McAfee®

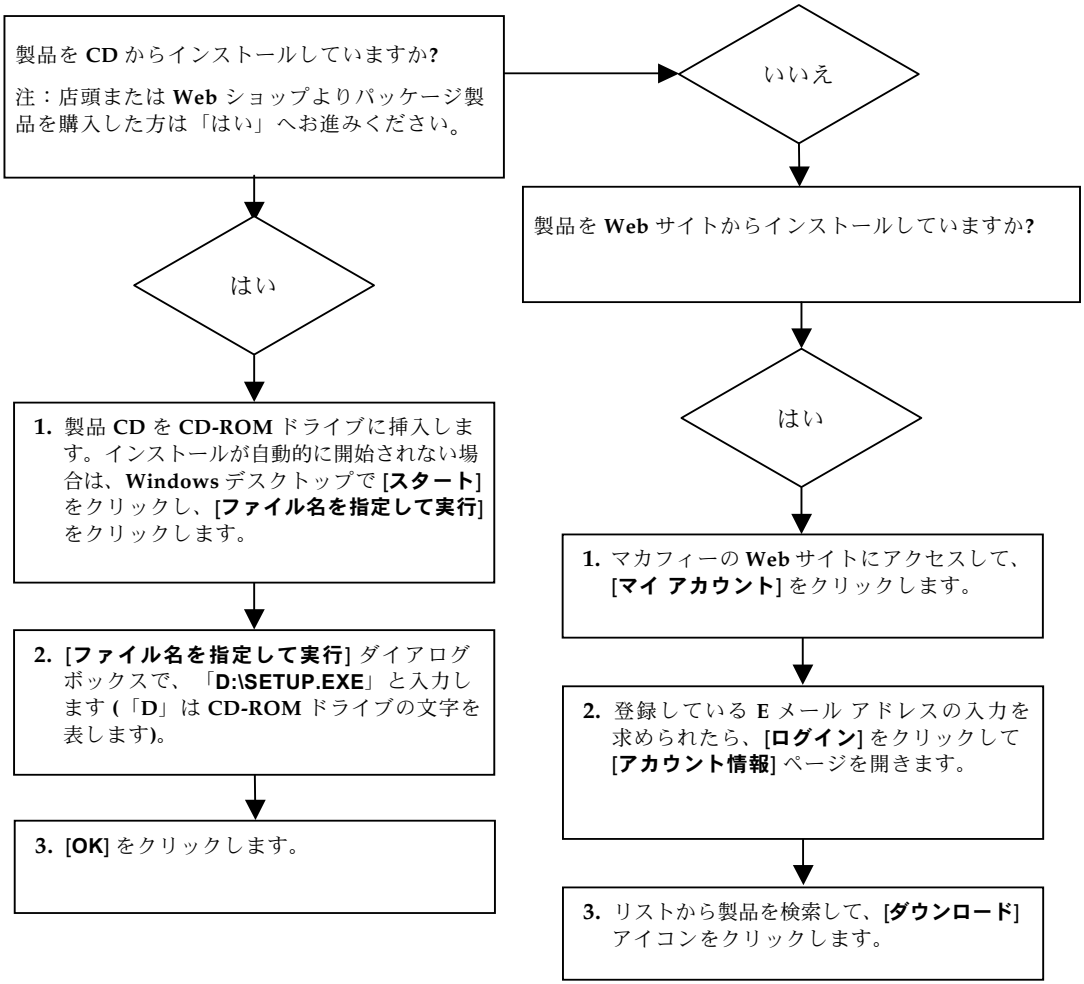
personal firewall plus

ユーザ ガイド

McAfee®

クイック スタート カード

CD または Web サイトから製品をインストールする場合は、本ページの内容を事前にご確認ください。尚、本ページのインストール手順は、各パソコン メーカのマカフィー プリインストール版をご利用のお客様は対象としておりません。インストールし直す必要がある場合は、各パソコン メーカが提供する手順書等をご確認ください。



詳細情報

ユーザ ガイドを表示するには、Acrobat Reader が必要です。インストールされていない場合は、McAfee の製品 CD から Acrobat Reader をインストールしてください (店頭または Web ショップよりパッケージ製品を購入したユーザが対象となります)。

1. 製品 CD を CD-ROM ドライブに挿入します。
2. Windows エクスプローラを開きます。Windows のデスクトップで **[スタート]** をクリックし、**[検索]** をクリックします。
3. 「マニュアル」フォルダを検索し、開くユーザ ガイドの PDF をダブルクリックします。

ユーザ登録の利点

製品の手順に従ってユーザ登録を直接送信することをお勧めします。ご登録いただくと、テクニカル サポート以外にも、次のような特典もご利用いただけます。

- Web、E メール、電話によるサポート
- McAfee VirusScan ソフトウェアご購入の際に、インストールから 1 年間、ウイルス定義ファイル (DAT) の更新提供

  次年度以降の更新料金については、http://jp.mcafee.com をご覧ください。
- McAfee SpamKiller ソフトウェアご購入の際に、インストールから 1 年間、McAfee SpamKiller フィルタの更新提供

  次年度以降の更新料金については、http://jp.mcafee.com をご覧ください。
- McAfee Internet Security Suite ソフトウェアご購入の際に、インストールから 1 年間、McAfee Internet Security Suite の更新提供

  次年度以降の更新料金については、http://jp.mcafee.com をご覧ください。

テクニカル サポート

テクニカル サポートが必要な場合は、http://www.mcafeehelp.jp/ にアクセスしてください。

目次

はじめに 1

McAfee Personal Firewall Plus へようこそ。

McAfee Personal Firewall Plus は、コンピュータと個人データを保護するための高度な機能を提供するソフトウェアです。McAfee Personal Firewall は、コンピュータとインターネットの間に障壁を確立し、インターネット トラフィックに不審な動作がないかどうかをバックグラウンドで監視します。

McAfee Personal Firewall Plus では、次の機能を使用できます。

- ハッカーのプローブと攻撃に対する防御
- 対ウイルス防御の補完
- インターネットおよびネットワーク アクティビティの監視
- 有害である可能性があるイベントのアラート発行
- 不審なインターネット トラフィックについて詳細情報の提供
- イベント レポート、自己テスト ツール、および E メールによるイベントのオンライン問い合わせなどを利用できる Hackerwatch.org 機能の統合
- 詳細な追跡機能とイベント調査機能の提供

新しい機能

- **Hackerwatch.org の統合強化**
  潜在的ハッカーのレポートが、これまで以上に簡単になりました。McAfee Personal Firewall Plus により、HackerWatch.org の機能性が向上し、有害な恐れがあるイベントをデータベースに送信できます。

- **アプリケーションの高度な知的処理**
  アプリケーションがインターネットにアクセスしようとすると、McAfee Personal Firewall は最初にアプリケーションをチェックし、信用できるかどうか、悪意のあるものであるかどうかを確認します。信用できることが確認されたアプリケーションは、McAfee Personal Firewall によってインターネットへのアクセスを自動的に許可されます。ユーザが許可する必要はありません。アプリケーションのデータベースによって、インターネットに接続している各アプリケーションの詳細を参照することができます。

- **トロイの木馬の高度な検出**
  McAfee Personal Firewall Plus では、アプリケーション接続管理機能と高度なデータベース機能が統合され、さらに多くの怪しいアプリケーションを検出 / ブロックできます。たとえば、トロイの木馬がインターネットにアクセスしてユーザの個人データに侵入することを防ぎます。

