

McAfee®

Internet Security Suite 2007

ユーザガイド

目次

McAfee Internet Security	7
McAfee SecurityCenter	9
機能	10
McAfee SecurityCenter を使用	11
ヘッダ	11
左の列	11
メインパネル	12
McAfee SecurityCenter アイコンについて	13
保護の状態について	15
保護の問題を修復	21
McAfee SecurityCenter 情報を表示	22
詳細メニューを使用	22
McAfee SecurityCenter のオプションの設定	23
保護の状態の設定	24
ユーザオプションの設定	25
更新オプションの設定	28
アラートのオプションの設定	32
よく使う機能を実行	35
よく使う機能を実行	35
最近のイベントを表示	36
コンピュータを自動的に保守	37
コンピュータを手動で保守	38
ネットワークを管理	39
ウイルスの詳細情報	40
McAfee QuickClean	41
McAfee QuickClean の機能について	42
機能	42
コンピュータをクリーニング	43
McAfee QuickClean を使用	45
McAfee Shredder	47
McAfee Shredder の機能について	48
機能	48
McAfee Shredder で不要なファイルを消去	49
McAfee Shredder を使用	50

McAfee Network Manager	51
機能	52
McAfee Network Manager のアイコンについて	53
管理されたネットワークをセットアップ	55
ネットワーク地図を使用	56
管理されたネットワークに参加	59
ネットワークをリモートで管理	63
状態の監視と権限	64
セキュリティ上の脆弱性を修復	67
 McAfee VirusScan	 69
機能	70
ウイルス対策を管理	73
ウイルス対策を使用	74
スパイウェア対策を使用	77
McAfee SystemGuards を使用	78
スクリプトスキャンを使用	87
E メール保護を使用	88
メッセージャー保護を使用	90
コンピュータを手動スキャン	91
手動スキャン	92
McAfee VirusScan を管理	97
信頼リストを管理	98
隔離したプログラム、Cookie、およびファイルを管理	99
最近のイベントとログを表示	101
匿名情報を自動報告	102
セキュリティアラートについて	103
その他の情報	105
よくある質問	106
トラブルシューティング	108
 McAfee Personal Firewall	 111
機能	112
ファイアウォールを起動	115
ファイアウォールによる保護を開始	115
ファイアウォールによる保護を停止	116
アラートを使用	117
アラートについて	118
情報アラートを管理	121
ゲーム中にアラートを表示	121
情報アラートを非表示化	121

ファイアウォールによる保護の設定	123
ファイアウォールのセキュリティレベルを管理	124
スマートリコメンデーションのアラートの設定	128
ファイアウォールによるセキュリティを最適化	130
ファイアウォールをロックおよび復元	133
プログラムと権限を管理	135
プログラムのインターネットアクセスを許可	136
プログラムに送信アクセスのみを許可	139
プログラムのインターネットアクセスをブロック	141
プログラムのアクセス権を削除	143
プログラムについての確認	144
システムサービスを管理	147
システム サービス ポートの設定	148
コンピュータ接続を管理	151
コンピュータ接続を信用	152
コンピュータ接続を禁止	156
ログ記録、監視、分析	161
イベントログを記録	162
統計を使用	165
インターネットトラフィックを追跡	166
インターネットトラフィックを監視	170
インターネットセキュリティについての確認	173
HackerWatch チュートリアルを起動	174

McAfee SpamKiller 175

機能	176
Web メールアカウントを管理	179
Web メールアカウントを追加	180
Web メールアカウントを変更	182
Web メールアカウントを削除	184
Web メールフィルタリングを管理	185
友人を管理	187
友人リストの管理方法について	188
友人リストを自動更新	190
フィルタリングオプションを変更	193
E メールメッセージのフィルタリングを変更	194
メッセージの処理方法を変更	196
文字セットによりメッセージをフィルタリング	197
迷惑メールを報告	198
パーソナルフィルタを管理	199
パーソナルフィルタの管理方法について	200
正規表現を使用	202
McAfee SpamKiller を保守	207
迷惑メール対策を管理	208
ツールバーを使用	209

フィッシング詐欺対策の設定	211
フィッシング詐欺対策を無効化/有効化	212
フィッシング詐欺フィルタを変更	213
その他の情報	215
よくある質問	216
McAfee Privacy Service	219
機能	220
パレンタルコントロールをセットアップ	221
ユーザのコンテンツの格付けグループの設定	222
ユーザの Cookie ブロックのレベルの設定	224
ユーザのインターネット使用時間制限の設定	229
Web サイトをブロック	230
Web サイトを許可	234
Web サイトによる Cookie の設定を許可	237
不適切な可能性のある Web 画像をブロック	239
インターネットでの情報を保護	241
広告、ポップアップ、Web バグをブロック	242
個人情報をブロック	244
パスワードを保護	245
Password Vault をセットアップ	246
McAfee Data Backup	249
機能	250
ファイルをアーカイブ	251
アーカイブオプションの設定	252
完全アーカイブとクイックアーカイブを実行	256
アーカイブ済みファイルを使用	259
ローカルアーカイブのエクスペローラを使用	260
アーカイブ済みファイルを復元	262
アーカイブを管理	264
McAfee EasyNetwork	265
機能	266
McAfee EasyNetwork の設定	267
McAfee EasyNetwork を起動	268
管理されたネットワークに参加	269
管理されたネットワークを切断	272
ファイルを共有および送信	273
ファイルを共有	274
ほかのコンピュータにファイルを送信	277
プリンタを共有	279
共有プリンタを使用	280

リファレンス	283
--------	-----

用語集	285
-----	-----

マカフィーについて	303
著作権	303

索引	305
----	-----

第 1 章

McAfee Internet Security

McAfee Internet Security Suite を使用すると、インターネット上の脅威から個人情報とコンピュータが保護され、重要なファイルが自動的にバックアップされるため、安心してインターネットを利用できます。信頼性の高いマカフィーの保護機能により常に最新のセキュリティ対策が行われるため、ネットサーフィン、オンラインショッピング、オンラインバンキング、E メール、メッセージャーの使用や、ファイルのダウンロードを安心して実行できます。新しく生まれ変わった McAfee SecurityCenter により、セキュリティの状態の表示やウイルスやスパイウェアのスキャンが簡単に実行できるだけでなく、製品を常に最新の状態に維持できます。契約している製品に関しては、最新のマカフィーソフトウェアと更新を自動的に受信できます。

McAfee Internet Security には次のプログラムが含まれています。

- McAfee SecurityCenter
- McAfee Privacy Service
- McAfee Shredder
- McAfee VirusScan
- McAfee Personal Firewall
- McAfee SpamKiller
- McAfee Data Backup
- McAfee Network Manager
- McAfee EasyNetwork (3 ユーザ版のみ)
- McAfee SiteAdvisor

第 2 章

McAfee SecurityCenter

McAfee SecurityCenter を使用すると、セキュリティ製品の起動、管理、および設定を簡単に行うことができます。

McAfee SecurityCenter では、ウイルスアラート、製品情報、サポート、契約状況などの情報を取得したり、マカフィーの Web サイトにあるツールおよびニュースにワンクリックでアクセスできます。

この章の内容

機能	10
McAfee SecurityCenter を使用	11
McAfee SecurityCenter のオプションの設定	23
よく使う機能を実行	35

機能

McAfee SecurityCenter の新機能と利点は次のとおりです。

新しくなった保護状態の表示

コンピュータのセキュリティ状態の把握、更新の確認、セキュリティ上の問題の修復を簡単に実行できるようになりました。

継続的な更新およびアップグレード

更新は、毎日自動的にインストールされます。マカフィーソフトウェアの新しいバージョンが提供された場合、契約期間内は無料で自動的に入手できます。これにより、常に最新の保護を利用できます。

リアルタイムのセキュリティアラート機能

緊急のウイルス発生やその他のセキュリティの脅威を通知します。また、脅威を削除または無効にし、また詳細を確認する対策オプションがあります。

契約の更新

さまざまな契約更新オプションが用意されているため、マカフィーによる保護を常に最新の状態に維持できます。

パフォーマンスツール

使用しないファイルを削除し、使用するファイルを最適化し、システムの復元を使用することにより、コンピュータのパフォーマンスを最適な状態に維持できます。

年中無休のテクニカルサポート

マカフィーのサポートスタッフが、毎日朝 9 時から夜 9 時まで、チャット、E メール、電話などで対応します。

安全なネットサーフィンの保護

McAfee SiteAdvisor ブラウザプラグインがインストールされていると、アクセスした Web サイトや、Web 検索結果に表示された Web サイトを評価し、スパイウェア、迷惑メール、およびオンライン詐欺からユーザーを保護します。Eメールの送信、ダウンロードファイル、リンク先、ポップアップや第三者のトラッキング Cookie などの迷惑行為に関するサイトの検査結果を示す、安全性評価の詳細を表示できます。

第 3 章

McAfee SecurityCenter を使用

タスクバーの右端の Windows 通知領域または Windows デスクトップにある McAfee SecurityCenter アイコン  から、McAfee SecurityCenter を実行します。

McAfee SecurityCenter を開くと、[ホーム] パネルにコンピュータのセキュリティの状態が表示され、更新、スキャン（McAfee VirusScan がインストールされている場合）などのよく使う機能に簡単アクセスできます。

ヘッダ

ヘルプ

プログラムのヘルプファイルを表示します。

左の列

更新

製品を更新して、最新の脅威から保護します。

スキャン

McAfee VirusScan がインストールされている場合、コンピュータの手動スキャンを実行します。

よく使う機能

[ホーム] パネルの表示、最近のイベントの表示、コンピュータネットワークの管理（対象のネットワークの管理機能のあるコンピュータの場合）、コンピュータの保守などのよく使う機能を実行します。McAfee Data Backup がインストールされている場合、データのバックアップも実行できます。

インストール済みのコンポーネント

コンピュータのセキュリティを保護しているセキュリティサービスを確認できます。

メインパネル

保護の状態

「保護されていますか？」の横には、コンピュータ全体の保護の状態が表示されます。その下には、カテゴリおよびタイプごとの保護の状態が表示されます。

SecurityCenter の情報

コンピュータでの最終更新日時、最後のスキャン日時（McAfee VirusScan がインストールされている場合）、および契約の有効期限が表示されます。

この章の内容

McAfee SecurityCenter アイコンについて	13
保護の状態について	15
保護の問題を修復	21
McAfee SecurityCenter 情報を表示	22
詳細メニューを使用	22

McAfee SecurityCenter アイコンについて

McAfee SecurityCenter アイコンは、タスクバーの右端の Windows 通知領域に表示されます。アイコンを使用すると、コンピュータの保護が万全であるかどうかの確認、実行中のスキャンの状態の表示（McAfee VirusScan がインストールされている場合）、更新の有無の確認、最近のイベントを表示、コンピュータの保守、マカフィーの Web サイトのサポートの利用ができます。

McAfee SecurityCenter を開いてその他の機能を使用

McAfee SecurityCenter が実行中である場合、タスクバーの右端の Windows 通知領域に McAfee SecurityCenter の [M] アイコン  が表示されます。

McAfee SecurityCenter を開いてその他の機能を使用するには

- メインの McAfee SecurityCenter アイコンを右クリックし、次のいずれかをクリックします。
 - SecurityCenter を開く
 - 更新
 - クイックリンク
サブメニューに、[ホーム]、[最近のイベントの表示]、[ネットワークの管理]、[コンピュータの保守]、および [データのバックアップ]（インストールされている場合）へのリンクが表示されます。
 - 契約の確認
（この項目は、1 つ以上の製品の契約が期限切れである場合に表示されます）
 - アップグレードセンター
 - カスタマサポート

保護の状態を確認

コンピュータの保護が万全ではない場合、タスクバーの右端の Windows 通知領域に、保護の状態のアイコン  が表示されます。このアイコンは、保護の状態により、赤色または黄色で表示されます。

保護の状態を確認するには

- 保護の状態のアイコンをクリックして McAfee SecurityCenter を開き、問題があれば修復します。

更新状態を確認

更新の有無を確認中である場合、タスクバーの右端の Windows 通知領域に更新アイコン  が表示されます。

更新の状態を確認するには

- 更新アイコンを選択すると、更新の状態がツールヒントに表示されます。

保護の状態について

コンピュータ全体のセキュリティ保護の状態は、McAfee SecurityCenter の **【保護されていますか？】** の下に表示されます。

保護の状態により、コンピュータが最新のセキュリティ脅威に対して完全に保護されているかどうか、対応の必要な問題があるかどうか、およびそれらの解決方法を確認できます。1 つの問題が複数の保護カテゴリに影響を与える場合、その問題を修復すると、複数のカテゴリが完全に保護されている状態に戻る場合があります。

保護の状態に影響を与える要因としては、外部のセキュリティ脅威、コンピュータにインストールされているセキュリティ製品、インターネットにアクセスする製品、およびこれらのセキュリティとインターネット製品の設定方法などがあります。

標準設定では、迷惑メール対策またはコンテンツのブロック機能がインストールされていない場合、これらの致命的ではない問題は自動的に無視され、全体の保護の状態を追跡されません。ただし、保護の問題のあとに **【無視】** リンクが表示される場合は、その問題を修復する必要があると判断するなら、無視することを選択できます。

保護されていますか？

McAfee SecurityCenter の **【保護されていますか？】** の下では、コンピュータ全体の保護の状態を確認できます。

- コンピュータが完全に保護されている場合（緑色）、**【はい】** が表示されます。
- コンピュータの一部が保護されていない場合（黄色）またはまったく保護されていない場合（赤色）、**【いいえ】** が表示されます。

保護の問題を自動的に解決するには、保護の状態の横にある **【修復】** をクリックします。ただし、解決されない問題が 1 つ以上あり、対応が必要な場合は、問題に続くリンクをクリックして推奨される対応を実行してください。

保護のカテゴリおよびタイプについて

McAfee SecurityCenter の【保護されていますか？】パネルでは、次のカテゴリおよびタイプごとの保護の状態を表示できます。

- コンピュータとファイル
- インターネットとネットワーク
- E メールとメッセージ
- パレンタルコントロール

McAfee SecurityCenter に表示される保護タイプは、インストールされている製品によって異なります。たとえば McAfee Data Backup ソフトウェアがインストールされている場合、「PC の状態」という保護タイプが表示されます。

カテゴリに保護の問題が存在しない場合、状態は緑色で表示されます。緑色のカテゴリをクリックすると、有効になっている保護タイプに続いて、すでに無視されている問題のリストが右側に表示されます。問題が存在しない場合、問題のかわりにウイルスについての報告が表示されます。【設定】をクリックしてそのカテゴリについてのオプションを変更することもできます。

カテゴリ内のすべての保護タイプの状態が緑色である場合、カテゴリの状態は緑色となります。同様に、すべての保護カテゴリの状態が緑色である場合、全体の保護の状態は緑色となります。

保護カテゴリの状態が黄色である場合は、問題を修復または無視して、保護の問題を解決します。問題が解決すると、状態は緑色に変わります。

コンピュータとファイルの保護について

コンピュータとファイルの保護カテゴリは、次の保護タイプから構成されます。

- **ウイルス対策** — リアルタイムスキャンは、ウイルス、ワーム、トロイの木馬、不審なスクリプト、複合的な攻撃、その他の脅威を阻止し、コンピュータを保護します。ファイル（圧縮された .exe ファイル、ブートセクタ、メモリ、重要なファイルを含む）がユーザまたはコンピュータによりアクセスされると、自動的にスキャンが実行され、検出されたファイルに対してウイルス駆除が試行されます。
- **スパイウェア対策** — スパイウェア対策は、無断で個人情報収集して転送するスパイウェア、アドウェア、およびその他の怪しいプログラムを迅速に検出して削除します。
- **SystemGuards** — SystemGuards（システムガード）は、コンピュータに対する変更を検出し、変更が行われるとアラートを表示します。アラートが表示されたら、変更を確認して、許可するかどうかを決定できます。
- **Windows の保護** — Windows の保護では、コンピュータの Windows Update の状態が表示されます。McAfee VirusScan がインストールされている場合、バッファオーバーフロー保護も使用できます。

[コンピュータとファイル] の保護の状態に影響を与える要因の 1 つとしては、外部からのウイルス脅威があります。たとえば、ウイルスの急激な増加が発生した場合、現在のウイルス対策ソフトウェアで保護できるでしょうか。また、他の要因としては、ウイルス対策ソフトウェアの設定、コンピュータを最新の脅威に対して保護するために最新の検出定義ファイルでソフトウェアが継続的に更新されているかなどがあります。

コンピュータとファイルの設定パネルを表示

[コンピュータとファイル] で問題が存在しない場合には、情報パネルから設定パネルを開くことができます。

コンピュータとファイルの設定パネルを開くには

- 1 [ホーム] パネルで、[コンピュータとファイル] をクリックします。
- 2 右パネルで [設定] をクリックします。

インターネットとネットワークの保護について

インターネットとネットワークの保護カテゴリは、次の保護タイプから構成されます。

- **ファイアウォールによる保護** — ファイアウォールによる保護は、侵入や不審なネットワークトラフィックからコンピュータを保護します。また、内向き（受信）と外向き（送信）それぞれのインターネット接続を管理します。
- **ワイヤレス保護** — ワイヤレス保護は、不正侵入とデータの盗聴から、家庭の無線 LAN を保護します。ただし、現在外部のワイヤレスネットワークに接続している場合、ネットワークのセキュリティレベルにより保護のレベルは異なります。
- **Web ブラウジング保護** — Web ブラウジング保護を有効にすると、インターネットの閲覧中にわずらわしい広告、ポップアップ、Web バグは表示されません。
- **フィッシング詐欺対策** — フィッシング詐欺対策では、E メール、メッセージャー、ポップアップなどのハイパーリンクを使用して個人情報を探取しようとする、詐欺目的の Web サイトのブロックを実現できます。
- **個人情報保護** — 個人情報保護では、重要な情報や機密情報の送信をブロックし、インターネットへの流出を防ぐことができます。

インターネットとネットワークの設定パネルを表示

[インターネットとネットワーク] で問題が存在しない場合には、情報パネルから設定パネルを開くことができます。

[インターネットとネットワーク] 設定パネルを開くには

- 1 [ホーム] パネルで、[インターネットとネットワーク] をクリックします。
- 2 右パネルで **[設定]** をクリックします。

E メールとメッセージの保護について

E メールとメッセージの保護カテゴリは、次の保護タイプから構成されます。

- **E メール保護** — E メール保護は、受信および送信する E メールメッセージと添付ファイルを自動的にスキャンし、ウイルス、スパイウェア、および潜在的な脅威を駆除します。
- **迷惑メール対策** — 迷惑メール対策は、迷惑メールメッセージが受信ボックスに配信されることを防ぎます。
- **メッセージ保護** — メッセージ（IM）保護は、受信および送信するメッセージ添付ファイルを自動的にスキャンし、ウイルス、スパイウェア、および潜在的な脅威を駆除します。また、メッセージクライアントにより、好ましくないコンテンツや個人情報がインターネットを介して転送されることを防ぎます。
- **安全なネットサーフィンの保護** — McAfee SiteAdvisor ブラウザプラグインがインストールされていると、アクセスした Web サイトや、Web 検索結果に表示された Web サイトを評価し、スパイウェア、迷惑メール、およびオンライン詐欺からユーザを保護します。E メールの送信、ダウンロードファイル、リンク先、ポップアップや第三者のトラッキング Cookie などの迷惑行為に対するサイトの検査結果を示す、安全性評価の詳細を表示できます。

E メールとメッセージの設定パネルを表示

[E メールとメッセージ] で問題が存在しない場合には、情報パネルから設定パネルを開くことができます。

[E メールとメッセージ] 設定パネルを開くには

- 1 [ホーム] パネルで、[E メールとメッセージ] をクリックします。
- 2 右パネルで [設定] をクリックします。

パレナルコントロールの保護について

パレナルコントロールの保護カテゴリーは、次の保護タイプから構成されます。

- **パレナルコントロール** — コンテンツのブロックは、危険性のある Web サイトをブロックし、好ましくないインターネットコンテンツからユーザを保護します。ユーザのインターネットのアクティビティや利用を監視したり制限できます。

パレナルコントロールの設定パネルを表示

[パレナルコントロール] で問題が存在しない場合には、情報パネルから設定パネルを開くことができます。

[パレナルコントロール] 設定パネルを開くには

- 1 [ホーム] パネルで、[パレナルコントロール] をクリックします。
- 2 右パネルで [設定] をクリックします。

保護の問題を修復

保護の問題のほとんどは自動的に解決されます。ただし、解決されない問題がある場合は、自分で解決する必要があります。

保護の問題を自動的に修復

保護の問題のほとんどは自動的に解決されます。

保護の問題を自動的に修復するには

- 保護の状態の横の **【修復】** をクリックします。

保護の問題を手動で修復

自動的に解消されない問題がある場合、問題に続くリンクをクリックして推奨される対応を確認してください。

保護の問題を手動で修復するには

- 次の操作のいずれかを実行します。
 - コンピュータのフルスキャンが過去 30 日以上実行されていない場合は、メインの保護の状態の左にある **【スキャン】** をクリックして手動スキャンを実行します（この項目は、McAfee VirusScan がインストールされている場合にのみ表示されます）。
 - 検出定義（DAT）ファイルが最新でない場合は、メインの保護の状態の左にある **【更新】** をクリックして保護を更新します。
 - プログラムがインストールされていない場合は、**【万全な保護を入手】** をクリックしてインストールします。
 - プログラムのコンポーネントが不足している場合は、再インストールします。
 - 万全の保護を行うためにプログラムの登録が必要な場合は、**【今すぐ登録】** をクリックして登録します（この項目は、1 つ以上のプログラムが期限切れである場合に表示されます）。
 - プログラムが期限切れである場合は、**【契約状況を確認】** をクリックしてアカウントの状態を確認します（この項目は、1 つまたは複数のプログラムが期限切れである場合に表示されます）。

McAfee SecurityCenter 情報を表示

保護の状態のパネルの下部にある [SecurityCenter の情報] では、McAfee SecurityCenter のオプションにアクセスできます。また、最終更新日時、最後のスキャン日時 (McAfee VirusScan がインストールされている場合)、および使用中のマカフィー製品の契約の有効期限を確認できます。

McAfee SecurityCenter の設定パネルを表示

オプションを変更する場合は、[ホーム] パネルから McAfee SecurityCenter の設定パネルを開くことができます。

McAfee SecurityCenter の設定パネルを開くには

- [ホーム] パネルの [SecurityCenter の情報] で、[設定] をクリックします。

インストールされている製品の情報を表示

製品のバージョン番号および後に更新されたときを示す、インストールされている製品のリストが表示されます。

マカフィー製品情報を表示するには

- [ホーム] パネルの [SecurityCenter の情報] で、[詳細を表示] をクリックして製品情報ウィンドウを開きます。

詳細メニューを使用

最初に McAfee SecurityCenter を開くと、左の列に標準メニューが表示されます。上級者の場合は、[詳細メニュー] をクリックして、その場所により詳細なコマンドメニューを開くことができます。最後に使用したメニューは、次に McAfee SecurityCenter を開いた際に表示されます。

詳細メニューは次の項目から構成されます。

- ホーム
- レポートとログ (過去 30、60、および 90 日間のタイプごとの [最近のイベント] リストとログも含まれます)
- 設定
- 復元
- ツール

第 4 章

McAfee SecurityCenter のオプションの設定

McAfee SecurityCenter は、コンピュータ全体のセキュリティ保護の状態を表示し、ユーザがマカフィー ユーザ アカウントを作成できるようにしたり、最新の製品更新を自動インストールしたり、ウイルスの急激な増加、セキュリティの脅威、および製品の更新をアラートとサウンドを使用して自動的に通知したりします。

[SecurityCenter の設定] パネルでは、次の機能についての McAfee SecurityCenter のオプションを変更できます。

- 保護の状態
- ユーザ
- 自動更新
- アラート

この章の内容

保護の状態の設定	24
ユーザオプションの設定	25
更新オプションの設定	28
アラートのオプションの設定	32

保護の状態の設定

コンピュータ全体のセキュリティ保護の状態は、McAfee SecurityCenter の **【保護されていますか？】** の下に表示されます。

保護の状態により、コンピュータが最新のセキュリティ脅威に対して完全に保護されているかどうか、対応の必要な問題があるかどうか、およびそれらの解決方法を確認できます。

標準設定では、迷惑メール対策またはコンテンツのブロック機能がインストールされていない場合、これらの致命的でない問題は自動的に無視され、全体の保護の状態を追跡されません。ただし、保護の問題のあとに **【無視】** リンクが表示される場合は、修復を行わずに問題を無視することを選択できます。以前に無視した問題を後で修復する場合、追跡対象となる保護の状態にその問題を追加できます。

無視された問題の設定

コンピュータ全体の保護の状態の一部として追跡する対象に、問題を追加または除外できます。保護の問題の後ろに **【無視】** リンクが表示されるとき、修復を行わない場合は問題を無視することを選択できます。以前に無視した問題を後で修復する場合、追跡対象となる保護の状態にその問題を追加できます。

無視された問題を設定するには

- 1 **【SecurityCenter の情報】** で **【設定】** をクリックします。
- 2 **【保護の状態】** の横の矢印をクリックしてパネルを展開してから、**【詳細設定】** をクリックします。
- 3 **【無視された問題】** パネルで、次のいずれかの操作を実行します。
 - 以前に無視した問題を追跡対象に追加するには、チェックボックスをオフにしてください。
 - 問題追跡対象から除外するには、チェックボックスをオンにしてください。
- 4 **【OK】** をクリックします。

ユーザオプションの設定

ユーザ権限を必要とするマカフィープログラムを実行している場合、標準設定では、その権限はコンピュータの Windows のユーザアカウントと一致します。マカフィー ユーザ アカウントを使用するよう切り替えると、これらのプログラムのユーザをより簡単に管理できます。

マカフィー ユーザ アカウントを使用するよう切り替えた場合、既存のユーザ名およびパレンタル コントロール プログラムの権利は自動的にインポートされます。ただし、初めて切り替える場合は管理者アカウントを作成する必要があります。管理者アカウントを作成したあと、ほかのマカフィー ユーザ アカウントの作成および設定を実行します。

マカフィー ユーザ アカウントに切り替え

標準設定では、Windows のユーザアカウントが使用されます。ただし、マカフィー ユーザ アカウントに切り替えると、Windows の追加ユーザアカウントを作成する必要がなくなります。

マカフィー ユーザ アカウントに切り替えるには

- 1 [SecurityCenter の情報] で [設定] をクリックします。
- 2 [ユーザ] の横の矢印をクリックしてパネルを展開してから、[詳細設定] をクリックします。
- 3 マカフィー ユーザ アカウントを使用するには、[切り替え] をクリックします。

初めてマカフィー ユーザ アカウントに切り替える場合は、**管理者アカウントを作成** (25 ページ) する必要があります。

管理者アカウントを作成

初めてマカフィーユーザを使用するよう切り替えた場合、管理者アカウントの作成を要求されます。

管理者アカウントを作成するには

- 1 [パスワード] ボックスにパスワードを入力し、[パスワードの確認] ボックスでパスワードを再入力します。
- 2 パスワードを忘れた場合のための質問をリストから選択し、[回答] ボックスに秘密の質問に対する回答を入力します。
- 3 [適用] をクリックします。

設定が終了すると、パネルのユーザ アカウント タイプが既存のユーザ名およびパレンタル コントロール プログラムの権限（存在する場合）で更新されます。初めてユーザアカウントを設定する場合は、[ユーザの管理] パネルが表示されます。

ユーザオプションの設定

マカフィー ユーザ アカウントを使用するよう切り替えた場合、既存のユーザ名およびパレンタル コントロール プログラムの権利は自動的にインポートされます。ただし、初めて切り替える場合は管理者アカウントを作成する必要があります。管理者アカウントを作成したあと、他のマカフィー ユーザ アカウントの作成および設定を実行します。

ユーザオプションを設定するには

- 1 [SecurityCenter の情報] で [設定] をクリックします。
- 2 [ユーザ] の横の矢印をクリックしてパネルを展開してから、[詳細設定] をクリックします。
- 3 [ユーザアカウント] で、[追加] をクリックします。
- 4 [ユーザ名] ボックスにユーザ名を入力します。
- 5 [パスワード] ボックスにパスワードを入力し、[パスワードの確認] ボックスでパスワードを再入力します。
- 6 McAfee SecurityCenter の開始時にこの新しいユーザで自動的にログインするには、[スタートアップユーザ] チェックボックスをオンにします。
- 7 [ユーザアカウントの種類] でこのユーザのアカウントタイプを選択してから、[作成] をクリックします。

注: ユーザアカウントを作成したあと、[パレンタルコントロール] で制限付きユーザのの設定を実行する必要があります。

- 8 ユーザのパスワード、自動ログイン、またはアカウントタイプを編集するには、リストからユーザ名を選択し、[編集] をクリックします。
- 9 完了したら、[適用] をクリックします。

管理者パスワードを取得

管理者パスワードを忘れてしまった場合、救済方法が用意されています。

管理者パスワードを取得するには

- 1 McAfee SecurityCenter の [M] アイコン  をクリックしてから、[ユーザの切り替え] をクリックします。
- 2 [ユーザ名] リストで [管理者] を選択し、[パスワードを忘れた場合] をクリックします。
- 3 管理者アカウントの作成時に選択した秘密の質問に対する回答を入力します。
- 4 [送信] をクリックします。

忘れてしまった管理者パスワードが表示されます。

管理者パスワードを変更

管理者パスワードを忘れてしまった場合、または管理者パスワードが攻撃を受けている可能性がある場合は、管理者パスワードを変更できます。

管理者パスワードを変更するには

- 1 McAfee SecurityCenter の [M] アイコン  をクリックしてから、[ユーザの切り替え] をクリックします。
- 2 [ユーザ名] リストで [管理者] を選択し、[パスワードの変更] をクリックします。
- 3 [古いパスワード] ボックスに、既存のパスワードを入力します。
- 4 [パスワード] ボックスに新しいパスワードを入力し、[パスワードの確認] ボックスでパスワードを再入力します。
- 5 [OK] をクリックします。

更新オプションの設定

McAfee SecurityCenter は、インターネットに接続している間、4 時間ごとにすべてのマカフィー サービスの更新の有無を自動的に確認し、最新の製品の更新を自動的にインストールします。ただし、タスクバーの右端の通知領域にある McAfee SecurityCenter アイコンを使用すると、いつでも手動で更新を確認できます。

更新を自動確認

インターネットに接続している場合、McAfee SecurityCenter は更新の有無を 4 時間ごとに自動的に確認します。ただし、更新のダウンロードまたはインストールの前に通知するように McAfee SecurityCenter を設定することもできます。

更新の自動確認を実行するには

- 1 [SecurityCenter の情報] で [設定] をクリックします。
- 2 [自動更新が有効です] 状態の横の矢印をクリックしてパネルを開いてから、[詳細設定] をクリックします。
- 3 [更新オプション] パネルで、次のいずれかを選択します。
 - サービスが更新されたら自動的に更新をインストールして通知 (推奨) (28 ページ)
 - 更新を自動的にダウンロードし、インストール可能な状態になったら通知 (29 ページ)
 - 更新をダウンロードする前に通知 (29 ページ)
- 4 [OK] をクリックします。

注: 最大限の保護を実現するため、自動的に更新の有無を確認してインストールするように McAfee SecurityCenter を設定することをお勧めします。ただし、セキュリティサービスの更新を手動のみで行いたい場合は、自動更新を無効化 (30 ページ) できます。

更新を自動的にダウンロードしてインストール

McAfee SecurityCenter の [更新オプション] で [サービスが更新されたら自動的に更新をインストールして通知 (推奨)] を選択した場合、McAfee SecurityCenter は自動的に更新のダウンロードおよびインストールを実行します。

更新を自動ダウンロード

[更新オプション] で **[更新を自動的にダウンロードし、インストール可能な状態になったら通知]** を選択した場合、McAfee SecurityCenter は自動的に更新をダウンロードし、インストールの準備が整うとユーザーに通知します。そこで、更新をインストールするか、**更新を延期** (30 ページ) するかを選択します。

自動ダウンロードされた更新をインストールするには

- 1 アラートの **[今すぐ製品を更新]** をクリックしてから **[OK]** をクリックします。

契約を確認するため、ダウンロード実行前に Web サイトへのログインを要求されることがあります。

- 2 契約を確認したあと、[更新] パネルの **[更新]** をクリックして更新のダウンロードおよびインストールを実行します。契約が期限切れである場合、アラートの **[プログラムの契約を更新]** をクリックして画面の指示に従います。

注: 更新を完了するためにコンピュータを再起動するようメッセージが表示される場合もあります。再起動する前に、作業中のデータをすべて保存し、すべてのプログラムを閉じてください。

更新のダウンロード前に通知

[更新オプション] パネルで **[更新をダウンロードする前に通知]** を選択すると、McAfee SecurityCenter は更新をダウンロードする前にユーザーに通知します。攻撃の脅威を排除するために、セキュリティサービスの更新のダウンロードおよびインストールを実行することを選択できます。

更新のダウンロードおよびインストールを実行するには

- 1 アラートの **[今すぐ製品を更新]** を選択してから **[OK]** をクリックします。
- 2 Web サイトにログインするように要求するメッセージが表示された場合は、ログインを実行します。

更新が自動的にダウンロードされます。

- 3 更新のインストールが終了したら、**[OK]** をクリックします。

注: 更新を完了するためにコンピュータを再起動するようメッセージが表示される場合もあります。再起動する前に、作業中のデータをすべて保存し、すべてのプログラムを閉じてください。

自動更新を無効化

最高の保護機能を提供するため、自動的に更新の有無を確認してインストールするように McAfee SecurityCenter を設定することをお勧めします。ただし、セキュリティサービスの更新を手動のみで行いたい場合は、自動更新を無効にできます。

注: 少なくとも 1 週間に一度は更新を手動で確認 (31 ページ) してください。更新の有無を確認しない場合、コンピュータは最新のセキュリティでは保護されなくなります。

自動更新を無効にするには

- 1 [SecurityCenter の情報] で [設定] をクリックします。
- 2 [自動更新が有効です] 状態の横の矢印をクリックしてパネルを展開します。
- 3 [オフ] をクリックします。
- 4 [はい] をクリックして変更を確認します。

状態はヘッダで更新されます。

7 日以内に更新の有無を手動で確認しない場合には、更新の有無の確認を要求するアラートが表示されます。

更新を延期

アラートが表示されたときにセキュリティサービスを更新する時間がない場合には、アラートをあとで表示するか無視するかを選択できます。

更新を延期するには

- 次の操作のいずれかを実行します。
 - アラートの [あとで表示] を選択し、[OK] をクリックします。
 - 何も操作をしないでアラートを閉じる場合は、[このアラートを閉じる] を選択してから [OK] をクリックします。

更新を手動で確認

McAfee SecurityCenter は、インターネットに接続している間、4 時間ごとに更新の有無を自動的に確認し、最新の製品の更新をインストールします。ただし、タスクバーの右端の Windows 通知領域にある McAfee SecurityCenter アイコンを使用すると、いつでも手動で更新を確認できます。

注: 最大限の保護を実現するため、自動的に更新の有無を確認してインストールするように McAfee SecurityCenter を設定することをお勧めします。ただし、セキュリティサービスの更新を手動のみで行いたい場合は、**自動更新を無効化** (30 ページ) できます。

更新を手動で確認するには

- 1 コンピュータがインターネットに接続されていることを確認します。
- 2 タスクバーの右端の Windows 通知領域に表示される McAfee SecurityCenter の [M] アイコン  を右クリックし、[更新] をクリックします。

McAfee SecurityCenter によって更新の有無の確認が行われている間も、ほかのタスクを継続して実行できます。

Windows のタスクバーの右端の通知領域には、アニメーションアイコンが表示されます。McAfee SecurityCenter による確認が完了すると、アイコンは自動的に表示されなくなります。

- 3 Web サイトにログインして契約を確認するように要求するメッセージが表示された場合は、Web サイトにログインして契約を確認します。

注: 更新を完了するためにコンピュータを再起動するようメッセージが表示される場合もあります。再起動する前に、作業中のデータをすべて保存し、すべてのプログラムを閉じてください。

アラートのオプションの設定

McAfee SecurityCenter は、アラートとサウンドを使用して、ウイルスの急激な増加、セキュリティの脅威、製品の更新を自動的に通知します。ただし、早急な対応が必要なアラートのみを表示するように McAfee SecurityCenter を設定することもできます。

アラートのオプションの設定

McAfee SecurityCenter は、アラートとサウンドを使用して、ウイルスの急激な増加、セキュリティの脅威、製品の更新を自動的に通知します。ただし、早急な対応が必要なアラートのみを表示するように McAfee SecurityCenter を設定することもできます。

アラートのオプションを設定するには

- 1 [SecurityCenter の情報] で [設定] をクリックします。
- 2 [アラート] の横の矢印をクリックしてパネルを展開してから、[詳細設定] をクリックします。
- 3 [アラートのオプション] パネルで、次のいずれかを選択します。
 - ウイルスの急激な増加、またはセキュリティの脅威が発生した場合にアラートを表示
 - ゲームモードが検出されたときに情報アラートを表示
 - アラートが発生したときに音を鳴らす
 - Windows の起動時にマカフィーの起動画面を表示
- 4 [OK] をクリックします。

注: アラート自体から今後の情報アラートを無効にするには、[今後このアラートを表示しない] チェックボックスをオンにします。あとで、[情報アラート] パネルでアラートを再有効化できます。

情報アラートの設定

情報アラートは、早急な対応を必要としないイベントが発生したことを通知します。今後の情報アラートを無効にした場合、あとで [情報アラート] パネルでアラートを再有効化できます。

情報アラートを設定するには

- 1 [SecurityCenter の情報] で [設定] をクリックします。
- 2 [アラート] の横の矢印をクリックしてパネルを展開してから、[詳細設定] をクリックします。
- 3 [SecurityCenter の設定] で [情報アラート] をクリックします。

- 4 [情報アラートを非表示] チェックボックスをオフにし、表示するリストのアラートのチェックボックスをオフにします。
- 5 [OK]をクリックします。

第 5 章

よく使う機能を実行

[ホーム] パネルの表示、最近のイベントの表示、コンピュータネットワークの管理（対象のネットワークの管理機能のあるコンピュータの場合）、コンピュータの保守などのよく使う機能を実行します。McAfee Data Backup がインストールされている場合、データのバックアップも実行できます。

この章の内容

よく使う機能を実行	35
最近のイベントを表示	36
コンピュータを自動的に保守	37
コンピュータを手動で保守	38
ネットワークを管理	39
ウイルスの詳細情報	40

よく使う機能を実行

[ホーム] パネルの表示、最近のイベントの表示、コンピュータの保守、ネットワークの管理（対象のネットワークの管理機能のあるコンピュータの場合）、データのバックアップ（McAfee Data Backup がインストールされている場合）などのよく使う機能を実行します。

よく使う機能を実行するには

- 標準メニューの **【よく使う機能】** で次のいずれかを実行します。
 - [ホーム] パネルに戻るには、**【ホーム】** をクリックします。
 - セキュリティソフトウェアにより検出された最近のイベントを表示するには、**【最近のイベント】** をクリックします。
 - 使用しないファイルの削除、データの最適化、および以前の設定へのコンピュータの復元を実行するには、**【コンピュータの保守】** をクリックします。
 - コンピュータネットワークを管理するには、対象のネットワークの管理機能のあるコンピュータで **【ネットワークの管理】** をクリックします。

Network Manager は、ネットワーク上のコンピュータに対して、セキュリティの弱点がないかどうかを監視します。このため、ユーザはネットワークのセキュリティ上の問題を識別できます。

- McAfee Data Backup がインストールされている場合、ファイルのバックアップを作成するには、**[データのバックアップ]** をクリックします。

自動バックアップにより、バックアップが必要な大切なファイルのコピーが任意の場所に保存されます。ファイルを暗号化し、CD/DVD、USB、外部ドライブ、またはネットワークドライブに保存します。

ヒント: 利便性を考慮し、よく使う機能にはさらに 2 つのアクセス方法を用意しました ([詳細メニュー] の **[ホーム]**、およびタスクバーの右端の McAfee SecurityCenter の **[M]** アイコンの **[クイックリンク]** メニュー)。[詳細メニュー] の **[レポートとログ]** から、最近のイベントおよび包括的なログをタイプごとに表示することもできます。

最近のイベントを表示

最近のイベントは、コンピュータに対する変更が発生したときに記録されます。たとえば、保護タイプが有効または無効にされた場合、脅威が削除された場合、インターネット接続の試行がブロックされた場合です。最近のイベント 20 件と、その詳細が表示されます。

イベントの詳細については、関連製品のヘルプファイルを参照してください。

最近のイベントを表示するには

- 1 メインの McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[最近のイベントの表示]** をクリックします。

最近のイベントがある場合、日付および簡単な説明とともにリストに表示されます。

- 2 **[最近のイベント]** で、**[詳細]** パネルで詳細情報を表示するイベントを選択します。

実行できる操作がある場合は、**[オプションの選択]** に表示されます。

- 3 より包括的なイベントのリストを表示するには、**[ログを表示]** をクリックします。

コンピュータを自動的に保守

貴重なドライブ容量を解放してコンピュータのパフォーマンスを最適化するには、McAfee QuickClean またはディスク最適化プログラムのタスクを定期的に行うスケジュールを設定します。これらのタスクには、ファイルとフォルダの削除、破棄、および最適化が含まれます。

コンピュータを自動的に保守するには

- 1 McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[コンピュータの保守]** をクリックします。
- 2 **[タスクスケジューラ]** で **[開始]** をクリックします。
- 3 操作リストで、**[QuickClean]** または **[ディスク最適化プログラム]** をクリックします。
- 4 次の操作のいずれかを実行します。
 - 既存のタスクを変更する場合は、タスクを選択して **[変更]** をクリックします。画面に表示された指示に従います。
 - 新しいタスクを作成する場合は、**[タスク名]** ボックスに名前を入力してから **[作成]** をクリックします。画面に表示された指示に従います。
 - タスクを削除する場合は、タスクを選択して **[削除]** をクリックします。
- 5 **[タスクの概要]** で、最後にタスクが実行された日時、次に実行される日時、およびその状態を確認します。

コンピュータを手動で保守

使用しないファイルの削除、データの最適化、または以前の設定へコンピュータの復元を実行するには、手動による保守タスクを実行します。

コンピュータを手動で保守するには

- 次の操作のいずれかを実行します。
 - QuickClean を使用する場合は、メインの McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[コンピュータの保守]** をクリックしてから **[開始]** をクリックします。
 - ディスクデフラグを使用する場合は、メインの McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[コンピュータの保守]** をクリックしてから **[分析]** をクリックします。
 - システム復元を使用するには、詳細メニューで、**[ツール]**、**[システムの復元]**、**[開始]** の順にクリックします。

使用しないファイルとフォルダを削除

貴重なドライブ容量を解放してコンピュータのパフォーマンスを最適化するには、McAfee QuickClean を使用します。

使用しないファイルとフォルダを削除するには

- 1 McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[コンピュータの保守]** をクリックします。
- 2 **[QuickClean]** で **[開始]** をクリックします。
- 3 画面に表示された指示に従います。

ファイルとフォルダを最適化

ファイルの断片化は、ファイルやフォルダが削除されて新しいファイルが追加された場合に起こります。この断片化によりディスクアクセスは遅くなり、コンピュータ全体のパフォーマンスも低下しますが、通常その度合いは深刻ではありません。

ファイルの断片をハードディスクの隣り合うセクタに書き換えてアクセスおよび読み込みの速度を高めるには、最適化を実行します。

ファイルとフォルダを最適化するには

- 1 McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[コンピュータの保守]** をクリックします。
- 2 **[ディスク最適化プログラム]** で **[分析]** をクリックします。
- 3 画面に表示された指示に従います。

コンピュータを以前の設定に復元

復元ポイントは、Windows が定期的に保存するコンピュータの記録、および重要なイベント発生時（プログラムまたはドライバのインストール時など）のコンピュータの記録です。また、いつでも独自の復元ポイントを作成して名前を付けることができます。

コンピュータに対して悪影響を与える変更を破棄して以前の設定に戻すには、復元ポイントを使用します。

コンピュータを以前の設定に復元するには

- 1 詳細メニューで **[ツール]**、**[システムの復元]** の順にクリックします。
- 2 **[システムの復元]** で **[開始]** をクリックします。
- 3 画面に表示された指示に従います。

ネットワークを管理

コンピュータにネットワーク管理権限がある場合、Network Manager を使用して、ネットワーク上のコンピュータにセキュリティの弱点がないかどうかを監視し、セキュリティ上の問題を識別できます。

コンピュータの保護の状態がネットワークで監視されない場合は、コンピュータはそのネットワークの一部ではないか、そのネットワークで管理されていないメンバーであるかのいずれかとなります。詳細については、Network Manager のヘルプファイルを参照してください。

ネットワークを管理するには

- 1 メインの McAfee SecurityCenter アイコンを右クリックしてから **[クイックリンク]** を選択し、**[ネットワークの管理]** をクリックします。
- 2 ネットワーク地図でこのコンピュータを示すアイコンをクリックします。
- 3 **[オプションの選択]** で、**[このコンピュータを監視]** をクリックします。

ウイルスの詳細情報

ウイルス情報ページおよびウイルス地図を使用すると、次の内容を実行できます。

- 最新のウイルス、虚偽のウイルス警告メール、その他の脅威の詳細を表示します。
- 無料のウイルス駆除ツールを入手してコンピュータを修復します。
- 世界のどの地域で多くのコンピュータが感染しているかを示す情報をリアルタイムで取得します。

ウイルスの詳細情報を確認するには

- 1 詳細メニューで **[ツール]**、**[ウイルス情報]** の順にクリックします。
- 2 次の操作のいずれかを実行します。
 - 無料のウイルス情報ページを使用してウイルスを調べます。
 - マカフィーの Web サイトで世界ウイルス地図を使用してウイルスを調べます。

第 6 章

McAfee QuickClean

インターネットを閲覧すると、不要なファイルがコンピュータ上にすぐに蓄積されてしまいます。McAfee QuickClean を使用すると、個人情報を保護し、インターネットや E メールを利用することで蓄積した不要なファイルを削除できます。McAfee QuickClean は、インターネットの閲覧中に蓄積した個人情報を含むファイル（Cookie、E メール、ダウンロードファイル、履歴など）を識別して削除します。McAfee QuickClean は、このような重要な情報を安全に削除することで個人情報を保護します。

また、McAfee QuickClean は怪しいプログラムも削除します。排除するファイルを指定すると、必要な情報を削除することなく不要なファイルを取り除くことができます。

この章の内容

McAfee QuickClean の機能について	42
コンピュータをクリーニング	43

McAfee QuickClean の機能について

このセクションでは、McAfee QuickClean の機能について説明します。

機能

McAfee QuickClean は、データの断片を安全に削除する効率的で使いやすいツールです。貴重なドライブ容量を解放して、コンピュータのパフォーマンスを最適化できます。

