2014 年 04 月 14 日

インターネットバンキングを悪用した不正送金への注意喚起

株式会社ラック
株式会社セキュアブレイン

多くの商取引がインターネットで決済されることが日常化し、お金と物の流れが変わりつつあります。情報セキュリティ業界では、ネットワークや機器の信頼性の向上、個人情報や機密情報の保護、コンピュータウイルスなど悪質なソフトの発見と対処といった様々な課題に対して、協力し対策を進めてまいりました。また、政府をはじめとした関連機関の多くも、利用者やサービス提供者に対して啓発を重ねてきたこともあり、日本ではインターネットサービスの普及度合いに比べ、ウイルス対策ソフトが浸透し、実際のサイバー事故の被害発生は、他国と比べても低く抑えられているといえます。

しかしながら、情報セキュリティ関係者の多くが警鐘を鳴らしてきた、他国で大きな脅威となっているインターネットバンキングでの不正送金による、銀行口座から預金が盗み取られる犯罪が、日本国内でも大きな問題になる危険性が高まっています。急速に拡大した日本のインターネットバンキングにおける利用者の理解と自己防衛意識は低く、日本の金融機関が狙われていることからも被害拡大が懸念されます。

昨年より、ラックの緊急対応チーム『サイバー救急センター』には、銀行口座から預金情報（現金）を窃取する、いわゆる不正送金被害に関する技術調査の依頼が急増しています。また、ラックと他のセキュリティ企業の共同研究の枠組みであるサイバー・グリッド・ジャパンに参加するセキュアブレインで把握している、インターネットバンキング利用者の不正送金対策の状況は、金融機関が様々な対策を打ち出しているにも関わらず、必ずしも十分ではないことを示しています。私たちは、昨今のインターネットバンキングに関連する被害の抑制には、サービス提供者側の対策だけでは不十分であり、利用者側の理解と具体的な対策の実施が必要だと考えています。

そのため、ラックとセキュアブレインは、インターネットバンキングに関連した対策の必要性を訴えるとともに、効果的な対策を広く呼びかけています。

不正送金が行われる仕組み

不正送金というと、犯罪者が銀行に対して悪の手を伸ばし、私たちの知らないところで預金データが操作されている、と理解されているのではないでしょうか。しかし、不正送金被害は、金融機関がハッカーに侵入されて起きているわけではありません。預金者が利用しているパソコンがウイルスに感染し、パスワードなどを含む口座情報などがそのパソコンから盗み出されることにより発生しています。つまり、不正送金による被害をなくすためには、インターネットバンキング利用者自身が危険を正しく理解し、自己防衛意識を持って自分のパソコンの必要最低限の用心をすることが重要となります。

不正送金被害の原因となる口座情報の盗み出しは、主に以下の二つの方法で行われています。

１．【フィッシング】 利用者が、本物とは違う偽物のインターネットバンキングサイトに誘導され、そこで入力された預金口座パスワード等の情報が盗まれ悪用される
２．【不正送金ウイルス】 利用者のパソコンが、その手のウイルスに感染し、預金口座の情報が盗まれ悪用される

いずれの手法においても、インターネットバンキング利用者のアカウント情報（サイトにログインするための情報と送金用のパスワード情報など）が、犯罪者の手に渡ってしまうことが被害に遭遇する始まりです。銀行のアカウント情報が盗まれるということは、銀行通帳と銀行印が盗られたことと同じで、不正送金を止めるのは至難の業となります。通帳と印鑑の場合は、その旨、銀行に知

らせて不正を防ぐ処置をとりますが、アカウント情報の場合、盗られたことに気付くことも困難です。

特に、昨今問題になっているのが、「ゼットボット」や「スパイアイ」などの不正送金ウイルスと呼ばれる銀行口座の情報を盗み取るために組織的に開発されているウイルスです。犯罪者は、このような高度な不正送金ウイルス作成ソフトを開発組織から購入し、銀行ごとに特化したウイルスを作成します。このソフトが出回っていることで、日本の大手銀行だけではなく、地方の銀行までが標的となっているのです。加えて、今後、クレジットカード会社や航空会社など、現金化できるポイントやマイルを取り扱う機関にも被害が拡大する危険があります。
不正送金ウイルスに感染すると、本物のインターネットバンキングサイトを閲覧した際に、それを察知して利用者の送金パスワードを含めたアカウント情報を収集する別の画面を本物に混ぜて表示します。利用者が騙されて入力したアカウント情報は、そのまま犯罪者に送られます。さらに昨今の調査においては、ウイルスがもつ遠隔操作機能により、感染したコンピュータの動作が盗み見られたり、銀行とのやり取りメールが操作されたり、送金操作されるなど、犯罪行為が複雑かつ深刻になっています。

