McAfee®

VirusScan® Plus

AntiVirus, Firewall & AntiSpyware

ユーザガイド

目次

概要 **3**

McAfee SecurityCenter (マカフィー・セキュリティーセンター) 5
McAfee SecurityCenter を使用 7
McAfee SecurityCenter の更新 13
保護の問題を修復または無視 17
アラートを使用 23
イベントを表示 29
McAfee VirusScan（マカフィー・ウイルススキャン） 31
コンピュータをスキャン 33
スキャン結果を使用 39
追加の保護の使用 45
ウイルス対策の設定 49
McAfee Personal Firewall (マカフィー・パーソナルファイアウォール) 65
ファイアウォールを起動 67
アラートを使用 69
情報アラートを管理 73
ファイアウォールによる保護の設定 75
プログラムと権限を管理 87
コンピュータ接続を管理 95
システムサービスを管理 103
ログ記録、監視、分析 109
インターネットセキュリティについての確認 119
McAfee QuickClean (マカフィー・クイッククリーン) 121
コンピュータをクリーニング 123
コンピュータの最適化 127
タスクのスケジュール 129
McAfee Shredder (マカフィー・シュレッダー) 135
McAfee Network Manager (マカフィー・ネットワークマネージャ) 139
管理されたネットワークをセットアップ 143
ネットワークをリモートで管理 149
ネットワークの監視 155
McAfee EasyNetwork (マカフィー・イージーネットワーク) 159
McAfee EasyNetwork の設定 161
ファイルを共有および送信 165
プリンタを共有 171

リファレンス 174

用語集 **175**

マカフィーについて **191**

ライセンス条項 191
Copyright 192
カスタマおよびテクニカルサポート 193
McAfee Virtual Technician (マカフィー・バーチャルテクニシャン) の使用 194

索引 **204**

第 1 章

概要

McAfee のファイアウォール、ウイルススキャンおよびスパイウェア対策技術のセキュリティをコンピュータに搭載します。 McAfee VirusScan Plus の使用により、ウイルスからコンピュータを守り、インターネットトラフィック上の不審なアクティビティを監視し、スパイウェアによる個人情報の漏えいを阻止します。

このセクションの内容

McAfee SecurityCenter....5
McAfee VirusScan....31
McAfee Personal Firewall....65
McAfee QuickClean....121
McAfee Shredder....135
McAfee Network Manager....139
McAfee EasyNetwork....159
リファレンス....174
マカフィーについて....191
カスタマおよびテクニカルサポート....193

第 2 章

McAfee SecurityCenter (マカフィー・セキュリティーセンター)

McAfee SecurityCenter (マカフィー・セキュリティーセンター) を使用することで、コンピュータのセキュリティの状態を監視し、ウイルス対策、スパイウェア対策、E メール保護、およびファイアウォールが最新の状態かどうかを簡単に確認でき、セキュリティ上の脆弱性に対処できます。またナビゲーションツールと管理画面で、コンピュータの保護機能全体を管理できます。

コンピュータの保護の設定管理を開始する前に McAfee SecurityCenter の画面を確認し、保護の状態、保護のカテゴリ、保護サービスの違いがわかるようにしてください。 その上で McAfee SecurityCenter を最新の状態に更新してください。

初期設定が完了したら、McAfee SecurityCenter を使用して、コンピュータの保護の状態を監視します。 保護に関する問題が検出されると、McAfee SecurityCenter からアラートが通知され、重大度に応じて問題を修復、または無視するかを判断できます。 また、スキャンの設定変更など McAfee SecurityCenter 内での変更を、イベントログで確認できます。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、**McAfee Virtual Technician** を実行します。

このセクションの内容

McAfee SecurityCenter の機能 6
McAfee SecurityCenter を使用 7
保護の問題を修復または無視 17
アラートを使用 23
イベントを表示 29

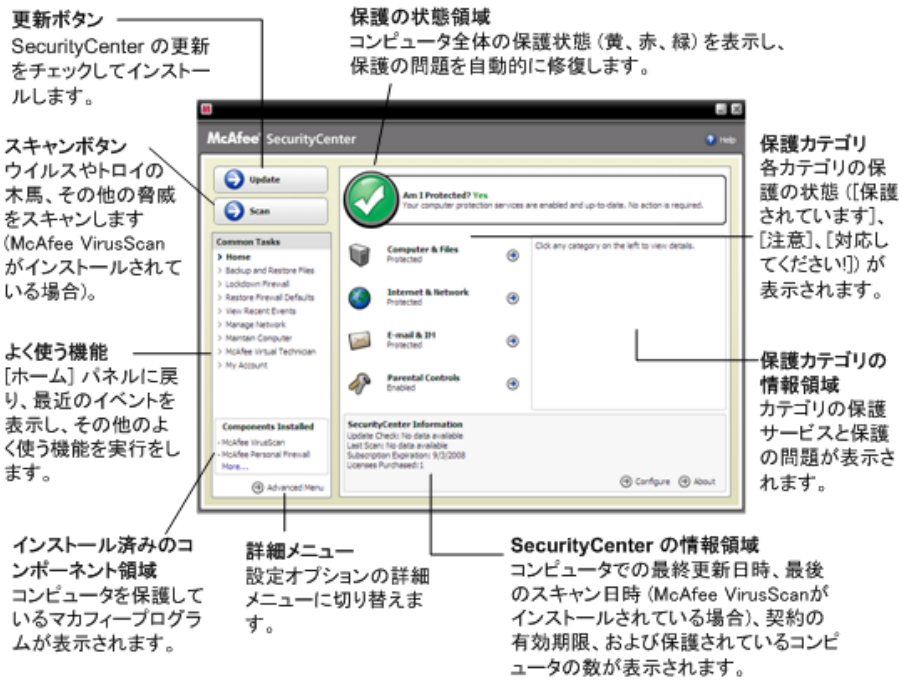
McAfee SecurityCenter の機能

簡略化した保護状態の表示	コンピュータの保護状態の把握、更新の確認、保護の問題の修復を簡単に実行できるようになりました。
自動化した更新およびアップグレード	McAfee SecurityCenter はプログラムを自動的にダウンロードして、インストールします。マカフィープログラムの新しいバージョンが利用可能で契約が有効な場合、新しいマカフィープログラムが配信され、コンピュータが常に最新のセキュリティで保護されます。
リアルタイムのセキュリティアラート機能	セキュリティアラートにより、緊急のウイルス発生やその他の脅威が通知されます。

第 3 章

McAfee SecurityCenter を使用

McAfee SecurityCenter の使用を開始する前に、コンピュータの保護の状態を管理するためのコンポーネントと設定領域を確認してください。この画像で使用されている用語の詳細については、8 ページの「**保護の状態について**」および 9 ページの「**保護カテゴリについて**」を参照してください。マカフィーアカウントの情報から、契約の有効期限を確認できます。



このセクションの内容

保護の状態について 8
保護カテゴリについて 9
保護サービスについて 10
契約の管理 11
McAfee SecurityCenter の更新 13

保護の状態について

コンピュータの保護の状態は、McAfee SecurityCenter の[ホーム]パネル上の、保護の状態の領域に表示されます。 ここには、最新のセキュリティ脅威からコンピュータが確実に保護されているかどうか、または外部からの攻撃や他のセキュリティプログラム、インターネットにアクセスするプログラムなどからの影響を受けているかどうかが表示されます。

コンピュータの保護の状態は、赤色、黄色、緑色で表示されます。

保護の状態	説明
赤色	このコンピュータは保護されていません。 McAfee SecurityCenter の[ホーム]パネルの保護の状態の領域には、コンピュータが保護されていない状態が赤色で表示されます。 McAfee SecurityCenter から、少なくとも 1 つの重要なセキュリティ問題がレポートされます。 万全な保護を維持するには、各保護カテゴリで、重要なセキュリティの問題をすべて修復する必要があります(問題のカテゴリの状態は赤色で[**対応してください！**]に設定されています)。 保護の問題の修復方法については、18 ページの「**保護の問題を修復**」を参照してください。
黄色	このコンピュータの一部は保護されていません。 McAfee SecurityCenter の[ホーム]パネルの保護の状態の領域には、コンピュータが保護されていない状態が黄色で表示されます。 McAfee SecurityCenter により、少なくとも 1 つの重要ではないセキュリティ問題がレポートされます。 万全な保護を維持するためには、各保護カテゴリに関連付けられている重要ではないセキュリティの問題を修復するか、または無視してください。 保護の問題を修復または無視する方法については、17 ページの「**保護の問題を修復または無視**」を参照してください。
緑色	このコンピュータは万全に保護されています。 McAfee SecurityCenter の[ホーム]パネルの保護の状態の領域には、コンピュータが保護されている状態が緑色で表示されます。 McAfee SecurityCenter からは、いかなるセキュリティ上の問題もレポートされていません。 各保護カテゴリに、コンピュータの保護サービスが表示されます。

保護カテゴリについて

McAfee SecurityCenter の保護サービスは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 メールとメッセンジャー、および保護者機能の 4 つのカテゴリに分けられます。この 4 つのカテゴリにより、コンピュータを保護するセキュリティサービスを参照、設定できます。

カテゴリ名をクリックして保護サービスを設定し、サービスに対して検出されるセキュリティ上の問題を表示できます。コンピュータの保護の状態が赤色か黄色の場合は、[必要なアクション] または [注意] メッセージに 1 つ以上のカテゴリが表示され、そのカテゴリ内で問題が検出されていることが通知されます。保護の状態の詳細については、8 ページの「**保護の状態について**」を参照してください。

保護カテゴリ	説明
コンピュータとファイル	次のサービスにより、コンピュータとファイルが保護されています。 ▪ ウイルス対策 ▪ スパイウェア対策 ▪ SystemGuards ▪ Windows 保護 ▪ PC の状態
インターネットとネットワーク	次のサービスにより、インターネットとネットワーク接続が保護されています。 ▪ ファイアウォールによる保護 ▪ フィッシング詐欺対策 ▪ 個人情報の保護
E メールとメッセンジャー	次のサービスにより、E メールとメッセンジャーが保護されています。 ▪ E メールのウイルス対策 ▪ メッセンジャーのウイルス対策 ▪ E メールのスパイウェア対策 ▪ メッセンジャーのスパイウェア対策 ▪ 迷惑メール対策
保護者機能	保護者機能には、次のサービスがあります。 ▪ コンテンツのブロック

保護サービスについて

保護サービスはコンピュータを保護する上で必要となる、さまざまなセキュリティコンポーネントです。保護サービスは、マカフィープログラムに直接対応しています。たとえば、McAfee VirusScan をインストールすると、ウイルス対策、スパイウェア対策、SystemGuards、スクリプトスキャンといった保護サービスが利用できます。これらの保護サービスの詳細については、McAfee VirusScan ヘルプを参照してください。

プログラムインストール直後には、プログラムに関連付けられたすべての保護サービスは標準設定で有効になっています。ただし、保護サービスはいつでも無効にできます。たとえば、McAFee Parental Controls のインストール時には、コンテンツブロックと個人情報の保護は両方とも有効になっています。コンテンツブロックを使用しない場合は、完全に無効化できます。タスクの設定またはメンテナンスの実行中に、一時的に保護サービスを無効にすることも可能です。

契約の管理

ご購入のマカフィー製品は、一定の期間、一定の数のコンピュータで使用できる契約になっています。契約期間はご購入の製品によりますが、通常、製品のご登録により契約が開始されます。製品の登録は簡単に行うことができます (インターネットに接続している必要があります)。登録により、最新の脅威からご使用のコンピュータを保護する自動更新を定期的に受信できるため、非常に重要です。

通常、製品のインストール時に製品登録を行いますが、インターネットに接続できないなどの理由がある場合は、15 日間、登録を延期することができます。15 日以内に製品を登録しない場合は、製品の更新やスキャンの実行ができなくなります。また、契約の有効期限が近づくと、画面メッセージにより定期的に通知を行います。これにより、有効期限前に製品を更新するか、弊社の Web サイトで自動更新を設定することで保護が途切れることを回避できます。

McAfee SecurityCenter に登録を求めるリンクが表示されている場合は、お客様の契約は現在登録されていません。契約の有効期限は、お客様のアカウントページで確認できます。

マカフィーアカウントへのアクセス

McAfee SecurityCenter からマカフィーアカウント情報 (アカウントページ) に簡単にアクセスできます。

1 [**よく使う機能**] で [**マイアカウント**] をクリックします。

2 マカフィーアカウントにログインします。

製品の登録

製品の登録は、通常、製品のインストール時に行います。登録が完了していない場合は、McAfee SecurityCenter に登録を求めるリンクが表示されます。また、通知も定期的に行われます。

- McAfee SecurityCenter の [ホーム] パネルで、[**SecurityCenter の情報**] で、[**契約を有効化してください。**] をクリックします。

ヒント: 定期的に表示されるアラートからも登録できます。

契約の確認

契約の期限が切れていないか確認してください。

- タスクバーの右端の通知領域に表示される McAfee SecurityCenter のアイコンを右クリックし、[**契約の確認**]をクリックします。

契約の更新

契約の有効期限が近づくと、McAfee SecurityCenter に契約の更新を求めるリンクが表示されます。また、有効期限前にも定期的にアラートで通知されます。

- McAfee SecurityCenter の [ホーム] パネルで、[**SecurityCenter の情報**] で、[**更新**] をクリックします。

ヒント: 定期的に表示される通知メッセージからも製品を更新できます。また、アカウントページで更新したり、自動更新を設定できます。

第 4 章

McAfee SecurityCenter の更新

McAfee SecurityCenter は、登録済みのマカフィープログラムを 4 時間ごとに確認し、オンラインで更新をインストールして、最新の状態を維持します。インストールおよび登録したプログラムによっては、最新のウイルス定義、ハッカー対策、迷惑メール対策、スパイウェア対策またはプライバシー保護のアップグレードがオンラインアップデートに含まれる場合があります。標準設定では 4 時間ごとに更新が確認されますが、更新の確認はいつでも可能です。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。

McAfee SecurityCenter の確認および更新のインストール方法を変更することもできますが、自動更新を有効にすることをお勧めします。たとえば、更新をダウンロードしてもインストールは保留するように設定したり、更新をダウンロードまたはインストールする前に通知するように McAfee SecurityCenter を設定できます。また、自動更新を無効にすることも可能です。

注: マカフィー製品を CD からインストールした場合、15 日以内に製品を登録しないと、製品の更新やスキャンの実行ができなくなります。

このセクションの内容

更新の確認.....13
自動更新の設定 14
自動更新を無効化 14

更新の確認

デフォルトでは、コンピュータがインターネットに接続すると、McAfee SecurityCenter によって 4 時間ごとに自動的に更新が確認されます。ただし、4 時間より短い間隔で更新の確認を行うこともできます。 自動更新を無効にする場合は、必ず手動で定期的に更新を確認してください。

- McAfee SecurityCenter の[ホーム]パネルで[**更新**]をクリックします。

ヒント:タスクバー右側の通知領域にある[McAfee SecurityCenter]アイコン を右クリックして、[**更新**]をクリックすると、McAfee SecurityCenter を起動せずに更新の確認をできます。

自動更新の設定

デフォルトでは、コンピュータがインターネットに接続すると、McAfee SecurityCenter によって 4 時間ごとに自動的に更新が確認されます。このデフォルト設定を変更する場合は、自動的に更新をダウンロードしてインストール可能な状態になったら通知するか、更新をダウンロードする前に通知するよう設定できます。

注:更新がダウンロードまたはインストール可能な状態になると、アラートで通知されます。 アラートから、更新をダウンロードまたはインストールするか、更新を延期するか決定できます。 表示されるアラートからプログラムを更新する場合は、ダウンロードおよびインストール前に契約を確認するプロンプトが表示される場合があります。 詳細については、23 ページの「**アラートを使用**」を参照してください。

1 McAfee SecurityCenter の設定パネルを開きます。

アクセス方法

1. [**よく使う機能**] で [**ホーム**] をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。

2 [SecurityCenter の設定]パネルの[**自動更新が無効です**]で[**オン**]をクリックし、[**詳細設定**]をクリックします。

3 以下のボタンのうち、いずれかをクリックします。

- **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)**
- **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**
- **更新をダウンロードする前に通知**

4 [**OK**]をクリックします。

自動更新を無効化

自動更新を無効にする場合は、最新のセキュリティ保護を維持するために、必ず定期的に更新を確認してください。手動での更新の確認については、13 ページの「**更新の確認**」を参照してください。

1 [SecurityCenter の設定] パネルを開きます。

アクセス方法

1. [**よく使う機能**] で [**ホーム**] をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。

2 [SecurityCenter の設定] パネルの [**自動更新が有効です**] で、[**オフ**] 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。

ヒント: [**オン**] ボタンをクリックするか、[更新オプション] パネルで [**自動更新を無効にして更新の有無を手動で確認**] を選択解除すると、自動更新を有効化することができます。

第 5 章

保護の問題を修復または無視

McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 重要な保護の問題は早急な対応が求められ、保護の状態が赤に変わります。 保護の問題が重要でない場合は、早急な対応は必要ではありませんが、保護のステータスが問題の種類に応じて変わる場合があります。 保護の状態を緑にするためには、すべての重要な問題を修復し、重要でない問題を修復するか無視するかを決定する必要があります。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。 McAfee Virtual Technician の詳細については、McAfee Virtual Technician ヘルプを参照してください。

このセクションの内容

保護の問題を修復 18
保護の問題を無視 20

保護の問題を修復

ほとんどのセキュリティの問題は自動的に修復されますが、手動による対応が必要な場合もあります。たとえば、ファイアウォールによる保護が無効になっている場合、McAfee SecurityCenter により自動的に有効化されますが、ファイアウォールによる保護がインストールされていない場合は、インストールする必要があります。以下の表に、保護の問題を手動で修復する際に必要な対応を示します。

問題	対応
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ません。	コンピュータを手動でスキャンします。詳細については、McAfee VirusScan ヘルプを参照してください。
定義ファイル (DAT) ファイルが最新ではありません。	保護を手動で更新してください。詳細については、McAfee VirusScan ヘルプを参照してください。
プログラムがインストールされていません。	マカフィーの Web サイトまたは CD からプログラムをインストールしてください。
プログラムのコンポーネントが不足しています。	マカフィーの Web サイトまたは CD からプログラムを再インストールしてください。
プログラムが登録されていないため、万全な保護を実行できません。	マカフィーの Web サイトでプログラムを登録してください。
お客様の契約は期限切れです。	マカフィーの Web サイトでアカウント状況を確認してください。詳細は、11 ページの「**契約の管理**」を参照してください。

注: 単一の保護の問題が複数の保護カテゴリに影響している場合もあります。この場合、1 つのカテゴリ内の問題を修復すると、ほかの保護カテゴリの問題も修復されます。

保護の問題を自動的に修復

McAfee SecurityCenter では、ほとんどの保護の問題を自動的に修復できます。 保護の問題が自動的に修復される際に McAfee SecurityCenter で変更された設定は、イベントログには記録されません。 イベントの詳細については、29 ページの「**イベントを表示**」を参照してください。

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]パネルの保護の状態領域で、[**修復**]をクリックします。

保護の問題を手動で修復

自動修復を実行しても 1 つ以上の保護の問題が解決されない場合、手動で問題を解決できます。

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、レポートされた問題を含む保護カテゴリをクリックします。

3　問題の詳細に続いて表示されているリンクをクリックします。

保護の問題を無視

McAfee SecurityCenter で重要でない問題が検出された場合は、その問題を修復または無視できます。その他の重要でない問題は自動的に無視されます (McAfee Anti-Spam や McAfee Parental Controls がインストールされていない場合など)。コンピュータの保護の状態が緑色である場合を除き、McAfee SecurityCenter の [ホーム] パネルの保護カテゴリ情報領域には、無視された問題は表示されません。コンピュータの保護の状態が緑でなくても、一度問題を無視した後であれば、保護カテゴリ情報領域内に無視した問題を表示させることはできます。

保護の問題を無視

McAfee SecurityCenter によって検出された重要でない問題を修復しない場合は、その問題を無視することができます。 問題を無視すると、McAfee SecurityCenter の保護カテゴリ情報領域からその問題が削除されます。

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、レポートされた問題を含む保護カテゴリをクリックします。

3 保護の問題の横にある[**無視**]リンクをクリックします。

無視した問題の表示または非表示

重大度に応じて、無視した保護の問題を表示または非表示にできます。

1 [アラートのオプション]パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2 [SecurityCenter の設定]パネルで[**無視された問題**]をクリックします。

3 [無視された問題]パネルで、次の手順を実行します。

- 問題を無視するには、チェックボックスを選択します。
- 保護カテゴリ情報領域の問題をレポートするには、チェックボックスの選択を解除します。

4 [**OK**]をクリックします。

ヒント:また、保護カテゴリ情報領域内のレポートされた問題の横にある[**無視**]リンクをクリックすると、問題を無視できます。

第 6 章

アラートを使用

アラートは、何らかの McAfee SecurityCenter イベントが発生すると、画面の右下隅に小さなポップアップ ダイアログ ボックスで表示されます。 アラートによって、イベントの詳細情報と、イベントに関連付けられた問題を解決するための推奨事項とオプションが提示されます。 アラートに、イベントに関する詳細情報へのリンクが含まれる場合もあります。 これらのリンクを使用して、マカフィーのグローバルサイトを起動したり、トラブルシューティングのために情報をマカフィーに送信できます。

アラートには赤、黄、緑の 3 種類があります。

アラートタイプ	説明
赤	レッドアラートは、ユーザの対応が必要となる、重要な通知です。 McAfee SecurityCenter によって保護の問題を自動的に修復できない場合、レッドアラートが表示されます。
黄	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。
緑	グリーンアラートは、ユーザの対応が必要ない、重要ではない通知です。 グリーンアラートは、イベントに関する基本情報を提示します。

アラートには保護の状態を監視および管理する重要な役割があるため、無効にすることはできません。 ただし、アラート発生時に音を鳴らしたり、起動時にマカフィーの起動画面を表示するなど、一部の情報アラートでその他のアラートオプションを表示したり設定するかどうかを制御できます。

このセクションの内容

情報アラートの表示と非表示 24
アラートのオプションの設定 26

情報アラートの表示と非表示

情報アラートは、パソコンのセキュリティを脅かすことのないイベントが発生したことを通知します。 たとえば、ファイアウォールを設定している場合、デフォルトでは、コンピュータのプログラムにインターネットへのアクセス権が付与されると情報アラートが表示されます。 特定の種類の情報アラートは非表示にできます。 すべての情報アラートを非表示にすることもできます。 また、全画面表示モードでゲームをプレイするときも、情報アラートをすべて非表示にできます。 ゲームが終了し、全画面表示モードが終了すると、情報アラートは再表示されます。

誤って情報アラートを非表示にしてしまった場合にも、いつでも再表示させることができます。 デフォルトでは、すべての情報アラートが表示されます。

情報アラートの表示または非表示

McAfee SecurityCenter を使用して、一部の情報アラートのみを非表示するか、すべての情報アラートを非表示にするかを設定できます。

1 [アラートのオプション]パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2 [SecurityCenter の設定] パネルで [**情報アラート**] をクリックします。

3 [情報アラート]パネルで、次の手順を実行します。

- 情報アラートを表示させるには、チェックボックスの選択を解除します。
- 情報アラートを非表示にするには、チェックボックスを選択します。
- すべての情報アラートを非表示にするには、[**情報アラートを表示しない**]チェックボックスを選択します。

4 [**OK**]をクリックします。

ヒント:アラートの[**今後このアラートを表示しない**]チェックボックスを選択すると、情報アラートを非表示にできます。 その場合、[情報アラート]パネルで該当するチェックボックスの選択を解除すると、その情報アラートを再表示できます。