第 7 章

コンピュータをクリーニング

McAfee QuickClean を使用すると、ファイルやフォルダを安全に削除できます。

インターネットを閲覧すると、ブラウザによりインターネットページと画像がそれぞれディスク上のキャッシュフォルダにコピーされます。これにより、再度同じページを表示したときに、ページが迅速に読み込まれます。インターネットで同じページを何度も閲覧し、そのページのコンテンツが頻繁に変更されない場合には、ファイルのキャッシュは有用です。しかし、多くの場合、キャッシュされたファイルは使用されないため、削除しても問題ありません。

次のクリーナを使用してさまざまな項目を削除できます。

- ごみ箱クリーナ: Windows のごみ箱の中身を削除します。
- 一時ファイルクリーナ: 一時フォルダに保存されているファイルを削除します。
- ショートカットクリーナ: 機能していないショートカットや、関連するプログラムが存在しないショートカットを削除します。
- 破損ファイルの断片クリーナ: コンピュータから破損ファイルの断片を削除します。
- レジストリクリーナ: コンピュータ上に存在していないプログラムの Windows レジストリ情報を削除します。
- キャッシュクリーナ: インターネットの閲覧中に蓄積したキャッシュファイルを削除します。このようなファイルは通常、インターネット一時ファイルとして保存されます。
- Cookie クリーナ: Cookie を削除します。このようなファイルは通常、インターネット一時ファイルとして保存されます。
Cookie は、Web サーバの要求に応じて、Web ブラウザによりコンピュータ上に保存される小さなファイルです。この Web サーバの Web ページを表示するたびに、ブラウザにより Cookie がサーバに送信されます。これらの Cookie は付箋のような役割を果たします。Web サーバは、これにより、ユーザが表示したページやページを表示する頻度を追跡できます。
- ブラウザ履歴クリーナ: ブラウザ履歴を削除します。
- Outlook Express E メールクリーナと Outlook E メールクリーナ (削除済み項目と送信済み項目用): Outlook の送信済みフォルダと削除済みフォルダからメールを削除します。
- 最近使用した項目クリーナ: Microsoft Office 文書など、コンピュータ上に保存されている最近使用した項目を削除します。

- ActiveX とプラグインのクリーナ: ActiveX コントロールとプラグインを削除します。

ActiveX は、プログラムにコントロールを実装するための技術です。ActiveX コントロールを実装すると、プログラムのインターフェースにボタンを追加できます。このようなコントロールの多くは無害ですが、ActiveX の技術を使用してコンピュータから情報が収集される場合もあります。

プラグインは、機能を追加するために大きなアプリケーションに組み込む小さなソフトウェアプログラムです。プラグインを使用すると、HTML ドキュメントに組み込まれたファイルが Web ブラウザによりアクセスされ、実行されます。これらのファイルは通常、ブラウザで認識されない形式（アニメーション、映像、音声ファイルなど）です。

- システム復元ポイントクリーナ: 古いシステム復元ポイントをコンピュータから削除します。

この章の内容

McAfee QuickClean を使用	45
-----------------------------	----

McAfee QuickClean を使用

このセクションでは、McAfee QuickClean の使用法について説明します。

コンピュータをクリーニング

使用していないファイルおよびフォルダを削除し、ディスク容量を解放して、コンピュータをより効率的に動作させることができます。

コンピュータをクリーニングするには

- 1 詳細メニューで **[ツール]** をクリックします。
- 2 **[コンピュータの保守]** をクリックして、**[McAfee QuickClean]** の下の **[開始]** をクリックします。
- 3 次のいずれかの操作を実行します。
 - **[次へ]** をクリックして、リスト内の標準設定のクリーナを使用します。
 - 適切なクリーナを選択または選択を解除して、**[次へ]** をクリックします。最近使用したクリーナの場合、**[プロパティ]** をクリックして、削除しないプログラムの選択を解除できます。
 - **[標準設定に戻す]** をクリックして標準設定のクリーナに戻し、**[次へ]** をクリックします。
- 4 分析が実行されたら、**[次へ]** をクリックしてファイルの削除を確認します。このリストを展開して、削除対象のファイルとファイルの場所を確認できます。
- 5 **[次へ]** をクリックします。
- 6 次のいずれかの操作を実行します。
 - **[次へ]** をクリックして標準設定の **[Windows の通常の削除方法でファイルを削除します]** を選択します。
 - **[Shredder を使用して安全な方法でファイルを削除します]** をクリックして、削除する回数を指定します。McAfee Shredder で削除したファイルは復元できません。
- 7 **[完了]** をクリックします。
- 8 **[QuickClean の概要]** に、削除されたレジストリファイルの数と、ディスクおよびインターネットファイルのクリーンアップ後に増加したディスクの空き容量が表示されます。

第 8 章

McAfee Shredder

削除したファイルは、ごみ箱を空にした後でも、コンピュータから復元できます。ファイルを削除しても、ディスクドライブ上のファイルが保存してあった場所が使用されていない場所としてマークされるだけで、データはまだ消えずに残っています。誰にでも入手可能な専用のツールを使用すると、削除したドキュメントを復元することが可能です。McAfee Shredder は、不要なファイルを安全な方法で永久に消去してプライバシーを守ります。

ファイルを永久に削除するには、既存のファイルに新しいデータを繰り返し上書きする必要があります。Microsoft Windows では、すべてのファイル操作が遅くなるため、ファイルを安全に削除しません。ドキュメントを抹消しても、プログラムによっては開いているドキュメントのコピーが隠しファイルとして一時的に保存されることもあるため、常にドキュメントの復元を防ぐことができるとは限りません。Windows Explorer で表示したドキュメントを抹消しただけでは、それらのドキュメントの一時的なコピーはまだ残っている可能性があります。

注: 抹消されたファイルはバックアップされません。McAfee Shredder により削除されたファイルは、復元できません。

この章の内容

McAfee Shredder の機能について	48
McAfee Shredder で不要なファイルを消去	49

McAfee Shredder の機能について

このセクションでは、McAfee Shredder の機能について説明します。

機能

McAfee Shredder を使用すると、ごみ箱の中身、インターネットの一時ファイル、Web サイトの履歴、ファイル、フォルダ、ディスクを消去できます。

第 9 章

McAfee Shredder で不要なファイルを消去

McAfee Shredder は、ごみ箱の中身、インターネットの一時ファイル、Web サイトの履歴など、不要なファイルを安全な方法で永久に消去してプライバシーを守ります。抹消するファイルおよびフォルダを選択したり、その場所を指定できます。

この章の内容

McAfee Shredder を使用.....50

McAfee Shredder を使用

このセクションでは、McAfee Shredder の使用法について説明します。

ファイル、フォルダ、ディスクを抹消

ごみ箱を空にしても、ファイルはコンピュータ上に存在しています。ただし、ファイルを抹消すると、データは永久に削除され、ハッカーによりアクセスされることはありません。

ファイル、フォルダ、ディスクを抹消するには

- 1 詳細メニューで **[ツール]**、**[Shredder]** の順にクリックします。
- 2 次のいずれかの操作を実行します。
 - ファイルとフォルダを抹消するには **[ファイルおよびフォルダの消去]** をクリックします。
 - ディスクを抹消するには **[ディスク全体のデータの消去]** をクリックします。
- 3 以下の抹消のレベルのうち、いずれかを選択します。
 - **簡易**: 選択した項目を一度だけ抹消します。
 - **厳重**: 選択した項目を 7 回に渡って抹消します。
 - **カスタム**: 選択した項目を最高 10 回に渡って抹消します。抹消の回数が増えるほど、ファイルの削除の安全性レベルが高くなります。
- 4 **[次へ]** をクリックします。
- 5 次のいずれかの操作を実行します。
 - ファイルを抹消する場合は、**[抹消するファイルを選択]** リストで **[ごみ箱の中身]**、**[インターネット一時ファイル]** または **[Web サイトの履歴]** をクリックします。ディスクを抹消する場合は、ディスクをクリックします。
 - **[参照]** をクリックして抹消するファイルの場所を指定し、ファイルを選択します。
 - **[抹消するファイルを選択]** リストに抹消するファイルのパスを入力します。
- 6 **[次へ]** をクリックします。
- 7 操作を完了するには、**[完了]** をクリックします。
- 8 **[終了]** をクリックします。

第 10 章

McAfee Network Manager

McAfee Network Manager では、家庭のネットワーク内のコンピュータおよびコンポーネントに関する情報をグラフィカルに表示できます。McAfee Network Manager を使用すると、ネットワーク上の管理された各コンピュータの保護の状態を監視したり、管理されたコンピュータに存在する、報告されているセキュリティ上の脆弱性をリモートで修復できます。

McAfee Network Manager を使用する前に、よく利用する機能について理解することができます。これらの機能の設定と使用方法に関する詳細は、McAfee Network Manager のヘルプに書かれています。

この章の内容

機能	52
McAfee Network Manager のアイコンについて	53
管理されたネットワークをセットアップ	55
ネットワークをリモートで管理	63

機能

McAfee Network Manager には、次の機能が搭載されています。

グラフィカルなネットワーク地図

McAfee Network Manager のネットワーク地図では、家庭のネットワーク上のコンピュータおよびコンポーネントに関するセキュリティの状態を簡単に把握できます。ネットワークに対して変更が行われると（たとえば、コンピュータの追加など）、その変更はネットワーク地図に反映されます。ネットワーク地図を更新したり、ネットワークの名称を変更したり、ネットワーク地図のコンポーネントを表示または非表示にして表示画面をカスタマイズできます。また、ネットワーク地図に表示されているすべてのコンポーネントに関する詳細を表示することもできます。

リモート管理

McAfee Network Manager のネットワーク地図を使用すると、家庭のネットワーク上のコンピュータに関するセキュリティの状態を管理できます。管理されたネットワークに参加するようほかのコンピュータを招待したり、管理されたコンピュータの保護の状態を監視したり、ネットワーク上のリモートコンピュータから既知のセキュリティ上の脆弱性を修復できます。

McAfee Network Manager のアイコンについて

次の表に、McAfee Network Manager のネットワーク地図で通常使用されるアイコンを示します。

アイコン	説明
	オンラインの管理されたコンピュータを示します。
	オフラインの管理されたコンピュータを示します。
	McAfee 2007 セキュリティソフトウェアがインストールされている、管理されていないコンピュータを示します。
	オフラインの管理されていないコンピュータを示します。
	McAfee 2007 セキュリティソフトウェアがインストールされていないオンラインのコンピュータ、または未知のネットワークデバイスを示します。
	McAfee 2007 セキュリティソフトウェアがインストールされていないオフラインのコンピュータ、または未知のネットワークデバイスを示します。
	保護および接続されている該当項目を示します。
	対応を必要とする該当項目を示します。
	対応を必要とする、切断されている該当項目を示します。
	家庭用のワイヤレスルータを示します。
	標準の家庭用ルータを示します。
	インターネットが接続されている状態を示します。
	インターネットが切断されている状態を示します。

第 11 章

管理されたネットワークをセットアップ

ネットワーク地図上の項目を使用し、メンバー（コンピュータ）をネットワークに追加すると、管理されたネットワークをセットアップできます。

この章の内容

ネットワーク地図を使用	56
管理されたネットワークに参加	59

ネットワーク地図を使用

コンピュータをネットワークに接続するたびに、McAfee Network Manager はネットワークの状態を分析し、メンバー（管理されたメンバーまたは管理されていないメンバー）の有無、ルータの属性、およびインターネットの状態を確認します。メンバーが検出されない場合は、McAfee Network Manager は、現在接続されているコンピュータがネットワーク上の最初のコンピュータと見なし、そのコンピュータを管理者権限のある管理されたメンバーであると自動的に認識します。標準設定では、ネットワーク名には、最初にネットワークに接続した McAfee 2007 セキュリティソフトウェアがインストール済みのコンピュータのワークグループまたはドメイン名が含まれます。ただし、ネットワーク名はいつでも変更できます。

ネットワークに対して変更を行った場合（たとえば、コンピュータの追加など）は、ネットワーク地図をカスタマイズできます。たとえば、ネットワーク地図を更新したり、ネットワークの名称を変更したり、ネットワーク地図のコンポーネントを表示または非表示にして表示画面をカスタマイズできます。また、ネットワーク地図に表示されているすべてのコンポーネントに関する詳細を表示することもできます。

ネットワーク地図にアクセス

ネットワーク地図にアクセスするには、McAfee SecurityCenter の [よく使う機能] のリストから McAfee Network Manager を起動します。ネットワーク地図では、家庭のネットワーク上のコンピュータおよびコンポーネントに関する情報をグラフィカルに表示できます。

ネットワーク地図にアクセスするには

- 標準メニューまたは詳細メニューで、[ネットワークの管理] をクリックします。
ネットワーク地図が右パネルに表示されます。

注: ネットワーク地図に初めてアクセスする場合、ネットワーク地図が表示される前に、ネットワーク上のほかのコンピュータを信頼することを要求するメッセージが表示されます。

ネットワーク地図を更新

ネットワーク地図はいつでも更新できます（たとえば、管理されたネットワークに別のコンピュータが追加された場合など）。

ネットワーク地図を更新するには

- 1 標準メニューまたは詳細メニューで、**[ネットワークの管理]** をクリックします。
ネットワーク地図が右パネルに表示されます。
- 2 **[オプションの選択]** の下の **[ネットワーク地図を更新]** をクリックします。

注: **[ネットワーク地図を更新]** リンクは、ネットワーク地図で項目が選択されていない場合にのみ使用できます。項目の選択を解除するには、選択した項目をクリックするか、ネットワーク地図の空いている領域をクリックします。

ネットワーク名を変更

標準設定では、ネットワーク名には、最初にネットワークに接続した McAfee 2007 セキュリティソフトウェアがインストール済みのコンピュータのワークグループまたはドメイン名が含まれます。この名前が適切でない場合は、名前を変更できます。

ネットワーク名を変更するには

- 1 標準メニューまたは詳細メニューで、**[ネットワークの管理]** をクリックします。
ネットワーク地図が右パネルに表示されます。
- 2 **[オプションの選択]** の下の **[ネットワークの名称を変更]** をクリックします。
- 3 **[ネットワーク名の変更]** ボックスにネットワーク名を入力します。
- 4 **[OK]** をクリックします。

注: **[ネットワーク名の変更]** リンクは、ネットワーク地図で項目が選択されていない場合にのみ使用できます。項目の選択を解除するには、選択した項目をクリックするか、ネットワーク地図の空いている領域をクリックします。

ネットワーク地図で項目を表示/非表示

標準設定では、家庭のネットワーク上のコンピュータおよびコンポーネントはすべてネットワーク地図に表示されます。ただし、項目を非表示にした場合でも、いつでも再び表示するように変更できます。非表示にできるのは、管理されていない項目のみです。管理されたコンピュータは非表示にできません。

目的...	標準メニューまたは詳細メニューで、 [ネットワークの管理] をクリックしてから、次の操作を実行します。
項目をネットワーク地図に非表示	ネットワーク地図の項目をクリックしてから、 [オプションの選択] の下の [この項目を表示しない] をクリックします。確認のダイアログボックスで、 [はい] をクリックします。
非表示の項目をネットワーク地図に表示	[オプションの選択] で [非表示の項目を表示] をクリックします。

項目の詳細を表示

ネットワーク地図のコンポーネントを選択し、ネットワーク地図に表示されているすべてのコンポーネントに関する詳細を表示することができます。この情報には、コンポーネント名、保護の状態など、コンポーネントの管理に必要な情報が含まれます。

項目の詳細を表示するには

- 1 ネットワーク地図で項目のアイコンをクリックします。
- 2 **[詳細]** に、項目の詳細が表示されます。

管理されたネットワークに参加

コンピュータをリモートで管理する前、またはネットワーク上のほかのコンピュータをリモートで管理する権限を得る前に、そのコンピュータをネットワーク上の信頼するメンバーに設定する必要があります。ネットワークメンバーシップは、管理者権限のある既存のネットワークメンバー（コンピュータ）により、新しいコンピュータに対して許可されます。信頼するコンピュータのみがネットワークに参加するようにするには、コンピュータを許可するユーザとコンピュータに参加させるユーザが互いを認証する必要があります。

コンピュータがネットワークに参加する場合、そのコンピュータのマカフィーによる保護の状態をネットワーク上のほかのコンピュータに公開することが要求されます。保護の状態をほかのコンピュータに公開することに同意した場合、そのコンピュータはネットワークの管理されたメンバーとなります。保護の状態をほかのコンピュータに公開することを拒否した場合、そのコンピュータはネットワークの管理されていないメンバーとなります。通常、ネットワーク上の管理されていないメンバーとは、ほかのネットワーク機能（ファイルまたはプリンタの共有など）にアクセスするゲストコンピュータとなります。

注: ほかのマカフィー ネットワーク プログラム（McAfee Wireless Network Security、McAfee EasyNetwork）がインストールされている場合、ネットワークに参加すると、そのコンピュータはこれらのプログラムでも管理されたコンピュータとして認識されます。McAfee Network Manager のコンピュータに割り当てられた権限レベルは、すべてのマカフィー ネットワーク プログラムに適用されます。ほかのマカフィー ネットワーク プログラムで適用されるゲスト、すべて、管理者の内容の詳細については各プログラムのユーザガイドやヘルプを参照してください。

管理されたネットワークに参加

管理されたネットワークへの招待を受信すると、招待を受け入れるか拒否するかを選択できます。このコンピュータとネットワーク上のほかのコンピュータとで、セキュリティ設定（コンピュータのウイルス対策サービスが最新であるかどうかなど）を互いに監視するかどうかを指定することもできます。

管理されたネットワークに参加するには

- 1 管理されたネットワーク上のほかのコンピュータが、ご使用のコンピュータのセキュリティ設定を監視するようにするには、[招待] ダイアログボックスの **「このコンピュータとこのネットワーク上のほかのコンピュータ間で、セキュリティ設定の相互監視を許可」** チェックボックスをオンにします。
- 2 **「参加」** をクリックします。
招待を受け入れると、2 枚のカードが表示されます。
- 3 表示されたカードが、ご使用のコンピュータを管理されたネットワークに招待したコンピュータに表示されているカードと同じであることを確認します。
- 4 **「確認」** をクリックします。

注: ご使用のコンピュータを管理されたネットワークに招待したコンピュータに表示されているカードが、セキュリティを確認するダイアログボックスに表示されているものと異なる場合、管理されたネットワーク上にセキュリティ侵害があったことを示します。ネットワークに参加するとコンピュータが危険にさらされる可能性があるため、セキュリティを確認するダイアログボックスの **「拒否」** をクリックします。

管理されたネットワークにコンピュータを招待

管理されたネットワークにコンピュータが追加された場合、または管理されていない別のコンピュータが存在する場合、そのコンピュータを管理されたネットワークに招待できます。ネットワーク上で管理者権限のあるコンピュータのみがほかのコンピュータをネットワークに招待できます。招待を送信するときに、参加するコンピュータに割り当てる権限レベルを指定することもできます。

管理されたネットワークにコンピュータを招待するには

- 1 ネットワーク地図で管理されていないコンピュータのアイコンをクリックします。
- 2 **「オプションの選択」** の下の **「このコンピュータを監視」** をクリックします。
- 3 **「管理されたネットワークに招待する」** ダイアログボックスで、次のいずれかをクリックします。
 - **ゲストとしてのアクセスを許可**
ゲストのアクセス権により、コンピュータはネットワークにアクセスできるようになります。
 - **管理されたすべてのネットワークアプリケーションに対してアクセスを許可**
すべてのアクセス権（ゲストアクセスと同様）により、コンピュータはネットワークにアクセスできるようになります。

- **管理されたすべてのネットワークアプリケーションに対して管理者としてのアクセスを許可**

管理者のアクセス権により、コンピュータは管理者権限でネットワークにアクセスできるようになります。また、このコンピュータは、管理されたネットワークに参加しようとするほかのコンピュータにアクセスを許可することもできます。

4 **【招待】** をクリックします。

管理されたネットワークへの招待がコンピュータに送信されます。送信先のコンピュータが招待を受け入れると、2 枚のカードが表示されます。

5 表示されたカードが、招待したコンピュータに表示されているカードと同じであることを確認します。

6 **【アクセスを許可】** をクリックします。

注: 管理されたネットワークに招待したコンピュータに表示されているカードが、セキュリティを確認するダイアログボックスに表示されているものと異なる場合、管理されたネットワーク上にセキュリティ侵害があったことを示します。そのコンピュータがネットワークに参加するとほかのコンピュータが危険にさらされる可能性があるため、セキュリティを確認するダイアログボックスの **【アクセスを拒否】** をクリックします。

ネットワーク上のコンピュータの信頼を取り消し

ネットワーク上のほかのコンピュータを信頼することに誤って同意してしまった場合、信頼を取り消すことができます。

ネットワーク上のコンピュータの信頼を取り消すには

- **【オプションの選択】** の下の **【このネットワーク上のコンピュータの信頼を取り消す】** をクリックします。

注: **【このネットワーク上のコンピュータの信頼を取り消す】** リンクは、ほかの管理されたコンピュータがネットワークに参加していないときのみ使用できます。

第 12 章

ネットワークをリモートで管理

管理されたネットワークをセットアップしたあと、McAfee Network Manager を使用して、ネットワークを構成するコンピュータおよびコンポーネントをリモートで管理できます。コンピュータおよびコンポーネントの状態および権限レベルを監視したり、セキュリティ上の脆弱性をリモートで修復できます。

この章の内容

状態の監視と権限.....	64
セキュリティ上の脆弱性を修復.....	67

状態の監視と権限

管理されたネットワークには、2 種類のメンバーがあります。管理されたメンバーと、管理されていないメンバーです。管理されたメンバーは、ネットワーク上のほかのコンピュータに対して、マカフィーによる保護の状態の監視を許可します。一方、管理されていないメンバーはこれを実行できません。通常、管理されていないメンバーは、ほかのネットワーク機能（ファイルまたはプリンタの共有など）にアクセスするゲストコンピュータです。ネットワーク上の管理されている別のコンピュータは、いつでも管理されていないコンピュータに対して、管理されたコンピュータになるように招待できます。同様に、管理されているコンピュータもいつでも管理されていないコンピュータになることができます。

管理されたコンピュータには、管理者、すべて、またはゲスト権限のいずれかが付与されています。管理者権限では、管理されたコンピュータはネットワーク上のほかの管理されたコンピュータすべての保護の状態を管理したり、ほかのコンピュータにネットワークへの参加を許可できます。すべての権限またはゲスト権限では、コンピュータはネットワークへのアクセスのみができます。コンピュータの権限レベルは、いつでも変更できます。

管理されたネットワークには、デバイス（ルータなど）も含まれるため、McAfee Network Manager を使用してこれらのデバイスも管理することができます。また、ネットワーク地図のデバイスの表示プロパティを設定したり変更することもできます。

コンピュータの保護の状態を監視

コンピュータがネットワークのメンバーでないか、コンピュータがネットワークの管理されていないメンバーであるかのいずれかの理由により、コンピュータの保護の状態がネットワークから監視されていない場合、監視するための要求を送信できます。

コンピュータの保護の状態を監視するには

- 1 ネットワーク地図の管理されていないコンピュータのアイコンをクリックします。
- 2 **[オプションの選択]** の下の **[このコンピュータを監視]** をクリックします。

コンピュータの保護の状態の監視を停止

プライベートネットワークの管理されているコンピュータの保護の状態の監視を停止します。すると、そのコンピュータは管理されていないコンピュータとなります。

コンピュータの保護の状態の監視を停止するには

- 1 ネットワーク地図の管理されたコンピュータのアイコンをクリックします。
- 2 **【オプションの選択】** の下の **【このコンピュータの監視を停止】** をクリックします。
- 3 確認のダイアログボックスで、**【はい】** をクリックします。

管理されたコンピュータの権限を変更

管理されたコンピュータの権限は、いつでも変更できます。これにより、ネットワーク上のほかのコンピュータの保護の状態（セキュリティ設定）を監視するコンピュータを調整できます。

管理されたコンピュータの権限を変更するには

- 1 ネットワーク地図の管理されたコンピュータのアイコンをクリックします。
- 2 **【オプションの選択】** の下の **【このコンピュータの権限を変更】** をクリックします。
- 3 権限の変更ダイアログボックスで、チェックボックスをオンまたはオフにし、このコンピュータおよび管理されたネットワーク上のほかのコンピュータが互いの保護の状態を監視するかどうかを決定します。
- 4 **【OK】** をクリックします。

デバイスを管理

McAfee Network Manager から、管理用 Web ページにアクセスしてデバイスを管理することができます。

デバイスを管理するには

- 1 ネットワーク地図のデバイスのアイコンをクリックします。
- 2 **【オプションの選択】** の下の **【このデバイスを管理】** をクリックします。Web ブラウザが開き、デバイスの管理 Web ページが表示されます。
- 3 Web ブラウザで、ログイン情報を入力し、デバイスのセキュリティ設定を設定します。

注: デバイスが McAfee Wireless Network Security で保護されているワイヤレスルータまたはアクセスポイントである場合、McAfee Wireless Network Security を使用してデバイスのセキュリティ設定を設定する必要があります。

デバイスの表示プロパティを変更

デバイスの表示プロパティを変更する場合、ネットワーク地図のデバイスの表示名を変更し、デバイスがワイヤレスルータであるかどうかを指定できます。

デバイスの表示プロパティを変更するには

- 1 ネットワーク地図のデバイスのアイコンをクリックします。
- 2 [オプションの選択] の下の [デバイスのプロパティを変更] をクリックします。
- 3 デバイスの表示名を指定するには、[名前] ボックスに名前を入力します。
- 4 デバイスの種類を指定するには、次のいずれかをクリックします。
 - **ルータ**
標準の家庭用ルータを示します。
 - **ワイヤレスルータ**
家庭用のワイヤレスルータを示します。
- 5 [OK] をクリックします。

セキュリティ上の脆弱性を修復

管理者権限のある管理されたコンピュータは、ネットワーク上の管理されたほかのコンピュータのマカフィーによる保護の状態を監視し、報告されているセキュリティ上の脆弱性をリモートで修復できます。たとえば、管理されたコンピュータのマカフィーによる保護の状態に、McAfee VirusScan が無効になっていることが示されている場合、管理者権限のある別のコンピュータが、リモートで McAfee VirusScan を有効にし、このセキュリティ上の脆弱性をリモートで修復できます。

セキュリティ上の脆弱性をリモートで修復すると、McAfee Network Manager は報告されている問題のほとんどを自動的に修復します。ただし、一部のセキュリティ上の脆弱性については、ローカルコンピュータでの手動操作が必要です。この場合、McAfee Network Manager はリモートで修復できる問題を修復してから、ユーザに対して、脆弱なコンピュータで McAfee SecurityCenter にログインして推奨される対処方法に従って残りの問題を修復するよう要求します。推奨される修復方法として、リモートコンピュータまたはネットワーク上のコンピュータで McAfee 2007 セキュリティソフトウェアをインストールするよう提案される場合もあります。

セキュリティ上の脆弱性を修復

McAfee Network Manager を使用し、管理されたリモートコンピュータのほとんどのセキュリティ上の脆弱性を自動的に修復できます。たとえば、リモートコンピュータで McAfee VirusScan が無効になっている場合、McAfee Network Manager を使用すると自動的に有効にできます。

セキュリティ上の脆弱性を修復するには

- 1 ネットワーク地図で項目のアイコンをクリックします。
- 2 [詳細] で、項目の保護の状態を表示します。
- 3 [オプションの選択] の下の [セキュリティ上の脆弱性を修復] をクリックします。
- 4 セキュリティ上の問題が修復されたら、[OK] をクリックします。

注: McAfee Network Manager はほとんどのセキュリティ上の脆弱性を自動的に修復しますが、問題によっては、ユーザに対して、脆弱なコンピュータで McAfee SecurityCenter を起動して推奨される対処方法に従うよう要求する場合があります。

リモートコンピュータにマカフィー セキュリティ ソフトウェアをインストール

ネットワーク上の 1 台または複数のコンピュータが McAfee 2007 セキュリティソフトウェアを実行していない場合、そのコンピュータのセキュリティの状態はリモートで監視できません。これらのコンピュータをリモートで監視する場合、各コンピュータに直接、McAfee 2007 セキュリティソフトウェアをインストールする必要があります。

リモートコンピュータにマカフィー セキュリティ ソフトウェアをインストールするには

- 1 リモートコンピュータのブラウザで、
<http://download.mcafee.com/jp/> を表示します。
- 2 画面の指示に従い、McAfee 2007 セキュリティソフトウェアをコンピュータにインストールします。

第 13 章

McAfee VirusScan

McAfee VirusScan は、包括的で信頼性の高い、最新のウイルスおよびスパイウェア対策機能を提供します。実績豊かなマカフィーのスキャン技術が駆使された McAfee VirusScan は、ウイルス、ワーム、トロイの木馬、不審なスクリプト、ルートキット、バッファオーバーフロー、複合的な攻撃、スパイウェア、怪しいプログラム (PUP)、その他の脅威を撃退します。

この章の内容

機能	70
ウイルス対策を管理	73
コンピュータを手動スキャン	91
McAfee VirusScan を管理	97
その他の情報	105

機能

このバージョンの McAfee VirusScan には、次の機能が搭載されています。

ウイルス対策

リアルタイムスキャンは、ユーザまたはコンピュータがファイルにアクセスしたときにスキャンを実行します。

スキャン

ハードディスク、フロッピーディスクおよび個々のファイルやフォルダからウイルスやその他の脅威を検出します。項目を右クリックしてスキャンすることもできます。

スパイウェアとアドウェアの検出

McAfee VirusScan は、スパイウェア、アドウェアなど、プライバシーを侵害したりコンピュータのパフォーマンスを低下させるプログラムを検出し、削除します。

自動更新

自動更新により、確認済みの最新の脅威や未確認の脅威からコンピュータを保護します。

高速バックグラウンドスキャン

バックグラウンドで実行される高速スキャン機能により、ウイルス、トロイの木馬、ワーム、スパイウェア、アドウェア、ダイアラーなどの脅威を、作業の妨げになることなく識別し、削除できます。

リアルタイムのセキュリティアラート

緊急のウイルス発生やその他のセキュリティの脅威を通知します。脅威の削除、無効化、または詳細を確認する対策オプションを提供します。

さまざまな侵入経路でウイルスを検出、削除

McAfee VirusScan は、E メール、メッセージャーの添付ファイル、インターネットからのダウンロードファイルなど、コンピュータへの侵入経路となる項目を監視し、ウイルスを削除します。

Eメールの監視によるワームのようなアクティビティの検出

ワームストッパーは、トロイの木馬がほかのコンピュータにワームを E メールで送信するのを遮断し、未知の E メールプログラムがほかのコンピュータに E メールを送信する前にユーザに通知します。

スクリプトの監視によるワームのようなアクティビティの検出

スクリプトストッパーは、危険性のある既知のスクリプトがコンピュータで実行されることを防止します。

McAfee X-ray for Windows

McAfee X-ray for Windows は、Windows では表示されないルートキットなどのプログラムの検出と削除を実行します。

バッファオーバーフロー保護

バッファオーバーフロー保護は、バッファオーバーフローからユーザを保護します。バッファオーバーフローは、不審なプログラムまたはプロセスがコンピュータのバッファ（データの一時的な記憶領域）の制限を越えるデータを保存しようとしたときに発生します。バッファオーバーフローが発生すると、隣接するバッファ内の有効なデータが壊されたり上書きされたりします。

McAfee SystemGuards

McAfee SystemGuards は、ウイルス、スパイウェア、またはハッカーのアクティビティの可能性のある特定の動作があるかどうかを検査します。

第 14 章

ウイルス対策を管理

ウイルス、スパイウェア、McAfee SystemGuards、およびスクリプトのリアルタイムな対策を管理できます。たとえば、スキャンを無効にしたり、スキャン対象を指定したりします。

詳細設定オプションを変更できるのは、管理者権限を持つユーザーのみです。

この章の内容

ウイルス対策を使用	74
スパイウェア対策を使用	77
McAfee SystemGuards を使用	78
スクリプトスキャンを使用	87
E メール保護を使用	88
メッセージ保護を使用	90

ウイルス対策を使用

ウイルス対策（リアルタイムスキャン）が開始されると、コンピュータ内のウイルスのアクティビティが常時監視されます。リアルタイムスキャンは、ユーザまたはコンピュータがファイルにアクセスするたびにスキャンを実行します。感染ファイルを検出すると、ウイルス対策は感染ファイルの駆除または削除を実行しようとします。ファイルの駆除または削除が実行できない場合、別の対応を実行するよう要求するアラートが表示されます。

関連項目

- [セキュリティアラートについて](#)（103 ページ）

ウイルス対策を無効化

ウイルス対策を無効にすると、コンピュータ内のウイルスアクティビティが常時監視されなくなります。ウイルス対策を停止する必要がある場合は、コンピュータをインターネットに接続していないことを確認してください。

注: ウイルス対策を無効にすると、スパイウェア、E メール、およびメッセージングに対するリアルタイムな対策も無効になります。

ウイルス対策を無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【ウイルス対策】** で **【オフ】** をクリックします。
- 4 確認のダイアログボックスで、次のいずれかを実行します。
 - 指定した時間の経過後にウイルス対策を再開する場合は、**【次の時間が経過したらリアルタイムスキャンを再有効化】** チェックボックスをオンにし、メニューから時間を選択します。
 - 指定した時間の経過後にウイルス対策を再開しない場合は、**【次の時間が経過したらリアルタイムスキャンを再有効化】** チェックボックスをオフにします。
- 5 **【OK】** をクリックします。

Windows の起動時にリアルタイム保護が起動するように設定されている場合は、コンピュータを再起動すると、保護が有効になります。

関連項目

- [リアルタイムな対策の設定](#)（75 ページ）

ウイルス対策を有効化

ウイルス対策は、コンピュータ内のウイルスアクティビティを常時監視します。

ウイルス対策を有効にするには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔コンピュータとファイル〕** をクリックします。
- 3 **〔ウイルス対策〕** で **〔オン〕** をクリックします。

リアルタイムな対策の設定

リアルタイムなウイルス対策は変更できます。たとえば、プログラムファイルと文書のみをスキャンしたり、Windows の起動時のリアルタイムスキャンを無効にすることができます（お勧めしません）。

リアルタイムな対策の設定

リアルタイムなウイルス対策は変更できます。たとえば、プログラムファイルと文書のみをスキャンしたり、Windows の起動時のリアルタイムスキャンを無効にすることができます（お勧めしません）。

リアルタイムな対策を設定するには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔コンピュータとファイル〕** をクリックします。
- 3 **〔ウイルス対策〕** で **〔詳細設定〕** をクリックします。
- 4 次のチェックボックスをオンまたはオフにします。
 - **ヒューリスティック方式を使用して未知のウイルスをスキャン:** ファイルと既知のウイルスのシグネチャを照合することで、未確認ウイルスの兆候を検出できます。このオプションでは最も徹底したスキャンが行われ、通常のスキャンよりも時間がかかります。
 - **シャットダウン時にフロッピードライブをスキャン:** コンピュータのシャットダウン時にフロッピードライブをスキャンします。
 - **スパイウェアと怪しいプログラム (PUP) をスキャン:** ユーザの許可なくデータを収集して送信する可能性のあるスパイウェア、アドウェア、その他のプログラムを検出して削除できます。
 - **トラッキング Cookie をスキャンして削除:** ユーザの許可なくデータを収集して送信する可能性のある Cookie を検出して削除できます。Cookie は、Web ページへのアクセス時にユーザを識別します。
 - **ネットワークドライブをスキャン:** ネットワークに接続しているドライブがスキャンされます。

- **バッファオーバーフロー保護を有効化:** バッファ オーバーフロー アクティビティが検出された場合に、アクティビティをブロックしてアラートを表示します。
- **Windows の起動時にリアルタイムスキャンを開始 (推奨):** リアルタイムな対策は、セッション中に無効にした場合でも、コンピュータを起動するたびに有効になります。

5 以下のボタンのうち、いずれかをクリックします。

- **すべてのファイル (推奨):** コンピュータで使用するすべての種類のファイルがスキャンされます。このオプションを使用すると、最も徹底したスキャンが実行されます。
- **プログラムファイルと文書のみ:** プログラムファイルと文書のみがスキャンされます。

6 [OK] をクリックします。

スパイウェア対策を使用

スパイウェア対策は、無断で情報を収集して転送するスパイウェア、アドウェア、およびその他の怪しいプログラム（PUP）を削除します。

スパイウェア対策を無効化

スパイウェア対策を無効にすると、無断で情報を収集して転送するスパイウェア、アドウェア、およびその他の怪しいプログラム（PUP）は検出されません。

スパイウェア対策を無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【スパイウェア対策】** で **【オフ】** をクリックします。

スパイウェア対策を有効化

スパイウェア対策は、無断で情報を収集して転送するスパイウェア、アドウェア、およびその他の怪しいプログラム（PUP）を削除します。

スパイウェア対策を有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【スパイウェア対策】** で **【オン】** をクリックします。

McAfee SystemGuards を使用

McAfee SystemGuards は、コンピュータに対する無認可の可能性のある変更を検出し、変更が行われるとアラートを表示します。アラートが表示されたら、変更を確認して、許可するかどうかを決定できます。

McAfee SystemGuards は次のカテゴリに分類されます。

プログラム用

プログラム用 SystemGuards は、スタートアップファイル、拡張子、および設定ファイルに対する変更を検出します。

Windows 用

Windows 用 SystemGuards は、Windows サービス、証明書、設定ファイルに対する変更を検出します。

ブラウザ用

ブラウザ用 SystemGuards は、Internet Explorer の設定に対する変更（ブラウザの属性やセキュリティ設定を含む）を検出します。

McAfee SystemGuards を無効化

McAfee SystemGuards を無効にすると、コンピュータに対する無認可の可能性のある変更は検出されません。

すべての McAfee SystemGuards を無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【SystemGuard による保護】** で **【オフ】** をクリックします。

McAfee SystemGuards を有効化

McAfee SystemGuards は、コンピュータに対する無認可の可能性のある変更を検出し、変更が行われるとアラートを表示します。

McAfee SystemGuards を有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【SystemGuard による保護】** で **【オン】** をクリックします。

McAfee SystemGuards の設定

McAfee SystemGuards は変更できます。変更が検出されるたびに、アラートを表示してイベントをログに記録するか、イベントログへの記録のみにするか、それぞれの McAfee SystemGuards を無効にするかどうかを決定できます。

McAfee SystemGuards の設定

McAfee SystemGuards は変更できます。変更が検出されるたびに、アラートを表示してイベントをログに記録するか、イベントログへの記録のみにするか、それぞれの McAfee SystemGuards を無効にするかどうかを決定できます。

McAfee SystemGuards を設定するには

- 1 詳細メニューで **[設定]** をクリックします。
- 2 **[設定]** パネルで **[コンピュータとファイル]** をクリックします。
- 3 **[SystemGuard による保護]** で **[詳細設定]** をクリックします。
- 4 **[SystemGuards]** リストで、関連する McAfee SystemGuards とその状態を表示するカテゴリをクリックします。
- 5 McAfee SystemGuards の名称をクリックします。
- 6 **[詳細]** の下にその McAfee SystemGuards に関する情報が表示されます。
- 7 **[オプションの選択]** で、次の対応のいずれかを実行します。
 - 変更の発生時にアラートを表示してイベントログを記録する場合は、**[アラートを表示]** をクリックします。
 - 変更が検出されても何も対応を実行しない場合は、**[ログ記録のみ]** をクリックします。変更はログに記録されるのみです。
 - McAfee SystemGuards をオフにする場合は、**[この SystemGuard を無効化]** をクリックします。変更の発生時にアラートは表示されず、イベントもログに記録されません。
- 8 **[OK]** をクリックします。

McAfee SystemGuards について

McAfee SystemGuards は、コンピュータに対する無認可の可能性のある変更を検出し、変更が行われるとアラートを表示します。アラートが表示されたら、変更を確認して、許可するかどうかを決定できます。

McAfee SystemGuards は次のカテゴリに分類されます。

プログラム用

プログラム用 SystemGuards は、スタートアップファイル、拡張子、および設定ファイルに対する変更を検出します。

Windows 用

Windows 用 SystemGuards は、Windows サービス、証明書、設定ファイルに対する変更を検出します。

ブラウザ用

ブラウザ用 SystemGuards は、Internet Explorer の設定に対する変更（ブラウザの属性やセキュリティ設定を含む）を検出します。

プログラム用 SystemGuards について

プログラム用 SystemGuards は、次の項目を検出します。

ActiveX のインストール

Internet Explorer を介してダウンロードした ActiveX プログラムを検出します。ActiveX プログラムは Web サイトからダウンロードされ、コンピュータの C:\Windows\Downloaded Program Files または C:\Windows\Temp\Temporary Internet Files に保存されます。また、CLSID（中括弧で囲まれた長い数字文字列）によりレジストリで参照されます。

Internet Explorer では通常、正規の ActiveX プログラムが多数使用されます。機能がわからない ActiveX プログラムは削除できます。削除してもコンピュータには影響ありません。あとでこのプログラムが必要になった場合は、このプログラムを必要とする Web サイトを閲覧したときに Internet Explorer によりダウンロードされます。

スタートアップ項目

スタートアップ レジストリ キーおよびフォルダへの変更を監視します。Windows レジストリのスタートアップ レジストリ キーおよび [スタート] メニューのスタートアップフォルダは、コンピュータ上のプログラムのパスを格納します。これら 2 つの場所にリストされているプログラムは、Windows の起動時に読み込まれます。スパイウェアやその他の怪しいプログラム (PUP) により、Windows の起動時にこれらの不正プログラムが読み込まれるように設定される可能性があります。

Windows のシェル実行フック

explorer.exe に読み込まれるプログラムのリストへの変更を監視します。シェル実行フックは、Windows シェルの explorer.exe に読み込まれるプログラムです。シェル実行フックプログラムは、コンピュータで実行されるすべての実行コマンドを受け取ります。explorer.exe シェルに読み込まれたすべてのプログラムは、別のプログラムが実際に起動される前に、追加のタスクを実行できます。スパイウェアや怪しいプログラム (PUP) によりシェル実行フックが使用され、セキュリティ対策プログラムの実行が阻止される可能性があります。

ShellServiceObjectDelayLoad

ShellServiceObjectDelayLoad にリストされたファイルに対する変更を監視します。これらのファイルは、コンピュータの起動時に explorer.exe によって読み込まれます。explorer.exe はコンピュータのシェルであるため、常に起動し、このキーに含まれるファイルを読み込みます。これらのファイルは、ユーザが操作を行う前の、起動プロセスの初期段階で読み込まれます。

Windows 用 SystemGuards について

Windows 用 SystemGuards は、次の項目を検出します。

コンテキスト メニュー ハンドラ

Windows のコンテキストメニューに無認可の変更が行われることを防止します。これらのメニューを使用すると、ファイルを右クリックして、そのファイルに関連する特定の操作を実行できます。

AppInit DLLs

Windows AppInit.DLLs に対する無認可の変更または追加を防止します。AppInit_DLLs レジストリ値には、user32.dll の読み込み時に読み込まれるファイルのリストが含まれています。AppInit_DLLs 値に含まれるファイルは Windows の起動ルーチンの初期段階で読み込まれます。このため、危険性のある .DLL の存在がユーザに認識されない可能性があります。

Windows Hosts ファイル

コンピュータの Hosts ファイルに対する変更を監視します。Hosts ファイルは、ドメイン名を特定の IP アドレスにリダイレクトするときに使用されます。たとえば、www.example.com を閲覧する場合、ブラウザは Hosts ファイルで example.com のエントリを確認し、このドメインの IP アドレスを指定します。一部のスパイウェアプログラムにより、Hosts ファイルが変更され、ブラウザが別のサイトにリダイレクトされたり、ソフトウェアの更新が適切に行われなくなることがあります。

Winlogon シェル

Winlogon シェルを監視します。Winlogon シェルは、Windows へのログオン時に読み込まれます。このシェルは Windows の管理に使用される主なユーザインターフェース (UI) で、通常は Windows Explorer (explorer.exe) となります。ただし、Windows シェルのかわりに別のプログラムを指定することは簡単にできます。変更されると、ユーザがログオンするたびに Windows シェル以外のプログラムが起動される可能性があります。

WinlogonUserInit

Windows のログオンユーザの設定への変更を監視します。
HKLM¥Software¥Microsoft WindowsNT¥CurrentVersion¥Winlogon
¥Userinit というキーは、Windows へのユーザログオン後に起動される
プログラムを指定します。標準設定プログラムでは、ユーザ名について
のプロフィール、フォント、色などの設定が復元されます。スパイウェア
や怪しいプログラム（PUP）が、自分自身をこのキーに追加することによ
り、起動を試行する可能性があります。

Windows プロトコル

ネットワークプロトコルへの変更を監視します。スパイウェアや怪しいプ
ログラム（PUP）により、コンピュータで情報の送受信に使用される特
定の方法が制御される可能性があります。これは、Windows プロトコル
のフィルタとハンドラを使用して実行されます。

WinSock LSP (Layered Service Provider)

ネットワーク上のデータを傍受して変更またはリダイレクトする可能性
のある、LSP (Layered Service Provider) を監視します。正当な LSP
には、パレンタル コントロール ソフトウェア、ファイアウォールなどのセ
キュリティプログラムが含まれています。スパイウェアは、LSP を使用し
てユーザのインターネットアクティビティを監視し、データを変更する可
能性があります。オペレーティングシステムの再インストールが必要な
事態にならないために、マカフィープログラムを使用してスパイウェアお
よび信頼できない LSP を自動的に削除します。

Windows シェルの Open コマンド

Windows シェル（explore.exe）の Open コマンドへの変更を防止しま
す。シェルの Open コマンドを使用すると、特定の種類のファイルが実
行されるたびに特定のプログラムを実行できます。たとえば、.exe アプ
リケーションが実行されるたびにワームが実行される可能性があります。

SharedTaskScheduler

Windows の起動時に実行されるプログラムのリストが含まれている、
SharedTaskScheduler レジストリキーを監視します。スパイウェアや怪
しいプログラム（PUP）により、このキーが変更され、これらの不正プロ
グラムがユーザの許可なくリストに追加される可能性があります。

Windows Messenger サービス

Windows Messenger サービスは、ポップアップメッセージの送信を可能にする Windows Messenger 機能です。スパイウェアや怪しいプログラム (PUP) によりこのサービスが有効にされ、未承諾広告を受信する可能性があります。また、このサービスは、リモートでプログラムを起動する既知の脆弱性を使用して、攻撃される可能性があります。

Windows win.ini ファイル

win.ini ファイルは、Windows の起動時に実行するプログラムのリストを含むテキストベースのファイルです。これらのプログラムを読み込む構文は、Windows で動作する古いバージョンのプログラムをサポートするために使用されるファイルに存在します。最近では、ほとんどのプログラムは、読み込みに win.ini ファイルを使用しません。ただし、一部のスパイウェアや怪しいプログラム (PUP) では、この構文を利用して Windows の起動時にこれらの不正なプログラムを読み込ませるように設計されているものがあります。

