

McAfee®

personal**firewall**plus

ユーザ ガイド

McAfee®

著作権

Copyright © 2005 McAfee, Inc. All Rights Reserved.

このマニュアルのいかなる部分も、McAfee, Inc. またはその代理店または関連会社の書面による許可なしに、形態、方法を問わず、複写、送信、転載、検索システムへの保存、および他言語に翻訳することを禁じます。

商標

ActiveSecurity、アクティブセキュリティ、Entercept、Enterprise Secure Cast、エンタープライズセキュアキャスト、E-Policy Orchestrator、イーポリシー・オーケストレーター、GroupShield、グループシールド、IntruShield、McAfee、マカフィー、NetShield、ネットシールド、SpamKiller、VirusScan、WebShield、ウェブシールドは米国法人 McAfee, Inc. またはその関係会社の登録商標です。McAfee ブランドの製品は赤を基調としています。本書中のその他の登録商標及び商標はそれぞれその所有者に帰属します。

ライセンス情報

ライセンス条項

お客様へ: お客様がお買い求めになられたライセンスに従い、該当する契約書(許諾されたソフトウェアの使用につき一般条項を定めるものです、以下「本契約」といいます)をよくお読みください。お買い求めになられたライセンスタイプがご不明の場合には、担当営業またはライセンス付与管理部門にご相談になるか、製品に付随する購入関係書類若しくは購入手続きにおいて別途受領された書類をご参照ください。本契約の規定に同意されない場合は、製品をインストールしないでください。この場合、弊社またはご購入元に速やかにご返品いただければ、所定の条件を満たすことによりご購入額全額をお返しいたします。