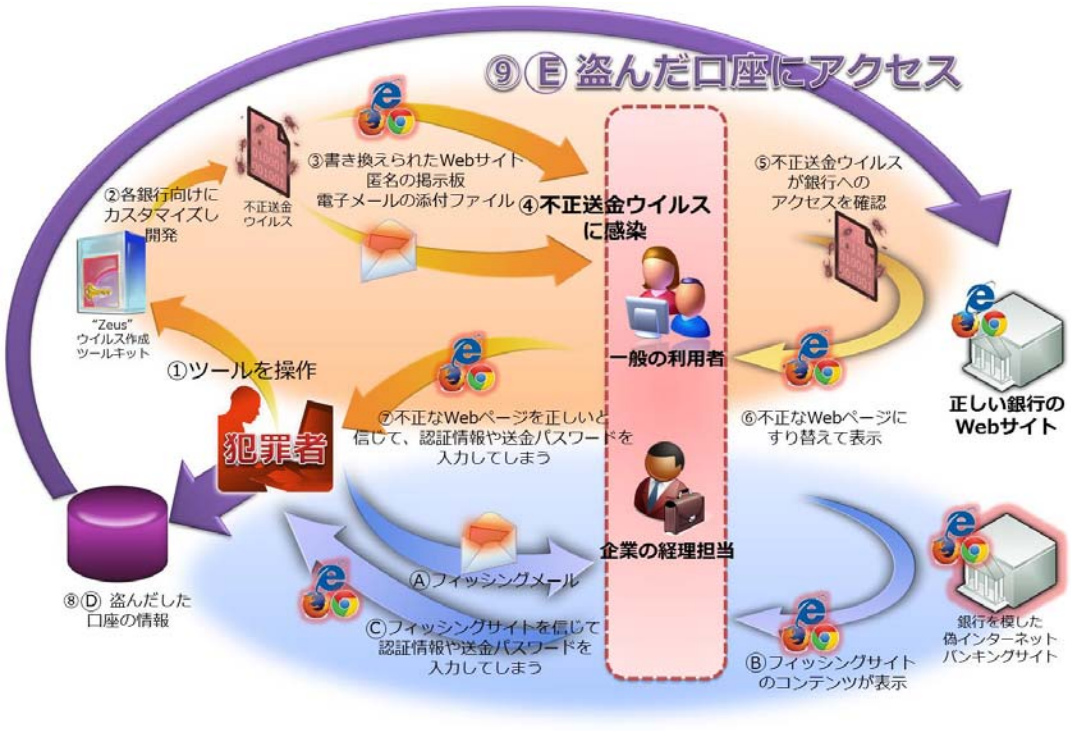


図-1 不正送金にいたる流れ

また、厄介なことに、インターネットバンキングの情報が盗まれた場合でも、すぐに銀行口座から不正送金が行われないことがあります。短いもので数日から数週間、長い場合には 2 か月程度間をあけて犯行を行うため、被害者が油断させられることにより犯罪行為の発見が遅れる場合もあります。

不正送金犯罪の被害を受けるお客様の状況

ラックの緊急対応チーム『サイバー救急センター』が、被害にあった複数のお客様のパソコン環境を調査したところ、すべての環境において不正送金ウイルスの感染が確認され、不正送金ウイルスによる感染被害が急拡大していることを実感しています。