ブラウザ用 SystemGuards について

ブラウザ用 SystemGuards は、次の項目を検出します。

ブラウザ ヘルパー オブジェクト

ブラウザ ヘルパー オブジェクト (BHO) への追加を監視します。BHO は Internet Explorer のプラグインとして動作するプログラムです。スパイウェアやブラウザハイジャックにより BHO が使用され、広告が表示されたり閲覧履歴が追跡される可能性があります。また、BHO は、一般的な検索ツールバーなど、多くの正規プログラムでも使用されます。

Internet Explorer バー

Internet Explorer バーに表示されるプログラムに対する変更を監視します。エクスプローラバーとは、Internet Explorer (IE) または Windows Explorer に表示される [検索]、[お気に入り]、[履歴] などのフレームの様な表示画面のことです。

Internet Explorer プラグイン

スパイウェアが Internet Explorer プラグインをインストールすることを防止します。Internet Explorer プラグインは、Internet Explorer の起動時に読み込まれる機能追加ソフトウェアです。スパイウェアにより Internet Explorer プラグインが使用され、広告が表示されたり閲覧履歴が追跡される可能性があります。正規のプラグインは Internet Explorer に機能を追加します。

Internet Explorer ShellBrowser

Internet Explorer ShellBrowser インスタンスへの変更を監視します。Internet Explorer の ShellBrowser には、Internet Explorer のインスタンスに関する情報と設定が含まれています。これらの設定が変更されたり新しい ShellBrowser が追加されると、この ShellBrowser により、Internet Explorer が完全に制御され、ツールバー、メニュー、ボタンなどの機能が追加される可能性があります。

Internet Explorer WebBrowser

Internet Explorer WebBrowser インスタンスへの変更を監視します。Internet Explorer の WebBrowser には、Internet Explorer のインスタンスに関する情報と設定が含まれています。これらの設定が変更されたり新しい WebBrowser が追加されると、この WebBrowser により、Internet Explorer が完全に制御され、ツールバー、メニュー、ボタンなどの機能が追加される可能性があります。

Internet Explorer URL 検索フック

Internet Explorer の URL 検索フックへの変更を監視します。URL 検索フックは、ブラウザのアドレスフィールドに、http:// や ftp:// などのプロトコルを入力せずにアドレスを入力した場合に使用されます。このようなアドレスが入力されると、ブラウザは URL 検索フックを使用して、入力された場所をインターネットで検索する可能性があります。

Internet Explorer URL

Internet Explorer で事前に設定されている URL の変更を監視します。これにより、スパイウェアや怪しいプログラム (PUP) によりユーザの許可なくブラウザ設定が変更されることを防止できます。

Internet Explorer 制限

Internet Explorer の制限を監視します。これにより、コンピュータの管理者は、ユーザにより Internet Explorer のホームページやその他のオプションが変更されることを防止できます。これらのオプションは、管理者が意図的に設定する場合のみに表示されるようになります。

Internet Explorer セキュリティゾーン

Internet Explorer のセキュリティゾーンを監視します。Internet Explorer では、4 つのセキュリティゾーン（インターネット、イントラネット、信頼済みサイト、制限付きサイト）が事前に定義されています。それぞれのセキュリティゾーンに対して、事前に定義されている設定をカスタマイズした設定を使用できます。セキュリティゾーンは、スパイウェアや怪しいプログラム（PUP）のターゲットとなります。セキュリティレベルを下げると、これらのプログラムがセキュリティアラートを回避し、検出されない可能性があります。

Internet Explorer 信頼済みサイト

Internet Explorer の信頼済みサイトを監視します。信頼済みサイトリストは、信頼している Web サイトの住所録です。一部のスパイウェアや怪しいプログラム（PUP）によりこのリストが書き換えられ、不審なサイトが信頼済みサイトとしてユーザの許可なく追加される可能性があります。

Internet Explorer のポリシー

Internet Explorer のポリシーを監視します。これらの設定は通常、システム管理者により変更されますが、スパイウェアにより変更される可能性があります。変更されると、別のホームページを設定できなくなったり、[ツール] メニューの [インターネットオプション] ダイアログボックスにタブが表示されなくなります。

スクリプトスキャンを使用

スクリプトにより、ファイルの作成、コピー、または削除が実行されることがあります。Windows のレジストリが開かれる場合もあります。

スクリプトスキャンは、危険性のある既知のスクリプトがほかのコンピュータで実行されることを自動的に防止します。

スクリプトスキャンを無効化

スクリプトスキャンを無効にすると、不審なスクリプトの実行は検出されません。

スクリプトスキャンを無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【スクリプトスキャンによる保護】** で **【オフ】** をクリックします。

スクリプトスキャンを有効化

ファイルを作成、コピー、削除したり、Windows レジストリを開いたりするスクリプトを実行した場合は、スクリプトスキャンによりアラートが表示されます。

スクリプトスキャンを有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【スクリプトスキャンによる保護】** で **【オン】** をクリックします。

E メール保護を使用

E メール保護は、受信（POP3）および送信（SMTP）する E メールメッセージと添付ファイルに含まれる、脅威を検出してブロックします。ウイルス、トロイの木馬、ワーム、スパイウェアなどの脅威を検出します。

E メール保護を無効化

E メール保護を無効にすると、受信（POP3）および送信（SMTP）する E メールメッセージと添付ファイルに含まれる、潜在的な脅威は検出されません。

E メール保護を無効にするには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔E メールとメッセージャー〕** をクリックします。
- 3 **〔E メール保護〕** で **〔オフ〕** をクリックします。

E メール保護を有効化

E メール保護は、受信（POP3）および送信（SMTP）する E メールメッセージと添付ファイルに含まれる脅威を検出します。

E メール保護を有効にするには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔E メールとメッセージャー〕** をクリックします。
- 3 **〔E メール保護〕** で **〔オン〕** をクリックします。

E メール保護の設定

E メール保護オプションを使用すると、受信および送信する E メールメッセージとワームをスキャンできます。ワームは自らの複製を作成してシステムリソースを消費します。それが原因で、パフォーマンスが低下したり、タスクが中断されたりします。ワームは、E メールメッセージを使用して自身のコピーを送信します。たとえば、アドレス帳に保存されているアドレスに E メールメッセージを転送しようとしています。

E メール保護の設定

E メール保護オプションを使用すると、受信および送信する E メールメッセージとワームをスキャンできます。

E メール保護を設定するには

- 1 詳細メニューで **[設定]** をクリックします。
- 2 **[設定]** パネルで **[E メールとメッセージ]** をクリックします。
- 3 **[E メール保護]** で **[詳細設定]** をクリックします。
- 4 次のチェックボックスをオンまたはオフにします。
 - **Eメールの受信メッセージをスキャン:** 受信 (POP3) メッセージに含まれる、潜在的な脅威が検出されます。
 - **Eメールの送信メッセージをスキャン:** 送信 (SMTP) メッセージに含まれる、潜在的な脅威が検出されます。
 - **ワームストッパーを有効化:** ワームストッパーは、E メールメッセージに含まれるワームをブロックします。
- 5 **[OK]** をクリックします。

メッセージ保護を使用

メッセージ保護は、受信メッセージの添付ファイルに含まれる脅威を検出します。

メッセージ保護を無効化

メッセージ保護を無効にすると、受信メッセージの添付ファイルに含まれる脅威は検出されません。

メッセージ保護を無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージ】** をクリックします。
- 3 **【メッセージの保護】** で **【オフ】** をクリックします。

メッセージ保護を有効化

メッセージ保護は、メッセージで受信したメッセージの添付ファイルに含まれる脅威を検出します。

メッセージ保護を有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージ】** をクリックします。
- 3 **【メッセージの保護】** で **【オン】** をクリックします。

第 15 章

コンピュータを手動スキャン

ハード ディスク ドライブ、フロッピーディスクおよび個々のファイルやフォルダからウイルスやその他の脅威を検出します。不審なファイルが検出されると、そのファイルからウイルスが駆除されます（怪しいプログラム（PUP）ではない場合）。ウイルスを駆除できない場合は、そのファイルを隔離または削除できます。

この章の内容

手動スキャン 92

手動スキャン

手動スキャンは、いつでも実行できます。たとえば McAfee VirusScan をインストールしている場合、スキャンを実行してコンピュータにウイルスまたはほかの脅威が含まれていないことを確認できます。または、リアルタイムスキャンが無効の場合、スキャンを実行してコンピュータが安全であることを確認できます。

手動スキャン設定を使用してスキャン

この種類のスキャンでは、指定した手動スキャン設定が使用されます。McAfee VirusScan では、圧縮ファイル（zip、cab など）の内部をスキャンします。ただし、圧縮ファイルは 1 つのファイルとして数えます。また、前回のスキャン以降にインターネットの一時ファイルを削除した場合は、スキャンしたファイル数が変わる場合があります。

手動スキャン設定を使用してスキャンを実行するには

- 1 標準メニューで **【スキャン】** をクリックします。スキャンが完了すると、スキャンおよび検出されたファイル数、駆除した項目数、および最後のスキャン日時が概要に表示されます。
- 2 **【完了】** をクリックします。

関連項目

- **手動スキャンの設定** (94 ページ)

手動スキャン設定を使用しないスキャン

この種類のスキャンでは、指定した手動スキャン設定は使用されません。McAfee VirusScan では、圧縮ファイル（zip、cab など）の内部をスキャンします。ただし、圧縮ファイルは 1 つのファイルとして数えます。また、前回のスキャン以降にインターネットの一時ファイルを削除した場合は、スキャンしたファイル数が変わる場合があります。

手動スキャン設定を使用しないでスキャンを実行するには

- 1 詳細メニューで **【ホーム】** をクリックします。
- 2 **【ホーム】** パネルで **【スキャン】** をクリックします。
- 3 **【スキャンする場所】** で、スキャンを実行するファイル、フォルダ、およびドライブの横にあるチェックボックスをオンにします。
- 4 **【オプション】** で、スキャンを実行するファイルの横にあるチェックボックスをオンにします。

- 5 **【今すぐスキャン】** をクリックします。スキャンが完了すると、スキャンおよび検出されたファイル数、駆除した項目数、および最後のスキャン日時が概要に表示されます。
- 6 **【完了】** をクリックします。

注: これらのオプションは保存されません。

Windows Explorer をスキャン

Windows Explorer 内から、選択したファイル、フォルダ、またはドライブをスキャンしてウイルスなどの脅威を検出できます。

Windows Explorer でファイルをスキャンするには

- 1 Windows Explorer を開きます。
- 2 スキャンするファイル、フォルダ、ドライブを右クリックし、次に **【スキャン】** をクリックします。徹底したスキャンが実行されるように、すべての標準設定スキャンオプションが選択されています。

手動スキャンの設定

手動スキャンまたはスケジュールスキャンの実行時には、スキャンを実行するファイルの種類、スキャンを実行する場所、およびスキャンの実行日時を指定できます。

スキャンするファイルの種類を指定

スキャンするファイルの種類を指定できます。

スキャンするファイルの種類を指定するには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔コンピュータとファイル〕** をクリックします。
- 3 **〔ウイルス対策〕** で **〔詳細設定〕** をクリックします。
- 4 **〔ウイルス対策〕** パネルで **〔手動スキャン〕** をクリックします。
- 5 次のチェックボックスをオンまたはオフにします。
 - **ヒューリスティック方式を使用して未知のウイルスをスキャン:** ファイルと既知のウイルスのシグネチャを照合することで、未確認ウイルスの兆候を検出できます。このオプションでは最も徹底したスキャンが行われ、通常のスキャンよりも時間がかかります。
 - **.zip とその他のアーカイブファイルをスキャン:** Zip ファイルなどのアーカイブファイルに含まれるウイルスの検出と削除を実行します。ウイルス作成者はウイルスを Zip ファイルに埋め込み、ウイルス対策スキャンの目をすり抜けるために、その Zip ファイルをさらに別の Zip ファイルに入れる場合があります。
 - **スパイウェアと怪しいプログラム (PUP) をスキャン:** ユーザの許可なくデータを収集して送信する可能性のあるスパイウェア、アドウェア、その他のプログラムを検出して削除できます。
 - **トラッキング Cookie をスキャンして削除:** ユーザの許可なくデータを収集して送信する可能性のある Cookie を検出して削除できます。Cookie は、Web ページへのアクセス時にユーザを識別します。
 - **ルートキットとその他のステルスプログラムをスキャン:** Windows に表示されないルートキットなどのプログラムの検出と削除を実行します。
- 6 以下のボタンのうち、いずれかをクリックします。
 - **すべてのファイル (推奨):** コンピュータで使用されるすべての種類のファイルがスキャンされます。このオプションを使用すると、最も徹底したスキャンが実行されます。
 - **プログラムファイルと文書のみ:** プログラムファイルと文書のみがスキャンされます。
- 7 **〔OK〕** をクリックします。

スキャンする場所を指定

手動スキャンまたはスケジュールスキャンでスキャンを実行する場所を指定できます。

スキャンする場所を指定するには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔コンピュータとファイル〕** をクリックします。
- 3 **〔ウイルス対策〕** で **〔詳細設定〕** をクリックします。
- 4 **〔ウイルス対策〕** パネルで **〔手動スキャン〕** をクリックします。
- 5 **〔標準設定のスキャン場所〕** で、スキャンを実行するファイル、フォルダ、およびドライブを選択します。

最も徹底したスキャンを実行する場合は、**〔重要なファイル〕** が選択されていることを確認します。
- 6 **〔OK〕** をクリックします。

スキャンをスケジュール

スキャンをスケジュールすると、特定の間隔でコンピュータのウイルスやほかの脅威を徹底的にチェックできます。

スキャンをスケジュールするには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔コンピュータとファイル〕** をクリックします。
- 3 **〔ウイルス対策〕** で **〔詳細設定〕** をクリックします。
- 4 **〔ウイルス対策〕** パネルで **〔スケジュールスキャン〕** をクリックします。
- 5 **〔スケジュールスキャンを有効化〕** が選択されていることを確認します。
- 6 スキャンを実行する曜日の横にあるチェックボックスをオンにします。
- 7 **〔開始時刻〕** リストの値をクリックして、開始時刻を指定します。
- 8 **〔OK〕** をクリックします。

ヒント: 標準設定のスケジュールを使用する場合は、**〔リセット〕** をクリックします。

第 16 章

McAfee VirusScan を管理

信頼リストから項目を削除したり、隔離したプログラム、Cookie、およびファイルを管理したり、イベントとログを表示したり、不審なアクティビティをマカフィーに報告できます。

この章の内容

信頼リストを管理	98
隔離したプログラム、Cookie、およびファイルを管理	99
最近のイベントとログを表示	101
匿名情報を自動報告	102
セキュリティアラートについて	103

信頼リストを管理

McAfee SystemGuards、プログラム、バッファオーバーフロー、または E メールプログラムを信頼すると、その項目が信頼リストに追加され、検出されなくなります。

誤ってプログラムを信頼したり、検出対象とするプログラムがある場合には、それらを信頼リストから削除する必要があります。

信頼リストを管理

McAfee SystemGuards、プログラム、バッファオーバーフロー、または E メールプログラムを信頼すると、その項目が信頼リストに追加され、検出されなくなります。

誤ってプログラムを信頼したり、検出対象とするプログラムがある場合には、それらを信頼リストから削除する必要があります。

信頼リストから項目を削除するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【コンピュータとファイル】** をクリックします。
- 3 **【ウイルス対策】** で **【詳細設定】** をクリックします。
- 4 **【ウイルス対策】** パネルで **【信頼リスト】** をクリックします。
- 5 リストから、信頼された McAfee SystemGuards、プログラム、バッファオーバーフロー、または E メールプログラムを選択し、その項目と信頼状態を表示します。
- 6 **【詳細】** で、その項目についての情報を表示します。
- 7 **【オプションの選択】** で対応をクリックします。
- 8 **【OK】** をクリックします。

隔離したプログラム、Cookie、およびファイルを管理

隔離したプログラム、Cookie、およびファイルは、復元または削除したり、分析のためにマカフィーへ送信できます。

隔離したプログラム、Cookie、およびファイルを復元

必要に応じて、隔離したプログラム、Cookie、およびファイルを復元できます。

隔離したプログラム、Cookie、およびファイルを復元するには

- 1 詳細メニューで **【復元】** をクリックします。
- 2 **【復元】** パネルで、必要に応じて **【プログラムと Cookie】** または **【ファイル】** をクリックします。
- 3 復元する、隔離したプログラム、Cookie、およびファイルを選択します。
- 4 隔離したウイルスの詳細については、**【詳細】** の検出名をクリックしてください。ウイルス情報ライブラリにウイルスの説明が表示されます。
- 5 **【オプションの選択】** で **【復元】** をクリックします。

隔離したプログラム、Cookie、およびファイルを削除

隔離したプログラム、Cookie、およびファイルを削除できます。

隔離したプログラム、Cookie、およびファイルを削除するには

- 1 詳細メニューで **【復元】** をクリックします。
- 2 **【復元】** パネルで、必要に応じて **【プログラムと Cookie】** または **【ファイル】** をクリックします。
- 3 復元する、隔離したプログラム、Cookie、およびファイルを選択します。
- 4 隔離したウイルスの詳細については、**【詳細】** の検出名をクリックしてください。ウイルス情報ライブラリにウイルスの説明が表示されます。
- 5 **【オプションの選択】** で **【削除】** をクリックします。

隔離したプログラム、Cookie、およびファイルをマカフィーに送信

隔離したプログラム、Cookie、およびファイルは、分析のためにマカフィーに送信できます。

注: 送信する隔離したファイルが最大サイズを超過している場合、ファイルが拒否されることがあります。ただし、ほとんどの場合、ファイルの拒否は発生しません。

隔離したプログラムまたはファイルをマカフィーに送信するには

- 1 詳細メニューで **【復元】** をクリックします。
- 2 **【復元】** パネルで、必要に応じて **【プログラムと Cookie】** または **【ファイル】** をクリックします。
- 3 マカフィーに送信する、隔離したプログラム、Cookie、またはファイルを選択します。
- 4 隔離したウイルスの詳細については、**【詳細】** の検出名をクリックしてください。ウイルス情報ライブラリにウイルスの説明が表示されます。
- 5 **【オプションの選択】** で **【マカフィーに送信】** をクリックします。

最近のイベントとログを表示

最近のイベントとログには、インストールされているすべてのマカフィー製品についてのイベントが表示されます。

[最近のイベント] では、コンピュータ上で発生した最新 30 件の重要なイベントを表示できます。ブロックされたプログラムを復元したり、リアルタイムスキャンを再有効化したり、バッファオーバーフローを信頼できます。

過去 30 日間に発生したすべてのイベントが記録されたログを表示することもできます。

イベントを表示

[最近のイベント] では、コンピュータ上で発生した最新 30 件の重要なイベントを表示できます。ブロックされたプログラムを復元したり、リアルタイムスキャンを再有効化したり、バッファオーバーフローを信頼できます。

イベントを表示するには

- 1 詳細メニューで **[レポートとログ]** をクリックします。
- 2 **[レポートとログ]** パネルで **[最近のイベント]** をクリックします。
- 3 表示するイベントを選択します。
- 4 **[詳細]** で、そのイベントについての情報を表示します。
- 5 **[オプションの選択]** で対応をクリックします。

ログを表示

ログには、過去 30 日間に発生したすべてのイベントが記録されています。

ログを表示するには

- 1 詳細メニューで **[レポートとログ]** をクリックします。
- 2 **[レポートとログ]** パネルで **[最近のイベント]** をクリックします。
- 3 **[最近のイベント]** パネルで **[ログを表示]** をクリックします。
- 4 表示するログの種類を選択してから、ログを選択します。
- 5 **[詳細]** で、そのログについての情報を表示します。

匿名情報を自動報告

ウイルス、怪しいプログラム (PUP)、ハッカー追跡情報を匿名でマカフィーに送信します。このオプションは、インストール時のみ選択できます。

個人情報収集されません。

マカフィーに報告

ウイルス、怪しいプログラム (PUP)、ハッカー追跡情報をマカフィーに送信します。このオプションは、インストール時のみ選択できます。

匿名情報を自動で報告するには

- 1 McAfee VirusScan のインストール時に、標準設定の **匿名情報の送信** をそのまま選択します。
- 2 **次へ** をクリックします。

セキュリティアラートについて

リアルタイムスキャンにより脅威が検出されると、アラートが表示されます。ほとんどのウイルス、トロイの木馬、スクリプト、およびワームについては、リアルタイムスキャンはこれらをファイルから自動的に駆除し、アラートを表示します。怪しいプログラム (PUP) および McAfee SystemGuards については、リアルタイムスキャンはファイルまたは変更を検出すると、アラートを表示します。バッファオーバーフロー、トラッキング Cookie、およびスクリプトアクティビティについては、リアルタイムスキャンは自動的にアクティビティをブロックし、アラートを表示します。

これらのアラートは、3 つの基本的な種類に分類できます。

- レッドアラート
- イエローアラート
- グリーンアラート

その後で、検出したファイル、検出した E メール、不審なスクリプト、潜在的なワーム、および怪しいプログラム (PUP)、McAfee SystemGuards、バッファオーバーフローの対処法を選択できます。

アラートを管理

マカフィー製品では、さまざまなアラートを利用して、セキュリティの管理を実現しています。これらのアラートは、3 つの基本的な種類に分類できます。

- レッドアラート
- イエローアラート
- グリーンアラート

レッドアラート

レッドアラートには、ユーザの対応が必要です。特定のアクティビティに対する自動応答の方法をマカフィー製品で決定できない場合があります。このような場合、レッドアラートに問題のアクティビティが説明され、選択肢が提供されます。

イエローアラート

イエローアラートは、通常ユーザの対応が必要となるものの、あまり重要ではない通知です。イエローアラートには問題のアクティビティが説明され、選択肢が提供されます。

グリーンアラート

グリーンアラートでは、ほとんどの場合イベントについての基本情報が説明されるのみで、ユーザの対応は不要です。

アラートのオプションの設定

特定のアラートで、今後表示しないと選択したあと、再び表示されるように戻したくなった場合は、変更することができます。アラートのオプションの設定の詳細については、McAfee SecurityCenter のマニュアルを参照してください。

第 17 章

その他の情報

この章では、よくある質問とトラブルシューティング（問題解決）の方法について説明します。

この章の内容

よくある質問	106
トラブルシューティング	108

よくある質問

ここでは、よくある質問とその回答を紹介します。

脅威が検出されました。どうしたらよいですか？

マカフィー製品では、アラートを使用してセキュリティを管理します。これらのアラートは、3 つの基本的な種類に分類できます。

- レッドアラート
- イエローアラート
- グリーンアラート

検出したファイル、検出した E メール、不審なスクリプト、潜在的なワーム、および怪しいプログラム (PUP)、McAfee SystemGuards、パッファオーバーフローの対処法を選択できます。

特定の脅威の詳細については、次のウイルス情報ライブラリを参照してください。<http://jp.mcafee.com/virusInfo/default.asp?affid=>

関連項目

- セキュリティアラートについて (103 ページ)

Netscape、Firefox、または Opera ブラウザで McAfee VirusScan を使用できますか？

Netscape、Firefox、または Opera を標準のブラウザに設定していても、McAfee VirusScan は実行できます。ただし、コンピュータに Microsoft Internet Explorer 6.0 以降がインストールされている必要があります。

スキャンを実行する際は、インターネットに接続する必要がありますか？

スキャンを実行する際は、インターネットに接続する必要はありませんが、最新の更新を入手するために、少なくとも 1 週間に一度インターネットに接続してください。

McAfee VirusScan は E メール の 添付ファイル を スキャン します か？

リアルタイムスキャンおよび E メール保護を有効にしている場合、E メールメッセージを受信すると添付ファイルがスキャンされます。

McAfee VirusScan は Zip で圧縮されたファイル を スキャン します か？

McAfee VirusScan は Zip で圧縮されたファイルおよびほかのアーカイブファイルをスキャンします。

送信メールのスキャンでエラーが発生するのはなぜですか？

送信 E メールメッセージのスキャン中に、次のエラーが発生する場合があります。

- プロトコルエラー。E メールサーバによって E メールメッセージが拒否されました。
プロトコルエラーまたはシステムエラーが発生した場合は、そのセッション内の残りの E メールメッセージの処理は続行し、サーバへ送られます。
- 接続エラー。E メールサーバへの接続が切断されました。
接続エラーが発生した場合は、コンピュータがインターネットに接続されているか確認し、E メールプログラムの**送信メール**リストからもう一度メッセージを送信してください。
- システムエラー。ファイルの処理エラーまたはシステムエラーが発生しました。
- 暗号化された SMTP 接続エラー。使用中の E メールプログラムから暗号化された SMTP 接続が検出されました。
暗号化された SMTP 接続が行われた場合は、E メールメッセージが確実にスキャンされるように E メールプログラムで暗号化された SMTP 接続を無効にしてください。

E メールメッセージの送信中にタイムアウトが発生した場合は、送信 E メールスキャンを無効にするか、E メールプログラムの暗号化された SMTP 接続を無効にしてください。

関連項目

- E メール保護の設定 (89 ページ)

トラブルシューティング

ここでは、発生する可能性のある一般的な問題について説明します。

ウイルスを駆除/削除できません

ウイルスの種類によっては、手動でウイルスを駆除しなければならない場合があります。コンピュータを再起動して、スキャンを再度実行してください。

コンピュータがウイルスを駆除または削除できない場合は、ウイルスを手動で削除する方法について、次のウイルス情報ライブラリを参照してください。<http://jp.mcafee.com/virusInfo/default.asp?affid=>

詳細については、マカフィーの Web サイトからカスタマサポートにお問い合わせください。

注: CD-ROM、DVD、および書き込み禁止になっているフロッピーディスクからはウイルスを駆除できません。

再起動しても、項目を削除できません

項目をスキャンして削除したあと、コンピュータの再起動が必要となる場合があります。

コンピュータの再起動後も項目を削除できない場合は、マカフィーにファイルを送信してください。

注: CD-ROM、DVD、および書き込み禁止になっているフロッピーディスクからはウイルスを駆除できません。

関連項目

- 隔離したプログラム、Cookie、およびファイルを管理 (99 ページ)

コンポーネントが見つからないかまたは壊れています

次のような場合には、McAfee VirusScan を正常にインストールできないことがあります。

- コンピュータに十分なディスク容量またはメモリがない場合。コンピュータがこのソフトウェアを実行するためのシステム要件に適合しているかどうかを確認してください。
- インターネットブラウザが正しく設定されていない場合。
- インターネット接続が間違っている場合。接続を確認してください。またはしばらくしてから再度接続してください。
- ファイルが不足しているか、インストールが失敗している場合。

上記の潜在的な問題を解決してから、McAfee VirusScan を再インストールしてください。

第 18 章

McAfee Personal Firewall

McAfee Personal Firewall は、コンピュータと個人データを保護する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バリア（ファイアウォール）を作り、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。

この章の内容

機能	112
ファイアウォールを起動	115
アラートを使用	117
情報アラートを管理	121
ファイアウォールによる保護の設定	123
プログラムと権限を管理	135
システムサービスを管理	147
コンピュータ接続を管理	151
ログ記録、監視、分析	161
インターネットセキュリティについての確認	173

機能

McAfee Personal Firewall は、内向き（受信）、外向き（送信）にかかわらず、すべてのトラフィックに対して万全のファイアウォールを提供します。また、既知の安全なプログラムは自動的に信用し、スパイウェア、トロイの木馬、キーロガーはブロックします。ファイアウォールを使用すると、ハッカーによる攻撃の阻止、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、悪意のあるイベントや不審なイベントに対する警告、インターネットトラフィックに関する詳細情報の確認など、ウイルス対策による保護を補うことができます。

標準的な保護レベルとカスタマイズ

ファイアウォールの標準保護設定で、侵入や不審なアクティビティから保護できます。また、必要に応じて設定をカスタマイズすることも可能です。

推奨事項のリアルタイム表示

状況に応じて表示される推奨事項を参考に、あるプログラムにインターネットアクセスを許可するかどうか、あるネットワークトラフィックを信用するかどうかを決定できます。

プログラムに対するすぐれたアクセス管理

アラートやイベントログを使用してそれぞれのプログラムのインターネットアクセスを管理できます。また、[プログラム許可機能] パネルで特定のプログラムに対してアクセス許可を設定することもできます。

ゲームのプレイ中の保護

全画面表示でゲームをプレイしている間は、侵入や不審なアクティビティに関するアラートに邪魔されないようにするため、ゲームが終了するまでアラートを表示しないようにファイアウォールを設定できます。

コンピュータの起動時の保護

Windows の起動が完了する前でも、侵入および怪しいプログラムやネットワークトラフィックからコンピュータを保護します。

システム サービス ポートの制御

システム サービス ポートにより、バックドアがコンピュータに仕掛けられる可能性があります。ファイアウォールを使用すると、特定のプログラムによって必要とされるシステム サービス ポートを作成したり、これらのポートの開閉を管理できます。

コンピュータ接続の管理

コンピュータにアクセスする可能性のあるリモート接続や IP アドレスを信用したり禁止できます。

HackerWatch 情報の統合

HackerWatch は、セキュリティ情報の収集元として機能しています。世界中のハッカー行為や侵入パターンを追跡するだけでなく、使用しているコンピュータ上のプログラムに関する最新情報を提供します。世界中のセキュリティイベントとインターネット上のポートに関する統計を確認できます。

ファイアウォールのロック

ロックすると、すべての内向き、外向きのインターネットトラフィックが無条件でブロックされます。

ファイアウォールの復元

ファイアウォールによる保護を簡単に標準設定に戻すことができます。McAfee Personal Firewall が思い通りに設定できない場合は、ファイアウォールを標準設定に戻すことができます。

トロイの木馬の高度な検出

プログラム接続管理機能と高度なデータベース機能が統合され、疑わ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を侵害することを防ぎます。

イベントログの記録

ログ記録を有効にするか無効にするかを指定できます。有効にした場合は、ログに記録するイベントタイプを指定できます。イベントログの記録では、最近の受信イベントおよび送信イベントを表示できます。侵入検知イベントを表示することもできます。

インターネットトラフィックの監視

グラフィカルで見やすい地図を表示して、悪質な攻撃やトラフィックの発信元を確認できます。また、発信元 IP アドレスの所有者の詳細情報と地理的な情報も確認できます。さらに、内向きおよび外向きのトラフィックを分析したり、プログラムが使用する帯域幅やアクティビティを監視できます。

侵入防止機能

侵入防止機能により、インターネット上の脅威から個人情報を保護できます。ヒューリスティック同様の機能を使い、攻撃の兆候や、ハッキング行為の特徴をブロックする、第三の保護レイヤーを提供します。

高度なトラフィック分析

内向き、外向きすべてのインターネットトラフィックや、外からの接続を常に探しているようなプログラムによる接続などを評価します。これにより、侵入される可能性のあるプログラムを発見して対処することができます。

ファイアウォールを起動

ファイアウォールをインストールするとすぐに、コンピュータは侵入や不審なネットワークトラフィックから保護されます。また、アラートの対処や、既知または未知のプログラムによるインターネットアクセスの管理も、すぐに行うことができます。スマートリコメンデーションが自動的に有効になり、セキュリティレベルは [標準] に設定されます。

ファイアウォールは [ネットワークとインターネット設定] パネルから無効にできますが、コンピュータは侵入や不審なネットワークトラフィックから保護されなくなります。また、内向き（受信）と外向き（送信）両方のインターネット接続を効率よく管理することもできなくなります。ファイアウォールによる保護を無効にする必要がある場合は、必要な場合にのみ、一時的に無効にしてください。[ネットワークとインターネット設定] パネルからファイアウォールを有効にすることもできます。

ファイアウォールは Windows Firewall を自動的に無効にし、自身を標準設定のファイアウォールに設定します。

注: ファイアウォールを設定するには、[ネットワークとインターネット設定] パネルを開きます。

ファイアウォールによる保護を開始

ファイアウォールによる保護を有効にすると、コンピュータは侵入や不審なネットワークトラフィックから保護されます。また、内向き（受信）と外向き（送信）両方のインターネット接続を管理できます。

ファイアウォールによる保護を有効にするには

- 1 McAfee SecurityCenter で、次のいずれかの操作を実行します。
 - [インターネットとネットワーク] を選択し、[設定] をクリックします。
 - [詳細メニュー] をクリックし、[ホーム] パネルから [設定] を選択し、[インターネットとネットワーク] をクリックします。
- 2 [インターネットとネットワークの設定] パネルの [ファイアウォールによる保護] の下で [オン] をクリックします。

ファイアウォールによる保護を停止

ファイアウォールによる保護を無効にすると、コンピュータは侵入や不審なネットワークトラフィックに対して脆弱な状態になります。ファイアウォールによる保護を有効にしないと、インターネット接続を管理できません。

ファイアウォールによる保護を無効にするには

- 1 McAfee SecurityCenter で、次のいずれかの操作を実行します。
 - **【インターネットとネットワーク】** を選択し、**【設定】** をクリックします。
 - **【詳細メニュー】** をクリックし、**【ホーム】** パネルから **【設定】** を選択し、**【インターネットとネットワーク】** をクリックします。
- 2 **【インターネットとネットワークの設定】** パネルの **【ファイアウォールによる保護】** の下で **【オフ】** をクリックします。

アラートを使用

ファイアウォールでは、セキュリティの管理に役立つさまざまなアラートが使用されます。これらのアラートは 4 つの種類に分類されます。

- トロイの木馬のブロックのアラート
- レッドアラート
- イエローアラート
- グリーンアラート

アラートには、アラートへの対処方法に関する情報や、コンピュータ上で実行されているプログラムに関する情報も含まれます。

アラートについて

ファイアウォールには 4 種類のアラートがあります。また、コンピュータ上で実行されているプログラムに関する情報や、プログラム情報を入手するための情報がアラートに含まれる場合もあります。

トロイの木馬のブロックのアラート

トロイの木馬は正規のプログラムを装っていますが、コンピュータを混乱させたり、被害を与えたり、コンピュータへの不正アクセスを可能にするプログラムです。トロイの木馬のアラートは、ファイアウォールがトロイの木馬を検出し、ブロックすると表示されます。また、別の脅威が存在していないかスキャンすることをお勧めします。このアラートは、セキュリティレベルが「オープン」に設定されている場合とスマートリコメンデーションが無効になっている場合を除き、すべてのセキュリティレベルで表示されます。

レッドアラート

最も一般的なアラートタイプはレッドアラートです。通常、レッドアラートにはユーザの対応が必要となります。ファイアウォールは、プログラムアクティビティやネットワークイベントに対する一連の対応を自動的に決定できない場合があります。この場合、アラートの最初に問題となっているプログラムアクティビティまたはネットワークイベントが記述され、次に 1 つまたは複数のオプションが表示されます。ユーザはいずれかのオプションを選択する必要があります。スマートリコメンデーションが有効な場合は、「プログラム許可機能」パネルにプログラムが追加されます。

次のような内容のアラートが表示されます。

- **プログラムがインターネットアクセスを要求しています:** インターネットアクセスを試行するプログラムがファイアウォールにより検出されました。
- **プログラムは変更されています:** なんらかの変更が行われているプログラムがファイアウォールにより検出されました。オンラインで更新されている可能性があります。
- **プログラムがブロックされました:** 「プログラム許可機能」パネルに登録されているため、ファイアウォールによりプログラムがブロックされました。

設定とプログラムアクティビティまたはネットワークイベントに応じて、次のようなオプションが表示されます。

- **アクセスを許可:** コンピュータ上のプログラムによるインターネットアクセスを許可します。「プログラム許可機能」パネルにルールが追加されます。

- **1 回のみアクセスを許可:** コンピュータ上のプログラムによるインターネットアクセスを一時的に許可します。たとえば、新しいプログラムをインストールするときに一度だけアクセスが必要となる場合があります。
- **アクセスをブロック:** プログラムのインターネットアクセスをブロックします。
- **送信アクセスのみを許可:** インターネットへの外向き（送信）の接続のみを許可します。通常、このアラートは、セキュリティレベルが [厳重] または [ステルス] に設定されている場合に表示されます。
- **このネットワークを信用する:** ネットワークから受信トラフィックと送信トラフィックを許可します。このネットワークは [信用 IP アドレス] セクションに追加されます。
- **今回はこのネットワークを信用しない:** ネットワークから受信トラフィックと送信トラフィックをブロックします。

イエローアラート

イエローアラートでは、ファイアウォールが検出したネットワークイベントに関する情報が通知されます。たとえば、**[新しいネットワークが検出されました]** アラートは、ファイアウォールが初めて実行された場合や、ファイアウォールがインストールされているコンピュータが新しいネットワークに接続した場合に表示されます。ネットワークを信用するかどうかを選択できます。ネットワークが信用されると、このネットワーク上のすべてのコンピュータからのトラフィックが許可され、信用 IP アドレスに追加されます。

グリーンアラート

多くの場合、グリーンアラートにはイベントに関する基本情報が表示されますが、対応する必要はありません。グリーンアラートは、セキュリティレベルが [標準]、[厳重]、[ステルス]、[ロック] に設定されている場合に表示されます。グリーンアラートの内容は次のとおりです。

- **プログラムは変更されています:** 以前にインターネットアクセスを許可したプログラムが変更されていることを通知します。プログラムをブロックすることもできますが、対応しない場合はデスクトップからアラートの表示が消え、プログラムによるインターネットアクセスは継続されます。
- **プログラムのインターネットアクセスが許可されました:** プログラムにインターネットアクセスが許可されたことを通知します。プログラムをブロックすることもできますが、対応しない場合はアラートの表示が消え、プログラムによるインターネットアクセスは継続されます。

ユーザアシスタンス

ファイアウォールのアラートには、多くの場合、補足的な情報が含まれます。この情報を参考にして、コンピュータのセキュリティを管理できます。含まれる情報には次のものがあります。

- **このプログラムの詳細情報:** マカフィーのグローバル セキュリティ サイトが開き、ご使用のコンピュータのファイアウォールが検出したプログラムに関する情報を取得できます。
- **このプログラムについてマカフィーに報告してください:** コンピュータ上のファイアウォールが検出した未知のファイルに関する情報を、マカフィーに送信します。
- **マカフィーによる推奨事項:** アラートへの対処に関するアドバイスです。たとえば、プログラムに対してアクセスを許可することが推奨されます。

情報アラートを管理

ファイアウォールでは、特定のイベント中に情報アラートを表示または隠すことができます。

ゲーム中にアラートを表示

標準設定では、全画面表示でゲームを実行している間は、ファイアウォールによる情報アラートは表示されません。ただし、ゲームの実行中に侵入や不審なアクティビティが検出された場合にも情報アラートを表示するように、ファイアウォールを設定することもできます。

ゲーム中にアラートを表示するには

- 1 [よく使う機能] パネルで [詳細メニュー] をクリックします。
- 2 [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで [保護の状態] をクリックします。
- 4 [詳細設定] をクリックします。
- 5 [アラートのオプション] パネルで [ゲームモードが検出されたときに情報アラートを表示] を選択します。

情報アラートを非表示化

情報アラートは、早急な対応を必要としないイベントについて通知します。

情報アラートを非表示にするには

- 1 [よく使う機能] パネルで [詳細メニュー] をクリックします。
- 2 [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで [保護の状態] をクリックします。
- 4 [詳細設定] をクリックします。
- 5 [SecurityCenter の設定] パネルで [情報アラート] をクリックします。

- 6 **【情報アラート】** パネルで、次のいずれかの操作を実行します。
 - 表示しないアラートタイプを選択します。
 - **【情報アラートを非表示】** を選択してすべての情報アラートを隠します。
- 7 **【OK】** をクリックします。

第 19 章

ファイアウォールによる保護の設定

ファイアウォールでは、セキュリティを管理したり、セキュリティイベントやアラートへの応答方法を調整するためにさまざまな方法が提供されます。

初めてファイアウォールをインストールした場合、保護レベルは標準セキュリティに設定されます。多くの場合は、この設定ですべてのセキュリティに対応できます。ただし、非常に厳重なレベルから許容範囲の広いレベルまで用意されており、他のセキュリティレベルに設定することもできます。

また、アラートへの対処方法や、プログラムのインターネットアクセスに関する推奨事項が表示される場合もあります。

この章の内容

ファイアウォールのセキュリティレベルを管理	124
スマートリコメンデーションのアラートの設定	128
ファイアウォールによるセキュリティを最適化	130
ファイアウォールをロックおよび復元	133

ファイアウォールのセキュリティレベルを管理

セキュリティレベルを設定することで、不審なネットワークトラフィックや内向き（受信）と外向き（送信）のインターネット接続がファイアウォールにより検出された場合の、アラートの管理および対処の度合いを決定できます。標準設定では、セキュリティレベルは「標準」に設定されています。

セキュリティレベルが「標準」でスマートリコメンデーションが有効な場合、レッドアラートには、未知のプログラムまたは変更されたプログラムのアクセスを許可またはブロックするオプションが表示されます。既知のプログラムが検出されると、グリーンアラート（情報）が表示され、アクセスは自動的に許可されます。アクセスを許可すると、そのプログラムは送信も受信も自由に行うことができます。

通常、セキュリティレベルが高くなる（ステルスおよび厳重）ほど、表示されるオプションとアラートの数が増え、ユーザの対応が必要となる場合が多くなります。

ファイアウォールには 6 種類のセキュリティレベルがあります。セキュリティレベルには次のものがあり、それぞれインターネット接続への対応が異なります。

- **ロック:** すべてのインターネット接続をブロックします。
- **ステルス:** すべての内向き（受信）インターネット接続をブロックします。
- **厳重:** すべてのインターネット接続要求に対してユーザが対応する必要があります。
- **標準:** 未知のプログラムや新しいプログラムがインターネットアクセスを要求した場合に通知されます。
- **信用:** 内向き（受信）外向き（送信）にかかわらずすべてのインターネット接続を許可し、自動的に「プログラム許可機能」パネルに追加します。
- **オープン:** 内向き（受信）外向き（送信）にかかわらずすべてのインターネット接続を許可します。

また、「ファイアウォールによる保護を標準設定に戻す」パネルから、セキュリティレベルを簡単に「標準」に戻すこともできます。

セキュリティレベルの設定: ロック

ファイアウォールのセキュリティレベルを [ロック] に設定すると、Web サイト、E メール、セキュリティ更新へのアクセスを含むすべてのネットワーク接続が受信、送信にかかわらずブロックされます。このセキュリティレベルを設定すると、インターネット接続を削除した場合と同じような結果になります。この設定を使用すると、[システムサービス] パネルで開くように設定したポートをブロックできます。ロック中でも、プログラムのブロックを通知するアラートは表示されます。

ファイアウォールのセキュリティレベルを [ロック] に設定するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [セキュリティレベル] パネルで、スライダーを移動して **[ロック]** を現在のレベルとして表示します。
- 3 **[OK]** をクリックします。

セキュリティレベルの設定: ステルス

ファイアウォールのセキュリティレベルを [ステルス] に設定すると、開かれているポート以外で、すべての受信接続がブロックされます。この設定は、インターネット上からご使用のコンピュータの存在を完全に隠します。セキュリティレベルを [ステルス] に設定すると、新しいプログラムがインターネットへの外向き（送信）接続を試行した場合、もしくは内向き（受信）の接続要求を受信した場合に、アラートが表示されます。ブロックされたプログラムと追加されたプログラムは、[プログラム許可機能] パネルに表示されます。

ファイアウォールのセキュリティレベルを [ステルス] に設定するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [セキュリティレベル] パネルで、スライダーを移動して **[ステルス]** を現在のレベルとして表示します。
- 3 **[OK]** をクリックします。

セキュリティレベルの設定: 厳重

セキュリティレベルを「厳重」に設定すると、新しいプログラムがインターネットへの外向き（送信）接続を試行した場合、もしくは内向き（受信）の接続要求を受信した場合にユーザに通知します。ブロックされたプログラムと追加されたプログラムは、「プログラム許可機能」パネルに表示されます。セキュリティレベルを「厳重」に設定すると、プログラムはその時点で必要な種類のアクセスのみを要求し、ユーザがそのアクセスを許可またはブロックします。設定後に、内向き（受信）と外向き（送信）両方の接続が必要となった場合は、「プログラム許可機能」パネルからすべてのアクセスを許可できます。

ファイアウォールのセキュリティレベルを「厳重」に設定するには

- 1 「ネットワークとインターネット設定」パネルで「詳細設定」をクリックします。
- 2 「セキュリティレベル」パネルで、スライダーを移動して「厳重」を現在のレベルとして表示します。
- 3 「OK」をクリックします。

セキュリティレベルの設定: 標準

標準設定のセキュリティレベルは「標準」で、このレベルをお勧めします。

セキュリティレベルを「標準」に設定すると、すべての接続がファイアウォールにより監視され、新しいプログラムがインターネットアクセスを試行した場合にアラートが表示されます。ブロックされたプログラムと追加されたプログラムは、「プログラム許可機能」パネルに表示されます。

ファイアウォールのセキュリティレベルを「標準」に設定するには

- 1 「インターネットとネットワークの設定」パネルで「詳細設定」をクリックします。
- 2 「セキュリティレベル」パネルで、スライダーを移動して「標準」を現在のレベルとして表示します。
- 3 「OK」をクリックします。

セキュリティレベルの設定: 信用

ファイアウォールのセキュリティレベルを [信用] に設定すると、受信、送信にかかわらずすべての接続が許可されます。信用セキュリティでは、すべてのプログラムのアクセスが自動的に許可され、[プログラム許可機能] パネルの許可プログラムのリストに追加されます。

ファイアウォールのセキュリティレベルを [信用] に設定するには

- 1 [ネットワークとインターネット設定] パネルで [詳細設定] をクリックします。
- 2 [セキュリティレベル] パネルで、スライダーを移動して [信用] を現在のレベルとして表示します。
- 3 [OK] をクリックします。

スマートリコメンデーションのアラートの設定

インターネットへのアクセスを試行するプログラムに対し、推奨事項を自動で実行するか、アラートへ表示するか、しないかを設定できます。

スマートリコメンデーションを参考にして、アラートへの対処方法を決定できます。スマートリコメンデーションを有効にすると（セキュリティレベルが「標準」の場合）、既知のプログラムは自動的に許可またはブロックされます。危険性のある未知のプログラムが検出された場合は、対処方法がアラートに表示されます。

スマートリコメンデーションを無効にすると、インターネットアクセスが自動的に許可/ブロックされることも、推奨される対処方法が表示されることもありません。

スマートリコメンデーションの表示のみを行うようにファイアウォールを設定した場合、アクセスの許可またはブロックを確認するメッセージがアラートに表示され、推奨される対処方法も表示されます。

