はじめに

このたびは、「McAfee.com パーソナルファイアウォール Plus」をご利用いただきありがとうございます。
お使いのパソコンでインターネットを利用するときは、ネットワークに接続するため、OSの標準設定では外部から不正接続が可能な状態となります。知らない間にお使いのパソコンに外部から入り込んで勝手な操作をされたり、データを破壊されたりするという被害は、ブロードバンド接続の増加とともに日々深刻度を増しています。そんな外敵による不正アクセスから、お使いのパソコンを守るのがファイアウォールソフトです。「McAfee.com パーソナルファイアウォール Plus」は、難しい設定の必要がなく、インストールするだけで外部からの不正なアクセスからパソコンを守ることができます。また、HackerWatch.orgとの統合や、ビジュアル・トレースの機能によってより的確なハッカー情報を得ることが可能となり、ハッキングの手口をデータベース化することで、多様化する手口に対応できる安心な製品です。
なお「McAfee.com パーソナルファイアウォール Plus」Ver.4.1より、アプリケーションごとの設定ができるようになり、高度な知識がなくても「スパイウェア」や「トロイの木馬」ウイルス対策が簡単に行なえる様になりました。

早速、「McAfee.com パーソナルファイアウォール Plus」でお使いのパソコンに対する不正な接続をシャットアウトしましょう。

目　次

第1章 「McAfee.com パーソナルファイアウォールPlus」をお使いいただく前に

動作環境

●**機種**──メーカーサポートのPC/AT互換機（DOS/V機）、NEC PC98-NXシリーズ

●**OS**──Windows XP *（Home Edition/Professional）
Windows Me/98/98（Second Edition）/95
Windows 2000 Professional *
＊Administrator権限でご使用ください。

●**CPU**──i486以上（Pentium以上推奨）

●**メモリ**
Windows Me/98/98（Second Edition）/95　32MB以上のメモリ（64MB以上推奨）
Windows XP/2000　64MB以上のメモリ（128MB以上推奨）

●**ハードディスク（インストールするために必要な容量）**
ハードディスクの空き容量　10MB以上

●**ディスプレイ**──800×600以上の解像度、256色以上

●**その他**──CD-ROM読み込み可能なドライブ
（CD-ROM使用でのインストール時のみ）
インストール、アップデートを行うためには、インターネットへ接続できる環境が必要となります。
Internet Explorer 5.0*以上
＊Internet Explorer 3.X から Internet Explorer 5.0へアップグレードする場合は、直接 (3.X→5.0）では無く、Internet Explorer 4.Xを経て（3.X→4.X→5.X）順にアップグレードしてください。

※Windows XP / 2000では、「McAfee.com パーソナルファイアウォールPlus」と、「驚速8」（「速パック8」の「驚速8」を含みます）、「驚速7」（「速パック7」の「驚速7」を含みます）、驚速2000（「速パック2000」の驚速2000を含みます）を同時にご利用いただくことはできません。「McAfee.com パーソナルファイアウォールPlus」をインストールする前に、お使いの「驚速8」、「驚速7」「驚速2000」を必ずアンインストールしてください。こちらで詳細をご確認ください。
http://www.sourcenext.info/mcafee/support/mpf_kyou.html

※「McAfee.comパーソナルファイアウォール Plus」と「京セラ製ブロードバンドルーター付属のプリンタサーバモニタプログラム」および「京セラ製無線LANカード(KY-LC-WL100）用のユーティリティ」を併用することはできません。どちらか一方の製品のみをお使いください。

「McAfee.comパーソナルファイアウォール Plus」はASP方式で常に最新のプログラムを提供しております。それに伴うマニュアルの最新版は以下の弊社ホームページから入手することができます。また、サポート情報もあわせてご確認ください。

http://www.sourcenext.info/mcafee/support.html

インターネットブラウザの設定を確認する

「McAfee.com パーソナルファイアウォールPlus」をお使いいただく前に、お使いのブラウザのセキュリティ設定を確認する必要があります。ここでは、Internet Explorer 6.0*の設定の確認・変更方法をご説明します。

※その他のバージョンのInternet Explorerでもほとんど同じ方法で確認できます。

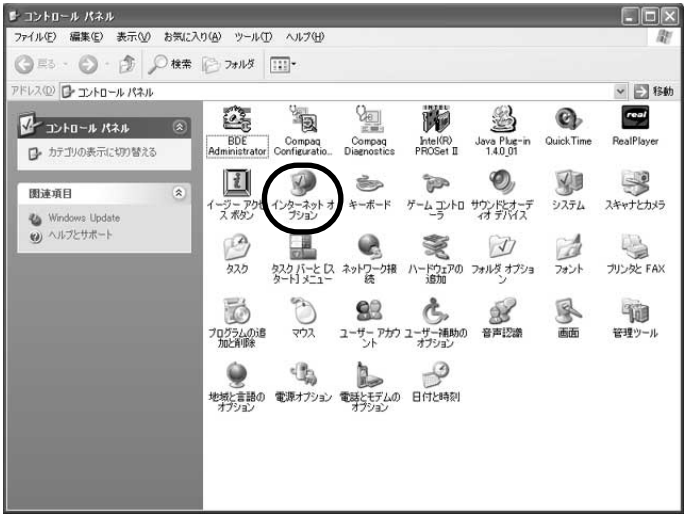
補足

WindowsXP以外のOSや、クラシックスタートメニューをお使いの場合、[スタート]ボタンから[設定]→[コントロールパネル]を選択します。

①［スタート］ボタンから［コントロールパネル］を選択します。

②［クラシック表示に切り替える］をクリックします。

③［インターネットオプション］アイコンをダブルクリックします。



④「インターネットのプロパティ」画面が表示されます。［セキュリティ］タブをクリックします。

⑤［インターネット］が選択されていることを確認します。［このゾーンのセキュリティのレベル］のスライドバーを［中］にして、［OK］をクリックします。

⑥「コントロールパネル」画面の右上の［×］をクリックして閉じます。

補足

セキュリティ設定のスライドバーが表示されない場合は、［既定のレベル］ボタンをクリックして表示させ、設定を行ってください。

補足

Windows2000およびXPで使用する場合、Administrator権限でご使用ください。

「McAfee.com パーソナルファイアウォール Plus」のアップデート方法

①タスクトレイの［McAfee.com SecurityCenter］アイコンMを右クリックして、［アップデート］を選択します。

②［今すぐ確認する］をクリックします。

③アップデータがある場合は、「アップデート」画面が開きます。[アップデート]ボタンをクリックします。

補足

アップデートの詳細を確認するには、[こちら]をクリックしてください。

④［ようこそ］画面の［次へ］ボタンをクリックします。

⑤通常は［次へ］ボタンをクリックします。インストール先を変更したい場合は［参照］ボタンを押してフォルダを選択してください。

⑥［インストールを開始］画面の［次へ］ボタンをクリックします。

注意

「McAfee.com パーソナルファイアウォールPlus」は、再起動後に全ての機能が使えるようになります。再起動しない状態で使用すると、エラーが発生することがありますので、必ず再起動してください。

補足

「McAfee.com セキュリティ・センター」の画面の表示方法は、12ページをご覧ください。

補足

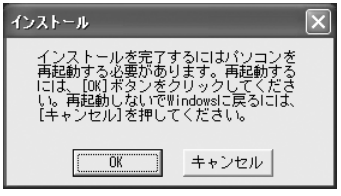
インストール完了の確認は、以下の2通りでも行えます。

A）［スタート］ボタンから［コントロールパネル］を選択し［プログラムの追加と削除］を開き、表示される［インストールされているプログラム一覧］で確認する。

B)［スタート］メニューから［プログラム］-［McAfee.com］を選択し、［McAfee.com Personal Firewall Plus］が表示されているか確認する。

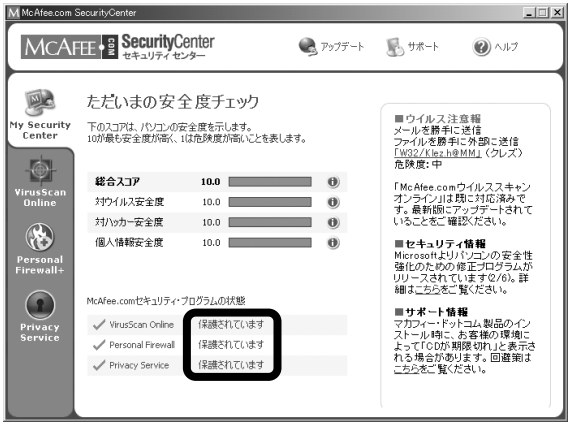
⑦［インストール］完了画面の［完了］ボタンをクリックします。

⑧再起動を促す画面が出ますので、［OK］をクリックして再起動してください。



●インストール（アップデート）の確認

インストールが正常に終了しているかを「McAfee.com セキュリティ・センター」の画面で確認できます。［保護されています］と表示されていれば、インストールは正常に終了しています。［インストールされていません］と表示された場合は、いったんアンインストールしてから、再度インストールをして、アップデートをしてください。



「McAfee.com パーソナルファイアウォール Plus」の機能

「McAfee.com パーソナルファイアウォールPlus」は、インストールするだけで、お使いのパソコンを不正な接続から守ります。
ここでは、「McAfee.com パーソナルファイアウォールPlus」がどのように不正接続からパソコンを守っているのか簡単に説明します。

●他のコンピュータからアクセスがあった場合、即時にアクセスをブロックします。

1）ブロックした際にアラートを表示して、対策を選択することができます。
2）簡単な操作で必要なアクセスのみ許可することが可能です。
3）あらかじめ利用するソフトや接続する相手を設定することができます。
4）頻繁にアクセスしてくる不正なアクセスを登録することができ、ブロックする判断が簡単になります。
5）設定レベルが5段階設定*してあり、変更が簡単にできます。
* セキュリティレベルを上げすぎると通常の動作を妨げる恐れがあります。

●アクセスのあった相手の所在地を追跡することができ、地図で表示します。

不正なアクセスとパソコンの動作を区別する手助けをします。アラートダイアログが表示された際に、「アクセスを追跡」を選択すると、世界地図上のどの地域からのアクセスかを表示します。何らかの操作をしようとして出たダイアログでその操作の発生に関係ありそうな地域からのアクセス時には、「このIPアドレスを承認する」を選択してください。

※必ずしも日本語のウェブサイトでのダウンロードが日本からのアクセスでない場合があります。アクセスをブロックすることによってパソコンの操作に支障がある場合は、「このIPアドレスを承認する」にしてください。

●その他の「パーソナルファイアウォール Plus」の特長

・HackerWatch.orgとの統合で、アクセスの詳細情報をHackerWatch.orgのデータと照らし合わせて、診断した結果を表示することができます。不正アクセスを届け出ることも簡単に行なうことができます。

・アクセスの記録をわかりやすいかたちで表示します。

第2章 「McAfee.com セキュリティ・センター」でお使いのパソコンの安全度をチェックする

「McAfee.com セキュリティ・センター」では、お使いのパソコンが、さまざまな外敵からどれくらい安全に保たれているか、多面的に診断します。また、診断結果から、「McAfee.com パーソナルファイアウォール Plus」のアップデートの必要性や、「McAfee.com セキュリティ・センター」以外のマカフィー・ドットコム製品のご紹介をします。また、各マカフィー・ドットコム製品の操作も「McAfee.com セキュリティ・センター」でできるので、それぞれのソフトを起動する必要がなく便利にお使いいただけます。

2-1

「McAfee.com セキュリティ・センター」のメイン画面の使い方

「McAfee.com パーソナルファイアウォールPlus」をインストールすると、自動的に「McAfee.com セキュリティ・センター」もインストールされます。インストール後はパソコンを起動すると自動的に起動し、タスクトレイに［McAfee.com SecurityCenter］アイコンMが常駐します。

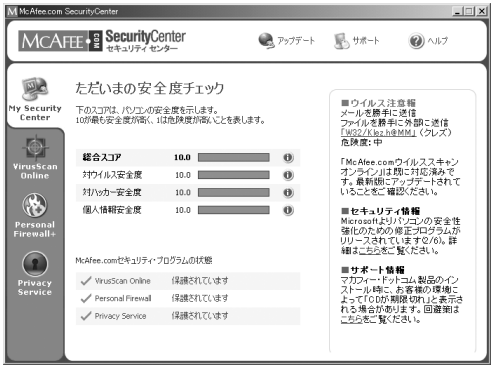
補足

他のソフトをインストールする場合など、「McAfee.com セキュリティ・センター」を終了させたい時は、タスクバーの［McAfee.com SecurityCenter］アイコンを右クリックして表示されるメニューから［終了］を選択します。

