McAfee®

VirusScan® 2008

Virus and Spyware Protection

ユーザガイド

目次

第 1 章

McAfee VirusScan（マカフィー・ウイルススキャン）

McAfee VirusScan with SiteAdvisor（マカフィー・ウイルススキャン with サイトアドバイザ）は、高度な検出、保護サービスでパソコンのセキュリティを最適化し、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します。 McAfee VirusScan（マカフィー・ウイルススキャン）では、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保護が拡張され、E メール、インスタントメッセージ、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。McAfee SiteAdvisor による独自の Web サイト安全性評価によって、危険な Web サイトを避けることができます。

このセクションの内容

第 2 章

McAfee SecurityCenter

McAfee SecurityCenter 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

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

見やすくなった保護の状態

コンピュータの保護の状態の把握、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。

自動的な更新およびアップグレード

登録済みのプログラムの更新を自動的にダウンロードおよびインストールします。 登録済みのマカフィープログラムの新しいバージョンが提供された場合、契約期間内は無料で自動的に入手できます。これにより、常に最新の保護を利用できます。

リアルタイムのセキュリティ アラート機能

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

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

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、16 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、15 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

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	コンピュータとファイルのカテゴリには、次の保護サービスが設定されています。 ▪ ウイルス対策 ▪ 怪しいプログラム（PUP）対策 ▪ システム監視機能 ▪ Windows 保護
インターネットとネットワーク	インターネットとネットワークのカテゴリには、次の保護サービスが設定されています。 ▪ ファイアウォール保護 ▪ 個人情報の保護
E メールとメッセンジャー	E メールとインスタントメッセージのカテゴリには、次の保護サービスが設定されています。 ▪ E メール保護 ▪ スパム対策
保護者機能	保護者機能のカテゴリには、次の保護サービスが設定されています。 ▪ コンテンツブロック

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、McAfee SecurityCenter の主要な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（マカフィー・ウイルススキャン）をインストールすると、ウイルス対策、怪しいプログラム（PUP）対策、システム監視機能、Windows 保護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（マカフィー・ウイルススキャン）ヘルプを参照してください。

プログラムインストール時には、プログラムに関連付けられたすべての保護サービスはデフォルト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 Privacy Service 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。

アカウント情報の管理

マカフィーアカウントを管理するには McAfee SecurityCenter からアカウント情報にアクセスして契約状況を確認してください。

注：CD からマカフィープログラムをインストールした場合は、マカフィーの Web サイトでプログラムを登録し、マカフィーアカウントを設定または更新する必要があります。 これは、定期的なプログラムの自動更新を入手できる場合に限ります。

アカウント情報の管理

McAfee SecurityCenter からマカフィーのアカウント情報（マイアカウント）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。

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。

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、スパム対策、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。 デフォルトでは 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、他のタスクを継続して実行できます。

McAfee SecurityCenter の確認および更新インストール方法を変更することもできますが、これはお勧めしません。 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:CD からマカフィープログラムをインストールした場合は、マカフィーの Web サイトでプログラムを登録しない限り、プログラムの定期的な自動更新を受信できません。

このセクションの内容

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、19 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。

機能の内容

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、11 ページの「**更新の確認**」を参照してください。

1 McAfee SecurityCenter の設定パネルを開きます。

機能の内容

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。

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**]をクリックすると、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

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（マカフィー・ウイルススキャン）ヘルプを参照してください。
シグネチャファイル（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（マカフィー・ウイルススキャン）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。
プログラムの期限が切れています。	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。

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、他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、25 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 Privacy Service 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。

機能の内容

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

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。

機能の内容

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。

機能の内容

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。

機能の内容

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。

機能の内容

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。

1　[アラートのオプション]パネルを開きます。

機能の内容

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。

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

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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）の機能

McAfee VirusScan（マカフィー・ウイルススキャン）には、次の機能が搭載されています。

総合的なウイルス対策

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。 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、インスタントメッセージ、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。 面倒な管理は必要ありません。

リソースに配慮したスキャンオプション

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他のタスクよりも優先度が高いことにご注意ください。 必要に応じて McAfee VirusScan（マカフィー・ウイルススキャン）のリアルタイムの手動スキャンオプションを柔軟にカスタマイズできます。カスタマイズしなくても、コンピュータは保護できます。

自動修復

リアルタイムスキャンまたは手動スキャンの実行中にセキュリティ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。このようにしてほとんどの脅威が検出され、ユーザの操作を必要とせずに無効化されます。 ただしまれに脅威を無効化できない場合もあります。 その場合、McAfee VirusScan（マカフィー・ウイルススキャン）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。

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、自動更新や手動スキャンなどの多数のタスクを一時停止できます。