ゲーム時の情報アラートの表示または非表示

全画面表示モードでゲームを行う際に、情報アラートをすべて非表示にできます。 ゲームが終了し、全画面表示モードが終了すると、情報アラートの表示が再開されます。

1　［アラートのオプション］パネルを開きます。

アクセス方法

1. ［**よく使う機能**］で［**ホーム**］をクリックします。
2. 右パネルの［**SecurityCenter の情報**］で、［**設定**］をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2　［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**］チェックボックスを選択するか、選択を解除します。

3　［**OK**］をクリックします。

アラートのオプションの設定

アラートの表示頻度は McAfee SecurityCenter で設定されていますが、一部の基本的なアラートオプションは調節できます。 たとえば、アラートの発生時に音を鳴らしたり、Windows 起動時の起動画面のアラートを非表示にできます。 また、オンラインコミュニティ内でのウイルスの発生やその他セキュリティ脅威に関して通知するアラートを非表示にできます。

アラート発生時に音を鳴らす

アラート発生時に音による通知を受け取る場合は、アラートごとに音が鳴るよう設定できます。

1 [アラートのオプション]パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2 [アラートのオプション]パネルの[**サウンド**]で、[**アラートが発生したときに音を鳴らす**]チェックボックスを選択します。

起動時の起動画面を非表示にする

デフォルトでは、Windows の起動時にはマカフィーの起動画面が表示され、McAfee SecurityCenter により保護が実行されていることが通知されます。 この起動画面を非表示にすることもできます。

1 [アラートのオプション]パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2 [アラートのオプション]パネルの[**起動画面**]で、[**Windows の起動時にマカフィーの起動画面を表示**]チェックボックスを選択します。

ヒント:[**Windows の起動時にマカフィーの起動画面を表示**]チェックボックスを選択すれば、いつでも起動画面を再表示できます。

ウイルス発生によるアラートの非表示

オンラインコミュニティ内でのウイルスの発生やその他の脅威に関して通知するアラートを非表示にできます。

1　[アラートのオプション] パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2　[アラートのオプション] パネルで、[**ウイルス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**] チェックボックスの選択を解除します。

ヒント: [**ウイルス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**] チェックボックスを選択すれば、いつでもウイルス発生によるアラートを再表示できます。

セキュリティメッセージの非表示

ホームネットワーク内の複数のコンピュータの保護に関するセキュリティ通知を非表示にできます。これらのメッセージには、契約内容、契約で保護可能なコンピュータの数、および契約を拡大してコンピュータを追加する方法などが含まれています。

1　[アラートのオプション] パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2　[アラートのオプション] パネルで、[**ウイルス情報またはセキュリティに関するメッセージの表示**] チェックボックスを選択解除します。

ヒント: [**ウイルス情報またはセキュリティに関するメッセージの表示**] チェックボックスを選択すれば、いつでもセキュリティメッセージを表示できます。

第 7 章

イベントを表示

イベントとは、保護カテゴリや関連する保護サービス内で行われた対応や設定変更のことです。 さまざまな保護サービスにより、さまざまなイベントの種類が記録されます。 たとえば、McAfee SecurityCenter では、保護サービスが有効化または無効化されるとイベントを記録し、ウイルス対策では、ウイルスが検出および削除されるたびにイベントを記録し、ファイアウォールによる保護では、インターネット接続がブロックされるたびにイベントを記録します。 保護カテゴリの詳細については、9 ページの「**保護カテゴリについて**」を参照してください。

トラブルシューティング発生時や他のユーザによって実行された操作を確認する場合に、イベントを表示できます。 保護者はイベントログを使用して、子供のインターネット利用を監視できます。 最近のイベントを表示して、直近の 30 個のイベントのみ確認できます。 すべてのイベントを表示して、発生したすべてのイベントの包括的なリストを確認できます。 すべてのイベントを表示する場合、McAfee SecurityCenter によってイベントログが起動され、発生した保護カテゴリに従ってイベントがソートされます。

このセクションの内容

最近のイベントを表示 29
すべてのイベントを表示 29

最近のイベントを表示

最近のイベントを表示して、直近の 30 個のイベントのみ確認できます。

- [**よく使う機能**]で[**最近のイベントを表示**]をクリックします。

すべてのイベントを表示

すべてのイベントを表示して、発生したすべてのイベントの包括的なリストを確認できます。

1. [**よく使う機能**]で[**最近のイベントを表示**]をクリックします。
2. [最近のイベント]パネルで[**ログを表示**]をクリックします。
3. イベントログの左ペイン(ウィンドウ枠)で、表示するイベントの種類をクリックします。

第 8 章

McAfee VirusScan（マカフィー・ウイルススキャン）

McAfee VirusScan（マカフィー・ウイルススキャン）は、ウイルス、トロイの木馬、トラッキング Cookie、スパイウェア、アドウェアおよび怪しいプログラムなどの最新のセキュリティ脅威から保護するための高度な検出および保護サービスを提供します。 E メール、インスタントメッセージ、Web などさまざまなポイントからの脅威の対象となるデスクトップ上のファイルおよびフォルダにも、保護機能が拡張されています。

McAfee VirusScan を使用すれば、いつでも、あるいは定期的にコンピュータを保護できます。面倒な管理も必要ありません。 作業や、ゲーム、Web 閲覧、E メールのチェック中にも、バックグラウンドで常に脅威を監視、スキャン、検出しています。 包括的なスキャンをスケジュールに従って実行し、高度なオプションセットを使用してコンピュータを定期的にチェックします。 必要に応じて McAfee VirusScan を柔軟にカスタマイズできますが、カスタマイズしなくてもコンピュータは保護できます。

コンピュータを通常どおり使用すると、ウイルスやワーム、およびその他の脅威が侵入する可能性があります。 脅威が侵入した場合は McAfee VirusScan から脅威が通知され、通常は被害が発生する前に感染したアイテムを消去または隔離します。 ただしまれに別の対応が必要となる場合もあります。 その場合、McAfee VirusScan を使用すれば、コンピュータの次回起動時に再スキャンしたり、検出したアイテムを保存したり削除するなど、アクションを決定できます。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。

このセクションの内容

McAfee VirusScan の機能 32
コンピュータをスキャン.....33
スキャン結果を使用.....39
スキャンの種類 42
追加の保護の使用 45
ウイルス対策の設定.....49

McAfee VirusScan の機能

包括的なウイルス対策	ウイルス、トロイの木馬、トラッキング Cookie、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含む、セキュリティ上の最新の脅威からユーザとコンピュータを保護します。保護機能はデスクトップやラップトップ上のファイルおよびフォルダにも拡張され、E メール、メッセンジャー、Web などさまざまな経路から侵入する脅威をターゲットとしています。面倒な管理は不要です。
リソースに配慮したスキャンオプション	スキャンオプションをカスタマイズできますが、初期設定でコンピュータは保護できます。スキャン速度が遅い場合は、オプションを無効にして、コンピュータリソースの使用を最小限に抑えることができます。ただしウイルス対策はほかのタスクよりも優先度が高いことにご注意ください。
自動修復	スキャンの実行中に脅威が検出されると、脅威の種類に応じて自動的に脅威が処理されます。これにより、操作することなく、ほとんどの脅威が検出され、無効になります。ただしまれに脅威を無効化できない場合もあります。McAfee VirusScan を使用すれば、コンピュータの次回起動時に再スキャンしたり、検出した項目を保存したり削除するなど、アクションを決定できます。
全画面表示モードでのタスクの一時停止	映画鑑賞やゲームなど、全画面表示でコンピュータを使用する場合、手動スキャンなどの多数のタスクを一時停止できます。

第 9 章

コンピュータをスキャン

McAfee SecurityCenter の起動前でも、McAfee VirusScan のリアルタイムウイルス対策が有害な可能性のあるウイルスやトロイの木馬、その他のセキュリティの脅威に対するコンピュータの保護を開始します。McAfee VirusScan のリアルタイムなウイルス対策では、設定したリアルタイムスキャンオプションを使用してファイルへのアクセス時にファイルをスキャンすることで、無効にするまでウイルスアクティビティが常時監視されます。ご使用のコンピュータを最新の脅威から継続的に保護するためには、リアルタイムなウイルス対策を無効にせず、さらに定期的なスケジュールを設定し、包括的に手動スキャンを実行します。スキャンオプションの設定の詳細は、49 ページの「**ウイルス対策の設定**」を参照してください。

McAfee VirusScan で、ウイルス対策に対するスキャンオプションをより詳細に設定すると、定期的に広範囲のスキャンを実行できます。McAfee SecurityCenter からフルスキャン、簡易スキャン、カスタムスキャンまたはスケジュールスキャンを実行できます。操作中に Windows Explorer で手動スキャンを実行することもできます。McAfee SecurityCenter でスキャンを実行すると、オンザフライでオプションのスキャンを変更できます。Windows Explorer からのスキャンの実行は、コンピュータセキュリティを有効にする簡単な方法です。

McAfee SecurityCenter または Windows Explorer のいずれを使用してスキャンが実行されたかは、終了したスキャン結果で確認できます。McAfee VirusScan によってウイルス、トロイの木馬、スパイウェア、アドウェア、Cookie およびほかの怪しいプログラムが検出、修復または隔離されたかどうかを、スキャンの結果で確認できます。スキャンの結果はさまざまな方法で表示されます。たとえば、感染状態と種類などのスキャン結果の概要および詳細情報を表示できます。また、一般的なスキャンと検出の統計を表示できます。

このセクションの内容

パソコンをスキャン 34
スキャン結果を表示.....37

パソコンをスキャン

VirusScan には、リアルタイムスキャン（脅威のアクティビティに対してリアルタイムに PC を監視）や Windows Explorer からの手動スキャンなど、一連のウイルス対策が用意されています。また、McAfee SecurityCenter からのフルスキャン、簡易スキャン、カスタムスキャンを実行でき、スキャンの実行をスケジュール設定してカスタマイズすることもできます。

設定...	手順...
リアルタイムスキャンを開始して、ウイルスのアクティビティに対して定期的にコンピュータを監視し、ユーザまたはコンピュータがアクセスするたびにファイルをスキャン	1. [コンピュータとファイルの設定] パネルを開きます。 アクセス方法 1. 左ペインで[**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. [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。 2. [**ウイルス対策**] で [**オン**] をクリックします。 **注:** リアルタイムスキャンは標準設定で有効になっています。
簡易スキャンを開始してコンピュータの脅威を簡単にチェック	1. 標準メニューで [**スキャン**] をクリックします。 2. [スキャンオプション] パネルの [簡易スキャン] で、[**開始**] をクリックします。
フルスキャンを開始してコンピュータの脅威を徹底的にチェック	1. 標準メニューで [**スキャン**] をクリックします。 2. [スキャンオプション] パネルの [フルスキャン] で、[**開始**] をクリックします。

設定...	手順...
ユーザの設定に基づいたカスタムスキャンを開始	1. 標準メニューで [**スキャン**] をクリックします。 2. [スキャンオプション] パネルの [選択オプション] で、[**開始**] をクリックします。 3. 次のオプションを選択または選択解除して、スキャンをカスタマイズします。 **すべてのファイルのすべての脅威** **未知のウイルス** **アーカイブファイル** **スパイウェアと潜在的な脅威** **トラッキング Cookie** **ステルスプログラム** 4. [**開始**] をクリックします。
手動スキャンを開始して、ファイル、フォルダおよびドライブの脅威をチェック	1. Windows Explorer を開きます。 2. 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。

設定...	手順...
スケジュールスキャンを開始してコンピュータの脅威を定期的にスキャン	1. [スケジュールスキャン] パネルを開きます。 アクセス方法 1. [**よく使う機能**]で[**ホーム**]をクリックします。 2. SecurityCenter の[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。 3. [コンピュータとファイル]情報領域で、[**設定**]をクリックします。 4. [コンピュータとファイルの設定]パネルで、ウイルス対策が有効化されているか確認し、[**詳細設定**]をクリックします。 5. [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。 2. [**スケジュールスキャンを有効化**] を選択します。 3. スキャンに使用されるプロセッサパワーを軽減するには、[**最小限のコンピュータリソースを使用するスキャン**] を選択します。 4. 1 日以上の日数を選択します。 5. 開始時刻を指定します。 6. [**OK**] をクリックします。

スキャン結果がスキャン完了アラートに表示されます。結果には、スキャン、検出、修復、隔離および削除された項目の数が表示されます。[**スキャンの詳細を表示**] をクリックして、スキャン結果の詳細または感染した項目を表示します。

注: スキャンオプションの詳細は、42 ページの「**スキャンの種類**」を参照してください。

スキャン結果を表示

スキャンが終了したら、結果を表示して、スキャンで検索された項目を確認し、現在のコンピュータの保護の状態を分析します。McAfee VirusScan によってウイルス、トロイの木馬、スパイウェア、アドウェア、Cookies およびほかの怪しいプログラムが検出、修復または隔離されたかどうかを、スキャンの結果で確認できます。

標準メニューまたは詳細メニューで、[**スキャン**] をクリックしてから、次のいずれかの操作を実行します。

設定...	手順...
スキャン結果をアラートに表示	スキャン結果をスキャン完了アラートに表示します。
スキャン結果に関する詳細を表示	スキャン完了アラートで [**スキャンの詳細を表示**] をクリックします。
スキャン結果のクイックサマリを表示	タスクバーの通知領域で、[**スキャン完了**] アイコンをポイントします。
スキャンと検出の統計を表示	タスクバーの通知領域で、[**スキャン完了**] アイコンをダブルクリックします。
検出された項目、感染状態および種類の詳細を表示	1. タスクバーの通知領域で、[**スキャン完了**] アイコンをダブルクリックします。 2. [フルスキャン]、[簡易スキャン]、[カスタムスキャン]、[手動スキャン] パネルそれぞれにある [**詳細**] をクリックします。
最新のスキャンの詳細を表示	タスクバーの通知領域に表示される [**スキャン完了**] アイコンをダブルクリックし、[フルスキャン]、[簡易スキャン]、[カスタムスキャン]、[手動スキャン] の各パネルにある [スキャン] で最新のスキャンの詳細を表示します。

第 10 章

スキャン結果を使用

スキャンの実行中に脅威が検出されると、脅威の種類に応じて自動的に脅威が処理されます。たとえば、McAfee VirusScan によって、コンピュータ上でウイルス、トロイの木馬またはトラッキング Cookie が検出されると、感染ファイルの駆除が試行されます。McAfee VirusScan は常にファイルを隔離してから、感染ファイルを駆除します。駆除されない場合、感染ファイルは隔離されます。

セキュリティの脅威によっては、McAfee VirusScan では正常にファイルの駆除または隔離ができない場合があります。この場合、McAfee VirusScan から脅威の取り扱いを決定するよう促されます。脅威の種類に応じてさまざまなアクションを選択できます。たとえば、ウイルスがファイル内で検出され、McAfee VirusScan ではそのファイルを正常に駆除または隔離できない場合、そのファイルへの以降のアクセスは拒否されます。トラッキング Cookie が検出され、McAfee VirusScan ではその Cookie を正常に駆除または隔離できない場合、削除するか信頼するかを決定できます。怪しいプログラムが検出され、McAfee VirusScan では自動的に対応されない場合、そのプログラムを隔離するか、信頼するかを決定する必要があります。

McAfee VirusScan によって隔離されるときは、その項目を暗号化し、ファイル、プログラムまたは Cookie がコンピュータに被害を及ぼさないようフォルダに隔離されます。隔離された項目は復元または削除できます。システムに影響を与えずに隔離された Cookie を削除できることがほとんどですが、任意で使用されているプログラムが隔離される場合は、復元を検討してください。

このセクションの内容

ウイルスとトロイの木馬について 39
怪しいプログラムについて 40
隔離されたファイルについて 40
隔離プログラムと Cookie について 41

ウイルスとトロイの木馬について

McAfee VirusScan がコンピュータのファイルでウイルスまたはトロイの木馬を検出した場合、ファイルの削除が試行されます。ファイルを駆除できない場合は、ファイルの隔離が試行されます。ファイルの隔離にも失敗した場合、ファイルへのアクセスが拒否されます (リアルタイムスキャンの場合のみ)。

1 [スキャン結果] パネルを開きます。

アクセス方法

1. タスクバーの右の方で、[**スキャン完了**]アイコンをダブルクリックします。
2. [手動スキャン]パネルの[スキャンの進捗状況]で、[**結果を表示**]をクリックします。

2 [スキャン結果] リストで、[**ウイルスとトロイの木馬**] をクリックします。

注: McAfee VirusScan によって隔離されたファイルを使用するには、40 ページの「**隔離されたファイルについて**」を参照してください。

怪しいプログラムについて

コンピュータ上で McAfee VirusScan が怪しいプログラムを検出した場合、そのプログラムを削除または信頼することができます。不明なプログラムの場合は、削除することをお勧めします。怪しいプログラムの削除とは、実際にシステム内でプログラムが削除されることとは異なります。また、隔離されたプログラムを削除しても、コンピュータやファイルに被害を及ぼすことはありません。

1 [スキャン結果] パネルを開きます。

アクセス方法

1. タスクバーの右の方で、[**スキャン完了**]アイコンをダブルクリックします。
2. [手動スキャン]パネルの[スキャンの進捗状況]で、[**結果を表示**]をクリックします。

2 [スキャン結果] リストで、[**怪しいプログラム**] をクリックします。

3 怪しいプログラムを選択します。

4 [**オプションの選択**] で、[**削除**] または [**信頼**] のいずれかをクリックします。

5 選択したオプションを確認します。

隔離されたファイルについて

McAfee VirusScan によって、感染したファイルが隔離される場合、項目は暗号化され、ファイルがコンピュータに被害を及ぼさないようにフォルダに移動されます。 隔離されたファイルは復元または削除できます。

1 [隔離ファイル]パネルを開きます。

アクセス方法

1. 左ペインで[**詳細メニュー**]をクリックします。
2. [**復元**]をクリックします。
3. [**ファイル**]をクリックします。

2 隔離されたファイルを選択します。

3 次のいずれかの操作を実行します。

- 感染したファイルを修復して、コンピュータ上の元の場所に戻すには、[**復元**]をクリックします。
- 感染したファイルをコンピュータから削除するには、[**削除**]をクリックします。

4 [**はい**]をクリックして、選択したオプションを確認します。

ヒント:複数のファイルを同時に復元または削除できます。

隔離プログラムと Cookie について

McAfee VirusScan によって、怪しいプログラムやトラッキング Cookie が隔離される場合、項目は暗号化され、プログラムまたは Cookie がコンピュータに被害を及ぼさないよう保護されたフォルダに移動されます。

1 [隔離プログラム]と[トラッキング Cookie]パネルを開きます。

アクセス方法

1. 左ペインで[**詳細メニュー**]をクリックします。
2. [**復元**]をクリックします。
3. [**プログラムと Cookie**]をクリックします。

2 隔離されたプログラムまたは Cookie を選択します。

3 次のいずれかの操作を実行します。

- 感染したファイルを修復して、コンピュータ上の元の場所に戻すには、[**復元**]をクリックします。
- 感染したファイルをコンピュータから削除するには、[**削除**]をクリックします。

4 処理を確定するには[**はい**]をクリックしてください。

ヒント:複数のプログラムと Cookie を同時に復元または削除できます。

スキャンの種類

McAfee VirusScan では、リアルタイムスキャン (リアルタイム (常時) にパソコンを脅威のアクティビティから監視します)、Windows Explorer からの手動スキャンなどのウイルス対策用の完全なスキャンオプションのセットを提供し、McAfee SecurityCenter からフルスキャン、簡易スキャン、カスタムスキャンを実行する機能、またはスケジュールスキャンが発生する場合、カスタマイズする機能を提供します。McAfee SecurityCenter でスキャンを実行すると、オンザフライでオプションのスキャンを変更できます。

リアルタイムスキャン:

リアルタイムでのウイルス対策では、ウイルスのアクティビティを常時監視し、ユーザまたはコンピュータがアクセスするたびにファイルをスキャンします。最新の脅威に対して常に保護された状態を維持するためには、リアルタイムのウイルス対策を有効にし、さらに包括的な手動スキャンもスケジュール設定します。

リアルタイムスキャンの標準設定のオプションを設定できます。オプションには、未知のウイルスのスキャンや、トラッキング Cookie およびネットワークドライブの脅威のチェックがあります。また、バッファオーバーフロー保護も利用できます。これはデフォルトで有効となっていますが、Windows Vista (64 ビット) を使用している場合は利用できません。詳細については、50 ページの「**リアルタイムスキャンオプションの設定**」を参照してください。

簡易スキャン

簡易スキャンでは、処理中の脅威のアクティビティ、重要な Windows ファイル、およびコンピュータ上のその他の感染する可能性が高い領域をチェックできます。

フルスキャン

フルスキャンでは、コンピュータ内に存在するウイルス、スパイウェア、およびその他の脅威に対してコンピュータ全体をチェックできます。

カスタムスキャン

カスタムスキャンでは、ユーザ自身がスキャン設定を選択して、コンピュータ上の脅威のアクティビティをチェックできます。カスタムスキャンのオプションには、すべてのファイル、アーカイブファイル、および Cookie のチェックに加え、未知のウイルス、スパイウェア、およびステルスプログラムのスキャンができます。

カスタムスキャンの標準設定のオプションを設定できます。オプションには、未知のウイルス、アーカイブファイル、スパイウェア、および潜在的な脅威、トラッキング Cookie、およびステルスプログラムの各スキャンがあります。また、最小限のコンピュータリソースを使用してスキャンすることもできます。詳細については、52 ページの「**カスタムスキャンオプションの設定**」を参照してください。

手動スキャン

手動スキャンでは、Windows Explorer から処理中のファイル、フォルダおよびドライブ内の脅威をすばやくチェックできます。

スケジュールスキャン

スケジュールスキャンでは、週や日に数回など、コンピュータのウイルスや他の脅威をチェックできます。スケジュールスキャンは、標準設定のスキャンオプションを使用して、コンピュータ全体を常にチェックします。標準設定では、週 1 回のスキャンがスケジュール設定されています。スキャン速度が遅い場合は、このオプションを無効にしてコンピュータリソースの使用を最小限に抑えることができます。ただしウイルス対策はほかのタスクよりも優先度が高いことにご注意ください。詳細は、55 ページの「**スキャンのスケジュール**」を参照してください。

注: 適切なスキャンオプションを開始する方法は、34 ページの「**パソコンをスキャン**」を参照してください。

第 11 章

追加の保護の使用

リアルタイムでのウイルス対策に加えて、McAfee VirusScan には、スクリプト、スパイウェア、危険性のある E メールやメッセンジャーの添付ファイルに対する追加保護機能が用意されています。標準設定では、スクリプトスキャン、スパイウェア、E メール、メッセンジャーの保護が有効になっています。

スクリプトスキャンによる保護

スクリプトスキャンによる保護は、危険性のあるスクリプトを検出し、コンピュータまたは Web ブラウザでの実行を回避します。ファイルの作成、コピーまたは削除や、Windows のレジストリを開くようなスクリプトなど、不審なスクリプトアクティビティを監視し、被害が発生する前に、アラートが表示されます。

スパイウェア対策

スパイウェア対策により、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が検出されます。スパイウェアとは、コンピュータに知らないうちにインストールされ、ユーザの動作を監視し、個人情報を収集し、追加のソフトウェアをインストールしたり、ブラウザのアクティビティをリダイレクトするなど、コンピュータの制御を妨害するソフトウェアです。

E メール保護

E メール保護により、送信する E メールおよび添付ファイル内の不審なアクティビティが検出されます。

メッセンジャーの保護

メッセンジャーの保護により、受信するメッセンジャーの添付ファイルから脅威が検出されます。また、メッセンジャープログラムでの個人情報の共有を回避できます。

このセクションの内容

スクリプトスキャンによる保護の開始 46
スパイウェア対策の開始.....46
E メール保護を開始 46
メッセンジャー保護を開始 47

スクリプトスキャンによる保護の開始

スクリプトスキャンによる保護により、危険性のあるスクリプトが検出され、コンピュータでの実行を回避できます。 スクリプトスキャンによる保護により、スクリプトによりファイルが作成、コピーまたは削除されたり、Windows のレジストリが変更されると、アラートが表示されます。