スマートリコメンデーションを有効化

スマートリコメンデーションを参考にして、アラートへの対処方法を決定できます。スマートリコメンデーションを有効にすると、プログラムは自動的に許可またはブロックされ、認識されていないプログラムや危険性があるプログラムに関してのみアラートが表示されます。

スマートリコメンデーションを有効にするには

- 1 「ネットワークとインターネット設定」パネルで**【詳細設定】**をクリックします。
- 2 「セキュリティレベル」パネルの**【スマートリコメンデーション】**で、**【スマートリコメンデーションを有効化】**を選択します。
- 3 **【OK】**をクリックします。

スマートリコメンデーションを無効化

スマートリコメンデーションを無効にすると、アラートへの対処方法に関する情報や、プログラムのアクセスの管理方法に関する情報は表示されません。スマートリコメンデーションを無効にしても、ファイアウォールによるプログラムの許可およびブロックは継続され、認識されていないプログラムや危険性があるプログラムに関するアラートは表示されます。また、脅威である可能性がある新しいプログラム、または脅威であると判明している新しいプログラムが検出されると、プログラムのインターネットアクセスがファイアウォールにより自動的にブロックされます。

スマートリコメンデーションを無効にするには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [セキュリティレベル] パネルの **[スマートリコメンデーション]** で、**[スマートリコメンデーションを無効化]** を選択します。
- 3 **[OK]** をクリックします。

スマートリコメンデーションの表示のみ

スマートリコメンデーションを参考にして、認識されていないプログラムや危険性があるプログラムに関するアラートの対処方法を決定できます。スマートリコメンデーションを **[表示のみ]** に設定すると、アラートへの対処に関する情報が表示されます。ただし、**[スマートリコメンデーションを有効化]** オプションとは異なり、表示される対処方法が自動的に適用されることはなく、プログラムのアクセスが自動的に許可またはブロックされることもありません。かわりに、アラートに表示される推奨事項を参考にして、プログラムを許可するかブロックするかを決定できます。

スマートリコメンデーションの表示のみをするには

- 1 [インターネットとネットワークの設定] パネルで **[詳細設定]** をクリックします。
- 2 [セキュリティレベル] パネルの **[スマートリコメンデーション]** で、**[表示のみ]** を選択します。
- 3 **[OK]** をクリックします。

ファイアウォールによるセキュリティを最適化

コンピュータのセキュリティを侵害する多くの方法が存在しています。たとえば、Windows が起動する前にインターネット接続を試行するプログラムがあります。また、コンピュータに詳しいユーザは、コンピュータに対して ping を実行し、ネットワークに接続しているかどうかを確認することができます。ファイアウォールを使用すると、ブート時の保護を有効にしたり ICMP ping 要求をブロックすることで、これらの種類の侵入を防御できます。前者の設定では Windows の起動中にプログラムのインターネットアクセスがブロックされ、後者の設定では他のユーザによりネットワーク上でコンピュータが検出される ping 要求がブロックされます。

標準インストールでは、サービス拒否攻撃やエクスプロイトなどの一般的な侵入行為を自動的に検出するよう設定されます。標準インストール設定を使用することにより、これらの攻撃やスキャンから保護されます。ただし、[侵入検知] パネルで、それぞれの攻撃またはスキャンに対する自動検出機能を無効化することもできます。

起動中のコンピュータを保護

ファイアウォールは Windows の起動時にコンピュータを保護できます。ブート時の保護を行うと、これまでにインターネットアクセスが許可および要求されていない新しいプログラムがすべてブロックされます。ファイアウォールを起動すると、起動中にインターネットアクセスを要求したプログラムに関連するアラートが表示され、この要求をブロックまたは許可できます。このオプションを使用するには、セキュリティレベルが [オープン] と [ロック] 以外である必要があります。

起動中のコンピュータを保護するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [セキュリティレベル] パネルの [セキュリティ設定] で、**[ブート時の保護を有効にする]** を選択します。
- 3 **[OK]** をクリックします。

注: ブート時の保護が有効になっている間は、ブロックされた接続と侵入はログに記録されません。

ping 要求の設定

ICMP Echo Request メッセージを送受信する ping ツールを使用すると、特定のコンピュータがネットワークに接続しているかどうかを確認できます。ファイアウォールを設定して、ご使用のコンピュータに対する ping の実行を防止または許可できます。

ICMP ping 要求の設定を行うには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [セキュリティレベル] パネルの **[セキュリティ設定]** で、次のいずれかの操作を実行します。
 - **[ICMP ping 要求を許可]** を選択し、ネットワーク上で ping 要求を使用したコンピュータの検出を許可します。
 - ping 要求によりご使用のコンピュータがネットワーク上で検出されることを防ぐには、**[ICMP ping 要求を許可]** のチェックボックスをオフにします。
- 3 **[OK]** をクリックします。

侵入検知の設定

侵入検知システム (IDS) では、すべてのデータパケットを監視し、不審なデータ転送または転送メソッドを検出します。IDS は、トラフィックとデータパケットを分析して、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。たとえば、ICMP パケットが検出されると、それらを既知の攻撃パターンと照合して不審なトラフィックかどうか分析します。ファイアウォールはパケットをシグネチャデータベースと比較します。不審な場合や危険性がある場合は、攻撃元コンピュータから送信されるパケットを破棄し、状況に応じてイベントをログに記録します。

標準インストールでは、サービス拒否攻撃やエクスプロイトなどの一般的な侵入行為を自動的に検出するよう設定されます。標準インストール設定を使用することにより、これらの攻撃やスキャンから保護されます。ただし、[侵入検知] パネルで、それぞれの攻撃またはスキャンに対する自動検出機能が無効化することもできます。

侵入検知の設定を行うには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[侵入検知]** をクリックします。

- 3 **【侵入を検出】** で、次のいずれかの操作を実行します。
 - 名前を選択し、攻撃やスキャンを自動的に検出します。
 - 攻撃またはスキャンの自動検出を無効にするには、名前の選択を解除します。
- 4 **【OK】** をクリックします。

ファイアウォールによる保護の状態の設定

McAfee SecurityCenter は、コンピュータの全体的な保護の状態を把握するため、問題を追跡します。ただし、保護の状態に影響する特定の問題を無視するようにファイアウォールを設定することもできます。次のような場合は、特定の問題を無視するように McAfee SecurityCenter を設定できます: ファイアウォールのセキュリティレベルが **【オープン】** の場合、ファイアウォールサービスが実行されていない場合、外向き通信用ファイアウォールがコンピュータにインストールされていない場合。

ファイアウォールの保護の状態を設定するには

- 1 **【よく使う機能】** パネルで **【詳細メニュー】** をクリックします。
- 2 **【設定】** をクリックします。
- 3 **【SecurityCenter の設定】** パネルで **【保護の状態】** をクリックします。
- 4 **【詳細設定】** をクリックします。
- 5 **【よく使う機能】** パネルで **【詳細メニュー】** をクリックします。
- 6 **【設定】** をクリックします。
- 7 **【SecurityCenter の設定】** パネルで **【保護の状態】** をクリックします。
- 8 **【詳細設定】** をクリックします。
- 9 **【無視された問題】** パネルで、次のオプションから 1 つまたは複数を選択します。
 - ファイアウォールのセキュリティレベルが **【オープン】** に設定されています。
 - ファイアウォールサービスが実行されていません。
 - 外向き通信用ファイアウォールがコンピュータにインストールされていません。
- 10 **【OK】** をクリックします。

ファイアウォールをロックおよび復元

ロック機能は、重大な問題が発生したコンピュータをネットワークから隔離して問題を解決する場合に役立ちます。また、プログラムのインターネットアクセスの管理方法を調査する場合にも有効です。

ファイアウォールを迅速にロック

ファイアウォールをロックすると、受信、送信にかかわらずすべてのネットワークトラフィックが即座にブロックされます。別のコンピュータからのアクセスがすべて停止され、コンピュータ上のプログラムによるインターネットアクセスもすべてブロックされます。

ファイアウォールをすぐにロックしてすべてのネットワークトラフィックをブロックするには

- 1 [標準メニュー] または [詳細メニュー] の [ホーム] パネルまたは [よく使う機能] パネルで、[ファイアウォールをロック] をクリックします。
- 2 [ファイアウォールをロック] パネルで [ロック] をクリックします。
- 3 ダイアログで [はい] をクリックし、受信トラフィックおよび送信トラフィックをすぐにブロックします。

ファイアウォールを迅速にロック解除

ファイアウォールをロックすると、受信、送信にかかわらずすべてのネットワークトラフィックが即座にブロックされます。別のコンピュータからのアクセスがすべて停止され、コンピュータ上のプログラムによるインターネットアクセスもすべてブロックされます。ファイアウォールをロックしたあと、ネットワークトラフィックを許可するには、ロックを解除します。

ファイアウォールのロックをすぐに解除してネットワークトラフィックを許可するには

- 1 [標準メニュー] または [詳細メニュー] の [ホーム] パネルまたは [よく使う機能] パネルで、[ファイアウォールをロック] をクリックします。
- 2 [ロックが有効です] パネルで [ロック解除] をクリックします。
- 3 ダイアログで [はい] をクリックし、ファイアウォールのロック解除とネットワークトラフィックの許可を行います。

ファイアウォールの設定を復元

ファイアウォールの元の保護設定を迅速に復元できます。セキュリティレベル設定は [標準] となり、スマートリコメンデーションが有効になります。また、信用 IP アドレスと禁止 IP アドレスがリセットされ、[プログラム許可機能] パネルからすべてのプログラムが削除されます。

ファイアウォールの設定を初期設定に戻すには

- 1 [標準メニュー] または [詳細メニュー] の [ホーム] パネルまたは [よく使う機能] パネルで、[ファイアウォールを標準設定に戻す] をクリックします。
- 2 [ファイアウォールによる保護を標準設定に戻す] パネルで [標準設定に戻す] をクリックします。
- 3 [ファイアウォールによる保護を標準設定に戻す] ダイアログで [はい] をクリックし、ファイアウォールの設定を標準設定に戻します。

セキュリティレベルの設定: オープン

ファイアウォールのセキュリティレベルを [オープン] に設定すると、受信、送信にかかわらずすべてのネットワーク接続が許可されます。以前にブロックしたプログラムに対してアクセスを許可するには、[プログラム許可機能] パネルを使用します。

ファイアウォールのセキュリティレベルを [オープン] に設定するには

- 1 [ネットワークとインターネット設定] パネルで [詳細設定] をクリックします。
- 2 [セキュリティレベル] パネルで、スライダーを移動して [オープン] を現在のレベルとして表示します。
- 3 [OK] をクリックします。

注: セキュリティレベルを [オープン] に設定しても、以前にブロックされたプログラムは引き続きブロックされます。これを防ぐには、プログラムのルールを [すべてのアクセス] に変更します。

第 20 章

プログラムと権限を管理

ファイアウォールを使用すると、インターネットへの送信/受信アクセスを必要とする既存のプログラムおよび新しいプログラムのアクセス権の管理や作成ができます。また、すべてのアクセスまたは送信アクセスのみをプログラムに許可できます。また、プログラムのアクセスをブロックすることもできます。

この章の内容

プログラムのインターネットアクセスを許可	136
プログラムに送信アクセスのみを許可	139
プログラムのインターネットアクセスをブロック	141
プログラムのアクセス権を削除	143
プログラムについての確認	144

プログラムのインターネットアクセスを許可

インターネットブラウザなど、一部のプログラムは、正常に動作するためにインターネットにアクセスする必要があります。

ファイアウォールの [プログラム許可機能] パネルでは次の操作を実行できます。

- プログラムのアクセスを許可する
- プログラムの送信アクセスのみを許可する
- プログラムのアクセスをブロックする

また、送信イベントログもしくは最近のイベントログから、すべてのアクセスまたは送信アクセスのみを許可することもできます。

プログラムにすべてのアクセスを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。McAfee Personal Firewall には自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、この権限は変更できます。

プログラムにすべてのアクセスを許可するには

- 1 [インターネットとネットワークの設定] パネルで [詳細設定] をクリックします。
- 2 [ファイアウォール] パネルで [プログラム許可機能] をクリックします。
- 3 [プログラム許可機能] で、[ブロック] または [送信アクセスのみ] に設定されているプログラムを選択します。
- 4 [対応] で [すべてのアクセスを許可] をクリックします。
- 5 [OK] をクリックします。

新しいプログラムにすべてのアクセスを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。ファイアウォールには自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、新しいプログラムを追加したり、権限を変更できます。

新しいプログラムにすべてのインターネットアクセスを許可するには

- 1 [インターネットとネットワークの設定] パネルで [詳細設定] をクリックします。
- 2 [ファイアウォール] パネルで [プログラム許可機能] をクリックします。

- 3 [プログラム許可機能] で [許可されたプログラムを追加] をクリックします。
- 4 [プログラムの追加] ダイアログで、追加するプログラムを参照して選択します。
- 5 [開く] をクリックします。
- 6 [OK] をクリックします。

新しく追加したプログラムが [プログラム許可機能] に表示されます。

注: 既存のプログラムと同様に、プログラムを選択して [対応] の [送信アクセスのみを許可] または [アクセスをブロック] をクリックすると、新しく追加したプログラムの権限を変更できます。

最近のイベントログからすべてのアクセスを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。最近のイベントログからプログラムを選択し、インターネットへのすべてのアクセスを許可できます。

最近のイベントログからプログラムにすべてのアクセスを許可するには

- 1 [よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で、イベントの説明を選択して [すべてのアクセスを許可] をクリックします。
- 3 [プログラム許可機能] ダイアログで [はい] をクリックし、プログラムのアクセスを許可します。

関連項目

- 送信イベントを表示 (164 ページ)

送信イベントログからすべてのアクセスを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。送信イベントログからプログラムを選択し、インターネットへのすべてのアクセスを許可できます。

送信イベントログからプログラムにすべてのインターネットアクセスを許可するには

- 1 [よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク]、[送信イベント] の順に選択します。

- 4 [送信イベント] パネルで送信元 IP アドレスを選択し、[アクセスを許可] をクリックします。
- 5 [プログラム許可機能] ダイアログで [はい] をクリックし、プログラムにすべてのインターネットアクセスを許可します。

関連項目

- [送信イベントを表示](#) (164 ページ)

プログラムに送信アクセスのみを許可

コンピュータにインストールされている一部のプログラムは、インターネットへの送信アクセスのみを必要とします。ファイアウォールを使用すると、インターネットへの送信アクセスのみをプログラムに許可できます。

プログラムに送信アクセスのみを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。McAfee Personal Firewall には自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、この権限は変更できます。

プログラムに送信アクセスのみを許可するには

- 1 [インターネットとネットワークの設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[プログラム許可機能]** をクリックします。
- 3 **[プログラム許可機能]** で、**[ブロック]** または **[すべてのアクセス]** に設定されているプログラムを選択します。
- 4 **[対応]** で **[送信アクセスのみを許可]** をクリックします。
- 5 **[OK]** をクリックします。

最近のイベントログから送信アクセスのみを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。最近のイベントログからプログラムを選択し、インターネットへの送信アクセスのみを許可できます。

最近のイベントログからプログラムに送信アクセスのみを許可するには

- 1 **[よく使う機能]** パネルで **[レポートとログ]** をクリックします。
- 2 **[最近のイベント]** で、イベントの説明を選択して **[送信アクセスのみを許可]** をクリックします。
- 3 **[プログラム許可機能]** ダイアログで **[はい]** をクリックし、プログラムの送信アクセスのみを許可します。

関連項目

- **送信イベントを表示** (164 ページ)

送信イベントログから送信アクセスのみを許可

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。送信イベントログからプログラムを選択し、インターネットへの送信アクセスのみを許可できます。

送信イベントログからプログラムに送信アクセスのみを許可するには

- 1 [よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク]、[送信イベント] の順に選択します。
- 4 [送信イベント] パネルで送信元 IP アドレスを選択し、[送信アクセスのみを許可] をクリックします。
- 5 [プログラム許可機能] ダイアログで [はい] をクリックし、プログラムの送信アクセスのみを許可します。

関連項目

- [送信イベントを表示](#) (164 ページ)

プログラムのインターネットアクセスをブロック

ファイアウォールを使用すると、プログラムによるインターネットアクセスをブロックできます。プログラムをブロックすると、ネットワーク接続に影響があったり、正常に動作するためにインターネットアクセスを必要とするプログラムが中断される場合があります。このような影響がないことを確認してください。

プログラムのアクセスをブロック

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。McAfee Personal Firewall には自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、この権限はブロックできます。

プログラムのインターネットアクセスをブロックするには

- 1 [インターネットとネットワークの設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[プログラム許可機能]** をクリックします。
- 3 **[プログラム許可機能]** で、**[すべてのアクセス]** または **[送信アクセスのみ]** に設定されているプログラムを選択します。
- 4 **[対応]** で **[アクセスをブロック]** をクリックします。
- 5 **[OK]** をクリックします。

新しいプログラムのアクセスをブロック

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。McAfee Personal Firewall には自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、新しいプログラムを追加したり、プログラムのインターネットアクセスをブロックできます。

新しいプログラムのインターネットアクセスをブロックするには

- 1 [インターネットとネットワークの設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[プログラム許可機能]** をクリックします。
- 3 **[プログラム許可機能]** で **[ブロックされたプログラムを追加]** をクリックします。
- 4 **[プログラムの追加]** ダイアログで、追加するプログラムを参照して選択します。

5 **【開く】** をクリックします。

6 **【OK】** をクリックします。

新しく追加したプログラムが **【プログラム許可機能】** に表示されます。

注: 既存のプログラムと同様に、プログラムを選択して **【対応】** の **【送信アクセスのみを許可】** または **【すべてのアクセスを許可】** をクリックすると、新しく追加したプログラムの権限を変更できます。

最近のイベントログからアクセスをブロック

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。ただし、最近のイベントログからプログラムのインターネットアクセスをブロックするように選択することもできます。

最近のイベントログからプログラムへのアクセスのブロックを行うには

- 1 **【よく使う機能】** パネルで **【レポートとログ】** をクリックします。
- 2 **【最近のイベント】** で、イベントの説明を選択して **【アクセスをブロック】** をクリックします。
- 3 **【プログラム許可機能】** ダイアログで **【はい】** をクリックし、プログラムをブロックします。

関連項目

- **送信イベントを表示** (164 ページ)

プログラムのアクセス権を削除

プログラムの許可を削除する前に、削除がコンピュータの機能やネットワーク接続に影響しないことを確認してください。

プログラムの許可を削除

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。McAfee Personal Firewall には自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、自動または手動で追加されたプログラムを削除できます。

新しいプログラムのプログラム許可を削除するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[プログラム許可機能]** をクリックします。
- 3 **[プログラム許可機能]** でプログラムを選択します。
- 4 **[対応]** で **[プログラムの許可を削除]** をクリックします。
- 5 **[OK]** をクリックします。

[プログラム許可機能] パネルからプログラムが削除されます。

注: プログラムの中には、対応が無効（灰色で表示）になっていて変更できないものがあります。

プログラムについての確認

プログラムに適用すべき権限がわからない場合は、マカフィーの HackerWatch の Web サイトで、プログラムに関する情報を取得できます。

プログラム情報を取得

コンピュータにインストールされているプログラムの多くは、インターネットへの送信/受信アクセスを必要とします。McAfee Personal Firewall には自動的にすべてのアクセスを許可するプログラムのリストがあります。ただし、この権限は変更できます。

ファイアウォールで表示される情報を参考にして、プログラムのインターネットアクセスを許可するかブロックするかを決定できます。マカフィーの HackerWatch の Web サイトが正常に表示されるように、インターネットに接続していることを確認します。このサイトは、プログラム、インターネットアクセスの要件、セキュリティの脅威に関する最新情報を提供します。

プログラム情報を取得するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[プログラム許可機能]** をクリックします。
- 3 **[プログラム許可機能]** でプログラムを選択します。
- 4 **[対応]** で **[詳細情報]** をクリックします。

送信イベントログからプログラム情報を取得

McAfee Personal Firewall では、送信イベントログに表示されるプログラムに関する情報を取得できます。

プログラムに関する情報を取得する前に、インターネットに接続していて、インターネットブラウザが使用できることを確認してください。

送信イベントログからプログラム情報を取得するには

- 1 [よく使う機能] パネルで **[レポートとログ]** をクリックします。
- 2 **[最近のイベント]** で **[ログを表示]** をクリックします。
- 3 **[インターネットとネットワーク]**、**[送信イベント]** の順に選択します。

- 4 [送信イベント] パネルで送信元 IP アドレスを選択し、[詳細情報] をクリックします。

HackerWatch の Web サイトでプログラムに関する情報を参照できます。HackerWatch では、プログラム、インターネットアクセスの要件、セキュリティ脅威に関する最新情報が提供されます。

関連項目

- [送信イベントを表示](#) (164 ページ)

第 21 章

システムサービスを管理

Web サーバやファイル共有サーバ プログラムといった特定のプログラムの中には、適切に動作するために、指定されたシステム サービス ポートを通じて別のコンピュータから要求していない接続を受け入れなければならないものもあります。多くの場合、これらのシステム サービス ポートはシステムの安全性を損なう原因となるため、ファイアウォールはこれらのポートを閉じます。しかし、リモートコンピュータからの接続を許可するには、システム サービス ポートが開いている必要があります。

一般的なサービスと標準ポートは次のとおりです。

- ファイル転送プロトコル (FTP) ポート 20～21
- メールサーバ (IMAP) ポート 143
- メールサーバ (POP3) ポート 110
- メールサーバ (SMTP) ポート 25
- Microsoft ディレクトリサーバ (MSFT DS) ポート 445
- Microsoft SQL サーバ (MSFT SQL) ポート 1433
- リモートアシスタンス/端末サーバ (RDP) ポート 3389
- リモート プロシージャ コール (RPC) ポート 135
- セキュア Web サーバ (HTTPS) ポート 443
- ユニバーサル プラグ アンド プレイ (UPNP) ポート 5000
- Web サーバ (HTTP) ポート 80
- Windows ファイル共有 (NETBIOS) ポート 137～139

この章の内容

システム サービス ポートの設定..... 148

システム サービス ポートの設定

コンピュータ上のサービスにリモートアクセスを許可するには、該当するサービスおよびオープンする関連ポートを指定する必要があります。確実に開く必要がある場合のみ、サービスとポートを選択してください。ポートを開く必要が生じることはめったにありません。

既存のシステム サービス ポートへのアクセスを許可

[システムサービス] パネルから既存のシステム サービス ポートを開いたり閉じたりして、コンピュータ上のネットワークサービスへのリモートアクセスを許可または拒否できます。システム サービス ポートを開くと、インターネットセキュリティの脅威に対してコンピュータが脆弱な状態になる可能性があるため、ポートは必要な場合に限り開きます。

システム サービス ポートへのアクセスを許可するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[システムサービス]** をクリックします。
- 3 **[システムサービスのポートを開く]** で、ポートをオープンするシステムサービスを選択します。
- 4 **[OK]** をクリックします。

既存のシステム サービス ポートへのアクセスをブロック

[システムサービス] パネルから既存のシステム サービス ポートを開いたり閉じたりして、コンピュータ上のネットワークサービスへのリモートアクセスを許可または拒否できます。システム サービス ポートを開くと、インターネットセキュリティの脅威に対してコンピュータが脆弱な状態になる可能性があるため、ポートは必要な場合に限り開きます。

システム サービス ポートへのアクセスをブロックするには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[システムサービス]** をクリックします。
- 3 **[システムサービスのポートを開く]** で、ポートを閉じるシステムサービスの選択を解除します。
- 4 **[OK]** をクリックします。

新しいシステム サービス ポートの設定

[システムサービス] パネルから新しいシステム サービス ポートを追加でき、ポートを開いたり閉じたりして、コンピュータ上のネットワークサービスへのリモートアクセスを許可または拒否できます。システム サービス ポートを開くと、インターネットセキュリティの脅威に対してコンピュータが脆弱な状態になる可能性があるため、ポートは必要な場合に限り開きます。

新しいシステム サービス ポートの作成と設定を行うには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[システムサービス]** をクリックします。
- 3 **[追加]** をクリックします。
- 4 **[ポートの構成を追加]** で、以下の内容を指定します。
 - プログラム名
 - 受信 TCP/IP ポート
 - 送信 TCP/IP ポート
 - 受信 UDP ポート
 - 送信 UDP ポート
- 5 新しい設定の説明を入力します (オプション)。
- 6 **[OK]** をクリックします。

新しく設定されたシステム サービス ポートが **[システムサービスのポートを開く]** に表示されます。

システム サービス ポートを変更

ポートが開いているか閉じているかにより、コンピュータ上のネットワークサービスへのアクセスが許可または拒否されます。[システムサービス] パネルから、既存のポートの送信/受信情報を変更できます。入力したポート情報が間違っていると、システムサービスは正常に動作しません。

システム サービス ポートを変更するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[システムサービス]** をクリックします。
- 3 システムサービスを選択し、**[編集]** をクリックします。

4 **[ポートの構成を追加]** で、以下の内容を指定します。

- プログラム名
- 受信 TCP/IP ポート
- 送信 TCP/IP ポート
- 受信 UDP ポート
- 送信 UDP ポート

5 変更した設定の説明を入力します（オプション）。

6 **[OK]** をクリックします。

設定を変更したシステム サービス ポートが **[システムサービスのポートを開く]** に表示されます。

システム サービス ポートを削除

ポートが開いているか閉じているかにより、コンピュータ上のネットワークサービスへのアクセスが許可または拒否されます。**[システムサービス]** パネルから、既存のポートと関連するシステムサービスを削除できます。ポートとシステムサービスが **[システムサービス]** パネルから削除されると、リモートコンピュータはご使用のコンピュータ上のネットワークサービスにアクセスできなくなります。

システム サービス ポートを削除するには

- 1 **[ネットワークとインターネット設定]** パネルで **[詳細設定]** をクリックします。
- 2 **[ファイアウォール]** パネルで **[システムサービス]** をクリックします。
- 3 システムサービスを選択し、**[削除]** をクリックします。
- 4 **[システムサービス]** ダイアログで **[はい]** をクリックし、システムサービスを削除します。

[システムサービス] パネルにシステム サービス ポートが表示されなくなります。

第 22 章

コンピュータ接続を管理

リモートコンピュータに関連付けられたインターネット プロトコル アドレス (IP) に基づいてルールを作成し、コンピュータへの特定のリモート接続を管理するようにファイアウォールを設定できます。信用できる IP アドレスのコンピュータからご使用のコンピュータへの接続を信用したり、未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

接続を許可する場合、信用するコンピュータが安全であることを確認してください。信用したコンピュータがワームやその他のメカニズムによってウイルスに感染すると、このコンピュータも危険にさらされることになります。また、信用するコンピュータをファイアウォールと最新のウイルス対策プログラムで保護することをお勧めします。[信用 IP アドレス] リストの IP アドレスからのトラフィックは、ログに記録されず、またイベントアラートの対象にもなりません。

未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

ファイアウォールは不要なトラフィックをすべてブロックするため、通常は、IP アドレスを禁止する必要はありません。あるインターネット接続によって危険にさらされることがわかっている場合を除き、IP アドレスは禁止しないでください。DNS サーバ、DHCP サーバ、または ISP のその他のサーバなどの重要な IP アドレスをブロックしないように特に注意してください。セキュリティの設定によっては、禁止されたコンピュータからのイベントをファイアウォールが検出した際に、アラートを表示させることができます。

この章の内容

コンピュータ接続を信用	152
コンピュータ接続を禁止	156

コンピュータ接続を信用

[信用 IP と禁止 IP] パネルの [信用 IP アドレス] で、信用 IP アドレスを追加、編集、削除できます。

[信用 IP と禁止 IP] パネルの [信用 IP アドレス] リストを使用して、特定のコンピュータからユーザのコンピュータへのトラフィックをすべて許可することができます。[信用 IP アドレス] リストの IP アドレスからのトラフィックは、ログに記録されず、またイベントアラートの対象にもなりません。

ファイアウォールはリストでチェックマークが付けられているすべての IP アドレスを信用し、信用 IP からのトラフィックに対して、すべてのポートのファイアウォールの通過を許可します。信用 IP アドレスからのイベントはファイアウォールでは記録されません。信用 IP アドレスのコンピュータとご使用のコンピュータの間で行われるアクティビティは、ファイアウォールでフィルタリングまたは分析されません。

接続を許可する場合、信用するコンピュータが安全であることを確認してください。信用したコンピュータがワームやその他のメカニズムによってウイルスに感染すると、このコンピュータも危険にさらされることになります。また、信用するコンピュータをファイアウォールと最新のウイルス対策プログラムで保護することをお勧めします。

信用するコンピュータ接続を追加

ファイアウォールを使用して、信用するコンピュータ接続と関連する IP アドレスを追加できます。

[信用 IP と禁止 IP] パネルの [信用 IP アドレス] リストを使用して、特定のコンピュータからユーザのコンピュータへのトラフィックをすべて許可することができます。[信用 IP アドレス] リストの IP アドレスからのトラフィックは、ログに記録されず、またイベントアラートの対象にもなりません。

信用 IP アドレスのコンピュータは、いつでもこのコンピュータに接続できます。信用 IP アドレスを追加、編集または削除するときは、安全なアドレスまたは削除可能なアドレスであることを確認してください。

信用するコンピュータ接続を追加するには

- 1 [ネットワークとインターネット設定] パネルで [詳細設定] をクリックします。
- 2 [ファイアウォール] パネルで [信用 IP と禁止 IP] をクリックします。
- 3 [信用 IP と禁止 IP] パネルで [信用 IP アドレス] をクリックします。

- 4 [追加] をクリックします。
 - 5 [信用 IP アドレスルールを追加] で、次のいずれかの操作を実行します。
 - [単一の IP アドレス] を選択し、IP アドレスを入力します。
 - [IP アドレスの範囲] を選択し、[開始 IP アドレス] ボックスおよび [終了 IP アドレス] ボックスに開始 IP アドレスおよび終了 IP アドレスを入力します。
 - 6 [ルールの有効期限] を選択し、ルールを施行する日数を入力します（オプション）。
 - 7 ルールの説明を入力します（オプション）。
 - 8 [OK] をクリックします。
 - 9 [信用 IP アドレスルールを追加] ダイアログで [はい] をクリックし、信用するコンピュータ接続を追加します。
- 新しく追加した IP アドレスが [信用 IP アドレス] に表示されます。

受信イベントログから信用するコンピュータを追加

受信イベントログから、信用するコンピュータ接続とそのコンピュータに関連する IP アドレスを追加できます。

信用 IP アドレスのコンピュータは、いつでもこのコンピュータに接続できます。信用 IP アドレスを追加、編集または削除するときは、安全なアドレスまたは削除可能なアドレスであることを確認してください。

受信イベントログから信用するコンピュータ接続を追加するには

- 1 [詳細メニュー] が有効になっていることを確認してください。[よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク] をクリックし、[受信イベント] をクリックします。
- 4 [受信イベント] パネルで送信元 IP アドレスを選択し、[このアドレスを信用] をクリックします。
- 5 [信用 IP アドレスルールを追加] ダイアログで [はい] をクリックし、IP アドレスを信用します。

新しく追加した IP アドレスが [信用 IP アドレス] に表示されます。

関連項目

- イベントログを記録 (162 ページ)

信用するコンピュータ接続を編集

ファイアウォールを使用して、信用するコンピュータ接続と関連する IP アドレスを編集できます。

信用 IP アドレスのコンピュータは、いつでもこのコンピュータに接続できます。信用 IP アドレスを追加、編集または削除するときは、安全なアドレスまたは削除可能なアドレスであることを確認してください。

信用するコンピュータ接続を編集するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[信用 IP と禁止 IP]** をクリックします。
- 3 [信用 IP と禁止 IP] パネルで **[信用 IP アドレス]** をクリックします。
- 4 IP アドレスを選択し、**[編集]** をクリックします。
- 5 **[信用 IP アドレスルールを追加]** で、次のいずれかの操作を実行します。
 - **[単一の IP アドレス]** を選択し、IP アドレスを入力します。
 - **[IP アドレスの範囲]** を選択し、**[開始 IP アドレス]** ボックスおよび **[終了 IP アドレス]** ボックスに開始 IP アドレスおよび終了 IP アドレスを入力します。
- 6 **[ルールの有効期限]** にチェックマークを入れ、ルールを施行する日数を入力します（オプション）。
- 7 ルールの説明を入力します（オプション）。
- 8 **[OK]** をクリックします。

変更した IP アドレスが **[信用 IP アドレス]** に表示されます。

信用するコンピュータ接続を削除

ファイアウォールを使用して、信用するコンピュータ接続と関連する IP アドレスを削除できます。

信用 IP アドレスのコンピュータは、いつでもこのコンピュータに接続できます。信用 IP アドレスを追加、編集または削除するときは、安全なアドレスまたは削除可能なアドレスであることを確認してください。

信用するコンピュータ接続を削除するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[信用 IP と禁止 IP]** をクリックします。

- 3 [信用 IP と禁止 IP] パネルで [信用 IP アドレス] をクリックします。
- 4 IP アドレスを選択し、[削除] をクリックします。
- 5 [信用 IP と禁止 IP] ダイアログで [はい] をクリックし、[信用 IP アドレス] の信用 IP アドレスを削除します。

コンピュータ接続を禁止

[信用 IP と禁止 IP] パネルの [禁止 IP アドレス] で、信用 IP アドレスを追加、編集、削除できます。

未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

ファイアウォールは不要なトラフィックをすべてブロックするため、通常は、IP アドレスを禁止する必要はありません。あるインターネット接続によって危険にさらされることがわかっている場合を除き、IP アドレスは禁止しないでください。DNS サーバ、DHCP サーバ、または ISP のその他のサーバなどの重要な IP アドレスをブロックしないように特に注意してください。セキュリティの設定によっては、禁止されたコンピュータからのイベントをファイアウォールが検出した際に、アラートを表示させることができます。

禁止するコンピュータ接続を追加

ファイアウォールを使用して、禁止するコンピュータ接続と関連する IP アドレスを追加できます。

未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

ファイアウォールは不要なトラフィックをすべてブロックするため、通常は、IP アドレスを禁止する必要はありません。あるインターネット接続によって危険にさらされることがわかっている場合を除き、IP アドレスは禁止しないでください。DNS サーバ、DHCP サーバ、または ISP のその他のサーバなどの重要な IP アドレスをブロックしないように特に注意してください。セキュリティの設定によっては、禁止されたコンピュータからのイベントをファイアウォールが検出した際に、アラートを表示させることができます。

禁止するコンピュータ接続を追加するには

- 1 [ネットワークとインターネット設定] パネルで [詳細設定] をクリックします。
- 2 [ファイアウォール] パネルで [信用 IP と禁止 IP] をクリックします。
- 3 [信用 IP と禁止 IP] パネルで [禁止 IP アドレス] をクリックします。
- 4 [追加] をクリックします。

- 5 [禁止 IP アドレスルールを追加] で、次のいずれかの操作を実行します。
 - [単一の IP アドレス] を選択し、IP アドレスを入力します。
 - [IP アドレスの範囲] を選択し、[開始 IP アドレス] ボックスおよび [終了 IP アドレス] フィールドに開始 IP アドレスおよび終了 IP アドレスを入力します。
- 6 [ルールの有効期限] にチェックマークを入れ、ルールを施行する日数を入力します（オプション）。
- 7 ルールの説明を入力します（オプション）。
- 8 [OK] をクリックします。
- 9 [禁止 IP アドレスルールを追加] ダイアログで [はい] をクリックし、禁止するコンピュータ接続を追加します。
新しく追加した IP アドレスが [禁止 IP アドレス] に表示されます。

禁止するコンピュータ接続を編集

ファイアウォールを使用して、禁止するコンピュータ接続と関連する IP アドレスを編集できます。

未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

ファイアウォールは不要なトラフィックをすべてブロックするため、通常は、IP アドレスを禁止する必要はありません。あるインターネット接続によって危険にさらされることがわかっている場合を除き、IP アドレスは禁止しないでください。DNS サーバ、DHCP サーバ、または ISP のその他のサーバなどの重要な IP アドレスをブロックしないように特に注意してください。セキュリティの設定によっては、禁止されたコンピュータからのイベントをファイアウォールが検出した際に、アラートを表示させることができます。

禁止されているコンピュータ接続を編集するには

- 1 [ネットワークとインターネット設定] パネルで [詳細設定] をクリックします。
- 2 [ファイアウォール] パネルで [信用 IP と禁止 IP] をクリックします。
- 3 [信用 IP と禁止 IP] パネルで [禁止 IP アドレス] をクリックします。
- 4 IP アドレスを選択し、[編集] をクリックします。

5 **【信用 IP アドレスルールを追加】** で、次のいずれかの操作を実行します。

- **【単一の IP アドレス】** を選択し、IP アドレスを入力します。
- **【IP アドレスの範囲】** を選択し、**【開始 IP アドレス】** ボックスおよび **【終了 IP アドレス】** フィールドに開始 IP アドレスおよび終了 IP アドレスを入力します。

6 **【ルールの有効期限】** にチェックマークを入れ、ルールを施行する日数を入力します（オプション）。

7 ルールの説明を入力します（オプション）。

【OK】 をクリックします。変更した IP アドレスが **【禁止 IP アドレス】** に表示されます。

禁止するコンピュータ接続を削除

ファイアウォールを使用して、禁止するコンピュータ接続と関連する IP アドレスを削除できます。

未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

ファイアウォールは不要なトラフィックをすべてブロックするため、通常は、IP アドレスを禁止する必要はありません。あるインターネット接続によって危険にさらされることがわかっている場合を除き、IP アドレスは禁止しないでください。DNS サーバ、DHCP サーバ、または ISP のその他のサーバなどの重要な IP アドレスをブロックしないように特に注意してください。セキュリティの設定によっては、禁止されたコンピュータからのイベントをファイアウォールが検出した際に、アラートを表示させることができます。

禁止されているコンピュータ接続を削除するには

- 1 **【ネットワークとインターネット設定】** パネルで **【詳細設定】** をクリックします。
- 2 **【ファイアウォール】** パネルで **【信用 IP と禁止 IP】** をクリックします。
- 3 **【信用 IP と禁止 IP】** パネルで **【禁止 IP アドレス】** をクリックします。
- 4 IP アドレスを選択し、**【削除】** をクリックします。
- 5 **【信用 IP と禁止 IP】** ダイアログで **【はい】** をクリックし、**【禁止 IP アドレス】** から IP アドレスを削除します。

受信イベントログからコンピュータを禁止

受信イベントログから、コンピュータ接続とそのコンピュータに関連する IP アドレスを禁止できます。

受信イベントログに表示される IP アドレスがブロックされます。したがって、コンピュータで意図的に開かれたポートが使用されている場合やインターネットアクセスを許可されたプログラムがある場合以外には、アドレスを禁止しても保護は強化されません。

意図的に開かれたポートがあり、これらのポートに対する特定のアドレス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 IP アドレス**リストにその IP アドレスを追加します。

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] パネルを使用して、不審または不要なインターネットアクティビティを行っている IP アドレスからの接続を禁止することができます。

受信イベントログから信用するコンピュータ接続を禁止するには

- 1 [詳細メニュー] が有効になっていることを確認してください。[よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク] をクリックし、[受信イベント] をクリックします。
- 4 [受信イベント] パネルで送信元 IP アドレスを選択し、[このアドレスを禁止] をクリックします。
- 5 [禁止 IP アドレスルールを追加] ダイアログで [はい] をクリックし、IP アドレスを禁止します。

新しく追加した IP アドレスが [禁止 IP アドレス] に表示されます。

関連項目

- イベントログを記録 (162 ページ)

侵入検知イベントログからコンピュータを禁止

侵入検知イベントログから、コンピュータ接続とそのコンピュータに関連する IP アドレスを禁止できます。

未知の IP、不審な IP、信用されていない IP のコンピュータからの接続を禁止することができます。

ファイアウォールは不要なトラフィックをすべてブロックするため、通常は、IP アドレスを禁止する必要はありません。あるインターネット接続によって危険にさらされることがわかっている場合を除き、IP アドレスは禁止しないでください。DNS サーバ、DHCP サーバ、または ISP のその他のサーバなどの重要な IP アドレスをブロックしないように特に注意してください。セキュリティの設定によっては、禁止されたコンピュータからのイベントをファイアウォールが検出した際に、アラートを表示させることができます。

侵入検知イベントログからコンピュータ接続を禁止するには

- 1 [よく使う機能] パネルで **[レポートとログ]** をクリックします。
- 2 **[最近のイベント]** で **[ログを表示]** をクリックします。
- 3 **[インターネットとネットワーク]** をクリックし、**[侵入検知イベント]** をクリックします。
- 4 **[侵入検知イベント]** パネルで送信元 IP アドレスを選択し、**[このアドレスを禁止]** をクリックします。
- 5 **[禁止 IP アドレスルールを追加]** ダイアログで **[はい]** をクリックし、IP アドレスを禁止します。

新しく追加した IP アドレスが **[禁止 IP アドレス]** に表示されます。

関連項目

- **イベントログを記録** (162 ページ)

第 23 章

ログ記録、監視、分析

ファイアウォールには、インターネットイベントとトラフィックに対して、見やすいログ記録、監視機能、分析機能があります。インターネットトラフィックとイベントを理解すると、インターネット接続を管理しやすくなります。

この章の内容

イベントログを記録.....	162
統計を使用	165
インターネットトラフィックを追跡.....	166
インターネットトラフィックを監視.....	170

イベントログを記録

ファイアウォールでは、ログ記録を有効にするか無効にするかを指定できます。有効にした場合は、ログに記録するイベントタイプを指定できます。イベントログの記録では、最近の受信イベントおよび送信イベントを表示できます。侵入検知イベントを表示することもできます。

イベントログの設定

ファイアウォールのイベントとアクティビティを追跡するため、表示するイベントのタイプを指定および設定できます。

イベントログの記録を設定するには

- 1 [ネットワークとインターネット設定] パネルで **[詳細設定]** をクリックします。
- 2 [ファイアウォール] パネルで **[イベントログ設定]** をクリックします。
- 3 [イベントログ設定] パネルで、次のいずれかの操作を実行します。
 - **[イベントログを記録]** を選択してイベントログの記録を有効にします。
 - **[イベントをログ記録しない]** を選択してイベントログの記録を無効にします。
- 4 **[イベントログ設定]** で、ログ記録を行うイベントタイプを指定します。イベントタイプには次のものがあります。
 - ICMP ping
 - 禁止 IP アドレスからのトラフィック
 - システム サービス ポートのイベント
 - 不明なポートのイベント
 - 侵入検知システム (IDS) イベント
- 5 特定のポートのログ記録を行わないようにするには、**[次のポートのイベントをログ記録しない]** を選択し、カンマ区切りで単一のポート番号を続けて入力するか、ダッシュを使用してポート番号の範囲を入力します。たとえば、137-139, 445, 400-5000 のように入力します。
- 6 **[OK]** をクリックします。

最近のイベントを表示

ログ記録が有効な場合、最近のイベントを表示できます。[最近のイベント] パネルには、イベントの日付と説明が表示されます。[最近のイベント] パネルには、インターネットアクセスが明示的にブロックされたプログラムのアクティビティのみが表示されます。

ファイアウォールの最近のイベントを表示するには

- [詳細メニュー] の [よく使う機能] パネルで、[レポートとログ] または [最近のイベントの表示] をクリックします。または、標準メニューの [よく使う機能] パネルの [最近のイベントの表示] をクリックします。

受信イベントを表示

ログ記録が有効な場合、受信イベントを表示したり、並べかえることができます。

受信イベントログには、次のカテゴリが記録されます。

- 日時
- 送信元 IP アドレス
- ホスト名
- 情報とイベントタイプ

ファイアウォールの受信イベントを表示するには

- 1 [詳細メニュー] が有効になっていることを確認してください。[よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク] をクリックし、[受信イベント] をクリックします。

注: 受信イベントログから IP アドレスを信用、禁止、追跡できます。

関連項目

- 受信イベントログから信用するコンピュータを追加 (153 ページ)
- 受信イベントログからコンピュータを禁止 (159 ページ)
- 受信イベントログからコンピュータを追跡 (167 ページ)

送信イベントを表示

ログ記録が有効な場合、送信イベントを表示できます。送信イベントには、送信アクセスを行ったプログラム名、イベントの日時、コンピュータ上のプログラムの場所が含まれます。

ファイアウォールの送信イベントを表示するには

- 1 [よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク]、[送信イベント] の順に選択します。

注: 送信イベントログからすべてのアクセスまたは送信アクセスのみを許可できます。また、プログラムに関する詳細情報を検索することもできます。

関連項目

- [送信イベントログからすべてのアクセスを許可](#) (137 ページ)
- [送信イベントログから送信アクセスのみを許可](#) (140 ページ)
- [送信イベントログからプログラム情報を取得](#) (144 ページ)

侵入検知イベントを表示

ログ記録が有効な場合、受信イベントを表示できます。侵入検知イベントには、イベントの日時、送信元 IP、ホスト名が表示されます。ログにはイベントタイプの説明も表示されます。

侵入検知イベントを表示するには

- 1 [よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク] をクリックし、[侵入検知イベント] をクリックします。

注: 侵入検知イベントログから IP アドレスを禁止および追跡できます。

関連項目

- [侵入検知イベントログからコンピュータを禁止](#) (160 ページ)
- [侵入検知イベントログからコンピュータを追跡](#) (168 ページ)

統計を使用

ファイアウォールは、マカフィーのセキュリティサイトである HackerWatch を活用して、世界中のインターネットのセキュリティイベントやポートアクティビティに関する統計を表示します。

世界中のセキュリティイベントの統計を表示

HackerWatch は世界中のインターネットのセキュリティイベントを追跡します。これらのイベントは McAfee SecurityCenter から表示できます。追跡された情報には、過去 24 時間、過去 7 日間、過去 30 日間で HackerWatch に報告された事象が表示されます。

世界中のセキュリティ統計を表示するには

- 1 詳細メニューが有効であることを確認し、**[ツール]** をクリックします。
- 2 **[ツール]** パネルで **[HackerWatch]** をクリックします。
- 3 **[イベント追跡]** にセキュリティイベントの統計が表示されます。

世界中のインターネットのポートアクティビティを表示

HackerWatch は世界中のインターネットのセキュリティイベントを追跡します。これらのイベントは McAfee SecurityCenter から表示できます。表示される情報には、過去 7 日間に HackerWatch に報告された上位のポートが含まれます。通常は、HTTP、TCP、UDP ポートの情報が表示されます。

全世界のポートアクティビティを表示するには

- 1 詳細メニューが有効であることを確認し、**[ツール]** をクリックします。
- 2 **[ツール]** パネルで **[HackerWatch]** をクリックします。
- 3 **[最近行われたポート アクティビティ]** に上位イベントポートのイベントが表示されます。

インターネットトラフィックを追跡

ファイアウォールには、インターネットトラフィックの追跡に関するさまざまなオプションがあります。これらのオプションを使用すると、ネットワークコンピュータを地理的に追跡したり、ドメイン情報やネットワーク情報を取得したり、受信イベントログおよび侵入検知イベントログからコンピュータを追跡できます。