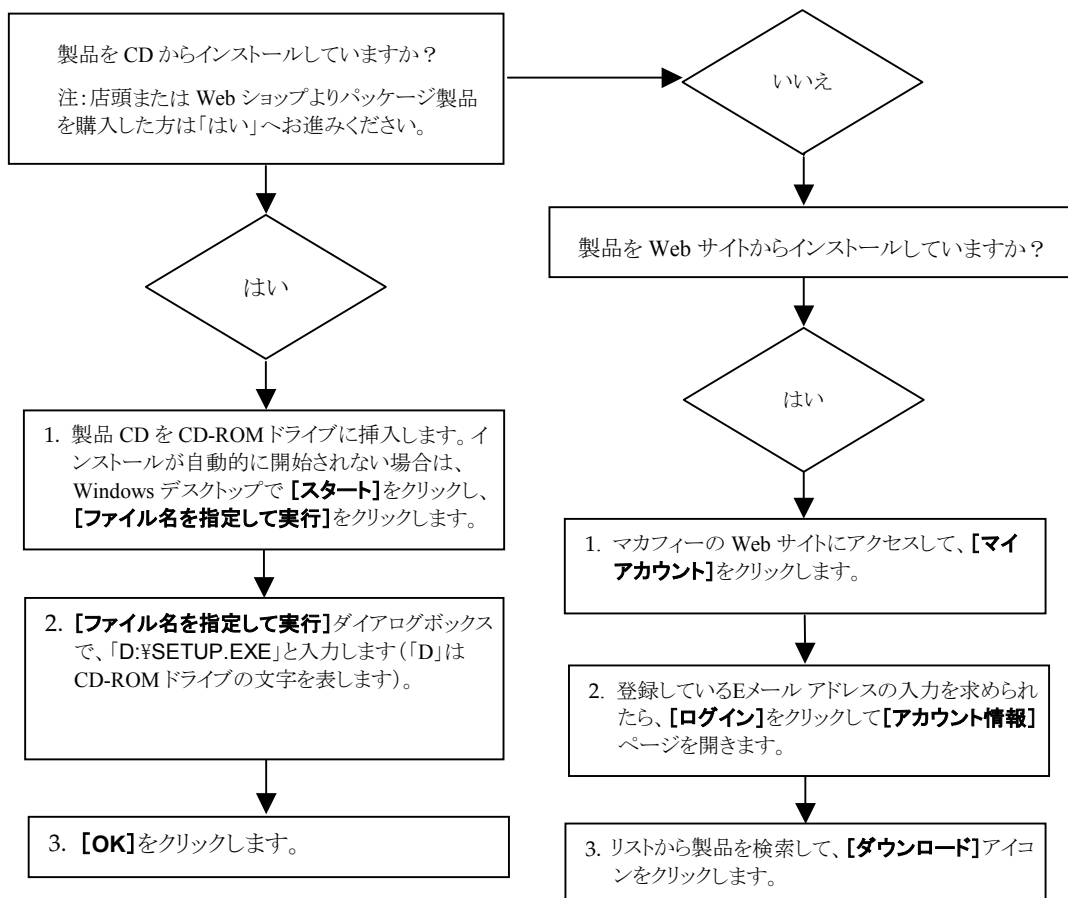
帰属

本製品には下記のソフトウェアおよびテクノロジーが含まれている場合があります。

- OpenSSL Toolkitで使用するためにOpenSSL Projectによって開発されたソフトウェア (<http://www.openssl.org/>)。 • Eric A. Youngによって作成された暗号化ソフトウェア、および Tim J. Hudson によって作成されたソフトウェア。 • GNU General Public License (GPL) あるいは、プログラムもしくはその一部の複製、変更、再頒布およびソースコードへのアクセスを許諾するフリーソフトウェアライセンスで使用(または再ライセンス)が許可されるソフトウェアプログラム。 GPL では、ソフトウェアを実行可能なバイナリ形式で配布する場合に、そのソースコードも一緒に提供することが定められています。本製品に GPL で配布されているソフトウェアが含まれている場合、そのソースコードが製品 CD に収録されています。フリーソフトウェアライセンスにより、弊社が製品のライセンス契約で規定している範囲を超えてソフトウェアプログラムの使用、複製、または変更を許諾しなければならない場合、これらの権利が本資料に記載されている権限または制約より優先されるものとします。 • Henry Spencer によって作成されたソフトウェア。 Copyright 1992, 1993, 1994, 1997 Henry Spencer. • Robert Nordier によって作成されたソフトウェア。 Copyright © 1996-7 Robert Nordier. • Douglas W. Sauder によって作成されたソフトウェア。 • Apache Software Foundation (<http://www.apache.org/>) によって開発されたソフトウェア。本ソフトウェアの使用許諾条件については、www.apache.org/licenses/LICENSE-2.0.txt を参照。 • International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation and others. • CrystalClear Software, Inc. によって開発されたソフトウェア。 Copyright © 2000 CrystalClear Software, Inc. • FEAD[®] Optimizer[®] technology, Copyright Netopsystems AG, Berlin, Germany. • Outside In[®] Viewer Technology © 1992-2001 Stellant Chicago, Inc. and/or Outside In[®] HTML Export, © 2001 Stellant Chicago, Inc. • Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000. • Software copyrighted by Expat maintainers. • Software copyrighted by The Regents of the University of California, © 1989. • Software copyrighted by Gunnar Ritter. • Software copyrighted by Sun Microsystems[®], Inc. © 2003. • Software copyrighted by Gisle Aas. © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, © 1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, © 2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. 本ソフトウェアの使用許諾条件については、www.python.org を参照。 • Software copyrighted by Beman Dawes, © 1994-1999, 2002. • Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • インディアナ大学 Extreme! 研究室 (<http://www.extreme.indiana.edu/>) によって開発されたソフトウェア。 • Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • カリフォルニア大学バークレー校によって開発されたソフトウェア。 • mod_ssl プロジェクト (<http://www.modssl.org/>) で使用するために Ralf S. Engelschall <rse@engelschall.com> によって開発されたソフトウェア。 • Software copyrighted by Kevlin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. 詳細については、<http://www.boost.org/libs/bind/bind.html> を参照。 • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Krempf, © 2001. アップデート、ドキュメント、改訂履歴については、http://www.boost.org を参照。 • Software copyrighted by Doug Gregor (gregor@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, © 2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, © 1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), © 2000. • Software copyrighted by Housemarque Oy <<http://www.housemarque.com/>>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002.

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 メーカー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 メーカーが提供する手順書等をご確認ください。



マカフィーは通知なしにいつでも更新 & サポート プランおよびポリシーを変更する権利を有します。McAfee および VirusScan は、McAfee, Inc と米国および他国におけるその提携企業の登録商標または商標です。
© 2005 McAfee, Inc. All Rights Reserved.

