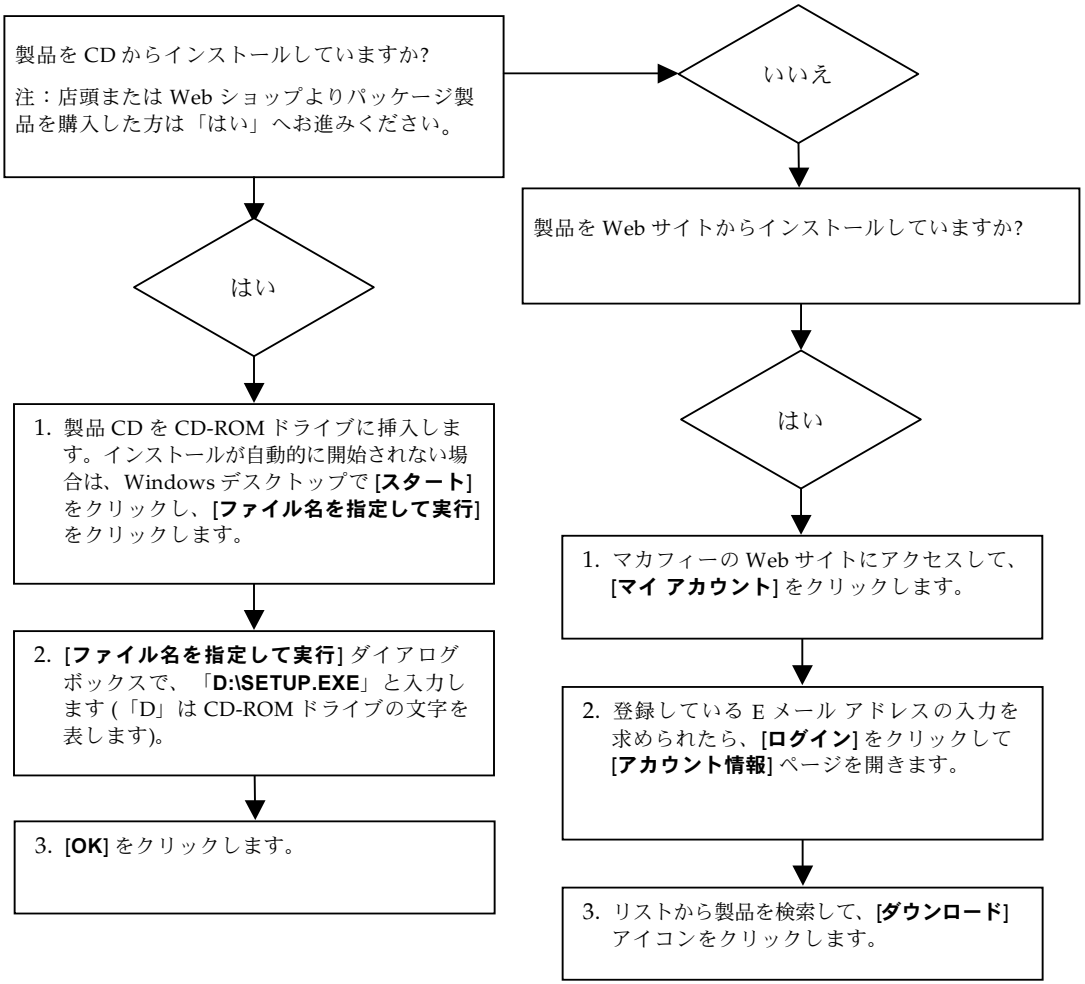
McAfee®

virusscan®

ユーザ ガイド

クイック スタート カード

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



詳細情報

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

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

ユーザ登録の利点

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

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

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

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

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

テクニカル サポート

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

目次

はじめに 1

McAfee VirusScan へようこそ。

McAfee VirusScan は、包括的で信頼性の高い、最新のウイルス保護機能を提供するウイルス対策です。実績豊かなマカフィーのスキャン技術が駆使された McAfee VirusScan は、ウイルス、ワーム、トロイの木馬、悪意のあるスクリプト、ハイブリッド攻撃などを撃退します。