リアルタイムでのウイルス対策の開始

McAfee VirusScan（マカフィー・ウイルススキャン）には、リアルタイムと手動の 2 種類のウイルス対策が用意されています。 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定期的に監視し、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。 手動のウイルス対策では、必要に応じてファイルをスキャンできます。 最新のセキュリティ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、定期的に包括的な手動スキャンもスケジュール設定します。 デフォルトでは、週 1 回のスキャンがスケジュール設定されています。 リアルタイムおよび手動によるスキャンの詳細については、55 ページの「**コンピュータをスキャン**」を参照してください。

ただし、たとえば、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の開始

デフォルトでは、リアルタイムでのウイルス対策は有効で、ウイルスやトロイの木馬、その他のセキュリティ脅威からコンピュータを保護します。リアルタイムでのウイルス対策を無効にする場合、コンピュータを保護するためには、再度有効化する必要があります。

1 コンピュータとファイルの設定パネルを表示

機能の内容

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。

リアルタイムなウイルス対策の停止

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表示

機能の内容

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。

第 9 章

追加の保護の開始

リアルタイムでのウイルス対策に加えて、McAfee VirusScan(マカフィー・ウイルススキャン)には、スクリプト、スパイウェア、危険性のあるEメールやインスタントメッセージ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。 デフォルトでは、スクリプトスキャン、スパイウェア対策、Eメール保護、インスタントメッセージ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、コンピュータでの実行を回避します。 ファイルを作成、コピーまたは削除したり、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、送受信する 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。

インスタントメッセージ保護

インスタントメッセージ保護により、受信するインスタントメッセージの添付ファイルからセキュリティ脅威が検出されます。 また、インスタントメッセージ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

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

機能の内容

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

機能の内容

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

機能の内容

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

機能の内容

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 10 章

ウイルス対策の設定

McAfee VirusScan (マカフィー・ウイルススキャン)には、リアルタイムと手動の 2 種類のウイルス対策が用意されています。 リアルタイムのウイルス対策スキャンは、ユーザまたはコンピュータがファイルにアクセスするたびにスキャンを実行します。 手動のウイルス対策では、必要に応じてファイルをスキャンできます。 保護の種類に応じて、さまざまな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。

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

リアルタイムでのウイルス対策を開始する場合、McAfee VirusScan(マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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他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。

機能の内容

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。

目的...	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	[**ヒューリスティック方式を使用して未知のウイルスをスキャン**]チェックボックスを選択します。
Cookie の検出	[**トラッキング Cookie をスキャンして削除**]チェックボックスを選択します。
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**]チェックボックスを選択します。
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**]チェックボックスを選択します。
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。

手動スキャンオプションの設定

手動のウイルス対策では、必要に応じてファイルをスキャンできます。手動スキャンを開始する場合は、McAfee VirusScan（マカフィー・ウイルススキャン）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。 手動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（マカフィー・ウイルススキャン）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。

デフォルトでは、McAfee VirusScan（マカフィー・ウイルススキャン）は、手動スキャン実行時にはコンピュータ上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、必要に応じてデフォルトの場所を変更できます。 たとえば、重要なシステム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。 手動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、デフォルト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。デフォルトでは、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、自動更新や手動スキャンなどの多数のタスクを一時停止できます。

手動スキャンオプションの設定

手動スキャンオプションを設定して、手動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。

1　[手動スキャン]パネルを開きます。

機能の内容

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　手動スキャンオプションを指定して、[**OK**]をクリックします。

目的...	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。	[**ヒューリスティック方式を使用して未知のウイルスをスキャン**]チェックボックスを選択します。
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。	[**.zip とその他のアーカイブファイルをスキャン**]チェックボックスを選択します。
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が検出されます。	[**スパイウェアと怪しいプログラム（PUP）をスキャン**]チェックボックスを選択します。
Cookie の検出。	[**トラッキング Cookie をスキャンして削除**]チェックボックスを選択します。
ルートキットとステルスプログラムは、既存の Windows システムファイルを変更および攻撃するプログラムです。	[**ルートキットとその他のステルスプログラムをスキャン**]チェックボックスを選択します。
インターネットの閲覧や文書の作成など、他のタスクが優先されるため、スキャンに使用されるプロセッサパワーが少なくなります。	[**最小限のコンピュータリソースを使用するスキャン**]チェックボックスを選択します。
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。

手動スキャンの場所の設定

手動スキャン実行時に、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します。 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 ［手動スキャン］パネルを開きます。

機能の内容

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 ［**標準設定のスキャン場所**］をクリックして、確認します。