ネットワークコンピュータを地理的に追跡

ビジュアル追跡機能は、コンピュータ名または IP アドレスを使用して、ご使用のコンピュータに接続または接続を試行しているコンピュータの地理的な場所を特定します。また、ビジュアル追跡機能を使用してネットワークや登録情報にアクセスすることもできます。ビジュアル追跡機能を実行すると世界地図が表示され、送信元コンピュータとご使用のコンピュータ間でデータが送受信されるときに使用される可能性が最も高いルートが表示されます。

コンピュータの地理的な場所を特定するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [ビジュアル追跡機能] をクリックします。
- 3 コンピュータの IP アドレスを入力して、[追跡] をクリックします。
- 4 [ビジュアル追跡機能] で [地図表示] を選択します。

注: ループ IP アドレス、プライベート IP アドレス、無効な IP アドレスのイベントは追跡できません。

コンピュータの登録情報を取得

ビジュアル追跡機能を使用して、McAfee SecurityCenter からコンピュータの登録情報を取得できます。情報には、ドメイン名、登録者名および住所、管理者連絡先などが含まれます。

コンピュータのドメイン情報を取得するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [ビジュアル追跡機能] をクリックします。
- 3 コンピュータの IP アドレスを入力して、[追跡] をクリックします。
- 4 [ビジュアル追跡機能] で [登録者表示] を選択します。

コンピュータのネットワーク情報を取得

ビジュアル追跡機能を使用して、McAfee SecurityCenter からコンピュータのネットワーク情報を取得できます。ネットワーク情報には、ドメインが存在するネットワークの詳細が含まれます。

コンピュータのネットワーク情報を取得するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [ビジュアル追跡機能] をクリックします。
- 3 コンピュータの IP アドレスを入力して、[追跡] をクリックします。
- 4 [ビジュアル追跡機能] で [ネットワーク表示] を選択します。

受信イベントログからコンピュータを追跡

受信イベントログに表示される IP アドレスは [受信イベント] パネルから追跡できます。

受信イベントログからコンピュータの IP アドレスを追跡するには

- 1 [詳細メニュー] が有効になっていることを確認してください。[よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク] をクリックし、[受信イベント] をクリックします。
- 4 [受信イベント] パネルで送信元 IP アドレスを選択し、[このアドレスを追跡] をクリックします。
- 5 [ビジュアル追跡機能] パネルで、次のいずれかの操作を実行します。
 - **地図表示:** 選択された IP アドレスからコンピュータの地理的な場所を特定します。
 - **登録者表示:** 選択した IP アドレスを使用してドメイン情報を特定します。
 - **ネットワーク表示:** 選択した IP アドレスを使用してネットワーク情報を特定します。
- 6 [終了] をクリックします。

関連項目

- インターネットトラフィックを追跡 (166 ページ)
- 受信イベントを表示 (163 ページ)

侵入検知イベントログからコンピュータを追跡

侵入検知イベントログに表示される IP アドレスは [侵入検知イベント] パネルから追跡できます。

侵入検知イベントログからコンピュータの IP アドレスを追跡するには

- 1 [よく使う機能] パネルで [レポートとログ] をクリックします。
- 2 [最近のイベント] で [ログを表示] をクリックします。
- 3 [インターネットとネットワーク] をクリックし、[侵入検知イベント] をクリックします。[侵入検知イベント] パネルで送信元 IP アドレスを選択し、[このアドレスを追跡] をクリックします。
- 4 [ビジュアル追跡機能] パネルで、次のいずれかの操作を実行します。
 - **地図表示:** 選択された IP アドレスからコンピュータの地理的な場所を特定します。
 - **登録者表示:** 選択した IP アドレスを使用してドメイン情報を特定します。
 - **ネットワーク表示:** 選択した IP アドレスを使用してネットワーク情報を特定します。
- 5 [終了] をクリックします。

関連項目

- [インターネットトラフィックを追跡](#) (166 ページ)
- [ログ記録、監視、分析](#) (161 ページ)

監視対象の IP アドレスを追跡

監視対象の IP アドレスを追跡して地理的な場所を特定できます。地図には、送信元コンピュータからご使用のコンピュータにデータが送信されるときに、使用される可能性が最も高いルートが表示されます。また、IP アドレスの登録情報とネットワーク情報も取得できます。

プログラムの帯域幅使用率を監視するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [トラフィックの監視] をクリックします。
- 3 [トラフィックの監視] で [アクティブなプログラム] をクリックします。
- 4 プログラムを選択し、プログラム名の下に表示される IP アドレスを選択します。

- 5 [プログラムアクティビティ] で [この IP を追跡] をクリックします。
- 6 [ビジュアル追跡機能] に、発信元コンピュータからご使用のコンピュータにデータが送信されるときに使用される可能性が最も高いルートが表示されます。また、IP アドレスの登録情報とネットワーク情報も取得できます。

注: 最新の統計を表示するには、[ビジュアル追跡機能] で [更新] をクリックします。

関連項目

- [インターネットトラフィックを監視](#) (170 ページ)

インターネットトラフィックを監視

ファイアウォールには、インターネットトラフィックを監視するための次のような方法があります。

- **トラフィックの分析グラフ:** 受信、送信にかかわらず最近のすべてのインターネットトラフィックが表示されます。
- **トラフィックの使用状況グラフ:** 過去 24 時間で最もアクティブなプログラムにより使用された帯域幅の使用率が表示されます。
- **アクティブなプログラム:** 現在ネットワーク接続を頻繁に行っているプログラムと、そのプログラムがアクセスしている IP アドレスが表示されます。

トラフィックの分析グラフについて

[トラフィック分析] グラフには、受信トラフィックと送信トラフィックが数値とグラフで表示されます。また、トラフィック監視機能を使用すると、現在ネットワーク接続を頻繁に行っているアプリケーションと、そのアプリケーションがアクセスしている IP アドレスを確認することができます。

[トラフィックの分析] パネルから、最近のすべてのインターネットトラフィック、現在の転送速度、平均転送速度、最大転送速度を表示できます。また、ファイアウォールを起動してからのトラフィック量や、現在または前の月のトラフィックの合計など、トラフィック量を表示することもできます。

[トラフィックの分析] パネルにはコンピュータのインターネットアクティビティがリアルタイムで表示され、最近の受信/送信インターネットトラフィックの量と割合、接続の速度、インターネットに転送された合計バイト数が表示されます。

緑色の実線は、受信トラフィックの現在の転送速度を表します。緑色の点線は、受信トラフィックの平均転送速度を表します。現在の転送速度と平均転送速度が同じである場合、点線はグラフに表示されません。実線が現在の転送速度と平均転送速度の両方を示します。

赤い実線は、送信トラフィックの現在の転送速度を表します。赤い点線は、送信トラフィックの平均転送速度を表します。現在の転送速度と平均転送速度が同じである場合、点線はグラフに表示されません。実線が現在の転送速度と平均転送速度の両方を示します。

関連項目

- [受信トラフィックと送信トラフィックを分析](#) (171 ページ)

受信トラフィックと送信トラフィックを分析

[トラフィック分析] グラフには、受信トラフィックと送信トラフィックが数値とグラフで表示されます。また、トラフィック監視機能を使用すると、現在ネットワーク接続を頻繁に行っているアプリケーションと、そのアプリケーションがアクセスしている IP アドレスを確認することができます。

受信トラフィックと送信トラフィックを分析するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [トラフィックの監視] をクリックします。
- 3 [トラフィックの監視] で [トラフィックの分析] をクリックします。

ヒント: 最新の統計を表示するには、[トラフィックの分析] で [更新] をクリックします。

関連項目

- [トラフィックの分析グラフについて](#) (170 ページ)

プログラムの帯域幅を監視

円グラフを表示して、過去 24 時間で最もアクティブなプログラムにより使用された帯域幅のおよその使用率を確認できます。円グラフには、プログラムによる帯域幅の相対使用量が視覚的に表示されます。

プログラムの帯域幅使用率を監視するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [トラフィックの監視] をクリックします。
- 3 [トラフィックの監視] で [トラフィックの使用状況] をクリックします。

ヒント: 最新の統計を表示するには、[トラフィックの使用状況] で [更新] をクリックします。

プログラムアクティビティを監視

内向きおよび外向きのプログラムアクティビティを表示できます。リモートコンピュータの接続とポートが表示されます。

プログラムの帯域幅使用率を監視するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [トラフィックの監視] をクリックします。
- 3 [トラフィックの監視] で [アクティブなプログラム] をクリックします。

4 次の情報を表示できます。

- プログラム アクティビティ グラフ: アクティビティのグラフを表示するプログラムを選択します。
- 受信中の接続: プログラム名の下から受信中の項目を選択します。
- コンピュータ接続: プログラム名、システムプロセス、サービスの下から IP アドレスを選択します。

注: 最新の統計を表示するには、[アクティブなプログラム] で [更新] をクリックします。

第 24 章

インターネットセキュリティについての確認

ファイアウォールは、マカフィーのセキュリティサイトである HackerWatch を活用して、プログラムと世界中のインターネットアクティビティに関する最新の情報を提供します。HackerWatch には、ファイアウォールに関する HTML チュートリアルも提供されます。

この章の内容

HackerWatch チュートリアルを起動.....174

HackerWatch チュートリアルを起動

McAfee SecurityCenter から HackerWatch にアクセスし、ファイアウォールについて学ぶことができます。

HackerWatch のチュートリアルを起動するには

- 1 詳細メニューが有効であることを確認し、[ツール] をクリックします。
- 2 [ツール] パネルで [HackerWatch] をクリックします。
- 3 [HackerWatch のリソース] で [チュートリアルを表示] をクリックします。

第 25 章

McAfee SpamKiller

McAfee SpamKiller は、迷惑メールおよびフィッシング詐欺メールをフィルタリングします。次の機能が搭載されています。

多彩なユーザ設定

- 複数の E メールアカウントのフィルタリング
- 友人リストへの連絡先のインポート
- カスタムフィルタの作成、およびマカフィーへの迷惑メールの報告（分析用）
- 迷惑メールまたは非迷惑メールとしてマークするオプション
- マルチユーザサポート（Windows XP および Vista）

フィルタリング

- フィルタの自動更新
- E メールメッセージのカスタムフィルタの作成
- 多層的なフィルタリングエンジン
- フィッシング詐欺フィルタ

この章の内容

機能.....	176
Web メールアカウントを管理	179
友人を管理	187
フィルタリングオプションを変更	193
パーソナルフィルタを管理	199
McAfee SpamKiller を保守	207
フィッシング詐欺対策の設定.....	211
その他の情報	215

機能

このバージョンの McAfee SpamKiller には、次の機能が搭載されています。

フィルタリング

的確な判定を行う高度なフィルタリング技術によりメール環境が向上します。

フィッシング詐欺

フィッシング詐欺の可能性のある Web サイトを識別し、ブロックすることができます。

インストール

セットアップと設定を簡単に行うことができます。

直感的な操作方法

直感的で使いやすい操作環境を提供します。

テクニカルサポート

E メール、チャット、電話でテクニカルサポートを行っています。

迷惑メールの処理

迷惑メールの処理に関するオプションの設定ができます。これにより、誤ってフィルタリングされた可能性のあるメッセージも表示できます。

サポートしている E メールプログラム

- すべての POP3 E メールプログラム。
- MAPI は Outlook 2000 以降をサポートしています。
- POP3 を使用する Web メールまたは MSN/Hotmail (有料版のみ) をサポートしています。

ツールバープラグインがサポートする E メールプログラム

- Outlook Express 6.0 以降
- Outlook 2000、XP、2003、または 2007
- Eudora 6.0 以降
- Thunderbird 1.5 以降

フィッシング詐欺対策がサポートするブラウザ

すべての HTTP 互換 Web ブラウザ（主に次のもの）

- Internet Explorer
- Firefox
- Netscape

第 26 章

Web メールアカウントを管理

迷惑メールのフィルタリング対象として Web メールアカウントを追加したり、Web メールアカウント情報を編集したり、フィルタリングが不要となった Web メールアカウントを削除できます。

Web メールフィルタも管理できます。たとえば、Web メールアカウントの E メールフィルタリングを無効/有効にしたり、フィルタリングされたメッセージを管理したり、ログを表示できます。

この章の内容

Web メールアカウントを追加	180
Web メールアカウントを変更	182
Web メールアカウントを削除	184
Web メールフィルタリングを管理	185

Web メールアカウントを追加

迷惑メールのフィルタリング対象として Web メールアカウントを追加します。

- POP3 Web メール (Yahoo! など)
- MSN/Hotmail (完全にサポートされるのは有料バージョンのみ)

POP3 または MSN/Hotmail Web メールアカウントを追加

迷惑メールのフィルタリング対象として Web メールアカウントを追加します。

POP3 または MSN/Hotmail Web メールアカウントを追加するには

- 1 詳細メニューで **設定** をクリックします。
- 2 **設定** パネルで **E メールとメッセージ** をクリックします。
- 3 **迷惑メール対策** で **詳細設定** をクリックします。
- 4 **迷惑メール対策** パネルで **Web メールアカウント** をクリックします。
- 5 **Web メールアカウント** パネルで **追加** をクリックします。
- 6 次のボックスで Web メールアカウントの情報を指定します。
 - **説明:** アカウントの説明です。このフィールドには任意の情報を入力できます。
 - **E メールアドレス:** アカウントの E メールアドレスを指定します。
 - **アカウントタイプ:** E メールアカウントの種類を指定します。
 - **サーバ:** アカウントのサーバの名前を入力します。
 - **ユーザ名:** アカウントのユーザの名前を入力します。
 - **パスワード:** アカウントへのアクセスに使用するパスワードを指定します。
 - **パスワードの確認:** パスワードをもう一度入力します。
- 7 **次へ** をクリックします。

8 **【確認オプション】** で、次のいずれかの操作を実行してこのアカウントの迷惑メールを確認する時間を決定します。

- **【確認頻度】** ボックスに値を入力します。

McAfee SpamKiller は、指定した間隔（分単位）でこのアカウントの迷惑メールを確認します。「0」を入力すると、インターネットに接続した場合にのみ確認が行われます。

- **【スタートアップで確認】** チェックボックスをオンにします。

McAfee SpamKiller は、コンピュータの再起動時に毎回アカウントを確認します。インターネットへの常時接続を使用している場合に、このオプションを使用します。

9 ダイヤルアップ接続を使用している場合は、**【接続オプション】** で次のいずれかの操作を実行して McAfee SpamKiller によるインターネットへの接続方法を決定します。

- **【ダイヤルアップ接続しない】** をクリックします。

McAfee SpamKiller は自動的にインターネットにダイヤルしません。ダイヤルアップ接続を手動で行う必要があります。

- **【接続を利用できないときにダイヤルアップ接続する】** をクリックします。

インターネット接続が無効になっている場合は、McAfee SpamKiller は指定のダイヤルアップ接続に接続します。

- **【指定された接続先に常にダイヤルアップ接続する】** をクリックします。

McAfee SpamKiller は、指定のダイヤルアップ接続に接続します。

- **【この接続先にダイヤルアップ接続する】** リストの登録項目をクリックします。

McAfee SpamKiller は、ここで指定した接続先にダイヤルアップ接続します。

- **【フィルタリングが完了したあとも接続を維持する】** チェックボックスをオンにします。

フィルタリングが完了したあともインターネット接続は維持されます。

10 **【完了】** をクリックします。

Web メールアカウントを変更

Web メールアカウントを有効/無効にしたり、情報を編集できます。たとえば、E メールアドレス、アカウントの説明、アカウントタイプ、パスワード、McAfee SpamKiller によりアカウントの迷惑メールを確認する頻度、インターネットへの接続方法などを変更することができます。

POP3 または MSN/Hotmail Web メールアカウントを編集

Web メールアカウントを有効/無効にしたり、情報を編集できます。たとえば、E メールアドレス、アカウントの説明、サーバの情報、McAfee SpamKiller によりアカウントの迷惑メールを確認する頻度、インターネットへの接続方法などを変更することができます。

POP3 または MSN/Hotmail Web メールアカウントを変更するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【Web メールアカウント】** をクリックします。
- 5 変更するアカウントを選択し、**【編集】** をクリックします。
- 6 次のボックスでアカウントの情報を編集します。
 - **説明:** アカウントの説明です。このフィールドには任意の情報を入力できます。
 - **E メールアドレス:** アカウントの E メールアドレスを指定します。
 - **アカウントタイプ:** E メールアカウントの種類を指定します。
 - **サーバ:** アカウントのサーバの名前を入力します。
 - **ユーザ名:** アカウントのユーザの名前を入力します。
 - **パスワード:** アカウントへのアクセスに使用するパスワードを指定します。
 - **パスワードの確認:** パスワードをもう一度入力します。
- 7 **【次へ】** をクリックします。

8 **【確認オプション】** で、次のいずれかの操作を実行してこのアカウントの迷惑メールを確認する時間を決定します。

- **【確認頻度】** ボックスに値を入力します。

McAfee SpamKiller は、指定した間隔（分単位）でこのアカウントの迷惑メールを確認します。「0」を入力すると、インターネットに接続した場合にのみ確認が行われます。

- **【スタートアップで確認】** チェックボックスをオンにします。

McAfee SpamKiller は、コンピュータの再起動時に毎回アカウントを確認します。インターネットへの常時接続を使用している場合に、このオプションを使用します。

9 ダイヤルアップ接続を使用している場合は、**【接続オプション】** で次のいずれかの操作を実行して McAfee SpamKiller によるインターネットへの接続方法を決定します。

- **【ダイヤルアップ接続しない】** をクリックします。

McAfee SpamKiller は自動的にインターネットにダイヤルしません。ダイヤルアップ接続を手動で行う必要があります。

- **【接続を利用できないときにダイヤルアップ接続する】** をクリックします。

インターネット接続が無効になっている場合は、McAfee SpamKiller は指定のダイヤルアップ接続に接続します。

- **【指定された接続先に常にダイヤルアップ接続する】** をクリックします。

McAfee SpamKiller は、指定のダイヤルアップ接続に接続します。

- **【この接続先にダイヤルアップ接続する】** リストの登録項目をクリックします。

McAfee SpamKiller は、ここで指定した接続先にダイヤルアップ接続します。

- **【フィルタリングが完了したあとも接続を維持する】** チェックボックスをオンにします。

フィルタリングが完了したあともインターネット接続は維持されます。

10 **【完了】** をクリックします。

Web メールアカウントを削除

フィルタが不要となった Web メールアカウントを削除できます。

Web メールアカウントを削除

E メールアカウントをフィルタリングする必要がない場合は、その E メールアカウントを削除します。

Web メールアカウントを削除するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【Web メールアカウント】** をクリックします。
- 5 削除するアカウントを選択し、**【削除】** をクリックします。

Web メールフィルタリングを管理

Web メールアカウントの E メールメッセージのフィルタリングを無効/有効にしたり、フィルタリングされたメッセージを管理したり、ログを表示できます。

Web メールフィルタリングを無効化

Web メールフィルタリングを無効にして、Eメールのフィルタリングを一時停止できます。

Web メールフィルタリングを無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【Web メールアカウント】** をクリックします。
- 5 無効にするアカウントの横にあるチェックボックスをオフにします。
- 6 **【OK】** をクリックします。

Web メールフィルタリングを有効化

Web メールアカウントを無効にした場合、再び有効にできます。

Web メールフィルタリングを有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【Web メールアカウント】** をクリックします。
- 5 有効にするアカウントの横にあるチェックボックスをオンにします。
- 6 **【OK】** をクリックします。

Web メールアカウントのフィルタリングされたメッセージを管理

Web メールアカウントのフィルタリングされたメッセージを表示、コピー、または削除できます。

Web メールアカウントのフィルタリングされたメッセージを表示、コピー、削除するには

- 1 詳細メニューで **[レポートとログ]** をクリックします。
- 2 **[レポートとログ]** パネルで **[フィルタリングされた Web メール]** をクリックします。
- 3 **[フィルタリングされた Web メール]** パネルで、表示、コピー、または削除するメッセージを選択します。
- 4 **[オプションの選択]** で次の操作のいずれかを実行します。
 - メッセージをクリップボードにコピーする場合は、**[コピー]** をクリックします。
 - メッセージを削除する場合は、**[削除]** をクリックします。

フィルタリングされた Web メールログを表示

フィルタリングされた Web メールログを表示できます。たとえば、E メールがフィルタリングされたタイミング、フィルタリングされた E メールを受信したアカウントなどを表示できます。

フィルタリングされた Web メールログを表示するには

- 1 詳細メニューで **[レポートとログ]** をクリックします。
- 2 **[レポートとログ]** パネルで **[最近のイベント]** をクリックします。
- 3 **[最近のイベント]** パネルで **[ログを表示]** をクリックします。
- 4 左パネルで **[E メールとメッセージ]** リストを展開してから、**[Web メールフィルタリングイベント]** をクリックします。
- 5 表示するログを選択します。
- 6 **[詳細]** で、そのログについての情報を表示します。

第 27 章

友人を管理

友人からのメッセージをすべて確実に受信するには、その友人のアドレスを友人リストに追加します。ドメインを追加したり、友人の編集または削除を実行したり、友人リストの自動更新のスケジュール設定を行うこともできます。

この章の内容

友人リストの管理方法について	188
友人リストを自動更新	190

友人リストの管理方法について

このセクションでは、友人リストの管理方法について説明します。

McAfee SpamKiller ツールバーから友人を手動で追加

友人からのメッセージをすべて確実に受信するには、その友人のアドレスを友人リストに追加します。

Outlook、Outlook Express、Windows Mail、Eudora または Thunderbird を使用している場合、McAfee SpamKiller ツールバーから友人を追加できます。

Outlook から友人を追加するには

- Outlook で、メッセージを選択してから **[友人を追加]** をクリックします。

Outlook Express、Windows Mail、Eudora または Thunderbird から友人を追加するには

- それぞれの閲覧画面で、メッセージを選択します。**[SpamKiller]** メニューで **[友人を追加]** をクリックします。

友人を手動で追加

友人からのメッセージをすべて確実に受信するには、その友人のアドレスを友人リストに追加します。ドメインを追加することもできます。

友人を手動で追加するには

- 1 詳細メニューで **[設定]** をクリックします。
- 2 **[設定]** パネルで **[E メールとメッセージャー]** をクリックします。
- 3 **[迷惑メール対策]** で **[詳細設定]** をクリックします。
- 4 **[迷惑メール対策]** パネルで **[友人]** をクリックします。
- 5 **[友人]** パネルで **[追加]** をクリックします。
- 6 次のボックスに友人の情報を入力します。
 - **名前:** 友人の名前を指定します。
 - **種類:** 1 つの E メールアドレスまたはドメイン全体のどちらで指定するかを指定します。
 - **E メールアドレス:** 友人の E メールアドレス、またはフィルタリングを実行しないドメインを指定します。
- 7 **[OK]** をクリックします。

友人を編集

友人の情報に変更があった場合（たとえば、E メールアドレスの変更など）、リストを更新することにより、その友人からのメッセージをすべて確実に受信できます。

友人を編集するには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔E メールとメッセージャー〕** をクリックします。
- 3 **〔迷惑メール対策〕** で **〔詳細設定〕** をクリックします。
- 4 **〔迷惑メール対策〕** パネルで **〔友人〕** をクリックします。
- 5 編集する友人を選択し、**〔編集〕** をクリックします。
- 6 次のボックスで友人の情報を編集します。
 - **名前:** 友人の名前を指定します。
 - **種類:** 1 つの E メールアドレスまたはドメイン全体のどちらで編集するかを指定します。
 - **E メールアドレス:** 友人の E メールアドレス、またはフィルタリングを実行しないドメインを指定します。
- 7 **〔OK〕** をクリックします。

友人を削除

友人をリストから削除し、フィルタリングが実行されるようにできます。

友人を削除するには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔E メールとメッセージャー〕** をクリックします。
- 3 **〔迷惑メール対策〕** で **〔詳細設定〕** をクリックします。
- 4 **〔迷惑メール対策〕** パネルで **〔友人〕** をクリックします。
- 5 削除する友人を選択し、**〔削除〕** をクリックします。

友人リストを自動更新

友人からのメッセージをすべて確実に受信するために、アドレス帳からアドレスを手動でインポートしたり、自動更新のスケジュール設定を行います。

アドレス帳から手動でインポート

アドレス帳からアドレスをインポートし、友人リストを更新できます。

アドレス帳から手動でインポートするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【アドレス帳】** をクリックします。
- 5 インポートするアドレス帳を選択してから、**【今すぐ実行】** をクリックします。
- 6 **【OK】** をクリックします。

アドレス帳を追加

友人からのメッセージをすべて確実に受信するために、アドレス帳がインポート対象に含まれるようにします。

アドレス帳を追加するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【アドレス帳】** をクリックします。
- 5 **【アドレス帳】** パネルで **【追加】** をクリックします。
- 6 **【種類】** リストで、インポートするアドレス帳の種類をクリックします。
- 7 必要に応じて、**【場所】** リストでインポートするアドレス帳の対象ファイルを選択します。
- 8 **【スケジュール】** リストの **【毎日】**、**【毎週】**、または **【毎月】** をクリックし、アドレス帳に新しいアドレスがあるかどうかを McAfee SpamKiller が確認する間隔を決定します。
- 9 **【OK】** をクリックします。

アドレス帳を編集

スケジュール設定された間隔でアドレス帳からアドレスをインポートし、友人リストを更新できます。アドレス帳を編集したり、インポートのスケジュールを変更することもできます。

アドレス帳を編集するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【アドレス帳】** をクリックします。
- 5 編集するアドレス帳を選択し、**【編集】** をクリックします。
- 6 次の操作のいずれかを実行します。
 - **【種類】** リストで、インポートするアドレス帳の種類をクリックします。
 - 必要に応じて、**【場所】** リストでインポートするアドレス帳の対象ファイルを選択します。
 - **【スケジュール】** リストの **【毎日】**、**【毎週】**、または **【毎月】** をクリックし、アドレス帳に新しいアドレスがあるかどうかを McAfee SpamKiller が確認する間隔を決定します。
- 7 **【OK】** をクリックします。

アドレス帳を削除

McAfee SpamKiller によってアドレス帳からアドレスを自動的にインポートしないようにするには、そのアドレス帳を削除します。

自動インポートからアドレス帳を削除するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【アドレス帳】** をクリックします。
- 5 削除するアドレス帳を選択し、**【削除】** をクリックします。

第 28 章

フィルタリングオプションを変更

フィルタリングオプションには、フィルタリングレベルの変更、特別フィルタの変更、メッセージの処理方法のカスタマイズ、フィルタリングする文字セットの指定、マカフィーへの迷惑メールの報告などが含まれます。

この章の内容

E メールメッセージのフィルタリングを変更	194
メッセージの処理方法を変更	196
文字セットによりメッセージをフィルタリング	197
迷惑メールを報告	198

E メールメッセージのフィルタリングを変更

メッセージをどの程度厳しくフィルタリングするかを変更できます。受信すべきメッセージが迷惑メールと判別されている場合、フィルタリングレベルを下げることができます。

特別フィルタを有効/無効にすることもできます。たとえば、標準設定では、大部分が画像であるメッセージはフィルタリングされます。これらのメッセージを受信する場合は、このフィルタを無効にします。

E メールフィルタリングレベルを変更

メッセージをどの程度厳しくフィルタリングするかを変更できます。たとえば、受信すべきメッセージが迷惑メールと判別されている場合、フィルタリングレベルを下げることができます。

E メールフィルタリングレベルを変更するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージング】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【フィルタリングオプション】** をクリックします。
- 5 **【フィルタリングオプション】** で、次の設定のいずれかにスライダを移動します。
 - **低:** ほとんどの E メールが許可されます。
 - **中-低:** 明らかに迷惑メールであるメッセージのみがフィルタリングされます。
 - **中:** 多くの E メールが許可されます。
 - **中-高:** 迷惑メールに似ている E メールはすべてフィルタリングされます。
 - **高:** 友人リストにある送信者からのメッセージのみが許可されます。
- 6 **【OK】** をクリックします。

特別フィルタを変更

特別フィルタを有効/無効にすることができます。たとえば、標準設定では、大部分が画像であるメッセージはフィルタリングされます。これらのメッセージを受信する場合は、このフィルタを無効にします。

特別フィルタを変更するには

- 1 詳細メニューで **[設定]** をクリックします。
- 2 **[設定]** パネルで **[E メールとメッセージ]** をクリックします。
- 3 **[迷惑メール対策]** で **[詳細設定]** をクリックします。
- 4 **[フィルタリングオプション]** を選択します。
- 5 **[特別フィルタ]** で、次のチェックボックスをオン/オフにします。
 - **隠しテキストを含むメッセージをフィルタリングします:** 迷惑メールのフィルタリングを回避するために隠しテキストが使用される場合があります。
 - **テキストに対して特定の比率の画像を含むメッセージをフィルタリングします:** 通常、大部分が画像であるメッセージは迷惑メールです。
 - **意図的な HTML フォーマットエラーを含むメッセージをフィルタリングします:** 迷惑メールのフィルタリングを回避するための無効なフォーマットが使用される場合があります。
 - **次のサイズを超えるメッセージはフィルタしない:** 指定されたサイズより大きいメッセージはフィルタリングされません。メッセージサイズの値は変更できます (有効な範囲は 0 ~ 250 KB)。
- 6 **[OK]** をクリックします。

メッセージの処理方法を変更

迷惑メールにタグを追加したりそのメッセージを処理する方法は、変更できます。たとえば、迷惑メールまたはフィッシング詐欺メールに追加するタグを変更したり、メッセージを SpamKiller フォルダまたは受信ボックスのどちらに保存するかを変更できます。

メッセージの処理方法を変更

迷惑メールにタグを追加したりそのメッセージを処理する方法は、変更できます。たとえば、迷惑メールまたはフィッシング詐欺メールに追加するタグを変更したり、メッセージを SpamKiller フォルダまたは受信ボックスのどちらに保存するかを変更できます。

McAfee SpamKiller による迷惑メールメッセージの処理方法を変更するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセンジャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【処理中】** をクリックします。
- 5 次のいずれかの操作を実行します。
 - **【迷惑メールとしてマークして SpamKiller フォルダに移動】** をクリックします。
これは標準設定です。迷惑メールメッセージは SpamKiller フォルダに移動されます。
 - **【迷惑メールとしてマークして受信ボックスに残す】** をクリックします。
迷惑メールメッセージは受信ボックスに保存されます。
 - **【迷惑メールの件名にカスタマイズ可能な次のタグを追加】** ボックスにカスタムタグを入力します。
指定したタグが迷惑メールメッセージの件名に追加されます。
 - **【フィッシング詐欺メールの件名にカスタマイズ可能な次のタグを追加】** ボックスにカスタムタグを入力します。
指定したタグがフィッシング詐欺メッセージの件名に追加されます。
- 6 **【OK】** をクリックします。

文字セットによりメッセージをフィルタリング

文字セットは、アルファベット、数値、その他の記号など、言語を表す場合に使用されます。特定の文字セットを含むメッセージをフィルタリングできます。ただし、正当なメールを受信する言語に対する文字セットはフィルタリングしないでください。

たとえば、英語で正当な E メールを受信するものの、イタリア語のメッセージをフィルタリングしたい場合、[西ヨーロッパ系言語] は選択しないでください。[西ヨーロッパ系言語] を選択すると、イタリア語のメッセージだけでなく、英語や西ヨーロッパ系言語の文字セットを持つその他の言語もフィルタリングされます。

文字セットによりメッセージをフィルタリング

特定の文字セットを含むメッセージをフィルタリングできます。ただし、受信する正当なメールの言語に対する文字セットはフィルタリングしないでください。

文字セットによりメッセージをフィルタリングするには

- 1 詳細メニューで **[設定]** をクリックします。
- 2 [設定] パネルで **[E メールとメッセージャー]** をクリックします。
- 3 **[迷惑メール対策]** で **[詳細設定]** をクリックします。
- 4 [迷惑メール対策] パネルで **[文字セット]** をクリックします。
- 5 フィルタリングする文字セットの横のチェックボックスをオンにします。
- 6 **[OK]** をクリックします。

迷惑メールを報告

マカフィーに迷惑メールを報告できます。報告された迷惑メールはマカフィーによって分析され、フィルタの更新のために活用されます。

迷惑メールを報告

マカフィーに迷惑メールを報告できます。報告された迷惑メールはマカフィーによって分析され、フィルタの更新のために活用されます。

マカフィーに迷惑メールを報告するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【マカフィーに報告】** をクリックします。
- 5 以下のチェックボックスのうち、いずれかを選択します。
 - **【迷惑メールとしてマーク】** をクリックしたときのレポート機能を有効化: 迷惑メールとしてマークするたびに、マカフィーにメッセージを報告します。
 - **【非迷惑メールとしてマーク】** をクリックしたときのレポート機能を有効化: 非迷惑メールとしてマークするたびに、マカフィーにメッセージを報告します。
 - **(ヘッダだけでなく) メッセージ全体を送信:** マカフィーにメッセージを報告する場合、(ヘッダだけでなく) メッセージ全体を送信します。
- 6 **【OK】** をクリックします。

第 29 章

パーソナルフィルタを管理

フィルタによって、McAfee SpamKiller が確認する E メールの内容が指定されます。

McAfee SpamKiller では多くのフィルタが使用されますが、新しいフィルタを作成するか、既存のフィルタを編集することによって、迷惑メールとして識別するメッセージの詳細を設定できます。たとえば、フィルタの表現に「住宅ローン」が含まれる場合、McAfee SpamKiller は「住宅ローン」という単語を含むメッセージを検索します。

フィルタを追加する際は、注意が必要です。通常の E メールに登場するようなテキストをフィルタリングするような設定はしないでください。

この章の内容

パーソナルフィルタの管理方法について	200
正規表現を使用	202

パーソナルフィルタの管理方法について

このセクションでは、パーソナルフィルタの管理方法について説明します。

パーソナルフィルタを追加

フィルタの作成は任意ですが、作成した場合は受信メッセージに影響を与えます。このため、迷惑メールでないメッセージにも使用される一般的な言葉については、フィルタを作成しないことをお勧めします。

フィルタを追加するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【パーソナルフィルタ】** をクリックします。
- 5 **【追加】** をクリックします。
- 6 **【項目】** リストでいずれかの項目をクリックし、メッセージの件名、本文、ヘッダ、送信者に含まれる単語または語句を検索するかどうかを決定します。
- 7 **【条件】** リストでいずれかの条件をクリックし、指定した単語または語句が含まれるメッセージを検索するか、または含まれないメッセージを検索するかどうかを決定します。
- 8 **【単語または語句】** ボックスで、メッセージ内で検索する文字列を入力します。たとえば、「住宅ローン」と指定した場合、「住宅ローン」という単語を含むメッセージがすべてフィルタリングされます。
- 9 **【このフィルタでは正規表現 (RegEx) を使用します】** チェックボックスをオンにし、フィルタ条件に正規表現を使って文字パターンを指定することもできます。文字パターンをテストするには、**【テスト】** をクリックします。
- 10 **【OK】** をクリックします。

パーソナルフィルタを編集

フィルタによって、McAfee SpamKiller が確認する E メールの内容が指定されます。McAfee SpamKiller では多くのフィルタが使用されますが、新しいフィルタを作成するか、既存のフィルタを編集することによって、迷惑メールとして識別するメッセージの詳細を設定できます。

フィルタを編集するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。

- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【パーソナルフィルタ】** をクリックします。
- 5 編集するフィルタを選択し、**【編集】** をクリックします。
- 6 **【項目】** リストでいずれかの項目をクリックし、メッセージの件名、本文、ヘッダ、送信者に含まれる単語または語句を検索するかどうかを決定します。
- 7 **【条件】** リストでいずれかの条件をクリックし、指定した単語または語句が含まれるメッセージを検索するか、または含まれないメッセージを検索するかどうかを決定します。
- 8 **【単語または語句】** ボックスで、メッセージ内で検索する文字列を入力します。たとえば、「住宅ローン」と指定した場合、「住宅ローン」という単語を含むメッセージがすべてフィルタリングされます。
- 9 **【このフィルタでは正規表現 (RegEx) を使用します】** チェックボックスをオンにし、フィルタ条件に正規表現を使って文字パターンを指定することもできます。文字パターンをテストするには、**【テスト】** をクリックします。
- 10 **【OK】** をクリックします。

パーソナルフィルタを削除

不要になったフィルタは削除することができます。削除すると、そのフィルタは完全に削除されます。

フィルタを削除するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【パーソナルフィルタ】** をクリックします。
- 5 削除するフィルタを選択し、**【削除】** をクリックします。
- 6 **【OK】** をクリックします。

正規表現を使用

正規表現は、特定の文字列を定義する場合に使用できる特殊文字やパターンです。例:

- 正規表現 `[0-9]*¥.[0-9]+`
浮動小数点の数字と一致します。この正規表現は、「12.12」、
「.1212」、および「12.0」と一致しますが、「12」とは一致しません。
- 正規表現 `¥D*[0-9]+¥D*`
数値を含むすべての単語と一致します。「SpamKi11er」や
「VIAGRA」と一致しますが、「SpamKiller」や「VIAGRA」とは一致しません。

正規表現を使用

正規表現は、特定の文字列を定義する場合に使用できる特殊文字やパターンです。

¥

次に続く文字が特殊文字であることを示します。たとえば、「n」は文字「n」と一致しますが、「¥n」は改行文字と一致します。「¥¥」は「¥」と、「¥(」は「(」と一致します。

^

入力文字列の先頭と一致します。

\$

入力文字列の末尾と一致します。

直前の文字と 0 回以上一致します。たとえば、「zo*」は「z」または「zoo」と一致します。

+

直前の文字と 1 回以上一致します。たとえば、「zo+」は「zoo」とは一致しますが、「z」とは一致しません。

?

直前の文字と 0 回または 1 回一致します。たとえば、「a?ve?」は「never」の「ve」と一致します。

.

改行文字を除く任意の 1 文字と一致します。

(pattern)

pattern と一致した文字列を記憶します。一致文字列は、[0]...[n] を使用して Matches コレクションから取得できます。かっこ () と一致するには、「¥(」または「¥)」を使用します。

x|y

x または y と一致します。たとえば、「z|wood」は「z」または「wood」と一致します。「(z|w)oo」は「zoo」または「wood」と一致します。

{n}

n には 0 以上の整数を指定します。正確に n 回一致します。たとえば、「o{2}」は「Bob」の「o」とは一致しませんが、「fooooood」の最初の 2 つの o と一致します。

{n,}

n には 0 以上の整数を指定します。少なくとも n 回一致します。たとえば、「o{2}」は「Bob」の「o」とは一致しませんが、「fooooood」のすべての o とは一致します。「o{1,}」は「o+」と同じ意味になります。「o{0,}」は「o*」と同じ意味になります。

{n,m}

m と n には 0 以上の整数を指定します。n ~ m 回一致します。たとえば、「o{1,3}」は「fooooood」の最初の 3 つの o と一致します。「o{0,1}」は「o?」と同じ意味になります。

[xyz]

文字セットを指定します。角かっこで囲まれた文字のいずれかと一致します。たとえば、「[abc]」は「plain」の「a」と一致します。

[^xyz]

除外する文字セットを指定します。角かっこで囲まれた文字以外の文字に一致します。たとえば、「[^abc]」は「plain」の「p」と一致します。

[a-z]

文字の範囲を指定します。指定された範囲にある文字と一致します。たとえば、「[a-z]」は小文字または大文字の英字「a」から「z」および「A」から「Z」の範囲にある任意の文字と一致します。

[A-Z]

文字の範囲を指定します。指定された範囲にある文字と一致します。たとえば、「[A-Z]」は大文字または小文字の英字「A」から「Z」および「a」から「z」の範囲にある任意の文字と一致します。

[^m-z]

除外する文字の範囲を指定します。指定範囲以外の文字と一致します。たとえば、「[^m-z]」は小文字の英字「m」から「z」の範囲外にある任意の文字と一致します。

¥b

単語の境界と一致します。単語の境界とは、単語とスペースとの間の位置のことです。たとえば、「er¥b」は「never」の「er」と一致しますが、「verb」の「er」とは一致しません。

¥B

単語境界以外と一致します。たとえば、「ea*r¥B」は「never early」の「ear」と一致します。

¥d

任意の 10 進数字と一致します。[0-9] と同じ意味になります。

¥D

10 進数字以外の任意の 1 文字と一致します。[^0-9] と同じ意味になります。

¥f

フォームフィード文字と一致します。

¥n

改行文字と一致します。

¥r

キャリッジリターン文字と一致します。

¥s

スペース、タブ、フォームフィードなどの任意の空白文字と一致します。「[¥f¥n¥r¥t¥v]」と同じ意味になります。

¥S

空白文字以外の任意の文字と一致します。「[^ ¥f¥n¥r¥t¥v]」と同じ意味になります。

¥t

タブ文字と一致します。

¥v

垂直タブ文字と一致します。

¥w

単語に使用される任意の文字と一致します。アンダースコアも含まれます。「[A-Za-z0-9_]」と同じ意味になります。

¥W

単語に使用される文字以外の任意の文字と一致します。「[^A-Za-z0-9_]」と同じ意味になります。

¥num

num と一致します。num には正の整数を指定します。すでに見つかった記憶されている部分と一致します。たとえば、「(.)¥1」は、連続する 2 つの同じ文字と一致します。¥n は n と一致します。n は 8 進数のエスケープ値となります。8 進数のエスケープ値は、1、2、または 3 桁である必要があります。たとえば、「¥11」と「¥011」の両方は、1 つのタブ文字と一致します。「¥0011」は「¥001」と「1」と同じ意味になります。8 進数のエスケープ値は、256 以下である必要があります。この値を超えた場合は、最初の 2 桁のみが表現となります。正規表現で ASCII コードを使用可能にします。

¥xn

n と一致します。n は 16 進数のエスケープ値となります。16 進数のエスケープ値は 2 桁である必要があります。たとえば、「¥x41」は「A」と一致します。「¥x041」は「¥x04」と「1」と同じ意味になります。正規表現で ASCII コードを使用可能にします。

第 30 章

McAfee SpamKiller を保守

McAfee SpamKiller の保守には、迷惑メール対策の管理、ツールバーの使用が含まれます。

迷惑メール対策を管理する場合、フィルタを無効または有効にできます。

ツールバーを使用する場合、McAfee SpamKiller で提供される E メールツールバーを無効/有効にしたり、ツールバーから迷惑メールまたは非迷惑メールとしてメッセージをマークできます。

この章の内容

迷惑メール対策を管理	208
ツールバーを使用	209

迷惑メール対策を管理

E メールメッセージのフィルタリングを無効または有効にできます。

E メールメッセージのフィルタリングを一時停止する場合には迷惑メール対策を無効にし、E メールメッセージをフィルタリングする場合には迷惑メール対策を有効にします。

迷惑メール対策を無効化

迷惑メール対策を無効にして、E メールメッセージのフィルタリングを一時停止できます。

フィルタリングを無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【オフ】** をクリックします。

迷惑メール対策を有効化

迷惑メール対策を有効にして、E メールメッセージをフィルタリングできます。

フィルタリングを有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【オン】** をクリックします。

ツールバーを使用

サポートされている E メールクライアント用の E メールツールバーを無効または有効にできます。

Outlook、Outlook Express、Windows Mail、Eudora または Thunderbird の E メールプログラムを使用している場合、McAfee SpamKiller ツールバーから迷惑メールまたは非迷惑メールとしてメッセージをマークすることもできます。

ツールバーを無効化

サポートされている E メールクライアントのためのツールバーを無効にできます。

ツールバーを無効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【Eメールのツールバー】** をクリックし、無効にするツールバーの横のチェックボックスをオフにします。
- 5 **【OK】** をクリックします。

ツールバーを有効化

無効にしたツールバーは、再び有効にできます。

ツールバーを有効にするには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【E メールとメッセージャー】** をクリックします。
- 3 **【迷惑メール対策】** で **【詳細設定】** をクリックします。
- 4 **【迷惑メール対策】** パネルで **【Eメールのツールバー】** をクリックし、有効にするツールバーの横のチェックボックスをオンにします。
- 5 **【OK】** をクリックします。

McAfee SpamKiller ツールバーから迷惑メールまたは非迷惑メールとしてメッセージをマーク

Outlook、Outlook Express、Windows Mail、Eudora または Thunderbird の E メールプログラムを使用している場合、McAfee SpamKiller ツールバーから迷惑メールまたは非迷惑メールとしてメッセージをマークすることもできます。

迷惑メールとしてメッセージをマークすると、メッセージには [SPAM] タグまたは選択したタグが追加され、受信ボックス、SpamKiller フォルダ (Outlook、Outlook Express、Windows Mail、Thunderbird の場合)、または Junk フォルダ (Eudora の場合) に保存されます。

非迷惑メールとしてメッセージをマークすると、メッセージタグが削除され、メッセージは受信ボックスに移動されます。

Outlook から迷惑メールまたは非迷惑メールとしてメッセージをマークするには

- 1 Outlook で、メッセージを選択します。
- 2 [SpamKiller] ツールバーで [迷惑メールとしてマーク] または [非迷惑メールとしてマーク] をクリックします。

Outlook Express、Windows Mail、Eudora、Thunderbird から迷惑メールまたは非迷惑メールとしてメッセージをマークするには

- 1 それぞれの閲覧画面で、メッセージを選択します。
- 2 [SpamKiller] メニューで [迷惑メールとしてマーク] または [非迷惑メールとしてマーク] をクリックします。

第 31 章

フィッシング詐欺対策の設定

不要な E メールは、迷惑メール（広告メール）、またはフィッシング詐欺（既知または不正な可能性のある Web サイトを使用して個人情報取得しようとするメール）として分類されます。

フィッシング詐欺フィルタを使用すると、不正な Web サイトから保護されます。既知のフィッシング詐欺サイトまたは不正な可能性のある Web サイトを参照すると、フィッシング詐欺フィルタのページにリダイレクトされます。

フィッシング詐欺対策を無効/有効にしたり、フィルタリングオプションを変更できます。

この章の内容

フィッシング詐欺対策を無効化/有効化	212
フィッシング詐欺フィルタを変更	213

フィッシング詐欺対策を無効化/有効化

フィッシング詐欺対策を無効/有効にできます。たとえば、信頼する Web サイトへのアクセスがブロックされてしまう場合に、フィッシング詐欺対策を無効にします。

フィッシング詐欺対策を無効化

信頼する Web サイトへのアクセスがブロックされてしまう場合に、フィッシング詐欺対策を無効にします。

フィッシング詐欺対策を無効にするには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔インターネットとネットワーク〕** をクリックします。
- 3 **〔フィッシング詐欺対策〕** で **〔オフ〕** をクリックします。

