報道関係者各位
プレスリリース

2013 年 12 月 5 日
株式会社 FFRI

金融機関が無償で提供するセキュリティ対策ソフトの利用者は 5 人に 1 人以下！
FFRI、インターネットバンキングに関するセキュリティ意識調査を実施
～セキュリティを重視しながらも、積極的な対策は不十分な利用者が多数～

サイバーセキュリティ領域において国内で独自の研究開発活動を展開している株式会社 FFRI（本社：東京都渋谷区、代表取締役社長：鵜飼裕司、以下 FFRI）は、2013 年 11 月 21 日～11 月 22 日、全国の 20～60 代男女のインターネットバンキング利用者を対象としてインターネットバンキングに関するセキュリティ意識調査を実施いたしました。

◆インターネットバンキングに関わる犯罪の被害に遭ったことがあるのは 10 人に 1 人以上
◆インターネットバンキングを選定する際のポイントは
1 位：手数料の安さ 51.4%、2 位：セキュリティ対策の充実 47.4%、3 位：健全な経営状態 46.0%
◆インターネットバンキングの利用履歴を毎回確認するのは 3 人に 1 人以下
◆金融機関の Web サイトの真正性（サイト証明書等）を確認しないのは 約 6 割
◆金融機関が無償で提供するセキュリティ対策ソフトを利用しているのは 5 人に 1 人以下

警視庁のまとめによると、今年のインターネットバンキングを利用した不正送金の被害額が、10 月 15 日までに 19 銀行で 766 件、計約 7 億 6,000 万円にのぼっており、過去最悪とされています。

本調査は、こうした状況をふまえ、インターネットバンキング利用者のセキュリティに関する意識や実態を把握すべく実施いたしました。本調査の結果から、セキュリティに関する意識を高く持ちながらも、その対策の不十分さが明らかになりました。次のページから、主な調査結果をご報告いたします。

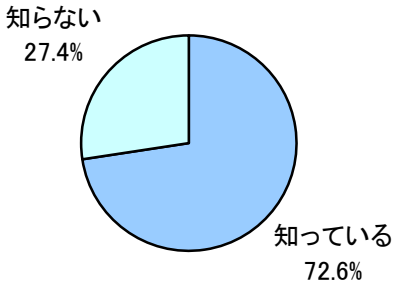
【調査概要】
・調査方法：インターネット調査
・対象者 ：インターネットバンキングを利用する全国の 20～60 代男女
・割付方法：性別×年代別の均等割付
・調査期間 ：2013 年 11 月 21 日～11 月 22 日
・回答者数 ：420 名

＊文中の表記について：<n>「有効回答数」を表しています。

◆<u>インターネットバンキングでの不正送金被害の拡大を知っているのは</u>　約 7 割

インターネットバンキングの不正送金被害が拡大していることを知っているかを尋ねると、72.6%の人が「知っている」と回答しています。インターネットバンキングのリスクについては多くの方が認識していることがわかりました。

Q.インターネットバンキングでの不正送金被害が拡大していることをご存知ですか？(n=420)