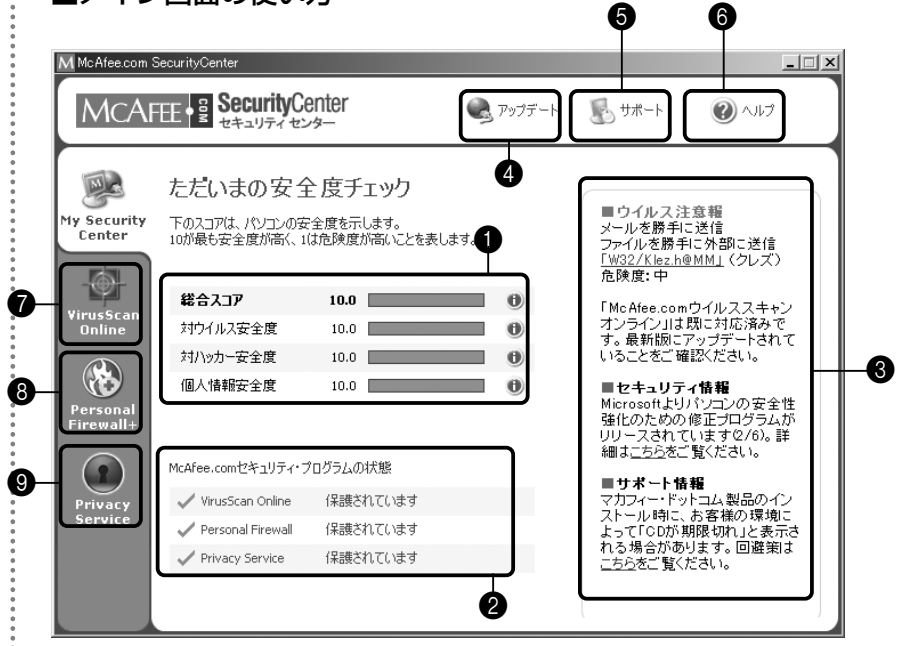
■メイン画面表示

① タスクトレイにある［McAfee.com SecurityCenter］アイコンMを右クリックして表示されるメニューから［SecurityCenterを開く］を選択します。

②［McAfee.com SecurityCenter］画面が表示されます。



■メイン画面の使い方



❶安全度チェック

各項目の安全度と総合評価が表示されます。より10に近いほうが安全です。各項目の右のアイコンをクリックすると詳しい評価を見ることができます。（p.13参照）

❷McAfee.comセキュリティ・プログラムの状態

各製品には使用期限があり、一定の期間ごとに継続利用の手続きが必要となります。ここでは、その使用期限が残り100日以内になると残りの期間を表示し、［継続］ボタンが表示されます。（p.17参照）

❸メッセージボード

最新のウイルス情報や、Microsoft Internet Explorerなどの、セキュリティ関連の修正プログラム情報などをお知らせします。

❹アップデート

お使いのマカフィー・ドットコム製品の最新バージョンの有無を確認することができます。また、アップデート方法もここで設定できます。(p.14～15参照)

❺サポート

サポート情報のページを開きます。もし、トラブルが発生した場合はここでご確認ください。

❻ヘルプ

「McAfee.com セキュリティ・センター」の操作方法がわからない時には、ヘルプを開いてご確認ください。

❼VirusScan Online

「McAfee.com ウイルススキャンオンライン」の操作画面に切り替えます。

❽Personal Firewall

「McAfee.com パーソナルファイアウォールPlus」の操作画面に切り替えます。

❾Privacy Service

「McAfee.com プライバシーサービス」の操作画面に切り替えます。

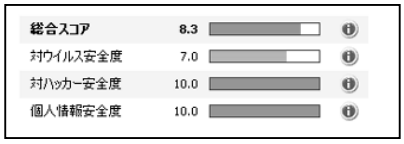
■メイン画面を閉じる

①「McAfee.com SecurityCenter」画面の右上［×］をクリックして閉じます。

2-2

安全度の確認と対処方法

お使いのパソコンの安全度を確認し、それぞれの対処方法を確認しましょう。



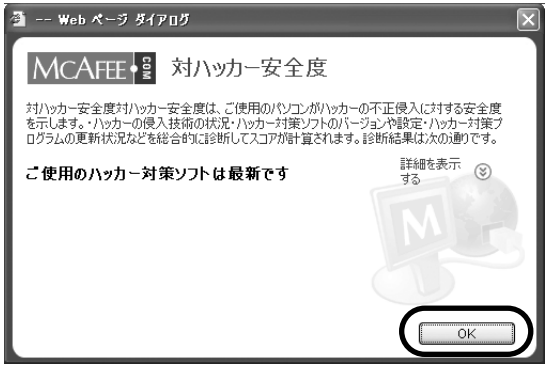
●評価が10の場合

最新の対策がとられています。問題ありません。

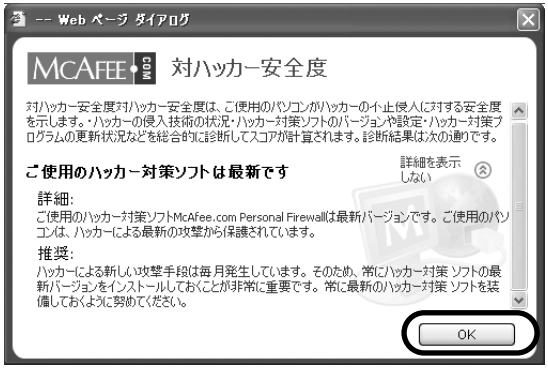
●評価が10未満の場合

安全対策に問題があります。右の ⓘ アイコンをクリックします。

診断結果が表示されます。［詳細を表示する］をクリックします。



［詳細］と［推奨］が表示されます。［推奨］に対処方法が記載されています。内容を確認して［OK］をクリックします。



2-3

アップデート方法を設定する

「McAfee.com パーソナルファイアウォールPlus」やその他インストール済みのマカフィー・ドットコム製品の、アップデートの確認・設定を行います。

●アップデートの有無の確認

［アップデート］ボタンをクリックし、表示される「McAfee.com SecurityCenterのアップデート」画面の［今すぐ確認する］をクリックします。

●アップデートの通知方法

［アップデート］ボタンをクリックし、表示される「McAfee.com SecurityCenterのアップデート」画面の［設定］をクリックします。

アップデートの通知方法を選択して［OK］をクリックします。

【アップデートをダウンロードする前に通知する（推奨）。】

自動的にアップデートを探し、アップデートがある場合ダウンロードする前に通知します。

【自動アップデートをオフにする。McAfee.com Servicesのアップデートを手動で行う。】

自動的にアップデートを探さず、アップデートの有無を手動で確認します。

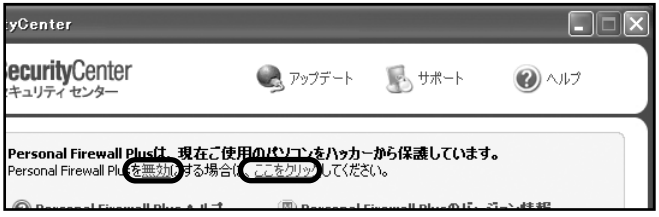
2-4

「McAfee.com パーソナルファイアウォールPlus」の有効/無効の切り替え

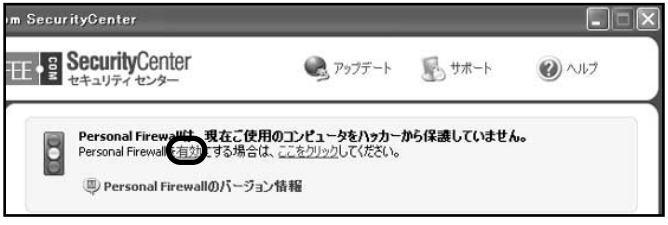
通常インストール後は有効になっていますが、何らかの理由によって「McAfee.com パーソナルファイアウォールPlus」を無効（不正アクセスからパソコンが守られていない状態）にする場合の方法を説明します。（必要な操作が終わったら、すぐに有効に戻すことをおすすめします。）

①［Personal Firewall Plus］アイコンをクリックします。

②「Personal Firewall Plus」操作パネルが表示されます。画面上部の［無効］または［ここをクリック］をクリックして、有効・無効を切り替えます。

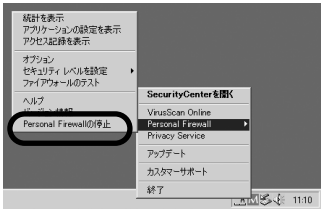


③「現在ご使用のパソコンをハッカーから保護していません。」と表示されます。［有効］をクリックすると、元の状態に戻ります。



補足

タスクトレイからも有効・無効を切り替えることができます。



2-5

製品の使用期限と継続使用の方法

ご使用の製品には有効期限が設定されており、期限が切れた後のご利用には 継続利用の手続きが必要となります。ここでは、継続して利用するための方法を説明します。なお、継続利用の手続きは、弊社Webサイトで継続用プログラムを購入して実行するだけで、簡単に実施できます（製品をアンインストールしてインストールといった作業は必要ありません）。継続利用の手続きは次のとおりです。

補足

期限が切れると各ソフトの操作画面でも注意がなされます。

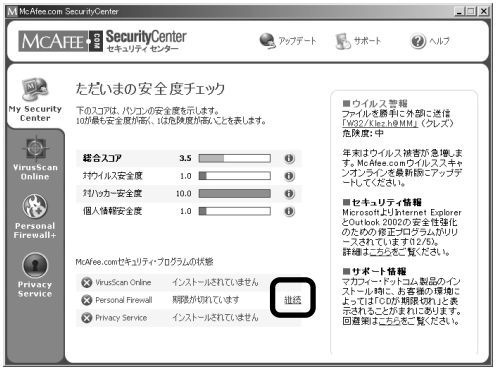
補足

有効期間が残り100日になると「継続」ボタンが現れます。

注意

継続手続きは、インターネットに接続してから行ってください。

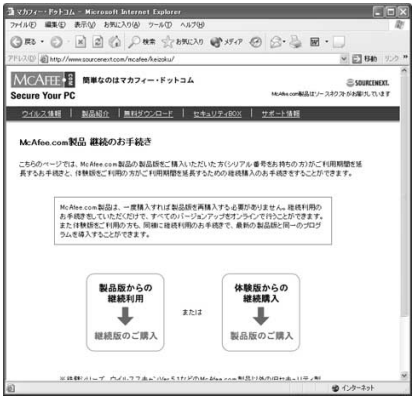
① ［McAfee.comセキュリティ・プログラムの状態］の、有効期間が少なくなったり、期限が切れたりしたソフト名の右に表示されている［継続］をクリックします。



② 「McAfee.com製品　継続のお手続き」ページが表示されます。画面の指示にしたがって継続の手続きを行ってください。

※製品版から継続利用のお客様は、必ず「継続版のご購入」を選択してください。

※体験版をご利用中のお客さまは「体験版からの継続購入」を選択してください。

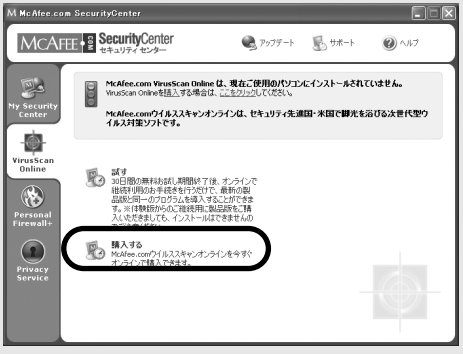


その他のマカフィー・ドットコム製品について

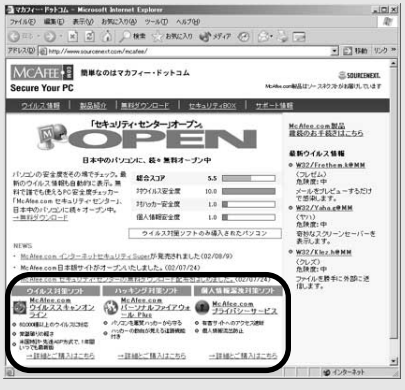
「McAfee.com セキュリティ・センター」では、簡単にマカフィー・ドットコム製品の購入ができます。

① 購入したい製品のアイコンをクリックします。

②［購入する］をクリックします。



③ オンラインショップページが表示されます。画面の指示に従って購入手続きを行ってください。



ヒント

30日間無料で試用できる、フル機能体験版もご用意しております。体験版をダウンロードする場合は、②の画面で［試す］をクリックし、表示される画面に従ってダウンロードしてください。

第3章 「McAfee.com パーソナルファイアウォールPlus」で不正なアクセスを防ぐ

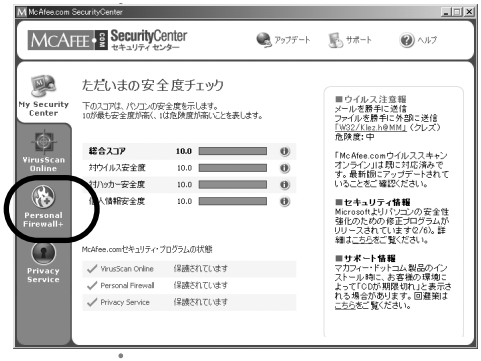
3-1

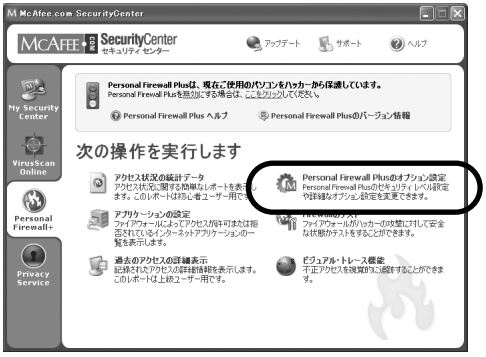
セキュリティレベルを設定する

セキュリティレベルとは、「McAfee.com パーソナルファイアウォールPlus」がお使いのパソコンを監視するレベルのことです。
お使いのシーンに合わせ、レベルを切り替えてお使いください。インストール時は［標準］の設定になっています。