フィッシング詐欺対策を有効化

フィッシング詐欺サイトからユーザを保護するために、フィッシング詐欺対策を有効にします。

フィッシング詐欺対策を有効にするには

- 1 詳細メニューで **〔設定〕** をクリックします。
- 2 **〔設定〕** パネルで **〔インターネットとネットワーク〕** をクリックします。
- 3 **〔フィッシング詐欺対策〕** で **〔オン〕** をクリックします。

フィッシング詐欺フィルタを変更

Web サイトがフィッシング詐欺サイトであるかどうかをマカフィーが決定する方法は、2 通りあります。1 つ目は、参照している Web サイトを既知の不正なサイトのリストと比較する方法です。2 つ目は、参照している Web サイトが不正であるかどうかを判定する方法です。

フィッシング詐欺フィルタを変更

Web サイトがフィッシング詐欺サイトであるかどうかをマカフィーが決定する方法は、2 通りあります。万全保護を行うには、両方のオプションを選択したままにしてください。

フィッシング詐欺オプションを変更するには

- 1 詳細メニューで **【設定】** をクリックします。
- 2 **【設定】** パネルで **【インターネットとネットワーク】** をクリックします。
- 3 **【フィッシング詐欺対策】** で **【詳細設定】** をクリックします。
- 4 次のチェックボックスをオン/オフにします。
 - **ブラックリストとホワイトリストの参照を有効にして詐欺目的の Web サイトを検出:** 参照している Web サイトを、既知の不正なサイトのリストと比較します。
 - **ヒューリスティック方式を有効にして詐欺目的の Web サイトを検出:** 参照している Web サイトが不正であるかどうかを判定します。
- 5 **【OK】** をクリックします。

第 32 章

その他の情報

この章では、よくある質問について説明します。

この章の内容

よくある質問216

よくある質問

ここでは、よくある質問とその回答を紹介します。

POP3、MSN/Hotmail、および MAPI のアカウントとは何ですか？

McAfee SpamKiller は、POP3、POP3 Web メール、MSN/Hotmail、および MAPI の E メールアカウントを処理できるように設計されています。これらのアカウントには若干の違いがあり、それによって McAfee SpamKiller でのフィルタリングの実行方法が変わります。

POP3

これは最も一般的なアカウントタイプで、インターネット Eメールの標準です。POP3 アカウントを持っている場合、McAfee SpamKiller はサーバに直接接続して、使用している Eメールプログラムがメッセージを取得する前にメッセージをフィルタリングします。

POP3 Web メール

POP3 Web メールアカウントは Web ベースの Eメールアカウントです。POP3 Web メールアカウントのフィルタリングは、POP3 アカウントのフィルタリングと同様です。

MSN/Hotmail

MSN/Hotmail アカウントは Web ベースの Eメールアカウントです。MSN/Hotmail アカウントのフィルタリングは、POP3 アカウントのフィルタリングと同様です。

MAPI

MAPI は Microsoft によって設計されたシステムで、インターネット E メール、ファックス、Exchange Server メッセージングなど、さまざまなタイプのメッセージングをサポートしています。このような理由から、MAPI は、企業で Microsoft Exchange Server が運用されている場合に企業環境で使用されることが多くなっています。ただし、個人のインターネット E メールに Microsoft Outlook を使用しているユーザも数多くいます。McAfee SpamKiller は MAPI アカウントにアクセスできますが、次の点に注意してください。

- 通常は、E メールプログラムを使用してメッセージを取得するまでフィルタリングは実行されません。
- McAfee SpamKiller でフィルタリングされるのは、標準設定の受信トレイとインターネット E メールだけです。

フィッシング詐欺フィルタとは何ですか？

不要な E メールは、迷惑メール（広告メール）、またはフィッシング詐欺メール（既知または不正な可能性のある Web サイトを使用して個人情報取得しようとするメール）として分類されます。

フィッシング詐欺を使用すると、ブラックリスト（フィッシング詐欺が確認されたサイトまたは関連不正サイト）またはグレーリスト（危険なコンテンツまたは完全に怪しい Web サイトへのリンクを含むサイト）に含まれているサイトから保護されます。

既知のフィッシング詐欺サイトや不正な可能性のあるサイトを参照すると、フィッシング詐欺フィルタのページにリダイレクトされます。

Cookie を使用する目的

マカフィーの Web サイトでは、Cookie と呼ばれるソフトウェアタグを使用して、Web サイトを再度訪問したユーザを識別します。Cookie とは、ご使用のコンピュータのハードディスクに送られる、数個のテキストを含んだファイルです。Cookie は、ユーザがサイトに再度アクセスしたことを確認するために使用されます。

マカフィーは、次の目的で Cookie を使用します。

- 契約上の許可と権限を管理する
- 訪問するたびにユーザが再度登録する必要がなくなるように、再度訪問しようとするユーザを識別する
- ユーザの購買傾向を把握し、ユーザのニーズに応じてサービスをカスタマイズする
- ユーザが関心のありそうな情報、製品、特別オファーを提示する

マカフィーは、お客様のニーズに応じて Web サイトをカスタマイズできるよう、お客様のお名前をお聞きます。

マカフィーは、Cookie を拒否するようブラウザを設定しているユーザに契約サービスを提供することができません。マカフィーは、収集した情報を第三者に販売、貸与、または共有することはありません。

マカフィーは、広告主が訪問者のブラウザに Cookie を設定することを許可します。マカフィーは、広告主の Cookie に含まれる情報にアクセスすることはできません。

第 33 章

McAfee Privacy Service

McAfee Privacy Service は、ユーザやその家族、個人データ、およびコンピュータを保護する高度な機能を提供するソフトウェアです。オンラインでの個人情報の漏えいを阻止し、個人情報の送出手をブロックし、有害な可能性のあるオンラインコンテンツ（画像、広告、ポップアップ、Web バグなど）をフィルタリングします。また、子供の Web 閲覧履歴の監視、制御、ログの記録を行う高度なパレンタルコントロールや、パスワードを記録できる安全な記憶領域も提供されます。

McAfee Privacy Service を使用する前に、よく利用する機能について理解することができます。これらの機能の設定と使用方法に関する詳細は、McAfee Privacy Service のヘルプを参照してください。

この章の内容

機能	220
パレンタルコントロールをセットアップ	221
インターネットでの情報を保護	241
パスワードを保護	245

機能

McAfee Privacy Service には、次の機能が搭載されています。

- Web ブラウジング保護
- 個人情報保護
- パレンタルコントロール
- パスワードの保管

Web ブラウジング保護

Web ブラウジング保護により、コンピュータ上で広告、ポップアップ、Web バグがブロックされます。広告とポップアップのブロックを使用すると、ブラウザでほとんどの広告とポップアップが表示されなくなります。Web バグのブロックを使用すると、Web サイトによりインターネットの利用状況を追跡され、不正な送信先に情報が送信されることを防止できます。広告、ポップアップ、Web バグのブロック機能を組み合わせることにより、セキュリティを強化し、インターネットの閲覧中に要求していないコンテンツが表示されることを防ぎます。

個人情報保護

個人情報保護により、個人情報（クレジットカード番号、銀行の口座番号、住所など）がインターネットを介して転送されることを防止できます。

パレンタルコントロール

パレンタルコントロールでは、コンテンツのレベルを設定し、ユーザが表示できる Web サイトとコンテンツを制限できます。また、インターネットの使用時間制限を設定し、ユーザがインターネットにアクセスできる時間を指定できます。さらに、特定の Web サイトへのアクセスを全体的に制限したり、年齢グループとそれぞれのグループで決められたキーワードに基づいてアクセスを許可またはブロックできます。

パスワードの保管

Password Vault は、個人のパスワードを記録できる安全な記憶領域です。この記憶領域に保存すると、マカフィー製品の管理者またはシステムの管理者を含むほかのユーザは、記録されたパスワードに一切アクセスできません。

第 34 章

パレンタルコントロールをセットアップ

ユーザを追加したあと、そのユーザについてのパレンタルコントロールをセットアップします。パレンタルコントロールは、ユーザのコンテンツの格付けのグループ、Cookie ブロックのレベル、インターネット使用時間制限を定義する設定です。コンテンツの格付けのグループでは、ユーザの年齢グループに応じて、利用可能なインターネットコンテンツおよび Web サイトの種類を決定します。Cookie ブロックのレベルでは、Web サイトについて、ユーザのログイン時にコンピュータに設定された Cookie の読み取りを許可するかどうかを指定します。インターネット使用時間制限では、ユーザがインターネットにアクセスできる曜日と時間を定義します。

また、未成年ユーザに適用される、グローバル パレンタル コントロールもいくつかセットアップできます。たとえば、未成年ユーザがインターネットを閲覧するときに、特定の Web サイトをブロック/許可したり、不適切な可能性のある画像を表示しないようにできます。また、すべてのユーザについて、グローバルの Cookie ブロックの設定ができます。ただし、各ユーザの Cookie ブロックのレベルがグローバルの Cookie ブロックの設定と異なる場合、グローバル設定が優先されます。

注: パレンタルコントロールをセットアップするには、管理者権限が必要です。

この章の内容

ユーザのコンテンツの格付けグループの設定	222
ユーザの Cookie ブロックのレベルの設定	224
ユーザのインターネット使用時間制限の設定	229
Web サイトをブロック	230
Web サイトを許可	234
Web サイトによる Cookie の設定を許可	237
不適切な可能性のある Web 画像をブロック	239

ユーザのコンテンツの格付けグループの設定

ユーザは、次のコンテンツの格付けのグループのいずれかに属することができます。

- 幼児
- 子供
- 10 代前半
- 10 代後半
- 成年

コンテンツは、ユーザが属するグループに基づいて格付け（使用可能またはブロック対象）されます。たとえば、特定の Web サイトについて、幼児グループに属するユーザに対してはブロックし、10 代後半グループに属するユーザに対してはアクセス可能とします。成年グループに属するユーザは、すべてのコンテンツにアクセスできます。標準設定では、新しいユーザは自動的に幼児グループに追加され、使用できるコンテンツは完全に制限されます。

管理者権限のあるユーザは、ユーザのコンテンツの格付けのグループを設定してから、それらのグループに基づいて Web サイトのブロック対象/使用可能を設定できます。ユーザに対してコンテンツの格付けをより厳格に行う場合、グローバルの「許可する Web サイト」リストに含まれていない Web サイトをユーザが閲覧できないようにすることができます。詳細については、「キーワードにより Web サイトをブロック (232 ページ)」および「Web サイトを許可 (234 ページ)」を参照してください。

ユーザのコンテンツの格付けグループの設定

ユーザのコンテンツの格付けグループでは、利用可能なインターネットコンテンツおよび Web サイトの種類が年齢に応じて決定されます。

ユーザのコンテンツの格付けグループを設定するには

- 1 「よく使う機能」で「ホーム」をクリックします。
- 2 「SecurityCenter の情報」で「設定」をクリックします。
- 3 「SecurityCenter の設定」パネルで、「ユーザ」の「詳細設定」をクリックします。
- 4 「ユーザ」パネルで「パレンタルコントロール」をクリックします。
- 5 リストからユーザ名を選択します。
- 6 「コンテンツの格付け」で、ユーザに割り当てる年齢グループをクリックします。

各年齢グループに応じてコンテンツを格付けすると、年齢や成長度に合わないコンテンツが表示されることを防止できます。

- 7 グローバルな「許可する Web サイト」リストに含まれていない Web サイトをユーザが閲覧することを制限するには、「このユーザのアクセスを「許可する Web サイト」リストの Web サイトに制限します」チェックボックスをオンにします。
- 8 [OK] をクリックします。

ユーザの Cookie ブロックのレベルの設定

Web サイトの中には、Cookie と呼ばれる小さなファイルをコンピュータ上に作成して、個人的な情報やインターネット利用状況を監視するものがあります。管理者権限のある場合は、次の Cookie ブロックのレベルのいずれかをユーザに割り当てることができます。

- すべての Cookie を許可
- すべての Cookie を拒否
- Cookie を受け入れるかどうかユーザに確認

[すべての Cookie を許可] という設定では、ユーザのログイン時にコンピュータに設定された Cookie を Web サイトが読み取ることができます。[すべての Cookie を拒否] という設定では、Cookie を Web サイトが読み取ることはできません。[Cookie を受け入れるかどうかユーザに確認] という設定では、Web サイトがコンピュータに Cookie を設定しようとするたびに、ユーザに通知します。ユーザは、Cookie を許可するか、拒否するかを状況に応じて選択できます。特定の Web サイトについて Cookie を許可するか、拒否するかをユーザが決定すると、その Web サイトについては今後はメッセージが表示されなくなります。

注: Cookie を有効にしないと正しく動作しない Web サイトもあります。

ユーザの Cookie ブロックのレベルの設定

Web サイトの中には、Cookie と呼ばれる小さなファイルをコンピュータ上に作成して、個人的な情報やインターネット利用状況を監視するものがあります。コンピュータ上で、ユーザごとに Cookie の処理方法を指定できます。

ユーザの Cookie ブロックのレベルを設定するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。

6 [Cookie のブロック] で、次のいずれかをクリックします。

- **すべての Cookie を許可:** このユーザが閲覧するすべての Web サイトは、コンピュータに設定された Cookie を読み取ることができます。
- **すべての Cookie を拒否:** このユーザが閲覧する Web サイトは、コンピュータに設定された Cookie を読み取ることができません。
- **Cookie を受け入れるかどうかユーザに確認:** このユーザが Web サイトの閲覧を試行すると、Cookie を許可するか、拒否するか の決定を要求するメッセージが表示されます。

7 [OK] をクリックします。

ユーザの Cookie 受け入れリストに Web サイトを追加

ユーザの Cookie のブロックレベルを、Web サイトによって Cookie が設定される際に許可を要求するよう設定している場合、特定の Web サイトについては表示なしに Cookie を設定できるようにするには、これらの Web サイトをユーザの Cookie 受け入れリストに追加します。

ユーザの Cookie 受け入れリストに Web サイトを追加するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。
- 6 [Cookie のブロック] で [リストを表示] をクリックします。
- 7 [Cookie を許可する Web サイト] で、[http://] ボックスに Web サイトのアドレスを入力してから [追加] をクリックします。
- 8 [終了] をクリックします。

ユーザの Cookie 受け入れリストの Web サイトを変更

Web サイトのアドレスが変更された場合、またはユーザの Cookie 受け入れリストに Web サイトを追加したときにアドレスを誤って入力した場合は、Cookie 受け入れリストの Web サイトを変更できます。

ユーザの Cookie 受け入れリストの Web サイトを変更するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。

- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。
- 6 [Cookie のブロック] で [リストを表示] をクリックします。
- 7 [Cookie を許可する Web サイト] で、[Web サイト] リストのエントリをクリックし、[http://] ボックスで Web サイトのアドレスを変更してから [更新] をクリックします。
- 8 [終了] をクリックします。

ユーザの Cookie 受け入れリストから Web サイトを削除

ユーザの Cookie 受け入れリストに Web サイトを誤って追加した場合は、Cookie 受け入れリストからその Web サイトを削除できます。

ユーザの Cookie 受け入れリストから Web サイトを削除するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。
- 6 [Cookie のブロック] で [リストを表示] をクリックします。
- 7 [Cookie を許可する Web サイト] で、[Web サイト] リストのエントリをクリックしてから [削除] をクリックします。
- 8 [削除の確認] ダイアログボックスで、[はい] をクリックします。
- 9 [終了] をクリックします。

ユーザの Cookie 拒否リストに Web サイトを追加

ユーザの Cookie のブロックレベルを、Web サイトによって Cookie が設定される際に許可を要求するよう設定している場合、特定の Web サイトについては表示なしに Cookie の設定を拒否するには、これらの Web サイトをユーザの Cookie 拒否リストに追加します。

ユーザの Cookie 拒否リストに Web サイトを追加するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。

- 6 [Cookie のブロック] で [リストを表示] をクリックします。
- 7 [Cookie を拒否する Web サイト] をクリックします。
- 8 [Cookie を拒否する Web サイト] で、[http://] ボックスに Web サイトのアドレスを入力してから [追加] をクリックします。
- 9 [終了] をクリックします。

ユーザの Cookie 拒否リストの Web サイトを変更

Web サイトのアドレスが変更された場合、またはユーザの Cookie 拒否リストに Web サイトを追加したときにアドレスを誤って入力した場合は、Cookie 拒否リストの Web サイトを変更できます。

ユーザの Cookie 拒否リストの Web サイトを変更するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。
- 6 [Cookie のブロック] で [リストを表示] をクリックします。
- 7 [Cookie を拒否する Web サイト] をクリックします。
- 8 [Cookie を拒否する Web サイト] で、[Web サイト] リストのエントリをクリックし、[http://] ボックスで Web サイトのアドレスを変更してから [更新] をクリックします。
- 9 [終了] をクリックします。

ユーザの Cookie 拒否リストから Web サイトを削除

ユーザの Cookie 拒否リストに Web サイトを誤って追加した場合は、Cookie 拒否リストからその Web サイトを削除できます。

ユーザの Cookie 拒否リストから Web サイトを削除するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。
- 6 [Cookie のブロック] で [リストを表示] をクリックします。
- 7 [Cookie を拒否する Web サイト] をクリックします。

- 8 **【Cookie を拒否する Web サイト】** で、**【Web サイト】** リストのエントリをクリックしてから **【削除】** をクリックします。
- 9 **【削除の確認】** ダイアログボックスで、**【はい】** をクリックします。
- 10 **【終了】** をクリックします。

ユーザのインターネット使用時間制限の設定

管理者権限がある場合、[インターネット使用時間制限] グリッドを使用して、ユーザがいつインターネットにアクセスできるかを指定できます。ユーザに対して、制限のないインターネットの使用を許可したり、制限されたインターネットの使用を許可したり、インターネットの使用を禁止することができます。

[インターネット使用時間制限] グリッドでは、インターネット使用時間を 30 分間隔で指定できます。グリッドの緑色の部分は、ユーザがインターネットにアクセスできる曜日と時間を示します。グリッドの赤色の部分は、アクセスが拒否される時間を示します。禁止されている期間に、ユーザがインターネットへアクセスしようとした場合、McAfee Privacy Service により、アクセスできないことが通知されます。

あるユーザがインターネットへのアクセスを完全に禁止されている場合、そのユーザはログインしてコンピュータを使用することはできますが、インターネットは使用できません。

ユーザのインターネット使用時間制限の設定

[インターネット使用時間制限] グリッドを使用して、ユーザがいつインターネットにアクセスできるかを指定できます。グリッドの緑色の部分は、ユーザがインターネットにアクセスできる曜日と時間を示します。グリッドの赤色の部分は、アクセスが拒否される時間を示します。

ユーザのインターネット使用時間制限を設定するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 [SecurityCenter の情報] で [設定] をクリックします。
- 3 [SecurityCenter の設定] パネルで、[ユーザ] の [詳細設定] をクリックします。
- 4 [ユーザ] パネルで [パレンタルコントロール] をクリックします。
- 5 リストからユーザ名を選択します。
- 6 [インターネット使用時間制限] で、グリッドをドラッグして、ユーザがインターネットにアクセスできる曜日と時間を指定します。
- 7 [OK] をクリックします。

Web サイトをブロック

管理者権限があれば、特定の Web サイトへのすべての未成年ユーザによるアクセスをブロックすることができます。ブロックされた Web サイトへのアクセスをユーザが試行すると、そのサイトがマカフィーによりブロックされているためアクセスできないことを示すメッセージが表示されます。

成年グループに属するユーザ（管理者を含む）は、Web サイトが **ブロックする Web サイト** リストに含まれているかどうかに関わらず、すべての Web サイトにアクセスできます。ブロックする Web サイトをテストするには、未成年ユーザとしてログインする必要があります。

管理者として、Web サイトに含まれるキーワードに基づいて Web サイトをブロックできます。マカフィーでは、キーワードのリストとそれに対応するルールの標準設定のリストを提供しています。このリストでは、特定の年齢グループのユーザに対して、キーワードを含む Web サイトへのアクセスを許可するかどうかが決まります。キーワードスキャンが有効になっている場合、キーワードの標準設定のリストは、ユーザに対するコンテンツの格付けに使用されます。ただし、固有の許可キーワードを標準設定のリストに追加し、キーワードと特定の年齢グループを関連付けることができます。追加したルールのキーワードが、標準設定のリストのキーワードに一致すると、既存のルールは無視されます。既存のキーワードを検索することも、新しいキーワードを指定して特定の年齢グループに関連付けることもできます。

Web サイトをブロック

特定の Web サイトへのすべての未成年ユーザによるアクセスをブロックします。ユーザがその Web サイトへのアクセスを試行すると、そのサイトがマカフィーによりブロックされていることを示すメッセージが表示されます。

Web サイトをブロックするには

- 1 **よく使う機能** で **ホーム** をクリックします。
- 2 McAfee SecurityCenter の **ホーム** パネルで **パレンタルコントロール** をクリックします。
- 3 **パレンタルコントロールの情報** セクションで **設定** をクリックします。
- 4 **パレンタルコントロールの設定** パネルで、**パレンタルコントロール** が有効になっていることを確認してから **詳細設定** をクリックします。

- 5 [ブロックする Web サイト] パネルで、[http://] ボックスに Web サイトのアドレスを入力してから [追加] をクリックします。
- 6 [OK] をクリックします。

ブロックする Web サイトを変更

Web サイトのアドレスが変更された場合、または [ブロックする Web サイト] リストに Web サイトを追加したときにアドレスを誤って入力した場合は、Web サイトを変更できます。

ブロックする Web サイトを変更するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [ブロックする Web サイト] パネルで、[ブロックする Web サイト] リストのエントリをクリックし、[http://] ボックスで Web サイトのアドレスを変更してから [更新] をクリックします。
- 6 [OK] をクリックします。

ブロックする Web サイトを削除

ある Web サイトをブロックする必要がなくなった場合には、[ブロックする Web サイト] リストから削除する必要があります。

ブロックする Web サイトを削除するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [ブロックする Web サイト] パネルで、[ブロックする Web サイト] リストのエントリをクリックしてから [削除] をクリックします。
- 6 [削除の確認] ダイアログボックスで、[はい] をクリックします。
- 7 [OK] をクリックします。

キーワードスキャンを無効化

標準設定ではキーワードスキャンが有効になっており、マカフィーのキーワードの標準設定のリストがユーザに対するコンテンツの格付けに使用されます。決してお勧めしませんが、キーワードスキャンはいつでも無効にすることができます。

キーワードスキャンを無効にするには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [グローバル パレンタル コントロール] パネルで、[キーワードスキャン] をクリックします。
- 6 [キーワードのスキャン] パネルで [オフ] をクリックします。
- 7 [OK] をクリックします。

キーワードにより Web サイトをブロック

コンテンツに基づいて Web サイトをブロックするときに、特定の Web サイトのアドレスが分からない場合、キーワードに基づいて Web サイトをブロックできます。キーワードを入力するだけで、そのキーワードが含まれる Web サイトを、どの年齢グループに対して表示/非表示にするかを決定できます。

キーワードにより Web サイトをブロックするには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [グローバル パレンタル コントロール] パネルで [キーワードスキャン] をクリックしたあと、オンになったことを確認します。
- 6 [グローバル パレンタル コントロール] パネルで、[キーワード] をクリックします。

- 7 **【検索】** ボックスにキーワードを入力します。
そのキーワードが含まれる Web サイトがブロックされるようになります。
- 8 最低年齢グループを指定するには、**【最低年齢】** スライダを移動します。
すると、その年齢グループ以上の年齢のユーザは、このキーワードが含まれる Web サイトを表示できます。
- 9 **【OK】** をクリックします。

Web サイトを許可

管理者の場合、標準設定およびブロックする Web サイトを上書きすると、すべてのユーザによる特定の Web サイトへのアクセスを許可できます。

ブロックする Web サイトの詳細については、「**Web サイトをブロック** (230 ページ)」を参照してください。

Web サイトを許可

ある Web サイトがどのユーザに対してもブロックされないようにするには、**[許可する Web サイト]** リストにその Web サイトを追加します。**[許可する Web サイト]** リストに Web サイトを追加すると、標準設定および**[ブロックする Web サイト]** リストに追加されていた Web サイトは無効になります。

Web サイトを許可するには

- 1 **[よく使う機能]** で **[ホーム]** をクリックします。
- 2 McAfee SecurityCenter の **[ホーム]** パネルで **[パレンタルコントロール]** をクリックします。
- 3 **[パレンタルコントロールの情報]** セクションで **[設定]** をクリックします。
- 4 **[パレンタルコントロールの設定]** パネルで、**[詳細設定]** をクリックします。
- 5 **[グローバル パレンタル コントロール]** パネルで、**[許可する Web サイト]** をクリックします。
- 6 **[許可する Web サイト]** パネルで、**[http://]** ボックスに Web サイトのアドレスを入力してから **[追加]** をクリックします。
- 7 **[OK]** をクリックします。

ヒント: **[許可する Web サイト]** リストに含まれていない Web サイトをユーザが閲覧できないようにすることもできます。詳細については、「**ユーザのコンテンツの格付けグループの設定** (222 ページ)」を参照してください。

許可する Web サイトを変更

Web サイトのアドレスが変更された場合、または [許可する Web サイト] リストに Web サイトを追加したときにアドレスを誤って入力した場合は、Web サイトを変更できます。

許可する Web サイトを変更するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [グローバル パレンタル コントロール] パネルで、[許可する Web サイト] をクリックします。
- 6 [許可する Web サイト] パネルで、[許可する Web サイト] リストのエントリをクリックし、[http://] ボックスでアドレスを変更してから [更新] をクリックします。
- 7 [OK] をクリックします。

許可する Web サイトを削除

許可する Web サイトはいつでも削除できます。設定によっては、[許可する Web サイト] リストから Web サイトを削除すると、マカフィーユーザがそのサイトにアクセスできなくなってしまう場合があります。

許可する Web サイトを削除するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [グローバル パレンタル コントロール] パネルで、[許可する Web サイト] をクリックします。
- 6 [許可する Web サイト] パネルで、[許可する Web サイト] リストのエントリをクリックしてから [削除] をクリックします。
- 7 [削除の確認] ダイアログボックスで、[はい] をクリックします。
- 8 [OK] をクリックします。

Web サイトによる Cookie の設定を許可

コンピュータに設定された Cookie をすべての Web サイトが読み取ることをブロックする場合や、Cookie を許可する前に特定のユーザにメッセージを表示するよう設定する場合、特定の Web サイトが正しく動作していないときは、これらのサイトすべてが Cookie を読み取ることができるように設定します。

Cookie および Cookie ブロックのレベルの詳細については、「**ユーザの Cookie ブロックのレベルの設定** (224 ページ)」を参照してください。

Web サイトによる Cookie の設定を許可

コンピュータに設定された Cookie をすべての Web サイトが読み取ることをブロックする場合や、Cookie を許可する前に特定のユーザにメッセージを表示するよう設定する場合、特定の Web サイトが正しく動作していないときは、これらのサイトすべてが Cookie を読み取ることができるように設定します。

Web サイトによる Cookie の設定を許可するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [グローバル パレンタル コントロール] パネルで、[Cookie] をクリックします。
- 6 [Cookie] パネルで、[http://] ボックスに Web サイトのアドレスを入力してから [追加] をクリックします。
- 7 [OK] をクリックします。

Cookie 受け入れリストを変更

Web サイトのアドレスが変更された場合、または [Cookie を許可] リストに Web サイトを追加したときにアドレスを誤って入力した場合は、Web サイトを変更できます。

Cookie 受け入れリストを変更するには

- 1 **【よく使う機能】** で **【ホーム】** をクリックします。
- 2 McAfee SecurityCenter の **【ホーム】** パネルで **【パレンタルコントロール】** をクリックします。
- 3 **【パレンタルコントロールの情報】** セクションで **【設定】** をクリックします。
- 4 **【パレンタルコントロールの設定】** パネルで、**【詳細設定】** をクリックします。
- 5 **【グローバル パレンタル コントロール】** パネルで、**【Cookie】** をクリックします。
- 6 **【Cookie】** パネルで、**【Cookie を許可】** リストのエントリをクリックし、**【http://】** ボックスでアドレスを変更してから **【更新】** をクリックします。
- 7 **【OK】** をクリックします。

Web サイトによる Cookie の設定をブロック

コンピュータに設定された Cookie を特定の Web サイトが読み取ることをブロックする場合、**【Cookie を許可】** リストからその Web サイトを削除します。

Web サイトによる Cookie の設定をブロックするには

- 1 **【よく使う機能】** で **【ホーム】** をクリックします。
- 2 McAfee SecurityCenter の **【ホーム】** パネルで **【パレンタルコントロール】** をクリックします。
- 3 **【パレンタルコントロールの情報】** セクションで **【設定】** をクリックします。
- 4 **【パレンタルコントロールの設定】** パネルで、**【詳細設定】** をクリックします。
- 5 **【グローバル パレンタル コントロール】** パネルで、**【Cookie】** をクリックします。
- 6 **【Cookie】** で、**【Cookie を許可】** リストのエントリをクリックしてから **【削除】** をクリックします。
- 7 **【削除の確認】** ダイアログボックスで、**【はい】** をクリックします。
- 8 **【OK】** をクリックします。

不適切な可能性のある Web 画像をブロック

インターネット閲覧中に不適切な可能性のある画像が表示されることをブロックし、大切な家族を保護できます。画像は、すべてのユーザ、または成年グループのメンバー以外のすべてのユーザに対してブロックできます。年齢グループの詳細については、「**ユーザのコンテンツの格付けグループの設定** (222 ページ)」を参照してください。

標準設定では、成年グループのメンバー以外のすべてのユーザに対して画像分析が有効になっています。ただし、管理者は画像分析をいつでも無効にできます。

不適切な可能性のある画像をブロック

標準設定では画像分析が有効になっており、インターネット閲覧中に不適切な可能性のある画像をブロックし、大切な家族を保護できます。不適切な可能性のある画像が検出された場合、カスタム画像で置き換えられ、元の画像がブロックされたことが表示されます。画像分析を無効にするには、管理者権限が必要です。

不適切な可能性のある画像をブロックするには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [パレンタルコントロール] をクリックします。
- 3 [パレンタルコントロールの情報] セクションで [設定] をクリックします。
- 4 [パレンタルコントロールの設定] パネルで、[詳細設定] をクリックします。
- 5 [グローバル パレンタル コントロール] パネルで、[画像分析] をクリックします。
- 6 [画像分析] パネルで、次のいずれかの操作を実行します。
 - すべてのユーザに対して不適切な可能性のある画像をブロックする場合は、[すべてのユーザ] をクリックします。
 - 成年グループのメンバー以外のすべてのユーザに対して不適切な可能性のある画像をブロックする場合は、[10 代のユーザと子供] をクリックします。
- 7 [OK] をクリックします。

第 35 章

インターネットでの情報を保護

インターネット閲覧中に家族や個人情報を保護するには、McAfee Privacy Service を使用します。たとえば、管理者の場合、インターネット使用中の広告、ポップアップ、Web バグをブロックするよう設定できます。ブロックする情報に情報を追加することにより、個人情報（名前、住所、クレジットカード番号、銀行の口座番号など）がインターネットを介して転送されることも防止できます。

この章の内容

広告、ポップアップ、Web バグをブロック	242
個人情報をブロック	244

広告、ポップアップ、Web バグをブロック

管理者は、インターネット使用中の広告、ポップアップ、Web バグをブロックするよう設定できます。広告とポップアップのブロックを使用すると、Web ブラウザでほとんどの広告とポップアップが表示されなくなります。これにより、インターネット閲覧中の速度と効率が向上します。Web バグのブロックを使用すると、Web サイトによりインターネットの利用状況を追跡され、不正な送信先に情報が送信されることを防止できます。Web バグ (Web ビーコン、ピクセルタグ、Clear GIF、または Invisible GIF と呼ばれます) は、HTML ページに組み込まれた画像ファイルであり、不正な送信元がコンピュータに Cookie を設定することができます。すると、設定された Cookie が不正な送信元に情報を転送する場合があります。

標準設定では、コンピュータ上で広告、ポップアップ、Web バグがブロックされます。管理者なら、広告、ポップアップ、Web バグを許可できます。

広告をブロック

インターネットへのアクセス中に表示される広告をブロックできます。

広告をブロックするには

- 1 **【よく使う機能】** で **【ホーム】** をクリックします。
- 2 McAfee SecurityCenter の **【ホーム】** パネルで **【インターネットとネットワーク】** をクリックします。
- 3 **【インターネットとネットワーク】** の情報セクションで **【設定】** をクリックします。
- 4 **【インターネットとネットワークの設定】** パネルで、**【Web ブラウジング保護】** の下の **【詳細設定】** をクリックします。
- 5 **【広告、ポップアップ、Web バグのブロック】** パネルで、**【インターネットの閲覧中に Web ページに表示される広告をブロックします】** チェックボックスをオンにします。
- 6 **【OK】** をクリックします。

ポップアップをブロック

インターネットへのアクセス中に表示されるポップアップをブロックできます。

ポップアップをブロックするには

- 1 **【よく使う機能】** で **【ホーム】** をクリックします。
- 2 McAfee SecurityCenter の **【ホーム】** パネルで **【インターネットとネットワーク】** をクリックします。

- 3 [インターネットとネットワーク] の情報セクションで **[設定]** をクリックします。
- 4 [インターネットとネットワークの設定] パネルで、**[Web ブラウジング保護]** の下の **[詳細設定]** をクリックします。
- 5 [広告、ポップアップ、Web バグのブロック] パネルで、**[インターネットの閲覧中に表示されるポップアップウィンドウをブロックします]** チェックボックスをオンにします。
- 6 **[OK]** をクリックします。

Web バグをブロック

Web バグ (Web ビーコン、ピクセルタグ、Clear GIF、または Invisible GIF と呼ばれます) は、HTML ページに組み込まれた画像ファイルであり、不正な送信元がコンピュータに Cookie を設定することができます。すると、設定された Cookie が不正な送信元に情報を転送する場合があります。Web バグをブロックし、コンピュータに Web バグが読み込まれることを防止します。

Web バグをブロックするには

- 1 **[よく使う機能]** で **[ホーム]** をクリックします。
- 2 McAfee SecurityCenter の **[ホーム]** パネルで **[インターネットとネットワーク]** をクリックします。
- 3 [インターネットとネットワーク] の情報セクションで **[設定]** をクリックします。
- 4 [インターネットとネットワークの設定] パネルで、**[Web ブラウジング保護]** の下の **[詳細設定]** をクリックします。
- 5 [広告、ポップアップ、Web バグのブロック] パネルで、**[このコンピュータで Web バグをブロック]** チェックボックスをオンにします。
- 6 **[OK]** をクリックします。

個人情報ブロック

ブロックする情報に情報を追加することにより、個人情報（名前、住所、クレジットカード番号、銀行の口座番号など）がインターネットを介して転送されることを防止できます。送信しようとした情報の中に個人情報が検出されると、次の内容が実行されます。

- 管理者にはメッセージが表示され、情報を送信するかどうかを決定できます。
- 管理者でないユーザには、ブロックされた情報が星印（*）で表示されます。たとえば、「サッカー日本代表の新監督が決定」という E メールを送信しようとしたときに、「日本代表」がブロック対象の個人情報として設定されている場合は、実際に送信される E メールには「サッカー*****の新監督が決定」と表示されます。

ブロックできる個人情報の種類は次のとおりです。名前、住所、郵便番号、社会保障情報（米国）、電話番号、クレジットカード番号、銀行口座、証券口座、および電話カード。別の種類の個人情報をブロックする場合には、種類を【その他】に設定します。

個人情報ブロック

ブロックできる個人情報の種類は次のとおりです。名前、住所、郵便番号、社会保障情報（米国）、電話番号、クレジットカード番号、銀行口座、証券口座、および電話カード。別の種類の個人情報をブロックする場合には、種類を【その他】に設定します。

個人情報をブロックするには

- 1 【よく使う機能】で【ホーム】をクリックします。
- 2 McAfee SecurityCenter の【ホーム】パネルで【インターネットとネットワーク】をクリックします。
- 3 【インターネットとネットワーク】の情報セクションで【設定】をクリックします。
- 4 【インターネットとネットワークの設定】パネルで、個人情報保護が有効になっていることを確認してから【詳細設定】をクリックします。
- 5 【ブロックされた情報】パネルで【追加】をクリックします。
- 6 リストからブロックする情報の種類を選択します。
- 7 個人情報を入力し、【OK】をクリックします。
- 8 【個人情報保護】ダイアログボックスで【OK】をクリックします。

第 36 章

パスワードを保護

Password Vault は、個人のパスワードを記録できる安全な記憶領域です。この記憶領域に保存すると、マカフィー製品の管理者またはシステムの管理者を含むほかのユーザは、記録されたパスワードに一切アクセスできません。

この章の内容

Password Vault をセットアップ246

Password Vault をセットアップ

Password Vault の使用を開始する前に、Password Vault のパスワードを設定する必要があります。Password Vault にアクセスできるのは、Password Vault のパスワードを知っているユーザのみです。Password Vault のパスワードを忘れた場合は、リセットすることができます。ただし、リセットを実行すると、これまでに Password Vault に保存されていたパスワードはすべて削除されます。

Password Vault のパスワードを設定したあとに、Vault 内のパスワードを追加、編集、削除できます。

Password Vault にパスワードを追加

Password Vault のパスワードを忘れた場合は、Password Vault にパスワードを追加できます。Password Vault は、Password Vault のパスワードを知っているユーザのみがアクセスできる、安全な領域です。

Password Vault にパスワードを追加するには

- 1 **【よく使う機能】** で **【ホーム】** をクリックします。
- 2 McAfee SecurityCenter の **【ホーム】** パネルで **【インターネットとネットワーク】** をクリックします。
- 3 **【インターネットとネットワーク】** の情報セクションで **【設定】** をクリックします。
- 4 **【インターネットとネットワークの設定】** パネルで、**【個人情報保護】** の下の **【詳細設定】** をクリックします。
- 5 **【個人情報保護】** パネルで **【Password Vault】** をクリックします。
- 6 **【パスワード】** ボックスに Password Vault のパスワードを入力し、**【パスワードの確認】** ボックスにパスワードを再び入力します。
- 7 **【開く】** をクリックします。
- 8 **【Password Vault】** パネルで **【追加】** をクリックします。
- 9 **【説明】** ボックスに、パスワードの説明（目的など）を入力してから、**【パスワード】** ボックスにパスワードを入力します。
- 10 **【追加】** をクリックして、**【OK】** をクリックします。

Password Vault のパスワードを変更

Password Vault の登録項目が常に正確で信頼性の高いものにするためには、パスワードの変更時にこれらを更新する必要があります。

Password Vault のパスワードを変更するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [インターネットとネットワーク] をクリックします。
- 3 [インターネットとネットワーク] の情報セクションで [設定] をクリックします。
- 4 [インターネットとネットワークの設定] パネルで、[個人情報保護] の下の [詳細設定] をクリックします。
- 5 [個人情報保護] パネルで [Password Vault] をクリックします。
- 6 [パスワード] ボックスに Password Vault のパスワードを入力します。
- 7 [開く] をクリックします。
- 8 [Password Vault] パネルでパスワードのエントリをクリックしてから、[編集] をクリックします。
- 9 [説明] ボックスのパスワードの説明（目的など）を変更してから、[パスワード] ボックスのパスワードを変更します。
- 10 [追加] をクリックして、[OK] をクリックします。

Password Vault のパスワードを削除

Password Vault のパスワードはいつでも削除できます。Vault から削除したパスワードは復元できません。

Password Vault のパスワードを削除するには

- 1 [よく使う機能] で [ホーム] をクリックします。
- 2 McAfee SecurityCenter の [ホーム] パネルで [インターネットとネットワーク] をクリックします。
- 3 [インターネットとネットワーク] の情報セクションで [設定] をクリックします。
- 4 [インターネットとネットワークの設定] パネルで、[個人情報保護] の下の [詳細設定] をクリックします。
- 5 [個人情報保護] パネルで [Password Vault] をクリックします。
- 6 [パスワード] ボックスに Password Vault のパスワードを入力します。
- 7 [開く] をクリックします。
- 8 [Password Vault] パネルでパスワードのエントリをクリックしてから、[削除] をクリックします。
- 9 [削除の確認] ダイアログボックスで、[はい] をクリックします。
- 10 [OK] をクリックします。

Password Vault のパスワードをリセット

Password Vault のパスワードを忘れた場合は、リセットすることができます。ただし、リセットを実行すると、これまでに入力したパスワードはすべて削除されます。

Password Vault のパスワードをリセットするには

- 1 **【よく使う機能】** で **【ホーム】** をクリックします。
- 2 McAfee SecurityCenter の **【ホーム】** パネルで **【インターネットとネットワーク】** をクリックします。
- 3 **【インターネットとネットワーク】** の情報パネルで **【設定】** をクリックします。
- 4 **【インターネットとネットワークの設定】** パネルで、**【個人情報保護】** の下の **【詳細設定】** をクリックします。
- 5 **【個人情報保護】** パネルで **【Password Vault】** をクリックします。
- 6 **【Password Vault をリセット】** で、**【パスワード】** ボックスに新しいパスワードを入力し、**【パスワードの確認】** ボックスにパスワードを再び入力します。
- 7 **【リセット】** をクリックします。
- 8 **【パスワードのリセットの確認】** ダイアログボックスで、**【はい】** をクリックします。

第 37 章

McAfee Data Backup

McAfee Data Backup を使用すると、ファイルを CD、DVD、USB ドライブ、外部ハードディスク、ネットワークドライブにアーカイブ（保管）し、データの不意の損失を防ぐことができます。ローカルアーカイブを使用すると、個人的なデータを CD、DVD、USB ドライブ、外部ハードディスク、ネットワークドライブにアーカイブ（バックアップ）できます。これにより、データの不意の損失に備えて、記録や文書、個人的に重要なデータがローカルにコピーされます。

McAfee Data Backup の使用を開始する前に、よく利用する機能について理解することができます。これらの機能の設定と使用方法に関する詳細は、McAfee Data Backup のヘルプに書かれています。プログラムの機能を確認したら、ローカルアーカイブの実行に使用するアーカイブメディアの容量が十分かどうか確認する必要があります。

この章の内容

機能	250
ファイルをアーカイブ	251
アーカイブ済みファイルを使用	259

機能

写真や音楽、その他の重要なファイルを保存したり、復元するために、McAfee Data Backup には次の機能が搭載されています。

スケジュールによるローカルアーカイブ

ファイルとフォルダを CD、DVD、USB ドライブ、外部ハードディスク、ネットワークドライブにアーカイブし、データを保護します。最初のアーカイブを実行したあとは、差分アーカイブが自動的に実行されます。

ワンクリックで復元

ファイルやフォルダを誤って削除してしまったり、壊してしまっても、最後にアーカイブしたファイルからデータを復元することができます。

圧縮と暗号化

標準設定では、アーカイブ済みファイルは圧縮されます。これにより、アーカイブメディアの容量を節約できます。セキュリティ強化策として、アーカイブが暗号化されるように標準で設定されています。

第 38 章

ファイルをアーカイブ

McAfee Data Backup を使用すると、ご使用のコンピュータ上のファイルを CD、DVD、USB ドライブ、外部ハードディスク、ネットワークドライブにアーカイブ（保管）できます。この方法でファイルをアーカイブすると、データを誤って消してしまったたり、壊してしまった場合でも、簡単に情報を復元できます。

ファイルのアーカイブを開始する前に、アーカイブの標準設定の保存場所（CD、DVD、USB ドライブ、外部ハードディスク、ネットワークドライブ）を選択する必要があります。アーカイブするフォルダやファイルタイプなど、いくつかの項目は事前に設定されていますが、これらの設定は変更できます。

ローカル アーカイブ オプションを設定すると、McAfee Data Backup の完全アーカイブまたはクイックアーカイブの頻度が設定できます。手動アーカイブはいつでも実行できます。

この章の内容

アーカイブオプションの設定	252
完全アーカイブとクイックアーカイブを実行	256

アーカイブオプションの設定

データのアーカイブ（保管）を開始する前に、ローカル アーカイブ オプションを設定する必要があります。たとえば、監視場所と監視するファイルタイプを設定する必要があります。監視場所とは、McAfee Data Backup が新規ファイルや変更ファイルの監視を行うコンピュータ内のフォルダのことです。監視対象のファイルタイプとは、McAfee Data Backup が監視場所内でアーカイブを行うファイルのタイプ（たとえば、.doc、.xls など）のことです。標準設定では、McAfee Data Backup は監視場所に保存されているすべてのファイルタイプを監視します。

監視場所には、重点監視する場所と部分的に監視する場所の 2 種類を設定できます。重点監視する場所を設定した場合、McAfee Data Backup は、このフォルダとサブフォルダ内の監視対象のファイルタイプをアーカイブします。部分的に監視する場所を設定した場合、McAfee Data Backup は、このフォルダ（サブフォルダは除く）の監視対象のファイルをアーカイブします。また、ローカルアーカイブから除外する場所を指定することもできます。標準設定では、Windows のデスクトップとマイドキュメントは重点監視する場所として設定されています。

監視対象のファイルタイプと場所を設定したら、アーカイブの保存場所（CD、DVD、USB、ネットワークドライブ、外部ハードディスクなど）を設定する必要があります。アーカイブの場所はいつでも変更できます。

セキュリティ上の理由とサイズの問題から、暗号化と圧縮は、アーカイブ済みファイルでは標準設定で有効になっています。暗号化とは、ファイルの内容をテキストからコードに変換し、解読方法を知らなければ読むことができないようにすることです。圧縮ファイルは、保存または転送時に必要な最小容量に圧縮されます。決してお勧めしませんが、暗号化と圧縮はいつでも無効にすることができます。

アーカイブ対象を追加

アーカイブの監視場所には、重点監視する場所と部分的に監視する場所の 2 種類を設定できます。重点監視する場所を設定すると、McAfee Data Backup はフォルダとサブフォルダのコンテンツの変更を監視します。部分的に監視する場所を設定すると、McAfee Data Backup はフォルダ（サブフォルダは除く）のコンテンツの変更のみを監視します。

アーカイブの場所を追加するには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 左パネルで [設定] をクリックします。

- 3 [ローカルアーカイブの設定] ダイアログボックスで[監視場所]をクリックします。



- 4 次のいずれかの操作を実行します。
- フォルダとそのすべてのサブフォルダのコンテンツをアーカイブするには、[重点監視する場所] の下の [フォルダを追加] をクリックします。
 - サブフォルダのコンテンツを除いてフォルダのコンテンツをアーカイブするには、[部分的に監視する場所] の下の [フォルダを追加] をクリックします。
- 5 [フォルダの選択] ダイアログボックスで、監視するフォルダを指定して [OK] をクリックします。
- 6 [保存] をクリックします。

ヒント: まだ作成していないフォルダを McAfee Data Backup の監視対象にするには、[フォルダの選択] ダイアログボックスの [新しいフォルダの作成] をクリックし、そのフォルダを監視場所として設定します。

アーカイブ ファイル タイプの設定

重点監視する場所と部分的に監視する場所で、アーカイブ対象のファイルタイプを指定できます。既存のファイルタイプのリストから選択するか、リストに新しいタイプを追加できます。