- **改善された追跡の表示**
  McAfee Personal Firewall Plus には、追跡の表示という侵入者追跡 ツールが組み込まれています。追跡の表示には、悪質な攻撃やトラフィックの発生元を示すグラフィカルで見やすい地図を表示する機能があり、発生元 IP アドレスの詳細な連絡先 / 所有者の情報と、コンピュータへの対応も表示されます。McAfee Personal Firewall Plus では、追跡の表示により多くの地理データが追加され、侵入者の発生場所をピンポイント式に示し、さらに詳細で視覚的な情報が得られます。追跡の表示によって、ユーザは侵入者の発生場所を視覚的に追跡できます。

- **使いやすさの向上**
  McAfee Personal Firewall Plus では、セットアップ アシスタントとユーザ チュートリアルによって、簡単にファイアウォールを設定し、使い方を学ぶことができます。この製品は、使用時に操作が必要ないように設計されていますが、ユーザにファイアウォールの機能を知っていただき、多いに活用していただけるようになっています。

- **高度な侵入検知**
  McAfee Personal Firewall Plus の侵入検知システム (IDS) は、一般的な攻撃タイプおよび不審な動作を検出します。侵入検知機能を有効にすると、すべてのデータ パケットが疑わしいデータの送信 / 受信メソッドの監視対象となり、イベント ログに記録されます。

- **高度なトラフィック分析**
  McAfee Personal Firewall Plus は、ユーザのコンピュータの受信データと送信データ、およびアプリケーション接続 (現在オープンな接続を「リスン (監視)」しているアプリケーションなど) を表示します。これにより、ユーザは侵入に対してオープンな状態になっているアプリケーションを表示して対応することができます。

システム要件

- Microsoft® Windows 98、Windows Me、Windows 2000 Pro、または Windows XP
- CPU:
  Windows 98、Windows ME — Pentium 150 MHz 以上
  Windows 2000 Pro、Windows XP — Pentium 233 MHz 以上
- 35MB のハードディスク空き容量 (インストール用)
- メモリ：
  Windows 98 — 32MB 以上 (64MB 推奨)
  Windows ME、Windows 2000 Pro、Windows XP — 64MB 以上 (128MB 推奨)
- Microsoft® Internet Explorer 5.5 以降

  注
  Internet Explorer の最新バージョンにアップグレードするには、Microsoft Web サイト (http://www.microsoft.com/japan) にアクセスしてください。

他のファイアウォールをアンインストールする

コンピュータ上に他のファイアウォール プログラムがインストールされている場合、McAfee Personal Firewall Plus をインストールする前に、それらをアンインストールする必要があります。アンインストール手順については、各ファイアウォール プログラムの手順に従ってください。

注

Windows XP を使用している場合、組み込みのファイアウォール機能を無効にしなくても、McAfee Personal Firewall Plus をインストールできます。ただし、無効にしてからインストールすることをお勧めします。無効にしないと、McAfee Personal Firewall Plus の受信イベント ログにイベントを受信できません。

デフォルト (標準の設定) のファイアウォールを設定する

McAfee Personal Firewall Plus では、コンピュータで Windows ファイアウォールが実行されていることを検出した場合でも、コンピュータのインターネット アプリケーションの許可とトラフィックを管理できます。

McAfee Personal Firewall Plus をインストールすると、Windows ファイアウォールが自動的に無効になり、デフォルト (標準の設定) のファイアウォールとして設定されます。すると、McAfee Personal Firewall Plus の機能とメッセージのみが有効になります。Windows セキュリティ センターまたは Windows コントロール パネルから Windows ファイアウォールを有効にして、両方のファイアウォールを同時に実行すると、状態およびアラート メッセージが重複するだけでなく、一部の McAfee Personal Firewall Plus ログ記録が失われる恐れがあります。

注

両方のファイアウォールを有効にすると、McAfee Personal Firewall Plus の [アクセス記録の表示] タブに、ブロックされたすべての IP アドレスが表示されなくなります。Windows ファイアウォールを使用するとこれらのイベントが無効になりブロックされてしまいます。McAfee Personal Firewall でイベントの検出およびログ記録ができなくなります。McAfee Personal Firewall Plus は別のセキュリティ機能に基づいてその他のトラフィックをブロックし、トラフィックをログに記録します。

ログ記録は Windows ファイアウォールでは、デフォルト (標準の設定) で無効になっています。ただし、両方のファイアウォールを有効にすると、Windows ファイアウォールのログ記録が有効になります。デフォルト (標準の設定) の Windows ファイアウォールのログは C:\Windows\pfirewall.log に保存されます。

McAfee Personal Firewall Plus をアンインストールするときに Windows ファイアウォールが自動で再有効化され、常にファイアウォールで常にコンピュータを保護している状態にします。

McAfee Personal Firewall Plus を無効にした場合、または Windows ファイアウォールを手動で有効化せずにセキュリティ設定を **[オープン]** にした場合、以前ブロックされたアプリケーション以外のすべてのファイアウォール保護が無効になります。

セキュリティ レベルを設定する

セキュリティ オプションを設定して、不要なトラフィックが検出された場合に McAfee Personal Firewall Plus が応答する方法を指定します。デフォルト (標準の設定) では、**[標準]** セキュリティ レベルが有効になっています。この設定は初心者のファイアウォール ユーザに適しています。上級のユーザなら、他の設定を使用することができます。**[標準]** セキュリティ レベルでは、アプリケーションがインターネット アクセスを要求しユーザがそれを許可するときに、アプリケーションにすべてのアクセスを承認します。すべてのアクセスでは、非システム ポートでアプリケーションによるデータの送信と不要なデータの受信を許可します。

セキュリティ設定を行うには

1. マカフィー・アイコンを右クリックし、**[Personal Firewall]** を選択してから **[ユーティリティ]** をクリックします。
2. **[セキュリティ設定]** アイコンをクリックします。
3. 選択するレベルにスライダを移動してセキュリティ レベルを設定します。

   初心者のファイアウォール ユーザの場合は、デフォルト (標準の設定) の **[標準]** 設定を使用します。セキュリティ レベルは、[ロック] から [オープン] まで変更できます。

   - **ロックダウン接続** — すべてのトラフィックが停止します。基本的に、インターネット接続を切断しているときと同じ状態です。[システム サービス] ページで開くように設定したポートをブロックすることができます。
   - **厳重セキュリティ** — アプリケーションは制限付きで使用するインターネットのアクセス タイプ (送信アクセスのみ、など) のみ要求し、ユーザはそれを許可またはブロックします。アプリケーションがすべてのアクセスを要求した場合、それを許可するか、送信アクセスのみに限定します。この設定は上級のファイアウォール ユーザに適しています。
   - **標準セキュリティ (推奨)** — アプリケーションがインターネット アクセスを要求しユーザがそれを許可するときに、アプリケーションにすべてのアクセスを承認します。すべてのアクセスでは、非システム ポートでアプリケーションによるデータの送信と不要なデータの受信を許可します。この設定は初心者のファイアウォール ユーザに適しています。
   - **信用セキュリティ** — 最初にインターネットにアクセスしようとするときに、すべてのアプリケーションが自動的に信用されます。ただし、コンピュータの新しいアプリケーションについてはアラートで通知するよう選択することもできます。ゲームやストリーミング メディアが動作しない場合などにこの設定を使用します。
   - **オープン** — ファイアウォールは無効になります。McAfee Personal Firewall Plus ではトラフィックはフィルタリングされません。

     注
     ファイアウォールが **[オープン]** セキュリティ設定または **[無効]** に設定されている場合、以前ブロックされたアプリケーションは引き続きブロックされます。この機能を無効にするには、アプリケーションの許可を **[すべてのアクセス]** に変更するか、**[許可]** リストで **[ブロック]** 許可ルールを削除します。

4 その他のセキュリティ設定を選択します。

注
コンピュータで Windows XP が実行されており、複数の XP ユーザが追加されている場合は、管理者権限でログインしているユーザのみこれらのオプションを利用できます。