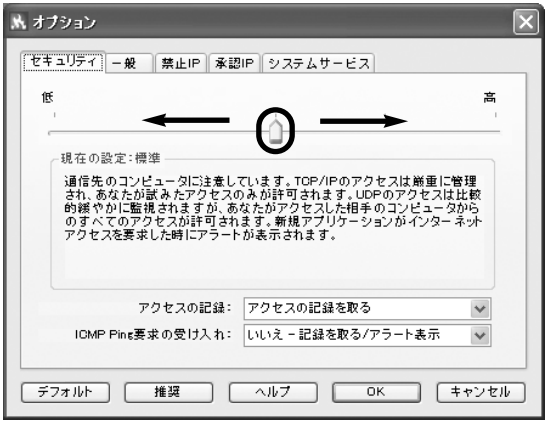
■オプション画面から設定を変更する

①［Personal Firewall Plus］アイコンをクリックして［Personal Firewall Plusのオプション設定］をクリックします。





②「オプション」画面が表示されます。［セキュリティ］タブのスライドバーで設定します。

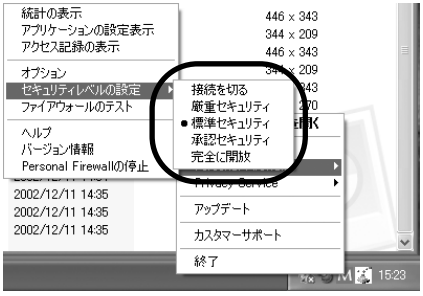


ヒント

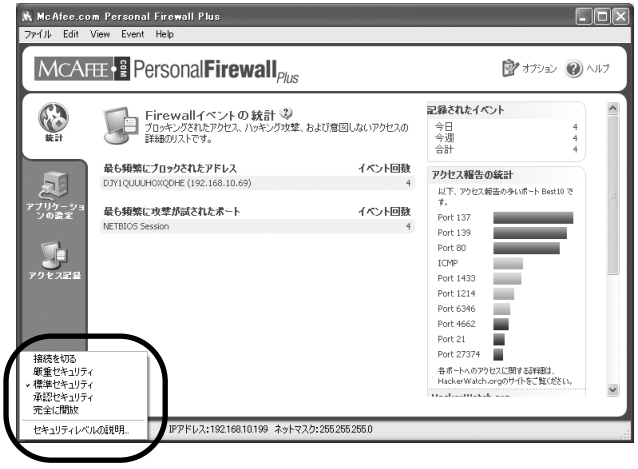
スライドバーを左右に動かすと、［現在の設定］にセキュリティレベルの説明が表示されます。よく読んで設定しましょう。

■タスクトレイから設定を変更する

タスクトレイにある［McAfee.com SecurityCenter］アイコンを右クリックして表示されるメニューから［Personal Firewall］―［セキュリティレベルの設定］からセキュリティレベルを設定します。



■メイン画面から設定を変更する



セキュリティレベルは、以下の説明どおりの設定になっています。ご利用の目的に合わせて選択してください。

【接続を切る】

アクセスはすべて遮断されます。この設定は本質的にはインターネットへの接続を切断することと同じです。 ［オプション］ダイアログの［システムサービス］で開くように設定したポートも遮断されます。

【厳重セキュリティ】

あなたのパソコンからの接続要求に対する応答のみが許可されます。 この設定では、UDPパケットを使用するアプリケーション（ビデオやオーディオをストリーミングするプログラムやゲーム）の多くは通信できません。 また

インターネットへの接続が必要なアプリケーションが承認を要求しますので、［外部へのアクセスのみ許可］するか、ブロックするかを選択してください。もし設定後にアプリケーションが［すべてのアクセスを許可］にすることを求めて来る時には、［すべてのアクセスを許可］するか、［外部へのアクセスのみ許可］を設定してください。この設定を使う際には「McAfee.com パーソナルファイアウォールPlus」の利用法をきちんと理解した上で行ってください。

【標準セキュリティ】

（推奨設定）通信を開始するパソコンだけがアクセスを返すことができます。UDPのアクセスは比較的緩やかに監視されています。アプリケーションはインターネットへ接続する最初の一回のみ、承認を求めてきます。その際には、［アクセスを許可］するか、［すべてのアクセスを拒否］するかを選択してください。 もし［アクセスを許可］した場合にはアプリケーションは非システムポートでの通信データを送受信できます。

【承認セキュリティ】

全てのアプリケーションがはじめてインターネットに接続しようとした時、自動的に通信が許可されます。（オプション設定で自動的に通信を許可せず、アラートダイアログを表示することも可能です。）ゲームまたはストリーミングメディアが動作しない場合はこの設定にすることをおすすめします。

【完全に開放】

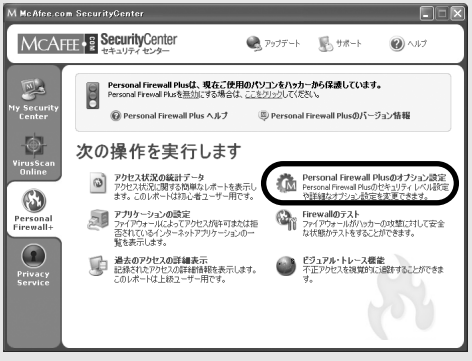
「McAfee.com パーソナルファイアウォールPlus」による保護は無効です。フィルタリングを行わないですべてのアクセスが許可されます。

ネットワークを利用して、サーバー的な役割をするアプリケーションを同時にご使用になる場合

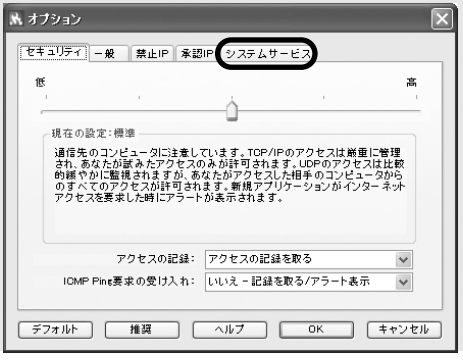
ネットワークを利用してサーバー的な役割をするソフトウェアをご使用になる場合は、そのソフトウェアを承認する設定が必要となる場合があります。ここでは、その設定方法をご紹介します。

①［Personal Firewall Plus］アイコンをクリックします。

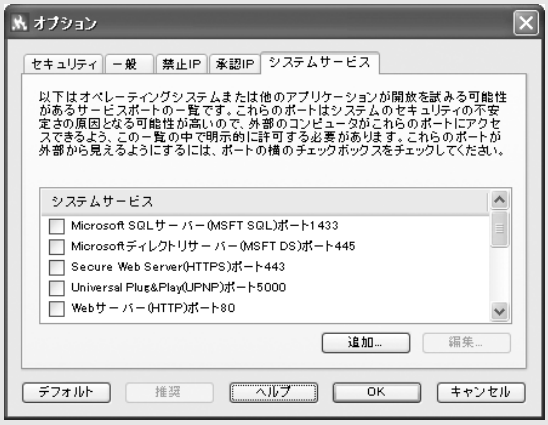
②［Personal Firewall Plusのオプション設定］をクリックします。



③「オプション」画面が表示されます。［システムサービス］タブをクリックします。



④［システムサービス］の一覧表示の中から、承認したいアプリケーションにチェックを入れます。



ヒント

承認したいアプリケーションが一覧に表示されない場合［追加］ボタンをクリックします。

「ポートの設定を追加」画面が表示されます。アプリケーション名を入力して［TCP/IP受信ポート］に以下の値を入力し［OK］をクリックします。

凄速シリーズ（2000/XPでのみ） "24491"
メールMAXSuite（2000/XPでのみ） "25" "110"
消えるMail（2000/XPでのみ） "25" "110"
見えないMail（2000/XPでのみ） "25" "110"
速いMail（2000/XPでのみ） "25" "110"（XPでモデムの場合300も）
凄速メールパワー（2000/XPでのみ） "25" "110"
遠近コン1・2 "80" "8080"
WindowsActiveSync "990""999" "5678" "5679"

ヒント

連続した数値「1,2,3,4,5」を入力する場合は「1-5」（「-」ハイフン）。複数の数値「1と4」を入力する場合は「1,4」（「,」カンマ）をお使いください。

ヒント

ここに記入されていないものに関しては、お使いのアプリケーション（ソフト）のメーカーに数値をお問い合わせください。他に設定の必要があるアプリケーションには、プリンタソフト、ファイル共有ソフトなどがあります。
当社の製品に関しての情報はhttp://www.sourcenext.comをご覧ください。

注意

全てのアクセスがアラートとして表示される訳ではありません。不正なアクセスのみをブロックする設定にしないとパソコンの動作が制限されます。

3-2

他のコンピュータから アクセスがあった場合の対処方法

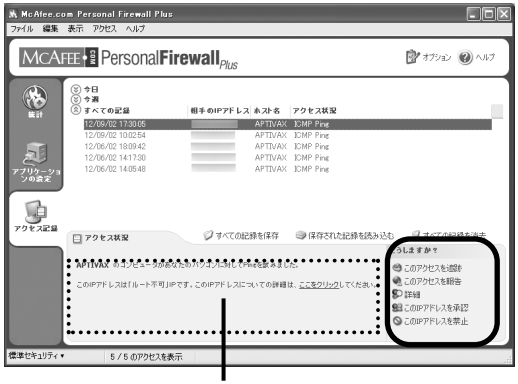
■アラートダイアログが出た時の対処法

お使いのパソコンに他のコンピュータから何らかのアクセスがあった場合、アラート画面が表示されます。その場合の対応方法を説明します。

① お使いのパソコンに他のコンピュータからアクセスがあった場合、画面右下にアラート画面が表示されます。［詳細を表示］をクリックします。

※「ウィンドウを閉じる」を選択した場合でもアクセスはブロックされています。それによって、パソコンの動作がおかしくなる時には、以下の説明を読んで、どの様な対策を取れば良いのか判断してください。

②「McAfee.com Personal Firewall Plus」画面が表示されます。情報を確認して次の操作を行ってください。



ここにアクセスされた場合の対応方法が表示されます。

【このアクセスを追跡】

クリックすると、アクセスしてきているコンピュータの居場所を地図上で確認できます。それによって、現在の報告されているアクセスの正当性を判断する手助けをします。行っている作業とは関連性のない地域からのアクセスは疑ってください。

【このアクセスを報告】

ハッキングと思われた場合、HackerWatch.orgにアクセスをレポートしましょう。その情報はデータベースに登録され、個々のデータを見ただけではわからないハッキングパターンを検出することができ、今後のハッキング対策に役立てられます。

【詳細を表示】

HackerWatch.orgにてアクセス内容の詳細を表示します。プログラム中の解説より、新しい情報が載っています。

【このIPアドレスを承認】

現在接続しようとしたIPアドレスからの接続を許可します。次回からは、このIPアドレスからの接続は全て許可されます。接続しようとしているIPアドレスのコンピュータが安全な場合は許可しましょう。

クリックすると「このアドレスを承認する」画面が表示されます。［OK］をクリックします。

【このIPアドレスを禁止】

現在接続しようとしたIPアドレスからの接続を禁止します。次回からは、このIPアドレスからの接続は全て禁止されます。接続しようとしているIPアドレスが危険だと判断した場合、接続を禁止しましょう。

クリックすると「このアドレスを禁止する」画面が表示されます。［OK］をクリックします。

補足

特定のサイトから複数のサービスを受ける時に（複数のソフトを使って特定サイトへ接続する時に）［このIPアドレスを承認］を選択すると便利です。

補足

特定のサイトから複数のポートへのアクセスが頻繁にある時には［このIPアドレスを禁止］を設定してください。

■疑うべきアクセスとは？

特定のサイトから複数のアクセスがある時

対処方法）

［このIPアドレスを禁止］を選択し、特定のIPアドレスからの接続を禁止します。

何もパソコンを操作していないのにアラートが出てくる時

対処方法）

［このアクセスを追跡］を選択し、どの地域からの接続が調べて、

補足

［このIPアドレスを禁止］は、［オプション］画面でも設定できます。詳しくは48ページをご覧ください。

補足

［このアクセスを追跡］は、「アクセス記録」画面からでも設定できます。詳しくは38ページをご覧ください。

接続を許可するか判断しましょう。

■安心して良いアクセスとは？

何かのソフトの動作をさせた時にアラートがでてくる場合。

対処方法）

アプリケーションのアクセスを許可してください。

普段は「外部へのアクセスのみ許可」すれば、そのアプリケーションの利用には問題ありません。なお、サーバー的な役割をするアプリケーションの場合のみ、「すべてのアクセスを許可」に設定してください。

IPアドレスによる設定を行なうために

IPアドレスは、数字の羅列で、 この数字はインターネット上のいわゆる住所を示すものです（正確に言うと4つの部分から構成された、それぞれ0から255までの数字です）。IPアドレスを理解していると、アクセスがあった場合に、不正なものかを判断する手助けになります