アーカイブするファイルタイプを設定するには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 左パネルで [設定] をクリックします。

- 3 [ローカルアーカイブの設定] ダイアログボックスで [ファイルタイプ] をクリックします。
- 4 ファイルタイプのリストを展開して、アーカイブするファイルタイプの横のチェックボックスを選択します。
- 5 [保存] をクリックします。

ヒント: [選択されたファイルタイプ] リストに新しいファイルタイプを追加するには、[カスタムのファイルタイプを [その他] に追加] ボックスにファイルの拡張子を入力して、[追加] をクリックします。新しいファイルタイプは自動的に監視対象のファイルタイプになります。

アーカイブ対象から除外

特定の場所（フォルダ）とそのコンテンツをオンラインでアーカイブしないようにするには、その場所をアーカイブの対象から除外します。

アーカイブの対象から除外するには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 左パネルで [設定] をクリックします。
- 3 [ローカルアーカイブの設定] ダイアログボックスで [監視中のフォルダ] をクリックします。
- 4 [監視から除外する場所] の下の [フォルダを追加] をクリックします。
- 5 [フォルダの選択] ダイアログボックスで、除外するフォルダを指定して [OK] をクリックします。
- 6 [保存] をクリックします。

ヒント: まだ作成していないフォルダを McAfee Data Backup の監視対象から除外するには、[フォルダの選択] ダイアログボックスの [新しいフォルダの作成] をクリックし、除外するフォルダを追加します。

アーカイブの保存場所を変更

アーカイブの保存場所を変更すると、以前に別の場所にアーカイブしたファイルは「未アーカイブ」として表示されます。

アーカイブの保存場所を変更するには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 左パネルで [設定] をクリックします。
- 3 [アーカイブ保存場所を変更] をクリックします。

- 4 [アーカイブ保存場所] ダイアログボックスで、次のいずれかを実行します。
 - [CD/DVD 書き込みドライブを選択] をクリックして、ご使用のコンピュータの CD または DVD ドライブを [書き込みドライブ] リストでクリックしてから、[保存] をクリックします。
 - [ドライブの場所を選択] をクリックし、USB ドライブ、ローカルドライブ、または外部ハードディスクのいずれかを指定して [OK] をクリックします。
 - [ネットワークの場所を選択] をクリックしてネットワークフォルダを選択し、[OK] をクリックします。
- 5 [選択されたアーカイブ保存場所] で、新しいアーカイブ保存場所を確認して、[OK] をクリックします。
- 6 確認のダイアログボックスで、[OK] をクリックします。
- 7 [保存] をクリックします。

アーカイブに対する暗号化と圧縮を無効化

アーカイブ済みファイルを暗号化し、解読方法を知らなければ読むことができないように変換することで、データの機密性を保護します。アーカイブ済みファイルを圧縮すると、ファイルのサイズを最小にすることができます。標準設定では、暗号化機能と圧縮機能の両方が有効になっています。ただし、これらのオプションはいつでも無効にできます。

アーカイブの暗号化および圧縮を無効にするには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 左パネルで [設定] をクリックします。
- 3 [ローカルアーカイブの設定] ダイアログボックスで [詳細設定] をクリックします。
- 4 [暗号化を有効にしてセキュリティを強化] チェックボックスをオフにします。
- 5 [圧縮を有効にして容量を削減] チェックボックスをオフにします。
- 6 [保存] をクリックします。

注: ファイルアーカイブ時の暗号化と圧縮は無効にしないことをお勧めします。

完全アーカイブとクイックアーカイブを実行

2 種類のアーカイブ（完全アーカイブとクイックアーカイブ）を実行できます。完全アーカイブを実行すると、監視するファイルタイプと場所の設定に従って、データが完全にアーカイブされます。クイックアーカイブを実行すると、完全アーカイブまたはクイックアーカイブの最終実行時から変更された監視中ファイルのみがアーカイブされます。

標準設定では、監視対象のファイルタイプの完全アーカイブを毎週月曜日の午前 9 時に実行し、最後の完全アーカイブまたはクイックアーカイブ以降 48 時間ごとにクイックアーカイブを実行するように設定されています。このスケジュールにより、ファイルの最新のアーカイブが常に維持されます。ただし、アーカイブが 48 時間ごとに実行されないように、必要に応じてスケジュールを調節できます。

監視場所のコンテンツのアーカイブを必要に応じて行いたい場合は、いつでも実行できます。たとえば、ファイルを変更してからアーカイブしたいときに、McAfee Data Backup による完全アーカイブまたはクイックアーカイブが数時間以内に実行されるように設定されていない場合は、手動でファイルをアーカイブできます。手動でファイルをアーカイブすると、設定された自動アーカイブの間隔はリセットされます。

不適切なタイミングで自動アーカイブまたは手動アーカイブが実行された場合には中断することもできます。たとえば、リソースを消費するタスクの実行中に自動アーカイブが開始された場合に、自動アーカイブを停止できます。自動アーカイブを停止すると、設定された自動アーカイブの間隔はリセットされます。

自動アーカイブをスケジュール

完全アーカイブとクイックアーカイブの頻度を設定し、データを常に保護できます。

自動アーカイブのスケジュールを設定するには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 左パネルで [設定] をクリックします。
- 3 [ローカルアーカイブの設定] ダイアログボックスで [全般] をクリックします。
- 4 完全アーカイブを毎日、毎週、または毎月実行するには、[完全アーカイブの実行間隔] で以下のいずれかをクリックします。
 - 日単位
 - 週単位
 - 月単位
- 5 完全アーカイブを実行する日の横のチェックボックスを選択します。

- 6 **【開始時刻】** リストの値をクリックして、完全アーカイブを実行する時間を指定します。
- 7 クイックアーカイブを毎日または毎時実行するには、**【クイックアーカイブ】** で以下のいずれかをクリックします。
 - **時間**
 - **日**
- 8 頻度を表す数値を **【クイックアーカイブの実行間隔】** ボックスに入力します。
- 9 **【保存】** をクリックします。

自動アーカイブを中断

McAfee Data Backup は、ユーザが定義したスケジュールに従って、監視場所内のファイルを自動的にアーカイブします。実行中の自動アーカイブはいつでも停止できます。

自動アーカイブを中断するには

- 1 左パネルで **【アーカイブを停止】** をクリックします。
- 2 確認のダイアログボックスで、**【はい】** をクリックします。

注: **【アーカイブを停止】** は、アーカイブの実行中にのみ表示されます。

アーカイブを手動で実行

自動アーカイブは、事前に定義されたスケジュールに従って実行されますが、クイックアーカイブと完全アーカイブはいつでも実行できます。クイックアーカイブは、完全アーカイブまたはクイックアーカイブの最終実行時以降に変更されたファイルのみをアーカイブします。完全アーカイブでは、すべての監視場所にある対象ファイルをアーカイブします。

クイックアーカイブまたは完全アーカイブを手動で実行するには

- 1 **【ローカルアーカイブ】** タブをクリックします。
- 2 クイックアーカイブを実行するには、左パネルの **【クイックアーカイブ】** をクリックします。
- 3 完全アーカイブを実行するには、左パネルの **【完全アーカイブ】** をクリックします。
- 4 **【アーカイブを開始する準備が整いました】** ダイアログボックスで、ストレージの容量と設定を確認し、**【続行】** をクリックします。

第 39 章

アーカイブ済みファイルを使用

ファイルをアーカイブすると、これらのファイルを McAfee Data Backup で操作できます。アーカイブ済みファイルは従来のエクスプローラ形式で表示されるため、簡単にファイルを見つけることができます。アーカイブのサイズが大きくなると、ファイルの並べ替えや検索が必要になります。ファイルを取得せずに、エクスプローラ表示でファイルを直接開き、内容を確認することもできます。

ローカルにコピーしたファイルが最新ではなかったり、不足していたり、壊れている場合は、アーカイブからファイルを取得します。また、McAfee Data Backup では、ローカルアーカイブやストレージメディアの管理に必要な情報が提供されます。

この章の内容

ローカルアーカイブのエクスプローラを使用	260
アーカイブ済みファイルを復元	262
アーカイブを管理	264

ローカルアーカイブのエクспローラを使用

ローカルアーカイブのエクспローラを使用すると、ローカルでアーカイブしたファイルの表示および操作を行うことができます。各ファイルの名前、タイプ、サイズ、状態（アーカイブ済み、未アーカイブ、アーカイブ中）、ファイルが最後にアーカイブされた日付を表示できます。これらの基準のいずれかに従ってファイルを並べ替えることもできます。

アーカイブが大きい場合、検索すると迅速にファイルを見つけることができます。ファイル名またはパスのすべてまたは一部を入力して検索し、次におよそのファイルサイズと最後にアーカイブされた日付を指定して検索対象を絞り込みます。

ファイルの場所がわかれば、ローカルアーカイブのエクспローラで直接ファイルを開くことができます。McAfee Data Backup は、そのファイルを作成したプログラムで直接ファイルを開き、ローカルアーカイブのエクспローラを表示したままファイルに変更を加えることができます。このファイルは、コンピュータ上の元の監視場所に保存され、定義されたアーカイブスケジュールに従って自動的にアーカイブされます。

アーカイブ済みファイルを並べ替え

アーカイブ済みのファイルとフォルダは、次の基準で並べ替えを行うことができます。名前、ファイルタイプ、サイズ、状態（アーカイブ済み、未アーカイブ、アーカイブ中）、ファイルが最後にアーカイブされた日付、コンピュータ上のファイルの場所（パス）

アーカイブ済みファイルを並べ替えるには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 右パネルで、列の名前をクリックします。

アーカイブ済みファイルを検索

アーカイブ済みファイルのリポジトリ（保管領域）が大きい場合、検索すると迅速にファイルを見つけることができます。ファイル名またはパスのすべてまたは一部を入力して検索し、次におよそのファイルサイズと最後にアーカイブされた日付を指定して検索対象を絞り込みます。

アーカイブ済みファイルを検索するには

- 1 ファイル名のすべてまたは一部を画面上部の[検索]ボックスに入力し、ENTER キーを押します。
- 2 パスのすべてまたは一部を[パスのすべてまたは一部]ボックスに入力します。

- 3 次のいずれかを実行して、検索するファイルのおよそのサイズを指定します。
 - [100 KB 未満]、[1 MB 未満]、または [1 MB より大きい] をクリックします。
 - [サイズ (KB)] をクリックし、ボックスに適切なサイズ値を指定します。
- 4 次のいずれかを実行して、ファイルのオンラインバックアップが最後に実行されたおよその日付を指定します。
 - [今週]、[今月] または [今年] をクリックします。
 - [日付を指定] をクリックして、リストで [アーカイブ済み] をクリックしたら、データリストから適切なデータ値を選択します。
- 5 [検索] をクリックします。

注: サイズまたは最後にアーカイブを実行した日付がわからない場合には、[不明] をクリックします。

アーカイブ済みファイルを使用

ローカルアーカイブのエクスプローラでアーカイブファイルを開き、コンテンツを確認できます。

アーカイブ済みファイルを開くには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 右パネルでファイル名をクリックし、[開く] をクリックします。

ヒント: ファイル名をダブルクリックして、アーカイブ済みのファイルを開くこともできます。

アーカイブ済みファイルを復元

監視対象のファイルが壊れた場合、不足している場合、または誤って削除された場合には、ローカルアーカイブからファイルのコピーを復元できます。したがって、定期的にファイルをアーカイブすることが重要です。ローカルアーカイブから古いバージョンのファイルを復元することもできます。たとえば、定期的にファイルをアーカイブしているときに、ファイルを以前のバージョンに戻したい場合には、アーカイブ保存場所のファイルを使用して以前のバージョンに戻すことができます。アーカイブ保存場所がローカルドライブまたはネットワークドライブの場合は、ファイルを参照できます。アーカイブ保存場所が外部ハードディスクまたは USB ドライブの場合は、ドライブをコンピュータに接続してからファイルを参照します。アーカイブ保存場所が CD または DVD の場合は、CD または DVD をコンピュータに挿入してからファイルを参照します。

あるコンピュータでアーカイブしたファイルを別のコンピュータから復元することもできます。たとえば、コンピュータ A で外部ハードディスクにファイルをアーカイブした場合、コンピュータ B でこれらのファイルを復元できます。これを実行するには、コンピュータ B に McAfee Data Backup をインストールしてその外部ハードディスクに接続する必要があります。McAfee Data Backup でファイルを参照すると、ファイルが **[不足ファイル]** リストに追加されます。

ファイルのアーカイブについては、「ファイルをアーカイブ」を参照してください。監視対象のファイルをアーカイブから意図的に削除した場合、**[不足ファイル]** リストのエントリも削除できます。

ローカルアーカイブから不足ファイルを復元

McAfee Data Backup のローカルアーカイブを使用すると、ローカルコンピュータ上の監視対象のフォルダで不足しているデータを復元できます。たとえば、監視対象のフォルダからファイルが移動または削除された場合、すでにアーカイブが行われていれば、ローカルアーカイブからファイルを復元できます。

ローカルアーカイブから不足ファイルを取得するには

- 1 **[ローカルアーカイブ]** タブをクリックします。
- 2 画面の下部にある **[不足ファイル]** タブで、復元するファイル名の横のチェックボックスを選択します。
- 3 **[復元]** をクリックします。

ヒント: **[すべてを復元]** をクリックすると、**[不足ファイル]** リストのファイルをすべて復元できます。

ローカルアーカイブから古いバージョンのファイルを復元

アーカイブ済みの古いバージョンのファイルを復元するには、ファイルの場所を指定して、**[不足ファイル]** リストに追加します。**[不足ファイル]** リスト内のほかのファイルと同様に、ファイルの復元を行うことができます。

ローカルアーカイブから古いバージョンのファイルを復元するには

- 1 **[ローカルアーカイブ]** タブをクリックします。
- 2 画面の下部にある **[不足ファイル]** タブで、**[参照]** をクリックし、アーカイブの保存場所を指定します。

アーカイブ済みフォルダの名前は次の形式になります。cre
yymmdd_hh-mm-ss_***。yyymmdd はファイルがアーカイブされた日付です。hh-mm-ss はファイルがアーカイブされた時刻です。*** は、実行したアーカイブのタイプを表します。完全アーカイブの場合には Full、クイックアーカイブの場合には Inc になります。

- 3 場所を選択して、**[OK]** をクリックします。

選択した場所に含まれるファイルは、**[不足ファイル]** リストに表示され、復元できる状態になっています。詳細については、「ローカルアーカイブから不足ファイルを復元」を参照してください。

変更ファイルのリストからファイルを削除

アーカイブ済みファイルを監視対象のフォルダから移動したり、削除すると、ファイルは自動的に **[不足ファイル]** リストに表示されます。さらに、アーカイブ済みファイルと監視対象のフォルダ内のファイルが一致しないという警告メッセージが表示されます。ファイルが監視対象のフォルダから移動されたか、意図的に削除された場合、**[不足ファイル]** リストからファイルを削除できます。

変更ファイルのリストからファイルを削除するには

- 1 **[ローカルアーカイブ]** タブをクリックします。
- 2 画面の下部にある **[不足ファイル]** タブで、削除するファイル名の横のチェックボックスを選択します。
- 3 **[削除]** をクリックします。

ヒント: **[すべてを削除]** をクリックすると、**[不足ファイル]** リストのファイルをすべて削除できます。

アーカイブを管理

完全アーカイブとクイックアーカイブに関する情報の概要は、いつでも表示できます。たとえば、現在監視中のデータの量、アーカイブ済みのデータの量、現在監視中でまだアーカイブされていないデータの量などの情報を表示できます。最後のアーカイブや次のアーカイブの日付といったスケジュールに関する情報も表示できます。

アーカイブアクティビティの概要を表示

アーカイブのアクティビティに関する情報は、いつでも表示できます。たとえば、アーカイブ済みのファイルの割合、監視中のデータのサイズ、アーカイブ済みのデータのサイズ、および監視中でまだアーカイブが行われていないデータのサイズを表示できます。最後のアーカイブおよび次のアーカイブの日時を表示することもできます。

バックアップのアクティビティの概要を表示するには

- 1 [ローカルアーカイブ] タブをクリックします。
- 2 画面の上部で、[アカウントの概要] をクリックします。

第 40 章

McAfee EasyNetwork

McAfee EasyNetwork を使用すると、家庭のネットワーク内のコンピュータ同士で安全にファイルを共有したり、簡単にファイルを転送できます。また、プリンタを自動的に共有することもできます。

McAfee EasyNetwork の使用を開始する前に、よく利用する機能について理解することができます。これらの機能の設定と使用方法に関する詳細は、McAfee EasyNetwork のヘルプに書かれています。

この章の内容

機能	266
McAfee EasyNetwork の設定	267
ファイルを共有および送信	273
プリンタを共有	279

機能

McAfee EasyNetwork には、次の機能が搭載されています。

ファイルの共有

McAfee EasyNetwork により、ご使用のコンピュータにあるファイルをローカルネットワーク上のほかのコンピュータと簡単に共有できます。ファイルを共有する場合、ほかのコンピュータに対してそのファイルへの読み取り専用のアクセスを許可します。管理されたネットワークのメンバーとなっているコンピュータ（すべてのアクセス権または管理者としてのアクセス権がある場合）のみがファイルを共有したり、ほかのメンバーによって共有されているファイルにアクセスできます。

ファイルの転送

管理されたネットワークのメンバーであるほかのコンピュータにファイルを送信できます。受信したファイルは、McAfee EasyNetwork の受信ボックスに表示されます。受信ボックスとは、ネットワーク上のほかのコンピュータから受信したすべてのファイルが一時的に保存される場所です。

プリンタの自動共有

管理されたネットワークに参加すると、McAfee EasyNetwork により、ご使用のコンピュータで設定されているすべてのローカルプリンタが自動的に共有されます。そのプリンタの現在の名称が共有プリンタの名称として使用されます。また、ネットワーク上のほかのコンピュータによって共有されているプリンタが検出されるため、それらのプリンタを設定して使用できます。

第 41 章

McAfee EasyNetwork の設定

McAfee EasyNetwork の機能を使用する前に、プログラムを起動し、管理されたネットワークに参加する必要があります。参加手続きをしたあとは、いつでもネットワークから切断できます。

この章の内容

McAfee EasyNetwork を起動.....	268
管理されたネットワークに参加.....	269
管理されたネットワークを切断	272

McAfee EasyNetwork を起動

標準設定では、McAfee EasyNetwork をインストールするとすぐに起動を確認するメッセージが表示されます。また、あとで起動することもできます。

McAfee EasyNetwork を起動

標準設定では、McAfee EasyNetwork をインストールするとすぐに起動を確認するメッセージが表示されます。また、あとで起動することもできます。

McAfee EasyNetwork を起動するには

- [スタート] メニューで [プログラム]、[McAfee] の順に選択し、[McAfee Easy Network] をクリックします。

ヒント: インストール中にデスクトップアイコンとクイック起動アイコンを作成すると、デスクトップの McAfee EasyNetwork アイコンをダブルクリックするか、タスクバーの右側の通知領域に表示される McAfee EasyNetwork アイコンをクリックすることで、McAfee EasyNetwork を起動できます。

管理されたネットワークに参加

McAfee SecurityCenter をインストールすると、コンピュータにネットワークエージェントが追加され、バックグラウンドで実行されます。McAfee EasyNetwork では、ネットワークエージェントは有効なネットワーク接続の検出、共有するローカルプリンタの検出、ネットワークの状態の監視を行います。

現在接続しているネットワーク上で、ネットワークエージェントを実行している別のコンピュータが見つからない場合、ご使用のコンピュータは自動的にネットワークのメンバーになります。また、そのネットワークが信頼されているネットワークかどうかを特定するためのメッセージが表示されます。ネットワークに参加する最初のコンピュータである場合は、ご使用のコンピュータの名前がネットワークの名称に含まれます。ただし、ネットワークの名称はいつでも変更できます。

コンピュータがネットワークに接続すると、現在そのネットワークに接続しているほかのすべてのコンピュータに参加要求が送信されます。要求は、ネットワークで管理権限を持ついずれかのコンピュータにより許可されます。許可を与えるコンピュータは、現在ネットワークに参加しているコンピュータの権限レベルも決定できます。権限レベルには、ゲスト（ファイルの転送のみ可能）またはすべて/管理者（ファイルの転送とファイルの共有が可能）などがあります。McAfee EasyNetwork では、管理者としてのアクセス権を持つコンピュータがほかのコンピュータにアクセスを許可し、権限を管理（コンピュータの権限の引き上げまたは引き下げ）します。すべてのアクセス権を持つコンピュータは、このような管理タスクは実行できません。コンピュータの参加が許可される前に、セキュリティチェックも実行されます。

注: ほかのマカフィー ネットワーク プログラム（McAfee Wireless Network Security や McAfee Network Manager）がインストールされている場合、ネットワークに参加すると、そのコンピュータはこれらのプログラムでも管理されたコンピュータとして認識されます。コンピュータに割り当てられた権限レベルは、すべてのマカフィー ネットワーク プログラムに適用されます。ほかのマカフィー ネットワーク プログラムで適用されるゲスト、すべて、管理者の内容の詳細については各プログラムのユーザガイドやヘルプを参照してください。

ネットワークに参加

McAfee EasyNetwork のインストール後、初めて信頼されているネットワークに接続すると、管理されているネットワークに参加するかどうかを確認するメッセージが表示されます。参加に同意すると、ネットワーク上で管理者としてのアクセス権を持つほかのすべてのコンピュータに要求が送信されます。このネットワーク上でプリンタまたはファイルを共有したり、ファイルを送信およびコピーするには、この要求が許可される必要があります。コンピュータがこのネットワークに接続した最初のコンピュータである場合は、ネットワークの管理権限が自動的に与えられます。

ネットワークに参加するには

- 1 [共有ファイル] ウィンドウで **[はい、今すぐネットワークに参加します]** をクリックします。
このネットワークの管理権限を持つコンピュータにより要求が許可されると、このコンピュータとネットワーク上のほかのコンピュータ間でお互いのセキュリティ設定の管理を許可するかどうかを確認するメッセージが表示されます。
- 2 このコンピュータとほかのコンピュータ間でお互いのセキュリティ設定の管理を許可するには **[はい]** をクリックします。許可しない場合は **[いいえ]** をクリックします。
- 3 セキュリティを確認するダイアログボックスに現在表示されているカードと同じカードが、許可を与えるコンピュータで表示されていることを確認し、**[確認]** をクリックします。

注: セキュリティを確認するダイアログボックスに表示されたものと同じカードが、許可を与えるコンピュータで表示されていない場合、管理されたネットワークのセキュリティが侵害されています。ネットワークに参加するとコンピュータが危険にさらされる可能性があるため、セキュリティを確認するダイアログボックスの **[拒否]** をクリックします。

ネットワークへのアクセスを許可

コンピュータが管理されたネットワークへの参加を要求すると、ネットワーク上で管理者としてのアクセス権を持つほかのコンピュータにメッセージが送信されます。このメッセージに最初に応答したコンピュータが、許可を与えるコンピュータとなります。許可を与えるコンピュータは、コンピュータに許可するアクセス権の種類を決定します。アクセス権の種類には、ゲスト、すべて、管理者があります。

ネットワークへのアクセスを許可するには

- 1 アラートで、次のチェックボックスのいずれかを選択します。
 - **ゲストとしてのアクセスを許可:** ほかのコンピュータにファイルを送信できますが、ファイルの共有はできません。
 - **管理されたすべてのネットワークアプリケーションに対してアクセスを許可:** ファイルの送信と共有を実行できます。
 - **管理されたすべてのネットワークアプリケーションに対して管理者としてのアクセスを許可:** ファイルの送信と共有、ほかのコンピュータへのアクセス許可、ほかのコンピュータの権限レベルの調整を実行できます。
- 2 **[アクセスを許可]** をクリックします。
- 3 セキュリティを確認するダイアログボックスに現在表示されているカードが、コンピュータで表示されていることを確認し、**[確認]** をクリックします。

注: セキュリティを確認するダイアログボックスに表示されたものと同じカードが、コンピュータで表示されていない場合、管理されたネットワークのセキュリティが侵害されています。このコンピュータによるネットワークアクセスを許可すると、ご使用のコンピュータが危険にさらされる可能性があるため、セキュリティを確認するダイアログボックスで **[拒否]** をクリックしてください。

ネットワーク名を変更

標準設定では、ネットワークに最初に参加したコンピュータの名前がネットワークの名称に含まれます。ただし、ネットワークの名称はいつでも変更できます。ネットワークの名称を変更すると、McAfee EasyNetwork に表示されるネットワークの説明が変更されます。

ネットワーク名を変更するには

- 1 **[オプション]** メニューの **[設定]** をクリックします。
- 2 **[設定]** ダイアログボックスの **[ネットワーク名]** ボックスにネットワークの名称を入力します。
- 3 **[OK]** をクリックします。

管理されたネットワークを切断

管理されたネットワークに参加していて、メンバーであることをやめる場合、ネットワークを切断できます。メンバーシップを取り消したあとも、いつでも再度ネットワークに参加できます。ただし、参加が許可され、再度セキュリティチェックを受ける必要があります。詳細については、「**管理されたネットワークに参加** (269 ページ)」を参照してください。

管理されたネットワークを切断

以前に参加した、管理されたネットワークを切断できます。

管理されたネットワークを切断するには

- 1 [ツール] メニューの [ネットワークの切断] をクリックします。
- 2 [ネットワークの切断] ダイアログボックスで、切断するネットワークの名称を選択します。
- 3 [ネットワークの切断] をクリックします。

第 42 章

ファイルを共有および送信

McAfee EasyNetwork により、ご使用のコンピュータにあるファイルをローカルネットワーク上のほかのコンピュータとの間で簡単に共有および送信できます。ファイルを共有する場合、ほかのコンピュータに対してそのファイルへの読み取り専用のアクセスを許可します。管理されたネットワークのメンバーとなっているコンピュータ（すべてまたは管理者としてのアクセス権がある場合）のみがファイルを共有したり、ほかのメンバーコンピュータによって共有されているファイルにアクセスできます。

この章の内容

ファイルを共有	274
ほかのコンピュータにファイルを送信	277

ファイルを共有

McAfee EasyNetwork により、ご使用のコンピュータにあるファイルをローカルネットワーク上のほかのコンピュータと簡単に共有できます。ファイルを共有する場合、ほかのコンピュータに対してそのファイルへの読み取り専用のアクセスを許可します。管理されたネットワークのメンバーとなっているコンピュータ（すべてまたは管理者としてのアクセス権がある場合）のみがファイルを共有したり、ほかのメンバーコンピュータによって共有されているファイルにアクセスできます。フォルダを共有すると、そのフォルダに含まれるすべてのファイルと、そのフォルダのサブフォルダが共有されます。ただし、共有されたあとでフォルダに追加されたファイルは自動的に共有されません。共有されているファイルまたはフォルダが削除されると、これらは自動的に [共有ファイル] ウィンドウから削除されます。ファイルの共有はいつでも停止できます。

共有ファイルにアクセスする方法は 2 つあります。1 つ目の方法は、McAfee EasyNetwork から直接ファイルを開く方法です。2 つ目の方法は、ご使用のコンピュータにファイルをコピーしてから、ファイルを開く方法です。共有ファイルの量が多い場合は、アクセスする共有ファイルを検索できます。

注: McAfee EasyNetwork を使用して共有されるファイルに、Windows Explorer を使用してほかのコンピュータからアクセスすることはできません。McAfee EasyNetwork のファイル共有は、安全な接続を介して実行されます。

ファイルを共有

ファイルを共有すると、そのファイルは、管理されたネットワークのすべてまたは管理者としてのアクセス権を持つすべてのメンバーに対して、自動的に使用可能になります。

ファイルを共有するには

- 1 Windows Explorer で、共有するファイルの場所を特定します。
- 2 Windows Explorer から McAfee EasyNetwork の [共有ファイル] ウィンドウにファイルをドラッグします。

ヒント: [ツール] メニューの [ファイル共有] をクリックしてファイルを共有することもできます。[共有] ダイアログボックスで共有するファイルを保存するフォルダを指定し、ファイルを選択して [共有] をクリックします。

ファイルの共有を停止

管理されたネットワークでファイルを共有している場合、いつでも共有を停止できます。ファイルの共有を停止すると、管理されたネットワークのほかのメンバーはファイルにアクセスできなくなります。

ファイルの共有を停止するには

- 1 [ツール] メニューの [ファイルの共有の停止] をクリックします。
- 2 [ファイルの共有の停止] ダイアログボックスで、共有を停止するファイルを選択します。
- 3 [共有しない] をクリックします。

共有ファイルをコピー

管理されたネットワーク上のコンピュータからご使用のコンピュータに、共有ファイルをコピーできます。以降でファイルの共有が停止されても、コピーしたファイルはご使用のコンピュータに残ります。

ファイルをコピーするには

- McAfee EasyNetwork の [共有ファイル] ウィンドウから、Windows Explorer の特定の場所または Windows のデスクトップにファイルをドラッグします。

ヒント: McAfee EasyNetwork でファイルを選択して、[ツール] メニューの [コピー先] をクリックしても共有ファイルをコピーできます。[フォルダにコピー] ダイアログボックスで、ファイルをコピーするフォルダを選択し、[保存] をクリックします。

共有ファイルを検索

ネットワークのメンバーが共有しているファイルを検索できます。検索条件を入力すると、McAfee EasyNetwork により、対応する検索結果が [共有ファイル] ウィンドウに自動的に表示されます。

共有ファイルを検索するには

- 1 [共有ファイル] ウィンドウで [検索] をクリックします。
- 2 [条件] リストで次のいずれかのオプションをクリックします。
 - 次のすべての単語を含む: [ファイル名またはパス名] リストで指定したすべての単語を含むファイル名またはパス名が検索されます。単語の順序は問いません。
 - 次のいずれかの単語を含む: [ファイル名またはパス名] リストで指定したいずれかの単語を含むファイル名またはパス名が検索されます。

- **次と完全に一致する文字列を含む:** [ファイル名またはパス名] リストで指定した同一の語句を含むファイル名またはパス名が検索されます。
- 3 ファイル名またはパス名の一部またはすべてを [ファイル名またはパス名] リストに入力します。
 - 4 [タイプ] リストで次のいずれかのファイルタイプをクリックします。
 - **すべて:** 共有されているすべてのファイルタイプが検索されます。
 - **文書:** 共有されているすべての文書が検索されます。
 - **画像:** 共有されているすべての画像ファイルが検索されます。
 - **動画:** 共有されているすべての動画ファイルが検索されます。
 - **音声:** 共有されているすべての音声ファイルが検索されます。
 - 5 [開始] リストと [終了] リストで、ファイルが作成された日にちの範囲を示す日付をクリックします。

ほかのコンピュータにファイルを送信

管理されたネットワークのメンバーであるほかのコンピュータにファイルを送信できます。McAfee EasyNetwork は、ファイルを送信する前に、ファイルを受信するコンピュータに十分な空き容量があるかどうかを確認します。

受信したファイルは、McAfee EasyNetwork の受信ボックスに表示されます。受信ボックスとは、ネットワーク上のほかのコンピュータから受信したすべてのファイルが一時的に保存される場所です。ファイルを受信するときに McAfee EasyNetwork を開いていた場合は、ファイルは即座に受信ボックスに表示されます。開いていない場合は、Windows のタスクバーの右側の通知領域にメッセージが表示されます。通知メッセージを表示したくない場合は、無効にできます。受信ボックスに同じ名前のファイルがすでに存在する場合は、新しいファイルの名前の最後に数字が追加されます。ファイルは、ユーザに受け入れられるまで（コンピュータ上のいずれかの場所にコピーされるまで）受信ボックスに保存されます。

ほかのコンピュータにファイルを送信

ファイルを共有していなくても、管理されたネットワーク上のほかのコンピュータに直接ファイルを送信できます。受信側のコンピュータのユーザがファイルを表示するには、ローカルの場所にファイルを保存する必要があります。詳細については、「ほかのコンピュータからファイルを受け入れ（278 ページ）」を参照してください。

ほかのコンピュータにファイルを送信するには

- 1 Windows Explorer で、送信するファイルを見つけます。
- 2 Windows Explorer から McAfee EasyNetwork のアクティブなコンピュータアイコンにファイルをドラッグします。

ヒント: CTRL キーを押しながらファイルを選択すると、1 つのコンピュータに複数のファイルを送信できます。[ツール] メニューの [送信] をクリックし、ファイルを選択して [送信] をクリックしてもファイルを送信できます。

ほかのコンピュータからファイルを受け入れ

管理されたネットワーク上のほかのコンピュータからご使用のコンピュータにファイルが送信された場合、ファイルを受け入れる（コンピュータ上のフォルダに保存する）必要があります。ご使用のコンピュータにファイルが送信されたときに、McAfee EasyNetwork を開いていない場合もしくは最前面で表示していない場合は、タスクバーの右側の通知領域に通知メッセージが表示されます。McAfee EasyNetwork を開いてファイルにアクセスするには、通知メッセージをクリックしてください。

ほかのコンピュータからのファイルを受信するには

- **【受信済み】** をクリックし、McAfee EasyNetwork の受信ボックスから Windows Explorer のフォルダにファイルをドラッグします。

ヒント: McAfee EasyNetwork の受信ボックスでファイルを選択し、**【ツール】** メニューの **【許可】** をクリックしても、ほかのコンピュータからのファイルを受信できます。**【フォルダに保存】** ダイアログボックスで、受信したファイルを保存するフォルダ選択し、**【保存】** をクリックします。

ファイルが送信されたときに通知を受信

管理されたネットワーク上のほかのコンピュータからご使用のコンピュータにファイルが送信されたときに、通知を受信できます。現在 McAfee EasyNetwork を開いていない場合もしくはデスクトップの最前面で表示していない場合は、Windows タスクバーの右側の通知領域に通知メッセージが表示されます。

ファイルが送信されたときに通知を受信するには

- 1 **【オプション】** メニューの **【設定】** をクリックします。
- 2 **【設定】** ダイアログボックスで **【ほかのコンピュータからファイルを受信した場合に通知】** チェックボックスをオンにします。
- 3 **【OK】** をクリックします。

第 43 章

プリンタを共有

管理されたネットワークに参加すると、McAfee EasyNetwork により、ご使用のコンピュータで設定されているすべてのローカルプリンタが自動的に共有されます。また、ネットワーク上のほかのコンピュータによって共有されているプリンタが検出されるため、それらのプリンタを設定して使用できます。

この章の内容

共有プリンタを使用280

共有プリンタを使用

管理されたネットワークに参加すると、McAfee EasyNetwork により、ご使用のコンピュータで設定されているすべてのローカルプリンタが自動的に共有されます。そのプリンタの現在の名称が共有プリンタの名称として使用されます。また、ネットワーク上のほかのコンピュータによって共有されているプリンタが検出されるため、それらのプリンタを設定して使用できます。ネットワーク プリント サーバ (ワイヤレス USB プリントサーバなど) を使用して印刷するようにプリンタドライバを設定している場合、McAfee EasyNetwork はプリンタをローカルプリンタとみなし、このプリンタをネットワーク上で自動的に共有します。プリンタの共有も、いつでも停止できます。

また、McAfee EasyNetwork は、ネットワーク上のほかのすべてのコンピュータにより共有されているプリンタを検出します。まだご使用のコンピュータに接続されていないリモートプリンタが検出されると、最初に McAfee EasyNetwork を開いたときに、[共有ファイル] ウィンドウに **[利用可能なネットワークプリンタ]** リンクが表示されます。これにより、利用可能なプリンタをインストールしたり、ご使用のコンピュータにすでに接続しているプリンタをアンインストールできます。また、ネットワーク上で検出されたプリンタのリストを更新することもできます。

管理されたネットワークに接続していて、まだ参加していない場合は、Windows のプリンタ コントロール パネルから共有プリンタにアクセスできます。

プリンタの共有を停止

プリンタの共有はいつでも停止できます。プリンタをインストールしているメンバーは、このプリンタで印刷できなくなります。

プリンタの共有を停止するには

- 1 [ツール] メニューの **[プリンタ]** をクリックします。
- 2 [ネットワークプリンタの管理] ダイアログボックスで、共有を停止するプリンタの名称をクリックします。
- 3 **[共有しない]** をクリックします。

利用可能なネットワークプリンタをインストール

管理されたネットワークのメンバーである場合、ネットワークで共有されているプリンタにアクセスできます。共有されているプリンタにアクセスするには、そのプリンタで使用されているプリンタドライバをインストールする必要があります。インストールしたあとに、所有者によりプリンタの共有が停止された場合は、このプリンタで印刷できなくなります。

利用可能なネットワークプリンタをインストールするには

- 1 [ツール] メニューの [プリンタ] をクリックします。
- 2 [利用可能なネットワークプリンタ] ダイアログボックスで、プリンタの名称をクリックします。
- 3 [インストール] をクリックします。

第 44 章

リファレンス

「用語集」では、マカフィー製品でよく使用されている用語とその定義について説明します。

「マカフィーについて」には、マカフィー株式会社に関する法的情報が記載されています。

用語集

8

802.11

ワイヤレス LAN 技術の IEEE 標準規格群。802.11 は、ワイヤレスクライアントと基地局間、または 2 つのワイヤレスクライアント間の無線インターフェースの仕様を規定します。802.11 には、802.11a (5GHz 帯で最大 54 Mbps の通信が可能)、802.11b (2.4 GHz 帯で最大 11Mbps の通信が可能)、802.11g (2.4GHz 帯で最大 54 Mbps の通信が可能) などの規格や、すべてのワイヤレスイーサネットのセキュリティ標準規格群である 802.11i が含まれます。

802.11a

ワイヤレス LAN の規格の 1 つで、5GHz 帯で最大 54 Mbps の通信を可能にする 802.11 の拡張仕様。802.11b より伝送速度は高速ですが、通信範囲は狭くなります。

802.11b

ワイヤレス LAN の規格の 1 つで、2.4 GHz 帯で 11 Mbps の通信を可能にする 802.11 の拡張仕様。現在、802.11b はワイヤレスの標準規格とみなされています。

802.11g

ワイヤレス LAN の規格の 1 つで、2.4 GHz 帯で最大 54 Mbps の通信を可能にする 802.11 の拡張仕様。

802.1x

McAfee Wireless Home Network Security ではサポートされていません。有線ネットワークおよびワイヤレスネットワーク用の IEEE 認証規格ですが、多くの場合、802.11 ワイヤレスネットワークと連携して使用されます。この標準規格では、クライアントと認証サーバ間で強力な相互認証を実現できます。また、802.1x では、ユーザごと、セッションごとに WEP キーを動的に変更できるため、静的な WEP キーを使用する際の管理上の負荷やセキュリティリスクを取り除くことができます。

C

Cookie

Web 上で、Web サーバによりクライアントシステムに保存される一連のデータ。同じ Web サイトを再び閲覧すると、ブラウザは Cookie のコピーをサーバに送信します。Cookie は、ユーザを特定して、要求された Web ページをカスタマイズして送信したり、ユーザのアカウント情報を送信したり、その他の管理目的で使用されます。

Cookie を利用することにより、Web サイトの利用者を記憶したり、Web サイトにアクセスした人数、日時、閲覧されたページを記録することができます。また、Cookie を使用すると、Web サイトをユーザの好みに合わせてカスタマイズすることができます。多くの Web サイトでは、特定のページにアクセスするときにユーザ名とパスワードを入力する必要があるため、毎回サインインする手間を省くために、利用者のコンピュータに Cookie が送信されます。ただし、Cookie が悪用される可能性もあります。オンラインの広告会社は、Cookie を利用して利用者がよくアクセスするサイトを調べ、利用者のお気に入りの Web サイトに広告を掲載します。サイトから送信された Cookie を許可する前に、信頼できるサイトかどうか確認してください。

Cookie は合法的な企業にとって情報源となりますが、同時にハッカーにとっても情報源となります。オンラインストアを持つ多くの Web サイトでは、クレジットカードやその他の個人情報を Cookie に保存して、購入手順を簡略化しています。残念ながらセキュリティ上のバグがある可能性があり、その場合、ハッカーは顧客のコンピュータに保存されている Cookie から情報にアクセスすることができます。

D

DNS

Domain Name System の略。階層的なシステムで、インターネット上のホストは、ドメイン名アドレス (bluestem.prairienet.org など) と IP アドレス (192.17.3.4 など) の両方を持ちます。ドメイン名アドレスはユーザにより使用されるもので、自動的に数値 IP アドレスに変換されます。数値 IP アドレスはパケット ルーティング ソフトウェアにより使用されます。DNS 名は、トップ レベル ドメイン (.com、.org、.net など)、セカンド レベル ドメイン (企業、組織、個人のサイト名)、場合によっては 1 つまたは複数のサブドメイン (セカンド レベル ドメイン内のサーバ) で構成されます。「DNS サーバ」および「IP アドレス」も参照してください。

DNS サーバ

Domain Name System サーバの略。ドメイン名システム (DNS) の照会に応答するコンピュータです。DNS サーバは、ホストコンピュータと、ホストコンピュータに対応する IP アドレスのデータベースを保持します。たとえば、apex.com という名前が照会されると、DNS サーバは Apex 社の IP アドレスを返します。ネームサーバともいいます。「DNS」および「IP アドレス」も参照してください。

E

E メール

インターネット、または会社の LAN や WAN で送信されるメッセージ。EXE (実行可能) ファイルまたは VBS (Visual Basic スクリプト) ファイル形式の E メール添付ファイルは、ウイルスやトロイの木馬を運ぶ手段としてますます一般的になりつつあります。

E メールクライアント

E メールアカウント。たとえば、Microsoft Outlook や Eudora など。

ESS (Extended Service Set)

単一のサブネットワークを構築する 2 つ以上のネットワークのセット。

I

IP アドレス

インターネット プロトコル アドレスまたは IP アドレスは点で区切られた 4 つの部分から構成される特有の番号です (例: 63.227.89.66)。大型のサーバから携帯電話を介して通信を行うノートパソコンまで、インターネット上のすべてのコンピュータには特有の IP 番号が割り当てられています。ドメイン名はすべてのコンピュータにはありませんが、IP はすべてのコンピュータにあります。

特殊な IP アドレスの種類を以下に示します。

- ルート不可 IP アドレス: これらは「プライベート IP 領域」とも呼ばれます。これらはインターネット上で使用できない 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: ループバックアドレスは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。これはデバイスに固定で、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、多くの場合、送信者が故意にトラフィックの発信元を偽装していることを意味します。アプリケーション固有の指示を含むパケットがその内容を理解するアプリケーションによって受信されない限り、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。

IP スプーフィング

IP パケット内の IP アドレスを偽装すること。この方法は、セッションハイジャックなどのさまざまな攻撃に使用されます。また、攻撃元を突き止められないように、迷惑メールのヘッダを偽装する場合にも使用されます。

L

LAN (Local Area Network)

比較的狭い範囲のコンピュータネットワーク。ほとんどの LAN は、単一の建物または建物のグループに限定されています。ただし、電話回線および電波を介して、1 つの LAN から、離れた場所にあるほかの LAN に接続できます。この方法で接続される LAN システムは、WAN (Wide Area Network) といいます。ほとんどの LAN では、通常、簡単なハブやスイッチを使用してワークステーションやコンピュータを接続します。LAN の各ノード（個々のコンピュータ）は、それぞれプログラムを実行する CPU を内蔵していますが、LAN 上のどこにあるデータやデバイス（プリンタなど）へもアクセスできます。つまり、データだけでなく、レーザープリンタなど高価なデバイスを多数のユーザで共有できます。また、LAN を使用してユーザ間でコミュニケーションを図ることもできます。たとえば、E メールの送信やチャットによってです。

M

MAC (メディアアクセス制御またはメッセージ認証コード)

メディアアクセス制御については、「MAC アドレス」を参照してください。メッセージ認証コードは、特定のメッセージ (RADIUS メッセージなど) の識別に使用されるコードです。このコードは、リプライ攻撃から保護するための固有の値を含むメッセージコンテンツの、暗号学的に強力なハッシュです。

MAC アドレス (メディアアクセス制御アドレス)

ネットワークにアクセスする物理デバイスに割り当てられた低レベルなアドレス。

Man-in-the-Middle 攻撃 (中間者攻撃)

攻撃者は、公開キーの交換時にメッセージを傍受し、要求された公開キーの代わりに自分のキーを再送します。最初に通信を行った 2 者では、そのまま直接通信を行っているとして認識されます。この攻撃では、クライアントではサーバとして認識され、サーバではクライアントとして認識されるプログラムが使用されます。この攻撃方法は、メッセージに対するアクセス権限を取得するため、またはメッセージを変更して再送するために使用される可能性があります。Man-in-the-Middle 攻撃という名称は、多数の人々がお互いに直接ボールを投げ合う中、中央にいる人物がボールを奪おうとする球技に由来します。

MAPI アカウント

Messaging Application Programming Interface の略。Microsoft 社が発表したインターフェースの仕様で、さまざまなメッセージングアプリケーションおよびワークグループアプリケーション (E メール、ボイスメール、FAX など) を、Exchange クライアントなどの単一のクライアントで利用できるようにします。このような理由から、MAPI は、企業で Microsoft Exchange Server が運用されている場合に企業環境で使用されることが多くなっています。ただし、個人のインターネット E メールに Microsoft Outlook を使用しているユーザも数多くいます。

MSN アカウント

Microsoft Network の略。オンラインサービスやインターネットのポータルサイトです。これは Web ベースのアカウントです。

N

NIC (ネットワークカード)

ノートパソコンやほかのデバイスに差し込み、それらと LAN を接続するためのカード。

P

Password Vault

個人のパスワードを記録できる安全な記録領域。この記憶領域に保存すると、マカフィー製品の管理者またはシステムの管理者を含むほかのユーザは、記録されたパスワードに一切アクセスできません。

PCI ワイヤレス アダプタ カード

デスクトップコンピュータとネットワークを接続します。このカードは、コンピュータ内部の PCI 拡張スロットに差し込みます。

POP3 アカウント

Post Office Protocol 3 の略。多くの個人ユーザがこの種類のアカウントを使用しています。TCP/IP ネットワークで一般的に使用される POP の現在の標準バージョンです。標準の E メールアカウントとしても知られています。

PPPoE

Point-to-Point Protocol Over Ethernet の略。PPPoE は、多くの DSL プロバイダによって使用されています。PPP で広く使用されているプロトコル層および認証を使用し、通常は多対多の接続が行われるイーサネットで一対一の接続を確立します。

R

RADIUS (Remote Access Dial-In User Service)

通常、リモートアクセス時に使用されるユーザ認証用プロトコル。このプロトコルは、元々はダイヤルインのリモート アクセス サーバで使用するために定義されたものですが、現在では、無線 LAN ユーザの共有秘密キーの 802.1x 認証などのさまざまな認証環境で使用されています。