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

クイック スタート カード	iii
1 はじめに	7
新しい機能	7
システム要件	9
他のファイアウォールをアンインストールする	10
デフォルト（標準の設定）のファイアウォールを設定する	10
セキュリティ レベルを設定する	11
McAfee Personal Firewall Plus をテストする	13
McAfee SecurityCenter を使用する	13
2 McAfee Personal Firewall Plus を使用する	15
[概要] ページについて	15
[アプリケーションの設定] ページについて	20
アプリケーション ルールを変更する	21
インターネット アプリケーションを許可またはブロックする	22
[受信イベント] ページについて	22
イベントを理解する	23
受信イベント ログのイベントを表示する	26
受信イベントに対応する	28
受信イベント ログを管理する	31
アラートについて	33
レッド アラート	34
グリーン アラート	40
ブルー アラート	42
索引	43

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](https://www.mcafee.com/hackerwatch) 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

- **ゲームソフトへの対応改善**
全画面モードでゲームソフトを実行しているときでも、McAfee Personal Firewall は、侵入や不審な活動からコンピュータを保護します。ゲームの実行中は、侵入や不審な活動を検出しても、アラートを表示しません。ゲーム終了後にレッドアラートを表示します。
- **アクセス処理の向上**
McAfee Personal Firewall では、アプリケーションに対してインターネット接続を動的に許可することができます。アプリケーションが終了すると、この許可は無効になります。インターネットへの接続を行う未知のプログラムが McAfee Personal Firewall Plus によって検出されると、レッドアラートが表示され、このアプリケーションにインターネット接続を一時的に許可するオプションが表示されます。

■ **セキュリティ オプションの向上**

McAfee Personal Firewall でロック機能を実行すると、インターネットとの送信トラフィックおよび受信トラフィックをすぐにブロックすることができます。McAfee Personal Firewall では、いくつかの方法でロックの設定を行うことができます。

■ **復元機能の向上**

McAfee Personal Firewall では、リセット オプションを使用すると、McAfee Personal Firewall の設定を標準設定に戻すことができます。不要な動作を禁止しているときに、訂正ができなくなってしまう場合には、現在の設定を破棄して、製品の標準設定に戻すことができます。

■ **インターネット 接続の保護**

受信接続の IP が DHCP または DNS サーバによって割り当てられている場合、インターネット接続が故意に無効にされることを防ぐために、ブルーアラートの接続を禁止するオプションは表示されません。受信接続の送信元が DHCP または DNS サーバで解決されない場合に、このオプションが表示されます。

■ **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 によって、HackerWatch.org の機能が向上し、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時、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。

■ **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**

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ます。また、発生元 IP アドレスの詳細な連絡先/所有者の情報と、地理的な情報が表示されます。

■ **使いやすきの向上**

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、大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
- Pentium 互換プロセッサを搭載したコンピュータ
Windows 98、Windows 2000 : 133 MHz 以上
Windows Me : 150 MHz 以上
Windows XP (Home および Pro) : 300 MHz 以上
- RAM
Windows 98、Windows Me、Windows 2000 : 64 MB
Windows XP (Home および Pro) : 128 MB
- 35 MB のハード ディスク空き容量 (インストール用)
- Microsoft Internet Explorer 5.5 以降

注意

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.jp>) 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。

注意

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。

注意

両方のファイアウォールを有効にすると、McAfee Personal Firewall Plus の [受信イベント] 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\firewall.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。【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。

セキュリティを設定するには

- 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、【オプション】を選択します。
- 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。

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** — すべてのトラフィックが停止します。【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** — アプリケーションは、明確に必要なタイプのインターネット アクセス（送信のみのアクセスなど）だけを要求し、ユーザがそのアクセスを許可または禁止します。アプリケーションがすべての（送受信）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。
- ◆ **標準（推奨）** — インターネット アクセスが承認されたアプリケーションに対して、すべてのアクセスを承認します。すべてのアクセスを承認すると、アプリケーションは要求していないデータを送信 / 受信できます。
- ◆ **信用** — 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、コンピュータ上で新しいアプリケーションが検出されたときに、アラートが表示されるように設定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。

注意

ファイアウォールのセキュリティ設定が【オープン】または【ロック】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【すべてのアクセスを許可】に変更するか、【アプリケーションの設定】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。

注意

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。

- ◆ **侵入検知システム (IDS) イベントを受信イベントにログ記録** — 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 要求の受け入れ** — 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を使用します。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 の設定変更を許可する** — 複数のユーザが追加されている場合に、制限ユーザが McAfee Personal Firewall の設定を変更できるようにします (Windows 2000 Professional または Windows XP のみ)。

- 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

侵入や不審な活動に対して脆弱かどうかを調べるために、インストールした McAfee Personal Firewall をテストすることができます。

システムトレイのマカフィー・アイコンから McAfee Personal Firewall をテストするには

- マカフィー・アイコン  を右クリックして、**【ファイアウォールをテスト】**を選択します。

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 の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。


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


注意

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。**【SecurityCenter を開く】** をクリックします。

McAfee SecurityCenter から McAfee Personal Firewall を開くには

- 1 SecurityCenter から **[Personal Firewall Plus]** タブをクリックします。
- 2 [オプションを選択する] メニューからタスクを選択します。


