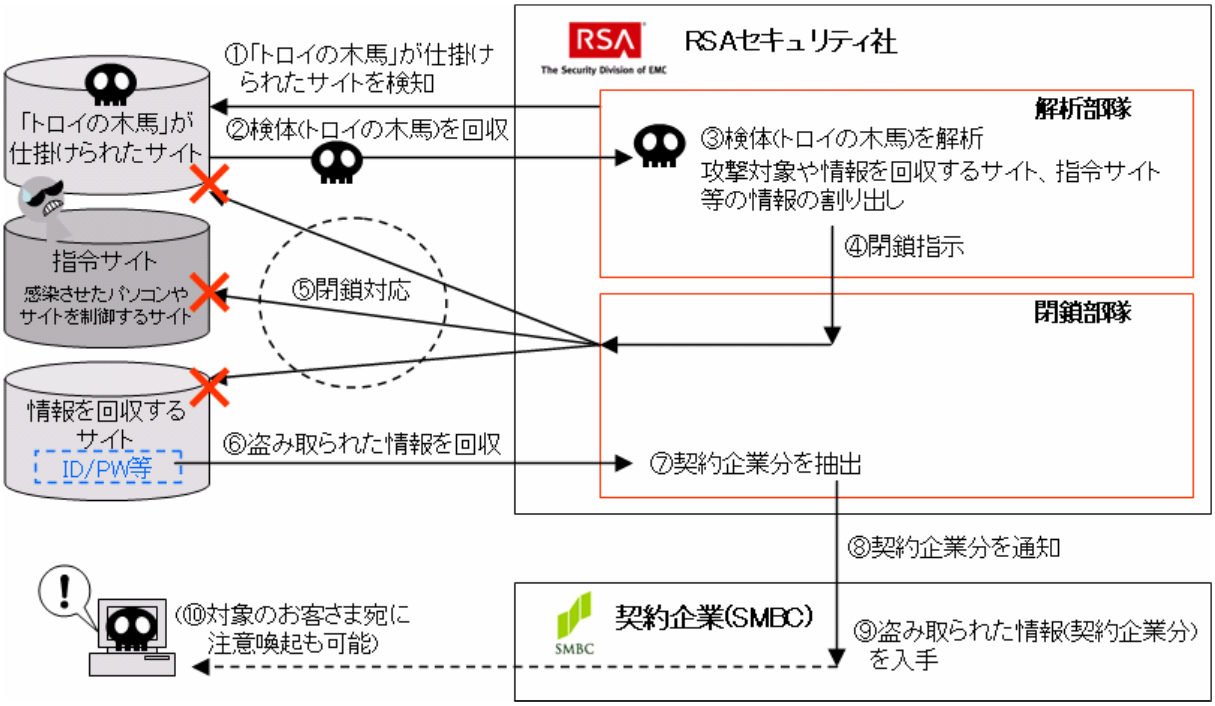
株式会社三井住友銀行

スパイウェア対策の強化について
～弊行のサービスを狙った「トロイの木馬」を配布するサイトを迅速に閉鎖～

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、弊行のインターネットサービスを狙ったスパイウェア「トロイの木馬(※1)」を配布しているサイト等を検知し、閉鎖するサービスを日本で初めて導入し、セキュリティ強化を図ります。

弊行では、スパイウェアの危険性について、従来からホームページのコンテンツ『やさしいセキュリティ教室』等でその内容を詳しく解説すると共に、ワンタイムパスワードをはじめとする各種対策を実施してまいりました。今回、ＲＳＡセキュリティ株式会社(※2)が提供する「RSA FraudActionサービス」の新機能である「Anti-Trojan Service」オプションを追加導入することで、スパイウェアに対して、全く新しいアプローチによる能動的な対策を行うことが可能となりました。

＜サービスのイメージ＞



従来はお客さまご自身でスパイウェアに侵入されないように対策を行なっていただいておりましたが、今後はお客さまご自身での対策に加え、弊行としても、本サービスを利用することで、危険なサイトを検知・閉鎖し、お客さまの個人情報等が盗まれ続ける状況を回避する対策が打てると共に、既にパソコンがスパイウェアに感染している可能性の高いお客さま向けに個別に適切な対応をお願いすることが可能となります。