●特殊な IPアドレス（特殊IPアドレス）の解説

幾つかのIPアドレスは、特殊な使われ方をするように決まっています。

“Non-ルータブル” IPアドレス:

よく"プライベートIPアドレス領域"と表現されます。これらのIPアドレスは、インターネット上で利用することはできません。プライベートIPアドレスは、10.x.x.x, 、172.x.x.x, 、192.168.x.x.に相当するアドレスの全てを指します。

“ループバック” IP アドレス:

“ループバック” アドレスは、一般的にテスト目的で使われます。これらのIPアドレスに送られた通信は、通信を始めた機器（パソコン）に直接帰ってきます。これらの通信は機器の中を出ることはなく、ハードウェアとソフトウェアのテストのために利用されます。“ループバック” IPアドレスは、127.x.x.x.に相当するアドレスの全てを指します。

ゼロIPアドレス:

これは無効なアドレスです。通信に空白のIP アドレスが使われたことを示します。これは明らかに普通ではなく、まれにしか起きないもので、送信者が意図的にアクセスの発信住所をごまかしていると考えられます。送信者は、アプリケーションがそのアプリケーショ

ンにだけ判る内容の送信を行なう場合にしか、返信を受け取ることができません。ゼロIPアドレスは単純に 0.0.0.0.というアドレスになります。また、255.255.255.255とあわせてブロードキャストアドレスと呼ばれ、同一LAN上の同報通信に使うアドレスとして知られています。

●よくあるアクセスごとの解説

0.0.0.0からのアクセス

0.0.0.0, の　IPアドレスのアクセスを見つけた場合には、2つの原因が考えられます。一つ目は（これが最も一般的な原因）は、壊れた受信データがあなたのパソコンに届いた場合です。インターネットは、100%完璧に信頼できるものではなく、データが通信中に壊れてしまうこともあります。パソコンが壊れたデータを破棄する前に「McAfee.com パーソナルファイアウォールPlus」がデータを捕まえてしまった時には、そのデータを不正アクセスとして誤認することがあります。もう一つの原因は、発信元が偽装されている場合です。偽装した通信は、“トロイの木馬”を誰かが探しているからだと考えることができます。しかし「McAfee.com パーソナルファイアウォールPlus」は、既にアクセスをブロックしていますので安心していただいて結構です。

127.0.0.1からのアクセス

基本的にどのようなネットワークにあっても、127.0.0.1というIPアドレスは、現在使用中のパソコンを指します。同時にlocalhostを参照する際にも同じで、localhostと言うコンピュータ名を指定してあるとIPアドレス 127.0.0.1.を探しに行く決まりになっています。

では、このアクセスはハッキングをされようとしていることの証明でしょうか？また、“トロイの木馬”や“スパイウェア”が、コンピュータを、乗っ取ろうとしているのでしょうか？それは、あまり起こり得るケースではありません。さまざまなソフトがこの“ループバック” アドレスを利用することによって、付加機能を提供しています。例えば、EmailソフトやWebサーバーが外部からWebブラウザーを使って接続ができるサービスを行なっています。その際にhttp://localhost/　というアドレスから始まる方法で利用する場合に、このループバックアドレスは利用されます。

しかし、「McAfee.com パーソナルファイアウォールPlus」はこれらのソフトが問題無く動くように作られております。そのため、127.0.0.1のアクセスを検知した場合、発信元が偽装されている場

合が考えられます。偽装した通信は、“トロイの木馬”を誰かが探しているからだと考えることができます。しかし、既にアクセスはブロックされていますので安心して頂いて結構です。

注；Netscape 6.2以上をご利用の場合は、127.0.0.1を「承認IPアドレス」に加えていただかないと、全ての機能が十分に動かないことが確認されております。

「McAfee.com パーソナルファイアウォールPlus」の設定の仕方

Netscape 6.2を例にとって説明すると、もし127.0.0.1を「承認IPアドレス」に加えない場合に、「友だちリスト」を利用できなくなる現象が確認されております。ですからこの127.0.0.1のアクセスを見つけても、パソコンが十分に機能していたら、このIPアドレスをブロックしておいていただいても問題ありません。Netscapeのように問題が見つかる場合には、「承認IPアドレス」に加えていただくと問題無くご利用になれます。

同じLAN上のコンピュータからのアクセス（192.168.0.0～192.168.255.255）

同じローカルエリアネットワーク(LAN)上のアクセスも、アクセスとして記録に残ります。「McAfee.com パーソナルファイアウォールPlus」はそれらの記録を緑色で表示します。なお、企業の社内LANの場合、［オプション］ダイアログの中の［承認IP］タブ内にある「LAN上のすべてのコンピュータを承認する」チェックボックスにチェックを入れてください。

上記の設定を行なうことで、LAN内で頻繁に発生するアクセスをブロックしないようになります。しかし、LAN内のアクセスも外部からのアクセスと同じくらい不正なものが起こりやすいことを、気に留めて置いてください。

特にDLSやCATV業者によっては、複数のユーザーを一つのLANの中に入れるような仕組みでサービスを提供しているところが存在します。その際には上記の設定を行なうことは避けてください。

プライベートIPアドレスからのアクセス

192.168.xxx.xxxで始まるIPアドレスや10.xxx.xxx.xxxで始まるものは、“non-ルータブルIPアドレス”や“プライベートIPアドレス”と呼ばれます。これらのIPアドレスは、同じ（ローカル）ネットワークを出ることはありません。　信頼していただいて問題ありません。

もしプライベートネットワークの中にいない時に、これらのIPアドレスからの接続が記録される場合には、発信元IPアドレスは、偽装していることが考えられます。

第4章 「McAfee.com パーソナルファイアウォールPlus」の動作結果を確認する

4-1

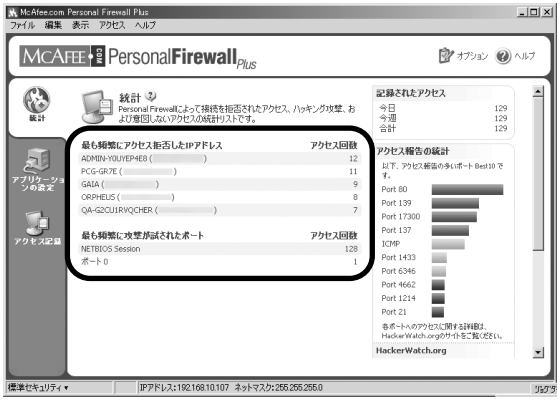
統計情報を表示する（初心者向け）

「McAfee.com パーソナルファイアウォールPlus」の動作について簡単な表示で確認できます。接続をブロックしたIPアドレスや攻撃されたポートが頻度の高い順に表示されます。他のコンピュータからの接続状況を確認しましょう。

① ［Personal Firewall Plus］アイコンをクリックします。

② ［アクセス状況の統計データ］をクリックします。

③「統計」画面が表示されます。内容を確認しましょう。



【最も頻繁にアクセス拒否したアドレス】

接続をブロックした回数の多いコンピュータ順に、[コンピュータ名]と[IPアドレス]、[回数]が表示されます。頻度の高いコンピュータで相手を知らない場合は注意する必要があります。

【最も頻繁に攻撃が試されたポート】

ブロックされた接続が、お使いのコンピュータのどのポートに接続しようとしていたのか回数の多い順に、[ポート]と[回数]が表示されます。

【記録されたアクセス】

お使いのコンピュータに接続が試されたアクセス回数を表示します。ブロックした、しないに関わらずカウントされます。

【アクセス報告の統計】

世界のコンピュータで、アクセス報告の多いポートが順に表示されます。

4-2

アプリケーションの設定

Internet Exprolerなどの、ネットワークにアクセスするアプリケーションに対する、アクセス許可状況の参照とアクセス許可の変更が、アプリケーション単位でできます。

①［Personal Firewall Plus］アイコンをクリックします。

②［アプリケーションの設定］をクリックします。

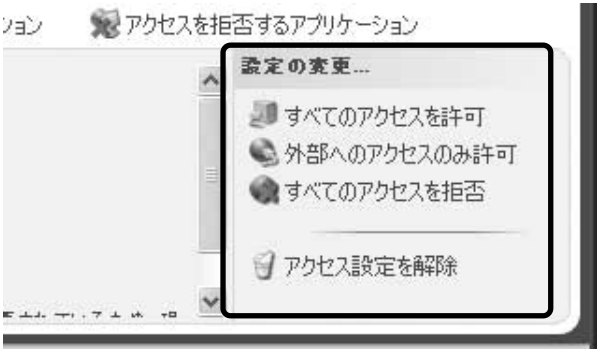
③［アプリケーションの設定］画面が表示されます。

■アクセス設定の変更方法

既に登録されているアプリケーションの設定を変更できます。
手順は以下のとおりです

①一覧中の設定を変更したいアプリケーションを選択します。

②画面右下の［設定の変更］の変更したい項目をクリックします。



補足

一覧に目的のアプリケーションがない場合は、次項の「一覧にないアプリケーションにアクセスの許可、拒否を設定する」をご参照ください。

【すべてのアクセスを許可】

ここをクリックすると、選択したアプリケーションのデータの送受信が可能になります。

【外部へのアクセスのみ許可】

ここをクリックすると、選択したアプリケーションのデータの送信のみが可能になります。

【すべてのアクセスを拒否】

ここをクリックすると、選択したアプリケーションのデータの送受信が不可能になります。

【アクセス設定を解除】

ここをクリックすると、選択したアプリケーションの設定が解除され、一覧から消えます。

■一覧にないアプリケーションにアクセスの許可、拒否を設定する

一覧にないアプリケーション（未設定のアプリケーション）にアクセスの許可と拒否の設定をすることができます。

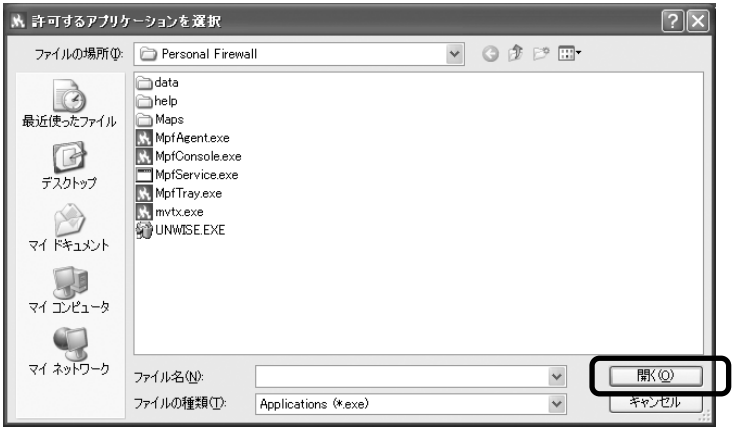
手順は以下のとおりです。

①［アプリケーションの設定］画面中の、アクセス許可をしたい場合は［アクセスを許可するアプリケーション］を、アクセス拒否をしたい場合は［アクセスを拒否するアプリケーション］をクリックします。

補足

アクセス設定を変更したい場合は、前項の「アクセス設定の変更方法」をご参照ください。

②変更したいアプリケーションを選択して［開く］をクリックします。
選択したアプリケーションのアクセスの許可、拒否が設定され、［アプリケーションの設定］画面中の一覧に表示されるようになります。



4-3

詳細情報を表示する（中上級者向け）

「McAfee.com パーソナルファイアウォールPlus」の動作について詳細なレポートを表示します。いつ、どのIPアドレスから、どのポートに接続があったかを表示します。また、各接続コンピュータに対しての対応も指示できます。

①［Personal Firewall Plus］アイコンをクリックします。

②［過去のアクセスの詳細表示］をクリックします。

③アクセス情報が表示されます。確認したい日を［今日］［今週］［すべての記録］をクリックして切り替えます。

④確認したいアクセスをクリックすると、詳細が［アクセス状況］に表示されます。

⑤選択しているアクセスの今後の対応について指定できます。［どうしますか？］で指定します。26ページの「IIPアドレスによる設定を行なうために」を参考に指定してください。

4-4

「McAfee.com パーソナルファイアウォールPlus」のテストを行なう

お使いの「McAfee.com パーソナルファイアウォールPlus」が正常に機能し、ハッカーからの攻撃に対して安全状態になっているかをインターネット上のサーバーからチェックすることができます。

①［Personal Firewall Plus］アイコンをクリックします。

②［Firewallのテスト］アイコンをクリックします。

③HackerWatch.orgのホームページが表示されます。画面の指示に従ってテストを行ってください。

注意

お使いの環境がルーターを使っている場合、［検査不可能］と表示されます。

注意

「NetBIOS」ポートが開いている」と表示される場合は、p.65の「「ファイアウォール」のテスト」を行なうと「NetBIOS」ポートが開いているとー」の項をご参照ください。