Windows から Personal Firewall を開くには

- 1 マカフィー・アイコン  を右クリックして、**[Personal Firewall]** をポイントします。
- 2 タスクを選択します。

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、タスクを選択します。

[概要] ページについて

McAfee Personal Firewall の概要は 4 つのページで構成されます。

- ◆ メイン概要
- ◆ アプリケーションの概要
- ◆ イベントの概要
- ◆ HackerWatch Summary

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](https://www.mcafee.com/hackerwatch) 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 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 の [メイン概要] ページを開くには





- マカフィー・アイコン  を右クリックして、[Personal Firewall] を選択し、[概要を表示] を選択します (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。[受信イベント] 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。

アイテム	説明
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。
新機能	[新機能] 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。 [受信イベント] 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

- 1 マカフィー・アイコン  を右クリックして **[Personal Firewall]** を選択し、**[概要を表示]** を選択します。
- 2 **[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、過去 15 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、ユーザのコンピュータにおいて過去 24 時間に最もアクティブなアプリケーションが使用している帯域幅の使用率が表示されます。 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
新機能	[新機能] 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 の各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

- 1 マカフィー・アイコン  を右クリックして、**[Personal Firewall]** を選択し、**[概要を表示]** を選択します。
- 2 **[表示を変更]** 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、 [受信イベント] 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の位置に合わせると、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。 [受信イベント] 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。

アイテム	説明
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 Summary] ページを表示するには

- 1 マカフィー・アイコン  を右クリックして、**[Personal Firewall]** を選択し、**[概要を表示]** を選択します。
- 2 **[表示の変更]** をクリックし、**[HackerWatch Summary]** を選択します。


[HackerWatch Summary] ページには次の情報が表示されます。

アイテム	説明
World Activity	[World Activity] 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 のアクセス発源地図が開きます。
Event Tracking	[Event Tracking] 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。
Global Port Activity	[Global Port Activity] には、過去 5 日間に攻撃と見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。

[アプリケーションの設定] ページを表示するには

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

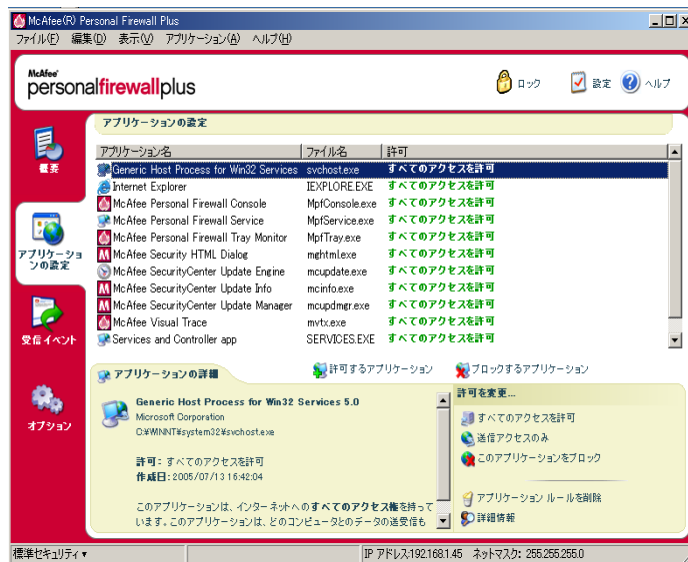


図 2-2. [アプリケーションの設定] ページ

[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
- 許可
- アプリケーションの詳細 : アプリケーション名とバージョン、企業名、パス名、許可、作成日、許可の種類の説明

アプリケーション ルールを変更する

McAfee Personal Firewall では、アプリケーションのアクセス ルールを変更できません。


アプリケーション ルールを変更するには

- 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]** を選択します。
- 2 **[アプリケーションの設定]** リストで、変更するアプリケーション ルールを右クリックし、別のレベルを選択します。
 - ◆ **すべてのアクセスを許可** – インターネットに対するすべてのアクセスを許可します。
 - ◆ **送信アクセスのみ** – インターネットに対する送信アクセスのみを許可します。
 - ◆ **このアプリケーションをブロック** – インターネットに対するアクセスを禁止します。

注意

ファイアウォールのセキュリティ設定が **[オープン]** または **[ロック]** 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アクセス ルールを **[すべてのアクセスを許可]** に変更するか、**[アプリケーションの設定]** リストで **[ブロック]** ルールを削除します。


アプリケーション ルールを削除するには

- 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]** を選択します。
- 2 **[アプリケーションの設定]** リストでアプリケーション ルールを右クリックし、**[アプリケーション ルールを削除]** を選択します。