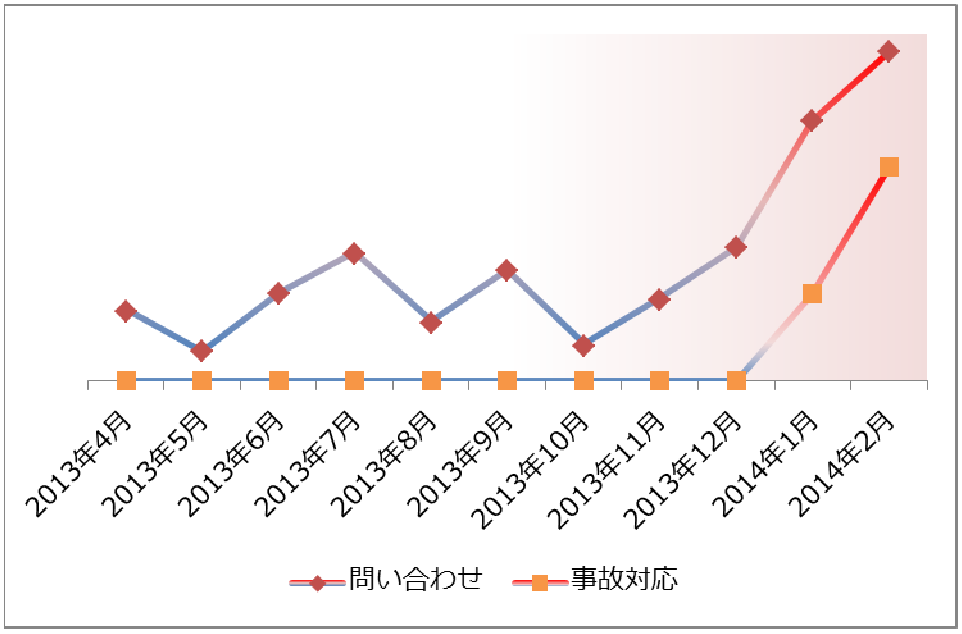


図-2 不正送金に関するラックへの支援要請推移

不正送金ウイルスの感染から、インターネットバンキング利用時でのアカウント情報の窃取、そして実際の不正送金操作までには、時間差があることが多いため、ウイルスにどの時点で感染し、どのような方法で口座情報が盗まれたかを把握するためには、被害にあったパソコンを専門的な解析技術によって調査する必要があります。

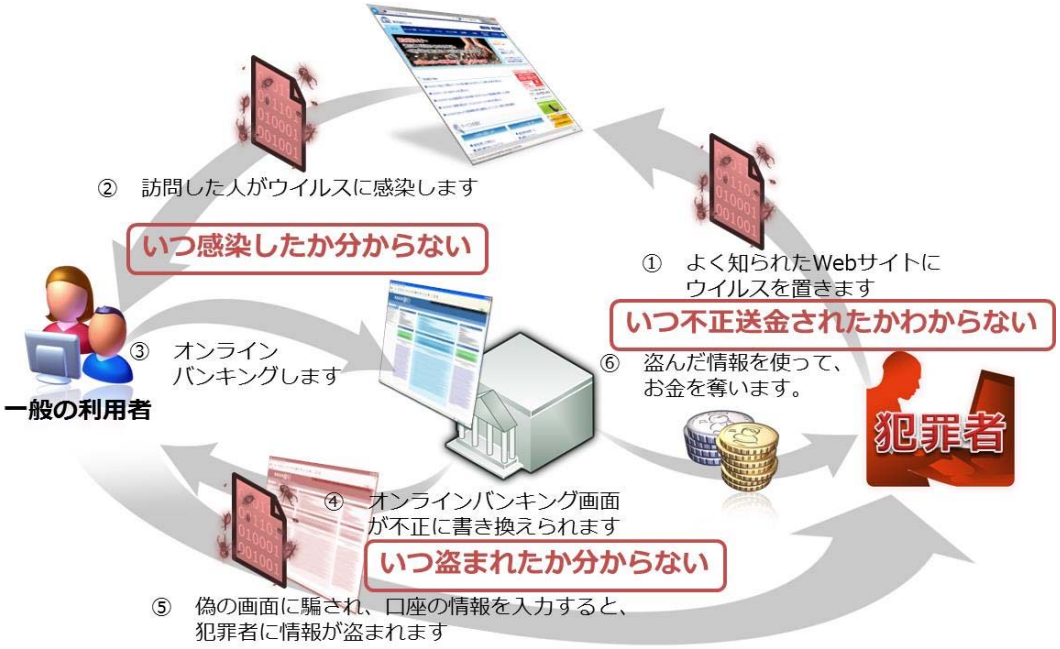


図-3 不正送金ウイルスの難しさ

しかも、不正送金ウイルスが亜種へ変化するペースは非常に速く、ウイルス対策ベンダーがウイルス被害の報告を得て対策用のウイルス定義ファイル（ウイルスの指名手配）を配布できたときには、ウイルスはすでに別の顔で涼しく振舞っていることが大半で、検出できないことがあります。こうしたウイルス対策ソフトによる発見を逃れる仕組みにより、これらの対策が非常に困難になっています。これは、ラックの緊急対応チームが被害企業を調査した際に、最新のウイルス対策ソフトが入っているにもかかわらず、当該ウイルスを検出できずに被害が発生している事例からも確認されています。