4-5

アクセスの追跡を行なう

外部からのアクセスを追跡し、地図や経路を表示することができます。

■選択したアクセスの追跡をする

①［Personal Firewall Plus］アイコンをクリックします。

②［過去のアクセスの詳細表示］をクリックします。

補足

追跡したいアクセスを右クリックし、表示されるメニューから［選択したアクセスを追跡］を選択することもできます。

③追跡したいアクセスを選択し、［このアクセスを追跡］をクリックします。

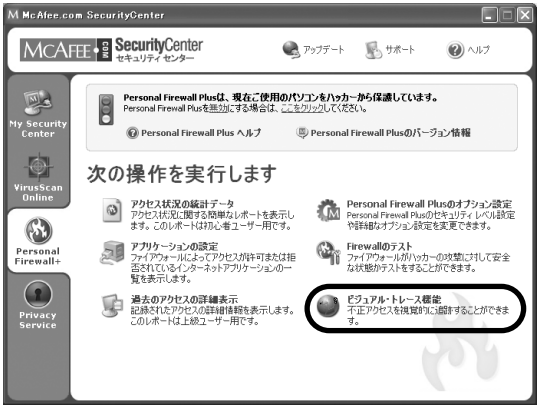
④ 地図が表示され、結果が表示されます。

【リスト表示】経路をリスト表示します。
【ネットワーク】ドメイン登録者についての説明を表示します。

■URLやホスト名、IPアドレスを指定して追跡する

①［Personal Firewall Plus］アイコンをクリックします。

②［ビジュアル・トレース機能］をクリックします。



③「ビジュアル・トレース機能」画面が表示されます。追跡したいURL、ホスト名またはIPアドレスを入力し、［追跡］をクリックします。

④地図が表示され、結果が表示されます。

4-6

HackerWatch.orgへの報告

ハッキングと思われた場合、HackerWatch.orgにアクセスをレポートすることができます。その情報は解析後、データベースに登録され、今後のハッキング対策に役立てられます。

HackerWach.orgユーザーIDの取得と方法

HackerWach.orgに報告をするためには、ユーザーIDが必要です。ユーザーIDの取得方法の手順は以下のとおりです。

①［オプション］ダイアログ（44ページ参照）の［一般］タブを選択して、［HackerWatchユーザーID情報］をクリックします。

②出て来たダイアログ中の［ユーザーIDの取得］をクリックします。

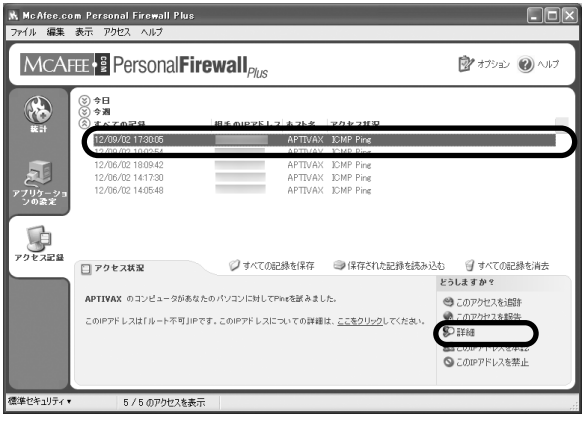
③出て来たページ中の必要事項を入力して、［HackerWatchユーザー使用許諾契約書に同意します。］にチェックを入れて、［続行］をクリックすると、メールでユーザーIDが送られてきます。

HackerWatch.orgへの報告

①［Personal Firewall Plus］アイコンをクリックします。

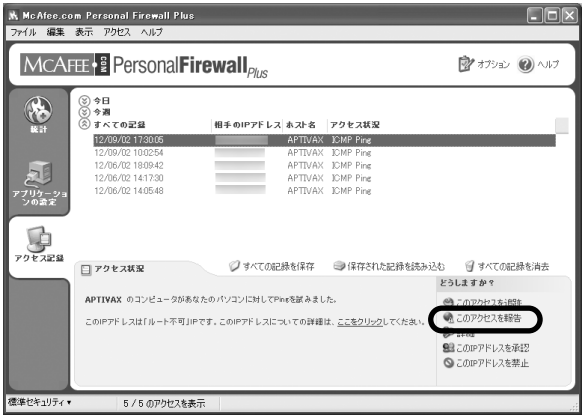
②［過去のアクセスの詳細表示］をクリックします。

③報告した方がいいと思われるアクセスを選択し、［詳細］をクリックします。



④HackerWatch.orgのページに接続し、報告の必要性があるかどうか表示されます。必要がある場合のみ次の手順に進んでください。

⑤HackerWatch.orgページの画面右上の［×］をクリックして閉じ、［このアクセスを報告］をクリックします。



⑥［HackerWatchユーザーID］に取得したIDを入れて［OK］をクリックします。

⑦しばらくして以下の画面が出ると報告完了です。

ヒント

p.61「送った情報はどうなるの？」をご参照ください。

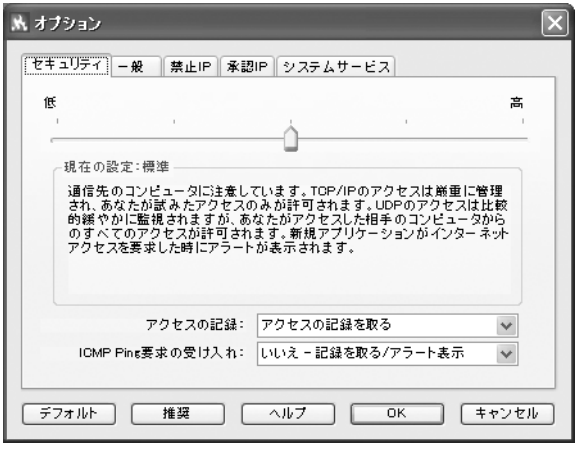
第5章 各種オプションを設定してより使いやすく

オプション画面の表示方法

- ［Personal Firewall Plus］アイコンをクリックします。次に［Personal Firewall Plusのオプション設定］をクリックして表示させます。
- 「McAfee.com Personal Firewall Plus」画面の右上にある［オプション］をクリックして表示させます。

5-1

セキュリティ



●現在の設定

セキュリティレベルは、以下の説明どおりの設定になっています。ご利用の目的に合わせて選択してください。

【接続を切る】

アクセスは全て遮断されます。この設定は本質的にはインターネットへの接続を切断することと同じです。［オプション］ダイアログの［システムサービス］で開くように設定したポートも遮断されます。

【厳重セキュリティ】

あなたのパソコンからの接続要求に対する応答のみが許可されます。この設定では、UDPパケットを使用するアプリケーション（ビデオやオーディ

注意

［厳重］に設定しているとUDPパケットのほとんどが遮断されます。

オをストリーミングするプログラムやゲーム）の多くは通信できません。またインターネットへの接続が必要なアプリケーションが承認を要求しますので、［外部へのアクセスのみ許可］するか、［すべてのアクセスを拒否］するかを選択してください。 もし設定後にアプリケーションが［すべてのアクセスを許可］にすることを求めて来る時には、［すべてのアクセスを許可］するか、［外部へのアクセスのみ許可］を設定してください。この設定を使う際には「McAfee.com パーソナルファイアウォールPlus」の利用法をきちんと理解した上で行ってください。

【標準セキュリティ】

(推奨設定) 通信を開始するパソコンだけがアクセスを返すことができます。UDPのアクセスは比較的緩やかに監視されています。アプリケーションはインターネットへ接続する最初の一回のみ、承認を求めてきます。その際には、［アクセスを許可］するか、［すべてのアクセスを拒否］するかを選択してください。 もし［アクセスを許可］した場合にはアプリケーションは非システムポートでの通信データを送受信できます。

【承認セキュリティ】

全てのアプリケーションがはじめてインターネットに接続しようとした時、自動的に通信が許可されます。（オプション設定で自動的に通信を許可せず、アラートダイアログを表示することも可能です。）ゲームまたはストリーミングメディアが動作しない場合はこの設定にすることをおすすめします。

【完全に開放】

「McAfee.com パーソナルファイアウォールPlus」による保護は無効です。フィルタリングを行わないで全てのアクセスが許可されます。

●アクセスの記録

検出されたアクセスの記録を取るかどうか指定できます。
［アクセスの記録を取る］を選択した場合はメインウィンドウの「アクセス記録」にそのアクセス記録が表示されます。

注意

あらかじめ、[アクセスの記録]ドロップダウンメニューの[アクセスの記録を取る]を選択してからping 要求の記録を取ってください。

●ICMP Ping要求の受け入れ

ICMP Pingとアクセス記録の動作を設定できます。ICMP Pingは主に追跡と通信の開始を試みる前の簡単なテストを行なうときによく使用されます、WinMXプログラムを実行中か、実行を完了している場合は、多数のpingが処理される場合があります。

- ［いいえ-記録を取る/アラートを表示］を選択すると、ping要求は拒否され、アクセスを受けた記録は残ります。
- ［いいえ-無視］を選択すると、ping要求は拒否されますが、記録

注意

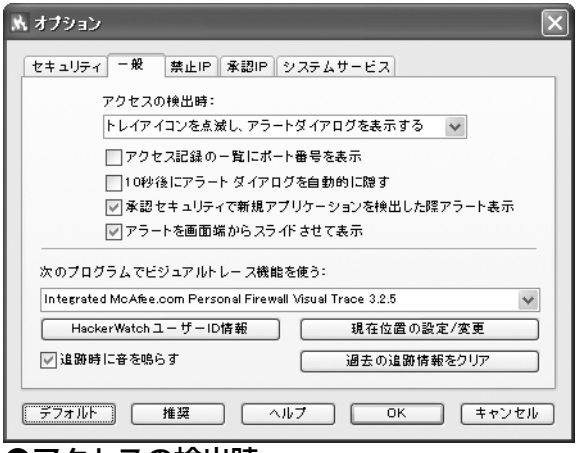
自分自身にpingを打つ時はこの設定をOFFにしてください。(推奨設定)通信を開始するコンピュータだけがトラフィック(通信)を返すことができます。

には残りません。

・［はい］を選択すると、ping要求は許可されて記録にも残りません。

5-2

一般



●アクセスの検出時

［アクセスが検出された場合］ドロップダウンメニューで、アクセスが検出された場合の通知方法を選択できます。次のオプションから選択します。

①**トレイアイコンを点滅する**：システムトレイ上のアイコンを点滅させる場合に選択します。

②**トレイアイコンを点滅し、アラートダイアログを表示する**：アクセスが検出されるとアラートダイアログが表示され、システム トレイ上のアイコンが点滅します。

③**何もしない**：アクセスが検出されると、記録は残りますが何も表示されません。

ヒント

メイン画面が開いている時にはトレイアイコンは点滅しません。

●アクセス記録にポート番号を表示

アクセスの発信元のポートと受信ポートが表示されます。

●10秒後にアラートダイアログを自動的に隠す

このオプションを選択すると、アクセスのアラートダイアログを表示してから10秒後にアラートダイアログは自動的に隠れます。

●承認セキュリティで新規アプリケーションを検出した際アラート表示

このオプションを選択（デフォルトの設定）すると、「承認セキュリ

ティ」レベルで新規に利用するアプリケーションや変更が行われたアプリケーションを検知した際にアラートを表示します。

●アラートを画面端からスライドさせて表示

この設定(デフォルト)を選択すると、アプリケーションがインターネットへのアクセスを要求するためのアラートがデスクトップ上に表示されます。アラートは、画面の端からスライドされるように表示されます。

●リストから使用するビジュアルトレース機能を選択する

ドロップダウンメニューで、アクセスの追跡に使用できるMcAfee.com Visual Traceのバージョンを選択できます。
デフォルトでは、「McAfee.com パーソナルファイアウォールPlus」に組み込まれている追跡機能が選択されます。McAfee.com Visual TraceまたはNeoTraceをお持ちの場合には、アクセス追跡時にいずれかのプログラムを使用するように選択できます。

ヒント

HackerWatch.org関連の設定その他の詳細は、p.41「HackerWatch.orgへの報告」をご参照ください。

●HackerWatchユーザーID情報

アクセスをHackerWatch.orgに報告するには、HackerWatch.orgへの登録が必要です。登録後、提出されたレポートは追跡され、追加情報または追加操作が必要になった場合にはHackerWatch.orgから通知が届きます。貴重な情報に対して、受信した情報を確認させていただくためにも登録は必要です。

ご連絡いただいた全ての電子メールアドレスの機密は保持されます。追加情報のリクエストがISP によって行われた場合、そのリクエストは HackerWatch.orgを経由しますので電子メールのアドレスが外部に漏れることはありません。

●追跡中に音を鳴らす

ビジュアルトレースにて追跡を行なう際の音響効果のオン/オフを切り替えるオプションです。

●現在位置の設定/変更

ビジュアルトレースの現在位置を変更または設定する場合にこのボタンをクリックします。

●過去の追跡情報をクリア

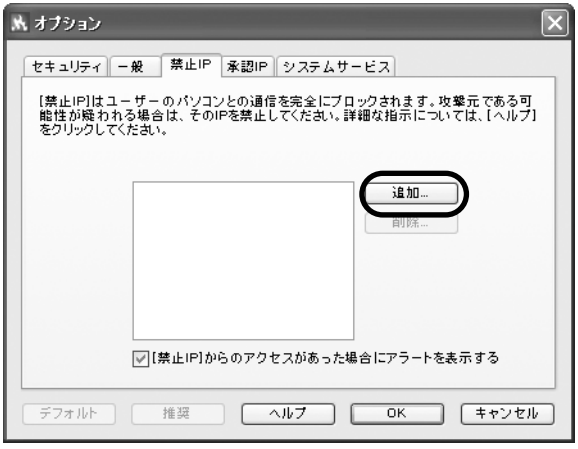
トレースキャッシュを消去すると、ビジュアルトレースで格納したアクセス追跡に関する情報は全て削除されます。