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。

インターネット アプリケーションを許可またはブロックする


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]** を選択します。
- 2 [アプリケーションの設定] ページで、次のオプションのいずれかをクリックします。
 - ◆ **すべてのアクセスを許可** — インターネットに対するすべてのアクセスを許可します。
 - ◆ **このアプリケーションをブロック** — インターネットに対するアクセスを許可しません。
 - ◆ **アプリケーションルールを削除** — アプリケーションルールを削除します。

[受信イベント] ページについて

[受信イベント] ページには、McAfee Personal Firewall Plus が迷惑なインターネット接続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。

[受信イベント] ページを表示するには

- マカフィー・アイコン  を右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します (図 2-3)。

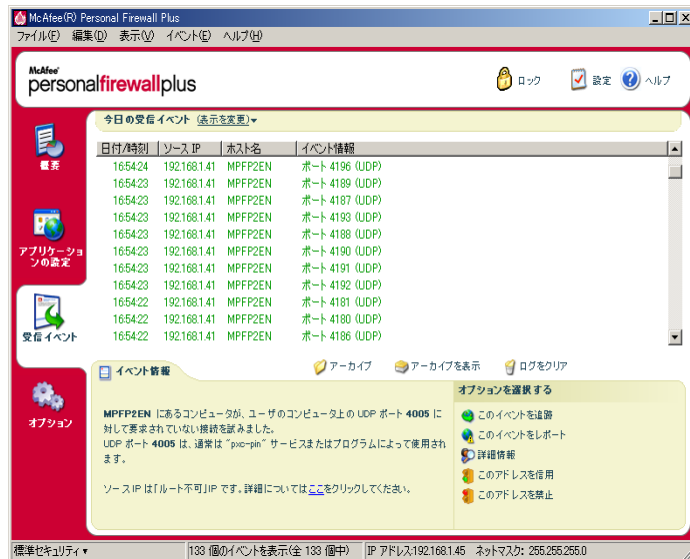


図 2-3. [受信イベント] ページ

[受信のイベント] ページには次の情報が表示されます。

- 日時
- 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、ホスト名または IP、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。

IP アドレスの種類

IP アドレスの中には、特殊なものがあります。

ルート不可 IP アドレス — 「プライベート 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。プライベート IP ブロックは 10.x.x.x、172.16.x.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。このアドレスが検出された場合、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。多くの場合は、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な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、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回ってスキャンしている徴候です。このようなアクティビティは McAfee Personal Firewall 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。これは、ループバックアドレスまたは「localhost」とも呼ばれます。

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、Web インターフェースから多くの個人メールや Web サーバを設定できます。このインターフェースにアクセスするには、Web ブラウザで「http://localhost/」と入力します。

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、他のコンピュータからトロイの木馬を探し回ってスキャンされていることの兆候です。このような侵入行為は McAfee Personal Firewall 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。

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 アドレス] 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た場合は、McAfee Personal Firewall の [信用 IP アドレス] リストに 127.0.0.1 を追加します。

[信用 IP アドレス] 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、特定の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 では、このようなイベントは、ローカル ネットワークで生成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 アドレス] オプションで **[マイローカル エリアネットワーク (LAN)]** 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ネットワークを使用している場合は、特に注意が必要です。このような場合は、**[マイローカルエリアネットワーク (LAN)]** オプションを選択しないでください。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] リストに追加してください。

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.xxx.xxx 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探し回って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。

イベントの情報を表示するには、イベントをクリックします。情報が **【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を表示するには、このオプションを使用します。

今日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、**【受信イベント】** を選択します。
- 2 受信イベント ログでエントリを右クリックし、**【今日のイベントを表示】** をクリックします。

今週のイベントを表示する

週ごとのイベントを表示するには、このオプションを使用します。

今週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、**【受信イベント】** を選択します。
- 2 受信イベント ログでエントリを右クリックし、**【今週のイベントの表示】** をクリックします。

すべての受信イベント ログを表示する

すべてのイベントを表示するには、このオプションを使用します。

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、**【受信イベント】** をクリックします。
- 2 受信イベント ログでエントリを右クリックし、**【完全なログを表示】** をクリックします。

[受信イベント] ページに、受信イベント ログのすべてのイベントが表示されます。

特定日のイベントを表示する

特定日のイベントを表示するには、このオプションを使用します。

特定日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、**[受信イベント]** を選択します。
- 2 受信イベント ログでエントリを右クリックし、**[この日のイベントだけを表示]** をクリックします。