セキュアブレインは、国内のインターネットバンキング利用者 250 万人に配布しているフィッシング・不正送金対策ソフト「PhishWall（フィッシュウォール）クライアント」で、不正送金の被害を防いでいます。過去 15 か月間で月平均 2,500 台以上のパソコンが不正送金ウイルスに感染していることが確認されており、特に昨年 11 月には月間の感染被害数が過去最高の 5000 台を超えました。不正送金ウイルスの攻撃を止めたはずのコンピュータで、その後何度も同様の攻撃が発生していることから、ウイルスの駆除が行われていないことが確認されています。これは、ウイルス対策ソフトでウイルスを駆除するなどの対策が行われていないか、ウイルス対策ソフトを過信するなどインターネットバンキング利用者が危険に気づかないという課題があることを意味しています。

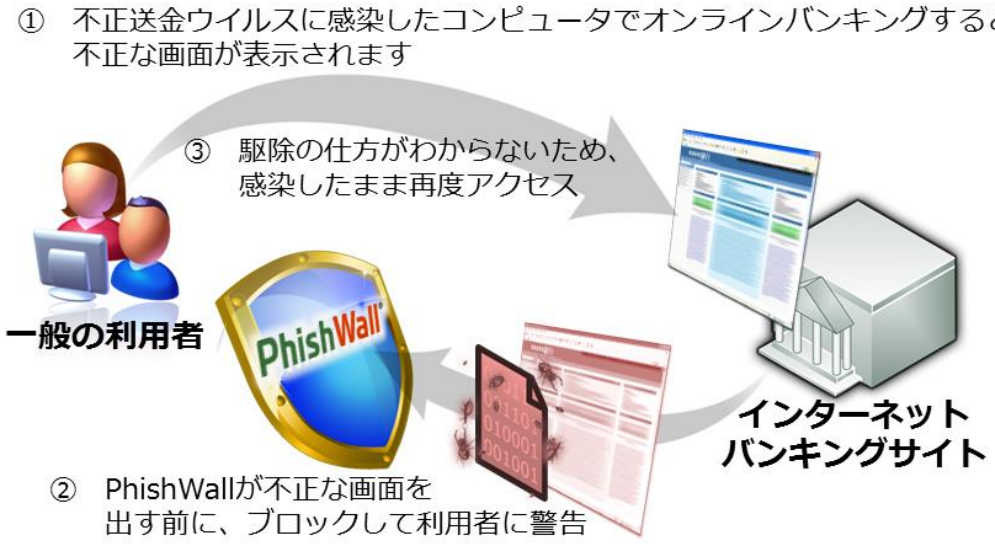


図-4 不正送金対策ソフトの防御と駆除の困難さ

また、被害を受けているのは個人利用者だけではなく、中小企業にも広がっています。比較的小規模の企業においては、経理部門の入出金処理に関して、申請者と承認者による入出金承認プロセスが整備されていないことが大半であり、一人のアカウントが窃取されるだけで、不正送金されてしまいます。企業の預金口座情報が窃取され、不正送金の被害を受けた場合、個人とは異なり、金額も膨大となり、極めて深刻な被害を受ける可能性があります。