5-3

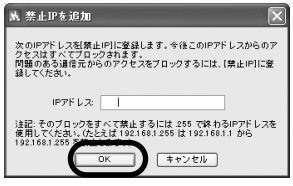
禁止IP

特定のコンピュータからのアクセスを完全に阻止したい場合はここに相手のIPアドレスを登録します。
禁止IPアドレスからのアクセスが検出されると、一般タブ内の「アクセスの検出時」で選択した方法でアラートが表示されます。
禁止IPの登録の手順は以下のとおりです。

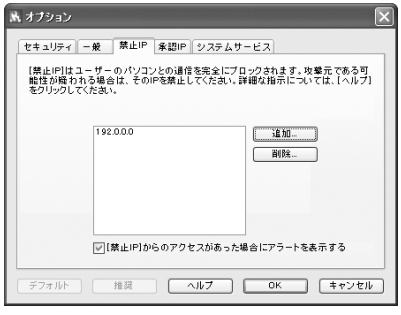
①［追加］をクリックします。［禁止IPを追加］ダイアログボックスが開きます。



②禁止するIPアドレスを入力して［OK］をクリックします。



③禁止IPの一覧に、入力したIPアドレスが表示されます。



注意

アラートが表示されるのは［禁止IPからのアクセスがあった場合にアラートを表示する］にチェックが入っている時のみです。

ヒント

メイン画面でログを選択して右クリックメニューやメニューバーの［アクセス］、または警告ダイアログから［選択されたIPアドレスを禁止する］を選択することでも登録が可能です。

ヒント

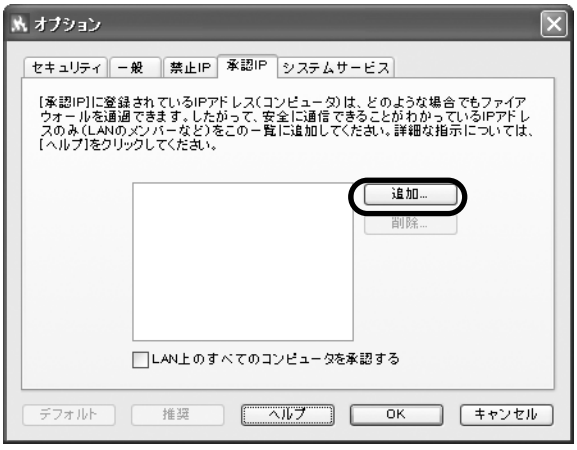
禁止IPアドレスの設定を解除するには、IPアドレスをクリックして、［削除］をクリックすると、一覧から削除されます。

5-4

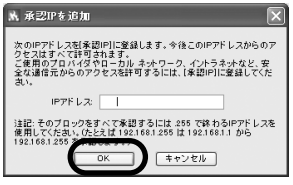
承認IP

特定のコンピュータからのアクセスを常に許可します。会社やご家庭で接続している他のパソコンなどのIPアドレスなど完全に安全だとわかっているIPアドレスを設定しておきましょう。［承認IP］の一覧にIPアドレスを追加する手順は以下のとおりです。

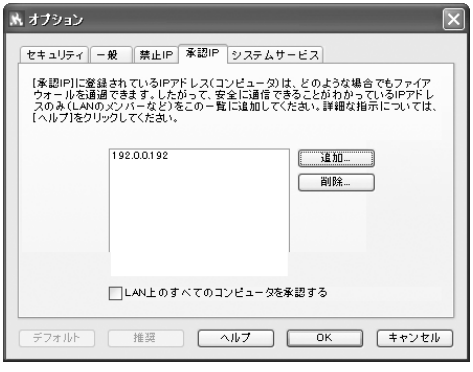
①［追加］をクリックします。



②常に承認するIPアドレスを入力して［OK］をクリックします。



③承認IPの一覧に、入力したIPアドレスが表示されます。



ヒント

オフィス用LANに接続されたコンピュータを使用しており、同じLANの別のコンピュータからのトラフィックを阻止する必要がない場合には、チェックボックスをオンにします。ただしこの機能はWindows95/98/98SE/Meでは使用できません。個別にIPアドレスを承認してください。

ヒント

［LAN上のすべてのコンピュータを承認する］にチェックを入れると、LAN内の接続が可能になります。

ヒント

メイン画面でログを選択して右クリックメニューやメニューバーの［アクセス］、またはアラートダイアログから［このIPアドレスを承認］を選択することでも登録が可能です。

ヒント

承認IPアドレスをクリックして、［削除］をクリックすると、リストから削除されます。

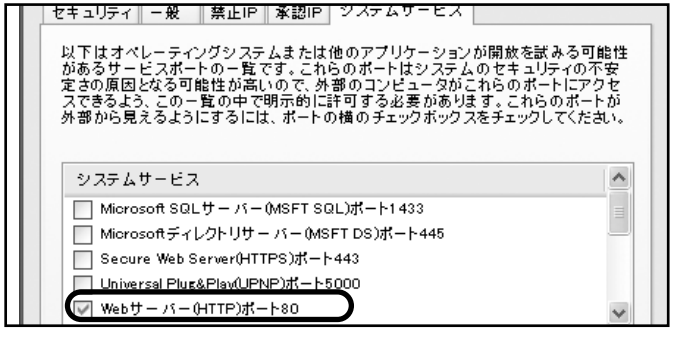
5-5

システムサービス

アプリケーションによっては、動作するために他のコンピュータから無条件に通信を受け入れなければならない場合があります。一般に、これらの接続はWebサイトホストやファイル共有などのサーバー的な役割をするソフトです。たとえば、電子メールを受信するためにポートを開く必要はありませんが、「McAfee.com パーソナルファイアウォール Plus」によって保護されているコンピュータが電子メールサーバーとして動作する場合、該当するアプリケーションアイテムをチェックして適切なポートを開く必要があります。ポートを開く必要があることを確認してからアプリケーションを開いてください。
一般的に利用されるアプリケーションとサーバーの多くは、あらかじめ登録してあります。

サーバー的な役割をするアプリケーションにポートを開く手順は以下のとおりです。

①［システムサービス］の一覧のシステムサービス名の横にあるチェックボックスをチェックします。



注意

アプリケーションの設定の変更を行なう場合、アプリケーション名や説明の変更は［編集］をクリックして直接入力してください。受信/送信ポートの変更の場合、新規にアプリケーションを追加してください。この場合以前のアプリケーションはチェックを外してください。

注意

UDP受信/送信ポートはセキュリティレベルを「厳重」に設定しているとほとんどのアクセスは阻止されます。レベルを「標準」に設定してご使用ください。

ヒント

ここに記入されていないものに関しては、お使いのアプリケーション（ユーティリティ）のメーカーに数値をお問い合わせください。当社の製品に関しての情報はhttp://www.sourcenext.com/support/をご覧ください。

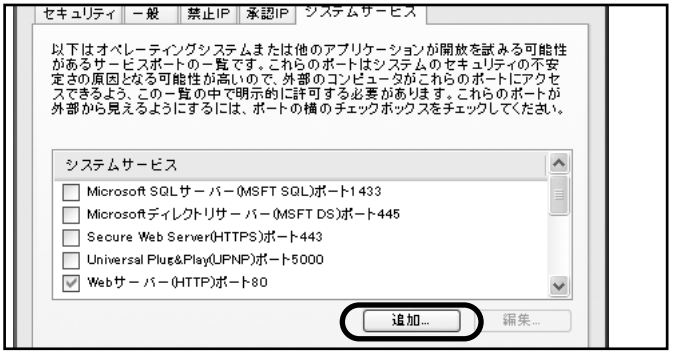
ヒント

連続した数値「1,2,3,4,5」を入力する場合は「1-5」（「-」ハイフン）。複数の数値「1と4」を入力する場合は「1,4」（「,」カンマ）をお使いください。

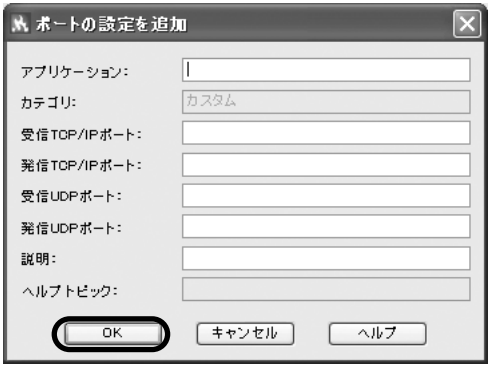
［システムサービス］の一覧にインターネットにアクセスするために必要なアプリケーションが定義されていない場合は［システムサービス］の一覧にアプリケーションを追加する必要があります。

※設定方法についてはp.22～23でも解説しておりますので、合わせてご参照ください。

②［追加］ボタンをクリックします。



③必要事項を入力して［OK］ボタンをクリックします。



第6章 「McAfee.com パーソナルファイアウォールPlus」のよくある質問

Q

ある決まったアプリケーション（ユーティリティ）が通信エラーになります。どうしたら通信ができるようになりますか？

A

あるアプリケーション（ユーティリティ）で通信エラーが出る場合は、そのアプリケーション（ユーティリティ）に対して、「McAfee.com パーソナルファイアウォールPlus」側で通信の承認をする必要があります。

方法は以下のとおりです。

①タスクトレイにある［セキュリティ・センター］アイコンを右クリックして、［Personal Firewall］→［オプション］を選択します。

②［システムサービス］タブをクリックします。

補足

初めから登録されているアプリケーションの一覧はヘルプをご覧ください。

補足

複数のアドレスを記入する場合はカンマ","で区切って記入してください。

補足

主なアプリケーションの値は次ページをご覧ください。一覧にない場合は、お使いのアプリケーション（ユーティリティ）のメーカーに数値をお問い合わせください。

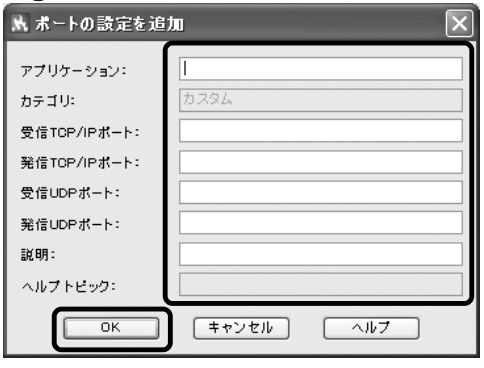
③一覧の中から通信を承認したいアプリケーションにチェックを入れます。

一覧に通信を承認したいアプリケーションが見つからない場合は以下の方法でアプリケーションを追加してください。

a.［追加］ボタンをクリックします。

b. 必要な項目を入れて［OK］ボタンをクリックします。

③-b

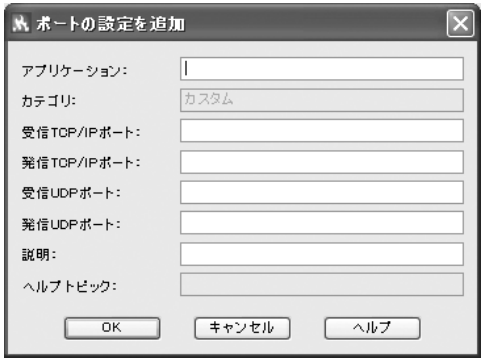


④［OK］ボタンをクリックします。

主なアプリケーションの設定値*

（いずれも［TCP/IP受信ポート］の欄にのみ入れます）

凄速シリーズ（2000/XPでのみ）"24491"
メールMAXSuite（2000/XPでのみ）　"25" "110"
消えるMail（2000/XPでのみ）　"25" "110"
見えないMail（2000/XPでのみ）"25" "110"
速いMail（2000/XPでのみ）　"25" "110"　XPモデム使用時3001も必要
凄速メールパワー（2000/XPでのみ）　"25" "110"
遠近コン1・2　"80" "8080"
WindowsActiveSync　"990""999" "5678" "5679"



Q

3COM製LANカードの3C595-TXを使っているのですが正常に動きません。なぜでしょうか？

A

3COM製LANカードの3C595-TXはWindows2000/XPに正式対応していませんので、動作は保証できません。Windows2000/XPに正式対応したLANカードをお使いください。

Q

Windows2000/XPに正式対応していないLANカードを使って一応動いているのですが、「McAfee.com パーソナルファイアウォールPlus」は正常に動きますか？

A

OSに正式に対応していないLANカードでは動作の保証はしておりません。ご注意ください。

Q

インストールやアンインストールでOSを再起動した後に、「アクティブデスクトップの修復」が表示されます。どうしたらいいでしょうか？

A

表示されている［修復する］をクリックすれば元どおりになります。

Q

ネットワークゲームをする場合の注意点は何でしょうか？

A

p.44の説明に従って「McAfee.com パーソナルファイアウォール Plus」側で通信の承認をする必要があります。ゲームごとの設定値はゲーム会社にお尋ねください。

Q

東京以外の場所を設定しているのに現在位置の設定が東京になってしまいます。どうすればよいでしょうか。

注意!!