3 手動スキャンの場所を指定して、［**OK**］をクリックします。

目的...	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**］チェックボックスを選択します。
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他の脅威を徹底的にチェックできます。 スケジュールスキャンは、デフォルト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。 デフォルトでは、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。

1　[スケジュールスキャン]ペインを開きます。

機能の内容

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**]をクリックしてデフォルト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 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 です。

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

機能の内容

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。

機能の内容

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、47 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 です。

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。
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。

SystemGuards	検出…
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。
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。
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。

SystemGuards	検出…
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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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。

機能の内容

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、52 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（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。 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（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（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（マカフィー・ウイルススキャン）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 11 章

コンピュータをスキャン

McAfee SecurityCenterの起動とともに、McAfee VirusScan（マカフィー・ウイルススキャン）のリアルタイムウイルス対策保護が有害な可能性のあるウイルスやトロイの木馬、その他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（マカフィー・ウイルススキャン）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セキュリティ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、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。 リアルタイム スキャン オプションおよび手動スキャンオプションの設定の詳細については、37 ページの「**ウイルス対策の設定**」を参照してください。

McAfee VirusScan（マカフィー・ウイルススキャン）で、手動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。 設定したスケジュールに基づいた特定の場所を対象として、McAfee SecurityCenter から手動スキャンを実行できます。 ただし、操作中に直接 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。 ただし、Windows Explorer からスキャンを実行すると、コンピュータセキュリティに有効です。

McAfee SecurityCenter または Windows Explorer のいずれを使用して手動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（マカフィー・ウイルススキャン）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 および他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基本概要または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

コンピュータをスキャン

McAfee SecurityCenter の標準メニューまたは詳細メニューのいずれかから手動スキャンを実行できます。 詳細メニューからスキャンを実行する場合、スキャンを実行する前に手動スキャンのオプションを確認できます。 標準メニューからスキャンを実行する場合、McAfee VirusScan（マカフィー・ウイルススキャン）で既存のスキャンオプションを使用して、即座にスキャンが開始されます。 また、既存のスキャンオプションを使用して、Windows Explorer のスキャンを実行できます。

- 次のいずれかの操作を実行します。

  McAfee SecurityCenter でスキャン

目的...	手順...
既存の設定を使用してスキャン	標準メニューで[**スキャン**]をクリックします。
変更した設定を使用してスキャン	詳細メニューで[**スキャン**]をクリックし、スキャンする場所とスキャンオプションを選択して、[**今すぐスキャン**]をクリックします。

  Windows Explorer でスキャン

  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。

注：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。

スキャン結果を表示

手動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（マカフィー・ウイルススキャン）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 および他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。

目的...	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	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てから、[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。

第 12 章

スキャン結果を使用

リアルタイムスキャンまたは手動スキャンの実行中にセキュリティ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（マカフィー・ウイルススキャン）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。 感染ファイルを駆除できない場合は、McAfee VirusScan（マカフィー・ウイルススキャン）によってそのファイルが隔離されます。

セキュリティの脅威によっては、McAfee VirusScan（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン）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、認識され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

McAfee VirusScan（マカフィー・ウイルススキャン）によって、リアルタイムスキャンまたは手動スキャン時に、コンピュータ上のファイルにウイルスまたはトロイの木馬が検出されると、ファイルの駆除が試行されます。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。

機能の内容

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（マカフィー・ウイルススキャン）によって隔離されたファイルを使用するには、61 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

McAfee VirusScan（マカフィー・ウイルススキャン）によって、リアルタイムスキャンまたは手動スキャン時に、不審なコンピュータ上でプログラムが検出されると、プログラムの削除または信頼が選択できます。 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。

機能の内容

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（マカフィー・ウイルススキャン）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。

機能の内容

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（マカフィー・ウイルススキャン）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。隔離された項目は復元または削除できます。多くの場合、システムに影響を与えずに、隔離された項目を削除できます。

1 [隔離プログラム]と[トラッキング Cookie]パネルを開きます。

機能の内容

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。

第 13 章

McAfee QuickClean

McAfee QuickClean 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

McAfee QuickClean には、必要のない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が用意されています。 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。

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。

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。

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。

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。

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。

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。

機能の内容

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。

機能の内容

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。

機能の内容

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。

機能の内容

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。

機能の内容

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。

機能の内容

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 14 章

McAfee Shredder

McAfee Shredder 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

McAfee Shredder は、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。

機能の内容

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。

機能の内容

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 15 章

McAfee Network Manager

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

McAfee Network Manager 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、McAfee 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

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

グラフィカルなネットワーク地図

McAfee Network Manager のネットワーク地図では、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、ネットワーク地図に表示されているすべてのコンポーネントに関する詳細を表示することもできます。