S

SMTP サーバ

Simple Mail Transfer Protocol の略。1 つのコンピュータからネットワーク上のほかのコンピュータにメッセージを送信するための TCP/IP プロトコルです。このプロトコルは、インターネット上で E メールを送信するために使用されます。

SSID (Service Set Identifier)

ワイヤレス LAN のサブシステム内のデバイスに付くネットワーク名。これは、各無線 LAN パケットの先頭に追加される 32 文字の平文です。SSID により各無線 LAN が識別されるため、ネットワークのすべてのユーザは、接続先のアクセスポイントに同じ SSID を設定する必要があります。SSID により、SSID が設定されていないクライアントデバイスからのアクセスを阻止できます。ただし、標準設定では、アクセスポイントは自身の SSID をビーコンに含めて送信します (SSID ブロードキャスト)。SSID ブロードキャストが無効になっていても、ハッカーがデータを傍受して、SSID を検出する可能性があります。

SSL (Secure Sockets Layer)

インターネットを介して個人情報を送信するために Netscape によって開発されたプロトコル。SSL は SSL 接続を介して転送されるデータを暗号化する公開キーを使用することにより機能します。SSL は、Netscape Navigator および Internet Explorer の両方でサポートされ、そして使用されています。また、多くの Web サイトで、クレジットカード番号などのユーザの個人情報を取得する場合には、このプロトコルが使用されています。仕様により、SSL 接続を要求する URL は、http: ではなく https: から始まります。

SystemGuards

SystemGuards は、コンピュータに対する無認可の変更を検出し、変更が行われるとアラートを表示します。

T

TKIP (Temporal Key Integrity Protocol)

WEP の後継にあたる規格で、暗号キーの再利用における WEP セキュリティの弱点が補強されています。TKIP では、10,000 パケットごとに一時キーが変更されます。この動的な配布方法により、ネットワークセキュリティを著しく強化できます。TKIP (セキュリティ) では、まず、クライアントとアクセスポイント間で、128 ビットの一時キーが共有されます。TKIP は、一時キーと (クライアントコンピュータの) MAC アドレスを組み合わせ、比較的大きな 16 オクテットの初期化ベクトルを追加して、データを暗号化するキーを作成します。これにより、各ステーションでは、データの暗号化に異なるキーストリームが使用されます。TKIP は、WEP と同様に、RC4 を使用して暗号化を行います。

U

URL

Uniform Resource Locator。インターネットアドレスの標準形式。

USB ワイヤレス アダプタ カード

拡張可能なプラグ アンド プレイのシリアルインターフェース。このインターフェースを使用すると、キーボード、マウス、ジョイスティック、プリンタ、スキャナ、ストレージデバイス、ビデオ会議用カメラなどの周辺機器に対して、標準的なワイヤレス接続を低コストで実現できます。

V

VPN (Virtual Private Network)

公衆回線を使用してノードが再結合されているネットワーク。たとえば、多くのシステムで、インターネットをデータ転送手段として使用するネットワークを作成できます。これらのシステムでは、暗号化などのセキュリティメカニズムを使用して、認証されたユーザのみにアクセスを許可し、データが傍受できないように設定されています。

W

Web バグ

自身を HTML ページに組み込むことで、不正な送信元による Cookie の設定を可能にする小さなグラフィックファイル。これらの Cookie により、不正な送信元に情報が転送される場合があります。Web バグは、Web ビーコン、ピクセルタグ、クリア GIF、透過 GIF と呼ばれます。

WEP (Wired Equivalent Privacy)

802.11 標準規格の一部として定義された暗号および認証プロトコル。初期のバージョンは RC4 に基づいて暗号化しますが、重大な弱点があります。WEP では、電波を介して転送されるデータを暗号化することにより、セキュリティの保護を行っています。ただし、最近では、WEP セキュリティに問題があることが判明しています。

Wi-Fi (Wireless Fidelity)

802.11b、802.11a、デュアルバンドなどのすべての種類の 802.11 ネットワークについて言及する際に一般的に使用される用語。この用語は、Wi-Fi Alliance によって使用されています。

Wi-Fi Alliance

ワイヤレス機器およびソフトウェアの主要メーカーによって構成される団体。この団体の目標は、802.11 ベースのすべての製品の互換性の認定、および 802.11 ベースのワイヤレス LAN 製品のすべての市場に、Wi-Fi を世界的なブランド名として広めることです。この団体は、相互互換性や業界の成長の促進を望むメーカーに対して、協会、テストラボ、情報交換の場として機能します。

すべての 802.11a/b/g 製品が Wi-Fi と呼ばれていますが、Wi-Fi Alliance のテストをパスした製品のみが、「Wi-Fi Certified」（登録商標）製品と呼ばれることができます。テストをパスした製品のパッケージには、「Wi-Fi Certified」と記された識別用シールを貼付し、使用する周波数帯を記載することが義務付けられています。この団体は、以前は Wireless Ethernet Compatibility Alliance (WECA) という名前でしたが、Wi-Fi ブランド名をより広めるために、2002 年 10 月に今の名前に変更されました。

Wi-Fi Certified

Wi-Fi Alliance によってテストされ、「Wi-Fi Certified」（登録商標）として承認された製品は、他社製品との互換性が保証された製品として認定されています。「Wi-Fi Certified」という認定が与えられた製品では、同様に認定されているすべてのブランドのアクセスポイントおよびクライアントハードウェアを使用できます。ただし、一般的に、同一の無線周波数を使用する Wi-Fi 製品（たとえば、2.4GHz の 802.11b または 11g、5GHz の 802.11a）は、「Wi-Fi Certified」認定が与えられていない製品とも動作します。

WPA (Wi-Fi Protected Access)

既存のまたはこれから登場するワイヤレス LAN システムに対して、データ保護およびアクセス制御のレベルを強化する標準規格。既存のハードウェアでは、ソフトウェアアップグレードとして使用できるよう作られています。WPA は、IEEE 802.11i 標準規格に対応しています。インストールが適切に行われると、ワイヤレス LAN のセキュリティレベルが強化され、確実にデータを保護し、ネットワークへのアクセスを認証ユーザのみに制限できるようになります。

WPA-PSK

企業クラスの強力なセキュリティ機能を必要とせず、認証サーバへのアクセス権のないホームユーザに対して設計された特別な WPA モード。このモードでは、ホームユーザは、手動で開始パスワードを入力して WPA-PSK モードを有効にします。各ワイヤレスコンピュータおよびアクセスポイントのパスワードは、定期的に変更する必要があります。「WPA2-PSK」および「TKIP」も参照してください。

WPA2

「WPA」も参照してください。WPA2 は WPA セキュリティ標準の更新バージョンで、IEEE 802.11i 標準に基づいています。

WPA2-PSK

「WPA-PSK」および「WPA2」も参照してください。WPA2-PSK は WPA-PSK と同様に、WPA2 標準に基づいています。WPA2-PSK の主な機能は、デバイスで複数の暗号化モード (AES、TKIP など) を同時にサポートできる点です。古いデバイスの場合、同時にサポートできる暗号化モードは通常 1 種類であるため、すべてのクライアントで同じ暗号化モードを使用する必要があります。

アーカイブ

監視対象のファイルのコピーをローカルの CD、DVD、USB ドライブ、外部ハードディスク、ネットワークドライブに作成すること。

アクセスポイント (AP)

802.11 クライアントをローカル エリア ネットワーク (LAN) につなげるネットワークデバイス。アクセスポイントを使用すると、ワイヤレスネットワークの通信範囲を拡張できます。ワイヤレスルータのことを指す場合もあります。

イベント

0.0.0.0 からのイベント

0.0.0.0 からのイベントが発生した場合には、次の 2 つの原因が考えられます。まず最初に考えられる原因は、何らかの理由で使用中のコンピュータが不正なパケットを受信したことです。インターネットは常に 100% 信頼できるものではなく、不適切なパケットが発生することもあります。ファイアウォールは、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、送信元 IP がスプーフ、つまり偽装されているときに起こります。パケットが偽装されている場合、誰かがトロイの木馬を探してコンピュータをスキャンしている可能性があります。このような行為は、ファイアウォールによってブロックされます。

127.0.0.1 からのイベント

送信元 IP が 127.0.0.1 になっているイベントが発生する場合があります。この IP は特別なアドレスで、ループバックアドレスといいます。

どのコンピュータを使用しているとしても、127.0.0.1 は常に使用しているローカルコンピュータを指します。このアドレスは「localhost」ともいいます。これは、コンピュータ名 localhost は常に IP アドレス 127.0.0.1 と解釈されるためです。自分のコンピュータに自分自身が侵入しようとしているのでしょうか？トロイの木馬やスパイウェアがコンピュータに侵入したのでしょうか？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、多くの個人向けのメールサーバや Web サーバは、<http://localhost/> などからアクセスできる Web インターフェースを介して、設定を行うことができます。

ただし、ファイアウォールはこのようなプログラムからのトラフィックを許可しているので、127.0.0.1 からのイベントが発生している場合、送信元 IP アドレスがスプーフ（偽装）されている可能性があります。パケットが偽装されている場合、誰かがトロイの木馬をスキャンしている可能性があります。この行為は、ファイアウォールによってブロックされます。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 アドレス】リストに追加する必要があります。こ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かどうかをファイアウォールが判断できない方法で通信を行います。

Netscape 6.2 の場合、127.0.0.1 を信用しないと、友人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プログラム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、ファイアウォールの【信用 IP アドレス】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する必要があります。

【信用 IP アドレス】 リストに 127.0.0.1 を追加して問題が解決した場合には、次の 2 つの選択肢を検討する必要があります。127.0.0.1 を信用すると、プログラムは動作しますが、スプーフ攻撃を受けやすくなります。このアドレスを信用しないと、プログラムは動作しませんが、スプーフ攻撃などの悪意のあるトラフィックからは従来どおり保護されます。

同じ LAN 上のコンピュータからのイベント

ほとんどの企業の LAN 設定の場合、LAN 上のコンピュータはすべて信用できます。

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内のものなので、ほとんどの場合は信用できます。

192.168 というブロックは 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、192.168.255.255 を【信用 IP アドレス】リストに追加してください。これにより、192.168.xxx.xxx ブロック全体が信用されます。

プライベートネットワーク以外で、これらの IP アドレス範囲からのイベントが発生した場合、送信元 IP アドレスが偽装されている可能性があります。パケットが偽装されている場合、誰かがトロイの木馬を探し回ってスキャンしている可能性があります。この行為は、ファイアウォールによってブロックされます。

プライベート IP アドレスはインターネット上の IP アドレスと異なり、これらのイベントをレポートしても効果はありません。

インターネット

インターネットは、非常に多くの相互接続ネットワークから構成されており、TCP/IP プロトコルを使用して場所を特定し、データを転送します。インターネットは、アメリカ国防総省が設立した大学コンピュータのリンクから発展し（1960 年代後半から 1970 年代前半にかけて）、ARPANET と呼ばれていました。今日のインターネットは、約 100,000 の独立したネットワークから構成されるグローバルネットワークです。

イントラネット

プライベートネットワーク。通常は企業内にあり、インターネットと非常に似た働きをします。学生や従業員が学外または社外にあるコンピュータからイントラネットにアクセスすることが一般的になりました。ファイアウォール、ログイン手続き、パスワードを使用してセキュリティを確保しています。

ウオードライバー

ノートパソコン、特殊なソフトウェア、ハードウェアなどを車に積み、街や住宅街、オフィス街などを移動しながら、ワイヤレス LAN トラフィックを傍受する侵入者のこと。

オンライン バックアップ リポジトリ

バックアップ後に監視中ファイルが保存されるオンラインサーバ上の場所。

キー

2 つのデバイス間で通信を認証するために使用される一連の文字または数字。暗号キーとも言います。両方のデバイスがキーを持っている必要があります。「WEP」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2-PSK」も参照してください。

キーワード

複数のファイルに関連性を持たせるために、バックアップ済みファイルに割り当てる言葉。ファイルにキーワードを割り当てると、インターネットに公開しているファイルを簡単に検索できます。

クイックアーカイブ

完全アーカイブまたはクイックアーカイブの最終実行時以降に変更された監視対象のファイルのみをアーカイブすること。

クライアント

コンピュータまたはワークステーション上で稼動し、サーバを使用して作業を実行するアプリケーション。たとえば、E メールクライアントは、Eメールの送受信を可能にするアプリケーションです。

コンテンツの格付けグループ

ユーザが属する年齢グループ。コンテンツは、ユーザが属するコンテンツの格付けグループに基づいて格付け（利用が許可、またはブロック）されます。コンテンツの格付けグループには、幼児、子供、10代前半、10代後半、成年があります。

サーバ

ほかのコンピュータ上で動作しているソフトウェアに特定のサービスを提供するコンピュータまたはソフトウェア。インターネットプロバイダー（ISP）の「メールサーバ」は、ISPのユーザ全員の受信メールと送信メールを処理するソフトウェアです。LAN上のサーバは、ネットワーク上のプライマリノードを構成するハードウェアです。特別なサービスやデータを提供するソフトウェアや、接続しているすべてのクライアントコンピュータに機能を提供するソフトウェアがインストールされている場合があります。

サービス拒否

サービス拒否（DoS）攻撃を受けると、個人や企業がインターネット上で通常使用できるサービスが使用不能になります。一般的に、サービスが使用不能な状態とは、Eメールなど特定のネットワークサービスが利用できない状態、またはすべてのネットワーク接続およびサービスが一時的に使用できなくなる状態を指します。最悪の場合、何百万人ものユーザがアクセスするWebサイトが一時的に停止してしまう可能性があります。また、サービス拒否攻撃を受けると、コンピュータシステムのプログラムおよびファイルが破壊される場合もあります。サービス拒否攻撃は、通常、悪意のあるユーザによって意図的に実行されますが、偶発的に発生する場合があります。サービス拒否攻撃は、コンピュータシステムに対するセキュリティ侵害の一種ですが、情報の盗難やセキュリティ上の被害が発生することはめったにありません。ただし、個人または企業がこのような攻撃を受けた場合、回復には多大な時間と費用がかかる可能性があります。

スクリプト

スクリプトにより、ファイルが作成、コピー、削除される場合があります。また、Windowsレジストリが開かれる場合もあります。

ドメイン

ネットワーク接続のアドレス。階層的な形式で、次のようにアドレスの所有者を表します：サーバ組織の種類。たとえば、www.whitehouse.govは、ホワイトハウスのWebサーバを指し、米国政府に属していることを表します。

トロイの木馬

トロイの木馬は、便利なアプリケーションを装うプログラムです。トロイの木馬は自己複製しないためウイルスではありませんが、破壊活動を行う場合があります。

ネットワーク

複数のコンピュータを接続すると、ネットワークが確立されます。

ネットワークドライブ

複数のユーザが共有するネットワーク上のサーバに接続されているディスクまたはテープドライブ。ネットワークドライブはリモートドライブと呼ばれることもあります。

ネットワーク地図

McAfee Network Manager では、家庭のネットワーク上のコンピュータおよびコンポーネントに関する情報をグラフィカルに表示できます。

ノード

ネットワークに接続された 1 台のコンピュータ。

パスワード

自分のコンピュータや特定のプログラム、Web サイトにアクセスするときに使用するコード（通常は英数字）。

バックアップ

監視対象のファイルのコピーを作成し、安全なオンラインサーバ上に保存すること。

バッファオーバーフロー

バッファオーバーフローは、不審なプログラムまたはプロセスがコンピュータのバッファ（データの一時的な記憶領域）の制限を越えるデータを保存しようとしたときに発生します。バッファオーバーフローが発生すると、隣接するバッファ内の有効なデータが壊されたり上書きされたりします。

パレンタルコントロール

パレンタルコントロールでは、コンテンツのレベルを設定し、ユーザが表示できる Web サイトとコンテンツを制限できます。また、インターネットの使用時間制限を設定し、ユーザがインターネットにアクセスできる時間を指定できます。さらに、特定の Web サイトへのアクセスを全体的に制限したり、年齢グループとそれぞれのグループで決められたキーワードに基づいてアクセスを許可またはブロックできます。

ファイアウォール

プライベートネットワークに対する不正アクセスを防止するために設計されたシステム。ファイアウォールはハードウェアおよびソフトウェアのどちらの形式でも実装できます。また、この 2 つを組み合わせることもできます。ファイアウォールは、インターネット（特にイントラネット）に接続されたプライベートネットワークに対する不正アクセスを防止するためによく使用されます。イントラネットに出入りするメッセージはすべてファイアウォールを通過します。ファイアウォールでは、各メッセージが検査され、指定されたセキュリティ基準を満たしていないメッセージはブロックされます。ファイアウォールは個人情報保護のための防御の最初の障壁と考えられています。データを暗号化すると、さらにセキュリティを強化できます。

フィッシング詐欺

クレジットカード番号、ユーザ ID、パスワードなど、重要な情報を盗み出す詐欺です。送信元をインターネットプロバイダ、銀行、オンラインショップに見せかけた E メールがユーザに送信されます。E メールは、特定のリストや、なんらかのリストを使ってユーザに送信されます（実際に受信者の何割かがその企業のサービスを使用していることを見込んで行われます）。

ブラウザ

ハイパーテキスト転送プロトコル（HTTP）を使用し、インターネットを通じて Web サーバに要求を送信するクライアントプログラム。Web ブラウザは、ブラウザユーザに対してコンテンツをグラフィック表示します。

ブラックリスト

悪意があるとみなされる Web サイトのリスト。詐欺目的で運営されている Web サイトや、ブラウザの脆弱性を攻撃してユーザに怪しいプログラムを送信する Web サイトなどがブラックリストに含まれます。

ブルートフォース攻撃

総当たり攻撃ともいいます。アプリケーションプログラムを使用して、暗号化されたデータ（パスワードなど）を復号化するために総当たりで調べる方法です。高度な技術は使用されません。泥棒があらゆる数字の組み合わせを試しながら金庫を破る場合のように、ブルートフォースクラッキングを行うアプリケーションは、考えられるすべての文字の組み合わせを順番に試行します。この方法では、暗号は確実に解読できますが、非常に時間がかかります。

プロキシ

1 つのネットワークアドレスだけを外部サイトに公開し、ネットワークとインターネットの間の障壁として機能するコンピュータ（またはそのコンピュータ上で動作するソフトウェア）。プロキシは、内部のすべてのコンピュータの仲介役として機能することにより、インターネットへのアクセスを提供しながら、ネットワーク ID を保護します。「プロキシサーバ」も参照してください。

プロキシサーバ

ローカルエリアネットワーク（LAN）とのインターネットトラフィックを管理するファイアウォールコンポーネント。プロキシサーバでは、人気のある Web ページなど、頻繁に要求されるデータを提供することにより、パフォーマンスを向上できます。また、著作権で保護されたファイルに対する不正なアクセス要求など、所有者が不適切であると見なした要求をフィルタリングし、破棄することができます。

プロトコル

2 つのデバイス間でデータ転送を行うための取り決め。ユーザとしてプロトコルについて知っておかなければならないのは、コンピュータまたはデバイスがほかのコンピュータと通信を行うには、正しいプロトコルがサポートされている必要があることです。プロトコルは、ハードウェアまたはソフトウェアのいずれかで実装できます。

ヘッダ

ヘッダは、メッセージのライフサイクルを通してメッセージに追加される情報です。ヘッダは、インターネットソフトウェアにメッセージの配信方法を通知します。ここでは、メッセージに対する返信が送信され、E メールメッセージに対する固有の識別子、およびその他の管理情報が送信されます。ヘッダフィールドの例には、To、From、CC、Date、Subject、Message ID、および Received があります。

ポート

情報がコンピュータに入ったりコンピュータから出たりする場所。たとえば、従来のアナログモデムはシリアルポートに接続されています。TCP/IP 通信のポート番号は、トラフィックをアプリケーション固有のストリームに分割するときに使用される仮定の値です。どのポートに接続しようとしているかプログラムがわかるように、ポートは SMTP や HTTP などの標準プロトコルに割り当てられます。TCP パケットの送信先ポートは、検索中のアプリケーションまたはサーバを示します。

ホットスポット

不特定多数のモバイル利用者に対し、ワイヤレスネットワークを介してブロードバンド ネットワーク サービスを提供するアクセスポイント (AP) が設置されている場所。通常、ホットスポットは、空港、駅、図書館、桟橋、会議場、ホテルなど、人が集まる場所に設置されています。一般的に、ホットスポットの通信範囲は広くありません。

ポップアップ

コンピュータの画面で、ウィンドウの最前面に表示される小さいウィンドウ。ポップアップウィンドウは、多くの場合、Web ブラウザで広告を表示するために使用されます。マカフィーは、ブラウザが Web ページを読み込むときに自動的に読み込まれるポップアップウィンドウをブロックします。ユーザがリンクをクリックしたことにより読み込まれるポップアップウィンドウは、ブロックされません。

ホワイトリスト

詐欺サイトではないとみなされ、アクセスが許可された Web サイトのリスト。

ライブラリ

McAfee Data Backup ユーザがファイルを公開するオンライン上のストレージ領域。ライブラリは、インターネットにアクセス可能なすべてのユーザがアクセスできるインターネット上の Web サイトです。

リアルタイムスキャン

ユーザまたはコンピュータによりアクセスされたときにファイルがスキャンされ、ウイルスやその他のアクティビティの有無が確認されます。

ルータ

1 つのネットワークから別のネットワークにパケットを転送するネットワークデバイス。ルータは、内部のルーティングテーブルに基づいて受信パケットをそれぞれ解読し、転送方法を決定します。送信パケットをルータ上のどのインターフェースへ転送するかは、送信元および宛先アドレスだけでなく、負荷、混雑状況、通信状態などの現在のトラフィックの状況なども組み合わせて決定されます。ルータという言葉は、アクセスポイントを指す場合もあります。

ローミング

サービスや接続が中断されることなく、1 つのアクセスポイントの通信範囲から別のアクセスポイントの通信範囲に移動できる機能。

ワーム

「ワーム」は自己複製を行うウイルスで、動作中のメモリに常駐し、E メールを使用して自身のコピーを送信します。ワームは自らの複製を作成してシステムリソースを消費します。それが原因で、パフォーマンスが低下したり、タスクが中断されたりします。

ワイヤレスアダプタ

コンピュータやほかのデバイスが、ワイヤレスネットワークに必要なワイヤレスルータと通信できるようにするための回路が備わっているアダプタ。ワイヤレスアダプタは、ハードウェアデバイスの主要回路に組み込まれているか、デバイスの適切なポートに挿入するアドオンとして提供されています。

圧縮

データ（ファイル）の保存または転送時に、容量を最小化するためにデータ（ファイル）を圧縮するプロセス。

暗号化

テキスト形式のデータをコード化する処理。解読方法を知らなければ読むことができないように変換します。

暗号文

暗号化されたデータ。暗号文は、暗号キーを使用して平文に変換（復号化）されない限り解読できません。

画像分析

不適切な可能性のある画像の表示をブロックします。画像は、成年グループのメンバー以外のすべてのユーザに対してブロックされます。

怪しいプログラム (PUP)

怪しいプログラム (PUP) とは、無断でデータを収集して転送するスパイウェア、アドウェア、その他のプログラムなどです。

外部ハードディスク

コンピュータケースの外部に存在するハードディスク。

隔離

不審なファイルが検出されると、これらのファイルは隔離されます。そのあとに、適切な対応をとることができます。

完全アーカイブ

監視するファイルタイプと場所の設定に従って、データを完全にアーカイブすること。

監視するファイルタイプ

監視場所内にあり、McAfee Data Backup がバックアップまたはアーカイブするファイルタイプ（たとえば、.doc、.xls など）。

監視場所

McAfee Data Backup が監視するコンピュータ上のフォルダ。

管理されたネットワーク

家庭のネットワークには、2 種類のメンバーがあります。管理されたメンバーと、管理されていないメンバーです。管理されたメンバーは、ネットワーク上のほかのコンピュータに対して、マカフィーによる保護の状態の監視を許可します。一方、管理されていないメンバーはこれを実行できません。

共有

選択されたバックアップ済みファイルに対するアクセスを E メールを受信者に一定期間許可する操作。ファイルを共有すると、バックアップ済みのファイルのコピーが指定した E メールを受信者に送信されます。受信者は、ファイルが共有されていることを示す E メールメッセージを McAfee Data Backup から受信します。また、E メールには共有ファイルへのリンクが含まれています。

共有秘密キー

「RADIUS」も参照してください。RADIUS メッセージの重要な部分を保護します。この共有秘密キーは、認証コードと認証サーバ間で、保護された形式で共有されるパスワードです。

公開

バックアップ済みファイルをインターネット上で使用可能にすること。

辞書攻撃

リスト内の多数の単語を試すことにより、パスワードを割り出す攻撃。この攻撃では、すべての組み合わせを手動で試す方法ではなく、自動的にパスワードを特定するツールが使用されます。

重点監視する場所

McAfee Data Backup が変更状況を監視するコンピュータ上のフォルダ（すべてのサブフォルダを含む）。重点監視する場所を設定した場合、McAfee Data Backup は、このフォルダとサブフォルダ内で監視対象のファイルタイプをバックアップします。

帯域幅

一定時間内に転送可能なデータの量。デジタルデバイスの場合、帯域幅は通常、ビット/秒 (bps) またはバイト/秒で表します。アナログデバイスの場合、帯域幅はサイクル/秒またはヘルツ (Hz) で表します。

統合ゲートウェイ

アクセスポイント、ルータ、およびファイアウォールの機能が統合されたデバイス。セキュリティ強化機能およびブリッジ機能が搭載されている場合もあります。

同期化

バックアップ済みファイルとローカルコンピュータ上のファイルとの不一致を解決すること。オンライン バックアップ リポジトリ内のファイルが別のコンピュータにあるファイルよりも新しい場合は、ファイルを同期化します。同期化を行うと、コンピュータ上のファイルのコピーがオンライン バックアップ リポジトリ上のファイルで更新されます。

認証

個人を識別する手段で、通常はユーザ名とパスワードに基づいて行われます。認証では、個人が利用者本人であるかどうかの確認は行われますが、アクセス権限の確認は行われません。

標準の E メールアカウント

多くの個人ユーザがこの種類のアカウントを使用しています。「POP3 アカウント」も参照してください。

不正アクセスポイント

企業により承認されていないアクセスポイント。問題は、不正アクセスポイントが、LAN (または無線 LAN) のセキュリティポリシーに準拠しないことが多いことです。不正アクセスポイントは、企業ネットワークにオープンで保護されていないインターフェースを作り出し、物理的に管理できない外部からのアクセスを可能にしてしまいます。

適切に保護されている無線 LAN では、不正ユーザによるものより不正アクセスポイントによる被害の方が大きくなります。有効な認証機構が使用されている場合は、認証されていないユーザが無線 LAN へのアクセスを試行しても、企業の機密情報を盗み出すことはできません。ただし、従業員またはハッカーが不正アクセスポイントに接続した場合は、大きな問題が生じます。不正アクセスポイントの存在は、802.11 対応デバイスを使用する誰もが企業ネットワークへのアクセスを可能にします。これにより、機密情報が盗まれる可能性が高くなります。

部分的に監視する場所

McAfee Data Backup が変更状況を監視しているコンピュータ上のフォルダ。部分的に監視する場所を設定した場合、McAfee Data Backup は、このフォルダ内で監視対象のファイルタイプをバックアップします。ただし、サブフォルダは含まれません。

復元

オンライン バックアップ リポジトリまたはアーカイブからファイルのコピーを取得すること。

平文 (ひらぶん)

暗号化されていないメッセージ。

無線 LAN (Wireless Local Area Network)

「LAN」も参照してください。無線 LAN は、ワイヤレス機器を使用して接続されるローカル エリア ネットワークです。ネットワークケーブルではなく、高周波の電波を使用して、ノード間の通信を行います。

マカフィーについて

McAfee, Inc. は、カリフォルニア州サンタ クララに本拠地を置く、不正侵入防止とリスク マネジメントのリーディング カンパニーです。マカフィーは、世界中で使用されているシステムとネットワークの安全を実現する先進的で実績のあるソリューションとサービスを提供しています。個人ユーザをはじめ、企業、官公庁・自治体、ISP など様々なユーザは、マカフィーの卓越したセキュリティ ソリューションを通じて、ネットワークを通じた攻撃や破壊活動を阻止し、またセキュリティ レベルを絶えず管理し、改善することができます。

著作権

Copyright © 2006 McAfee, Inc. All Rights Reserved. この資料のいかなる部分も、McAfee, Inc. 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。McAfee および McAfee の製品名は、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。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。

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・オーケストレイター、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。

索引

8

802.11	285
802.11a	285
802.11b	285
802.11g	285
802.1x	285

C

Cookie	286
Cookie を使用する目的	218
Cookie 受け入れリストを変更	237

D

DNS	286
DNS サーバ	286

E

E メール	286
E メールクライアント	287
E メールとメッセージャーの設定パネルを 表示	19
E メールとメッセージャーの保護について ..	19
E メールのフィルタリングレベルを変更	194
E メールメッセージのフィルタリングを変更	194
E メール保護の設定	89, 107
E メール保護を使用	88
E メール保護を無効化	88
E メール保護を有効化	88
ESS (Extended Service Set)	287

H

HackerWatch チュートリアルを起動	174
------------------------------	-----

I

IP アドレス	287
IP スプーフィング	287

L

LAN (Local Area Network)	288
--------------------------------	-----

M

MAC (メディアアクセス制御またはメッセージ 認証コード)	288
MAC アドレス (メディアアクセス制御アドレ ス)	288
Man-in-the-Middle 攻撃 (中間者攻撃) ..	288
MAPI アカウント	288
McAfee Data Backup	249
McAfee EasyNetwork	265
McAfee EasyNetwork の設定	267
McAfee EasyNetwork を起動	268
McAfee Internet Security	7
McAfee Network Manager	51
McAfee Network Manager のアイコンについ て	53
McAfee Personal Firewall	111
McAfee Privacy Service	219
McAfee QuickClean	41
McAfee QuickClean の機能について	42
McAfee QuickClean を使用	45
McAfee SecurityCenter	9
McAfee SecurityCenter アイコンについて ..	13
McAfee SecurityCenter のオプションの設定	23
McAfee SecurityCenter の設定パネルを表 示	22
McAfee SecurityCenter を開いてその他の機 能を使用	13
McAfee SecurityCenter を使用	11
McAfee SecurityCenter 情報を表示	22
McAfee Shredder	47
McAfee Shredder で不要なファイルを消去 ..	49
McAfee Shredder の機能について	48
McAfee Shredder を使用	50
McAfee SpamKiller	175
McAfee SpamKiller ツールバーから迷惑メー ルまたは非迷惑メールとしてメッセージを マーク	210
McAfee SpamKiller ツールバーから友人を手 動で追加	188

McAfee SpamKiller を保守	207
McAfee SystemGuards について	80
McAfee SystemGuards の設定	79
McAfee SystemGuards を使用	78
McAfee SystemGuards を無効化	78
McAfee SystemGuards を有効化	78
McAfee VirusScan	69
McAfee VirusScan は E メール添付ファイル をスキャンしますか?	107
McAfee VirusScan は Zip で圧縮されたファ イルをスキャンしますか?	107
McAfee VirusScan を管理	97
MSN アカウント	288

N

Netscape、Firefox、または Opera ブラウザ で McAfee VirusScan を使用できますか?	106
NIC (ネットワークカード)	289

P

Password Vault	289
Password Vault にパスワードを追加	246
Password Vault のパスワードをリセット	248
Password Vault のパスワードを削除	247
Password Vault のパスワードを変更	246
Password Vault をセットアップ	246
PCI ワイヤレス アダプタ カード	289
ping 要求の設定	131
POP3 アカウント	289
POP3 または MSN/Hotmail Web メールアカ ウントを追加	180
POP3 または MSN/Hotmail Web メールアカ ウントを編集	182
POP3、MSN/Hotmail、および MAPI のアカ ウントとは何ですか?	216
PPPoE	289

R

RADIUS (Remote Access Dial-In User Service)	289
--	-----

S

SMTP サーバ	289
SSID (Service Set Identifier)	290
SSL (Secure Sockets Layer)	290
SystemGuards	290

T

TKIP (Temporal Key Integrity Protocol)	290
---	-----

U

URL	290
USB ワイヤレス アダプタ カード	290

V

VPN (Virtual Private Network)	291
-------------------------------------	-----

W

Web サイトによる Cookie の設定をブロック	238
Web サイトによる Cookie の設定を許可	237
Web サイトをブロック	230, 234
Web サイトを許可	222, 234
Web バグ	291
Web バグをブロック	243
Web メールアカウントのフィルタリングされた メッセージを管理	185
Web メールアカウントを管理	179
Web メールアカウントを削除	184
Web メールアカウントを追加	180
Web メールアカウントを変更	182
Web メールフィルタリングを管理	185
Web メールフィルタリングを無効化	185
Web メールフィルタリングを有効化	185
WEP (Wired Equivalent Privacy)	291
Wi-Fi (Wireless Fidelity)	291
Wi-Fi Alliance	291
Wi-Fi Certified	291
Windows Explorer をスキャン	93
Windows 用 SystemGuards について	82
WPA (Wi-Fi Protected Access)	292
WPA2	292
WPA2-PSK	292
WPA-PSK	292

あ

アーカイブ	292
アーカイブ ファイル タイプの設定	253
アーカイブアクティビティの概要を表示	264
アーカイブオプションの設定	252
アーカイブに対する暗号化と圧縮を無効化	255
アーカイブの保存場所を変更	254
アーカイブを管理	264

アーカイブを手動で実行	257
アーカイブ済みファイルを検索	260
アーカイブ済みファイルを使用	259, 261
アーカイブ済みファイルを復元	262
アーカイブ済みファイルを並べ替え	260
アーカイブ対象から除外	254
アーカイブ対象を追加	252
アクセスポイント (AP)	292
アドレス帳から手動でインポート	190
アドレス帳を削除	191
アドレス帳を追加	190
アドレス帳を編集	191
アラートについて	118
アラートのオプションの設定	32
アラートを管理	104
アラートを使用	117
イベント	293
イベントログの設定	162
イベントログを記録	153, 159, 160, 162
イベントを表示	101
インストールされている製品の情報を表示	22
インターネット	294
インターネットセキュリティについての確認	173
インターネットでの情報を保護	241
インターネットとネットワークの設定パネルを 表示	18
インターネットとネットワークの保護について	18
インターネットトラフィックを監視	169, 170
インターネットトラフィックを追跡	166, 167, 168
イントラネット	294
ウイルスの詳細情報	40
ウイルスを駆除/削除できません	108
ウイルス対策を管理	73
ウイルス対策を使用	74
ウイルス対策を無効化	74
ウイルス対策を有効化	75
ウォードライバー	294
オンライン バックアップ リポジトリ	294

か

キー	294
キーワード	295
キーワードスキャンを無効化	232
キーワードにより Web サイトをブロック	222, 232
クイックアーカイブ	295

クライアント	295
ゲーム中にアラートを表示	121
コンテンツの格付けグループ	295
コンピュータとファイルの設定パネルを表示	17
コンピュータとファイルの保護について	17
コンピュータのネットワーク情報を取得	167
コンピュータの登録情報を取得	166
コンピュータの保護の状態の監視を停止	65
コンピュータの保護の状態を監視	64
コンピュータをクリーニング	43, 45
コンピュータを以前の設定に復元	39
コンピュータを自動的に保守	37
コンピュータを手動スキャン	91
コンピュータを手動で保守	38
コンピュータ接続を管理	151
コンピュータ接続を禁止	156
コンピュータ接続を信用	152
コンポーネントが見つからないかまたは壊れ ています	109

さ

サーバ	295
サービスが更新されたら自動的に更新をイン ストールして通知	28
サービス拒否	295
システム サービス ポートの設定	148
システム サービス ポートを削除	150
システム サービス ポートを変更	149
システムサービスを管理	147
スキャンするファイルの種類を指定	94
スキャンする場所を指定	95
スキャンをスケジュール	95
スキャンを実行する際は、インターネットに接 続する必要はありますか?	106
スクリプト	295
スクリプトスキャンを使用	87
スクリプトスキャンを無効化	87
スクリプトスキャンを有効化	87
スパイウェア対策を使用	77
スパイウェア対策を無効化	77
スパイウェア対策を有効化	77
スマートリコメンデーションのアラートの設定	128
スマートリコメンデーションの表示のみ	129
スマートリコメンデーションを無効化	129
スマートリコメンデーションを有効化	128

セキュリティアラートについて	74, 103, 106
セキュリティレベルの設定	
オープン	134
ステルス	125
ロック	125
嚴重	126
信用	127
標準	126
セキュリティ上の脆弱性を修復	67
その他の情報	105, 215

た

ツールバーを使用	209
ツールバーを無効化	209
ツールバーを有効化	209
デバイスの表示プロパティを変更	66
デバイスを管理	65
ドメイン	295
トラフィックの分析グラフについて	170, 171
トラブルシューティング	108
トロイの木馬	296

な

ネットワーク	296
ネットワークコンピュータを地理的に追跡 ..	166
ネットワークドライブ	296
ネットワークに参加	270
ネットワークへのアクセスを許可	270
ネットワークをリモートで管理	63
ネットワークを管理	39
ネットワーク上のコンピュータの信頼を取り消 し	61
ネットワーク地図	296
ネットワーク地図で項目を表示/非表示	58
ネットワーク地図にアクセス	56
ネットワーク地図を更新	57
ネットワーク地図を使用	56
ネットワーク名を変更	57, 271
ノード	296

は

パーソナルフィルタの管理方法について ..	200
パーソナルフィルタを管理	199
パーソナルフィルタを削除	201
パーソナルフィルタを追加	200
パーソナルフィルタを編集	200
パスワード	296

パスワードを保護	245
バックアップ	296
バッファオーバーフロー	296
パレンタルコントロール	296
パレンタルコントロールの設定パネルを表示	20
パレンタルコントロールの保護について	20
パレンタルコントロールをセットアップ	221
ファイアウォール	297
ファイアウォールによるセキュリティを最適化	130
ファイアウォールによる保護の状態の設定	132
ファイアウォールによる保護の設定	123
ファイアウォールによる保護を開始	115
ファイアウォールによる保護を停止	116
ファイアウォールのセキュリティレベルを管理	124
ファイアウォールの設定を復元	134
ファイアウォールをロックおよび復元	133
ファイアウォールを起動	115
ファイアウォールを迅速にロック	133
ファイアウォールを迅速にロック解除	133
ファイル、フォルダ、ディスクを抹消	50
ファイルが送信されたときに通知を受信 ..	278
ファイルとフォルダを最適化	38
ファイルの共有を停止	275
ファイルをアーカイブ	251
ファイルを共有	274
ファイルを共有および送信	273
フィッシング詐欺	297
フィッシング詐欺フィルタとは何ですか？ ..	217
フィッシング詐欺フィルタを変更	213
フィッシング詐欺対策の設定	211
フィッシング詐欺対策を無効化	212
フィッシング詐欺対策を無効化/有効化	212
フィッシング詐欺対策を有効化	212
フィルタリングオプションを変更	193
フィルタリングされた Web メール ログを表 示	186
ブラウザ	297
ブラウザ用 SystemGuards について	84
ブラックリスト	297
プリンタの共有を停止	280
プリンタを共有	279
ブルートフォース攻撃	297
プロキシ	297

プロキシサーバ.....	297	ユーザの Cookie 拒否リストの Web サイト を変更.....	227
プログラムアクティビティを監視.....	171	ユーザの Cookie 受け入れリストから Web サイトを削除.....	226
プログラムと権限を管理.....	135	ユーザの Cookie 受け入れリストに Web サ イトを追加.....	225
プログラムにすべてのアクセスを許可.....	136	ユーザの Cookie 受け入れリストの Web サ イトを変更.....	225
プログラムについての確認.....	144	ユーザのインターネット使用時間制限の設定	229
プログラムに送信アクセスのみを許可.....	139	ユーザのコンテンツの格付けグループの設定	222, 234, 239
プログラムのアクセスをブロック.....	141	よくある質問.....	106, 216
プログラムのアクセス権を削除.....	143	よく使う機能を実行.....	35
プログラムのインターネットアクセスをブロック	141	ら	
プログラムのインターネットアクセスを許可	136	ライブラリ.....	298
プログラムの許可を削除.....	143	リアルタイムスキャン.....	298
プログラムの帯域幅を監視.....	171	リアルタイムな対策の設定.....	74, 75
プログラム情報を取得.....	144	リファレンス.....	283
プログラム用 SystemGuards について.....	81	リモートコンピュータにマカフィー セキュリティ ソフトウェアをインストール.....	68
ブロックする Web サイトを削除.....	231	ルータ.....	299
ブロックする Web サイトを変更.....	231	ローカルアーカイブから古いバージョンのファ イルを復元.....	263
プロトコル.....	298	ローカルアーカイブから不足ファイルを復元	262
ヘッダ.....	298	ローカルアーカイブのエクスプローラを使用	260
ポート.....	298	ローミング.....	299
ほかのコンピュータからファイルを受け入れ	277, 278	ログを表示.....	101
ほかのコンピュータにファイルを送信.....	277	ログ記録、監視、分析.....	161, 168
ホットスポット.....	298	わ	
ポップアップ.....	298	ワーム.....	299
ポップアップをブロック.....	242	ワイヤレスアダプタ.....	299
ホホワイトリスト.....	298	漢字	
ま		圧縮.....	299
マカフィー ユーザ アカウントに切り替え.....	25	暗号化.....	299
マカフィーについて.....	303	暗号文.....	299
マカフィーに報告.....	102	画像分析.....	299
メッセージの処理方法を変更.....	196	怪しいプログラム (PUP).....	299
メッセージャー保護を使用.....	90	外部ハードディスク.....	299
メッセージャー保護を無効化.....	90	隔離.....	300
メッセージャー保護を有効化.....	90	隔離したプログラム、Cookie、およびファイル をマカフィーに送信.....	100
や			
ユーザオプションの設定.....	25, 26		
ユーザの Cookie ブロックのレベルの設定	224, 237		
ユーザの Cookie 拒否リストから Web サイ トを削除.....	227		
ユーザの Cookie 拒否リストに Web サイト を追加.....	226		

隔離したプログラム、Cookie、およびファイルを管理	99, 108
隔離したプログラム、Cookie、およびファイルを削除	99
隔離したプログラム、Cookie、およびファイルを復元	99
完全アーカイブ	300
完全アーカイブとクイックアーカイブを実行	256
監視するファイルタイプ	300
監視場所	300
監視対象の IP アドレスを追跡	168
管理されたコンピュータの権限を変更	65
管理されたネットワーク	300
管理されたネットワークにコンピュータを招待	60
管理されたネットワークに参加	59, 269, 272
管理されたネットワークをセットアップ	55
管理されたネットワークを切断	272
管理者アカウントを作成	25
管理者パスワードを取得	26
管理者パスワードを変更	27
既存のシステム サービス ポートへのアクセスをブロック	148
既存のシステム サービス ポートへのアクセスを許可	148
機能	10, 42, 48, 52, 70, 112, 176, 220, 250, 266
起動中のコンピュータを保護	130
許可する Web サイトを削除	235
許可する Web サイトを変更	235
共有	300
共有ファイルをコピー	275
共有ファイルを検索	275
共有プリンタを使用	280
共有秘密キー	300
脅威が検出されました。どうしたらよいですか？	106
禁止するコンピュータ接続を削除	158
禁止するコンピュータ接続を追加	156
禁止するコンピュータ接続を編集	157
個人情報ブロック	244
公開	300
広告、ポップアップ、Web バグをブロック	242
広告をブロック	242
更新オプションの設定	28
更新のダウンロード前に通知	29
更新をダウンロードする前に通知	28
更新を延期	29, 30
更新を自動ダウンロード	29
更新を自動確認	28
更新を自動的にダウンロードし、インストール可能な状態になったら通知	28
更新を自動的にダウンロードしてインストール	28
更新を手動で確認	30, 31
更新状態を確認	14
項目の詳細を表示	58
再起動しても、項目を削除できません	108
最近のイベントとログを表示	101
最近のイベントログからアクセスをブロック	142
最近のイベントログからすべてのアクセスを許可	137
最近のイベントログから送信アクセスのみを許可	139
最近のイベントを表示	36, 163
使用しないファイルとフォルダを削除	38
自動アーカイブをスケジュール	256
自動アーカイブを中断	257
自動更新を無効化	28, 30, 31
辞書攻撃	300
手動スキャン	92
手動スキャンの設定	92, 94
手動スキャン設定を使用してスキャン	92
手動スキャン設定を使用しないスキャン	92
受信イベントログからコンピュータを禁止	159, 163
受信イベントログからコンピュータを追跡	163, 167
受信イベントログから信用するコンピュータを追加	153, 163
受信イベントを表示	163, 167
受信トラフィックと送信トラフィックを分析	170, 171
重点監視する場所	300
詳細メニューを使用	22
情報アラートの設定	32
情報アラートを管理	121
情報アラートを非表示化	121
状態の監視と権限	64
信用するコンピュータ接続を削除	154
信用するコンピュータ接続を追加	152
信用するコンピュータ接続を編集	154

信頼リストを管理	98	保護の状態について	15
侵入検知イベントログからコンピュータを禁止	160, 164	保護の状態の設定	24
侵入検知イベントログからコンピュータを追跡	164, 168	保護の状態を確認	13
侵入検知イベントを表示	164	保護の問題を自動的に修復	21
侵入検知の設定	131	保護の問題を手動で修復	21
新しいシステム サービス ポートの設定	149	保護の問題を修復	21
新しいプログラムにすべてのアクセスを許可	136	無視された問題の設定	24
新しいプログラムのアクセスをブロック	141	無線 LAN (Wireless Local Area Network)	302
世界中のインターネットのポートアクティビティを表示	165	迷惑メールを報告	198
世界中のセキュリティイベントの統計を表示	165	迷惑メール対策を管理	208
正規表現を使用	202, 203	迷惑メール対策を無効化	208
送信イベントログからすべてのアクセスを許可	137, 164	迷惑メール対策を有効化	208
送信イベントログからプログラム情報を取得	144, 164	友人リストの管理方法について	188
送信イベントログから送信アクセスのみを許可	140, 164	友人リストを自動更新	190
送信イベントを表示	137, 138, 139, 140, 142, 145, 164	友人を管理	187
送信メールのスキャンでエラーが発生するのはなぜですか?	107	友人を削除	189
帯域幅	301	友人を手動で追加	188
著作権	303	友人を編集	189
統計を使用	165	利用可能なネットワークプリンタをインストール	281
統合ゲートウェイ	301		
同期化	301		
匿名情報を自動報告	102		
特別フィルタを変更	194		
認証	301		
標準の E メールアカウント	301		
不正アクセスポイント	301		
不適切な可能性のある Web 画像をブロック	239		
不適切な可能性のある画像をブロック	239		
部分的に監視する場所	301		
復元	301		
文字セットによりメッセージをフィルタリング	197		
平文(ひらぶん)	302		
変更ファイルのリストからファイルを削除	263		
保護されていますか?	15		
保護のカテゴリおよびタイプについて	16		