ゲームをしていない時は設定を解除することをおすすめします。

A

［区/市/町/村］と［都/道/府/県］には一つの場所だけを入力してください。例えば“○○県XX郡△△市”であれば［区/市/町/村］には△△、［都/道/府/県］には○○を**半角ローマ字**で入れてください。またそれでも東京になってしまう場合はお近くの県庁所在地を入れてみてください。

Q

HackerWatch.orgが英語で表示されます。

A

インターネットエクスプローラーの言語設定に日本語以外の言語が登録されていると優先順位に関係なく英語で表示されます。
以下の方法で回避できます。
1.インターネットエクスプローラーを起動します。
2.メニューから［ツール］-［インターネットオプション］を選択します。
3.［全般］タブの［言語］をクリックします。
4.言語一覧に［日本語］のみ登録されているのを確認後［OK］をクリックしてください。

Q

［禁止IP］と［承認IP］に同じIPアドレスを登録できますか？

A

できません。もし何らかのタイミングで登録できた場合には［禁止IP］として動作します。

Q

［システムサービス］に登録されているアプリケーションを削除できますか？

A

できません。必要がない場合はチェックを外してお使いください。

Q

「McAfee.com パーソナルファイアウォールPlus」の何が新しいのですか?

A

McAfee.comは、「Personal Firewall Ver.4.1」に幾つかの大きな機能強化をしました。インターネット接続の際の操作性とセキュリティを強化するために、外部へのアクセスのフィルタリングとアプリケーション認証の仕組みを実装しました。これらの機能によっ

て、許可するアプリケーションを選択するだけでインターネットへの接続をプログラムごとにコントロールすることができます。つまりアプリケーション認証と外部への接続のフィルタリングによって、スパイウェアやトロイの木馬が勝手にデータを送信することを防ぎます。
また、これらの機能強化にともなって、McAfee.comはインターフェイスとアラート通知の仕組みを改良いたしました。

Q

なぜアプリケーションはインターネットに接続するのですか？

A

「McAfee.com パーソナルファイアウォールPlus」は、アプリケーションがインターネットへ通信をしようとする際に、その通信を検知しダイアログを表示します。ご利用されていることが確実なアプリケーションの場合、通信を許可してください。なお、アプリケーションは、次に掲げる動作を行なうためにインターネットに接続しようとします。設定をする際の参考にしてください。

・アプリケーションが「自動アップデート」するとき（Windows Updateなど。）
・アプリケーションがEmail、News、音楽データを、インターネット上のサーバーから取得するとき
・ライセンス登録－アプリケーションのライセンス管理のためライセンスサーバーへ認証を行なうとき
・インターネットに接続しようとした。－他のアプリケーションがインターネットに接続するために、一緒に動作をする(例；explorer.exe, rundll.exe, svchost.exe)とき

Q

なぜアプリケーションにはサーバー的な役割をするものがあるのですか？

A

アプリケーションがサーバー的な役割で外部からアクセスを受けるのは、未知の相手からの（匿名による）アクセスが行なわれる可能性がある際です。オンラインゲームや、インターネットメッセンジ

ャー、ファイル共有（P2Pソフト）がその典型的なものになります。未知の相手からの接続をアプリケーションが受け付ける仕様になっており、そのアプリケーションを利用する場合のみ許可することをおすすめします。なお、ゲームをやらない時には、そのゲームのアプリケーション許可レベルを厳しくするような使い方をすることで安全性が増します。「McAfee.com パーソナルファイアウォール Plus」を利用する際の参考にしてください。

Q

どんなときにシステムサービスを使ってポートを空けないといけないのですか？

A

システムサービスを使ってポートを空ける必要があるのはアプリケーションが他のコンピュータから未知の相手からの接続を許可しなければ成らない仕様になっているときのみです。（アプリケーション毎に通信状態を設定している場合には、再度ポート毎に設定する必要はありません。）
この設定を利用する場合は、以下のような例が含まれます。
・Mail Server: Emailを受け取るためにこの設定をする必要はありません。パソコンがメールサーバーの役目をするときのみです。
・Web Server: Webブラウザーを実行する為にこの設定をする必要はありません。パソコンがWebサーバーの役目をするときのみです。

Q

なぜ explorer.exe は、インターネットに接続しようとするのですか?

A

explorer.exe は、Internet ExplorerでFTPサイトをツリー表示する際に使われます。もし厳重セキュリティにするのでしたら、explorer.exe は外部へのアクセスのみに設定することをおすすめします。（全てのアクセスをexplorer.exeに対して与えないでください。）

Q

「McAfee.com パーソナルファイアウォールPlus」Ver4.1を入れたら（アップデートしたら）初めに何をすれば良いのですか?

A

「McAfee.com パーソナルファイアウォールPlus」を入れて初めにやらなければならないことは、インターネットに接続しようとするアプリケーションに許可レベルを設定することです。

はじめて「McAfee.com パーソナルファイアウォールPlus」をインストールした時には、複数のアプリケーションがインターネットへ接続しようとしてアラートダイアログが表示されることがあります。そのアプリケーションが信用できるものであるならば、許可する設定にしてください。

ひとつのアプリケーションにつき、ひとつのダイアログしか出てきませんので、あまり頻繁にアプリケーションアラートが表示されることはありません。アプリケーションの状態は「McAfee.com パーソナルファイアウォールPlus」の［アプリケーションの設定］ページに一覧表示されます。

主なアプリケーションについては、以下の表をご覧ください。

Windows95、98、98SE、Me、2000、XP（Home、Pro）共通

アプリケーション	[アプリケーション名]	[ファイル名]
【Explorer】	Windows Explorer	explorer.exe
【Internet Explorer】 （インターネットを閲覧する時）	Internet Explorer	Iexploer.exe
【Outlook Express】 （電子メールの送受信を行なう時）	Outlook Express	msimn.exe
【Microsoft 重要な更新の通知（Ver.4）】	Windows Critical Update Nofitication Windows Critical Update Nofitication	Wucrtupd.exe Wuloader.exe
【McAfee.com VirusScan Online】	McAfee.com Virus Map Report	mcvsmap.exe

Windows2000、XP（Home、Pro）のみ

アプリケーション	[アプリケーション名]	[ファイル名]
【LANやインターネットなどに接続する時】 （最初から登録されている場合があります）	Generic Host Process for Win32 Services Services and Controller App	svchost.exe services.exe

Q

"外部へのアクセスのみ許可" と "すべてのアクセスを許可" の違いは何ですか?

A

"外部へのアクセスのみ許可"では、アプリケーションがインターネット（ネットワークを含む）上のコンピュータと通信をする際に、データを受け取ることはできますが、こちらが要求していないデータは受け取らない設定です。
"すべてのアクセスを許可"では、アプリケーションが行なう通信のみならず、他のネットワーク上のコンピュータからの接続を可能にします。"すべてのアクセスを許可"の設定は、十分に注意して不必要に許可をしないようにすることをおすすめします。

※アクセスに対する設定を厳しくしすぎると、アプリケーションが正常に動かなくなることがあります。アプリケーションの動作に応じて設定することをおすすめします。

Q

なぜ"アプリケーションが変更された"アラートが表示されるの？

A

このアラートはアプリケーションに何かの変更があったときに表示されます。以下の例の場合には通信を許可してください。

・Waol.exe
AOL をご利用のユーザーでTODアップデートが行なわれた場合、次回AOL起動時に表示されます。
・Iexplorer.exe
Internet Explorerをご利用で自動アップデートを行なった場合、次回Internet Explorer 起動時に表示されます。
・Inetinfo.exe
IISをご利用で、最新パッチを当てた際に表示されます。

重要:アプリケーションのアップデートを行なっていないのにもかかわらず「アプリケーションが変更されました」とアラートが表示される場合、コンピュータウイルスやトロイの木馬に感染し

ている可能性があります。「McAfee.com ウイルススキャン オンライン」等のウイルス対策ソフトを使用して、一度お使いのパソコンをスキャンしてください。問題がないことを確認した後にアクセスの許可設定を変更してください。

Q

"セキュリティレベル"とは何ですか?

A

セキュリティレベルは、ユーザーが簡単に通信に対するセキュリティの度合いを5段階で変更できるようにあらかじめ設定したものです。各項目に対する説明は以下のとおりです。

接続を切る

アクセスはすべて遮断されます。 この設定は本質的にはインターネットへの接続を切断することと同じです。[オプション] ダイアログの [システムサービス] で開くように設定したポートも遮断されます。

厳重セキュリティ

あなたのパソコンからの接続要求に対する応答のみが許可されます。この設定では、UDPパケットを使用するアプリケーション（ビデオやオーディオをストリーミングするプログラムやゲーム）の多くは通信できません。 またインターネットへの接続が必要なアプリケーションが承認を要求しますので、[外部へのアクセスのみ許可] するか、ブロックするかを選択してください。 もし設定後にアプリケーションが [すべてのアクセスを許可] にすることを求めて来る時には、[すべてのアクセスを許可] するか、[外部へのアクセスのみ許可] を設定してください。この設定を使う際にはファイアウォールの利用法をきちんと理解した上で行ってください。

標準セキュリティ

(推奨設定) 通信を開始するパソコンだけがアクセスを返すことができます。UDPのアクセスは比較的緩やかに監視されています。アプリケーションはインターネットへ接続する最初の一回のみ、承認を求めてきます。その際には、[アクセスを許可] するか、[すべてのアクセスを拒否] するかを選択してください。 もし [アクセスを許可] した場合にはアプリケーションは非システムポートでの通信データを送受信できます。

承認

全てのアプリケーションがはじめてインターネットに接続しよう

とした時、自動的に通信が許可されます。（オプション設定で自動的に通信を許可せず、アラートダイアログを表示することも可能です。）ゲームまたはストリーミングメディアが動作しない場合はこの設定にすることをおすすめします。

完全に開放

ファイアウォールによる保護は無効です。 フィルタリングを行なわないで全てのアクセスが許可されます。

Q

HackerWatch.orgに送った情報は、どうなるの？

A

HackerWatch.orgのサーバーに送られたデータは、まずふるいを掛けられ解析されます。そのデータが実際に表示に反映されるには、数分から数時間の時間が掛かります。どのくらいのデータが送ってこられるかによって、その間に掛かる時間は差があります。なお解析済みの情報は［統計］ページに表示されます。

Q

「McAfee.com パーソナルファイアウォールPlus」のアクセスリスト内で色分けされたアクセス記録は何を意味するのですか？

A

・緑色のアクセス記録は、ローカル IP またはルーティング不可能な IP (たとえば 192.168.XXX.XXX) からのアクセスです。LANで使われているパソコンの場合は、このアクセスは正常なものと考えていただいて結構です。
・灰色のアクセス記録は、ループバック アダプタ (127.0.0.1) や無効な IP (0.0.0.0) など、改ざんされた可能性がある IP アドレスからのアクセスです。安全でないアクセスと確認されるまでは、許可しないことをおすすめします。
・赤色のアクセス記録は、禁止された IP アドレスからのアクセスです。

アクセス記録の説明領域にはヘルプのリンクも表示され、このヘルプによって、これらのソースからアクセスが表示された理由を確認できます。

Q

「McAfee.com パーソナルファイアウォールPlus」はインターネット接続を共有する環境で動作しますか？

A

Windowsの全てのバージョンについて、インターネット接続共有(ICS)に関するすべての問題が修正されました。Personal FirewallとICSとの競合はありません。

Q

「McAfee.com パーソナルファイアウォールPlus」はパソコンのパフォーマンスにどのような影響を及ぼしますか？

A

パフォーマンスへの影響はほとんどありません。一般に、リソースの消費と速度の低下は、2 つの原因で発生します。1つは、トラフィックを検査するフィルタがCPUを使用すること、もう1つは、このフィルタがパケットをブロックするか受け入れるかを判断する時間を必要とすることです。

CPUのオーバーヘッドは無視できます。負荷が重いシステムでも測定するのが困難なほどです。ただし、120MHz以下の古いパソコンでは、一定のオーバーヘッドが測定される可能性があります。

追加されるパケット レイテンシー(遅れ)は1ミリ秒未満であり、事実上ゼロと考えることができます。

Q

トロイの木馬とは何ですか？

A

インターネットからパソコンへのいたずらや悪意ある行為のほとんどは、リモートアクセスによるトロイの木馬（RAT:Remote Access Trojan)プログラムによるものです。

通常、トロイの木馬は、悪意のない動作を行なうように見えますが、

悪意ある動作をするプログラムです。かわいいアニメーションを表示したり、何らかのユーティリティのように見えることもあります。近年の有名になったトロイの木馬は、電子メール クライアントとして動くものでした。

トロイの木馬はどのようにしてパソコンに感染するのでしょうか？その答えは、パソコンの使用者がトロイの木馬を持ち込むということです。したがって、ソフトウェアの取得元に注意することが重要です。たとえば、チャットで知り合った人からソフトウェアをもらう時には気を付けてください。これはトロイの木馬を押しつけられる最も多いパターンです。これらはゲームなどのプログラムに見えるため、多くの人がだまされる手口です。

トロイの木馬の多くは、インターネットに接続されているかどうかにかかわりなく、パソコンを破壊する可能性があります。悪意のある人が作成したプログラムを実行すると、パソコンは簡単に他人に利用されてしまいます。

しかし自分をしっかりと守れるのは自分だけです。ウイルススキャン、ファイアウォールなどのソフトを信頼しすぎると、警戒心が緩みます。防弾チョッキを着ていても、注意しないで狩猟場を歩き回る人はいないはずです。それと同様に、常に外部からの攻撃に注意していることが重要になります。

次のことをよく念頭に置いてパソコンをご利用ください。

- トロイの木馬は、ファイアウォールだけでは阻止できません。また、トロイの木馬プログラムを実行してしまうと、「McAfee.com ウイルススキャンオンライン」などのウイルス対策ソフトによってブロックされない限り、トロイの木馬がシステムに感染します。
- トロイの木馬による被害を避ける唯一の方法は、信頼できないソース（発信源）からソフトをダウンロードしないことです。オンラインで知り合った人は、決して信頼されるソース（発信源）ではないことを覚えておいてください。

Q

「McAfee.com パーソナルファイアウォールPlus」は、Microsoft(R) Internet Information Services(IIS)に対応していますか?