リモート管理

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

McAfee Network Manager のアイコンについて

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

アイコン	説明
	オンラインの管理されたコンピュータを示します。
	オフラインの管理されたコンピュータを示します。
	McAfee 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 16 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、ネットワーク地図上の項目を使用し、メンバー（コンピュータ）をネットワークに追加します。 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。

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コンポーネント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

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のワークグループまたはドメイン名が含まれます。ただし、ネットワーク名はいつでも変更できます。

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

ネットワーク地図にアクセス

ネットワーク地図では、家庭のネットワーク上のコンピュータおよびコンポーネントに関する情報をグラフィカルに表示できます。

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

ネットワーク地図を更新

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

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のワークグループまたはドメイン名が含まれます。 他の名称を使用したい場合は、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コンポーネントはすべてネットワーク地図に表示されます。 ただし、項目を非表示にした場合でも、いつでも再び表示するように変更できます。 非表示にできるのは、管理されていない項目のみです。管理されたコンピュータは非表示にできません。

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

項目の詳細を表示

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

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**]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。 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とで、セキュリティ設定（コンピュータのウイルス対策サービスが最新であるかどうかなど）を互いに監視するかどうかを指定することもできます。

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監視を許可**］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他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監視**］をクリックします。

3 ［管理されたネットワークに招待する］ダイアログボックスで、次のいずれか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。

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、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 17 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コンポーネントをリモートで管理できます。 コンピュータおよびコンポーネントの状態および権限レベルを監視したり、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

状態の監視と権限

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監視を許可できます。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、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です。 ネットワーク上の管理されている別のコンピュータは、いつでも管理されていないコンピュータに対して、管理されたコンピュータになるように招待できます。 同様に、管理されているコンピュータもいつでも管理されていないコンピュータになることができます。

管理されたコンピュータには、管理者、すべて、またはゲスト権限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他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、他のコンピュータにネットワークへの参加を許可できます。 すべての権限またはゲスト権限では、コンピュータはネットワークへのアクセスのみができます。 コンピュータの権限レベルは、いつでも変更できます。

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

コンピュータの保護の状態を監視

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

1 ネットワーク地図の管理されていないコンピュータのアイコンをクリックします。

2 [**オプションの選択**]の下の[**このコンピュータを監視**]をクリックします。

コンピュータの保護の状態の監視を停止

ネットワークの管理されているコンピュータの保護の状態の監視を停止します。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監視することはできません。

1　ネットワーク地図で管理されたコンピュータのアイコンをクリックします。

2　[**オプションの選択**]の下の[**このコンピュータの監視を停止**]をクリックします。

3　確認のダイアログボックスで、[**はい**]をクリックします。

管理されたコンピュータの権限を変更

管理されたコンピュータの権限は、いつでも変更できます。 これにより、ネットワーク上の他のコンピュータの保護の状態を監視するコンピュータを変更できます。

1　ネットワーク地図で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オンまたはオフにし、このコンピュータおよび管理されたネットワーク上のほかのコンピュータが互いの保護の状態を監視するかどうかを決定します。

4　[**OK**]をクリックします。

デバイスを管理

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

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他のコンピュータのマカフィーによる保護の状態を監視し、報告されているセキュリティ上の脆弱性をリモートで修復できます。 たとえば、管理されたコンピュータのマカフィーによる保護の状態に、McAfee VirusScan（マカフィー・ウイルススキャン）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（マカフィー・ウイルススキャン

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（マカフィー・ウイルススキャン

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監視できません。 これらのコンピュータをリモートで監視する場合、各コンピュータに直接、McAfee 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　セキュリティソフトウェアをインストールするコンピュータ上で、McAfee SecurityCenter を開きます。

2　［**よく使う機能**］で［**マイアカウント**］をクリックします。

3　インストール時にセキュリティソフトウェアに登録した E メールアドレスとパスワードを使用してログインします。

4　該当する製品を選択して、［**ダウンロード/インストール**］アイコンをクリックし、画面の指示に従います。

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 IEEE 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 IEEE 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。

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

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。

D

DAT

(Data signature files)使用しているコンピュータまたは USB ドライブ上でウイルス、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を検出する際の定義を含むファイル。

DNS

(Domain Name System)ホスト名またはドメイン名を IP アドレスに変換するシステム。 Web では DNS を使用して、読み取り可能な Web アドレス(www.myhostname.com など)を簡単に IP アドレス(111.2.3.44 など)に変換でき、Web サイトをロードできます。 DNS を使用しない場合、IP アドレスを Web ブラウザに直接入力する必要があります。