- **受信イベント ログの侵入検知システム (IDS) の記録** — このオプションを選択すると、IDS で検出されたイベントは受信イベント ログに表示されます。侵入検知システムは、一般的な攻撃タイプおよび不審な動作を検出します。侵入検知機能を有効にすると、すべての受信 / 送信データ パケットが疑わしいデータ転送または転送メソッドの監視対象となります。そして、「署名」データベースと比較され、有害なコンピュータからのパケットを自動的に排除します。

  IDS は攻撃者が使用する特定のトラフィック パターンを検出します。IDS はマシンが受信するすべてのパケットを監視し、不審なトラフィックや攻撃を受けているトラフィックを検出します。たとえば、McAfee Personal Firewall が ICMP パケットを発見した場合、ICMP トラフィックを既知の攻撃パターンを比較して、不審なトラフィック パターンのパケットであるかどうかを分析します。

- **ICMP ping 要求の許可** — ICMP トラフィックは主に追跡や ping を実行するときに使用します。ping は通信を開始する前に簡単にテストするときに使用します。ピアツーピア ファイル共有プログラムを使用している場合、または使用していた場合は、ping を頻繁に使用します。このオプションを選択すると、受信イベント ログに ping をログせずに、すべての ping 要求を許可します。このオプションを選択しない場合、すべての ping 要求をブロックし、受信イベント ログに ping をログに記録します。

- **制限ユーザによる Personal Firewall Plus の設定変更を許可する** — コンピュータで Windows XP が実行されており、複数の XP ユーザが追加されているときに、制限された XP ユーザに McAfee Personal Firewall Plus 設定の変更を許可する場合は、このチェックボックスをオンにします。

5 変更が終了したら、**[OK]** をクリックします。

McAfee Personal Firewall Plus をテストする

McAfee Personal Firewall Plus をテストするには

1 マカフィー・アイコン  を右クリックして、**[Personal Firewall]** をポイントしてから、**[ファイアウォールをテスト]** をクリックします。

2 McAfee Personal Firewall Plus によって Internet Explorer が起動し、マカフィーが運営する Web サイトである http://www.hackerwatch.org/ が表示されます。[Hackerwatch.org Probe] ページに表示される指示に従って、McAfee Personal Firewall Plus をテストします。

注
ほとんどのオフィス ネットワーク (LAN) のように、プロキシ サーバまたはネットワーク アドレス変換 (NAT) サーバを経由してインターネットに接続している場合は、正しく読み取ることができません。Hackerwatch.org のファイアウォール テスト ツールは、ファイアウォールのテストを要求したコンピュータを探知し、そのコンピュータをテストします。プロキシ サーバまたは NAT サーバを経由してインターネットに接続している場合、サーバは各コンピュータからのファイアウォールテスト要求を単にリレーするだけなので、Hackerwatch.org は間違ったコンピュータをテストします。テストの結果は、対象のコンピュータではなくプロキシ サーバに関するものになります。

McAfee SecurityCenter を使用する

McAfee SecurityCenter では、Windows システム トレイにあるアイコンまたは Windows デスクトップからセキュリティに関するすべての操作を実行できます。McAfee SecurityCenter では、次の有用なタスクを実行できます。

- コンピュータのセキュリティ分析を行う
- 1 つのアイコンから McAfee 製品のサービスを起動、管理、設定する
- 最新のウイルス情報と最新の製品情報を表示する
- マカフィーの Web サイトにある FAQ (よくある質問) やアカウントの詳細に迅速にリンクする

注
McAfee SecurityCenter の機能の詳細については、**[McAfee SecurityCenter]** ダイアログ ボックスで **[ヘルプ]** をクリックしてください。

McAfee SecurityCenter が実行中で、コンピュータにインストールされている McAfee のすべての機能が有効になっている場合、赤色の [M] アイコン  が Windows のシステム トレイに表示されます。この領域は、通常は Windows デスクトップの右下隅にあり、時計が表示されています。

コンピュータにインストールされている McAfee アプリケーションが 1 つでも無効になっている場合は、マカフィー・アイコンは黒色  に変わります。

McAfee SecurityCenter を開くには

1 マカフィー・アイコン  を右クリックします。

2 **[SecurityCenter を開く]** をクリックします。

McAfee Personal Firewall Plus 機能にアクセスするには

1 マカフィー・アイコン  を右クリックします。

2 **[Personal Firewall]** をポイントし、使用する機能をクリックします。

McAfee Personal Firewall Plus を使用する

2

McAfee Personal Firewall Plus を開くには

マカフィー・アイコン を右クリックして **[Personal Firewall]** を選択し、**[概要]**、**[アプリケーションの設定]**、**[アクセス記録の表示]**、**[ユーティリティ]** のいずれかをクリックします。

[概要] ページについて

McAfee Personal Firewall Plus の [概要] ページは、[メイン概要]、[アプリケーションの概要]、[イベントの概要]、および [HackerWatch の概要] の 4 つがあります。これらのページには、最近の受信イベント、アプリケーションの状態、HackerWatch.org によってレポートされる世界規模での不正侵入アクティビティが表示されます。さらに、McAfee Personal Firewall Plus で実行される共通タスクへのリンクも表示されます。

McAfee Personal Firewall Plus の [概要] ページを開くには、マカフィー・アイコンを右クリックし、**[Personal Firewall]** を選択して **[概要]** をクリックします。[メイン概要] ページが表示されます (図 2-1)。

図 2-1 [メイン概要] ページ

別の [概要] ページへ移動するには、それぞれ以下のボタンをクリックします。

アイテム	説明
表示を変更	各ページのリストを開くには、**[表示を変更]** をクリックします。リストから、表示するページを選択します。
 右矢印	次の [概要] ページに移動するには、右矢印をクリックします。
 左矢印	前の [概要] ページに移動するには、左矢印をクリックします。
 ホーム	[ホーム] アイコンをクリックすると、**[メイン概要]** ページに戻ります。

[メイン概要] ページには次の情報が表示されます。

アイテム	説明
セキュリティ設定	セキュリティ設定の状態によって、ファイアウォールの設定のセキュリティ レベルが分かります。セキュリティ レベルを変更するには、リンクをクリックします。
ブロックされたイベント	ブロックされたイベントの状態として、その日にブロックされたイベントの数が表示されます。[アクセス記録の表示] ページのイベント詳細を表示するには、リンクをクリックします。
アプリケーション ルールの変更	アプリケーション ルールの状態として、最近変更されたアプリケーション ルールの数が表示されます。許可されたアプリケーションおよびブロックされたアプリケーションのリストを表示し、許可するアプリケーションを変更するには、リンクをクリックします。
新しく許可されたアプリケーション	**[新しく許可されたアプリケーション]** には、インターネットへの完全なアクセスを許可された最新のアプリケーションが表示されます。
最新のイベント	**[最新のイベント]** には、最新の受信イベントが表示されます。イベントを追跡したり、IP アドレスを信用したりするには、それぞれリンクをクリックします。IP アドレスを信用すると、ユーザのコンピュータがその IP アドレスからのトラフィックをすべて受信します。
デイリー レポート	**[デイリー レポート]** には、McAfee Personal Firewall Plus によってその日、週、月にブロックされた受信イベントの数が表示されます。[アクセス記録の表示] ページのイベント詳細を表示するには、リンクをクリックします。
アクティブな アプリケーション	**[アクティブなアプリケーション]** には、現在コンピュータで実行され、インターネットにアクセスしているアプリケーションが表示されます。各アプリケーションをクリックすると、そのアプリケーションの接続先 IP アドレスが表示されます。
共通タスク	**[共通タスク]** のリンクをクリックすると、ファイアウォールの動作を表示してタスクを実行できる McAfee Personal Firewall Plus のページへ移動します。