1 コンピュータとファイルの設定パネルを表示します。

アクセス方法

1. 左ペインで[**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. [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。

2 [**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。

注: スクリプトスキャンによる保護はいつでも無効化できますが、無効にすると危険性のあるスクリプトに対する脆弱性からの保護を実行できません。

スパイウェア対策の開始

スパイウェア対策を有効化して、ユーザの知らない間に情報を収集して伝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検出し削除できます。

1 コンピュータとファイルの設定パネルを表示します。

アクセス方法

1. 左ペインで[**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. [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。

2 [**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。

注: スパイウェア対策はいつでも無効化できますが、無効にすると怪しいプログラムに対する脆弱性を保護できません。

E メール保護を開始

E メール保護を有効化して、E メールや添付ファイルの送信(SMTP)や受信(POP3)に含まれる脅威やワームを検出します。

1 E メールとメッセンジャーの設定パネルを表示

アクセス方法

1. 左ペインで[**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. [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。

2 [**E メール保護**]で[**オン**]をクリックします。

注: E メール保護はいつでも無効化できますが、無効にすると E メール脅威に対する脆弱性からの保護を実行できません。

メッセンジャー保護を開始

インスタントメッセージ保護を有効にして、受信するインスタントメッセージの添付ファイルに含まれるセキュリティ脅威を検出します。

1 E メールとメッセンジャーの設定パネルを表示

アクセス方法

1. 左ペインで[**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. [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。

2 [**メッセンジャーの保護**]で[**オン**]をクリックします。

注: インスタントメッセージ保護はいつでも無効化できますが、無効にすると危険性のあるインスタントメッセージの添付ファイルに対する脆弱性からの保護を実行できません。

第 12 章

ウイルス対策の設定

スケジュールスキャン、カスタムスキャン、およびリアルタイムスキャンに別のオプションを設定できます。たとえば、リアルタイムでの保護により継続的にコンピュータが監視されているため、基本的なスキャンオプションのセットを選択すると、手動による保護やオンデマンド保護など、さらに包括的なスキャンオプションを利用できます。

また、SystemGuards や信頼リストを使用して、パソコン上の無断での変更や不正な変更を VirusScan で監視および管理する方法を決定できます。SystemGuards により、コンピュータ上の Windows のレジストリや重要なシステムファイルに対して実行された不正な変更を監視、ログ記録、レポートおよび管理できます。レジストリおよびファイルが不正に変更されると、コンピュータに被害が及んだり、セキュリティが侵害されたり、重要なシステムファイルが損害を受ける可能性があります。信頼リストを使用して、ファイル、レジストリの変更 (SystemGuards)、プログラム、またはバッファオーバーフローを検出するルールを信頼するか削除するかどうかを決定できます。検出された項目を信頼し、今後この項目によるアクティビティに関する通知が不要な場合は、この項目を信頼リストに追加します。リストに追加すると、この項目は検出されなくなり、また通知されることもありません。

このセクションの内容

リアルタイム スキャン オプションの設定.....50
カスタムスキャンオプションの設定.....52
スキャンのスケジュール.....55
McAfee SystemGuards オプションを使用 56
信頼リストの使用 62

リアルタイム スキャン オプションの設定

リアルタイムでのウイルス対策を開始する場合、McAfee VirusScan のデフォルトのオプションセットを使用してファイルをスキャンできますが、必要に応じてデフォルトのオプションを変更できます。

リアルタイム スキャン オプションを変更するには、スキャン時のチェック事項と、スキャンする場所、スキャンするファイルの種類を指定する必要があります。 たとえば、McAfee VirusScan のチェック対象として、未知のウイルスをチェックするか、または Web サイトがユーザの行動を追跡するための Cookie をチェックするかどうかを決定し、スキャンする場所として、コンピュータにマッピングされるネットワークドライブをスキャンするのか、または単にローカルドライブをスキャンするのかを決定できます。 また、スキャンするファイルの種類を指定できます（すべてのファイル、または最もウイルスが検出されやすいプログラムファイル、文書など）。

リアルタイム スキャン オプションを変更する場合は、バッファオーバーフロー保護がコンピュータに適用されているかどうかを指定する必要があります。 バッファとは、コンピュータの情報を一時的に保持するために使用されるメモリの一部です。 バッファオーバーフローは、怪しいプログラムまたはプロセスが保存しようとする情報量がバッファの制限を越えた場合に発生します。 バッファオーバーフローが発生すると、セキュリティ攻撃に対する脆弱性が高まります。

リアルタイムスキャンオプションの設定

リアルタイムスキャンオプションを設定して、リアルタイムスキャンの検出対象、スキャンする場所およびファイルの種類をカスタマイズできます。オプションには、未知のウイルスのスキャンと、トラッキング Cookie、バッファオーバーフロー保護が含まれています。また、リアルタイムスキャンを設定して、コンピュータにマッピングされるネットワークドライブをチェックできます。

1 [リアルタイムスキャン] パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. SecurityCenter の[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。
3. [コンピュータとファイル]情報領域で、[**設定**]をクリックします。
4. [コンピュータとファイルの設定]パネルで、ウイルス対策が有効化されているか確認し、[**詳細設定**]をクリックします。

2 リアルタイムスキャンオプションを指定して、[**OK**] をクリックします。

設定...	手順...
未知のウイルスおよび既知のウイルスの新しい亜種の検出	[**未知のウイルスをスキャン**] を選択します。
Cookie の検出	[**トラッキング Cookie をスキャンして削除**] を選択します。
ネットワークに接続しているドライブ上のウイルスおよびその他の脅威を検出	[**ネットワークドライブをスキャン**] を選択します。
バッファオーバーフローからコンピュータを保護	[**バッファオーバーフロー保護を有効化**] を選択します。
スキャンするファイルの種類を指定	[**すべてのファイル（推奨）**] または [**プログラムファイルと文書のみ**] をクリックします。

リアルタイムなウイルス対策の停止

スキャンオプションを変更したり、パフォーマンスの問題を解決する場合など、リアルタイムスキャンを一時的に停止する場合もあります。リアルタイムなウイルス対策を無効にすると、コンピュータは保護されず、McAfee SecurityCenter の保護の状態は赤になります。保護の状態の詳細については、McAfee SecurityCenter ヘルプの「保護の状態について」を参照してください。

リアルタイムでのウイルス対策を一時的に停止し、再開時間を指定できます。15 分、30 分、45 分、60 分後のいずれかを指定して、保護を再開でき、また、再開しないよう指定もできます。

1 [コンピュータとファイルの設定] パネルを開きます。

アクセス方法

1. 左ペインで[**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. [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。

2 [**ウイルス対策**] で [**オフ**] をクリックします。

3 ダイアログボックスで、リアルタイムスキャンを再開する時間を選択します。

4 [**OK**] をクリックします。

カスタムスキャンオプションの設定

カスタムウイルス対策では、必要に応じてファイルをスキャンできます。カスタムスキャンを開始する場合は、McAfee VirusScan は、より包括的なスキャンオプションのセットを使用して、ウイルスおよび危険性のある項目を確認します。カスタムスキャンオプションを変更するには、スキャン時の確認事項を決定している必要があります。たとえば、未知のウイルス、スパイウェアやアドウェアなどの怪しいプログラム、コンピュータへの不正アクセスを可能にするルートキットなどのステルスプログラム、およびユーザの閲覧履歴を追跡する Cookie を検出対象とするかどうかを指定できます。また、チェック対象ファイルの種類を指定する必要があります。たとえば、McAfee VirusScan がすべてのファイルをチェックするのか、または最もウイルスが検出されるプログラムファイルや文書だけをチェックするのか指定できます。また、アーカイブファイル (たとえば .zip ファイル) をスキャン対象に含めるかどうかも指定できます。

標準設定では、McAfee VirusScan は、カスタムスキャン実行時にはコンピュータ上、およびすべてのネットワークドライブのすべてのドライブおよびフォルダをチェックします。ただし、必要に応じて標準設定の場所を変更できます。たとえば、重要なパソコンのファイルやデスクトップ上の項目、またはプログラムファイルフォルダ内の項目のみをスキャンすることもできます。カスタムスキャンを開始する場合は、定期的なスキャンスケジュールを設定できます。スケジュールスキャンは、標準設定のスキャンオプションを使用して、コンピュータ全体を常にチェックします。標準設定では、週 1 回のスキャンがスケジュール設定されています。

スキャン速度が遅い場合は、このオプションを無効にしてコンピュータリソースの使用を最小限に抑えることができます。ただしウイルス対策は他のタスクよりも優先度が高いことにご注意ください。

注: 映画鑑賞やゲームなど、全画面表示でコンピュータを使用する場合、自動更新やカスタムスキャンなどの多数のタスクを一時停止できます。

カスタムスキャンオプションの設定

カスタムスキャンオプションを設定して、カスタムスキャンの検出対象、スキャンする場所およびファイルの種類をカスタマイズできます。オプションには、未知のウイルス、アーカイブファイル、スパイウェア、怪しいプログラム、トラッキング Cookie、ルートキットおよびステルスプログラムのスキャンが含まれます。カスタムスキャン実行時に、ウイルスやその他の危険性のある項目を検索する場所を設定することもできます。コンピュータ上のすべてのファイル、フォルダ、ドライブをスキャンすることも、特定のフォルダおよびドライブを限定的にスキャンすることもできます。

1 [カスタムスキャン] パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. SecurityCenter の[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。
3. [コンピュータとファイル]情報領域で、[**設定**]をクリックします。
4. [コンピュータとファイルの設定]パネルで、ウイルス対策が有効化されているか確認し、[**詳細設定**]をクリックします。
5. [ウイルス対策]パネルで[**手動スキャン**]をクリックします。

2 カスタムスキャンオプションを指定して、[**OK**] をクリックします。

設定...	手順...
未知のウイルスおよび既知のウイルスの新しい亜種の検出	[**未知のウイルスをスキャン**] を選択します。
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	[**アーカイブファイルをスキャン**] を選択します。
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検出	[**スパイウェアと潜在的な脅威をスキャン**] を選択します。
Cookie の検出	[**トラッキング Cookie をスキャンして削除**] を選択します。
既存の Windows システムファイルを変更および攻撃するルートキットとステルスプログラムを検出	[**ステルスプログラムのスキャン**] を選択します。
インターネットの閲覧や文書の作成など、ほかのタスクが優先されるため、スキャンに少ないプロセッサパワーを使用	[**最小限のコンピュータリソースを使用するスキャン**] を選択します。

設定...	手順...
スキャンするファイルの種類を指定	[**すべてのファイル（推奨）**] または [**プログラムファイルと文書のみ**] をクリックします。

3 [**標準設定のスキャン場所**] をクリックして、スキャンまたはスキップする場所を選択または選択解除して、[**OK**] をクリックします。

設定...	手順...
コンピュータ上のすべてのファイルおよびフォルダをスキャン	[**マイ コンピュータ**] を選択します。
コンピュータ上の特定のファイル、フォルダ、ドライブをスキャン	[**マイ コンピュータ**] チェックボックスの選択を解除し、1 つ以上のフォルダまたはドライブを選択します。
重要なシステムファイルをスキャン	[**マイ コンピュータ**] チェックボックスの選択を解除し、[**重要なシステムファイル**] チェックボックスを選択します。

スキャンのスケジュール

スキャンをスケジュールして、週や日に数回など、コンピュータのウイルスやほかの脅威をチェックできます。スケジュールスキャンは、標準設定のスキャンオプションを使用して、コンピュータ全体を常にチェックします。標準設定では、週 1 回のスキャンがスケジュール設定されています。 スキャン速度が遅い場合は、このオプションを無効にしてコンピュータリソースの使用を最小限に抑えることができます。ただしウイルス対策は他のタスクよりも優先度が高いことにご注意ください。

標準設定のスキャンオプションを使用してコンピュータ全体のウイルス、およびその他の脅威をチェックするスキャンをスケジュールします。標準設定では、週 1 回のスキャンがスケジュール設定されています。

1 [スケジュールスキャン] パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. SecurityCenter の[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。
3. [コンピュータとファイル]情報領域で、[**設定**]をクリックします。
4. [コンピュータとファイルの設定]パネルで、ウイルス対策が有効化されているか確認し、[**詳細設定**]をクリックします。
5. [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。

2 [**スケジュールスキャンを有効化**] を選択します。

3 スキャンに使用されるプロセッサパワーを軽減するには、[**最小限のコンピュータリソースを使用するスキャン**] を選択します。

4 1 日以上の日数を選択します。

5 開始時刻を指定します。

6 [**OK**] をクリックします。

ヒント: [**リセット**] をクリックして標準設定のスケジュールを復元できます。

McAfee SystemGuards オプションを使用

SystemGuards により、コンピュータ上の Windows のレジストリや重要なシステムファイルに対して実行された不正な変更を監視、ログ記録、レポートおよび管理できます。 レジストリおよびファイルが不正に変更されると、コンピュータに被害が及んだり、セキュリティが侵害されたり、重要なシステムファイルが損傷を受ける可能性があります。

レジストリおよびファイルの変更は頻繁にコンピュータ上で発生します。 ほとんどの変更は危険性がないため、SystemGuards のデフォルトの設定では、重大な脅威となりうる不正な変更に対して信頼できる高度な保護を提供するよう設定されています。 たとえば、重大な脅威を引き起こす可能性のある変更が SystemGuards で検出されると、その不正な活動はただちにレポート、記録されます。 一般的な変更ではあるものの、被害の可能性がゼロではない場合は、記録のみが実行されます。 ただし、デフォルトでは、標準でリスクの低い変更の監視は無効になっています。 SystemGuards の技術により、保護機能を拡張設定してあらゆる環境に適用できます。

SystemGuards には次の 3 種類があります: プログラム用 SystemGuards、Windows 用 SystemGuards およびブラウザ用 SystemGuards。

プログラム用 SystemGuards

プログラム用 SystemGuards は、コンピュータのレジストリや Windows に不可欠なその他の重要ファイルに対する不正な変更を検出します。 これらの重要なレジストリ項目およびファイルには、ActiveX のインストール、スタートアップ項目、Windows シェル実行フック、および ShellServiceObjectDelayLoad が含まれます。 これらを監視することで、プログラム用の SystemGuards 技術は、Windows 起動時に自動的に起動されるスパイウェアや怪しいプログラムに加え、不審な ActiveX プログラムを停止します。

Windows 用 SystemGuards

Windows 用 SystemGuards も、コンピュータのレジストリや Windows に不可欠なその他の重要ファイルに対する不正な変更を検出します。 これらの重要なレジストリ項目およびファイルには、コンテキスト メニュー ハンドラ、appInit DLLs および Windows Hosts ファイルが含まれます。 これらを監視することで、Windows 用の SystemGuards 技術は、不正な情報や個人情報の送受信を防止します。 また、ユーザやユーザの家族にとって重要なプログラムの表示や動作を不正に変更する不審なプログラムの停止にも有効です。

ブラウザ用 SystemGuards

プログラム用、Windows 用 SystemGuards と同様、ブラウザ用 SystemGuards も、コンピュータのレジストリや Windows に不可欠なその他の重要ファイルに対する不正な変更を検出します。 ただし、ブラウザ用 SystemGuards は、Internet Explorer アドオン、Internet Explorer URL および Internet Explorer セキュリティゾーンのような重要なレジストリ項目およびファイルに対する変更を監視します。 これらを監視することで、ブラウザ用 SystemGuards は、不審な Web サイトへのリダイレクトをはじめとする不正なブラウザアクティビティ、知らないうちに行われるブラウザ設定やオプションの変更、不審な Web サイトの信頼などを防止します。

McAfee SystemGuards による保護を有効化

SystemGuards による保護を有効化すると、コンピュータ上で変更された不正な Windows のレジストリやファイルが検出され、アラートが表示されます。 レジストリおよびファイルが不正に変更されると、コンピュータに被害が及んだり、セキュリティが侵害されたり、重要なシステムファイルが損傷を受ける可能性があります。

1 コンピュータとファイルの設定パネルを表示します。

アクセス方法

1. 左ペインで[**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. [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。

2 [**SystemGuard による保護**]で[**オン**]をクリックします。

注: [**オフ**]をクリックして SystemGuards による保護を無効化できます。

SystemGuards オプションの設定

[SystemGuards]パネルを使用して、Windows のファイル、プログラムおよび Internet Explorer に関連付けられた不正なレジストリやファイルの変更に対して、保護、ログ記録およびアラートオプションを設定します。 レジストリおよびファイルが不正に変更されると、コンピュータに被害が及んだり、セキュリティが侵害されたり、重要なシステムファイルが損害を受ける可能性があります。

1 [SystemGuards]パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. SecurityCenter の[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。

3. [コンピュータとファイル]情報領域で、[**設定**]をクリックします。
4. [コンピュータとファイルの設定]パネルで、SystemGuard による保護が有効化されているか確認し、[**詳細設定**]をクリックします。

2 リストから SystemGuard の種類を選択します。

- **プログラム用 SystemGuards**
- **Windows 用 SystemGuards**
- **ブラウザ用 SystemGuards**

3 [**オプションの選択**]で、次のいずれかの操作を実行します。

- プログラム用、Windows 用、ブラウザ用 SystemGuards に関連付けられた不正なレジストリおよびファイルの変更を検出し、ログに記録し、レポートするには、[**アラートを表示**]をクリックします。
- プログラム用、Windows 用、ブラウザ用 SystemGuards に関連付けられた不正なレジストリおよびファイルの変更を検出してログに記録するには、[**ログ記録のみ**]をクリックします。
- プログラム用、Windows 用、ブラウザ用 SystemGuards に関連付けられた不正なレジストリおよびファイルの変更の検出を無効にするには、[**この SystemGuard を無効化**]をクリックします。

注: SystemGuards の種類の詳細については、58 ページの「**SystemGuards の種類について**」を参照してください。

McAfee SystemGuards の種類について

McAfee SystemGuards は、コンピュータのレジストリおよび Window のその他の重要なファイルへの、不正な変更を検出します。 SystemGuards は 3 種類あります。 プログラム用 SystemGuards、Windows 用 SystemGuards およびブラウザ用 SystemGuards

プログラム用 SystemGuards

プログラム用 SystemGuards 技術により、Windows の起動時に自動的に起動されるスパイウェアや怪しいプログラムだけでなく、(インターネットからダウンロードした)不審な ActiveX プログラムが阻止されます。

SystemGuards	検出...
ActiveX のインストール	ActiveX のレジストリが不正に変更されると、コンピュータに被害が及んだり、セキュリティが侵害されたり、重要なシステムファイルが損害を受ける可能性があります。

SystemGuards	検出...
スタートアップ項目	スパイウェア、アドウェア、怪しいプログラムによりスタートアップ項目のファイルの変更がインストールされると、コンピュータの起動時に怪しいプログラムが実行される可能性があります。
Windows のシェル実行フック	スパイウェア、アドウェア、怪しいプログラムにより Windows のシェル実行フックがインストールされると、セキュリティプログラムが適切に動作しなくなる可能性があります。
ShellServiceObjectDelayLoad	スパイウェア、アドウェア、怪しいプログラムにより ShellServiceObjectDelayLoad のレジストリが変更されると、コンピュータの起動時に有害なファイルが実行される可能性があります。

Windows 用 SystemGuards

Windows 用 SystemGuards 技術により、不正な情報や個人情報の送受信が防止されます。 また、ユーザやユーザの家族にとって重要なプログラムの表示や動作を不正に変更する不審なプログラムの停止にも有効です。

SystemGuards	検出...
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 ハンドラのレジストリが不正に変更されると、Windows メニューの表示や動作に影響が出る可能性があります。 コンテキストメニューを使用すると、ファイルの右クリックなど、コンピュータ上でアクションを実行できます。
AppInit DLLs	Windows AppInit_DLL のレジストリが不正に変更されると、コンピュータを起動したときに有害なファイルが実行される可能性があります。
Windows Hosts ファイル	スパイウェア、アドウェア、怪しいプログラムにより Windows Hosts ファイルが不正に変更されると、ブラウザが不正な Web サイトにリダイレクトされたり、ソフトウェアの更新がブロックされる可能性があります。
Winlogon シェル	スパイウェア、アドウェア、怪しいプログラムにより Winlogon シェルのレジストリが変更されると、Windows Explorer の代わりに他のプログラムが実行される可能性があります。
WinlogonUserInit	スパイウェア、アドウェア、怪しいプログラムにより WinlogonUserInit のレジストリが変更されると、Windows にログオンしたときに怪しいプログラムが実行される可能性があります。

SystemGuards	検出...
Windows プロトコル	スパイウェア、アドウェア、怪しいプログラムにより Windows プロトコルのレジストリが変更されると、コンピュータがインターネットで情報を送受信する方法に影響が出る可能性があります。
WinSock LSP (Layered Service Provider)	スパイウェア、アドウェア、怪しいプログラムにより WinSock LSP（Layered Service Provider）のレジストリが変更されると、インターネットで送受信した情報が傍受されたり変更される可能性があります。
Windows シェルの Open コマンド	Windows シェルの Open コマンドが不正に変更されると、ワームやその他の不正プログラムがコンピュータ上で実行される可能性があります。
SharedTaskScheduler	スパイウェア、アドウェア、怪しいプログラムにより SharedTaskScheduler のレジストリおよびファイルが変更されると、コンピュータの起動時に有害なファイルが実行される可能性があります。
Windows Messenger サービス	スパイウェア、アドウェア、怪しいプログラムにより Windows Messenger サービスのレジストリが変更されると、コンピュータに未承諾広告が表示されたり、リモートからプログラムが実行される可能性があります。
Windows win.ini ファイル	スパイウェア、アドウェア、怪しいプログラムにより Win.ini ファイルが変更されると、コンピュータの起動時に怪しいプログラムが実行される可能性があります。

ブラウザ用 SystemGuards

ブラウザ用 SystemGuards 技術により、不審な Web サイトへのリダイレクトをはじめとする不正なブラウザアクティビティ、知らないうちに行われるブラウザ設定やオプションの変更、不審な Web サイトの信頼などを防止します。

SystemGuards	検出...
ブラウザ ヘルパー オブジェクト	スパイウェア、アドウェア、怪しいプログラムによりブラウザ ヘルパー オブジェクトが使用されると、Web 閲覧履歴が追跡されたり、未承諾広告が表示される可能性があります。
Internet Explorer バー	Internet Explorer のバー（[検索]や[お気に入り]など）のレジストリが不正に変更されると、Internet Explorer の表示および動作に影響が出る可能性があります。

SystemGuards	検出...
Internet Explorer アドオン	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer アドオンがインストールされると、Web 閲覧履歴が追跡されたり、未承諾広告が表示される可能性があります。
Internet Explorer ShellBrowser	Internet Explorer ShellBrowser のレジストリが不正に変更されると、Web ブラウザの表示や動作に影響が出る可能性があります。
Internet Explorer WebBrowser	Internet Explorer Web Browser のレジストリが不正に変更されると、Web ブラウザの表示や動作に影響が出る可能性があります。
Internet Explorer URL 検索フック	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer URL 検索フックのレジストリが変更されると、Web で検索を実行したときに不正な Web サイトにリダイレクトされる可能性があります。
Internet Explorer URL	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer URL のレジストリが変更されると、ブラウザの設定に影響が出る可能性があります。
Internet Explorer 制限	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer 制限のレジストリが変更されると、ブラウザの設定やオプションに影響が出る可能性があります。
Internet Explorer セキュリティゾーン	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer セキュリティゾーンのレジストリが変更されると、コンピュータの起動時に有害なファイルが実行される可能性があります。
Internet Explorer 信頼済みサイト	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer 信頼済みサイトのレジストリが変更されると、不正な Web サイトがブラウザにより信頼される可能性があります。
Internet Explorer のポリシー	スパイウェア、アドウェア、怪しいプログラムにより Internet Explorer ポリシーのレジストリが変更されると、ブラウザの表示やオプションに影響が出る可能性があります。