DNS サーバ

（Domain Name System サーバ）ホスト名またはドメイン名に関連する IP アドレスを戻すコンピュータ。「DNS」も参照してください。

E

E メール

（E 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。「Web メール」も参照してください。

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）単一のサブネットワークを構築する 2 つ以上のネットワークのセット。

I

IP 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。

IP 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の識別番号。 TCP/IP プロトコルを使用するネットワークでは、宛先の IP アドレスに基づいてメッセージの経路が指定されます。 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）。

L

LAN

（Local Area Network）比較的狭い範囲のコンピュータネットワーク（たとえば建物内など）。 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)Microsoft 社が発表したインターフェースの仕様で、さまざまなメッセージングアプリケーションおよびワークグループアプリケーション(E メール、ボイスメール、FAX など)を、Exchange クライアントなどの単一のクライアントで利用できるようにします。

MSN

(Microsoft Network)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

N

NIC

(ネットワークカード)ノートパソコンや他のデバイスに差し込み、それらと LAN を接続するためのカード。

P

Password Vault

個人のパスワードを記録できる安全な記録領域。 この記憶領域に保存すると、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。

PCI ワイヤレス アダプタ カード

(Peripheral Component Interconnect)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)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)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。

R

RADIUS

(Remote Access Dial-In User Service)通常、リモートアクセス時に使用されるユーザ認証用プロトコル。 この RADIUS プロトコルは、元々はダイヤルインのリモート アクセス サーバで使用するために定義されたものですが、現在では、無線 LAN ユーザの共有秘密キーの 802.1x 認証などのさまざまな認証環境で使用されています。

S

SMTP

（Simple Mail Transfer Protocol）1 つのコンピュータからネットワーク上の他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）Wi-Fi（802.11）ネットワークを特定するトークン（秘密キー）。 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）インターネットを介して個人情報を送信するために Netscape によって開発されたプロトコル。 SSL は SSL 接続を介して転送されるデータを暗号化する公開キーを使用することにより機能します。 SSL 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）特に暗号キーを再利用して、WEP セキュリティの脆弱性に対処するプロトコル。 TKIP では、10,000 パケットごとに一時キーが変更されます。この動的な配布方法により、ネットワークセキュリティを著しく強化できます。 TKIP (セキュリティ) では、まず、クライアントとアクセスポイント間で、128 ビットの一時キーが共有されます。 TKIP は、一時キーと（クライアントコンピュータの）MAC アドレスを組み合わせ、比較的大きな 16 オクテットの初期化ベクトルを追加して、データを暗号化するキーを作成します。 これにより、各ステーションでは、データの暗号化に異なるキーストリームが使用されます。 TKIP は RC4 を使用して暗号化を実行します。

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）インターネットアドレスの標準形式。

USB

（Universal Serial Bus）キーボードやジョイスティック、プリンタなど周辺機器に装着できる標準的なシリアルインターフェース。

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 スロットに差し込むワイヤレス アダプタ カード。

V

VPN

(Virtual Private Network)公衆回線の管理機関を活用して、公衆回線の内部に設定された仮想専用回線網。 VPN によって、広域におよぶ WAN(wide area network)や支社を接続する専用ネットワークが構築でき、外部から社内 LAN への接続が可能になります。

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。 すると、設定された Cookie が不正な送信元に情報を転送する場合があります。 Web バグは、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

インターネットを介して電子的に送受信されるメッセージ。「E メール」も参照。

WEP

(Wired Equivalent Privacy)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)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。

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

(Wireless Local Area Network)ワイヤレス接続に使用するローカル エリア ネットワーク(LAN)。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）既存のまたはこれから登場するワイヤレス LAN システムに対して、データ保護およびアクセス制御のレベルを強化する標準規格。 既存のハードウェアでは、ソフトウェアアップグレードとして使用できるよう作られています。WPA は、IEEE 802.11i 標準規格に対応しています。 インストールが適切に行われると、ワイヤレス LAN のセキュリティレベルが強化され、確実にデータを保護し、ネットワークへのアクセスを認証ユーザのみに制限できるようになります。

WPA-PSK

企業クラスの強力なセキュリティ機能を必要とせず、認証サーバへのアクセス権のないホームユーザに対して設計された特別な WPA モード。 このモードでは、ホームユーザは、手動で開始パスワードを入力して WPA-PSK モードを有効にします。各ワイヤレスコンピュータおよびアクセスポイントのパスフレーズは、定期的に変更する必要があります。「WPA2-PSK」および「TKIP」も参照してください。

WPA2

IEEE 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。

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。

アクセスポイント

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（AP）から他のアクセスポイントへの伝送が行なわれます。

