インターネットを利用する皆様に

インターネット利用における基本的なウイルス対策の実施のお願い

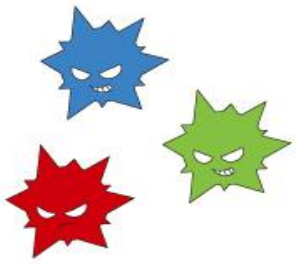
最近、ネットバンキングへのアクセスの際に入力したＩＤ・パスワードが第三者に不正に取得され、これらのＩＤ・パスワードを不正に利用し、他人名義の銀行口座へ不正送金を行う不正アクセス事案が多発しています。現時点の被害総額は、すでに昨年の一年間を上回っており※、深刻な状況です。

※　平成 25 年 1 月～7 月末現在の被害状況　398 件、被害総額約 3 億 6,000 万円（平成 24 年　被害総額　約 4,800 万円、平成 23 年　被害総額　約 3 億 800 万円）

また、ネットバンキング以外でも、複数のインターネットサービスにおいて、いわゆるリスト型攻撃による不正ログインが多発しています。

このような不正アクセスは、パソコン等のウイルス感染等が原因となっていることが多いことから、未然の被害防止のため、インターネットを利用する皆さま方において、基本的なウイルス対策や適切なＩＤ・パスワード管理を徹底していただくことが必要です。

特にお盆や夏休み明けにインターネットを利用する場合には、パソコン等のウイルス感染等の被害に遭う可能性が高いことから、最低限実施していただきたい基本的なウイルス対策、ＩＤ・パスワード管理のポイントについて、ご紹介します。



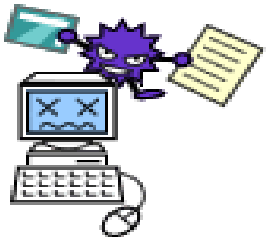
１．ウイルス対策

（１）ウイルス感染のリスク

「ウイルス」とは、コンピュータに何らかの不正な動作をさせるプログラムです。

現在のウイルスの多くは、感染してもコンピュータ自体は正常に動作しているように見えているため、利用者が感染に気付きにくいものになってきています。それは現在のウイルスが次のような目的を持っており、可能な限り利用者に気付かれないように動作するからです。

●個人情報を盗み出す



感染したウイルスにより、コンピュータ上に保存されている情報（データ）が勝手に送信されたり、キーボード入力を盗み見されたりすること等をいいます。最近のネットバンキングの不正送金もこのカテゴリーに含まれます。これ以外にも、以下のような被害を受ける可能性があります。

- 盗まれたクレジットカード情報で勝手に買い物をされる
- 盗まれたオークションサイトの ID とパスワードがオークション詐欺に悪用される
- 盗まれた ID・パスワードが別のサイトでの詐欺に悪用される
- 自分のふりをして勝手にオンライントレード（株の売買など）が行われる
- 自分のメールソフトに保存されたメールアドレスが流出することでメールをやり取りしている友人などが迷惑メールの送付対象になる
- 自分のホームページが改ざんされて閲覧者にウイルスを感染させる「危険なホームページ」にされてしまう、など

●第三者への攻撃の踏み台にする

「踏み台」とは、気づかないうちに不正侵入されて乗っ取られ、他サイトへの侵入や攻撃、迷惑メール配信の中継地点に利用されているコンピュータをいいます。踏み台に使われると、知らない間にあなたのパソコンが様々な犯罪に利用され、結果としてあなたが捜査の対象となる可能性があります。場合によっては、管理責任を問われる可能性もあります。

（２）ウイルス感染が疑われる症状・事象

最近のウイルスには、画面表示が崩れたり、コンピュータが起動しなくなったりといった目に見える「わかりやすい」症状を見せるものはほとんどありません。そのため、パソコン利用者が感染に気付きにくくなっています。