信頼リストの使用

McAfee VirusScan を使用して、ファイルやレジストリの変更（SystemGuard）、またはプログラムやバッファオーバーフローを検出する場合、検出された項目を信頼するか削除するかの選択が要求されます。 検出された項目を信頼し、今後この項目によるアクティビティに関する通知が不要な場合は、この項目を信頼リストに追加します。リストに追加すると、この項目は検出されなくなり、また通知されることもありません。 項目を信頼リストに登録したが、この項目のアクティビティをブロックする必要がある場合は、ブロックできます。 ブロックすると、その項目がコンピュータ上で実行されコンピュータに変更を加えることを防止でき、アクティビティに関して通知されることもありません。 また、信頼リストから項目を削除することもできます。 削除すると、McAfee VirusScan によって再度その項目のアクティビティが検出されます。

信頼リストを管理

[信頼リスト]パネルを使用して、以前検出され信頼済の項目を、信頼またはブロックできます。 また、信頼リストから項目を削除すると、McAfee VirusScan によって再度検出されます。

1 [信頼リスト]パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. SecurityCenter の[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。
3. [コンピュータとファイル]情報領域で、[**設定**]をクリックします。
4. [コンピュータとファイルの設定]パネルで、ウイルス対策が有効化されているか確認し、[**詳細設定**]をクリックします。
5. [ウイルス対策]パネルで[**信頼リスト**]をクリックします。

2 以下の信頼リストのうち、いずれかの種類を選択します。

- **プログラム用 SystemGuards**
- **Windows 用 SystemGuards**
- **ブラウザ用 SystemGuards**
- **信頼するプログラム**
- **信頼するバッファオーバーフロー**

3 [**オプションの選択**]で、次のいずれかの操作を実行します。

- Windows レジストリまたはコンピュータ上の重要なシステムファイルの変更を通知なく許可するには、[**信頼**]をクリックします。

- Windows レジストリまたはコンピュータ上の重要なシステムファイルの変更を通知なくブロックするには、[**ブロック**]をクリックします。
- 信頼リストから検出された項目を削除するには、[**削除**]をクリックします。

4　[**OK**]をクリックします。

注: 信頼リストの種類の詳細については、63 ページの「**信頼リストの種類について**」を参照してください。

信頼リストの種類について

[信頼リスト]パネルの SystemGuards は、McAfee VirusScan（マカフィー・ウイルススキャン）によって検出された、以前許可なく変更されたレジストリとファイルを表します。ただし、アラートまたは[スキャン結果]パネルで許可したものに限ります。 M[信頼リスト]パネルで管理可能な信頼リストには、プログラム用 SystemGuards、Windows 用 SystemGuards、ブラウザ用 SystemGuards、信頼するプログラム、および信頼するバッファオーバーフローの 5 種類があります。

オプション	説明
プログラム用 SystemGuards	[信頼リスト]パネルのプログラム用 SystemGuards は、McAfee VirusScan によって検出された、以前許可なく変更されたレジストリとファイルを表します。ただし、アラートまたは[スキャン結果]パネルで許可したものに限ります。 プログラム用 SystemGuards では、ActiveX のインストール、スタートアップ項目、Windows のシェル実行フック、および ShellServiceObjectDelayLoad に関連した、レジストリとファイルの許可のない変更を検出されます。 レジストリおよびファイルが不正に変更されると、コンピュータに被害が及んだり、セキュリティが侵害されたり、重要なシステムファイルが損害を受ける可能性があります。

オプション	説明
Windows 用 SystemGuards	[信頼リスト]パネルの Windows 用 SystemGuards は、McAfee VirusScan によって検出された、以前許可なく変更されたレジストリとファイルを表します。ただし、アラートまたは[スキャン結果]パネルから選択されたものです。 Windows 用 SystemGuards は、コンテキスト メニュー ハンドラ、AppInit DLLs、Windows Hosts ファイル、Winlogon シェル、および Winsock LSP (Layered Service Provider)などに関連する、レジストリとファイルの許可のない変更を検出します。 ご使用のコンピュータのレジストリおよびファイルが許可なく変更されると、インターネット上での情報の送受信方法が影響を受ける可能性があり、プログラムの表示や動作が変更され、怪しいプログラムの実行が許可される可能性があります。
ブラウザ用 SystemGuards	[信頼リスト]パネルのブラウザ用 SystemGuards は、McAfee VirusScan によって検出された、以前許可なく変更されたレジストリとファイルを表します。ただし、アラートまたは[スキャン結果]パネルから選択したものに限ります。 ブラウザ用 SystemGuards は、ブラウザ ヘルパー オブジェクト、Internet Explorer アドオン、Internet Explorer URL、Internet Explorer セキュリティゾーンなどに関する、レジストリの許可のない変更と不審な動作を検出します。 レジストリのこの種類の許可のない変更によって、不審な Web サイトへのリダイレクトや、ブラウザ設定およびオプションの変更、不審な Web サイトの信用などの、ブラウザの不正なアクティビティが発生する恐れがあります。
信頼するプログラム	信頼するプログラムは、McAfee VirusScan によって以前検出された怪しいプログラムである可能性がありますが、アラートまたは[スキャン結果]パネルで信頼することを選択したプログラムです。
信頼するバッファオーバーフロー	信頼するバッファオーバーフローは、McAfee VirusScan(マカフィー・ウイルススキャン)によって以前検出された不審なアクティビティである可能性がありますが、アラートまたは[スキャン結果]パネルで信頼することを選択したプログラムです。 バッファオーバーフローにより、コンピュータが攻撃されたりファイルが損傷を受ける可能性があります。バッファオーバーフローは、怪しいプログラムまたはプロセスが保存しようとする情報量がバッファの制限を越えた場合に発生します。

第 13 章

McAfee Personal Firewall (マカフィー・パーソナルファイアウォール)

McAfee Personal Firewall (マカフィー・パーソナルファイアウォール)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。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。

このセクションの内容

McAfee Personal Firewall の機能 66
ファイアウォールを起動 67
アラートを使用 69
情報アラートを管理 73
ファイアウォールによる保護の設定 75
プログラムと権限を管理 87
コンピュータ接続を管理 95
システムサービスを管理 103
ログ記録、監視、分析 109
インターネットセキュリティについての確認 119

McAfee Personal Firewall の機能

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コンピュータを保護できます。また、保護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優れたアクセス管理	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、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を表示しないようにします。
コンピュータの起動時の保護	Windows が起動するとすぐに、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	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の開閉を管理できます。
コンピュータ接続の管理	ほかのコンピュータとご使用のコンピュータ間のリモート接続を許可またはブロックできます。
HackerWatch 情報の統合	HackerWatch の Web サイトから世界中のハッカー行為や侵入パターンを追跡できます。また、コンピュータ上のプログラムに関する現在のセキュリティ情報、および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が提供されます。
ファイアウォールのロック	ロックすると、コンピュータとインターネット間のすべての送受信トラフィックが完全にブロックされます。
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	不審なアプリケーションを検出およびブロックできます。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送信することを防ぎます。
イベントログの記録	最近の受信、送信、および侵入イベントが記録されます。
インターネットトラフィックの監視	世界中の地図を表示して、悪質な攻撃やトラフィックの発信元を追跡できます。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、送受信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	インターネット上の脅威からプライバシーを保護できます。ヒューリスティックな機能を使い、攻撃の兆候や、ハッキング行為の特徴をブロックする、第三の保護レイヤを提供します。
高度なトラフィック分析	送信、受信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。

第 14 章

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 [自動] に設定されます (プログラムにインターネットへの送信アクセスのみ許可するためのオプションが含まれます)。

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。

このセクションの内容

ファイアウォールによる保護を開始 67
ファイアウォールによる保護を停止 68

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。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が無効です**]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

コンピュータを侵入や不審なネットワークトラフィックから保護しない場合、ファイアウォールを無効にできます。 ファイアウォールを無効にした場合、インターネット接続を管理できません。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**オフ**]をクリックします。

第 15 章

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、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

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。

このセクションの内容

アラートについて 70

アラートについて

ファイアウォールには 3 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。

レッドアラート

レッドアラートは、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。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。このアラートは、すべてのセキュリティレベルで表示されます。

イエローアラート

最も一般的なアラートタイプはイエローアラートで、ファイアウォールが検出した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関する情報が通知されます。この場合、アラートに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説明され、1 つ以上のオプションに対応する必要があります。たとえば、[**新しいネットワーク接続**] アラートは、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。新しいネットワークに割り当てる信用レベルを指定できます。指定した信用レベルは [ネットワーク] リストに表示されます。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] パネルに既知のプログラムが自動的に追加されます。

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。標準設定では、グリーンアラートは無効です。

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。

第 16 章

情報アラートを管理

全画面表示でゲームをプレイしている間などの特定のイベント中に、侵入や不審な活動が検出された場合に、情報アラートを表示または隠すように、ファイアウォールを設定できます。

このセクションの内容

ゲーム中にアラートを表示 73
情報アラートを非表示化 73

ゲーム中にアラートを表示

全画面表示でゲームをプレイしている間に、侵入や不審な活動が検出された場合に、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できます。

1 [McAfee SecurityCenter]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]パネルの[**アラート**]で、[**詳細設定**]をクリックします。

4 [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。

5 [**OK**]をクリックします。

情報アラートを非表示化

侵入や不審な活動が検出された場合に、情報アラートが表示されないように、ファイアウォールを設定できます。

1 [McAfee SecurityCenter]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]パネルの[**アラート**]で、[**詳細設定**]をクリックします。

4 [SecurityCenter の設定]パネルで[**情報アラート**]をクリックします。

5 [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。

- [**情報アラートを表示しない**]を選択してすべての情報アラートを隠します。

- アラートの非表示の選択を解除します。

6 [**OK**]をクリックします。

第 17 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、コンピュータの保護のセキュリティレベルは [自動] に設定されていて、プログラムはインターネットへの送信アクセスのみが許可されています。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、ほか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。

このセクションの内容

ファイアウォールのセキュリティレベルを管理.....76
スマートリコメンデーションのアラートの設定 79
ファイアウォールによるセキュリティを最適化 81
ファイアウォールをロックおよび復元.....84

ファイアウォールのセキュリティレベルを管理

ファイアウォールのセキュリティレベルを設定することで、アラートの管理および対処の度合いを決定できます。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に、これらのアラートが表示されます。標準設定では、送信アクセスについてのファイアウォールのセキュリティレベルが [自動] に設定されています。

セキュリティレベルが [自動] でスマートリコメンデーションが有効な場合、イエローアラートには、受信アクセスを必要とする未知の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。標準設定では、グリーンアラートは無効ですが、既知のプログラムが検出され、アクセスが自動的に許可されると、グリーンアラートが表示されます。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 (ステルスおよび標準) 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。

次の表では、ファイアウォールの 3 種類のセキュリティレベルを説明しています。それぞれインターネット接続への対応が異なります。

レベル	説明
ステルス	開かれているポート以外で、すべての内向き (受信) 接続がブロックされます。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。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、または内向き (受信) 接続要求を受信した場合、ファイアウォールにより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。
標準	内向き (受信) 、外向き (送信) の接続が監視され、新しいプログラムがインターネットアクセスを試行すると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。
自動	プログラムに対して、インターネットへの送受信または送信アクセスのみのいずれかを許可します。標準設定のセキュリティレベルは [自動] で、プログラムに対して送信のみのアクセスが許可されます。 完全アクセスを許可すると、ファイアウォールはプログラムを自動的に信頼し、[プログラム許可機能] パネルで許可されたプログラムのリストにそのプログラムを追加します。 送信アクセスのみを許可すると、インターネット接続のみ実行する際に、ファイアウォールはプログラムを自動的に信頼します。内向き (受信) 接続の場合は自動的に信頼されません。

また、[ファイアウォールを標準設定に戻す] パネルから、セキュリティレベルを簡単に [自動] (送信アクセスのみを許可) に戻すこともできます。

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、すべての内向き (受信) 接続がブロックされ、インターネット上で使用しているコンピュータの存在を隠すことができます。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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。

4 [**OK**] をクリックします。

注: ステルスモードでは、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、または内向き (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。

セキュリティレベルの設定: 標準

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。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 [**OK**]をクリックします。

セキュリティレベルの設定: 自動

ファイアウォールのセキュリティレベルを [自動] に設定すると、完全アクセスまたは送信アクセスのみのいずれかを許可できます。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [セキュリティレベル] パネルで、スライダーを移動して [**自動**] を現在のレベルとして表示します。

4 次のいずれかの操作を実行します。

- 完全な送受信ネットワークアクセスを許可するには、[**すべてのアクセスを許可**] を選択します。
- 送信のみのネットワークアクセスを許可するには、[**送信アクセスのみを許可**] を選択します。

5 [**OK**] をクリックします。

注: [**送信アクセスのみを許可**] は標準設定のオプションです。

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が適用されている場合 (セキュリティレベルが [自動] に設定されていて、送信アクセスのみ有効な場合)、既知のプログラムを自動的に許可し、潜在的に危険なプログラムをブロックします。

スマートリコメンデーションが適用されていない場合は、インターネットアクセスの許可もブロックも行われず、アラートにアドバイスは表示されません。

スマートリコメンデーションが [表示] に設定されている場合は、アクセスの許可またはブロックを問うアラートが表示され、アラートにアドバイスが表示されます。

スマートリコメンデーションを有効化

ファイアウォールのスマートリコメンデーションを有効化すると、プログラムの許可またはブロックが自動的に実行され、認識されていないプログラムや潜在的に危険なプログラムについてアラートが表示されます。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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適用**] をクリックします。

4 [**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

ファイアウォールのスマートリコメンデーションを無効化すると、プログラムの許可またはブロックが実行され、認識されていないプログラムや潜在的に危険なプログラムについてアラートが表示されます。ただし、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。また、ファイアウォールにより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自動的にブロックされます。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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適用しない**] をクリックします。

4 [**OK**] をクリックします。

スマートリコメンデーションを表示

スマートリコメンデーションを表示すると、アラートにアドバイスのみ表示されます。そのため、認識されていないプログラムや潜在的に危険なプログラムの許可またはブロックの判断はユーザが行うことになります。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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表示**] をクリックします。

4 [**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はさまざまな方法で侵害されます。たとえば、Windows の起動時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。コンピュータに詳しいユーザは、コンピュータを追跡または 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。また、UDP プロトコルを使用して、メッセージ単位 (データグラム) でコンピュータに情報を送信することもできます。ファイアウォールは、Windows の起動時にプログラムのインターネットアクセスをブロックしたり、ほか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 要求をブロックしたり、ほかのユーザによりメッセージ単位 (データグラム) でコンピュータに情報が送信されるのを無効にして、前述のような侵入からコンピュータを保護します。

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一般的な侵入行為の自動的検出が設定されます。 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。自動的に検出する攻撃とスキャンの種類は[侵入検知] パネルで無効化できます。

起動中のコンピュータを保護

Windows の起動時にコンピュータを保護して、起動中にインターネットへのアクセスを要求する新しいプログラムをブロックできます。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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [セキュリティレベル] パネルの [**セキュリティ設定**] で、[**Windows 起動時に保護を有効化**] をクリックします。

4 [**OK**] をクリックします。

注: 起動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

他のユーザによってネットワーク上の使用しているコンピュータの検出を許可または拒否できます。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。
- [**ICMP ping 要求を許可**]の選択を解除して、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拒否します。

4 [**OK**]をクリックします。

UDP の設定

ほかのネットワークコンピュータユーザが UDP プロトコルを使用して、ご使用のコンピュータにメッセージ単位 (データグラム) の情報を送信できるように設定できます。ただし、システムサービスポートを閉じてこのプロトコルをブロックした場合にのみ、設定可能です。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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。

- [**UDP トラッキングを有効化**] を選択して、ほかのコンピュータユーザによるコンピュータへのメッセージ単位 (データグラム) の情報送信を許可します。
- [**UDP トラッキングを有効化**] の選択を解除して、ほかのコンピュータユーザがご使用のコンピュータにメッセージ単位 (データグラム) の情報を送信できないようにします。

4 [**OK**] をクリックします。

侵入検知の設定

侵入を検出して、攻撃や不正スキャンからコンピュータを保護できます。標準設定では、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。ただし、1 つ以上の攻撃またはスキャンに対して、自動検出を無効化できます。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [ファイアウォール]パネルで[**侵入検知**]をクリックします。

4 [**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。

5 ［**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 へのレポート対象とならない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。

1 [McAfee SecurityCenter] パネルの [**SecurityCenter の情報**] で、[**設定**] をクリックします。

2 [SecurityCenter の設定] パネルの [**保護の状態**] で、[**詳細設定**] をクリックします。

3 [無視された問題] パネルで、次のオプションから 1 つ以上を選択します。

- **ファイアウォールによる保護が無効です。**
- **ファイアウォールサービスが実行されていません。**
- **ファイアウォールによる保護がインストールされていません。**
- **Windows Firewall が無効です。**
- **外向き通信用ファイアウォールがインストールされていません。**

4 [**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ネットワーク接続が内向き (受信)、外向き (送信) にかかわらずすべてブロックされます。ロックすると、コンピュータのネットワークケーブルの接続を解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] パネルで開かれているポートがブロックされ、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。

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、コンピュータとインターネット間のすべてのネットワークトラフィックをブロックできます。

1 [McAfee SecurityCenter] パネル (ウィンドウ枠) の [**よく使う機能**] 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 [**ファイアウォールのロックダウンを有効にする**] をクリックします。

3 [**はい**] をクリックして、確認します。

ヒント: タスクバー右側の通知領域にある [McAfee SecurityCenter] アイコンを右クリックして、[**クイック リンク**] をクリックし [**ファイアウォールのロック**] をクリックしても、ファイアウォールをロックできます。

ファイアウォールを迅速にロック解除

ファイアウォールのロックを解除すると、コンピュータと、インターネットを含むネットワーク間のすべてのネットワークトラフィックが許可されます。

1 [McAfee SecurityCenter] パネル (ウィンドウ枠) の [**よく使う機能**] 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 [**ファイアウォールのロックダウンの無効化**] をクリックします。

3 [**はい**] をクリックして、確認します。

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。この復元によりセキュリティレベルは [自動] にリセットされ、送信アクセスのみ許可されます。これにより、スマートリコメンデーションが有効化され、[プログラム許可機能] パネルにデフォルトプログラムと権限のリストが復元され、信用する IP アドレスと禁止された IP アドレスが削除され、システムサービス、イベントログ設定および侵入検知が復元されます。

1 [McAfee SecurityCenter] 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　[**はい**] をクリックして、確認します。

4　[**OK**] をクリックします。

第 18 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。 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対して制御できます。 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。

このセクションの内容

プログラムのインターネットアクセスを許可 88
プログラムに送信アクセスのみを許可 90
プログラムのインターネットアクセスをブロック 91
プログラムのアクセス権を削除 92
プログラムについての確認 93

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、送信イベントログまた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があるプログラム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

コンピュータ上でブロックされた既存のプログラムを許可すると、インターネットへの完全な送受信アクセスが可能になります。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 [**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**]のプログラムを選択します。

5 [**対応**]で[**アクセスを許可**]をクリックします。

6 [**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

コンピュータ上でブロックされた新規のプログラムを許可すると、インターネットへの完全な送受信アクセスが可能になります。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 [**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。

5 [**プログラムの追加**]ダイアログボックスで、追加するプログラムを参照して選択し、[**開く**]をクリックします。

注: プログラムを選択して、[**対応**]で[**送信アクセスのみを許可**]または[**アクセスをブロック**]をクリックすることにより、既存のプログラムと同様、新規に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

最近のイベントログに表示されるブロックされた既存のプログラムを許可すると、インターネットへの完全な送受信アクセスが可能になります。

1 [McAfee SecurityCenter]パネルで、[**詳細メニュー**]をクリックします。

2 [**レポートとログ**]をクリックします。

3 [**最近のイベント**]で、イベントの説明を選択し、[**アクセスを許可**]をクリックします。

4 [プログラム許可機能]ダイアログで[**はい**]をクリックして、確認します。

関連項目

- **送信イベントを表示** (111 ページ)

送信イベントログからすべてのアクセスを許可

送信イベントログに表示されるブロックされた既存のプログラムを許可すると、インターネットへの完全な送受信アクセスが可能になります。

1 [McAfee SecurityCenter]パネルで、[**詳細メニュー**]をクリックします。

2 [**レポートとログ**]をクリックします。

3 [**最近のイベント**]で[**ログを表示**]をクリックします。

4 [**インターネットとネットワーク**]をクリックして、[**送信イベント**]をクリックします。

5 プログラムを選択して、[**オプションの選択**]で[**アクセスを許可**]をクリックします。

6 [プログラム許可機能]ダイアログで[**はい**]をクリックして、確認します。

プログラムに送信アクセスのみを許可

コンピュータ上の一部のプログラムには、送信インターネットアクセスが必要です。 ファイアウォールにより、インターネットへの送信アクセスのみ許可するプログラム権限を設定できます。

プログラムに送信アクセスのみを許可

プログラムのインターネットへの送信アクセスのみ許可できます。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 [**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**]のプログラムを選択します。

5 [**対応**]で[**送信アクセスのみを許可**]をクリックします。

6 [**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

最近のイベントログに表示されるブロックされた既存のプログラムを許可すると、インターネットへの送信アクセスのみ可能になります。

1 [McAfee SecurityCenter]パネルで、[**詳細メニュー**]をクリックします。

2 [**レポートとログ**]をクリックします。

3 [**最近のイベント**]で、イベントの説明を選択し、[**送信アクセスのみを許可**]をクリックします。

4 [プログラム許可機能]ダイアログで[**はい**]をクリックして、確認します。

送信イベントログから送信アクセスのみを許可

送信イベントログに表示されるブロックされた既存のプログラムを許可すると、インターネットへの送信アクセスのみ可能になります。

1 [McAfee SecurityCenter]パネルで、[**詳細メニュー**]をクリックします。

2 [**レポートとログ**]をクリックします。

3 [**最近のイベント**]で[**ログを表示**]をクリックします。

4 [**インターネットとネットワーク**]をクリックして、[**送信イベント**]をクリックします。

5 プログラムを選択して、[**オプションの選択**]で[**送信アクセスのみを許可**]をクリックします。

6　[プログラム許可機能]ダイアログで[**はい**]をクリックして、確認します。

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

プログラムのインターネットアクセスを送信、受信ともブロックできます。

1　[McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3　[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。

4　[**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**]のプログラムを選択します。

5　[**対応**]で[**アクセスをブロック**]をクリックします。

6　[**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

新しいプログラムのインターネットアクセスを送信、受信ともブロックできます。

1　[McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3　[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。

4　[**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。

5　[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、[**開く**]をクリックします。

注: 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

最近のイベントログに表示されているプログラムが、インターネットアクセスで送受信されるのをブロックできます。

1 [McAfee SecurityCenter]パネルで、[**詳細メニュー**]をクリックします。

2 [**レポートとログ**]をクリックします。

3 [**最近のイベント**]で、イベントの説明を選択し、[**アクセスをブロック**]をクリックします。

4 [プログラム許可機能]ダイアログで[**はい**]をクリックして、確認します。

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

プログラムがインターネットアクセスで送受信されるのを削除できます。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 [**プログラム許可機能**]でプログラムを選択します。

5 [**対応**]で[**プログラムの許可を削除**]をクリックします。

6 [**OK**]をクリックします。

注: プログラムの中には、特定の対応が無効 (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

マカフィーの HackerWatch の Web サイトからプログラム情報を取得して、インターネットへの送受信アクセスの許可またはブロックを選択できます。

注:マカフィーの HackerWatch の Web サイトが表示されるように、インターネットに接続していることを確認します。このサイトに、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。