イベント

応答をトリガするユーザ、デバイスまたはコンピュータによって開始されたアクション。 イベントログにイベントを記録します。

インターネット

インターネットは、非常に多くの相互接続ネットワークから構成されており、TCP/IP プロトコルを使用して場所を特定し、データを転送します。 インターネットは、アメリカ国防総省が設立した大学コンピュータのリンクから発展し (1960 年代後半から 1970 年代前半にかけて)、ARPANET と呼ばれていました。 今日のインターネットは、約 100,000 の独立したネットワークから構成されるグローバルネットワークです。

イントラネット

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。

ウイルス

自己複製を行い、ファイルやデータを変更する可能性のあるプログラム。 多くの場合、信頼できるユーザから送信されたように装ったり、便利なコンテンツを含んでいるかのように装います。

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。

オンデマンドスキャン

オンデマンドで(この機能の起動時に)開始されるスキャン。 リアルタイムスキャンとは異なり、オンデマンドスキャンは自動的には開始されません。

オンライン バックアップ リポジトリ

バックアップ後にファイルが保存されるオンラインサーバ上の場所。

キー

2 つのデバイス間で通信を認証するために使用される一連の文字および数字。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」、「WPA」、「WPA2」、「WPA-PSK」、「WPA2- PSK」も参照してください。

キーワード

複数のファイルに関連性を持たせるために、バックアップ済みファイルに割り当てる言葉。 ファイルにキーワードを割り当てると、インターネットに公開しているファイルを簡単に検索できます。

キャッシュ

コンピュータ上の一時的な記憶領域です。 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。

クイックアーカイブ

完全アーカイブまたはクイックアーカイブの最終実行時以降に変更されたファイルのみをアーカイブすること。「完全アーカイブ」も参照。

クライアント

コンピュータまたはワークステーション上で稼動し、サーバを使用して作業を実行するアプリケーション。 たとえば、E メールクライアントは、E メールの送受信を可能にするアプリケーションです。

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

[保護者機能の設定]の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。

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

ネットワークでのトラフィックの速度を低下させるか、または中断させる攻撃の種類。 サービス拒否攻撃（Dos 攻撃）は、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。 情報の盗難やセキュリティ上の他の脆弱性が発生することはめったにありません。

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。

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、スクリプトは平文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」を参照。

ダイアラー

インターネット接続の確立に役立つソフトウェア。 悪意を持って使用する場合、ダイアラーは、追加費用なしで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のリダイレクトが可能です。

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。 この場合、ドメインによってパフォーマンスを向上できます。 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.abc.com では abc がドメインです)。

トロイの木馬

正規のプログラムを装っているが、重要なファイルに損害を与えたり、パフォーマンスを低下させたり、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。

ネットワーク

アクセスポイントおよびそれらに結び付けられたユーザの集合。

ネットワークドライブ

複数のユーザが共有するネットワーク上のサーバに接続されているディスクまたはテープドライブ。ネットワークドライブはリモートドライブと呼ばれることもあります。

ネットワーク地図

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。

ノード

ネットワークに接続された 1 台のコンピュータ。

パスワード

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、文字と数字の組合せです)。

バックアップ

重要なファイルのコピーを作成し、安全なオンラインサーバ上に保存すること。

バッファオーバーフロー

怪しいプログラムまたはプロセスがコンピュータのバッファ(データの一時的な記憶領域)の制限を越えるデータを保存しようとしたときに発生する条件。 バッファオーバーフローにより、近くのバッファデータが破損または上書きされます。

ファイアウォール

プライベートネットワークに対する不正アクセスを防止するために設計されたシステム(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

不正利用目的で個人の重要な情報（クレジットカード番号や社会保障番号、ユーザ ID やパスワードなど）を取得するよう設計されたインターネット詐欺。

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

機能を追加するために大きなアプリケーションと連動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

フィッシング対策で不正とみなされる Web サイトのリスト。

ブルートフォース攻撃

高度な技術は使用せずに、パスワードなどの暗号化されたデータを復号する網羅的な方法（ブルートフォース）。 この方法では暗号は確実に解読できますが、非常に時間がかかります。 また、ブルートフォース攻撃は総当り攻撃ともいいます。

プロキシ

1 つのネットワークアドレスだけを外部サイトに公開し、ネットワークとインターネットの間の障壁として機能するコンピュータ (またはそのコンピュータ上で動作するソフトウェア)。 プロキシを使用すれば、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」も参照してください。

プロキシサーバ

ローカルエリアネットワーク (LAN) とのインターネットトラフィックを管理するファイアウォールコンポーネント。 プロキシサーバでは、人気のある Web ページなど、頻繁に要求されるデータを提供することにより、パフォーマンスを向上できます。また、著作権で保護されたファイルに対する不正なアクセス要求など、所有者が不適切であると見なした要求をフィルタリングし、破棄することができます。