それでも次のような動作が見られた場合は、ウイルスに感染している可能性があります。

●動作が遅くなる

●タスクマネージャの CPU 使用率が勝手に上下し続ける

●マウスをクリックしていないのにクリック音がする､等

（３）ウイルス感染を確認するチェックリスト

以下の項目のうち 1 つでも当てはまる場合にはウイルス感染の可能性は極めて高いといえます。

●メーカーのサポートの切れた古い OS を使っている。

・Windows 98, 98SE, ME, 2000 は不可

・Windows XP は SP3 に、Windows Vista は SP2 に、Windows 7 は SP1 に更新する必要あり

●Windows Update を実行したことがない、または Windows Update を知らない。

●自動更新の設定になっていない、または設定できない。

●ウイルス対策ソフトを導入していない。

●ウイルス対策ソフトのウイルス定義ファイル（パターンファイル）を更新していない。

●古いブラウザを使っている。

・Internet Explorer6, Firefox 2.x など

上記はあくまで最低限の項目を列挙したものであり、これらの項目のいずれにも当てはまらなくても、100%安全な状態であるとは限らないことに注意が必要です。

（４）ウイルス感染の対策

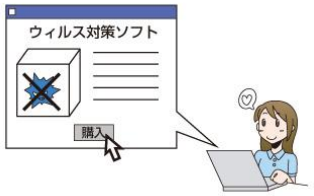
手順１　対策必要物品の確認と環境整備

１－１　メモリの確認と増設

パソコンの搭載メモリが少ない状態で、本手順の対策を実施するとメモリ容量の不足によりパソコンの動作が急激に遅くなります。

搭載メモリ容量の確認を行い、足りない場合は購入しメモリの増設を行いましょう。

１－２　ウイルス対策ソフトの確認と購入



ウイルスからパソコンを守るためには、ウイルス対策ソフトを導入（インストール）し常時保護を行う必要があります。

ウイルス対策ソフトが導入されているか、更新期限が過ぎていないかを確認し、不備がある場合は、事前に準備しましょう。

手順２　駆除前の準備

２－１　データのバックアップ

感染しているパソコンにおいては、希に駆除および対策の途中でシステムが起動しなくなる場合があります。起動しなくなった場合は、Cドライブの内容を一旦消去し Windows のシステムを入れ直すリカバリが必要になりますので、必要な方はデータのバックアップを行いましょう。

２－２　Windows ファイアウォールの設定

駆除を行っている途中での再感染を防ぐために、外部からの感染攻撃について、Windows ファイアウォールを使い遮断します。特に、3G無線機器でインターネット接続を行っている方は、ブロードバンドルータによる保護が困難であることから、Windows ファイアウォールで守ることが特に重要になります。

Windows OS 名、バージョンにより方法が異なりますので、バージョンを確認の上、Windows ファイアウォールの設定を行いましょう。

手順３　ウイルス駆除

３－１　Windows Update

ソフトウェアのアップデートを
知らせるアイコンとメッセージ

Windows Update を行い、ウイルスの感染源の一つであるセキュリティホール(ぜい弱性)の修正を行いましょう。

Windows Update については､以下のアドレスにアクセスすることで、インストールが可能です。

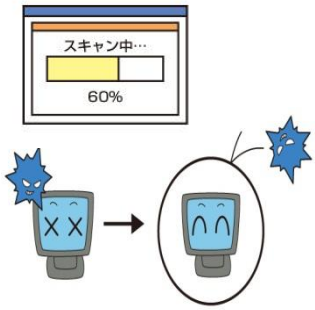
- Microsoft 公式サイト：http://update.microsoft.com/
- OS ごとの詳細な Windows Update 手順：

http://www.microsoft.com/ja-jp/security/pc-security/j_musteps.aspx

３－２　ウイルス対策ソフトの導入と駆除

インターネット上の様々な危険からあなたのパソコンを守るためには、ウイルス対策ソフトを導入（インストール）し、常時保護することが重要です。

導入（インストール）していない方は必ず導入してください。



手順４　今後の感染の脅威から身を守るために

４－１　ウイルス対策ソフトの定期的な更新

ウイルス対策ソフトは、購入すればずっと同じように使い続けられる訳ではありません。常に新しい種類のウイルスが発見されており、新種のウイルスに対応するためには、ウイルス対策ソフトのホームページから定期的にウイルスを発見するための定義ファイル（ウイルスパターンファイル）をダウンロードして更新する必要があります。任意に更新を行い、最新の状態になっていることを更新日等で確認してください。