1 [McAfee SecurityCenter]パネルで、[**インターネットとネットワーク**]をクリックしてから[**設定**]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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 [**プログラム許可機能**]でプログラムを選択します。

5 [**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

送信イベントログで、マカフィーの HackerWatch の Web サイトからプログラム情報を取得して、インターネットへの送受信アクセスを許可またはブロックするプログラムを選択できます。

注:マカフィーの HackerWatch の Web サイトが表示されるように、インターネットに接続していることを確認します。このサイトに、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。

1 [McAfee SecurityCenter]パネルで、[**詳細メニュー**]をクリックします。

2 [**レポートとログ**]をクリックします。

3 [最近のイベント]で、イベントを選択して[**ログを表示**]をクリックします。

4 [**インターネットとネットワーク**]をクリックして、[**送信イベント**]をクリックします。

5 IP アドレスを選択し、[**詳細情報**]をクリックします。

第 19 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。信用する 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。信用する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。[**ネットワーク**] リストの信用する 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 アドレス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。

このセクションの内容

コンピュータ接続について 96
コンピュータ接続を禁止 100

コンピュータ接続について

コンピュータ接続とは、すべてのネットワーク上のほかのコンピュータとご使用のコンピュータ間の接続です。[**ネットワーク**] リストで IP アドレスを追加、編集および削除できます。これらの IP アドレスは、コンピュータへの接続時に信頼レベルを割り当てるネットワークに関連付けられています。割り当てる信頼レベルは、信用、標準および公開のいずれかです。

レベル	説明
信用	ファイアウォールは IP からのトラフィックを許可し、すべてのポートを経由したトラフィックをコンピュータに送信します。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。標準設定では、ファイアウォールによって検出された最初のプライベートネットワークは [**ネットワーク**] リストに [信用] として表示されます。信用するネットワークは、ローカルネットワークまたはホームネットワーク上のコンピュータなどです。
標準	ファイアウォールは、コンピュータへの接続時に IP からのトラフィック (ネットワーク上のほかのコンピュータからのトラフィックを除く) を制御し、[**システムサービス**] リストのルールに従って、その IP を許可またはブロックします。ファイアウォールは、トラフィックをログに記録し、標準 IP アドレスからのイベントアラートを生成します。標準ネットワークは、社内ネットワーク上のコンピュータなどです。
公開	ファイアウォールは、[**システムサービス**] リストのルールに従って公開ネットワークからのトラフィックを制御します。公開ネットワークは、カフェ、ホテルまたは空港からインターネット接続するネットワークなどです。

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。信用する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。

コンピュータ接続を追加

信用、標準または公開の各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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [ファイアウォール] パネルで [**ネットワーク**] をクリックします。

4 [ネットワーク] パネルで [**追加**] をクリックします。

5 コンピュータが IPv6 ネットワークで接続されている場合、[**IPv6**] チェックボックスを選択します。

6 [**ルールを追加**] で、次のいずれかの操作を実行します。

- [**単一**] を選択し、[**IP アドレス**] ボックスに IP アドレスを入力します。
- [**範囲**] を選択して、[**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。コンピュータが IPv6 ネットワークで接続されている場合、[**開始 IP アドレス**] および [**プレフィックスの長さ**] ボックスに開始 IP アドレスとプレフィックスの長さを入力します。

7 [**タイプ**] で、次のいずれかの操作を実行します。

- このコンピュータ接続を信頼できる接続として指定する場合は、[**信用**] を選択します (ホームネットワーク上のコンピュータなどが対象)。
- このコンピュータ接続を信頼できる接続として指定する場合は、[**標準**] を選択します (社内ネットワーク上のコンピュータなどが対象)。
- このコンピュータ接続を公衆ネットワークとして指定する場合は、[**公開**] を選択します (インターネットカフェやホテル、空港などのコンピュータなどが対象)。

8 システムサービスでインターネット接続共有 (ICS) が使用される場合、追加できる IP アドレスの範囲は 192.168.0.1 から 192.168.0.255 です。

9 [**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)。

10 ルールの説明を入力します (オプション)。

11 [**OK**] をクリックします。

注: インターネット接続共有 (ICS) の詳細については、「新しいシステムサービスの設定」を参照してください。

受信イベントログから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および標準コンピュータ接続と、コンピュータに関連する IP アドレスを追加できます。

1 [McAfee SecurityCenter] パネルの [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 [**レポートとログ**] をクリックします。

3 [**最近のイベント**] で [**ログを表示**] をクリックします。

4 [**インターネットとネットワーク**] をクリックして、[**受信イベント**] をクリックします。

5 送信元 IP アドレスを選択して、[**オプションの選択**] で次のいずれかの操作を実行します。

- [**この IP を「信用」に追加**] をクリックして、このコンピュータを「信用」として [**ネットワーク**] リストに追加します。
- [**この IP を「標準」に追加**] をクリックして、このコンピュータ接続を「標準」として [**ネットワーク**] リストに追加します。

6 [**はい**] をクリックして、確認します。

コンピュータ接続を編集

信用、標準または公開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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [ファイアウォール] パネルで [**ネットワーク**] をクリックします。

4 [ネットワーク] パネルで IP アドレスを選択し、[**編集**] をクリックします。

5 コンピュータが IPv6 ネットワークで接続されている場合、[**IPv6**] チェックボックスを選択します。

6 [**ルールを編集**] で、次のいずれかの操作を実行します。

- [**単一**] を選択し、[**IP アドレス**] ボックスに IP アドレスを入力します。
- [**範囲**] を選択して、[**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。コンピュータが IPv6 ネットワークで接続されている場合、[**開始 IP アドレス**] および [**プレフィックスの長さ**] ボックスに開始 IP アドレスとプレフィックスの長さを入力します。

7 [**タイプ**] で、次のいずれかの操作を実行します。

- このコンピュータ接続を信頼できる接続として指定する場合は、[**信用**] を選択します (ホームネットワーク上のコンピュータなどが対象)。
- このコンピュータ接続を信頼できる接続として指定する場合は、[**標準**] を選択します (社内ネットワーク上のコンピュータなどが対象)。
- このコンピュータ接続を公衆ネットワークとして指定する場合は、[**公開**] を選択します (インターネットカフェやホテル、空港などのコンピュータなどが対象)。

8 [**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)。

9 ルールの説明を入力します (オプション)。

10 [**OK**] をクリックします。

注: 信用しているプライベートネットワークから、ファイアウォールにより自動的に追加された標準設定のコンピュータ接続は、編集できません。

コンピュータ接続を削除

信用、標準または公開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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [ファイアウォール] パネルで [**ネットワーク**] をクリックします。

4 [ネットワーク] パネルで IP アドレスを選択し、[**削除**] をクリックします。

5 [**はい**] をクリックして、確認します。

コンピュータ接続を禁止

[禁止 IP] パネルで、禁止 IP アドレスを追加、編集および削除できます。

未知の IP、不審な IP、信用されていない IP アドレス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。

禁止するコンピュータ接続を追加

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。

注: 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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [ファイアウォール] パネルで [**禁止 IP**] をクリックします。

4 [禁止 IP] パネルで [**追加**] をクリックします。

5 コンピュータが IPv6 ネットワークで接続されている場合、[**IPv6**] チェックボックスを選択します。

6 [**ルールを追加**] で、次のいずれかの操作を実行します。

- [**単一**] を選択し、[**IP アドレス**] ボックスに IP アドレスを入力します。
- [**範囲**] を選択して、[**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。コンピュータが IPv6 ネットワークで接続されている場合、[**開始 IP アドレス**] および [**プレフィックスの長さ**] ボックスに開始 IP アドレスとプレフィックスの長さを入力します。

7 [**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)。

8 ルールの説明を入力します (オプション)。

9 [**OK**] をクリックします。

10 [**はい**] をクリックして、確認します。

禁止するコンピュータ接続を編集

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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [ファイアウォール] パネルで [**禁止 IP**] をクリックします。

4 [禁止 IP] パネルで [**編集**] をクリックします。

5 コンピュータが IPv6 ネットワークで接続されている場合、[**IPv6**] チェックボックスを選択します。

6 [**ルールを編集**] で、次のいずれかの操作を実行します。

- [**単一**] を選択し、[**IP アドレス**] ボックスに IP アドレスを入力します。
- [**範囲**] を選択して、[**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。コンピュータが IPv6 ネットワークで接続されている場合、[**開始 IP アドレス**] および [**プレフィックスの長さ**] ボックスに開始 IP アドレスとプレフィックスの長さを入力します。

7 [**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)。

8 ルールの説明を入力します (オプション)。

9 [**OK**] をクリックします。

禁止するコンピュータ接続を削除

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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [ファイアウォール] パネルで [**禁止 IP**] をクリックします。

4 [禁止 IP] パネルで IP アドレスを選択し、[**削除**] をクリックします。

5 [**はい**] をクリックして、確認します。

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

すべての受信トラフィックを IP アドレスからブロックする場合、システムサービスポートが開いているか閉じているかに関係なく、[**禁止 IP**] リストに IP アドレスを追加します。

1 [McAfee SecurityCenter] パネル (ウィンドウ枠) の [**よく使う機能**] で、[**詳細メニュー**] をクリックします。

2 [**レポートとログ**] をクリックします。

3 [**最近のイベント**] で [**ログを表示**] をクリックします。

4 [**インターネットとネットワーク**] をクリックして、[**受信イベント**] をクリックします。

5 送信元 IP アドレスを選択して、[**オプションの選択**] で [**この IP を禁止**] をクリックします。

6 [**はい**] をクリックして、確認します。

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。

1 [McAfee SecurityCenter] パネル (ウィンドウ枠) の [**よく使う機能**] で、[**詳細メニュー**] をクリックします。

2 [**レポートとログ**] をクリックします。

3 [**最近のイベント**] で [**ログを表示**] をクリックします。

4 [**インターネットとネットワーク**] をクリックして、[**侵入検知イベント**] をクリックします。

5 送信元 IP アドレスを選択して、[**オプションの選択**] で [**この IP を禁止**] をクリックします。

6 [**はい**] をクリックして、確認します。

第 20 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介し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。

このセクションの内容

システムサービスポートの設定 104

システムサービスポートの設定

システムサービスポートを設定して、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。[**ネットワーク**] リストに信用、標準または公開として記載されているコンピュータに対して、システムサービスポートを開いたり閉じたりできます。

一般的なシステムサービスと関連するポートは次のとおりです。

- 一般的なオペレーティングシステムポート 5357
- 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
- ネットワークタイムプロトコルポート 123
- リモートデスクトップ/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

また、システムサービスポートを設定すると、そのコンピュータに接続しているほかコンピュータも、同じネットワークを経由してインターネット接続を共有できます。インターネット接続共有 (ICS) といわれるこの接続方法では、インターネット接続を共有している一方のコンピュータが、接続されているほかのコンピュータのゲートウェイとして機能します。

注: コンピュータに、Web または FTP サーバ接続のいずれかを受け入れるアプリケーションを搭載している場合、接続を共有しているコンピュータの関連するシステムサービスポートを開き、そのポートへの接続の転送を許可する必要がある場合もあります。

既存のシステムサービスポートへのアクセスを許可

既存のポートを開いて、コンピュータ上のネットワークシステムサービスへのリモートアクセスを許可できます。

注: 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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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。

4 [**システムサービスのポートを開く**] で、ポートを開くシステムサービスを選択します。

5 [**編集**] をクリックします。

6 次のいずれかの操作を実行します。

- 信用、標準または公開ネットワーク上のすべてのコンピュータ (ホームネットワーク、社内ネットワークまたはインターネット接続のネットワークなど) に対してポートを開くには、[**信用、標準および公開**] を選択します。
- 標準ネットワーク (社内ネットワークなど) 上のコンピュータに対してポートを開くには、[**標準 (信用も含む)**] を選択します。

7 [**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

既存のポートを閉じて、コンピュータ上のネットワークシステムサービスへのリモートアクセスをブロックできます。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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。

4 [**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横のチェックボックスの選択を解除します。

5 [**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

ポートを開くか閉じて、コンピュータ上のリモートアクセスを許可またはブロックできるコンピュータ上で、新しいネットワークサービスポートを設定できます。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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。

4 [**追加**] をクリックします。

5 [システムサービス] パネルの [**システム サービス ルールを追加**] で、次の項目を入力します。

- システムサービス名
- システムサービスカテゴリ
- ローカル TCP/IP ポート
- ローカル UDP ポート

6 次のいずれかの操作を実行します。

- 信用、標準または公開ネットワーク上のすべてのコンピュータ (ホームネットワーク、社内ネットワークまたはインターネット接続のネットワークなど) に対してポートを開くには、[**信用、標準および公開**] を選択します。
- 標準ネットワーク (社内ネットワークなど) 上のコンピュータに対してポートを開くには、[**標準 (信用も含む)**] を選択します。

7 インターネット接続を共有しているほかの Windows のネットワークコンピュータに、このポートのアクティビティ情報を送信する場合は、[**このポートのネットワークアクティビティをインターネット接続共有を使用しているネットワークコンピュータに転送します**] を選択します。

8 新しい設定の説明を入力します (オプション)。

9 [**OK**] をクリックします。

注: コンピュータに、Web または FTP サーバ接続のいずれかを受け入れるプログラムを搭載している場合、接続を共有しているコンピュータの関連するシステムサービスポートを開き、そのポートへの接続の転送を許可する必要がある場合もあります。インターネット接続共有 (ICS) を使用している場合、[**ネットワーク**] リストに信用するコンピュータ接続を追加する必要もあります。詳細については、「コンピュータ接続を追加」を参照してください。

システムサービスポートを変更

既存のシステムサービスポートに関するネットワークの送受信アクセス情報を変更できます。

注: 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。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**] で、[**詳細設定**] をクリックします。

3 [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。

4 システムサービスの横のチェックボックスをクリックし、[**編集**] をクリックします。

5 [システムサービス] パネルの [**システム サービス ルールを追加**] で、次の項目を変更します。

- システムサービス名
- ローカル TCP/IP ポート
- ローカル UDP ポート

6 次のいずれかの操作を実行します。

- 信用、標準または公開ネットワーク上のすべてのコンピュータ (ホームネットワーク、社内ネットワークまたはインターネット接続のネットワークなど) に対してポートを開くには、[**信用、標準および公開**] を選択します。
- 標準ネットワーク (社内ネットワークなど) 上のコンピュータに対してポートを開くには、[**標準 (信用も含む)**] を選択します。

7 インターネット接続を共有しているほかの Windows のネットワークコンピュータに、このポートのアクティビティ情報を送信する場合は、[**このポートのネットワークアクティビティをインターネット接続共有を使用しているネットワークコンピュータに転送します**] を選択します。

8 変更した設定の説明を入力します (オプション)。

9 [**OK**] をクリックします。

システム サービス ポートを削除

既存のシステム サービス ポートをコンピュータから削除できます。 削除すると、リモートコンピュータからコンピュータのネットワークサービスにはアクセスできなくなります。

1 [McAfee SecurityCenter] パネルで、[**インターネットとネットワーク**] をクリックしてから [**設定**] 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が有効です**]で、[**詳細設定**]をクリックします。

3 [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。

4 システムサービスを選択し、[**削除**]をクリックします。

5 プロンプトで、確認のために[**はい**]をクリックします。

第 21 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。

このセクションの内容

イベントログを記録 110
統計を使用 112
インターネットトラフィックを追跡 113
インターネットトラフィックを監視 116

イベントログを記録

ファイアウォールにより、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、送信イベントおよび侵入イベントを表示できます。

イベントログの設定

記録するファイアウォールのイベントの種類を指定して設定できます。デフォルトでは、すべてのイベントおよびアクティビティに対してイベントログの記録が有効です。

1 [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が有効です**]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 まだ選択していない場合は、[**イベントログの有効化**]を選択します。

4 [**イベントログの有効化**]で、記録するイベントの種類を選択し、記録しないイベントの種類の選択を解除します。 イベントタイプには次のものがあります。

- ブロックされたプログラム
- 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。 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。

- [**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できます。 受信イベントには、日時、送信元 IP アドレス、ホスト名、情報およびイベントの種類が含まれます。

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**]をクリックして、[**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。

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。

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**]をクリックして、[**送信イベント**]をクリックします。

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。

侵入検知イベントを表示

ログ記録が有効な場合、受信侵入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、種類が表示されます。

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**]をクリックして、[**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。

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。

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。

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。

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。

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。

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。

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**]をクリックして、[**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 IP 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。

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。

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**]をクリックして、[**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 IP 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。

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。

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。

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、[トラフィックの監視] に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。

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、[トラフィックの監視] に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。

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。

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。

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。

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 22 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活動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。

このセクションの内容

HackerWatch チュートリアルを起動..... 120

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。

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 リソース**]で[**チュートリアルの表示**]をクリックします。

第 23 章

McAfee QuickClean (マカフィー・クイッククリーン)

McAfee QuickClean (マカフィー・クイッククリーン) で不要なファイルを削除し、コンピュータのパフォーマンスを向上させることができます。 また、ごみ箱を空にして一時ファイル、ショートカットを削除し、破損ファイルの断片、レジストリファイル、キャッシュファイル、Cookie、ブラウザ履歴ファイル、送信済みおよび削除済み E メール、最近使用したファイル、Active X ファイル、およびシステム復元ポイントファイルを削除します。 また、McAfee QuickClean では、McAfee Shredder のコンポーネントを使用して、名前や住所などの個人情報や機密情報を含む項目を安全な方法で永久に削除し、プライバシーを守ります。 ファイルの抹消の詳細については、「McAfee Shredder」を参照してください。

ディスク最適化プログラムにより、コンピュータのハードドライブへの保存時にファイルやフォルダが断片化されないように調整できます。 ハードドライブを定期的に最適化することで、これらの断片化されたファイルおよびフォルダを後ですばやく取得できるように整理することができます。

コンピュータを手動で保守しない場合は、McAfee QuickClean およびディスク最適化プログラムの両方を、独立したタスクとしてさまざまな頻度で自動実行するようにスケジュールできます。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。

このセクションの内容

McAfee QuickClean の機能 122
コンピュータをクリーニング 123
コンピュータの最適化 127
タスクのスケジュール 129

McAfee QuickClean の機能

ファイルクリーナ	不要なファイルを安全で効率的に削除するさまざまなクリーナを使用して削除します。これらのファイルを削除することにより、コンピュータのハードドライブの空き容量が増加し、パフォーマンスが改善されます。

第 24 章

コンピュータをクリーニング

McAfee QuickClean により、コンピュータ上に作成された不要なファイルが削除されます。ごみ箱が空になり、一時ファイル、ショートカット、破損ファイルの断片、レジストリファイル、キャッシュファイル、Cookie、ブラウザ履歴ファイル、送信済み E メールと削除済み E メール、最近使用したファイル、Active-X ファイル、およびシステム復元ポイントファイルが削除されます。McAfee QuickClean により、他の必要な情報に影響を与えることなくこれらの項目を削除できます。

McAfee QuickClean のクリーナを使用して、コンピュータから不要なファイルを削除できます。以下の表に、McAfee QuickClean のクリーナを示します。

名前	機能
ごみ箱クリーナ	ごみ箱内のファイルを削除します。
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。 レジストリは、Windows によって設定情報が格納されるデータベースです。レジストリには、各ユーザのプロフィール、およびシステムのハードウェア、インストールされたプログラムおよびプロパティの設定に関する情報が含まれます。Windows は動作中にこの情報を継続的に参照します。
キャッシュクリーナ	Web ページの閲覧中に蓄積したキャッシュファイルを削除します。通常、これらのファイルはキャッシュフォルダに一時ファイルとして保存されます。 キャッシュフォルダは、コンピュータ上の一時的な記憶領域です。Web 閲覧の速度と効率を向上するために、次回閲覧時にはリモートサーバからではなくキャッシュから Web ページを取得できます。

名前	機能
Cookie クリーナ	Cookie を削除します。通常、これらのファイルは一時ファイルとして保存されます。 Cookie は情報を含む小さなファイルで、通常ユーザ名と現在の日時を含み、Web を閲覧するコンピュータに保存されています。Cookie は主に Web サイトで使用され、以前に登録したユーザまたはサイトにアクセスしたユーザを特定します。ただし、同時にハッカーにとっても情報源となります。
ブラウザ履歴クリーナ	Web 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 (送信済み項目と削除済み項目)	送信済み E メールと削除済み E メールを Outlook と Outlook Express から削除します。
最近使用した項目クリーナ	これらのプログラムで作成した、最近使用したファイルを削除します。 ▪ Adobe Acrobat ▪ Corel WordPerfect Office (Corel 事務所) ▪ Jasc ▪ Lotus ▪ Microsoft Office ▪ RealPlayer ▪ Windows 履歴 ▪ Windows Media Player ▪ WinRAR ▪ WinZip
ActiveX クリーナ	ActiveX コントロールを削除します。 ActiveX は、複合した機能を追加するためにプログラムまたは Web ページで使用されるソフトウェアコンポーネントで、通常のプログラムまたは Web ページの一部として表示されます。ActiveX コントロールの多くは無害ですが、コンピュータから情報が収集される場合もあります。
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 (最新のものを除く) をコンピュータから削除します。 システム復元ポイントは、Windows によって作成され、コンピュータへの変更がマークされるため、問題が発生した場合に以前の状態に戻すことができます。

このセクションの内容

コンピュータをクリーニング 125

コンピュータをクリーニング

McAfee QuickClean のクリーナを使用して、コンピュータから不要なファイルを削除できます。 完了すると、[**McAfee QuickClean の概要**]に、クリーンアップ後に増加した空き容量、削除されたファイル数、および最後にコンピュータで McAfee QuickClean の操作を実行した日時が表示されます。

1 [McAfee SecurityCenter]ペイン(ウインドウ枠)の[**よく使う機能**]で、[**コンピュータの保守**]をクリックします。

2 [**McAfee QuickClean**]で[**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。[最近使用した項目クリーナ]を選択する場合は、[**プロパティ**]をクリックして、リスト内の最近作成したファイルを選択または選択を解除し、[**OK**]をクリックします。
- [**デフォルトに戻す**]をクリックして、標準設定のクリーナを戻し、[**次へ**]をクリックします。

4 分析が実行されたら、[**次へ**]をクリックします。

5 ファイルの削除を確認するには、[**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、削除する回数を最高 10 回で指定し、[**次へ**]をクリックします。 消去する情報が大量にある場合、ファイルの抹消には時間がかかります。

7 クリーンアップ中にファイルまたは項目がロックされていた場合、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があります。このメッセージを閉じるには[**OK**]をクリックします。

8 [**完了**]をクリックします。

注: McAfee Shredder で削除したファイルは復元できません。 ファイルの抹消の詳細については、「McAfee Shredder」を参照してください。

第 25 章

コンピュータの最適化

ディスク最適化プログラムは、コンピュータ上のファイルとフォルダを配置し、コンピュータのハードドライブに保存するときに散在（断片化）しないようにします。 ハードドライブを定期的に最適化することで、これらの断片化されたファイルおよびフォルダを後ですばやく取得できるように整理することができます。

このセクションの内容

コンピュータの最適化 127

コンピュータの最適化

コンピュータを最適化して、ファイルとフォルダのアクセスおよび読み込みの性能を向上します。

1 ［McAfee SecurityCenter］パネル（ウインドウ枠）の［**よく使う機能**］で、［**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。

注: ディスク最適化プログラムの詳細については、Windows のヘルプを参照してください。

第 26 章

タスクのスケジュール

タスクスケジューラを使用して、McAfee QuickClean またはディスク最適化プログラムをコンピュータ上で実行する頻度を自動化します。 たとえば、毎週日曜日の午後 9 時にごみ箱を空にするよう McAfee QuickClean タスクのスケジュールを設定できます。また、毎月末にコンピュータのハードドライブを最適化するようディスク最適化プログラムタスクのスケジュールを設定できます。 タスクの作成、変更、削除はいつでも実行することができます。 スケジュールタスクを実行するには、コンピュータにログインする必要があります。 タスクが何らかの理由で実行されない場合は、次回ログイン後の 5 分後に再スケジュールされます。