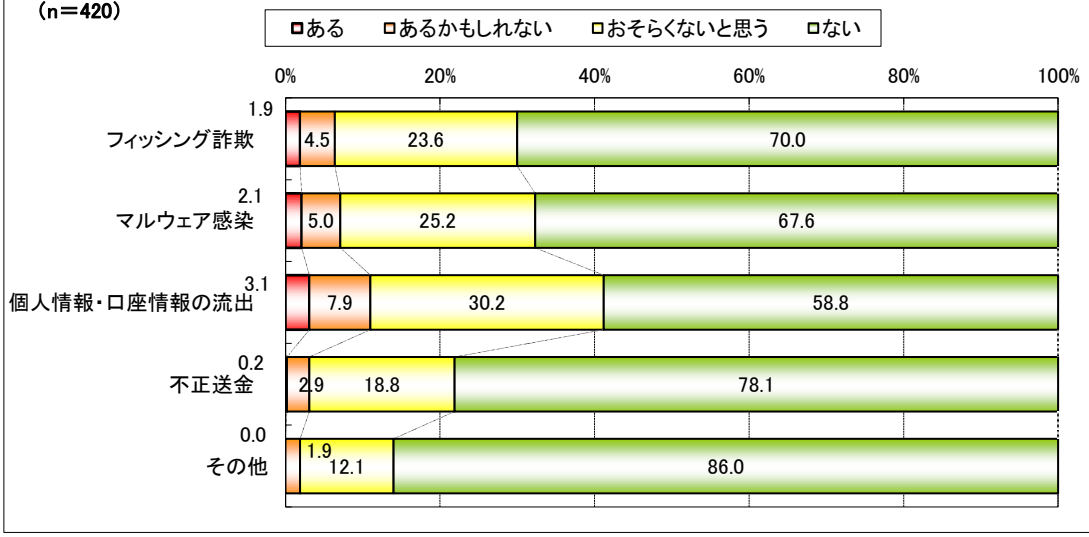


◆インターネットバンキングに関わる<u>犯罪の被害に遭ったことがある</u>のは　10 人に 1 人以上

フィッシング詐欺、マルウェア感染、個人情報・口座情報の流出、不正送金等、インターネットバンキングに関わる犯罪の被害に遭ったことがあるかを尋ねたところ、「個人情報・口座情報の流出」の被害が最も多く、「ある（3.1%）」「あるかもしれない（7.9%）」を合わせて、11.0%と 10 人に 1 人以上が被害を経験していることがわかりました。

**Q.あなたが今までにインターネットバンキングに関する犯罪被害に遭った、
もしくは被害に遭いそうになった経験について、当てはまるものを選択してください。**

**実害の有無は問いません。
例えば、フィッシングサイトと思われるWebサイトにアクセスしたが、
セキュリティ対策ソフトの警告により口座情報等を入力する前に気付いたケースや、
セキュリティ対策ソフトがマルウェアを検出したことによって気付いたケースなども含みます。
（n＝420）**