プロトコル

2 つのデバイス間でデータ転送を行うための形式（ハードウェアまたはソフトウェア）。 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場合、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。

ポート

情報がコンピュータに入ったりコンピュータから出たりする場所。 たとえば、従来のアナログモデムはシリアルポートに接続されています。

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」も参照してください。

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

詐欺サイトではないとみなされ、アクセスが許可された Web サイトのリスト。

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。

ライブラリ

ユーザがファイルをバックアップし公開するオンライン上のストレージ領域。 McAfee Data Backup ライブラリは、インターネットにアクセス可能なすべてのユーザがアクセスできるインターネット上の Web サイトです。

リアルタイムスキャン

ユーザまたは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。

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。 ルータは内部ルーティングテーブルに基づき、受信パケットを読み込んで転送します。転送方法の判断には、送信元や宛先アドレスの組み合わせだけでなく、回線負荷や回線コスト、混雑した回線などの現在のトラフィック状態も使用されます。 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。

レジストリ

Windows の設定情報を格納するデータベース。 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。

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。

ワーム

動作中のメモリに常駐し、E メールを使用して自身のコピーを送信する、自己複製を行うウイルス。ワームは自らの複製を作成してシステムリソースを消費します。それが原因で、パフォーマンスが低下したり、タスクが中断されたりします。

ワイヤレスアダプタ

コンピュータや 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、メモリー 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。

圧縮

ファイルの保存または転送時に、容量を最小化するためにファイルを圧縮するプロセス。

暗号化

テキスト形式のデータをコード化する処理。解読方法を知らなければ読むことができないように変換します。 暗号化されたデータは暗号文ともいいます。

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。

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。

画像のフィルタリング

Web 閲覧中に表示される不適切な可能性のある画像をブロックする保護者機能オプション。

怪しいプログラム（PUP）

無断で個人情報を収集して送信するプログラム（スパイウェアやアドウェアなど）。

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

隔離方法 たとえば、McAfee VirusScan（マカフィー・ウイルススキャン）では、不審なファイルは検出後に隔離されるため、コンピュータまたはファイルに被害が及びません。

完全アーカイブ

ファイルタイプと場所の設定に従って、データを完全にアーカイブすること。「クイックアーカイブ」も参照してください。

監視するファイルタイプ

監視場所内にあり、McAfee Data Backup がバックアップまたはアーカイブするファイルタイプ (たとえば、.doc、.xls など)。

監視場所

McAfee Data Backup が監視するコンピュータ上のフォルダ。

管理されたネットワーク

家庭のネットワークには、2 種類のメンバーがあります。 管理されたメンバーと、管理されていないメンバーです。 管理されたメンバーは、ネットワーク上の他のコンピュータに対して、保護の状態の監視を許可できます。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。

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 Data Backup から受信します。 また、E メールには共有ファイルへのリンクが含まれています。

共有秘密キー

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。

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。 Data Backup ライブラリを検索することで、公開したファイルにアクセスできます。

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。

重点監視する場所

McAfee Data Backup が変更状況を監視しているコンピュータ上のフォルダ。 重点監視する場所を設定した場合、McAfee Data Backup は、このフォルダとサブフォルダ内で監視対象のファイルタイプをバックアップします。

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が含まれます。 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したい場合は、その項目をリストから削除する必要があります。

帯域幅

一定時間内に転送可能なデータの量。

統合ゲートウェイ

アクセスポイント、ルータ、およびファイアウォールの機能が統合されたデバイス。 セキュリティ強化機能およびブリッジ機能が搭載されている場合もあります。

同期化

バックアップ済みファイルとローカルコンピュータ上のファイルとの不一致を解決すること。 オンライン バックアップ リポジトリ内のファイルが別のコンピュータにあるファイルよりも新しい場合は、ファイルを同期化します。

認証

個人を識別する手段で、通常は一意の名前とパスワードによって行われます。

標準の E メールアカウント

「POP3」を参照。

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。

部分的に監視する場所

McAfee Data Backup が変更状況を監視しているコンピュータ上のフォルダ。 部分的に監視する場所を設定した場合、McAfee Data Backup は、このフォルダ内で監視対象のファイルタイプをバックアップします。ただし、サブフォルダは含まれません。

復元

オンライン バックアップ リポジトリまたはアーカイブからファイルのコピーを取得すること。

平文 (ひらぶん)

暗号化されていないテキスト。「暗号化」も参照してください。

保護者機能

青少年の Web 閲覧や動作を規制することができる設定 保護者機能を設定するには、画像フィルタリングを有効または無効にして、コンテンツ レーティング グループを選択し、Web 閲覧の制限時間を設定します。