このセクションの内容

McAfee QuickClean タスクのスケジュール 129
McAfee QuickClean タスクの変更 130
McAfee QuickClean タスクの削除 131
ディスク最適化プログラムタスクのスケジュール..... 132
ディスク最適化プログラムタスクの変更 132
ディスク最適化プログラムタスクの削除 133

McAfee QuickClean タスクのスケジュール

McAfee QuickClean タスクをスケジュールすると、1 つ以上のクリーナを使用して自動的にコンピュータの不要物を削除できます。 完了すると、[**QuickClean の概要**]に次回タスクが実行される日時が表示されます。

1 [タスクスケジューラ]ペイン(ウインドウ枠)を開きます。

アクセス方法

1. McAfee SecurityCenter の[**よく使う機能**]で、[**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。

2 [**スケジュール設定する操作を選択**]リストで、[**McAfee QuickClean**]をクリックします。

3 [**タスク名**]ボックスにタスク名を入力し、[**作成**]をクリックします。

4 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。 [最近使用した項目クリーナ]を選択する場合は、[**プロパティ**]をクリックして、リスト内の最近作成したファイルを選択または選択を解除し、[**OK**]をクリックします。
- [**デフォルトに戻す**]をクリックして、標準設定のクリーナを戻し、[**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。

- [**スケジュール**]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、削除する回数を最高 10 回で指定し、[**スケジュール**]をクリックします。

6 [**スケジュール**]ダイアログボックスで、タスクを実行する頻度を選択し、[**OK**]をクリックします。

7 [最近使用した項目クリーナ]プロパティを変更すると、コンピュータを再起動するようメッセージが表示されます。 このメッセージを閉じるには[**OK**]をクリックします。

8 [**完了**]をクリックします。

注: McAfee Shredder で削除したファイルは復元できません。 ファイルの抹消の詳細については、「McAfee Shredder」を参照してください。

McAfee QuickClean タスクの変更

スケジュール設定した McAfee QuickClean タスクを変更すると、クリーナや自動実行の頻度を変更できます。 完了すると、[**QuickClean の概要**]に次回タスクが実行される日時が表示されます。

1 [タスクスケジューラ]ペイン(ウインドウ枠)を開きます。

アクセス方法

1. McAfee SecurityCenter の[**よく使う機能**]で、[**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。

2 [**スケジュール設定する操作を選択**]リストで、[**McAfee QuickClean**]をクリックします。

3 [**既存のタスクを選択**]リストでタスクを選択し、[**変更**]をクリックします。

4 次のいずれかの操作を実行します。

- [**次へ**]をクリックして、タスク用に選択したクリーナを許可します。

- 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。 [最近使用した項目クリーナ]を選択する場合は、[**プロパティ**]をクリックして、リスト内の最近作成したファイルを選択または選択を解除し、[**OK**]をクリックします。
- [**デフォルトに戻す**]をクリックして、標準設定のクリーナを戻し、[**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。

- [**スケジュール**]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、削除する回数を最高 10 回で指定し、[**スケジュール**]をクリックします。

6 [**スケジュール**]ダイアログボックスで、タスクを実行する頻度を選択し、[**OK**]をクリックします。

7 [最近使用した項目クリーナ]プロパティを変更すると、コンピュータを再起動するようメッセージが表示されます。 このメッセージを閉じるには[**OK**]をクリックします。

8 [**完了**]をクリックします。

注: McAfee Shredder で削除したファイルは復元できません。 ファイルの抹消の詳細については、「McAfee Shredder」を参照してください。

McAfee QuickClean タスクの削除

タスクを自動実行しない場合は、スケジュール設定した McAfee QuickClean タスクを削除できます。

1 [タスクスケジューラ]ペイン（ウインドウ枠）を開きます。

アクセス方法

1. McAfee SecurityCenter の[**よく使う機能**]で、[**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。

2 [**スケジュール設定する操作を選択**]リストで、[**McAfee QuickClean**]をクリックします。

3 [**既存のタスクを選択**]リストでタスクを選択します。

4 [**削除**]をクリックし、削除を確認するには[**はい**]をクリックします。

5 [**完了**]をクリックします。

ディスク最適化プログラムタスクのスケジュール

ディスク最適化プログラムタスクをスケジュールすると、コンピュータのハードドライブを自動的に最適化する頻度をスケジュールできます。 完了すると、[**ディスク最適化プログラム**]に次回タスクが実行される日時が表示されます。

1 [タスクスケジューラ]ペイン(ウインドウ枠)を開きます。

アクセス方法

1. McAfee SecurityCenter の[**よく使う機能**]で、[**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。

2 [**スケジュール設定する操作を選択**]リストで、[**ディスク最適化プログラム**]をクリックします。

3 [**タスク名**]ボックスにタスク名を入力し、[**作成**]をクリックします。

4 次のいずれかの操作を実行します。

- [**スケジュール**]をクリックして標準設定の[**空き容量が少ない場合でもディスクの最適化を実行**]オプションを選択します。
- [**空き容量が少ない場合でもディスクの最適化を実行**]オプションの選択を解除して、[**スケジュール**]をクリックします。

5 [**スケジュール**]ダイアログボックスで、タスクを実行する頻度を選択し、[**OK**]をクリックします。

6 [**完了**]をクリックします。

ディスク最適化プログラムタスクの変更

ディスク最適化プログラムタスクを変更すると、コンピュータのハードドライブを自動的に最適化する頻度を変更できます。 完了すると、[**ディスク最適化プログラム**]に次回タスクが実行される日時が表示されます。

1 [タスクスケジューラ]ペイン(ウインドウ枠)を開きます。

アクセス方法

1. McAfee SecurityCenter の[**よく使う機能**]で、[**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。

2 [**スケジュール設定する操作を選択**]リストで、[**ディスク最適化プログラム**]をクリックします。

3 [**既存のタスクを選択**]リストでタスクを選択し、[**変更**]をクリックします。

4 次のいずれかの操作を実行します。

- [**スケジュール**]をクリックして標準設定の[**空き容量が少ない場合でもディスクの最適化を実行**]オプションを選択します。
- [**空き容量が少ない場合でもディスクの最適化を実行**]オプションの選択を解除して、[**スケジュール**]をクリックします。

5 [**スケジュール**]ダイアログボックスで、タスクを実行する頻度を選択し、[**OK**]をクリックします。

6 [**完了**]をクリックします。

ディスク最適化プログラムタスクの削除

タスクを自動実行しない場合は、スケジュール設定したディスク最適化プログラムタスクを削除できます。

1 [タスクスケジューラ]ペイン(ウインドウ枠)を開きます。

アクセス方法

1. McAfee SecurityCenter の[**よく使う機能**]で、[**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。

2 [**スケジュール設定する操作を選択**]リストで、[**ディスク最適化プログラム**]をクリックします。

3 [**既存のタスクを選択**]リストでタスクを選択します。

4 [**削除**]をクリックし、削除を確認するには[**はい**]をクリックします。

5 [**完了**]をクリックします。

第 27 章

McAfee Shredder (マカフィー・シュレッダー)

McAfee Shredder (マカフィー・シュレッダー) は、ご使用のコンピュータのハードドライブから項目を完全に削除(または抹消)します。 手動でファイルおよびフォルダを削除したり、ごみ箱を空にしたり、またはインターネット一時ファイルを削除した場合でも、入手可能な専用のツールを使用することで誰でも情報を復元することができます。 また、プログラムによっては開いているファイル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、削除したファイルの復元が可能です。 McAfee Shredder は、これらの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。 抹消されたファイルは復元できないことに注意してください。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。

このセクションの内容

McAfee Shredder の機能 136
ファイル、フォルダ、ディスクの抹消 137

McAfee Shredder の機能

ファイルとフォルダを完全に削除

ファイルの関連情報を復元できないようにするためにコンピュータのハードドライブから項目を削除します。これにより、ごみ箱およびインターネット一時ファイルにあるファイルやフォルダ、また書き換え可能 CD、外部ハードディスクおよびフロッピーディスクのようなコンピュータ全体のデータを削除して安全な方法で永久にプライバシーを守ります。

ファイル、フォルダ、ディスクの抹消

McAfee Shredder を使用すると、特別なツールを使用しても、ごみ箱やインターネット一時ファイルにある削除済みファイルやフォルダ内の情報を復元できなくなります。 McAfee Shredder では、単一の項目を抹消する回数を最大で 10 回まで指定できます。 抹消の回数が多くなるほど、ファイルの削除の安全性レベルが高くなります。

ファイルとフォルダを抹消

コンピュータのハードドライブから、ごみ箱およびインターネット一時ファイル内にある項目を含む、ファイルおよびフォルダを抹消できます。

1 **Shredder** を開きます。

アクセス方法

1. [**よく使う機能**]の下の[McAfee SecurityCenter]ペイン（ウインドウ枠）で、[**詳細メニュー**]をクリックします。
2. 左ペイン（ウインドウ枠）で、[**ツール**]をクリックします。
3. [**Shredder**]をクリックします。

2 [**オプションの選択**]の下の[ファイルとフォルダを抹消]パネルで、[**ファイルおよびフォルダの消去**]をクリックします。

3 [**抹消のレベル**]で、次の抹消のレベルのいずれかをクリックします。

- **簡易**: 選択した項目の抹消を 1 回実行します。
- **厳重**: 選択した項目の抹消を 7 回実行します。
- **カスタム**: 選択した項目の抹消を最高 10 回実行します。

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。

- [**抹消するファイルを選択**]リストで、[**ごみ箱の中身**]または[**インターネット一時ファイル**]のいずれかをクリックします。
- [**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、[**Open（開く）**]をクリックします。

6 [**次へ**]をクリックします。

7 [**開始**]をクリックします。

8 Shredder が終了したら、[**終了**]をクリックします。

注:Shredder がタスクを実行している間はどのファイルにもアクセスしないでください。

ディスク全体のデータの抹消

ディスク全体のデータを 1 回で抹消できます。 外部ハードディスク、書き換え可能 CD、およびフロッピーディスクのようなリムーバブルドライブのみ抹消できます。

1 **Shredder** を開きます。

アクセス方法

1. [**よく使う機能**]の下の[McAfee SecurityCenter]ペイン(ウインドウ枠)で、[**詳細メニュー**]をクリックします。
2. 左ペイン(ウインドウ枠)で、[**ツール**]をクリックします。
3. [**Shredder**]をクリックします。

2 [**オプションの選択**]の下の[ファイルとフォルダを抹消]ペイン(ウインドウ枠)で、[**ファイルおよびフォルダの消去**]をクリックします。

3 [**抹消のレベル**]で、次の抹消のレベルのいずれかをクリックします。

- **簡易**: 選択したドライブの抹消を 1 回実行します。
- **厳重**: 選択したドライブの抹消を 7 回実行します。
- **カスタム**: 選択したドライブの抹消を 10 回実行します。

4 [**次へ**]をクリックします。

5 [**ディスクの選択**]リストで、抹消するドライブをクリックします。

6 [**次へ**]をクリックし、確認するには[**はい**]をクリックします。

7 [**開始**]をクリックします。

8 Shredder が終了したら、[**終了**]をクリックします。

注:Shredder がタスクを実行している間はどのファイルにもアクセスしないでください。

第 28 章

McAfee Network Manager (マカフィー・ネットワークマネージャ)

McAfee Network Manager (マカフィー・ネットワークマネージャ) は、ホームネットワーク内のコンピュータおよびその他のデバイス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管理したり、管理されたコンピュータに存在する、セキュリティ上の脆弱性をリモートで修復できます。McAfee Total Protection の機能である Network Manager でネットワークに接続しようとする侵入者 (ユーザが認識または信頼していないコンピュータやデバイス) の監視も行います。

Network Manager の使用を開始する前に、いくつかの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、Network Manager のヘルプに書かれています。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。

このセクションの内容

McAfee Network Manager の機能 140
McAfee Network Manager のアイコンについて 141
管理されたネットワークをセットアップ 143
ネットワークをリモートで管理 149
ネットワークの監視 155

McAfee Network Manager の機能

グラフィカルなネットワーク地図

ホームネットワーク上のコンピュータおよびデバイスに関する保護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、ネットワーク地図のすべてのコンポーネントの詳細を表示することもできます。

リモート管理

ホームネットワーク上のコンピュータの保護の状態を管理します。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。

ネットワークの監視

この機能を有効にすると、McAfee Network Manager によりネットワークが監視され、友人または侵入者が接続する場合に通知されます。ネットワークの監視は McAfee Total Protection を購入している場合のみ使用できます。

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 SecurityCenter 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 SecurityCenter 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 SecurityCenter 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オフラインの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。
	早急な対応を必要とす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 29 章

管理されたネットワークをセットアップ

管理されたネットワークをセットアップするには、ネットワークを信頼し(信頼していない場合)、メンバー (コンピュータ) をネットワークに追加します。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許可される前に、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。

たとえば、コンピュータの追加など、ネットワークに変更を加えた後でも、ネットワーク地図に表示される項目に関連付けられている詳細が表示されます。

このセクションの内容

ネットワーク地図を使用 144
管理されたネットワークに参加 146

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場合は、McAfee Network Manager はネットワークを分析し、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を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 SecurityCenter がインストール済みのコンピュータ名が含まれます。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項目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項目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

ネットワーク地図では、家庭のネットワーク上のコンピュータおよびデバイスに関する情報をグラフィカルに表示できます。

- 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。

注: McAfee Personal Firewall を使用していて、ネットワークをまだ信頼していない場合は、最初にネットワーク地図にアクセスしたときネットワークを信頼するよう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)。

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。

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: ネットワーク地図で項目が選択されていない場合に限り、[**ネットワーク地図を更新**] リンクを使用できます。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。

ネットワークの名称を変更

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 SecurityCenter がインストール済みのコンピュータ名が含まれます。ほかの名称を使用する場合は、名称を変更できます。

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。

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**] 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: ネットワーク地図で項目が選択されていない場合に限り、[**ネットワークの名称を変更**] リンクを使用できます。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、ホームネットワーク上のコンピュータおよびデバイス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。

設定...	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項目を選択すると、ネットワーク地図に表示されているすべての項目に関する詳細を表示することができます。この情報には、項目名、保護の状態など、項目の管理に必要となる情報が含まれます。

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他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を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際は、そのコンピュータのマカフィーによる保護状態をネットワーク上の他のコンピュータに公開するよう要求されます。 保護の状態を他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。 保護の状態を他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、他のネットワーク機能(ファイルの送信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: 他のマカフィー ネットワーク プログラム(McAfee EasyNetwork など)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。また、ネットワーク上のその他のコンピュータで、このコンピュータのセキュリティ設定を管理するかどうかも決定できます。

1 [管理されたネットワーク] ダイアログボックスで、[**このネットワークのすべてのコンピュータにセキュリティ設定の管理を許可**] チェックボックスが選択されているかどうか確認します。

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 [**OK**] 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、[管理されたネットワーク] ダイアログボックスで [**キャンセル**] をクリックしてください。

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。

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管理**] 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、次のいずれかの操作を実行します。

- [**管理されたネットワークプログラムへのゲストアクセスを許可**] をクリックして、ネットワークへのアクセスを許可します (家庭での一時ユーザ用にこのオプションを使用できます)。
- [**管理されたネットワークプログラムへのすべてのアクセスを許可**] をクリックして、ネットワークへのアクセスを許可します。
- [**管理されたネットワークプログラムへの管理者アクセスを許可**] をクリックして、管理者権限がある場合にネットワークへのアクセスを許可します。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 [**OK**] 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、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。

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

誤ってネットワーク上の他のコンピュータを信頼してしまった場合は、信頼を取り消すことができます。

- [**オプションの選択**]の下の[**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: ネットワーク上に管理者権限のある管理されたコンピュータが他にある場合は、[**ネットワーク上のコンピュータの信頼を取り消す**]リンクを使用できません。

第 30 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、ネットワークを構成するコンピュータおよびデバイスをリモートで管理できます。コンピュータおよびデバイスの状態および権限レベルを管理したり、多くのセキュリティ上の脆弱性をリモートで修復できます。

このセクションの内容

状態と権限の管理..... 150
セキュリティ上の脆弱性を修復..... 152

状態と権限の管理

管理されたネットワークには、管理されたメンバーと管理されていないメンバーがあります。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管理を許可できます。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 (ファイルの送信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者権限のある管理された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、管理者権限のあるコンピュータは、いつでも管理された別のコンピュータを管理されていないコンピュータに変更できます。

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管理

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管理されていない場合、管理するための要求を送信できます。

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管理を停止

ネットワーク内で管理されているコンピュータの保護の状態の管理を停止します。ただし、取り消すと、コンピュータは管理されない状態になり、リモートから保護の状態を管理することはできません。

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管理を停止**] 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を管理するコンピュータを変更できます。

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　[権限を変更] ダイアログボックスで、チェックボックスを選択するか、選択を解除し、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管理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

ネットワーク地図から、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。

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**] で [**このデバイスを管理**] をクリックします。Web ブラウザが起動され、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。

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、ワイヤレスルータでない場合は［**標準ルータ**］を、ワイヤレスの場合は［**ワイヤレスルータ**］をクリックします。

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管理し、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。推奨される解決方法として、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 SecurityCenter の最新のバージョン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修復できます。 たとえば、McAfee VirusScan がリモートコンピュータ上で無効であれば、有効にできます。

1 ネットワーク地図の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 を開い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 SecurityCenter の最新のバージョンを使用していない場合、そのコンピュータの保護の状態はリモートで管理できません。これらのコンピュータをリモートで管理する場合、各コンピュータに直接、McAfee SecurityCenter の最新のバージョンをインストールする必要があります。

1 リモートで管理するコンピュータで次の操作を実行します。

2 マカフィーのログイン情報を入力します。ログイン情報は、McAfee ソフトウェアを登録した時に使用した E メールアドレスとパスワードです。

3 ブラウザで、弊社の Web サイトからログインして、[**マイアカウント**] をクリックします。

4 インストールする製品を検索して、[**Download (ダウンロード)**] ボタンをクリックしてから画面に表示される手順に従います。

ヒント: ネットワーク地図を操作して、McAfee セキュリティソフトウェアをリモートコンピュータにインストールする方法を確認することもできます。[**オプションの選択**] で [**パソコンを保護する**] をクリックします。

第 31 章

ネットワークの監視

McAfee Total Protection がインストールされている場合、McAfee Network Manager でも侵入者を監視します。不明なコンピュータまたはデバイスがネットワークに接続すると通知されるため、友人または侵入者かどうかを決定できます。認識または信頼されているコンピュータまたはデバイスは友人となり、そうでないものは侵入者となります。コンピュータまたはデバイスを友人としてマークする場合、友人がネットワークに接続するたびに通知するかどうか決定できます。コンピュータまたはデバイスを侵入者としてマークする場合、侵入者が接続するたびに自動的にアラートが表示されます。

このバージョンの McAfee Total Protection をインストールまたはアップグレードしてから初めてネットワークに接続するとき、各コンピュータやデバイスが自動的に友人としてマークされるため、それらがネットワークに接続しても通知されません。3 日後、ネットワークに接続する不明なコンピュータやデバイスの通知が開始されるので、ユーザ自身がそれらを侵入者としてマークします。

注: McAfee Total Protection の詳細については、弊社 Web サイトにアクセスしてください。

このセクションの内容

新たな友人の検出を停止 155
友人としてマーク 156
侵入者としてマーク..... 156
ネットワークの監視通知の再有効化..... 156
ネットワークの監視を停止..... 157

新たな友人の検出を停止

このバージョンの McAfee Total Protection をインストール後にネットワークに接続してから最初の 3 日間は、各コンピュータやデバイスが友人としてマークされ、それらの接続は通知されません。この 3 日間は、自動で友人としてマークすることを停止できますが、あとで再開することはできません。

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。

2 [**オプションの選択**] で、[**新たな友人の検出を停止**] をクリックします。

友人としてマーク

ネットワーク上のコンピュータまたはデバイスを認識して信頼する場合のみ、友人としてマークします。コンピュータまたはデバイスを友人としてマークする場合、それらがネットワークに接続するたびに通知するかどうか決定できます。

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。

2 ネットワーク地図で項目をクリックします。

3 [**オプションの選択**] で、[**友人または侵入者としてマーク**] をクリックします。

4 ダイアログボックスで [**友人**] をクリックします。

5 この友人がネットワークに接続するたびに通知するには、[**このコンピュータまたはデバイスがネットワークに接続するときに通知する**] チェックボックスをクリックします。

侵入者としてマーク

ネットワーク上のコンピュータまたはデバイスを認識または信頼しない場合、侵入者としてマークします。侵入者がネットワークに接続するたびに自動的にアラートが表示されます。

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。

2 ネットワーク地図で項目をクリックします。

3 [**オプションの選択**] で、[**友人または侵入者としてマーク**] をクリックします。

4 ダイアログボックスで、[**侵入者**] をクリックします。

ネットワークの監視通知の再有効化

ネットワークの監視通知を無効にできますが、推奨しません。無効にすると、ネットワークに不明なコンピュータや侵入者が接続した場合に通知されません。通知を無効にした場合 (たとえば、アラートの [**今後このアラートを表示しない**] チェックボックスを選択した場合など) 、いつでも通知を再有効化できます。

1 [アラートのオプション] パネルを開きます。

アクセス方法

1. [**よく使う機能**]で[**ホーム**]をクリックします。
2. 右パネルの[**SecurityCenter の情報**]で、[**設定**]をクリックします。
3. [**アラート**] で [**詳細設定**] をクリックします。

2 [SecurityCenter の設定] パネルで [**情報アラート**] をクリックします。

3 [情報アラート] パネルで、次のチェックボックスが選択されていないことを確認します。

- **新しいパソコンまたはデバイスがネットワークに接続したときにアラートを表示しない**
- **侵入者がネットワークに接続したときにアラートを表示しない**
- **通知しないように設定した友人に対してアラートを表示しない**
- **不明なパソコンまたはデバイスが検出されたときに通知しない**
- **McAfee で新しい友人の検出が完了したときにアラートを表示しない**

4 [**OK**] をクリックします。

ネットワークの監視を停止

ネットワークの監視を無効にすると、ホームネットワークまたは接続しているほかのネットワークに侵入者が接続してもアラートが表示されません。

1 [インターネットとネットワークの設定] パネルを開きます。

アクセス方法

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。

2 [**ネットワークの監視**] で [**オフ**] をクリックします。

第 32 章

McAfee EasyNetwork (マカフィー・イージーネットワーク)

McAfee EasyNetwork (マカフィー・イージーネットワーク) 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。 ただし、この機能を活用するためには、ネットワーク内のコンピュータに McAfee EasyNetwork を必ずインストールしてください。

McAfee EasyNetwork 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 EasyNetwork のヘルプに書かれています。

注: McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。

このセクションの内容

McAfee EasyNetwork の機能.....160
McAfee EasyNetwork の設定.....161
ファイルを共有および送信.....165
プリンタを共有.....171

McAfee EasyNetwork の機能

ファイルの共有

McAfee EasyNetwork により、ネットワーク上のほかのコンピュータとファイルを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に対して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コンピュータ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(メンバー)に対してすべてのアクセス権または管理者としての権が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、ネットワーク上の他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、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 33 章

McAfee EasyNetwork の設定

McAfee EasyNetwork を使用する前に、管理されたネットワークに参加する必要があります。 管理されたネットワークに参加した後で、ファイルを共有したり、検索したり、ネットワーク上の他のコンピュータにファイルを送信できます。 また、プリンタも共有することができます。 ネットワークの切断はいつでも可能です。

このセクションの内容

McAfee EasyNetwork を開く..... 161
管理されたネットワークに参加 162
管理されたネットワークを切断..... 164

McAfee EasyNetwork を開く

McAfee EasyNetwork は、Windows の [スタート] メニューから、またはデスクトップにあるアイコンをクリックして開くことができます。

- [**スタート**] メニューで、[**プログラム**]、[**McAfee**] の順に選択し、[**McAfee EasyNetwork**] をクリックします。