特定のインターネット アドレスのイベントを表示する

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表示する場合は、このオプションを使用します。

特定のインターネット アドレス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、**[受信イベント]** をクリックします。
- 2 受信イベント ログでエントリを右クリックし、**[このインターネット アドレスのイベントだけを表示]** をクリックします。

イベント情報が同じイベントを表示する

受信イベント ログ内で、選択したイベントと、[イベント情報] 列の情報が同じイベントを表示する場合は、このオプションを使用します。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。

イベント情報が同じ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、**[受信イベント]** をクリックします。
- 2 受信イベント ログでエントリを右クリックし、**[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。

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。

選択したイベントを追跡するには

- 1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します。
- 2 受信イベント ログで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

HackerWatch.org からアドバイスを取得するには

- 1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します。
- 2 **[受信イベント]** ページでイベントのエントリを選択し、**[オプションを選択する]** ペインで **[詳細情報]** をクリックします。

Web ブラウザが開き、HackerWatch.org の Web サイトが表示されます。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、**[受信イベント]** を選択します。
- 2 レポートするイベントをクリックし、**[オプションを選択する]** 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 にレポートされます。

HackerWatch.org にサインアップする

[概要] ページを初めて開くと、McAfee Personal Firewall は 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

[受信イベント] ページを使用して、常に接続を許可する [信用 IP アドレス] リストに IP アドレスを追加できます。

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] ページ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。

[信用 IP アドレス] リストに IP アドレスを追加するには

- 1 マカフィー・アイコンを右クリックして [Personal Firewall] を選択し、[受信イベント] を選択します。
- 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。

[信用 IP アドレス ルールを追加] ダイアログに表示される 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 マカフィー・アイコンを右クリックして [Personal Firewall] を選択し、[オプション] を選択します。
- 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 アドレスがチェックされて表示されます。

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、それらのポートからのアクセスをブロックする必要がある場合にのみ、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] ページ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。

すべての受信トラフィックの IP アドレスが表示される [受信イベント] ページを使用して、不審または不要なインターネット活動を行っている IP アドレスからの接続を禁止することができます。

[禁止 IP アドレス] リストに IP アドレスを追加するには

- 1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します。
- 2 [受信イベント] ページに、すべての受信トラフィックの IP アドレスが表示されます。IP アドレスを選択して、次のいずれかを実行します。
 - ◆ IP アドレスを右クリックして、**[ソース IP アドレスを禁止]** 選択します。
 - ◆ **[オプションを選択する]** メニューで、**[このアドレスを禁止]** をクリックします。
- 3 [禁止 IP アドレス ルールを追加] ダイアログで、次の設定の 1 つまたは複数を使用して、禁止 IP アドレス ルールを設定します。
 - ◆ **シングル IP アドレス** : 禁止する IP アドレスです。標準の設定では、[受信イベント] ページで選択した IP アドレスが表示されます。
 - ◆ **IP アドレス範囲** : [開始 IP アドレス] と [終了 IP アドレス] に IP アドレスを指定します。この範囲内の IP アドレスが禁止されます。
 - ◆ **このルールの期限指定** : 禁止 IP アドレス ルールの有効期限 (日付と時刻) です。ドロップダウン メニューから日付と時刻を選択します。
 - ◆ **説明** : 新しいルールの説明です。必要に応じて入力します。
 - ◆ **[OK]** をクリックします。
- 4 ダイアログ ボックスで、**[はい]** をクリックして設定を確認します。**[いいえ]** をクリックすると、[禁止 IP アドレス ルールを追加] ダイアログに戻ります。

禁止されたインターネット接続からのイベントが検出されると、[アラート設定] ページで指定した方法に従ってアラートが表示されます。

IP アドレスが追加されたことを確認するには

- 1 **[オプション]** 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

[受信イベント] 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作成して、記録されたすべての受信イベントを保存できます。情報には、日付と時刻、ソース IP、ホスト名、ポート、イベント情報などが含まれます。受信イベント ログは非常に大きくなる可能性があるため、受信イベント ログのアーカイブは定期的に作成してください。

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、**[受信イベント]** を選択します。
- 2 [受信イベント] ページで **[アーカイブ]** をクリックします。
- 3 [ログを保管] ダイアログで **[はい]** をクリックして、次に進みます。
- 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。

注: 標準の設定では、受信イベント ログは定期的に保管されます。[イベント ログ設定] ページで **[ログ記録されたイベントを自動的に保管]** をオンにすると、自動保管が有効になり、このオプションをオフにすると無効になります