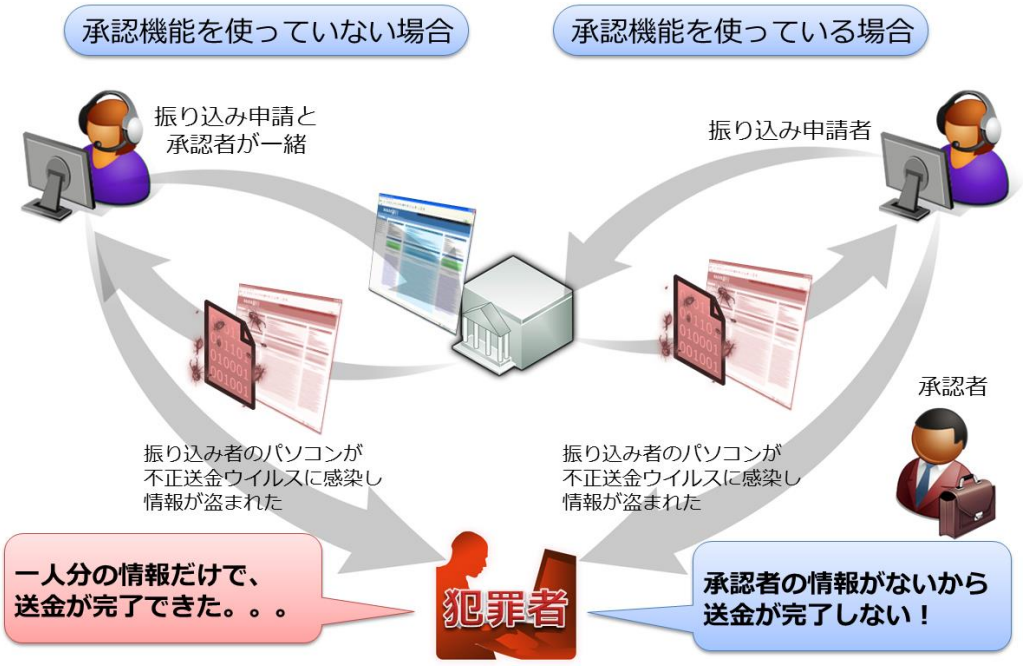


図-5 振り込み承認機能の利用有無の差

ラックおよびセキュアブレインが有している危機感を裏付ける情報が、警察庁、総務省、経済産業省が発表した以下の資料に掲載されております。

平成 26 年 3 月 27 日
不正アクセス行為の発生状況およびアクセス制御機能に関する技術の研究開発の状況
https://www.npa.go.jp/cyber/statics/h25/pdf041.pdf（警察庁）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000072.html（総務省）
http://www.meti.go.jp/press/2013/03/20140327009/20140327009.html（経済産業省）

別紙１：不正アクセス行為の発生状況
http://www.soumu.go.jp/main_content/000280516.pdf

上記資料では、2013 年（平成 25 年）のインターネットバンキングでの不正送金の件数が、前年の 95 件から約 14 倍の 1,325 件に急増したと発表されています。また、3 月 13 日に開催されたシンポジウムでは、警察庁は 2013 年の不正送金被害額は約 14 億円で、過去最悪だったと説明しています。2014 年に入ってからは、1 月と 2 月の 2 か月間だけで 6 億円の被害がすでに発生しており、昨年後半から拡大した被害が継続していることを表しています[i]。被害件数と金額の増加ペースは驚異的であり、今後、より深刻な状況になることが危惧されます。

不正送金犯罪への対策について

すでに数年前より、大手銀行や地方銀行を中心に、不正送金に関する情報開示や対策技術の提供が開始されています。手段や対策に関して積極的な情報公開が行われ、メディアも一体となった周知活動が行われております。しかしながら、不正送金の被害はさらに深刻さを増しており、インターネットバンキング利用者の適切な理解と積極的な参画なしに、対策は進まない状況であると考えています。
ここでは、利用者の意識、技術での対策と、企業がインターネットバンキングを利用する際の留意点について説明いたします。

1.知識を得て、心構えしましょう

まずは、利用者は、インターネットバンキングにまつわる危険と必要な用心は何かをご理解ください。基本的には送金パスワード（第二暗証番号、OTP など）のように極めて重要なパスワードをログイン時に入力させることはありません。また、インターネットバンキング上で「合言葉」の変更を促すこともありません。そういったことが理解できれば、対策を行うこともできます。また、情報は次々変化していきます。積極的に最新情報に触れ、普段から注意を怠らないように努めましょう。

- 常に最新の情報を得ましょう
  犯罪者の手口は日々巧妙化しています。皆様がお使いの銀行のサイトには、わかりやすく最新情報が掲載されています。もちろん、インターネットのニュースサイトで不正送金の話題を見つけたら、ぜひ内容を確認してください。ラックやセキュアブレイン、ウイルス対策ソフトメーカーの Web サイトにも最新の情報が公開されている場合もありますので、それらを確認することも重要です。
  重要なことは、これらの情報は、自分自身が情報に関心を持って取りに行かないと手に入らないということです。すぐ身の回りにある危険についてまずは目を向けてみてください。