ヒント: デスクトップ上の [McAfee EasyNetwork] アイコンをダブルクリックしても開くことができます。

管理されたネットワークに参加

現在接続しているネットワーク上に McAfee SecurityCenter を搭載したコンピュータが存在しない場合は、ご使用のコンピュータがネットワークのメンバーとなります。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、そのネットワークに接続している他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、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）またはすべて/管理者（ファイルの転送とファイルの共有）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他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。

注: 他のマカフィー ネットワーク プログラム（McAfee Network Manager など）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 EasyNetwork 内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。

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、管理された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他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。 ネットワーク上の最初のコンピュータに自動的に管理者権限が付与されます。

1 ［共有ファイル］ウィンドウで［**このネットワークに参加する**］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他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他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[**OK**]をクリックします。許可しない場合は[**キャンセル**]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、[**OK**]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で[**キャンセル**]をクリックしてください。

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他のコンピュータにメッセージが送信されます。 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。

1　アラートで、適切なアクセスレベルをクリックします。

2　[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、次のいずれかの操作を実行します。

- [**管理されたネットワークプログラムへのゲストアクセスを許可**]をクリックして、ネットワークへのアクセスを許可します(家庭での一時ユーザ用にこのオプションを使用できます)。
- [**管理されたネットワークプログラムへのすべてのアクセスを許可**]をクリックして、ネットワークへのアクセスを許可します。
- [**管理されたネットワークプログラムへの管理者アクセスを許可**]をクリックして、管理者権限がある場合にネットワークへのアクセスを許可します。 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他のコンピュータにアクセスを許可することもできます。

3　[**OK**]をクリックします。

4　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カードと同じカードが、コンピュータで表示されていることを確認し、[**アクセスを許可**]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。 そのコンピュータがネットワークにアクセスすると他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。

ネットワークの名称を変更

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。

1 [**オプション**]メニューで[**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、メンバーでいることをやめる場合、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した後もいつでもネットワークに再参加できますが、権限が必要です。 参加の詳細については、162 ページの「**管理されたネットワークに参加**」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。

1 コンピュータをネットワークから切断します。

2 McAfee EasyNetwork の [**ツール**] メニューで [**ネットワークの切断**] をクリックします。

3 [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。

4 [**ネットワークの切断**] をクリックします。

第 34 章

ファイルを共有および送信

McAfee EasyNetwork により、ファイルをローカルネットワーク上の他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、他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、他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。

注:多数のファイルを共有すると、コンピュータリソースに影響が出る場合があります。

このセクションの内容

ファイルを共有 166
ほかのコンピュータにファイルを送信 169

ファイルを共有

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、他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は共有されません。 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[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場合は、McAfee EasyNetwork から直接ファイルを開くか、コンピュータにコピーしてから開きます。 共有ファイルのリストが大規模で、ファイルの場所を特定するのが困難な場合は、ファイルを検索することもできます。

注:McAfee EasyNetwork で共有しているファイルは、Windows Explorer を使用している他のコンピュータからアクセスできません。McAfee EasyNetwork の共有ファイルは、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、使用可能になります。

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**]をクリックしても、ファイルを共有できます。 [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他のメンバーはファイルにアクセスできなくなります。

1 [**ツール**]メニューで[**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 [**OK**]をクリックします。

共有ファイルをコピー

共有ファイルをコピーしておくと、そのファイルが共有されなくなった後もファイルを維持できます。 管理されたネットワーク上にあるどのコンピュータからも共有ファイルをコピーできます。

- 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 内の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]ウィンドウに表示されます。

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**]リストから適切な**条件** (167 ページ)を選択します。
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. [**ファイルタイプ**]リストから適切な**ファイルタイプ** (167 ページ)を選択します。
5. [**開始**]リストと[**終了**]リストから日付を選択して、ファイルを作成した日付の範囲を指定します。

検索条件

以下の表に、共有ファイルの検索時に指定できる検索条件を示します。

ファイル名またはパス名

条件	説明
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**]リストで指定した文字列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が検索されます。

ファイルタイプ

タイプ	説明
すべて	共有されているすべてのファイルが検索されます。
ドキュメント	共有されているすべての文書ファイルが検索されます。
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。
圧縮済み	すべての圧縮ファイル（.zip ファイルなど）が検索されます。

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、ネットワーク上の他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、タスクバーの右端の通知領域にメッセージが表示されます。 たとえば、作業の邪魔になるため、通知メッセージを受信したくない場合は、この機能を無効にできます。 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他のコンピュータに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、170 ページの「**ほかのコンピュータからファイルを受け入れ**」を参照してください。

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他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(コンピュータ上に保存する)必要があります。 ファイルがコンピュータに送信されたときに McAfee EasyNetwork が実行されていない場合は、タスクバーの右隅にある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。

- [**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、他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他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、通知メッセージを受信できます。 McAfee EasyNetwork が実行されていない場合は、タスクバーの右隅にある通知領域に通知メッセージが表示されます。

1. [**オプション**]メニューで[**設定**]をクリックします。
2. [設定]ダイアログボックスで[**別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選択します。
3. [**OK**]をクリックします。

第 35 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ローカルプリンタが共有されます。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、McAfee EasyNetwork により、ネットワーク上の他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共有します。 プリンタの共有も、いつでも停止できます。

このセクションの内容

共有プリンタを使用..... 172

共有プリンタを使用

ネットワーク上のコンピュータが共有し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 McAfee EasyNetwork により検出されると、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、プリンタのリストを更新して、最新情報を表示しているかどうか確認できます。

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

プリンタの共有を停止すると、メンバーはそのプリンタを使用できなくなります。

1 [**ツール**]メニューで[**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は共有プリンタにアクセスできますが、プリンタが使用するプリンタドライブのインストールが必要です。 プリンタの所有者がプリンタの共有を停止すると、そのプリンタは使用できなくなります。

1 [**ツール**]メニューで[**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。

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。

用語集

8

802.11

無線 LAN でデータ転送を行うための標準規格のセット。802.11 は Wi-Fi といいます。

802.11a

5GHz 帯で最大 54Mbps のデータを転送する 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

2.4GHz 帯で最大 11Mbps のデータを転送する 802.11 の拡張仕様。802.11a より伝送速度は低下しますが、通信範囲は広くなります。

802.1x

有線ネットワークおよびワイヤレスネットワーク用の認証規格。802.1x は、一般的に 802.11 ワイヤレスネットワークが使用されています。**認証** (184 ページ)も参照。

A

ActiveX コントロール

通常のプログラムまたは Web ページの一部として表示される複合した機能を追加するためにプログラムまたは Web ページで使用されるソフトウェアコンポーネント。ActiveX コントロールの多くは無害ですが、コンピュータから情報が収集される場合もあります。

C

Cookie

閲覧したページに関する情報を保存するために多くの Web サイトで使用されている小さなテキストファイルで、Web を閲覧するコンピュータに保存される。ログイン情報、登録情報、ショッピングカート情報、ユーザ設定が含まれます。Cookie は主に Web サイトで使用され、以前に登録したユーザまたは Web サイトにアクセスしたユーザを特定します。ただし、同時にハッカーにとっても情報源となります。

D

DAT

ウイルス定義ファイル。シグネチャファイルとも呼ばれ、ウイルス、トロイの木馬、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) を特定、検出し、ファイルを修復する定義が含まれています。

DNS

Domain Name System の略。11.2.3.44 などの IP アドレスを www.mcafee.com などのドメイン名に変換するデータベースシステムです。

E

E メール

電子メール。コンピュータのネットワーク経由で電子的に送受信されるメッセージです。**Web メール** (179 ページ)も参照。

E メールクライアント

E メールを送受信するためにコンピュータ上で実行するプログラム (Microsoft Outlook など)。

ESS

Extended service set の略。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です。

I

IP アドレス

インターネットプロトコルアドレス。TCP/IP ネットワーク上のコンピュータまたはその他の機器を識別するために使用するアドレスです。IP アドレスは、ピリオドで 4 つに区切られた 32 ビットの数値アドレスで表します。0 から 255 までの数字を入力できます (たとえば 192.168.1.100)。

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

ローカルエリアネットワーク。比較的狭い範囲のコンピュータネットワーク (たとえば建物内など) です。LAN 上のコンピュータは相互通信が可能で、プリンタやファイルなどのリソースを共有できます。

Launchpad

U3 対応 USB プログラムの起動や管理の開始場所として動作する U3 インターフェースコンポーネント。

M

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 (NIC、ネットワークインターフェースカード) に割り当てられた一意のシリアル番号。

Man-in-the-Middle 攻撃 (中間者攻撃)

気付かれることなく 2 者間の通信に介入し、メッセージを傍受して可能であれば改変する攻撃手法。

MAPI

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プログラムおよびワークグループプログラム (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。

MSN

Microsoft Network の略。Microsoft 社によって提供されている、検索エンジン、E メール、インスタントメッセージ、ポータルなどの Web ベースのサービス群です。

N

NIC

ネットワークインターフェースカード。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です。

P

PCI ワイヤレスアダプタカード

Peripheral Component Interconnect の略。コンピュータ内部の PCI 拡張スロットに差し込むワイヤレスアダプタカード。

POP3

Post Office Protocol 3 の略。E メールクライアントプログラムと E メールサーバ間のインターフェース。ほとんどのホームユーザは POP3 の E メールアカウントを使用しています。POP3 メールアカウントは、標準の E メールアカウントとして知られています。

PPPoE

Point-to-Point Protocol Over Ethernet の略。伝送形式としてイーサネットを用いて Point-to-Point Protocol (PPP) ダイアルアッププロトコルを使用する方法です。

R

RADIUS

Remote Access Dial-In User Service の略。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。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。通信を開始する前に、2 者間で共有するテキストまたはキー (通常はパスワード)。共有秘密キーは、RADIUS メッセージの重要な部分の保護に使用されます。**RADIUS** (177 ページ)も参照。

S

SMTP

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 の略。Wi-Fi (802.11) ネットワークを特定するトークン (秘密キー) です。SSID は、ネットワーク管理者によって設定され、ネットワークに参加するユーザに提供されます。

SSL

Secure Sockets Layer の略。インターネット上で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 接続を要求する URL は、http: ではなく https: から始まります。

SystemGuards

McAfee は、コンピュータの未許可の変更を検出すると警告し、発生を通知します。

T

TKIP

Temporal Key Integrity Protocol の略(ティーキップと読む)。無線 LAN の 802.11i 暗号化標準の一部です。TKIP は 802.11 無線 LAN を保護するために使用される次世代の WEP です。TKIP では、パケットごとのキーミキシング、メッセージ整合性チェック、リキーイングメカニズムが実現されており、WEP の欠点を補います。

U

U3

You:Simplified, Smarter, Mobile。USB ドライブから直接 Windows 2000、または Windows XP プログラムを実行するためのプラットフォーム。U3 は M-Systems 社と SanDisk 社により 2004 年に開発されました。ユーザは、データや設定をインストールもしくは保存することなく、Windows コンピュータ上で U3 プログラムを実行できます。

URL

Uniform Resource Locator の略。インターネットアドレスの標準形式です。

USB

Universal Serial Bus の略。キーボードやマウスから webcam、スキャナ、プリンタまで、複数のデバイスを接続する業界標準のコネクタであり、現在のコンピュータのほとんどで使用されています。

USB ドライブ

コンピュータの USB ポートに挿入する小さなメモリドライブ。USB ドライブは小さなディスクドライブのように動作し、コンピュータからコンピュータへ簡単にファイルを移動できます。

USB ワイヤレスアダプタカード

コンピュータの USB ポートに差し込むワイヤレスアダプタカード。

V

VPN

Virtual Private Network の略。インターネットなどのホストネットワークを介して構成されているプライベート通信ネットワークです。VPN 接続を介して送受信されるデータは暗号化され、強力なセキュリティ機能があります。

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。Cookie を設定されると、Cookie が不正な送信元に情報を転送する場合があります。Web バグは、Web ビーコン、ピクセルタグ、クリア GIF、透過 GIF とも呼ばれます。

Web メール

Web ベースのメール。Microsoft Outlook などのコンピュータベースの E メールクライアントではなく、主に Web ブラウザを介してアクセスする E メールサービス。**E メール** (176 ページ)も参照。

WEP

Wired Equivalent Privacy の略。Wi-Fi (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 の略。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 Wi-Fi Alliance によって使用される用語です。

Wi-Fi Alliance

無線ハードウェアおよびソフトウェアの主要なプロバイダで構成される団体。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 ベースの無線 LAN 製品のすべての市場で 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、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。

Wi-Fi Certified

Wi-Fi Alliance によってテストされ、承認されること。Wi-Fi Alliance によっ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。

WLAN

無線 LAN (Wireless Local Area Network) の略。無線 LAN は、無線接続を使用するローカルエリアネットワーク (LAN) 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、通信を行います。

WPA

Wi-Fi Protected Access の略。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、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フレーズは、定期的に変更する必要があります。**WPA2-PSK** (180 ページ)および **TKIP** (178 ページ)も参照。

WPA2

802.11i 標準に基づいた WPA セキュリティ標準の更新バージョン。

WPA2-PSK

WPA-PSK に類似し、WPA2 標準に基づいた特別な WPA モード。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。

あ

アーカイブ

重要なファイルのコピーを 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作成すること。**バックアップ** (185 ページ)と比較。

アクセスポイント (AP)

イーサネットのハブに差し込まれたネットワークデバイス (一般的にワイヤレスルータと呼ばれる) またはワイヤレスネットワークの利用者に対する通信範囲を拡張するスイッチ。ワイヤレスネットワークの利用者がモバイル機器を用いてローミングする場合、接続を維持するため、あるアクセスポイントから他のアクセスポイントへの伝送が行われます。

圧縮

保存または転送時に必要な最小容量にファイルを圧縮する方法。

怪しいプログラム (PUP)

ユーザがダウンロードに同意する可能性はあるが、被害を与える可能性があるソフトウェアプログラム。怪しいプログラム (PUP) により、インストール先のコンピュータのセキュリティ設定やプライバシー設定が変更される可能性があります。PUP の中にはスパイウェア、アドウェア、およびダイアラーが含まれているものもあり、ユーザがダウンロードしたプログラムと共にダウンロードされる場合があります。

暗号化

情報をエンコードし、権限のない第三者がアクセスできないようにする方法。データをエンコードするプロセスでは、キーおよび数学的アルゴリズムが使用されます。適切なキーがないと、暗号化された情報は復号化できません。検出を逃れるために暗号化を使用するウイルスもあります。

暗号文

暗号化されたテキスト暗号文は、平文に変換 (復号化) されない限り解読できません。**暗号化** (180 ページ)も参照。

い

一時ファイル

オペレーティングシステムまたはその他のプログラムにより、メモリ内またはディスク上に作成されるファイル。セッション中に使用され、使用後に破棄されます。

イベント

事前定義された基準に従い、セキュリティソフトウェアが検出した、コンピュータシステムまたはプログラムにおけるインシデントまたは問題。通常は、通知の送信やイベントログへのエントリの追加などのアクションは、イベントの発生によってトリガされます。

イントラネット

通常は企業内にあり、許可されたユーザのみアクセスできるプライベートコンピュータネットワーク。

う

ウイルス

自己複製し、ユーザの知らない間にコンピュータに感染するコンピュータプログラム。

ウォードライバー

Wi-Fi 対応のコンピュータや一部の特殊なハードウェアまたはソフトウェアを携帯して、Wi-Fi (802.11) ネットワークを探しながら街中を移動する人。

お

オンデマンドスキャン

選択されたファイル、アプリケーション、またはネットワークデバイスに、脅威や脆弱性、その他の怪しいプログラムが存在するかどうかを確認するための検査のうち、あらかじめスケジュールが設定されたもの。即座に実行したり、スケジュールで設定した時刻や定期的な間隔で実行したりすることができます。オンアクセススキャンと比較。脆弱性も参照。

か

外部ハードディスク

コンピュータの外部に存在するハードディスク。

隔離

ウイルス、スパム、不審なコンテンツ、または怪しいプログラム (PUP) が含まれている疑いがあるファイルまたはフォルダを強制的に分けて、これらのファイルまたはフォルダを開いたり実行したりできないようにすること。

監視するファイルタイプ

監視場所内にあり、McAfee Backup and Restore がアーカイブまたはバックアップするファイルタイプ (たとえば、.doc、.xls)。

監視場所

McAfee Backup and Restore が監視するコンピュータ上のフォルダ。

き

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および数字。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** (179 ページ)、**WPA** (179 ページ)、**WPA2** (180 ページ)、**WPA2- PSK** (180 ページ)、**WPA-PSK** (180 ページ)も参照。

キャッシュ

頻繁に、または最近アクセスしたデータのコンピュータ上の一時的な記憶領域。たとえば、Web 閲覧の速度と効率を向上するために、次回閲覧時にはリモートサーバからではなくキャッシュから Web ページを取得できます。

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 メールの受信者に一定期間許可すること。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 メールの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 Backup and Restore 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

通信を開始する前に、2 者間で共有するテキストまたはキー (通常はパスワード)。共有秘密キーは、RADIUS メッセージの重要な部分の保護に使用されます。**RADIUS** (177 ページ)も参照。

く

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プログラム。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。

こ

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。Backup and Restore を検索することで、公開したファイルにアクセスできます。

ごみ箱

Windows で削除されたファイルやフォルダ用のごみ箱。

コンテンツの格付けグループ

保護者機能における、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。

さ

サーバ

他のコンピュータやプログラムとの接続を許可し、適切な応答を返すコンピュータまたはプログラム。たとえば、E メールメッセージの送受信を行うたびに、E メールプログラムは E メールサーバに接続します。

サービス拒否 (DOS) 攻撃

コンピュータ、サーバまたはネットワークに対する攻撃の種類であり、ネットワークでのトラフィックの速度を低下または中断させる。通常のトラフィックの速度が低下するか、完全に妨害されるほどの要求がネットワークで行われた場合に発生します。サービス拒否攻撃は、攻撃対象に対して偽の接続要求を大量に送信することにより、正規の要求に対する応答を不可能にするものです。

し

辞書攻撃

パスワードの解明のために一般的な言葉が使用されているブルートフォース攻撃の種類。

システム復元ポイント

コンピュータのメモリまたはデータベースのコンテンツのスナップショット (画像)。Windows は、定期的に、そして重要なシステムイベントの発生時 (プログラムやドライバのインストール時など) に、復元ポイントを作成します。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。

ショートカット

コンピュータの別のファイルの位置情報のみが含まれるファイル。

信頼リスト

ユーザが信頼した項目や、検出されていない項目のリスト。たとえば、不審なプログラムやレジストリの改変など、誤って信頼した項目を再度検出対象に戻す場合は、その項目をリストから削除する必要があります。

す

スクリプト

自動的に実行されるコマンドのリスト (ユーザは作業を行いません)。プログラムとは異なり、通常、スクリプトはプレーンテキスト形式で保存されており、実行されるたびにコンパイルされます。マクロやバッチファイルもスクリプトの一種です。

スマートドライブ

USB ドライブ (178 ページ)を参照。

た

ダイアラー

ユーザの標準設定のインターネットサービスプロバイダ以外の第三者にインターネット接続をリダイレクトするソフトウェア。ダイアラーによって接続がリダイレクトされると、コンテンツプロバイダ、ベンダー、その他の第三者への接続料金が請求されます。

帯域幅

一定時間内に転送可能なデータの量 (スループット)。

と

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。

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デバイスもあります。

ドメイン

ローカルサブネットワークまたはインターネット上のサイトの記述子。ローカルエリアネットワーク (LAN) で、ドメインは、特定のセキュリティデータベースによって管理されているクライアントコンピュータおよびサーバコンピュータで構成されるサブネットワークです。インターネット上で、ドメインはすべての Web アドレスに含まれます。たとえば、www.mcafee.com では mcafee がドメインです。

トロイの木馬

自己複製はしないが、コンピュータのセキュリティを侵害し、被害を与えるプログラム。通常、トロイの木馬はユーザ操作によりメールで送信されるものであり、トロイの木馬自身がメールを送信するわけではありません。また、ユーザは Web サイトまたはピアツーピアネットワークを介して、トロイの木馬を気づかないうちにダウンロードすることもあります。

に

認証

電子通信において送信者のデジタルアイデンティティを確認する手段。

ね

ネットワーク

論理ユニットとしてグループ分けされた IP ベースシステム (ルータ、スイッチ、サーバ、ファイアウォールなど) の集合。たとえば、「財務ネットワーク」の場合は、財務部門にサービスを提供するサーバ、ルータ、システムのすべてが含まれます。**ホームネットワーク** (187 ページ)も参照。

ネットワーク地図

ホーム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。

の

ノード

ネットワークに接続された 1 台のコンピュータ。

は

パスワード

コンピュータ、プログラム、Web サイトへのアクセスに使用するコード (通常、文字と数字の組み合わせです)。

パスワードボールト

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、管理者を含む他のユーザは、記録されたパスワードに一切アクセスできません。

バックアップ

重要なファイルのコピーを作成し、通常は安全なオンラインサーバ上に保存すること。**アーカイブ** (180 ページ)と比較。

バッファオーバーフロー

オペレーティングシステムまたはアプリケーションで、怪しいプログラムまたはプロセスがバッファ (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する状況。バッファオーバーフローにより、メモリが破損したり、近くのバッファデータが上書きされます。

ひ

標準の E メールアカウント

POP3 (177 ページ)を参照。

平文 (ひらぶん)

暗号化されていないテキスト。**暗号化** (180 ページ)も参照。

ふ

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 (ハードウェア、ソフトウェア、またはその両方)。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。イントラネットで送受信されるメッセージはすべてファイアウォールを通過します。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。

ファイルの断片

ディスク全体に散在している余分なファイル。ファイルの断片化は、ファイルが追加または削除された場合に起こり、コンピュータのパフォーマンスを低下させます。

フィッシング詐欺

銀行や正規の企業など、信頼できる送信元であるかのように偽装した E メールを送信し、パスワード、社会保障番号、クレジットカード情報などの個人情報を不正に取得する方法。フィッシングメールは通常、E メール内にあるリンクをクリックして、連絡先の詳細やクレジットカード情報を確認または更新するように受信者に要求します。

不正アクセスポイント

未許可のアクセスポイント。不正アクセスポイントが安全な社内ネットワークに設置されると、第三者にネットワーク権限が与えられる恐れがあります。不正アクセスポイントが設置されると、Man-in-the-Middle 攻撃 (中間者攻撃) が行われる恐れもあります。

ブラウザ

インターネットで Web ページの表示に使用されるプログラム。一般的な Web ブラウザには Microsoft Internet Explorer および Mozilla Firefox が含まれます。

プラグイン

ソフトウェアに機能を追加したり、一部の機能を強化したりする小さなソフトウェアプログラム。たとえば、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。

ブラックリスト

迷惑メール対策においては、メッセージが迷惑メールである疑いがあるため受信を拒否する E メールアドレスのリスト。フィッシング対策においては、不正とみなされる Web サイトのリスト。**ホワイトリスト** (187 ページ)と比較。

ブルートフォース攻撃

暗号を解読するまで、あらゆる組み合わせの文字を試みて、パスワードまたは暗号キーを見つけるハッキング方法。

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)。プロキシを使用すれば、ネットワークの身元情報を明かすことなく、ネットワーク内部のコンピュータがインターネットに接続できます。**プロキシサーバ** (187 ページ)も参照。

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

コンピュータやデバイスがデータを交換できるようにするルールセット。階層化されたネットワークアーキテクチャ (Open Systems Interconnection モデル) では、各階層には、その階層における通信方法を指定した独自のプロトコルがあります。コンピュータまたはデバイスを使用して他のコンピュータと通信を行うには、的確なプロトコルがサポートされている必要があります。Open Systems Interconnection (OSI)も参照。