マカフィーについて

McAfee, Inc.は、カリフォルニア州サンタクララに本拠地を置く、不正侵入防止とリスクマネジメントのリーディングカンパニーです。マカフィーは、世界中で使用されているシステムとネットワークの安全を実現する先進的で実績のあるソリューションとサービスを提供しています。 個人ユーザをはじめ、企業、官公庁・自治体、ISP など様々なユーザは、マカフィーの卓越したセキュリティソリューションを通じて、ネットワークを通じた攻撃や破壊活動を阻止し、またセキュリティレベルを絶えず管理し、改善することができます。

著作権

商標

ActiveSecurity、アクティブセキュリティ、Entercept、Enterprise Secure Cast、エンタープライズセキュアキャスト、E-Policy Orchestrator、イーポリシー・オーケストレイター、GroupShield、グループシールド、IntruShield、McAfee、マカフィー、NetShield、ネットシールド、SpamKiller、VirusScan、WebShield、ウェブシールド。

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。

第 18 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

McAfee Virtual Technician（注： McAfee Virtual Technician (MVT) 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 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

McAfee 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 VirusScan（マカフィー・ウイルススキャン）をダウンロードして実行します。

サポートおよびダウンロード

該当する国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、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	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
中国	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
台湾	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
チェコスロバキア	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
イギリス	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
イタリア	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
日本	www.mcafeehelp.jp	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
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
トルコ	www.mcafeehelp.com	tr.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	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	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
チェコスロバキア	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

イギリス	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/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
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
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
トルコ	download.mcafee.com/products/manuals/tr/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	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	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf

台湾	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
チェコスロバキア	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
イギリス	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/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
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
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
トルコ	download.mcafee.com/products/manuals/tr/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	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	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
チェコスロバキア	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
イギリス	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/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
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
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
トルコ	download.mcafee.com/products/manuals/tr/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	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	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
チェコスロバキア	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
イギリス	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
オランダ	download.mcafee.com/products/manuals/nl/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
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
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
トルコ	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
米国	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

該当する国のスレットセンター、ウイルス情報、および HackerWatch のサイトについては、次の表を参照してください。

国	セキュリティ情報	ウイルス情報	HackerWatch
オーストラリア	www.mcafee.com/us/threat_center	http://au.mcafee.com/virusInfo	http://www.hackerwatch.org
ブラジル	www.mcafee.com/us/threat_center	http://br.mcafee.com/virusInfo/	http://www.hackerwatch.org/?lang=pt-br
カナダ（英語）	www.mcafee.com/us/threat_center	http://ca.mcafee.com/virusInfo	http://www.hackerwatch.org
カナダ（フランス語）	www.mcafee.com/us/threat_center	http://ca.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=fr-ca
中国	www.mcafee.com/us/threat_center	http://cn.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=zh-cn
台湾	www.mcafee.com/us/threat_center	http://tw.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=zh-tw
チェコスロバキア	www.mcafee.com/us/threat_center	http://cz.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=cs
デンマーク	www.mcafee.com/us/threat_center	http://dk.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=da

フィンランド	www.mcafee.com/us/threat_center	http://fi.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=fi
フランス	www.mcafee.com/us/threat_center	http://fr.mcafee.com/virusInfo/	http://www.hackerwatch.org/?lang=fr
ドイツ	www.mcafee.com/us/threat_center	http://de.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=de
イギリス	www.mcafee.com/us/threat_center	http://uk.mcafee.com/virusInfo	http://www.hackerwatch.org
イタリア	www.mcafee.com/us/threat_center	http://it.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=it
日本	www.mcafee.com/us/threat_center	http://jp.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=jp
韓国	www.mcafee.com/us/threat_center	http://kr.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=ko
メキシコ	www.mcafee.com/us/threat_center	http://mx.mcafee.com/virusInfo/	http://www.hackerwatch.org/?lang=es-mx
ノルウェー	www.mcafee.com/us/threat_center	http://no.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=no
ポーランド	www.mcafee.com/us/threat_center	http://pl.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=pl
ポルトガル	www.mcafee.com/us/threat_center	http://pt.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=pt-pt
スペイン	www.mcafee.com/us/threat_center	http://es.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=es
スウェーデン	www.mcafee.com/us/threat_center	http://se.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=sv
トルコ	www.mcafee.com/us/threat_center	http://tr.mcafee.com/virusInfo	http://www.hackerwatch.org/?lang=tr
米国	www.mcafee.com/us/threat_center	http://us.mcafee.com/virusInfo	http://www.hackerwatch.org

索引

た

な

は

ま

ら

わ