[アプリケーションの概要] ページを表示するには、**[表示の変更]** をクリックし、**[アプリケーションの概要]** を選択します。[アプリケーションの概要] ページには次の情報が表示されます。

アイテム	説明
トラフィックの監視	**[トラフィックの監視]** には、ユーザのコンピュータの過去 10 分間のインターネット接続による受信 / 送信トラフィック量が表示されます。トラフィックの監視の詳細を表示するには、グラフをクリックします。
アクティブなアプリケーション	**[アクティブなアプリケーション]** には、ユーザのコンピュータにおいて過去 24 時間に最も実行中のアプリケーションが使用している帯域幅の使用率を表しています。 **アプリケーション** — インターネットにアクセスしているアプリケーション **%** — アプリケーションによる帯域幅の使用率 **許可** — アプリケーションに許可されているインターネット アクセスの種類 **作成日** — アプリケーション ルールが作成された日
新しく許可されたアプリケーション	**[新しく許可されたアプリケーション]** には、インターネットへの完全なアクセスを許可された最新のアプリケーションが表示されます。
アクティブなアプリケーション	**[アクティブなアプリケーション]** には、現在コンピュータで実行され、インターネットにアクセスしているアプリケーションが表示されます。各アプリケーションをクリックすると、そのアプリケーションの接続先 IP アドレスが表示されます。
共通タスク	**[共通タスク]** のリンクをクリックすると、アプリケーションの状態を表示してアプリケーションに関連するタスクを実行できる McAfee Personal Firewall Plus のページへ移動します。

[イベントの概要] ページを表示するには、**[表示の変更]** をクリックし、**[イベントの概要]** を選択します。[イベントの概要] ページには次の情報が表示されます。

アイテム	説明
ポート比較	**[ポート比較]** には、使用しているコンピュータで過去 30 日間に最も頻繁に侵入が試みられたポートの円グラフが表示されます。ポート名をクリックすると、[アクセス記録の表示] ページの詳細情報が表示されます。さらに、マウス ポインタをポート番号に合わせると、ポートの説明が表示されます。
最も頻繁な攻撃	**[最も頻繁な攻撃]** には、頻繁にブロックされた IP アドレス、各アドレスに対する最近の受信イベント発生日、各アドレスからの過去 30 日間の受信イベント数が表示されます。[アクセス記録の表示] ページのイベント詳細を表示するには、イベントのリンクをクリックします。
デイリー レポート	**[デイリー レポート]** には、McAfee Personal Firewall Plus によってその日、週、月にブロックされた受信イベントの数が表示されます。受信イベント ログのイベント詳細を表示するには、数のリンクをクリックします。
最新のイベント	**[最新のイベント]** には、最新の受信イベントが表示されます。イベントを追跡したり、IP アドレスを信用したりするには、それぞれリンクをクリックします。IP アドレスを信用すると、ユーザのコンピュータがその IP アドレスからのトラフィックをすべて受信します。
共通タスク	**[共通タスク]** のリンクをクリックすると、イベントの詳細を表示してイベントに関連するタスクを実行できる McAfee Personal Firewall Plus のページへ移動します。

[HackerWatch の概要] ページを表示するには、**[表示の変更]** をクリックし、**[HackerWatch の概要]** を選択します。[HackerWatch の概要] ページには次の情報が表示されます。

アイテム	説明
ワールド アクティビティ	**[ワールド アクティビティ]** には、最近 HackerWatch.org によってレポートされたブロック対象アクティビティを示す世界地図が表示されます。地図をクリックすると、HackerWatch.org の [アクセス発生源地図] が開きます。
イベント数	**[イベント数]** には、HackerWatch.org にレポートされた受信イベントの数が表示されます。
グローバル ポート アクティビティ	**[グローバル ポート アクティビティ]** には、過去 5 日間に攻撃とみなされるアクティビティが最も多く発生したポートが表示されます。ポートのリンクをクリックすると、ポート番号とポートの説明が表示されます。
共通タスク	**[共通タスク]** のリンクをクリックすると、世界規模のハッカーの活動に関する詳細な情報が表示されている HackerWatch.org の Web ページが表示されます。

[アプリケーションの設定] ページについて

[アプリケーションの設定] ページを使用して、許可されているアプリケーションとブロックされているアプリケーションのリストを表示します。

マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アプリケーションの設定]** をクリックします。[アプリケーションの設定] ページが表示されます (図 2-2)。

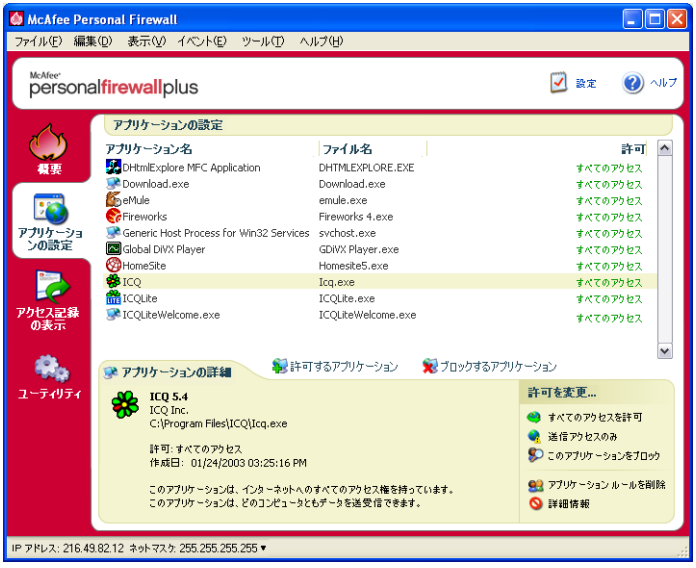


図 2-2 [アプリケーションの設定] ページ

[アプリケーションの設定] ページには次の情報が表示されます。

- アプリケーション名
- ファイル名
- 現在の許可レベル
- アプリケーションの詳細 : パス名、許可のタイム スタンプ、許可のタイプの説明

許可を変更する

McAfee Personal Firewall Plus を使用すると、インターネット アクセスを必要とするアプリケーション別に許可レベルを設定できます。

許可レベルを変更するには

1. マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アプリケーションの設定]** をクリックします。
2. **[許可]** リストで、アプリケーションの許可レベルを右クリックし、別のレベルを選択します。
   - アプリケーションにデータの送受信の両方を許可するには、**[すべてのアクセスを許可]** をクリックします。
   - アプリケーションによるデータの受信を防止するには、**[送信アクセスのみ]** をクリックします。
   - アプリケーションによるデータの送受信を防止するには、**[このアプリケーションをブロック]** をクリックします。

     注
     ファイアウォールが **[オープン]** セキュリティ設定または **[無効]** に設定されている場合、以前ブロックされたアプリケーションは引き続きブロックされます。この機能を無効にするには、アプリケーションの許可を **[すべてのアクセス]** に変更するか、**[許可]** リストで **[ブロック]** 許可ルールを削除します。

許可のレベルを削除するには、次の手順に従います。

1. マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アプリケーションの設定]** をクリックします。
2. **[許可]** リストで、アプリケーションの許可レベルを右クリックし、**[アプリケーション ルールを削除]** をクリックします。

次にアプリケーションがインターネット アクセスを要求したときに、その許可レベルを設定し、リストに再び追加できます。

アプリケーションを変更する

許可またはブロックされるインターネット アプリケーションのリストを変更するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アプリケーションの設定]** をクリックします。