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。保管されるアーカイブには、イベントの日時、ソース IP、ホスト名、ポート、イベント情報が含まれます。

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、**[受信イベント]** を選択します。
- 2 [受信イベント] ページで **[アーカイブを表示]** をクリックします。
- 3 アーカイブ ファイル名を選択または参照して、**[開く]** をクリックします。

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。

警告：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。

受信イベント ログのアーカイブをクリアするには

- 1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します。
- 2 **[受信イベント]** ページで **[ログをクリア]** をクリックします。
- 3 ダイアログで **[はい]** をクリックしてログをクリアします。

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。

クリップボードにイベントをコピーするには

- 1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します。
- 2 受信イベント ログで、イベントを右クリックします。
- 3 **[イベント テキス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。
 - ◆ コマンド ラインで notepad と入力するか、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]** の順にポイントします。**[メモ帳]** を選択します。
- 5 **[編集]** をクリックし、次に **[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。

受信イベント ログからイベントを削除するには

- 1 マカフィー・アイコンを右クリックして **[Personal Firewall]** を選択し、**[受信イベント]** を選択します。
- 2 **[受信イベント]** ページで、削除するイベントのエントリをクリックします。
- 3 **[編集]** メニューで、**[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。

注意

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、**[オプション]** 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]** (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。

- **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（標準または嚴重セキュリティの場合）。
- **アプリケーションが変更されました** — このアラートは、Personal Firewall 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。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（信用、標準、または嚴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（嚴重セキュリティの場合）。

注意

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。

「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。McAfee VirusScan がインストールされていない場合は、McAfee SecurityCenter を開くことができます。

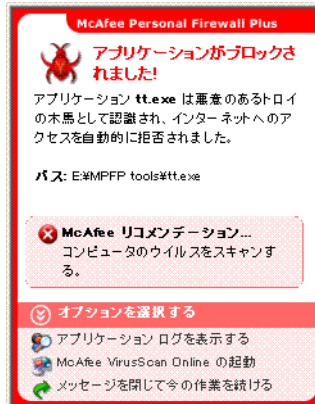


図 2-4. 「アプリケーションがブロックされました！」アラート

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、**[アプリケーション ログを表示する]** をクリックします（詳細は [22 ページの「\[受信イベント\] 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 Online の起動]** 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。
- **[送信アクセスを承認]** をクリックして、送信アクセスを許可します（**厳重セキュリティ**）。

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 / ネットワーク接続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。

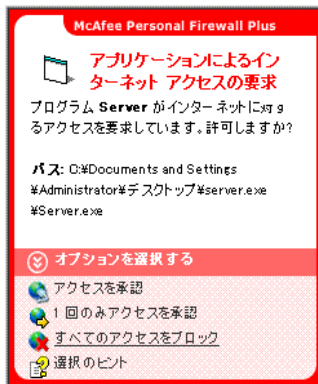


図 2-5. 「アプリケーションによるインターネット アクセスの要求」アラート

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)。

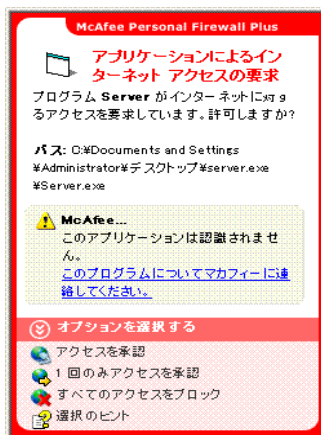


図 2-6. アプリケーションが認識されない場合のアラート

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。

- **【アクセスを承認】** をクリックして、このアプリケーションのインターネット接続をすべて許可します。
- **【1回のみアクセスを承認】** をクリックして、このアプリケーションのインターネット接続を一時的に許可します。アプリケーションが終了すると、この許可は無効になります。
- **【すべてのアクセスをブロック】** をクリックして、このアプリケーションのインターネット接続をすべて禁止します。
- **【送信アクセスを承認】** をクリックして、送信アクセスを許可します (**厳重セキュリティ**)。
- **【選択のヒント】** をクリックして、アプリケーションのアクセス許可に関するオンライン ヘルプを表示します。

「アプリケーションが変更されました」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. 「アプリケーションが変更されました」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。

- **【アクセスを承認】** をクリックして、このアプリケーションのインターネット接続をすべて許可します。
- **【1回のみアクセスを承認】** をクリックして、このアプリケーションのインターネット接続を一時的に許可します。アプリケーションが終了すると、この許可は無効になります。
- **【すべてのアクセスをブロック】** をクリックして、このアプリケーションのインターネット接続をすべて禁止します。
- **【送信アクセスを承認】** をクリックして、送信アクセスを許可します（**厳重セキュリティ**）。
- **【選択のヒント】** をクリックして、アプリケーションのアクセス許可に関するオンラインヘルプを表示します。

