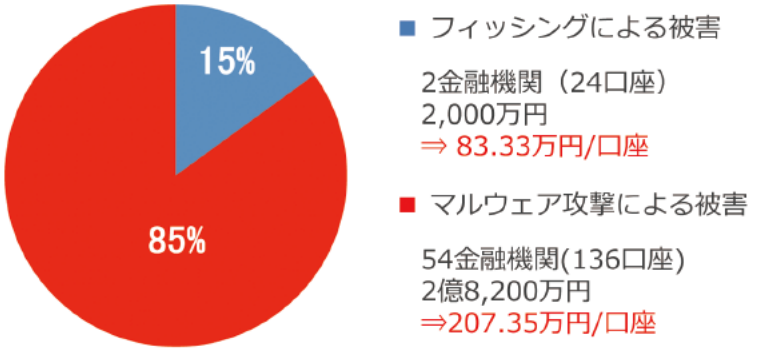
FOCUS

インターネットバンキングユーザーを狙う新しい脅威

インターネットバンキングを取り巻く状況

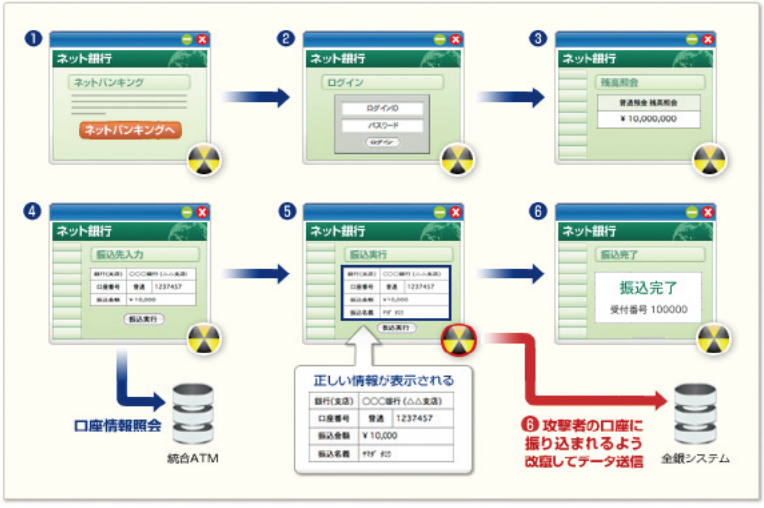
従来、インターネットバンキングユーザーをターゲットとした攻撃は、金融機関などを装ってメールを送信し、メール内のリンクから偽のWebサイトにアクセスさせて、口座情報や認証情報を盗み出すフィッシング詐欺や、フィッシングと組み合わせて、ZeusやSpyEyeなどのオンラインバンキングマルウェアを使って同様の情報を奪取する攻撃がある。

図1:インターネットバンキングの被害状況



出所：警察庁広報資料（平成23年12月15日）
インターネットバンキングに係る不正アクセス禁止法違反等事件の発生状況について

図2:MITBを使った攻撃シナリオの一例



2011年12月に警察庁が発表したインターネットバンキングを狙ったサイバー攻撃の被害状況(図1)によると、被害状況の内訳は、フィッシング詐欺よりもマルウェアによるものがかなり大きな割合を占めていることがわかる。

新しい脅威(MITB攻撃)の出現

近年、欧米を中心にインターネットバンキングのユーザーをターゲットとしたMITB(Man in the Browser)攻撃による被害が拡大している。攻撃の手法としては、コンピュータに感染したマルウェアがブラウザを乗っ取り、ユーザーがインターネットバンキングサイトにログインした後に、マルウェアがブラウザの画面を書き換えて認証情報を奪取したり、送金情報を不正に変更するといったものである。(図2)