2 **[アプリケーション名]** リストにアプリケーションを追加するか、アプリケーションをこのリストから削除します。

- 新規の「許可する」アプリケーションを追加するには、**[許可するアプリケーション]** をクリックし、許可するアプリケーションを選択して、**[開く]** をクリックします。
- 新規の「ブロックする」アプリケーションを追加するには、**[ブロックするアプリケーション]** をクリックし、ブロックするアプリケーションを選択して、**[開く]** をクリックします。
- リストからアプリケーションを削除するには、**[アプリケーション ルールを削除]** をクリックします。

[アクセス記録の表示] ページについて

[アクセス記録の表示] ページには、McAfee Personal Firewall Plus が迷惑なインターネット トラフィックをブロックしたときに作成される受信イベント ログを表示できます。

マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。[アクセス記録の表示] ページが表示されます (図 2-3)。

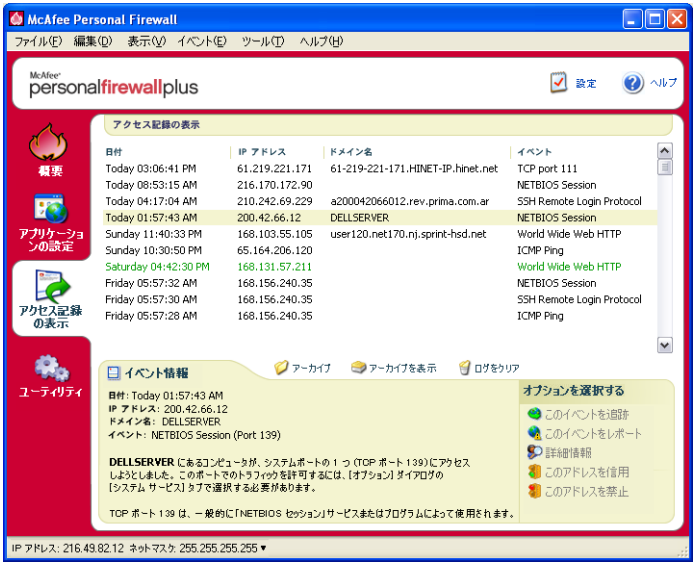


図 2-3 [アクセス記録の表示] ページ

[アクセス記録の表示] ページには次の情報が表示されます。

- タイムスタンプ
- ソース IP
- ホスト名
- サービスまたはアプリケーション名
- イベントの詳細 : 接続タイプ、接続ポート、ポート イベントの説明

イベントを理解する

IP アドレスについて

IP アドレスは、0 から 255 までの 4 つの数字で構成されます。これらの数値は、インターネット上でトラフィックを送信可能な特定の場所を示します。

特別な IP アドレス

IP アドレスの中には、特殊なものがいくつかあります。

ルート不可 IP アドレス —「個人 IP スペース」とも呼ばれます。これらはインターネット上では使用できない IP アドレスです。個人 IP ブロックは 10.x.x.x、172.16.x.x ～ 172.31.x.x、192.168.x.x です。

ループバック IP アドレス — テストの目的に使用されます。この IP アドレスのブロックに送信されたトラフィックは、パケットを生成したデバイスにすぐ返されます。この IP アドレスはデバイスと切り離されることなく、主にハードウェアとソフトウェアのテストに使用されます。ループバック IP のブロックは 127.x.x.x です。

Null IP アドレス — これは無効なアドレスです。このアドレスが表示された場合、トラフィックに空の IP アドレスがあったことを示しています。これは明らかに正常でなく、多くは送信者が故意にトラフィックの発信元を曖昧にしていることを意味します。アプリケーションに対する特別の指示を含むパケットの内容を理解するアプリケーションによってパケットが受信されない限り、送信者はそのトラフィックに対する応答を受信できません。0 で始まるアドレス (0.x.x.x) は、すべて Null アドレスです。たとえば、0.0.0.0 は Null IP アドレスです。

0.0.0.0 からのイベント

IP アドレス 0.0.0.0 からのイベントが発生する状況には、2 つの原因が考えられます。まず最も一般的な原因は、何らかの理由によって、使用中のコンピュータが不適切に形成されたパケットを受信したことです。インターネットは常に 100% 信頼がおけるわけではなく、したがって不適切なパケットが発生することがあります。McAfee Personal Firewall Plus は、TCP/IP がパケットを検証する前にパケットを認識するため、これらのパケットがイベントとして報告されることがあります。

もう一方の状況は、ソース IP がスプーフ、つまり偽装されたものであるときに起こります。スプーフされたパケットは、誰かがトロイの木馬を探してスキャンしている徴候であり、その対象が偶然使用中のコンピュータになった場合です。このような行為は、McAfee Personal Firewall Plus によってブロックされるため、ユーザのコンピュータは安全に守られます。

127.0.0.1 からのイベント

ソース IP が 127.0.0.1 と記されているイベントがあります。この IP は特別であり、ループバック アドレスと呼ばれることに注意してください。

基本的には、どのようなコンピュータを使用している場合でも、127.0.0.1 は常に自分自身を指します。このアドレスは「localhost」とも呼ばれます。これは、コンピュータ名 localhost が常に IP アドレス 127.0.0.1 に解決されるためです。

これは自分のコンピュータが自分自身に侵入しようとしていることを意味するのでしょうか ? トロイの木馬やスパイウェアによってコンピュータが乗っ取られているのでしょうか ? そうではありません。多くの合法的なプログラムがコンポーネント間の通信用にループバック アドレスを使用しています。たとえば、多くの個人メールや Web サーバを設定するには、http://localhost/ などからアクセスできる Web インターフェイスを使用します。

ただし、McAfee Personal Firewall Plus はこのようなプログラムからのトラフィックを許可することから、127.0.0.1 からのイベントが表示された場合、多くはソース IP アドレスが「スプーフ」、つまり偽装されたものであることを意味します。スプーフされたパケットは通常の場合、誰かがトロイの木馬をスキャンしていることの兆候です。このような行為は、McAfee Personal Firewall Plus によってブロックされるため、ユーザのコンピュータは安全に守られます。127.0.0.1 からのイベントのレポートは、意味がないため必要ありません。

ただし、Netscape 6.2 以上をはじめとする一部のプログラムでは、127.0.0.1 を [信用 IP] リストに追加する必要があります。そのようなプログラムのコンポーネントは、トラフィックがローカルであるかどうかを McAfee Personal Firewall Plus が判断できない方法で相互に通信します。

Netscape 6.2 の場合、127.0.0.1 を信用しなければ、友人に関するリストを使用できません。したがって、127.0.0.1 からのトラフィックがあり、コンピュータ上のすべてのアプリケーションが正常に動作している場合、このトラフィックをブロックしても安全です。ただし、Netscape などの プログラムで問題が発生している場合は、McAfee Personal Firewall Plus の [信用 IP] リストに 127.0.0.1 を追加し、問題が解決されたかどうかを確認します。

[信用 IP] リストに 127.0.0.1 を追加することで問題が解決する場合、次の 2 つの選択肢を比較検討する必要があります。127.0.0.1 を信用した場合、プログラムは動作しますが、スプーフ攻撃に対してよりオープンになります。このアドレスを信用しない場合、プログラムは動作しませんが、そのような悪意のあるトラフィックからこれまで通り保護されます。

ユーザの LAN 上のコンピュータからのイベント

ローカル エリア ネットワーク (LAN) 上のコンピュータからイベントが生成されることがあります。McAfee Personal Firewall Plus では、このようなイベントは、「自分のコンピュータの近く」から送信されていることを示すために緑色で表示されます。