- いつもと違いがないかを確認しましょう

インターネットバンキングは、ご自身の口座からの振り込みに利用される場合がほとんどで、頻繁に使う機能ではないかもしれません。そのためどのような画面だったか、どのような操作だったかを忘れてしまうこともありますが、重要なことは利用者が違和感を持つことです。先月の操作と違う、必要以上に情報を入れるように求められたなど、何か気になると思ったら、インターネットバンキングの利用を中断し、金融機関の Web サイトにあるインターネットバンキングの説明ページを見直してください。

特に、送金パスワードや乱数表の確認番号のような重要情報の窃取画面は、本物と同じように作られています。乱数表の内容を全部、もしくはいつもより多い桁数入れるように促された場合など、いったん操作を止めて深呼吸してみてください。例えば、銀行の窓口で行員さんが暗証番号を尋ねることはないのと同じように、乱数表の全てを入力することはあり得ません。

- 利用履歴をこまめに確認しましょう

  インターネットバンキングの利用の有無にかかわらず、週に一度程度は口座の利用履歴をご確認し、異常な変化に気付くことです。口座の情報が窃取された後、しばらくしてから不正送金が行われる場合もありますので、安心はできません。また、ログイン時には前回のログインなどを調査し不審なものがないかを確認しましょう。そして、メールによる送金通知を有効にし、メールの送り先を携帯電話のメールにしてください。

2.技術で守る

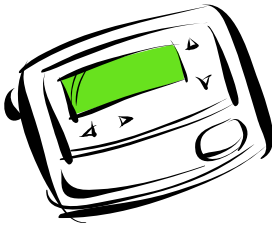
- メールで送られるワンタイムパスワードを使用する

  インターネットバンキングのパスワード（暗証番号）を ATM の暗証番号同様に一度決めた固定の番号にした場合、パスワードが盗まれると犯罪者は自由に口座へアクセスしてしまいます。そのため、インターネットバンキングの利用毎に、パスワードがインターネットバンキングから送られてくるワンタイムパスワード方式を利用することで、多少の手間で安全性を高めることができます。

  最近の不正送金ウイルスはパソコンのメールを盗むことはもちろん、画面そのものを盗み見るような高度な機能まで備えたものもあります。このような状況もあるため、ワンタイムパスワードであっても過信しないようにしてください。携帯電話のメール機能が使える場合は、ワンタイムパスワードのメールを受け取るのを振り込みに使うパソコンでなく、携帯電話のメールに送信する事を強く推奨します。

- トークンによるワンタイムパスワードを利用する

  トークンとは、ワンタイムパスワードを都度作り出す機器です。振り込みや住所変更など重要な操作を行う際に求められる番号を、パソコンとは別の機器が作り出す仕組みを使って安全を確保します。銀行によって、無料で提供されたり、有料で購入する場合がありますが、できるだけ利用したい機能です。



- 不正送金対策ソフトを活用する

  不正送金ウイルスは、インターネット操作を盗み見る Man In The Browser（MITB）と呼ばれる攻撃を仕掛けます。MITB は、インターネットバンキングの利用を検知して様々な情報を奪う画面を利用する画面に表示させ、口座情報を窃取します。この動きを監視するのが、不正送金対策ソフトです。ウイルス対策ソフト同様に、完全に攻撃を検知できるとは限りませんが、ウイルス対策ソフトと併せて使用していただきたい対策技術です。

  不正送金対策ソフトには、セキュアブレインの「PhishWall クライアント」、トラスティア(Trusteer)の「ラポート(Rapport)」、サート(SaAT)の「ネチズン(Netizen)」などが知られています。

お使いのインターネットバンキングサイトが無料で配布している場合もありますので、まずはご確認をお願いします。

▼ セキュアブレイン 「PhishWall クライアント」ダウンロードサイト
http://www.securebrain.co.jp/products/phishwall/install.html

- OS やアプリなどを最新の状況にする

最近の不正送金ウイルスは、電子メールに添付されて感染を広げるだけではなく、正しい Web サーバーの内容を書き換えてウイルスを配布する水飲み場型攻撃も使用されます。これにより Web を閲覧しただけで不正送金ウイルスに感染することがあります。Windows（Internet Explorer)や Java、Adobe Flash、Adobe Reader、Office など、PC にセットアップされているソフトウェアは、必ず最新の状況にアップデートし、犯罪者が付け入る隙をなくしておきましょう。
各 OS やソフトウェアの自動更新機能を使うと、更新の手間を省くことができます。

