IT サービス&サポート Safemode
セーフモード　ITサービス＆サポート・PC修理・データ復旧 他
http://safemode.jp/
〒326-0844 栃木県足利市鹿島町125-1-216
TEL：080-6792-6169　E-mail ：info@safemode.jp

PCセキュリティ診断サービスのご紹介

改訂日: 2014年5月23日（サービス内容・料金は予告なく改訂される場合があります。）

■PCセキュリティにご不安がある際にご利用いただける、PCセキュリティ状態の診断サービスです。

インターネットに接続されているPCは、一般社会と同じように様々なリスクに曝されています。

セキュリティ対策をしっかりとしないと、下記のような様々なトラブルが発生する可能性があります。

・大切なデータが壊されたり、漏えいしたりする。
・クレジットカードの情報が盗まれ、悪用される。
・IDやパスワードが盗まれ、振込等、様々に悪用される。
・メールが勝手に送信される。
・PCの動作がおかしくなる。変な画面が表示される。
等

インターネットに接続しているPCのセキュリティ状態にご不安がある場合、専門技術者によるPCセキュリティ診断を受けることができます。

PCセキュリティ診断では、PCセキュリティに関する各項目について現状を診断した上、診断結果に基づいて必要な対策や注意点を明確にします。診断終了時、「PCセキュリティ診断書」を提出させていただきます。

■PCセキュリティ診断内容と診断料金 → ■PCセキュリティ対策内容と料金

診断結果から、技術者によるセキュリティ対策作業をご要望の場合

PCセキュリティ診断（標準項目）

診断料：**4,000円**(PC1台当り、税抜、出張費別)

診断項目	チェックポイント
ウィルス対策の状況	1.ホームページ閲覧時のウィルス対策 2.ウィルス対策ソフトの有無 2が有の場合→下記項目を診断 3.ウィルス定義ファイル更新状況 4.定期的なウィルススキャンの実施状況
スパイウェア対策の状況	対策の有無
Windows更新状況	自動更新の設定状況/更新状況
ソフトウェア更新状況	ウィルスに狙われやすいソフトについて確認 1.Java 2.Acrobat Reader 3.Flash　4.Office
不正侵入対策の状況	1.Windowsログインパスワード 2..遠隔操作ソフトの有無

PCセキュリティ対策　項目別料金

項目	料金(税抜)
ウィルスチェック	6000円～ ウィルス対策ソフトの有無/データ量等によって異なります
ウィルスチェックと駆除(ウィルス対策ソフトで駆除できる範囲)	12,000円～ ウィルス対策ソフトの有無/データ量等によって異なります。
特定ウィルス/スパイウェア等駆除	8,000円～ 駆除の技術難易度によって異なります0
スパイウェア対策導入一式	5,000円
ブラウザのセキュリティ設定変更	2,000円/ブラウザ毎
Windows更新等設定修正	1,000円/1設定につき
ソフトウェア更新設定修正	2,000円/ 1ソフトウェア
外部侵入経路(ポート)対策(ルーター設定)	5,000円～円 ルーター機種/設定状況等によって異なります。
上記項目外技術作業およびセキュリティ対策説明等	4,000円/30分

典型的なケースの対策料金例）
ブラウザ1種類のセキュリティ設定変更、Windowsの設定変更1箇所、ソフトウェア更新設定変更1箇所および項目外作業(30分以内)で、計9,000円+税