多くの企業内 LAN の設定では、[信用 IP] オプションで **[LAN 上のすべてのコンピュータを信用]** を選択する必要があります。

ただし、状況によっては、「ローカル」ネットワークが外部のネットワークと同じくらい、またはそれ以上に危険な場合があります。DSL やケーブル モデムなどの広帯域幅の公共ネットワークを使用している場合、これは特に注意が必要な点です。このような場合は、**[LAN 上のすべてのコンピュータを信用]** オプションを選択しないことをお奨めします。

ブロードバンドに接続された家庭用ネットワークを使用している場合、代わりにご使用のローカルコンピュータの IP アドレスを [信用 IP アドレス] リストに手動で追加します。ブロック全体を信用するには .255 形式のアドレスを使用できます。たとえば、IP 192.168.255.255 を信用することで、ICS (Internet Connection Sharing) ネットワーク全体を信用できます。

プライベート IP アドレスからのイベント

192.168.xxx.xxx、10.xxx.xxx.xxx というフォーマットの IP アドレス、および 172.16.0.0 - 172.31.255.255 の IP アドレスは、ルート不可 IP アドレスまたはプライベート IP アドレスと呼ばれます。これらの IP アドレスはご使用のネットワークと密着しているので、ほとんどの場合信頼することができます。

ブロック 192.168 は Microsoft Internet Connection Sharing (ICS) で使用されます。ICS の使用中にこの IP ブロックからのイベントが発生した場合は、IP アドレス 192.168.255.255 を [信用 IP アドレス] リストに追加してください。これによって、192.168.xxx.xxx ブロック全体を信頼することになります。

プライベートネットワーク以外でこれらの IP の範囲からのイベントが発生した場合、ソース IP アドレスが「スプーフ」、つまり、偽装されている可能性があります。スプーフされたパケットは通常の場合、誰かがトロイの木馬をスキャンしていることの兆候です。このような行為は、McAfee Personal Firewall Plus によってブロックされるため、ユーザのコンピュータは安全に守られます。

プライベート IP アドレスは接続されているネットワークによって異なるコンピュータを指すことがあり、これらのイベントをレポートしても効果がないので、レポートの必要はありません。

受信イベント ログのイベントを表示する

受信イベント ログでは、さまざまな方法でイベントを表示できます。デフォルト (標準の設定) では、その日に発生したイベントのみが表示されます。これを変更して、過去 1 週間のイベントや、すべてのイベントを表示することもできます。

さらに、特定の日の受信イベント、特定のインターネット アドレス (IP アドレス) からの受信イベント、または同じイベント情報を持つイベントだけを表示することもできます。

イベントの情報については、イベントをクリックするとその情報が [アクセス記録の表示] ページ下部の **[イベント情報]** 領域に表示されます。

今日のイベントを表示する

今日発生したイベントだけを表示するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 **[表示]** メニューで、**[今日のイベントの表示]** をクリックします。

受信イベント ログに、その日に発生したイベントだけが表示されます。

今週のイベントを表示する

今週発生したイベントを表示するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 **[表示]** メニューで、**[今週のイベントの表示]** をクリックします。

受信イベント ログに、その週に発生したイベントだけが表示されます。

すべての受信イベント ログを表示する

受信イベント ログ内のすべてのイベントを表示するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 **[表示]** メニューで、**[完全なログを表示]** をクリックします。

[アクセス記録の表示] ページに、アーカイブを除く、受信イベント ログのすべてのイベントが表示されます。

選択した日のイベントだけを表示する

これは、特定日のイベントだけを表示する場合に役立ちます。その日に発生していないイベントはすべて非表示になります。

特定日のイベントすべてを表示するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 **[表示]** メニューで、**[選択した日のイベントだけを表示]** をクリックします。

その日のイベントが受信イベント ログに表示されます。

選択したインターネット アドレスのイベントだけを表示する

これは、特定のインターネット アドレスで発生した他のイベントを調べる必要がある場合に役立ちます。他のすべてのイベントは非表示になります。

特定のインターネット アドレスのすべてのイベントを表示するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 **[表示]** メニューで、**[選択したインターネット アドレスのイベントだけを表示]** をクリックします。

選択したインターネット アドレスで発生したイベントが受信イベント ログに表示されます。

イベント情報が同じイベントだけを表示する

これは、受信イベント ログ内に、**[イベント情報]** 列に選択したイベントと同じイベント情報をもつイベントが存在するかどうかを調べる場合に役立ちます。このイベントが何回発生したか、また同じソースからのイベントかどうかを調べることができます。[イベント情報] 列には、イベントの説明と、そのポートを使用する共通のプログラムまたはサービス (既知の場合) が表示されます。

同じイベント情報をもつすべてのイベントを表示するには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 **[表示]** メニューで、**[イベント情報が同じイベントだけを表示]** をクリックします。

同じイベント情報を持つイベントだけが受信イベント ログに表示されます。

受信イベントに対応する

受信イベント ログのイベントの詳細を表示できるだけではなく、受信イベント ログのイベントについて IP アドレスのビジュアル 追跡を実行したり、ハッカー対策オンライン コミュニティ、HackerWatch.org の Web サイトでイベントの詳細を確認したりすることもできます。

選択したイベントを追跡する

受信イベント ログのイベントについて、IP アドレスの追跡の表示を実行できます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 追跡するイベントを右クリックし、**[選択したイベントを追跡]** をクリックします。

追跡の対象となるイベントをダブルクリックして実行することもできます。

McAfee Personal Firewall Plus では、デフォルト (標準の設定) では組み込みの追跡の表示 プログラムによる追跡が実行されます。

HackerWatch.org からアドバイスを取得する

次の手順を実行することで、ハッカー対策オンライン コミュニティ、HackerWatch.org からイベントの詳細情報を取得できます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 詳細情報を取得するイベントを検索してクリックします。

3 **[イベント]** メニューの **[イベントの詳細]** をクリックします。

Web ブラウザが開き、HackerWatch.org の Web サイト (http://www.hackerwatch.org/) が表示されます。ここに、イベント タイプの詳細情報とそのイベントをレポートすべきかどうかに関するアドバイスが表示されます。

イベントをレポートする

コンピュータへの攻撃と思われるイベントをレポートするには

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 レポートするイベントをクリックし、右下のペインで **[このイベントをレポート]** をクリックします。

ユーザ固有の ID を使用して、イベントが HackerWatch.org の Web サイトにレポートされます。

HackerWatch.org にサインアップする

McAfee Personal Firewall Plus は、[概要] ページが初めて開かれたとき、HackerWatch.org に接続してユーザ固有の ID を生成します。既存ユーザの場合は、サインアップが自動的に認証されます。新規ユーザは、ニックネームと E メールアドレスを入力し、HackerWatch.org からの確認 E メールの認証リンクをクリックし、この Web サイトでイベント フィルタ /E メール機能を使用できるようにしなければなりません。

ユーザ ID を認証しないで HackerWatch.org にイベントをレポートすることもできます。ただし、イベントをフィルタし、他のユーザに E メールで送信するには、このサービスにサインアップする必要があります。

サービスにサインアップすると、登録情報をトラックし、HackerWatch.org がユーザから詳細な情報やアクションを必要とする場合にユーザに通知できます。受信したすべての情報が有効であることを確認するためにも、ユーザはサインアップを行う必要があります。

HackerWatch.org に提供された E メール アドレスはすべて機密情報として管理されます。ISP から追加情報が求められた場合、その要求は HackerWatch.org に転送され、ユーザの E メールアドレスが公開されることはありません。

アドレスを信用する

許可する必要がある IP アドレスを含むイベントが受信イベント ログに表示されている場合、その IP アドレスからの接続を常に許可するように McAfee Personal Firewall Plus を設定できます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 信用する IP アドレスを含むイベントを右クリックし、**[ソース IP アドレスを信用]** をクリックします。