- ウイルス対策ソフトを活用する

最新のウイルス対策ソフトであっても、日々大量に作成されるコンピュータウイルスを、完全に発見し駆除することは困難です。しかしながら、継続動作させておくことでパソコンに感染したウイルスを発見することがあります。無料のウイルス対策ソフトでも駆除できる場合もありますが、インターネットバンキングを利用するパソコンでは、インターネットバンキングを保護する機能がある有料のウイルス対策ソフトを使用して可能な限り安全な環境を手に入れましょう。
なお、ウイルス対策ソフトを利用していても、ウイルス定義ファイルの契約をしていない方も多くいます。かならず定義ファイルは最新なものを使うようにしてください。

3.仕組みで守る

インターネットバンキングの特徴を理解し、対策技術も導入すると安全性が向上しますが、インターネットバンキングの利用方法を一工夫すると、より安全になります。そして、企業がインターネットバンキングを利用するときには、法人契約向けに提供されている仕組みを使うなど、確実な対策を行いましょう。

- ネットの閲覧やメールの受信と、インターネットバンキングの端末を分ける

ネット閲覧やメール受信など情報端末としてのパソコンは、ウイルス感染の危険にさらされています。例えると、預金通帳と銀行印を持って繁華街に出かけるようなものです。可能であれば、ネット閲覧やメール受信をするパソコンと、インターネットバンキングを行うパソコンを分け、ウイルスやフィッシングといった脅威からできるだけ隔離したインターネットバンキング環境を手に入れましょう。
別のパソコンを用意できない場合は、パソコンのログオンアカウントを新たに追加し、インターネットバンキング専用アカウントで送金処理を行うことも有効です。
また、今は Windows が狙われることが多いので、MacOS や iOS、Android など他の OS を使用することも、有効です。

- 複数人の承認プロセスを設ける

企業でインターネットバンキングを使用する場合、振り込み申請とその承認という二つの処理を分けることで、セキュリティを高めることができます。しかし、小規模な企業の場合、一人の経理担当が振り込みと承認を兼ねて運用されるケースも見受けられます。複数人の承認プロセスを設けることにより、一人が不正送金ウイルスなどにアカウント情報が盗まれても、もう一人が不正送金を防ぐ

こと も可能ですので、承認手順を見直し、守ってください。

- 振込限度額を下げる
  インターネットバンキングの利用開始時は、振り込み限度額が高く設定されていることがあります。必要以上に限度額が高いことで被害が大きくなることがありますので、通常行う振り込み金額にあわせて、限度額の設定を見直してください。

以上

---

[i]不正送金被害が過去最悪ペース、2014 年 2 月までに 6 億円の被害
http://itpro.nikkeibp.co.jp/article/NEWS/20140314/543828/

株式会社ラックについて

ラックは、1986 年にシステム開発事業で創業、1995 年にいち早くセキュリティ事業を開始。2012 年 4 月にグループの合併により、株式会社ラックとして新たにスタート。サイバーセキュリティ分野のリーディングカンパニーとして、豊富な実績を誇る「脆弱性診断サービス」、日本最大級の「セキュリティ監視センターJSOC」による 24 時間 365 日のセキュリティ監視・分析サービス、情報漏えい事故などの緊急対応・支援をする「サイバー119」の提供をはじめ、金融機関向け基盤システム開発で培った「システム開発」など、官公庁・企業・団体等のお客様に IT トータルソリューションサービスを提供しています。

セキュアブレインについて：

株式会社セキュアブレインは、インターネット上の脅威が多様化する中、Web サービスを提供する事業者や企業に IT セキュリティを届ける、サイバーセキュリティ専門会社です。「より快適で安心できるネットワーク社会を実現するために、一歩進んだ技術で貢献する」というビジョンのもと、信頼性の高いセキュリティ情報と高品質なセキュリティ製品・サービスを提供する、日本発のセキュリティの専門企業です。詳細は、http://www.securebrain.co.jp をご覧ください。

【報道機関からのお問い合わせ先】

株式会社ラック　広報担当
Tel: 03-6757-0130　E-mail: pr@lac.co.jp

株式会社セキュアブレイン 広報担当：丸山　芳生（まるやま　よしお）
e-mail：info@securebrain.co.jp　　電話：03-3234-3001、FAX：03-3234-3002
〒102-0083　東京都千代田区麹町 2-6-7 麹町 RK ビル 4F