PCセキュリティ診断内容

診断項目	チェックポイント	説明
ウィルス対策の状況	1.ホームページ閲覧時のウィルス対策 2.ウィルス対策ソフトの有無 2が有の場合→下記項目を診断 3.ウィルス定義ファイル更新状況 4.定期的なウィルススキャンの実施状況	1.ブラウザ(ホームページを閲覧するためのソフト)の設定によっては、ウィルスを仕掛けているホームページを閲覧しただけで、ウィルスが侵入する可能性があります。 2.ウィルス対策ソフトによって機能や性能が異なりますが、ウィルス対策ソフトが無いという状況は最悪です。ウィルス対策ソフトを名乗るウィルスソフトも存在するので、選択が大切です。 【ご参考までに】弊社が評価したウィルス対策ソフト(各々特徴が違います) 技術的に最優秀と思うのは「カスペルスキー」、但し一般ユーザーには設定が難しいかもしれません。無難なところで、「ノートン」、「ウィルスバスター」です。動作の軽さでは「ESET」→遅いPCにお奨めです。以上、有料ソフトです。無料ウィルス対策ソフトのお奨めは「Microsoft Security Essentials」です。但し、Windows 10には「Windows defender」というウィルス・スパイウェア対策ソフトが(2014年1月現在)標準で付いてます。Windows 7にも「defender」が標準でありますが、これはスパイウェア対策機能のみなので、ウィルス対策ソフトを別途導入する必要性があります。 3.「ウィルス定義ファイル」とは、ウィルス対策ソフト会社で今までに発見・登録されたウィルスを検出または駆除するための情報データベースです。ウィルス定義ファイルに登録されていないウィルスは検出も駆除もできません。従って、ウィルス定義ファイルを(自動更新設定等で)最新にしておく必要があります。クラウド型のウィルス対策ソフトでは、PC側でのウィルス定義ファイルの更新は不要です。 4.ウィルス対策ソフトはウィルス侵入時に検知する場合もありますが、必ずしも侵入時に検知できるものではありません。侵入時に検知できなかったウィルス (ウィルス定義ファイルにあるウィルス)については、(定期的な自動)ウィルススキャンが行われる必要性があります。
スパイウェア対策の状況	対策の有無	スパイウェアとは、PCユーザーの操作内容(クリックした箇所やキーボード入力等の情報)や個人情報などを収集したりするソフトのことをいいます。スパイウェアがPCから得て外部に送信されたデータは、スパイウェアの作成元に送られています。 スパイウェアが行う活動の内容は、実は無料ソフト等のインストール時に表示される利用条件の中に書かれている事が多いため、インストール時にその利用条件を承諾してしまっている以上、スパイウェアの活動は直ちに違法と言えるものではないかもしれません。しかし、利用条件をまともに読む人はほとんどいないため、ほとんどのユーザはスパイウェアに気づかず、スパイウェアごとソフトをインストールしてしまう事が多いのが実態です。
Windows更新状況	自動更新の設定状況/ 更新状況	WindowsはPCを扱うための各種基本ソフトウェアの大規模集合体です。ソフトウェアは人間が作成するので、大規模になるとどうしても欠陥がつきまといます。それらの欠陥が発見される都度、修正のために「更新」されます。ウィルス作成者(ハッカー)は、このような欠陥を攻撃する場合が多いので、「更新」は「自動」で行われるようにする事が一番です。PCの環境が変わるような大幅な更新では、更新後の環境では実行できなくなるソフトがある可能性もあるので、PCユーザーに更新するかどうか判断を求めるウィンドウが表示される場合もあります(例えば、新しいWindows Service Pack導入時やInternet Exprolerバージョン更新時等)。大変とは思いますが、このようなウィンドウの表示内容は良く確かめて、「はい」、「いいえ」を適切に判断する必要があります。
ソフトウェア更新状況	ハッカーに狙われやすいソフトについて確認 1.Java 2.AcrobatReader 3.Flash 4.Office	ハッカーは、量的効果を高めるために広く使われているソフトを仕掛けの対象として狙うことが多いものです。従って、WindowsやAndroid(タブレット、スマートフォン)、iOS(iPhone、iPad)等がよく対象となります。 Windows上で多くの方がお使いになっているソフトもその対象となる場合が多いのです。Windows PC上でよく狙われるソフトは、以下の3つです。これらのソフトも「自動更新」されるように設定しておくことが一番です。 Java: ホームページ内のソフトがJavaでつくられていることが多い。 Acrobat Reader PDF文書を表示するための標準的なソフト Flash 絵や文字、写真などが動くホームページを表示するための標準的なソフト
不正侵入対策の状況	1.Windowsログインパスワード 2..外部からの侵入経路の状況(ポート開放状況)	1.Windowsログインパスワードが無ければ、ルーター経由で侵入できたハッカーは比較的簡単にそのPCを乗っ取ることができます。インターネット接続しているPCでは、ログインパスワードを設定しておくのが安全です。ただし、設定したログインパスワードは忘れないでください。PCを使えなくなりますので・・・(実際、忘れてしまったというお客様から緊急のパスワード解除の依頼が多いので・・)。 2.ハッカーは、そのPCへ侵入できそうかどうかを「ポートスキャン」という方法で試す場合が多いのです。この「ポート」というのは、インターネットとPCの間でやり取りする送受信のチャンネル番号的なものです(ポートの番号割り当ては標準化されています。例えば、ホームページ(http)は80番とされています) ハッカーはポートスキャンという方法で、解放されているポートの有無を調べ、不用意に開放しているポートがあれば、そこから侵入を試みることができます。

■付記 「PCセキュリティを守るPC利用の基本」

PCセキュリティを守るのは、一般社会で様々なリスクから身を守るのと同じようです。リスクを知り、リスクに応じた適切な対処を行えば、より安全です。

ダウンロード:特に無料ソフトのダウンロードには注意が必要です。そのソフト自体がウィルスという可能性もありますし、無料ソフトでは、不要・迷惑なソフト(マルウェア)が一緒にダウンロードされる場合がありますので、無料ソフトダウンロード時には途中の画面を注意してよく見る必要があります。

不審なメール: 不審なメールは開封しないようにしましょう。また、知っている方や組織からのメールであっても、添付ファイルを開く際は注意が必要です。場合によっては、ウィルス感染したPCから自動的に送られてきたウィルスメールという可能性もあります。

パスワード: ちゃんと管理して漏えいに気をつけましょう。ハッカーに解析されるリスクを低減するために、できるだけ文字数が多く、数字とアルファベット混在で、かつ辞書にある単語を避けたパスワードにします。たまにパスワードを変更するのが、より安全策です。ご自分のパスワードを忘れないように！

ネット詐欺:よくある事例のひとつとしては、銀行からのメールを装ったもの受信される場合が有ります。パスワードの再確認等の名目で、メール内のお客様情報変更等のホームページアドレスをクリックすると、該当の銀行に酷似したホームページが表示されます。偽のホームページ内でIDやパスワード等を入力すると、その情報が悪用されるリスクがあります。