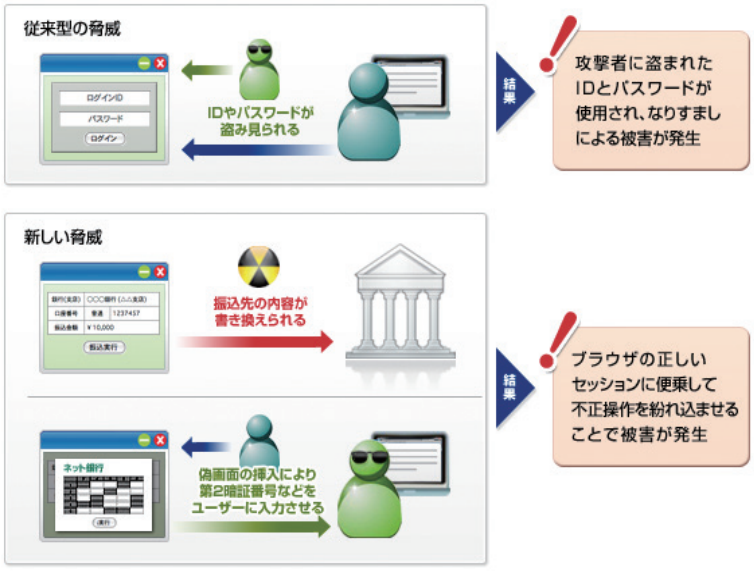
日本国内でも2012年10月に大手銀行各社のネットバンキングサービスで偽画面を表示させて乱数表の情報入力などを促すマルウェアが問題となったが、これもMITBマルウェアによるものと考えられる。

ユーザーからすると、アクセスしているのは本物のWebサイトであり、マルウェアによって不正に書き換えられたブラウザの表示内容にしたがって疑いなく処理を進めてしまう。オンラインバンキングサービスを提供する側からしても、正当な手続きによってログインしたユーザーによるトランザクションなので、オンライン詐欺の被害に気付くのが難しい攻撃となっている。(図3)

有効な対策の選択

MITB攻撃は、乱数表やUSBトークンなどによるワンタイムパスワードや二要素認証といった認証技術を回避する目的で編み出された攻撃手法であり、ユーザーによる正当な認証手続を経たセッショ

図3:従来の脅威との違い



ンに便乗するため、従来のログイン保護技術や認証技術では防御できない。

また、MITB攻撃は、ブラウザに干渉するマルウェアを使った攻撃だが、新しいマルウェアが数万種も発生している現状では、パターンマッチングによる従来のマルウェア対策技術ではMITBマルウェアの感染をリアルタイムに防ぐことも困難となっているのが現状である。

こういった現状に対し、有効と考えられる対策としては、大きく3つ考えられている。

一つは、アウトオブバンド認証で、Webブラウザ以外の通信チャネル(携帯電話やSMSなど)を併用して認証を行うことで、二要素認証を強化したタイプの対策である。

もう一つは、リスクベース認証である。今までのネットバンキングサービスの利用状況から、アクセス元のIPアドレスやロケーション、利用時間帯、マウスクリックの間隔などの様々なデータを分析することで、不正アクセスの可能性が高いと思われる状況を検知した場合には取引を中断させ、インターネット以外の手段(電話等)で顧客に確認を行うなどの対策だ。

最後の一つは、セキュアブラウザだ。前述のとおり、MITB攻撃は一種のマルウェア攻撃であり、MITBマルウェアはWebブラウザに干渉することで、偽の画面を表示させたり、不正に送金情報を変更するが、端末自体にマルウェアが感染したとしても、マルウェアがWebブラウザに干渉できないように保護することができる。

お客様「が」守る から、お客様「を」守る へ

FFRIでは、この3つ目のアプローチを実現するFFRI Limosaを開発した。セキュアブラウザは、コンシューマー向けの統合セキュリティソフトの幾つかで既に提供されているが、FFRI Limosaは、コンシューマーではなく、Webサービス事業者を販売対象としている。いまやネットバンキングは、社会インフラの一つであり、その情報セキュリティ対策を顧客の自己責任に任せるのではなく、サービス提供者側が顧客を守り、自社サービスの付加価値を向上させるソリューションとして考えていただきたいからである。

FFRI Limosaが提供する3つのメリット

①MITBの攻撃対象であるブラウザを保護することで、MITB攻撃の脅威から顧客を守り、安全なWebサービスを提供できる。

②サイトにログインする際に、自動的にダウンロードされてブラウザがセキュアになるため、ユーザーに余計な操作をさせる必要がない。

③導入・運用・サポートコストの安さ。銀行の基幹システムに手を加える必要はなく、WebサイトからFFRI Limosaをダウンロードさせる仕組みさえ構築できれば良いため、アウトオブバンド認証やリスクベース認証のような大掛かりなシステム変更の必要もない。また、USBトークンのような物理的なデバイスと違って紛失のリスクもないため、サポートコストも削減できる。(**図4**)

図4:FFRI Limosaによるブラウザの保護