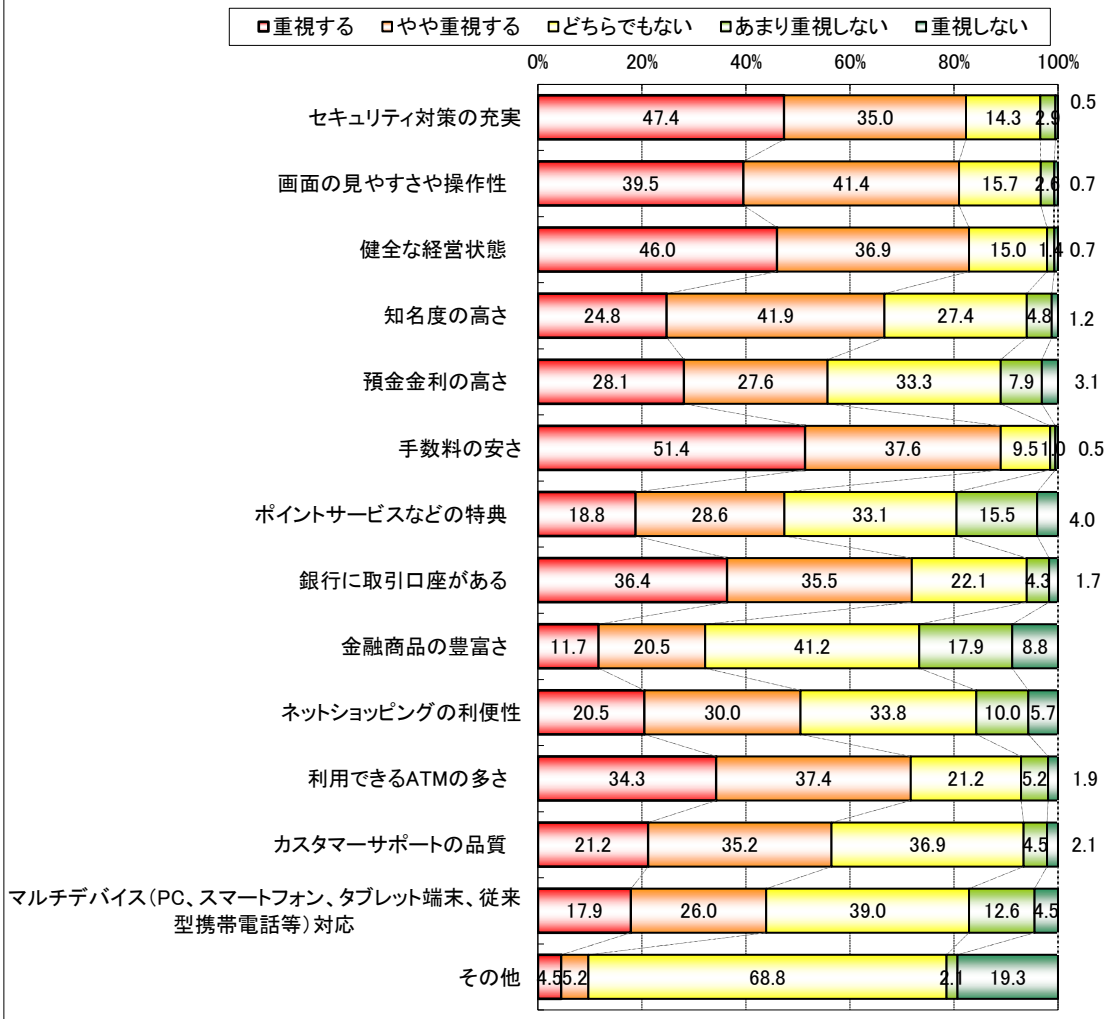
◆<u>インターネットバンキングを選定する際のポイント</u>は

1 位：手数料の安さ　51.4%、<u>2 位：セキュリティ対策の充実　47.4%</u>、3 位：健全な経営状態　46.0%

インターネットバンキングを選定する際のポイントを尋ねたところ、「重視する」のは「手数料の安さ（51.4%）」、「