3 [このアドレスを信用] 確認メッセージに表示される IP アドレスが正しいことを確認し、**[OK]** をクリックします。

この IP アドレスが **[信用 IP アドレス]** リストに追加されます。

IP アドレスが追加されたことを確認するには

1 **[ユーティリティ]** タブをクリックします。

2 **[信用 IP アドレスと禁止 IP アドレス]** アイコンをクリックし、続いて **[信用 IP アドレス]** タブをクリックします。

[信用 IP アドレス] リストにこの IP アドレスが表示されます。

アドレスを禁止する

IP アドレスが受信イベント ログに表示される場合、そのアドレスからのトラフィックがブロックされたことが分かります。したがって、コンピュータがシステム サービス機能を使用して意図的に開かれたポートを備えている場合やトラフィック受信許可のあるアプリケーションを備えている場合を除き、アドレスを禁止しても保護は追加されません。

意図的に開かれたポートがあり、特定の IP アドレスがそれらのポートからアクセスできないようにブロックする必要のある場合にのみ、禁止リストにその IP アドレスを追加します。

禁止する IP アドレスを含むイベントが受信イベント ログに表示されている場合、その IP アドレスからの接続を常に防止するように McAfee Personal Firewall Plus を設定できます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 禁止する IP アドレスを含むイベントを右クリックし、**[ソース IP アドレスを禁止]** をクリックします。

3 [このアドレスを禁止] 確認メッセージに表示される IP アドレスが正しいことを確認し、**[OK]** をクリックします。

この IP アドレスが **[禁止 IP アドレス]** リストに追加されます。

IP アドレスが追加されたことを確認するには

1 **[ユーティリティ]** タブをクリックします。

2 **[信用 IP アドレスと禁止 IP アドレス]** アイコンをクリックし、続いて **[禁止 IP アドレス]** タブをクリックします。

その IP アドレスが **[禁止 IP アドレス]** リストに表示されます。

受信イベント ログを管理する

[アクセス記録の表示] ページでは、McAfee Personal Firewall Plus により迷惑なインターネット トラフィックがブロックされたときに作成される受信イベント ログを管理できます。

受信イベント ログのアーカイブを作成する

現在の受信イベント ログのアーカイブをハード ドライブ上のファイルに作成できます。イベント ログは非常に大きくなる可能性があるため、イベント ログのアーカイブを定期的に作成することをお勧めします。

受信イベント ログのアーカイブを作成するには

1. マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。
2. **[ファイル]** メニューの **[アーカイブ ログ]** をクリックします。
3. 確認メッセージに対して **[はい]** をクリックします。
4. **[保存]** をクリックしてデフォルト (標準の設定) の場所にアーカイブを保存するか、アーカイブを保存する場所を参照して選択します。

アーカイブを作成した受信イベント ログを表示する

過去にアーカイブを作成した受信イベント ログをすべて表示できます。

> **注**
> アーカイブを表示する前に、現在の受信イベント ログのアーカイブを作成する必要があります。これを行わないと、アーカイブの表示時に現在の受信イベント ログがクリアされます。

1. マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。
2. [ファイル] メニューの **[保管したログを表示]** をクリックします。
3. アーカイブ ファイル名をクリックし (ファイル名の参照が必要な場合があります)、**[開く]** をクリックします。

   アーカイブが作成されたデータが受信イベント ログに表示されます。

受信イベント ログをクリアする

受信イベントログの情報をすべてクリアできます。

> **注**
> 一度クリアした受信イベント ログは復元できません。後からイベント ログが必要になると思われる場合、イベント ログをクリアする代わりにアーカイブを作成してください。

1. マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。
2. **[ファイル]** メニューの **[ログをクリア]** をクリックします。
3. 確認ボックスで **[はい]** をクリックしてログをクリアします。

   イベント ログが空になります。

表示されたイベントをエクスポートする

イベント ログをテキスト ファイルにエクスポートできます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 [ファイル] メニューの **[表示されたイベントをエクスポート]** をクリックします。

3 イベントの保存場所を参照して選択します。

4 必要であればファイル名を変更し、**[保存]** をクリックします。

選択した場所に .txt ファイルとしてイベントが保存されます。

クリップボードにイベントをコピーする

イベントをクリップボードにコピーし、メモ帳を使用してテキストファイルに貼り付けることができます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 エクスポートする受信イベント ログのイベントをクリックします。

3 **[編集]** メニューの **[選択したイベントをクリップボードにコピー]** をクリックします。

4 メモ帳を開きます。

Windows の [スタート] ボタンをクリックして [プログラム]、[アクセサリ] の順に選択し、[メモ帳] をクリックします。

5 **[編集]** メニューの **[貼り付け]** をクリックします。メモ帳にイベントが表示されます。必要なイベントがすべて表示されるまで、この手順を繰り返します。

6 安全な場所にメモ帳ファイルを保存します。

選択したイベントを削除する

受信イベント ログからイベントを削除できます。

1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[アクセス記録の表示]** をクリックします。

2 削除する受信イベント ログのイベントをクリックします。

3 **[編集]** メニューの **[選択したイベントの削除]** をクリックします。

受信イベント ログからイベントが削除されます。

アラートについて

McAfee Personal Firewall Plus を使用しているときに表示されるアラートの種類をよく理解しておいてください。確信を持ってアラートに対応できるように、表示される可能性のある以下のアラートの種類と、選択できる対応を確認してください。

注

アラートに表示される推奨事項を参考にしてアラートへの対応方法を決定することができます。アラートにスマート リコメンデーションを表示するには、**[ユーティリティ]** タブをクリックし、**[アラート設定]** アイコンをクリックして、**[スマート リコメンデーション]** リストから **[スマート リコメンデーションを使用]** (デフォルト (標準の設定)) または **[スマート リコメンデーションだけを表示]** を選択します。

レッド アラート

レッド アラートには、早急な対応を必要とする重要な情報が表示されます。

- **インターネット アプリケーションがブロックされました！**— このアラートは、McAfee Personal Firewall Plus によってアプリケーションのインターネット アクセスがブロックされたときに表示されます。たとえば、トロイの木馬プログラムのアラートが表示された場合は、このプログラムによるインターネットへのアクセスが自動的に拒否され、コンピュータのウイルス スキャンが促されます。

- **アプリケーションによるインターネット アクセスの要求** — このアラートは、McAfee Personal Firewall Plus によって新規のアプリケーションのインターネット トラフィックまたはネットワーク トラフィックが検出されると表示されます (標準または厳重セキュリティの場合)。

- **[アプリケーションの変更]**— このアラートは、McAfee Personal Firewall Plus によって以前にインターネットへのアクセスを許可していたアプリケーションへの変更が検出されると表示されます。問題のアプリケーションを最近アップグレードしていない場合は、変更されたアプリケーションによるインターネットへのアクセスを承認するときに注意が必要です (信頼、標準、または厳重セキュリティの場合)。

- **アプリケーションによるサーバ アクセスの要求** — このアラートは、以前にインターネットへのアクセスを許可していたアプリケーションが、サーバとしてインターネットへのアクセスを要求していることを McAfee Personal Firewall Plus が検出すると表示されます (厳重セキュリティの場合)。

  注

  Windows XP SP2 標準の自動更新設定では、Windows OS やコンピュータで実行している Microsoft のプログラムに、メッセージを表示せずにアップデートのダウンロード、インストールを実行します。Windows のサイレント アップデートからアプリケーションが変更されると、次回 Microsoft アプリケーションを起動するときに McAfee Personal Firewall Plus アラートが表示されます。

  重要

  最新の状態に維持する目的でオンライン製品アップデートを取得するためにインターネットアクセスを必要とするアプリケーション (McAfee サービスなど) には、アクセスを許可する必要があります。