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　トロイの木馬

ユーザーに気づかれずにパソコンに入り込み、様々な活動を行う不正プログラムです。感染すると、

・パソコンの画面・操作・保存されているファイル全てを見られる、または外部に送信される
・自分のパソコンで勝手に悪質なホームページを立ち上げられる
・自分のパソコンから勝手に悪質なメールなどが送信される
・更に悪質なウイルス等に感染させられてしまう

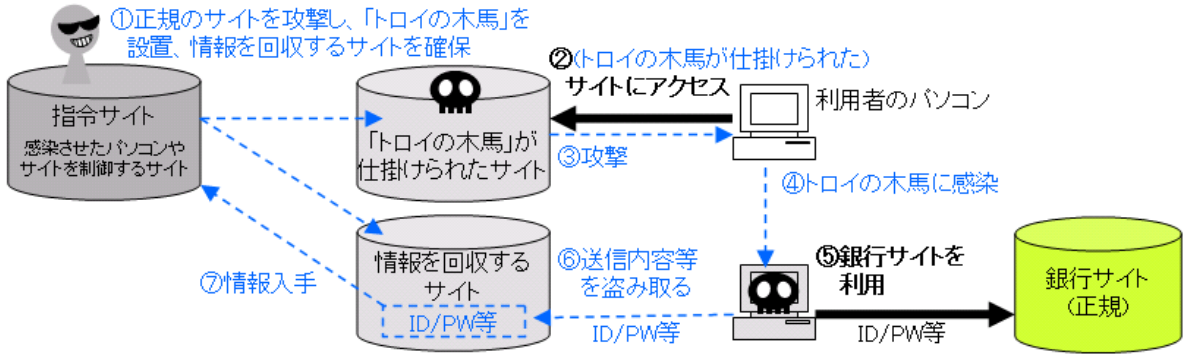
等のリスクに晒されます。パソコン内部から活動を行うため、感染した状態では、外部からの攻撃に対して対策を行っても効果はなく、感染したパソコンは悪意の第三者のコントロール下に置かれた状態になってしまいます。

(参考)「トロイの木馬」名前の由来

古代ギリシャ時代トロイ戦争において、難攻不落の城を落とすため、ギリシャ軍が城の前に撤退を装い巨大な木馬を放置。城の人間が戦利品として城内に引き入れたところ、夜になって木馬の中に潜んでいた兵士が城の内部から火を放ち、陥落させたという逸話からこの名称が付いたと言われています。

※2　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、200,000 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： サイトから感染するトロイの木馬の一例



※青字・点線部分：利用者の気付かないところで進行する箇所

① 悪意の第三者が予め脆弱性（セキュリティ上の問題）のあるサイトに密かに攻撃をしかけ、悪意の第三者のコントロール化に置き、そこにトロイの木馬（ウイルス）を仕掛けます。

②～④ 仕掛けられたサイトを閲覧した際、閲覧者のパソコンに脆弱性があった場合、感染します。

⑤～⑦ 感染したパソコンがトロイの木馬内に設定された特定サイト（主に金融機関サイト）にアクセスすると、送信情報等を根こそぎ盗み取られてしまいます。

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 ダイレクト取扱開始当初より）

SMBC ダイレクトでは、取引のレベルに応じて、お申込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 （平成 17 年 10 月より）

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 （平成 17 年 10 月より）

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」 （平成 17 年 10 月より）

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。

○ 暗証入力時にソフトウェアキーボードを実装 （平成 17 年 11 月より）

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 （平成 18 年 2 月より）

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うサービスです。1 分毎に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 （平成 18 年 5 月より）

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 （平成 19 年 7 月より）

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、「RSA FraudAction サービス」を採用しました。また平成 21 年 7 月からは「検知サービス」オプションを追加導入し、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、自ら怪しいサイトを抽出することで、閉鎖までの時間を更に短縮することを可能としました。

○ EV SSL サーバ証明書の導入 （平成 19 年 8 月より）

「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 （平成 19 年 12 月より）

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 （平成 20 年 10 月より）

SMBC ダイレクトの暗証カードを安全にお客さまにご利用いただくため、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を導入しております。

○ 法人向けインターネットサービス（平成 15 年 1 月より）

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（平成 20 年 7 月より）

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「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。