セキュリティ対策の充実（47.4%）」、「健全な経営状態（46.0%）」の順でした。

手数料の安さと同様にセキュリティ対策の充実を重視する人が多いことが明らかになりました。

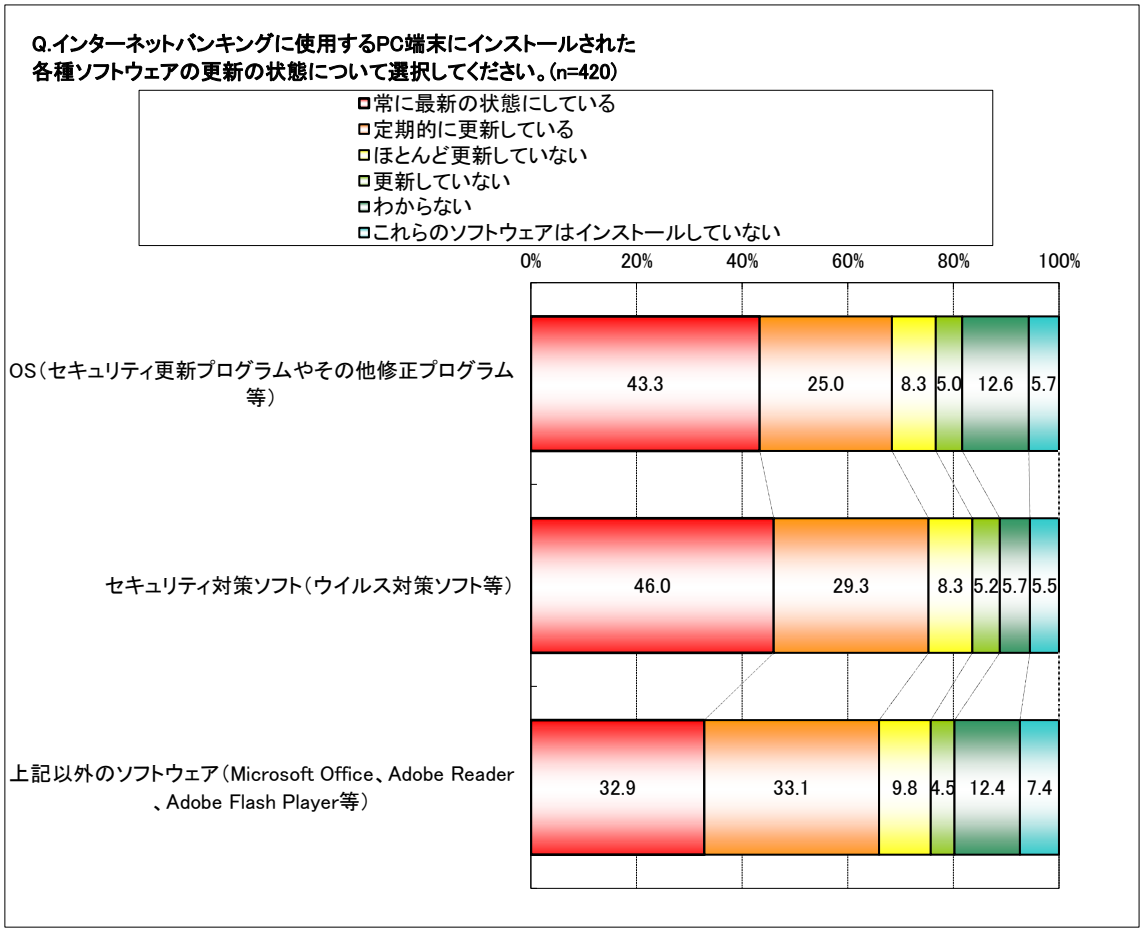
Q.インターネットバンキングを選定する際のポイントについてあてはまるものをそれぞれひとつずつ選択してください。(n=420)