A

「McAfee.com パーソナルファイアウォールPlus」はサーバー用としては作られておりません。その為、IISのセキュリティホールへの対策は含まれておりません。

IISをご利用の「McAfee.com パーソナルファイアウォールPlus」ユーザーはご自身の責任にてご利用ください。またセキュリティ修正プログラムの更新を、強くおすすめします。

Q

「ファイアウォールのテスト」を行なうと、NetBIOS ポートが開いていると表示されます

A

「McAfee.com パーソナルファイアウォールPlus」の「承認セキュリティ」、「標準セキュリティ」または「完全に開放」の設定を使用している場合、お客様のパソコンから開始したアクセスは全てのUDP 通信を受け入れます。つまり、お客様が上記の設定で「ファイアウォールのテスト」を行なうと（または　www.grc.com でファイアウォールのテストをすると)、UDP によるNetBIOSのスキャンに反応します。

この状態でも、未知のコンピュータやIPアドレスに対して通信を開始しない限り、危険ではありません。しかし、Kazaa、Napster や AIM などのファイル共有（ピアツーピア）ソフトを使用する場合は、注意する必要があります。

対策としては、WindowsOS のプロトコル設定で TCP/IP 上のNetBIOS (NetBIOS over TCP/IP)プロトコルを無効にするか、または「McAfee.com パーソナルファイアウォールPlus」の［オプション］ダイアログの［セキュリティ］タブで厳重セキュリティに設定してください。WindowsOSの設定方法は、Microsoftのマニュアルかwebサイトでご確認ください。

Q

記録に残っている情報に不明なIPからのアクセスが表示される。

A

何者かがIP アドレスを改ざんして「ping」をしてきた場合、「不明なIP」としてアクセス記録に表示されることがあります。この時には追跡することができません。しかし既にブロックされているので大丈夫です。その際に、あなたのパソコンやその中にある情報が相手に知られることはありませんので、安心していただいて結構です。

pingは、カタログ会社が使用する「切手と宛先付きの返信用封筒」に似ています。発信元のIPは「返信先の住所」に相当します。ping元は、返信先の住所を書いた封筒を送信し、受信者が自己の存在を示す1枚の紙切れをその封筒に入れて返信することを求めます。しかし、本当の住所が書かれていなければ、「McAfee.com パーソナルファイアウォールPlus」がブロックしなかった場合でも、ただ無効な住所に反応していることを返すだけです。

Q

ご使用のパソコンが何者かによってハッキングされている場合

A

「McAfee.com パーソナルファイアウォールPlus」からの警告は、必ずしもお客様のパソコンが誰かにハッキングされていることを示すわけではありません。
警告は、次の3つに分類されます。

アプリケーションが原因の警告：

最もよくある警告です。ご使用中のアプリケーションが原因で、アクセスを検出します。アクセスリストでアクセスに関する情報を確認してください。使用中のアプリケーションについてアクセス情報が記述されている場合には、オプションを変更して、この警告が再び表示されないように設定できます。

ランダム 探査（スキャニング）：

ご使用中のアプリケーションと関係がない警告が表示された場合でも、お客様が攻撃対象にされているとは限りません。多くのハッカー予備軍がスキャナーで不特定多数の IP アドレスにランダ

ムにアクセスしています。多くの悪質なプログラム作成者によってこのようなスキャニングが実行されているため、ほとんど毎日のようにヒットがあっても不思議ではありません。そのため、次の2点を念頭においてください。

・これらの探査（スキャニング）はランダムに行なわれていますので、あなたのパソコンがハッキング対象となっている訳ではありません。 ダイアルアップとブロードバンドによる接続を両方行なう設定を行なっている方は、アクセスが発生することがあります。これは、他のダイアルアップユーザーが使っていたIPアドレスが割り振られるために、他のユーザーが使っていたサービス（Emailなど）のアクセスが届くことがあります。「McAfee.com パーソナルファイアウォールPlus」はアクセスを既に止めていますので、安心していただいて結構です。

・「McAfee.com パーソナルファイアウォールPlus」は既に、これらの探査（スキャニング）によってパソコンが応答しないようにして、パソコンを保護します。（全てのアクセスを許可する設定以外。）このため、あなたパソコンは探査（スキャニング）プログラムには見えず、悪質なプログラム作成者もあなたのパソコンを認識することができません。

プロバイダによるアクセス：

プロバイダ業者（ISP）によっては、使用状況などの確認のためにユーザーに対して定期的にパソコンにアクセスする場合があります。ご契約のプロバイダのマニュアルやWebサイトを確認して、その際の「McAfee.com パーソナルファイアウォールPlus」の設定方法などを確認してください。

本当のハッキング：

上記のパターンに当てはまらず、 類似したアドレスもしくは特定のIPアドレスから繰り返しアクセスが発生している場合は、実際にあなたのパソコンが攻撃を受けている可能性があります。ただし、すでに攻撃は止められていますので、あなたのパソコンに対する全てのアクセスをHackerWatch.org へ報告する必要はありません。度重なるアクセスに悩まされる場合には、その IPアドレス を[禁止IP]に登録することをおすすめします。

用語集

A-Z

あ行

DSL（デジタル加入者回線）

高速インターネット接続の 1 つ。家庭や通常の電話回線を使用した小規模事業向けに用意されたものです。

圧縮

ファイルのサイズを小さくすることです。圧縮すると、インターネットへの接続時間も短縮されます。送信者が圧縮して送ったファイルは受信者が解凍することになるので、同じ圧縮・解凍ソフトを持っていることを確認してから送ると良いでしょう。圧縮するソフトはインターネットからもダウンロードができます。

アップグレード

ハードウェアやソフトウェアを新しいバージョンのものに取り換えて、より高機能なものにすることです。

アップデート

新しいものに「更新」することです。アプリケーションでは、古いバージョンから新しいバージョンに変更することでもあります。

アプリケーション

ワープロや表計算ソフトウェアなどの、ユーザーが目的に応じて使うものを総称して呼んでいます。

アンインストール

一度ハードディスクなどにインストールしたソフトウェアを削除することです。

アクセス

ネットワーク活動に関する事象。

インストール

Windowsでは「セットアップ」ともいいます。ハードウェアやソフトウェアを、コンピュータに組み込んで使えるようにすることです。最近のソフトウェアは、「インストーラー」がついていて簡単にインストールできるものが多くなっています。

ウィンドウ

ワープロソフトなどを起動すると、窓のような画面が開きますが、これを「ウィンドウ」と呼びます。開いたり閉じたり、窓のような

ところからこの名称がついています。

オンライン・ヘルプ

コンピュータの画面上から見ることができるマニュアルのことです。「McAfee.com パーソナルファイアウォールPlus」のヘルプがこれに当たります。

か行

拡張子

「拡張子」は、ファイルがどのような形式で作られているのか、どのソフトで作られているのかを表示するものです。ファイル名の最後にある、ピリオドに続く3～4文字が拡張子です。拡張子によって、そのファイルが文書なのか、プログラムなのか、画像なのか、といった情報を得ることができます。

クリック

マウスボタンを一度カチッと押すことです。
ダブルクリックは、すばやく2回続けて、カチカチッとボタンを押すことです。
右クリックは、マウスの右側のボタンを1回カチッと押すことです。デスクトップ上やアイコンの上などで右クリックすると、その時にできる操作が小さなメニューとなって現れます。

ケーブル モデム

従来のモデムやDSLのような電話回線の代わりにケーブル テレビのネットワークを介してデータをやり取りするモデムのことです。

さ行

再起動

Windowsをいったん終了して、もう一度起動することです。Windowsの［スタート］メニューから［Windowsの終了］を選択し、ダイアログの［再起動する］にチェックすると再起動します。

サーバー

他のコンピュータに自身の持っている機能やデータを提供するコンピュータのこと。他のユーザ間のファイルの共有を手助けするファイルサーバー。電子メールの送受信を一手に引き受けるメールサーバー等があります。

常駐ソフト

Windowsを起動したときから自動的に稼働しているアプリケーションで、タスクトレイにアイコンが入っています。そのアイコンを右クリックして出てくるメニューで終了や常駐解除などの操作がで

きます。

ショートカット

よく使うプログラムやファイルを簡単に開くことができる機能です。よく使うプログラムのショートカット・アイコンをデスクトップに置くなどしておくと、ファイルを探してたくさんのウィンドウを開いたり閉じたりしなくても済むので大変便利です。ひとつのオリジナルから、いくつでもショートカットは作れますが、実体はひとつです。ショートカット自身は分身なので実体ではありません。ですから、ショートカットだけを残して本物のファイルを削除してしまうと、ショートカットは本物を見つけられません。本物を削除したらショートカットも削除した方が良いでしょう。

信頼のおけるアプリケーション

「McAfee.com パーソナルファイアウォールPlus」において、安全であることがわかっており、ユーザーのコンピュータでインターネット接続を行なうことを承認されたアプリケーションのこと。これらのアプリケーションには、作業中のコンピュータでの必要なタスクを実行することが要求されます。

た行

ダイアログボックス

設定や操作の確認のために、一時的に表示されるウィンドウのことです。ファイルを削除しようとするときに、［ファイルを削除しますか？］という画面が表示されます。これがダイアログボックスです。

ダウンロード

他のコンピュータ上においてある情報を、自分のコンピュータに読み込むことです。

タスクトレイ

タスクバー右側の時計表示がある部分です。ここにアイコンが入っているアプリケーションは、常駐アプリケーションといい、Windowsを起動したときから自動的に稼働しているアプリケーションです。

タスクバー

画面の一番下に表示されている細長いバーのことです。現在実行中のプログラムが表示されています。

ドライブレター

ボリュームラベルとは違う（ボリュームラベルは自分好みの名前が付けられる）ドライブ固有に割り当てられたアルファベット。一般にフロッピーデイスクはAドライブ、C以降がハードディスクやCD-ROMドライブになっています。

ドラッグ& ドロップ

画面上のアイコンなどに矢印（マウスポインタ）を合わせてボタンを押したまま画面上で移動（移動することを「ドラッグ」といいます）して目的の場所に来たらマウスボタンを放します（放すことを「ドロップ」といいます）。そうするとアイコンやファイルが、その場所に移ります。アイコンの場所を変えるだけでなく、ファイルをコピーしたり、文書ファイルをプリンタのアイコンに重ねることで印刷できたり、用途はさまざまです。

トロイ（トロイの木馬）

ゲーム、ユーティリティ、などのアプリケーションを装った破壊的なプログラムのこと。トロイの木馬が実行されると、有効なプログラムの振りをしてコンピュータ システムに危害を及ぼします。

は行

バージョン

同一製品の改訂版を表す数字です。一般的に、数字が大きいほど最新版となります。大抵は「Ver.1.0、Ver.2.0、Ver.3.0」のように数字が増えていき、小さな改訂のときは「Ver.1.0、Ver.1.1、Ver.1.2」となります。

バージョンアップ

ソフトウェアやハードウェアを改訂·改版することです。バージョンアップした製品は、新しい機能を追加したり不具合な点を改善したりしています。

パケット

他のパケットと関連付けられた1つのデータ単位。インターネット上で送信されるファイルを構成します。ファイルはTCPプロトコルによってパケットに小分けにされてインターネットを介して送信されます。そして受信者側のコンピュータに到達すると、TCPによって再び組み立てられます。

フォルダ

ファイルをしまっておく入れ物のことです。ファイルをそれぞれのグループに分けて、整理して保存しておくことができます。

Windowsではディレクトリという言い方もしますが、Windows95からはフォルダと呼ばれるようになりました。フォルダは、必要に応じて自分で作ることができ、自由に名前をつけられます。

ま行

マウント

ドライブに入れたフロッピーディスクやCD-ROMなどをWindowsが認識（アイコンとして見える状態になる）して使える状態になることです。

ゆ行

ユーティリティ

コンピュータをさらに使いやすくしてくれるソフトウェアのことです。「McAfee.com パーソナルファイアウォールPlus」もユーティリティのひとつです。