４－２　ＯＳ、ソフトウェアの定期的な更新

コンピュータ上で動くＯＳやソフトウェアは、セキュリティホール（ぜい弱性）が含まれている可能性が常に存在します。多くのウイルスは、修正プログラムが提供されているぜい弱性を悪用しており、既存の修正プログラムを全て適用するだけでも、感染の危険性は低減します。

また、メーカーのサポート期限切れのソフトウェアは、修正プログラムが提供されなくなっており、このようなソフトウェアを使い続けることはウイルス感染の危険を高めます。

４－３　不審なホームページやメール、ソフトウェアを開かない

ウイルス感染源は、メールの添付ファイルを開くことで感染するものから、ホームページを閲覧することで感染するもの（「Web 閲覧感染型」）、正規のプログラムに見せかけた悪意のあるプログラムをインストールすることで感染するものまで多岐に渡ります。ウイルスの感染源を正しく理解し、不審なホームページやメール、ソフトウェアを開かないことが重要です。

Web 閲覧感染型については、正規のホームページを閲覧していたとしても、ホームページが改ざんされ、ウイルスへのリンクが埋め込まれている場合には、ホームページを閲覧するだけでウイルスに感染することがあります。これらの多くはプログラムのセキュリティホール（ぜい弱性）を悪用したものであり、Web 閲覧感染型ウイルスに利用されるプログラム（Adobe Reader、Adobe Flash Player、JRE、Microsoft Office 等）のバージョンを確認し、アップデートを行うことが有効です。

独立行政法人情報処理推進機構（IPA）では、パソコンにインストールされているプログラムのバージョンが最新のものであるか確認できるツール（MyJVN バージョンチェッカ）を提供しておりますので、必要に応じてご参照ください。

- MyJVN バージョンチェッカインストールサイト：
  http://jvndb.jvn.jp/apis/myjvn/vccheck.html

また、このほか、警視庁も、ネットバンキングに係る不正アクセス被害の防止対策について周知しておりますので、以下のサイトをご参照ください。

http://www.keishicho.metro.tokyo.jp/haiteku/haiteku/haiteku428.htm

２．ＩＤ・パスワード管理

（１）複数のサービスでＩＤ・パスワードを使い回すリスク

最近、ソーシャル・ネットワーク・サービス（ＳＮＳ）やフリーメールサービス、クラウドサービスなど様々なインターネットサービスが普及して暮らしが便利になる一方で、複数のサービスで同じＩＤ・パスワードの使い回しが行われている実態が指摘されています。

複数のサービスで同じＩＤ・パスワードを使うことは、ＩＤ・パスワードを忘れてサービスが利用できなくなる可能性を低くしますが、使用しているＩＤ・パスワードがひとたび盗まれてしまうと、**そのＩＤ・パスワードによって他のサービスも不正に利用されるリスクや、サービスに登録されている個人情報等が盗まれてしまうリスク**が高まります。例えば、他社のインターネットサービスのＩＤ・パスワードが別のサイトで不正に利用されたために、記憶にない商品の購入やサービス利用の請求が届くことも考えられます。

（２）ＩＤ・パスワード管理のポイント

このような被害から身を守るためには、ＩＤ・パスワードが盗まれた際のリスクを認識し、**守りたい情報の重要度に合わせて、適切な管理を心がける**必要があります。例えば、クレジットカード情報などが登録されているサービスについては、特に異なるＩＤ・パスワードを使うようにするなどが考えられます。

情報セキュリティに関するキャッチフレーズ

「知る・守る・続ける」

このほか、詳細な情報セキュリティ対策に関する情報は、以下のサイトをご参照ください。

総務省「国民のための情報セキュリティサイト」

http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/