◆<u>インターネットバンキングで利用するセキュリティ対策ソフトを更新しているのは</u>　7 割以上

インターネットバンキングに使用する PC 端末にインストールされた各種ソフトウェアの更新状態について尋ねると、OS、その他のソフトウェアともに「常に最新の状態にしている」「定期的に更新している」を合わせて約 7 割となりました。ウイルス対策ソフト等のセキュリティ対策ソフトに関しては「常に最新の状態にしている（46.0%）」「定期的に更新している(29.3%)」を合わせて 75.3%で 7 割以上となっており、特に意識の高さが表れました。

一方で、別の設問で不正送金の被害拡大について認識していると答えた方の中にも、約 2 割の人がインターネットバンキング利用端末のセキュリティに配慮されていないということがわかりました。

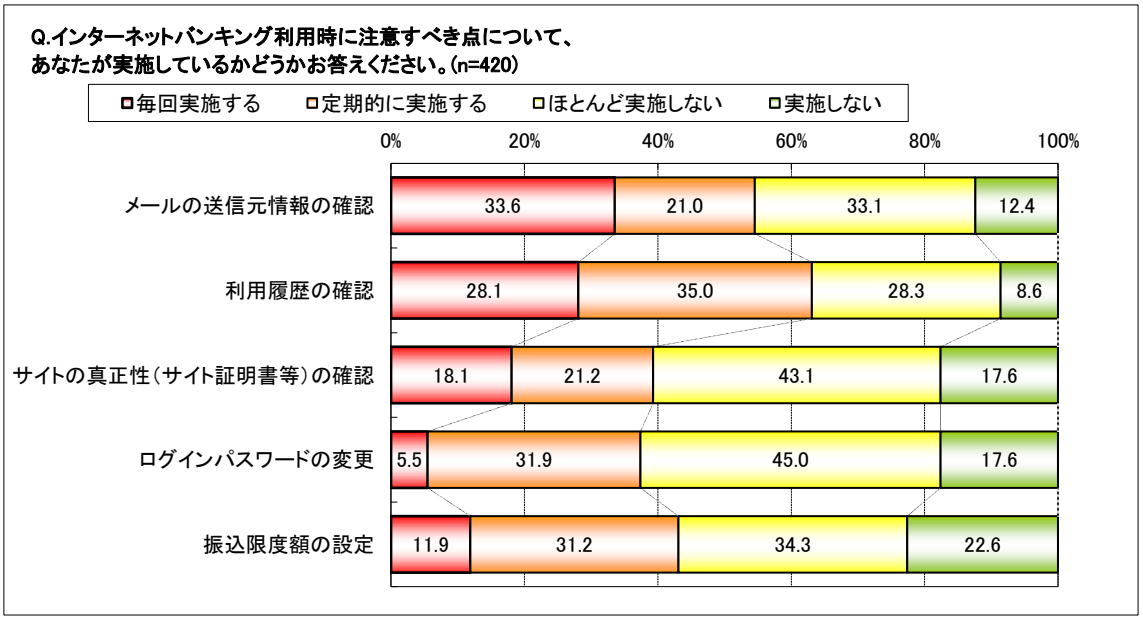


◆インターネットバンキングの利用履歴を毎回確認するのは　3 人に 1 人以下

◆金融機関の Web サイトの真正性（サイト証明書等）を確認しないのは　約 6 割

インターネットバンキング利用時に注意すべき点について実施していることを質問すると、「利用履歴の確認」を「毎回実施する」人が、28.1%と約3割でした。

「サイトの真正性（サイト証明書等）の確認」は「ほとんど実施しない（43.1%）」「実施しない（17.6%）」を合わせて 60.7%と約 6 割。「ログインパスワードの変更」に関しても「ほとんど実施しない（45.0%）」「実施しない（17.6%）」を合わせて 62.6%と約 6 割でした。OSやセキュリティ対策ソフト等の更新頻度に比べ、インターネットバンキング利用時に注意すべき点については意識が低いことがうかがわれます。



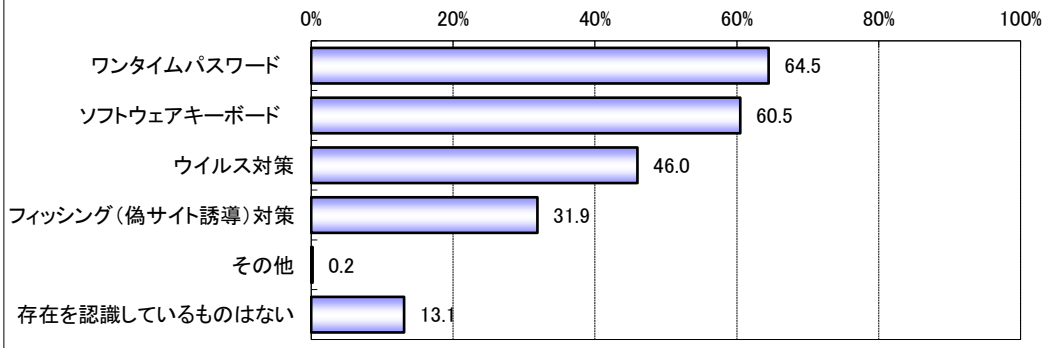
◆金融機関のワンタイムパスワード、ソフトウェアキーボードの認知は　6割超

◆金融機関のフィッシング対策の認知は　わずか約 3 割

金融機関がインターネットバンキング利用者に提供している各種セキュリティ対策について、存在を認識しているものを質問したところ、「ワンタイムパスワード」は 64.5%、「ソフトウェアキーボード」は 60.5%と、6 割以上が認知していることがわかりました。その一方で「ウイルス対策」は 46.0%、「フィッシング(偽サイト誘導)対策」は 31.9%と認知が低く、「存在を認識しているものはない」と答えた人も 13.1%でした。

インターネットバンキングで利用を強制されている対策（ワンタイムパスワード、ソフトウェアキーボード）の認知は高く、金融機関が推奨しているものの、利用者が自身でダウンロードをする必要がある等、利用者の意志に委ねられている部分がある対策（ウイルス対策、フィッシング対策）の認知は低い傾向があると考えられます。

Q.あなたが利用している金融機関がインターネットバンキング利用者に対して提供しているセキュリティ対策について、存在を認識しているものを選択してください。（いくつでも）(n=420)