「インターネット アプリケーションがブロックされました」アラート

トロイの木馬プログラムのアラート (図 2-4) が表示された場合は、McAfee Personal Firewall Plus によってこのプログラムによるインターネットへのアクセスが自動的に拒否され、コンピュータのウイルス スキャンが促されます。

図 2-4 「インターネット アプリケーションがブロックされました」アラート

イベントの簡単な説明を確認し、次のオプションから選択します。

- 受信イベント ログからイベントについての詳細情報を取得するには、**[詳細情報を調べる]** をクリックします (詳細は 21 ページの「[アクセス記録の表示] ページについて」を参照)。
- コンピュータのウイルスをスキャンするには、**[McAfee VirusScan を起動]** をクリックします。
- McAfee Personal Firewall Plus によって実行された処理以外に何も行わない場合は、**[メッセージを閉じて今の作業を続ける]** をクリックします。

アプリケーションによるインターネット アクセスの要求

[セキュリティの設定] オプションで、**[標準]** または **[厳重]** を選択すると、新規または変更されたアプリケーションのインターネット / ネットワーク トラフィックが検出されたときに、McAfee Personal Firewall Plus によってアラート (図 2-5) が表示されます。

図 2-5 「アプリケーションによるインターネット アクセスの要求」アラート

アプリケーションによるインターネット アクセスの許可に対して注意を促すアラートが発生した場合は、**[詳細については、ここをクリックしてください。]** をクリックしてアプリケーションの詳細情報を取得してください。このオプションは、McAfee Personal Firewall Plus でスマート リコメンデーションの使用が有効になっている場合にのみ表示されます。

マカフィーでは、インターネットにアクセスしようとするアプリケーションを認識できない場合があります (図 2-6)。

図 2-6 「認識されないアプリケーション」アラート

マカフィーでは、認識していないアプリケーションをどのように扱うべきかについての推奨はできません。アプリケーションについてマカフィーに報告するには、**[このプログラムについてマカフィーに連絡してください]** をクリックしてください。アプリケーションに関連する情報を入力する Web ページが表示されます。可能な限り詳しく入力してください。

入力された情報は、その他のリサーチ ツールと併せて、弊社の HackerWatch オペレータによって使用され、アプリケーションの保証が、既知のアプリケーション データベースにあるかどうかを判断するために役立てられます。データベースにある場合は、McAfee Personal Firewall でどのように処理されるべきかが決定されます。

イベントの簡単な説明を確認し、次のオプションから選択します。

- 非システム ポートでアプリケーションによるデータの送信と不要なデータの受信を許可するには、**[アクセスを承認]** をクリックします。
- アプリケーションによるデータの送受信を禁止するには、**[すべてのアクセスをブロック]** をクリックします。

「アプリケーションの変更」アラート

[セキュリティの設定] オプションで、**[信用]**、**[標準]** または **[厳重]** セキュリティを選択した場合、インターネットへのアクセスが以前に許可されたアプリケーションへの変更が McAfee Personal Firewall Plus によって検出されると、このアラート (図 2-7) が表示されます。問題のアプリケーションを最近アップグレードしていない場合は、変更されたアプリケーションによるインターネットへのアクセスを承認するときに注意が必要です。

図 2-7「アプリケーションの変更」アラート

イベントの簡単な説明を確認し、次のオプションから選択します。

- 非システム ポートでアプリケーションによるデータの送信と不要なデータの受信を許可するには、**[アクセスを承認]** をクリックします。
- アプリケーションによるデータの送受信を禁止するには、**[すべてのアクセスをブロック]** をクリックします。

「アプリケーションによるサーバ アクセスの要求」アラート

[セキュリティの設定] オプションで **[厳重]** セキュリティを選択すると、以前にインターネットへのアクセスを許可していたアプリケーションによるサーバとしてのインターネット アクセス要求が McAfee Personal Firewall Plus によって検出すると、アラート (図 2-8) が表示されます。

図 2-8「アプリケーションによるサーバ アクセスの要求」アラート

たとえば、MSN Messenger が、チャット中にファイルを送信するためのサーバ アクセスを要求すると、アラートが表示されます。

イベントの簡単な説明を確認し、次のオプションから選択します。

- アプリケーションによるデータの送受信の両方を許可するには、**[アクセスを承認]** をクリックします。
- アプリケーションによるデータの受信を禁止するには、**[発信アクセスに限定]** をクリックします。
- アプリケーションによるデータの送受信を禁止するには、**[すべてのアクセスをブロック]** をクリックします。

グリーン アラート

グリーン アラートは、McAfee Personal Firewall Plus での変更事項を通知するものです。たとえば、McAfee Personal Firewall Plus によって自動的にインターネットへのアクセスが許可されたアプリケーションや、新しく生成されたアプリケーション ルールなどが通知されます。

[インターネット アクセスを許可されたプログラム] — このアラートは、すべての新規アプリケーションまたは変更されたアプリケーションによるインターネット アクセスを McAfee Personal Firewall Plus が自動的に承認したときに表示され、その状況をユーザに通知します (信用セキュリティ)。変更されたアプリケーションとは、たとえば自動的にインターネットへのアクセスが許可されるようにルールが変更されたアプリケーションなどを指します。

アプリケーションによるインターネット アクセスの許可

[セキュリティの設定] オプションで **[信用]** を選択すると、McAfee Personal Firewall Plus によってすべての新規アプリケーションまたは変更されたアプリケーションのインターネット アクセスが自動的に承認され、アラート (図 2-9) が表示されます。

図 2-9 インターネット アクセスを許可されたプログラム

イベントの簡単な説明を確認し、次のオプションから選択します。

- インターネット アプリケーション ログからイベントの詳細を取得するには、**[アプリケーション ログを表示]** をクリックします (詳細については、19 ページの「[アプリケーションの設定] ページについて」を参照)。
- このようなタイプのアラートを表示しない場合は、**[このアラート タイプをオフにする]** をクリックします。
- McAfee Personal Firewall Plus によって実行された処理以外に何も行わない場合は、**[メッセージを閉じて今の作業を続ける]** をクリックします。

ブルー アラート

ブルー アラートには、対応する必要がない情報が表示されます。

- **[接続試行のブロック]** — このアラートは、McAfee Personal Firewall Plus が不要なインターネット トラフィックまたはネットワーク トラフィックをブロックすると表示されます。(信頼、標準、または厳重セキュリティの場合)。

「接続試行のブロック」アラート

信用セキュリティ、**標準**セキュリティ、**厳重**セキュリティを選択すると、不要なインターネット / ネットワーク トラフィックがブロックされたときに McAfee Personal Firewall Plus によってアラート (図 2-10) が表示されます。

図 2-10 「接続試行のブロック」アラート

イベントの簡単な説明を確認し、次のオプションから選択します。

- McAfee Personal Firewall Plus の受信イベント ログからイベントの詳細を取得するには、**[イベント ログを表示]** をクリックします (詳細については、21 ページの「[アクセス記録の表示] ページについて」 を参照)。
- このイベントの IP アドレスの追跡の表示を実行するには、**[このアドレスを追跡]** をクリックします。
- このアドレスによるユーザのコンピュータへのアクセスをブロックするには、**[このアドレスを禁止]** をクリックします。この IP アドレスが [禁止 IP アドレス] リストに追加されます。
- このアドレスによるユーザのコンピュータへのアクセスを許可するには、**[このアドレスを信用]** をクリックします。
- McAfee Personal Firewall Plus によって実行された処理以外に何も行わない場合は、**[メッセージを閉じて今の作業を続ける]** をクリックします。

索引

か

く

し

て

は