「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。

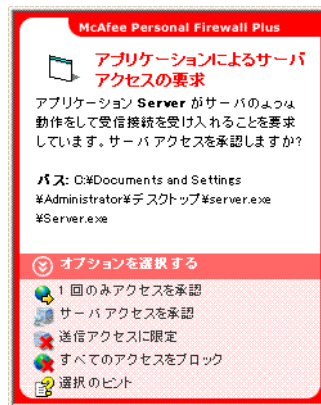


図 2-8. 「アプリケーションによるサーバアクセスの要求」アラート

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。

- **[1回のみアクセスを承認]** をクリックして、このアプリケーションのインターネット接続を一時的に許可します。アプリケーションが終了すると、この許可は無効になります。
- **[サーバアクセスを承認]** をクリックして、このアプリケーションのインターネット接続をすべて許可します。
- **[送信アクセスに限定]** をクリックして、このアプリケーションによるデータの受信を禁止します。
- **[すべてのアクセスをブロック]** をクリックして、このアプリケーションのインターネット接続をすべて禁止します。
- **[選択のヒント]** をクリックして、アプリケーションのアクセス許可に関するオンラインヘルプを表示します。

グリーン アラート

グリーン アラートは、McAfee Personal Firewall でのイベントを通知するものです。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たアプリケーション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。

- 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 ログを表示する]** をクリックします（詳細については、20 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。
- **[すべてのアクセスをブロック]** をクリックして、このアプリケーションのインターネット接続をすべて禁止します。

「アプリケーションが変更されました」アラート

[セキュリティの設定] オプションで **【信用】** セキュリティを選択した場合、McAfee Personal Firewall によってすべての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 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 ログを表示する】** をクリックします（詳細については、[20 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。
- **【すべてのアクセスをブロック】** をクリックして、インターネット接続をすべて禁止します。

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、または嚴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、**嚴重**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。

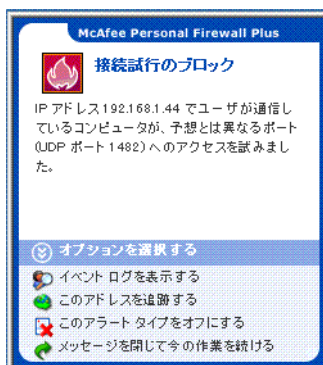


図 2-10. 「接続試行のブロック」アラート

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 ログを表示する】** をクリックします（詳細については、[22 ページの「\[受信イベント\] 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

H

HackerWatch.org

- アドバイス, 28
- イベントのレポート先, 28
- サインアップ, 29

I

IP アドレス

- 禁止, 30
- 信用する, 29
- 概要, 23

M

McAfee Personal Firewall Plus

- 使用, 15
- テスト, 13

McAfee SecurityCenter, 13

P

Personal Firewall のテスト, 13

W

Windows 自動更新, 34

Windows ファイアウォール, 10

あ

新しい機能, 7

アプリケーションの設定

- アプリケーション ルールの変更, 21
- 許可とブロック, 22
- 概要, 20

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要求, 34
- アプリケーションによるサーバアクセスの要求, 34
- アプリケーションの変更, 34

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, 34

許可するアプリケーション, 40

接続試行のブロック, 42

アンインストール

他のファイアウォール, 10

い

イベント

0.0.0.0 からのイベント, 24

127.0.0.1 からのイベント, 24

HackerWatch.org のアドバイス, 28

イベント ログのアーカイブ作成, 31

イベント ログのクリア, 32

エクスポート, 32

概要, 22

コピー, 32

削除, 33

詳細情報, 28

対応, 28

追跡

アーカイブを作成したイベント ログの表示, 31

説明, 22

表示

今日, 26

同じイベント情報のイベント, 27

今週のイベント, 26

すべてのイベント, 26

特定アドレスからのイベント, 27

特定日のイベント, 27

プライベート IP アドレスからのイベント, 25

ユーザの LAN 上のコンピュータからのイベント, 25

ループバック, 24

レポート, 28

イベント ログ

概要, 22

管理, 31

表示, 31

イベント ログのイベントの表示, 26

イベントの追跡, 28

イベントをレポートする, 28

か

概要ページ, 15

く

クイック スタート カード, iii

し

システム要件, 9

て

デフォルトのファイアウォール、設定, 10

は

はじめに, 7