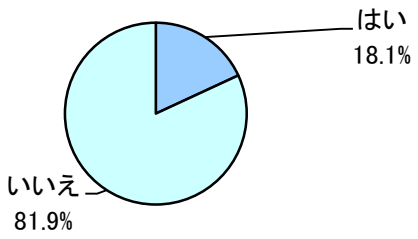


◆金融機関が無償で提供するセキュリティ対策ソフトを利用するのは 5 人に 1 人以下

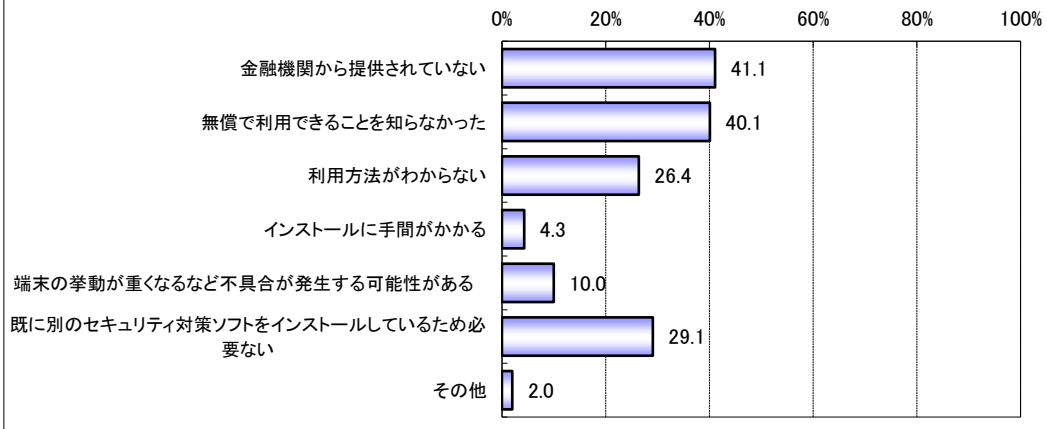
金融機関から提供されているセキュリティ対策ソフトを利用しているかどうかを尋ねると、「はい」が18.1%と 5 人に 1 人以下でした。

利用しない理由を質問したところ、「金融機関から提供されていない(41.1)%」が最も多く、「無償で利用できることを知らなかった(40.1%)」「利用方法がわからない(26.4%)」といった、利用者への認知不足と考えられるものや、「インストールに手間がかかる(4.3%)」「端末の挙動が重くなるなど不具合が発生する可能性がある(10.0%)」といった、インストールの手間や動作性の悪さを挙げる人もいました。また、「既に別のセキュリティ対策ソフトをインストールしているため必要ない」と考える人も 29.1%と約 3 割でした。「その他」と答えた人の中には、「信頼できないソフトだから使えない(30 代、男性、自営業)」といった意見がありました。

Q.金融機関から無償で提供されているセキュリティ対策ソフトを利用していますか？
※セキュリティ対策ソフトを提供されていない／利用しているかわからない方は、
いいえをお選びください。(n=365)



Q.金融機関から無償で提供されているセキュリティ対策ソフトを利用しない理由は何ですか？
以下からあてはまるものをすべて選択してください。(いくつでも)(n=299)



◆利用者自身がセキュリティ対策ソフトの出す警告の内容を判断して操作する必要性は
３人に１人が「どちらでもない」　理由は「判断が難しい」「よくわからない」

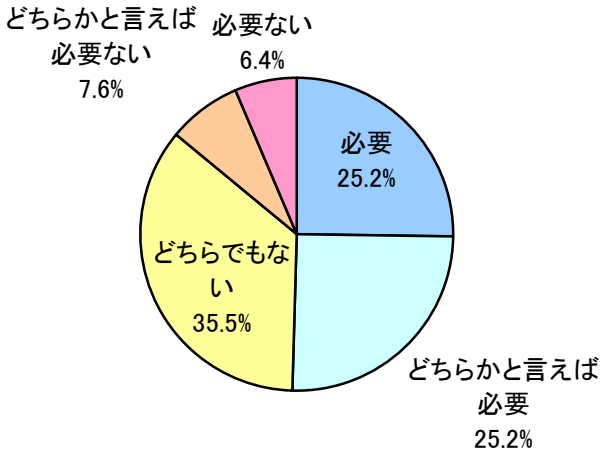
セキュリティ対策ソフトの出す警告の内容を利用者が判断して操作することの必要性について質問すると、「必要（25.2%）」「どちらかと言えば必要（25.2%）」と合わせて、過半数の人が必要と感じていることがわかりました。その理由としては、「その程度の手間は安全のためには仕方がない（男性、50 代、会社員[技術系]）」「何が起こっているかを把握するため（男性、20 代、学生）」「金融機関も完全ではないので、自己責任も必要（女性、60 代、無職）」等でした。

「必要ない（6.4%）」「どちらかと言えば必要ない（7.6%）」と答えた人は、合わせて 14.0%。その理由は「難しい言葉を並べて警告されるより、手順をわかりやすくして強制的にできるほうがいい（女性、20 代、パート・アルバイト）」「お年寄りが対応できないから（男性、30 代、自営業）」「パソコン操作に詳しくないので面倒（女性、50 代、その他）」「知識のない人に操作をさせるようなソフトでは効果が期待できない（男性、50 代、会社員[技術系]）」等でした。