ほ

ポート

コンピュータ利用デバイスの内外にデータを通過させるハードウェアの場所。パソコンには、ディスクドライブ、モニタ、およびキーボードを接続する内部ポート、およびモデム、プリンタ、マウスその他の周辺機器を接続する外部ポートなど、さまざまな種類のポートがあります。

ホームネットワーク

ファイルおよびインターネットアクセスを共有するため、家庭で接続している 2 台以上のコンピュータ。**LAN** (176 ページ)も参照。

ホットスポット

Wi-Fi (802.11) アクセスポイント (AP) の設置されている場所。無線ノート型 PC でホットスポットを使用すれば、インターネットに接続できます。ホットスポットは信号を送出し続けており (つまり、常にその場所を明らかにしています)、認証が要求されることもありません。ホットスポットは、空港など、人が集まる場所に設置されています。

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。

ホワイトリスト

安全と見なされた Web サイトまたは E メールアドレスのリスト。ホワイトリストにある Web サイトとは、ユーザがアクセスを許可された Web サイトです。ホワイトリストにある E メールアドレスとは、メッセージの受信を許可した信頼できる送信元です。**ブラックリスト** (186 ページ)と比較。

め

メッセージ認証コード (MAC)

コンピュータ間で転送されるメッセージの暗号化に使用されるセキュリティコード。コンピュータによって復号コードが有効と認識されると、メッセージが受信されます。

り

リアルタイムスキャン

ユーザまたはユーザのコンピュータがアクセスする際にファイルやフォルダをスキャンして、ウイルスやその他のアクティビティの有無を確認すること。

る

ルータ

1 つのネットワークから別のネットワークにデータパケットを転送するネットワークデバイス。ルータは、送信元アドレスと宛先アドレス、および現在のトラフィック状況に基づいて、受信パケットをそれぞれ解読し、転送方法を決定します。ルータはアクセスポイント (AP) と呼ばれることもあります。

ルートキット

コンピュータまたはコンピュータネットワークに管理者としてアクセスする権限を取得するためのツール (プログラム) 群。ルートキットには、スパイウェアやその他の怪しいプログラム (不正に隠蔽されたプログラム) など、コンピュータ上のデータや個人情報を盗み、セキュリティやプライバシーを侵害するプログラムが含まれます。

れ

レジストリ

各ユーザ、システムのハードウェア、インストールされたプログラムおよびプロパティの設定に関する情報を保存するために Windows が使用するデータベース。このデータベースは、値が設定されたキーに分割されています。怪しいプログラムはレジストリキーの値を変更したり、新しいレジストリキーを作成したりして、悪質なコードを実行できます。

ろ

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すること。

わ

ワーム

他のドライブ、システム、ネットワークに自身の複製を作成して拡散するウイルス。大量メール送信ワームは、感染を拡大するために、添付ファイルを開いたり、ダウンロードしたファイルを実行したりするなどのユーザ操作を必要とします。現在の E メールウイルスのほとんどはワームです。自己増殖するワームは、感染の拡大にユーザ操作を必要としません。自己増殖するワームの例が、Blaster や Sasser です。

ワイヤレスアダプタ

コンピュータや PDA にワイヤレス機能を追加するデバイス。USB ポート、PC カード (CardBus) スロット、メモリカードスロットを介して、または PCI バス内に追加されます。

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。

ライセンス条項

お客様へ: お客様がお買い求めになられたライセンスに従い、該当する契約書(許諾されたソフトウェアの使用につき一般条項を定めるものです、以下「本契約」といいます)をよくお読みください。 お買い求めになられたライセンスの種類がわからない場合は、販売およびライセンス関連部署にご連絡いただくか、製品パッケージに付随する注文書、または別途送付された注文書(パンフレット、製品 CD またはソフトウェアパッケージをダウンロードした Web サイト上のファイル)をご確認ください。 本契約の規定に同意されない場合は、製品をインストールしないでください。 この場合、弊社またはご購入元に速やかにご返品いただければ、所定の条件を満たすことによりご購入額全額をお返しいたします。

Copyright

第 36 章

カスタマおよびテクニカルサポート

McAfee SecurityCenter は、問題を検出するとただちに重要な問題かどうかをレポートします。 重要な保護の問題は早急な対応が求められ、保護の状態が赤に変わります。 保護の問題が重要でない場合は、早急な対応は必要ではありませんが、保護のステータスが問題の種類に応じて変わる場合があります。 保護の状態を緑にするためには、すべての重要な問題を修復し、重要でない問題を修復するか無視するかを決定する必要があります。 保護の問題を診断する上で詳細情報が必要な場合は、McAfee Virtual Technician を実行します。 McAfee Virtual Technician の詳細については、McAfee Virtual Technician ヘルプを参照してください。

セキュリティソフトウェアをマカフィー以外のパートナーまたはプロバイダから購入した場合、Web ブラウザを開いて **http://www.mcafee.com/japan/mcafee/support/**にアクセスします。その後[パートナーリンク]で、パートナーまたはプロバイダを選択し、McAfee Virtual Technician にアクセスします。

注:McAfee Virtual Technician をインストールおよび実行するには、Windows 管理者としてコンピュータにログインする必要があります。管理者としてログインしないと、MVT では問題を解決できない場合があります。 Windows 管理者としてログインする方法については、Windows のヘルプを参照してください。 Windows Vista では、MVT の実行時に、管理者としてログインするよう要求されます。 メッセージが表示されたら、[**同意する**]をクリックします。 McAfee Virtual Technician は、Mozilla Firefox では使用できません。

このセクションの内容

McAfee Virtual Technician の使用 194

McAfee Virtual Technician (マカフィー・バーチャルテクニシャン) の使用

McAfee Virtual Technician（注：McAfee Virtual Technician (MVT/マカフィー・バーチャルテクニシャン)は、一部製品では使用できない場合があります）は、マカフィーのテクニカルサポート担当者に代わってご使用の McAfee SecurityCenter (マカフィー・セキュリティーセンター) プログラムに関する情報を収集します。 McAfee Virtual Technician を実行すると、McAfee SecurityCenter プログラムが正常に作動しているかどうかが検査されます。 問題が検出されると、問題の修復が提案されるか、または問題に関する詳細情報が表示されます。 検査が完了すると分析結果が表示され、必要に応じてさらなるテクニカルサポートを問い合わせることができます。

コンピュータとファイルのセキュリティや整合性を保守する上で McAfee Virtual Technician が収集した情報には、個人を特定できる情報は含まれていません。

注: McAfee Virtual Technician の詳細については、McAfee Virtual Technician の［**ヘルプ**］アイコンをクリックしてください。

McAfee Virtual Technician の起動

Virtual Technician は、コンピュータの保護に関する問題を解決するため、McAfee SecurityCenter プログラムに関する情報を収集します。プライバシー保護のため、この情報には個人を特定する情報は含まれていません。

1 [**よく使う機能**] で [**McAfee Virtual Technician**] をクリックします。

2 画面に表示される手順に従い、McAfee Virtual Technician をダウンロードして実行します。

該当する国または地域のマカフィーサポートとダウンロードのサイトおよびユーザガイドについては、次の表を参照してください。

サポートおよびダウンロード

国と地域	マカフィーサポート	マカフィーダウンロード
オーストラリア	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
ブラジル	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
カナダ (英語)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp

カナダ (フランス語)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
中国 (簡体中国語)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
チェコ共和国	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
デンマーク	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
フィンランド	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
フランス	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
ドイツ	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
ギリシャ	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
ハンガリー	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
イタリア	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
日本	www.mcafeehelp.com	jp.mcafee.com/root/downloads.asp
韓国	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
メキシコ	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
ノルウェー	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
ポーランド	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
ポルトガル	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
ロシア	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
スロバキア	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
スペイン	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
スウェーデン	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
台湾	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
トルコ	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp

英国	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
米国	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection ユーザガイド

国と地域	McAfee ユーザガイド
オーストラリア	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
ブラジル	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
カナダ (英語)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
カナダ (フランス語)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
中国 (簡体中国語)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
チェコ共和国	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
デンマーク	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
フィンランド	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
フランス	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
ドイツ	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
ギリシャ	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
ハンガリー	http://download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
イタリア	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
韓国	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
メキシコ	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
ノルウェー	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf

ポーランド	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
ポルトガル	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
ロシア	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
スロバキア	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
スペイン	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
スウェーデン	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
トルコ	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
米国	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security ユーザガイド

国と地域	McAfee ユーザガイド
オーストラリア	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
ブラジル	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
カナダ（英語）	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
カナダ（フランス語）	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
中国（簡体中国語）	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
チェコ共和国	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
デンマーク	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
フィンランド	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
フランス	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf

ドイツ	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
ギリシャ	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
ハンガリー	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
イタリア	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
韓国	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
メキシコ	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
ノルウェー	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
ポーランド	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
ポルトガル	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
ロシア	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
スロバキア	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
スペイン	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
スウェーデン	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
トルコ	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
米国	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus ユーザガイド

国と地域	McAfee ユーザガイド
オーストラリア	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf

ブラジル	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
カナダ (英語)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
カナダ (フランス語)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
中国 (簡体中国語)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
チェコ共和国	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
デンマーク	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
フィンランド	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
フランス	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
ドイツ	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
ギリシャ	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
ハンガリー	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf
イタリア	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
韓国	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
メキシコ	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
ノルウェー	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
ポーランド	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
ポルトガル	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
ロシア	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
スロバキア	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
スペイン	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf

スウェーデン	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
トルコ	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
米国	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan ユーザガイド

国と地域	McAfee ユーザガイド
オーストラリア	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
ブラジル	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
カナダ（英語）	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
カナダ（フランス語）	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
中国（簡体中国語）	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
チェコ共和国	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
デンマーク	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
フィンランド	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
フランス	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
ドイツ	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
ギリシャ	download.mcafee.com/products/manuals/el/VS_userguide.2008.pdf
ハンガリー	download.mcafee.com/products/manuals/hu/VS_userguide.2008.pdf
イタリア	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
韓国	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf

メキシコ	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
ノルウェー	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
ポーランド	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
ポルトガル	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
ロシア	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
スロバキア	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
スペイン	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
スウェーデン	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
トルコ	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
米国	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

該当する国または地域のスレットセンターおよびウイルス情報については、次の表を参照してください。

国と地域	セキュリティ本部	ウイルス情報
オーストラリア	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
ブラジル	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
カナダ（英語）	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
カナダ（フランス語）	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
中国（簡体中国語）	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo

チェコ共和国	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
デンマーク	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
フィンランド	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
フランス	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
ドイツ	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
ギリシャ	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
ハンガリー	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
イタリア	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
日本	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
韓国	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
メキシコ	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
オランダ	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
ノルウェー	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
ポーランド	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
ポルトガル	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
ロシア	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
スロバキア	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
スペイン	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
スウェーデン	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
台湾	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
トルコ	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
英国	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
米国	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

該当する国または地域の HackerWatch のサイトについては、次の表を参照してください。

国と地域	HackerWatch
オーストラリア	www.hackerwatch.org
ブラジル	www.hackerwatch.org/?lang=pt-br
カナダ (英語)	www.hackerwatch.org
カナダ (フランス語)	www.hackerwatch.org/?lang=fr-ca

中国 (簡体中国語)	www.hackerwatch.org/?lang=zh-cn
チェコ共和国	www.hackerwatch.org/?lang=cs
デンマーク	www.hackerwatch.org/?lang=da
フィンランド	www.hackerwatch.org/?lang=fi
フランス	www.hackerwatch.org/?lang=fr
ドイツ	www.hackerwatch.org/?lang=de
ギリシャ	www.hackerwatch.org/?lang=el
ハンガリー	www.hackerwatch.org/?lang=hu
イタリア	www.hackerwatch.org/?lang=it
日本	www.hackerwatch.org/?lang=jp
韓国	www.hackerwatch.org/?lang=ko
メキシコ	www.hackerwatch.org/?lang=es-mx
オランダ	www.hackerwatch.org/?lang=nl
ノルウェー	www.hackerwatch.org/?lang=no
ポーランド	www.hackerwatch.org/?lang=pl
ポルトガル	www.hackerwatch.org/?lang=pt-pt
ロシア	www.hackerwatch.org/?lang=ru
スロバキア	www.hackerwatch.org/?lang=sk
スペイン	www.hackerwatch.org/?lang=es
スウェーデン	www.hackerwatch.org/?lang=sv
台湾	www.hackerwatch.org/?lang=zh-tw
トルコ	www.hackerwatch.org/?lang=tr
英国	www.hackerwatch.org
米国	www.hackerwatch.org

索引

8

802.11 175
802.11a 175
802.11b 175
802.1x....175

A

ActiveX コントロール 175

C

Cookie 175
Copyright....192

D

DAT 175
DNS....176

E

ESS 176
E メール 176, 179
E メールクライアント....176
E メール保護を開始 46

H

HackerWatch チュートリアルを起動 120

I

IP アドレス 176
IP スプーフィング....176

L

LAN 176, 187
Launchpad....176

M

MAC アドレス 176
Man-in-the-Middle 攻撃 (中間者攻撃) .176
MAPI....177
McAfee EasyNetwork 159
McAfee EasyNetwork の機能 160
McAfee EasyNetwork の設定 161
McAfee EasyNetwork を開く 161
McAfee Network Manager....139
McAfee Network Manager のアイコンについて 141
McAfee Network Manager の機能 140
McAfee Personal Firewall....65
McAfee Personal Firewall の機能 66
McAfee QuickClean....121
McAfee QuickClean タスクの削除 131
McAfee QuickClean タスクのスケジュール 129
McAfee QuickClean タスクの変更 130
McAfee QuickClean の機能 122
McAfee SecurityCenter 5
McAfee SecurityCenter の機能....6
McAfee SecurityCenter の更新....13
McAfee SecurityCenter を使用 7
McAfee Shredder 135
McAfee Shredder の機能....136
McAfee SystemGuards オプションを使用 56
McAfee SystemGuards による保護を有効化....57
McAfee SystemGuards の種類について .58
McAfee Virtual Technician の起動 194
McAfee Virtual Technician の使用 194
McAfee VirusScan....31
McAfee VirusScan の機能 32
MSN 177

N

NIC 177

P

PCI ワイヤレスアダプタカード 177
ping 要求の設定....81
POP3....177, 185
PPPoE....177

R

RADIUS....177, 182

S

SMTP 177
SSID....178

SSL....178
SystemGuards....178
SystemGuards オプションの設定....57

T

TKIP....178, 180

U

U3....178
UDP の設定....82
URL....178
USB....178
USB ドライブ....178, 184
USB ワイヤレスアダプタカード....178

V

VPN....179

W

Web バグ....179
Web メール....176, 179
WEP....179, 182
Wi-Fi....179
Wi-Fi Alliance....179
Wi-Fi Certified....179
WLAN....179
WPA....180, 182
WPA2....180, 182
WPA2-PSK....180, 182
WPA-PSK....180, 182

あ

アーカイブ....180, 185
アクセスポイント (AP)....180
新しいシステムサービスポートの設定....106
新しいプログラムにすべてのアクセスを許可....88
新しいプログラムのアクセスをブロック....91
圧縮....180
怪しいプログラム (PUP)....180
怪しいプログラムについて....40
アラートについて....70
アラートのオプションの設定....26
アラート発生時に音を鳴らす....26
アラートを使用....14, 23, 69
新たな友人の検出を停止....155
暗号化....181, 185
暗号文....181
一時ファイル....181
イベント....181
イベントログの設定....110
イベントログを記録....110
イベントを表示....18, 29
インターネットセキュリティについての確認....119
インターネットトラフィックを監視....116
インターネットトラフィックを追跡....113
イントラネット....181
ウイルス....181
ウイルス対策の設定....33, 49
ウイルスとトロイの木馬について....39
ウイルス発生によるアラートの非表示....27
ウォードライバー....181
オンデマンドスキャン....181

か

外部ハードディスク....181
概要....3
隔離....182
隔離されたファイルについて....40
隔離プログラムと Cookie について....41
カスタマおよびテクニカルサポート....193
カスタムスキャンオプションの設定 43, 52, 53
監視するファイルタイプ....182
監視対象の IP アドレスを追跡....115
監視場所....182
管理されたコンピュータの権限を変更....151
管理されたネットワークにコンピュータを招待....147
管理されたネットワークに参加 146, 162, 164
管理されたネットワークを切断....164
管理されたネットワークをセットアップ....143
キー....182
既存のシステムサービスポートへのアクセスを許可....105
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....105
起動時の起動画面を非表示にする....26
起動中のコンピュータを保護....81
キャッシュ....182
共有....182
共有秘密キー....182
共有ファイルを検索....167
共有ファイルをコピー....167
共有プリンタを使用....172
禁止するコンピュータ接続を削除....101
禁止するコンピュータ接続を追加....100
禁止するコンピュータ接続を編集....101

クライアント.....182
契約の確認.....11
契約の管理.....11, 18
契約の更新.....12
ゲーム時の情報アラートの表示または非表示.....25
ゲーム中にアラートを表示.....73
検索条件.....167
公開.....182
更新の確認.....13, 14
項目の詳細を表示.....145
ごみ箱.....183
コンテンツの格付けグループ.....183
コンピュータ接続について.....96
コンピュータ接続を管理.....95
コンピュータ接続を禁止.....100
コンピュータ接続を削除.....99
コンピュータ接続を追加.....96
コンピュータ接続を編集.....98
コンピュータの最適化.....127
コンピュータの登録情報を取得.....113
コンピュータのネットワーク情報を取得.....113
コンピュータの保護の状態の管理を停止.150
コンピュータの保護の状態を管理.....150
コンピュータをクリーニング.....123, 125
コンピュータをスキャン.....33

さ

サーバ.....183
サービス拒否 (DOS) 攻撃.....183
最近のイベントログからアクセスをブロック 92
最近のイベントログからすべてのアクセスを許可.....89
最近のイベントログから送信アクセスのみを許可.....90
最近のイベントを表示.....29, 110
辞書攻撃.....183
システムサービスポートの設定.....104
システムサービスポートを削除.....107
システムサービスポートを変更.....107
システムサービスを管理.....103
システム復元ポイント.....183
自動更新の設定.....14
自動更新を無効化.....14
受信イベントログからコンピュータを禁止.102
受信イベントログからコンピュータを追加...97
受信イベントログからコンピュータを追跡.114
受信イベントを表示.....111
受信トラフィックと送信トラフィックを分析..116
状態と権限の管理.....150
情報アラートの表示と非表示.....24
情報アラートの表示または非表示.....24
情報アラートを管理.....73
情報アラートを非表示化.....73
ショートカット.....183
侵入検知イベントログからコンピュータを禁止.....102
侵入検知イベントログからコンピュータを追跡.....114
侵入検知イベントを表示.....111
侵入検知の設定.....82
侵入者としてマーク.....156
信頼リスト.....183
信頼リストの種類について.....63
信頼リストの使用.....62
信頼リストを管理.....62
スキャン結果を使用.....39
スキャン結果を表示.....37
スキャンの種類.....42
スキャンのスケジュール.....43, 55
スクリプト.....183
スクリプトスキャンによる保護の開始.....46
スパイウェア対策の開始.....46
すべてのイベントを表示.....29
スマートドライブ.....184
スマートリコメンデーションのアラートの設定.....79
スマートリコメンデーションを表示.....80
スマートリコメンデーションを無効化.....79
スマートリコメンデーションを有効化.....79
製品の登録.....11
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.....112
世界中のセキュリティイベントの統計を表示.....112
セキュリティ上の脆弱性を修復.....152
セキュリティメッセージの非表示.....27
セキュリティレベルの設定
　自動.....77
　ステルス.....77
　標準.....77
送信イベントログからすべてのアクセスを許可.....89
送信イベントログから送信アクセスのみを許可.....90

送信イベントログからプログラム情報を取得 93
送信イベントを表示 89, 111

た

ダイアラー 184
帯域幅....184
タスクのスケジュール 129
追加の保護の使用....45
ディスク最適化プログラムタスクの削除 ...133
ディスク最適化プログラムタスクのスケジュール....132
ディスク最適化プログラムタスクの変更 ...132
ディスク全体のデータの抹消 138
デバイスの表示プロパティを変更....151
デバイスを管理....151
同期化....184
統計を使用 112
統合ゲートウェイ 184
ドメイン 184
トラフィックの分析グラフについて....116
トロイの木馬 184

な

認証 175, 184
ネットワーク 185
ネットワークコンピュータを地理的に追跡 .113
ネットワーク上のコンピュータの信頼を取り消し 148
ネットワークドライブ....185
ネットワークに参加....162
ネットワークの監視....155
ネットワークの監視通知の再有効化 156
ネットワークの監視を停止 157
ネットワークの名称を変更 145, 164
ネットワークへのアクセスを許可 163
ネットワークをリモートで管理 149
ネットワーク地図 185
ネットワーク地図で項目を表示/非表示....145
ネットワーク地図にアクセス 144
ネットワーク地図を更新....144
ネットワーク地図を使用....144
ノード....185

は

パスワード 185
パスワードボールト 185
パソコンをスキャン 34, 43
バックアップ 180, 185
バッファオーバーフロー 185
標準の E メールアカウント....185
平文 (ひらぶん)....185
ファイアウォール 186
ファイアウォールによるセキュリティを最適化 81
ファイアウォールによる保護の状態の設定 83
ファイアウォールによる保護の設定....75
ファイアウォールによる保護を開始 67
ファイアウォールによる保護を停止 68
ファイアウォールのセキュリティレベルを管理 76
ファイアウォールの設定を復元 84
ファイアウォールを起動....67
ファイアウォールを迅速にロック....84
ファイアウォールを迅速にロック解除....84
ファイアウォールをロックおよび復元 84
ファイル、フォルダ、ディスクの抹消 137
ファイルが送信されたときに通知を受信 ..170
ファイルとフォルダを抹消 137
ファイルの共有を停止 166
ファイルの断片 186
ファイルを共有 166
ファイルを共有および送信....165
フィッシング詐欺....186
不正アクセスポイント....186
ブラウザ 186
プラグイン....186
ブラックリスト 186, 187
プリンタの共有を停止....172
プリンタを共有 171
ブルートフォース攻撃 186
プロキシ 187
プロキシサーバ....187
プログラムアクティビティを監視....117
プログラム情報を取得....93
プログラムと権限を管理 87
プログラムにすべてのアクセスを許可 88
プログラムに送信アクセスのみを許可....90
プログラムについての確認....93
プログラムのアクセス権を削除 92
プログラムのアクセスをブロック 91
プログラムのインターネットアクセスを許可 88
プログラムのインターネットアクセスをブロック 91
プログラムの許可を削除 92
プログラムの帯域幅を監視....117

プロトコル 187
ポート 187
ホームネットワーク 185, 187
ほかのコンピュータからファイルを受け入れ 170
ほかのコンピュータにファイルを送信.....169
保護カテゴリについて.....9, 29
保護サービスについて 10
保護の状態について 7, 8
保護の問題を自動的に修復 18
保護の問題を修復 8, 18
保護の問題を修復または無視.....8, 17
保護の問題を手動で修復.....19
保護の問題を無視 20
ホットスポット 187
ポップアップ 187
ホワイトリスト 186, 187

ま

マカフィーアカウントへのアクセス.....11
マカフィーについて 191
無視した問題の表示または非表示 20
メッセージ認証コード (MAC).....188
メッセンジャー保護を開始.....47

や

友人としてマーク.....156

ら

ライセンス条項.....191
リアルタイムスキャン 188
リアルタイムスキャンオプションの設定 42, 50
リアルタイムなウイルス対策の停止 51
リファレンス.....174
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 153
利用可能なネットワークプリンタをインストール.....172
ルータ.....188
ルートキット.....188
レジストリ.....188
ローミング 188
ログ記録、監視、分析.....109

わ

ワーム 188
ワイヤレスアダプタ.....189