「どちらでもない（35.5%）」と回答した人も 3 割以上おり、「本当は必要なのかもしれないが、判断が難しい（女性、50 代、パート・アルバイト）」「利用者自らが判断することに限界があるように思える（女性、40 代、会社員[事務系]）」「よくわからない（男性、30 代、会社員[事務系]）」「金融機関が対策すべき（女性、60 代、パート・アルバイト）」といった理由が挙がりました。

警告内容を判断し、対応するのは自己責任と考える利用者が多く見られる反面、金融機関が提供している無償のセキュリティ対策ソフトの警告やその対応方法がすべての利用者とってわかりやすいものになっておらず、利用者による判断や操作が難しい場合があることや、セキュリティ対策を金融機関に依存したいと考える利用者もいることが明らかになりました。

Q.現在、金融機関から提供されている無償のセキュリティ対策ソフトは、多くの場合、インターネットバンキング利用者がセキュリティ対策ソフトの出す警告の内容を判断して操作する必要がありますが、利用者が自らそういった判断や操作をすることの必要性についてどのようにお考えですか。その理由も合わせてお答えください。(n=420)



◆インターネットバンキングの利用にあたって、金融機関のセキュリティ対策に今後期待することは
セキュリティの強化、利用者に依存しないセキュリティ対策、必要に応じた適切な情報提供、不正利用による被害の補償

インターネットバンキングの利用にあたって、金融機関のセキュリティ対策に今後期待することを質問すると、「セキュリティの強化」や「利用者に依存しないセキュリティ対策」、「必要に応じた適切な情報提供」「不正利用による被害の補償」等の意見が挙がりました。

・セキュリティの強化

「最新のセキュリティ対策を必ず実施してほしい（男性、60 代、無職）」「不正送金を発生前にブロックしてほしい（女性、50 代、パート・アルバイト）」「本人確認の強化（女性、40 代、会社員（事務系））」「指紋認証の導入（男性、30 代、公務員）」「認証発信端末を固定化（複数台）してほしい。登録端末以外からの依頼は実施しない、もしくは電話やメールで確認するようにしては（男性、60 代、無職）」等

・利用者に依存しないセキュリティ対策

「個人の端末にセキュリティ対策するのは当然だが、金融機関も十分な対策を実施してほしい（男性、60 代、無職）」「利用者が対応するのではなく、金融機関側が対策をして利用者が安全に利用できる環境を提供するのが当たり前（女性、30 代、会社員（事務系））」等

・必要に応じた適切な情報提供

「注意勧告だけでなく、被害状況も示して脅威を実感できるようにしてほしい（50 代、女性、専業主婦）」「不正に関する情報や対策をすばやく発信してほしい（女性、60 代、パート・アルバイト）」「広報活動をもっとわかりやすく、大々的にすべき（女性、30 代、その他）」等

・不正利用による被害の補償

「被害を受けた場合、補償してほしい（女性、60 代、自営業）」「不正利用された場合の補償内容や手続き手順などを Web サイトで詳しく説明してほしい（女性、20 代、専業主婦）」等

・その他

「これ以上利便性が落ちるセキュリティ対策なら不要。個人的にはスキミングのほうが怖い（男性、50 代、公務員）」「セキュリティ対策を進めるとログインの簡便さがなくなるのでバランスをとってほしい（女性、30 代、パート・アルバイト）」「利用者にはずっと無料でセキュリティ対策をしてほしい（男性、50 代、会社員[その他]）」等

◎インターネットバンキングのセキュリティは、金融機関と利用者が一体となって、はじめて実現されるもの　～利用者側の対策は必要だが、利用者のリテラシーに依存する対策では不十分～

インターネットバンキングの普及により、インターネットバンキングが攻撃者にとって魅力的な攻撃対象となり、攻撃手法が進化し続けていることから、不正送金等のインターネットバンキングの犯罪被害は拡大傾向にありますが、今回の調査では「インターネットバンキングを選定する際のポイント」として、「手数料の安さ」に次いで「セキュリティ対策の充実」を挙げた人が多いことなどから、金融機関や関係省庁、セキュリティ関連団体等による注意喚起により、インターネットバンキングを利用する際のセキュリティへの意識の高さがうかがえました。

その一方で、「利用履歴やサイトの真正性の確認」、「金融機関から無償で提供されているセキュリティ対策ソフトの利用」等を積極的に行う利用者は、まだ少ないことがわかりました。

金融機関から無償で提供されているセキュリティ対策ソフトを利用しない理由として、「既に別のセキュリティ対策ソフトをインストールしているため必要ない」と判断する人が約 3 割でしたが、不正送金の原因の一つであるMITB（Man in the Browser）攻撃※1を仕掛けるためのマルウェアを作成するツールが、アンダーグラウンドマーケットで流通しており、攻撃者が日々無数の亜種を生成している現在、市販のセキュリティ対策製品による対応が追い付かず、被害が拡大しています。また、フィッシング攻撃と違って、MITB 攻撃では利用者がアクセスしているのは正規のインターネットバンキングサイトであり、サーバー証明書などでサイトの真正性を確認しても意味がありません。さらに、MITB 攻撃では、利用者が正規の認証プロセスを経てログインした後に Web ブラウザを不正に操ることが可能となるため、ユーザー認証を強化する対策も役に立たないのが現状です。

インターネットバンキングシステムを攻撃対象とした場合、攻撃者の観点から最も攻略しやすいのは、強固なセキュリティ対策が施された金融機関側の環境ではなく、金融機関と比較して脆弱な利用者側の環境です。MITB 攻撃のような利用者を狙った攻撃の場合、金融機関側のシステムを強固にするだけでは対策が難しく、利用者側での対策も必要となります。

※1　マルウェアが Web ブラウザを乗っ取り、利用者がインターネットバンキングサイトにアクセスする際にマルウェアが Web 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したりすること。SpyEye や Zeus などのバンキングマルウェアの多くに MITB 攻撃の機能が実装されています。

FFRI では、従来のセキュリティ対策の弱点を巧妙に狙った MITB 攻撃に対しては、その対策に特化したソリューションが必要と考えています。また、今回の調査では、様々な理由により、金融機関が提供するセキュリティ対策製品を利用していない利用者が多数存在していることがわかりましたが、利用者の知識やリテラシーに依存しない対策が必要とも考えています。その発想から生まれたのが、MITB（Man in the Browser）攻撃対策製品「FFRI Limosa」（http://www.ffri.jp/products/limosa/index.htm）です。「FFRI Limosa」は、MITB 攻撃の対象である Web ブラウザを堅牢化するためのソリューションです。利用者がインターネットバンキングサイトにアクセスし、ログインする際にサイトからセキュアモジュール（FFRI Limosa）がダウンロードされ、自動的に Web ブラウザに適用されるため、利用者がほとんど意識することなく、Web ブラウザを堅牢化します。「FFRI Limosa」が、Web ブラウザに干渉するための入口を塞ぐことによって、仮に利用者の PC 端末がマルウェアに感染していても、マルウェアによる Web ブラウザへの介入を防御し、安全なブラウジング環境を保護します。

FFRI では、インターネットバンキングをより安心・安全に利用していただけるよう、今後も攻撃者の思考を先読みし、サイバーセキュリティ上の未知の脅威に対抗するプロアクティブな研究開発体制を強化してまいります。

■株式会社 FFRI について

当社は 2007 年、日本において世界トップレベルのセキュリティリサーチチームを作り、IT 社会に貢献すべく設立されました。現在では日々進化しているサイバー攻撃技術を独自の視点で分析し、日本国内で対策技術の研究開発に取り組んでいます。研究内容は国際的なセキュリティカンファレンスで継続的に発表し、海外でも高い評価を受けておりますが、これらの研究から得られた知見やノウハウを製品やサービスとしてお客様にご提供しています。主力製品となる、「FFR yarai」はミック経済研究所調べ※2による エンドポイント型標的型攻撃対策分野における出荷金額において No.1 を獲得しております。

※2　出典:「情報セキュリティソリューション市場の現状と将来展望 2013【外部攻撃防御型ソリューション編】」

本件に関するお問い合わせ先
写真・資料等がご入用の場合もお問い合わせください。
株式会社 FFRI
コーポレートコミュニケーション部　PR 担当
TEL:03-6277-1811
E-Mail:pr@ffri.jp　　URL:http://www.ffri.jp