McAfee VirusScan では、以下の機能を使用できます。

ActiveShield — ユーザやコンピュータがファイルにアクセスするたびに、リアルタイムでファイルをスキャンします。

スキャン — ハードディスク、フロッピーディスク、および個別のファイルとフォルダからウイルスや不審なプログラムを検出できます。

隔離 — 適切な操作を実行できるようになるまで、感染ファイルや不審なファイルを暗号化し、隔離フォルダに一時的に隔離します。

悪意ある活動の検出 — 悪意のあるスクリプトやワームによるウイルス性の活動 / 動作を監視します。

新しい機能

このバージョンの McAfee VirusScan には、以下の新機能が含まれています。

- **怪しいプログラムのスキャン**
  McAfee VirusScan では、Windows Explorer のショートカット メニューおよび Microsoft Outlook ツールバーのアイコンから、不要なプログラム (スパイウェア、アドウェア、ダイアラなど) の手動スキャン、送信 E メールのスキャン、インスタント メッセージ (IM) スキャンを実行できます。

- **送信 E メールの大容量添付ファイルをスキャン**
  McAfee VirusScan は E メール プログラムのタイムアウトで中断されることなく、サイズの大きな添付ファイルをスキャンできるように最適化されています。

- **E メール スキャン**
  McAfee VirusScan は、Microsoft Outlook、Netscape Mail、Eudora、Pegasus のような代表的な E メール クライアントで、受信 E メール (POP3)、送信 E メール (SMTP)、E メールの添付ファイルを自動的にスキャンします。

- **インスタント メッセンジャー スキャン**
  McAfee VirusScan は、AOL インスタント メッセンジャー、MSN メッセンジャーのような代表的なインスタント メッセージ クライアントで、受信ファイル転送を自動スキャンします。

- **悪意ある活動の検出**
  McAfee VirusScan は、スクリプト ストッパー™ および ワームストッパー™ によって、悪意のあるスクリプトやワームなどにより発生するウイルス性の活動 / 動作を検知、警告してブロックします。
- **ウイルス自動駆除**
  感染が検出されると、McAfee VirusScan は感染ファイルのウイルスを自動的に駆除しようとします。
- **スケジュール スキャン**
  特定の間隔で自動スキャンを実行するようスケジュールすることによって、コンピュータ全体のウイルスをチェックできます。
- **ファイルの隔離**
  隔離機能を使用すると、感染ファイルや不審なファイルを暗号化し、適切な操作を実行できるようになるまで一時的に隔離フォルダに隔離できます。隔離されたファイルは、ウイルスを駆除した後、元の場所に復元できます。
- **AVERT ウイルス解析依頼**
  McAfee VirusScan には、解析のため、不審なファイルを隔離してからマカフィー・ウイルス緊急対策チーム (AVERT™) へ直接送信する機能が追加されました。
- **世界ウイルス地図**
  ウイルス追跡情報を匿名で送信して世界ウイルス地図に追加できます。このセキュリティ保護されている機能には無料で自動登録でき、McAfee SecurityCenter を通じて全世界の最新感染率を表示できます。

システム要件

- Microsoft® Windows 98、Windows Me、Windows 2000 Pro、または Windows XP
- プロセッサを搭載したパーソナル コンピュータ :
  Windows 98、Windows ME — Pentium 150 MHz 以上
  Windows 2000 Pro、Windows XP — Pentium 233 MHz 以上
- RAM:
  Windows 98 — 32MB 以上 (64MB 推奨)
  Windows ME、Windows 2000 、Windows XP — 64MB 以上 (128MB 推奨)
- 40 MB のハード ディスク空き容量
- Microsoft® Internet Explorer 5.5 以降

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

McAfee VirusScan をテストする

McAfee VirusScan を初めて使用する前に、インストール結果をテストすることをお勧めします。次の手順に従って、ActiveShield とスキャン機能を個別にテストします。

ActiveShield をテストする

ActiveShield をテストするには

1 Web ブラウザで http://www.eicar.org/ にアクセスします。

2 **[The AntiVirus testfile eicar.com]** リンクをクリックします。

3 ページの下部にスクロールします。**[Download]** の下に 4 つのリンクが表示されます。

4 **[eicar.com]** をクリックします。

ActiveShield が正常に機能している場合、リンクをクリックした直後に eicar.com ファイルが検出されます。感染したファイルの削除または隔離を試行して、ActiveShield によるウイルスの処理の方法を確認できます。詳細については、23 ページの「ActiveShield がウイルスを検出した場合」を参照してください。

スキャンをテストする

テスト ファイルが ActiveShield によって検出されることを防ぐため、スキャン テスト前に ActiveShield を無効にする必要があります。無効にした後でテスト ファイルをダウンロードしてください。

テスト ファイルをダウンロードするには

1 ActiveShield を無効にします。マカフィー・アイコンを右クリックして **[VirusScan]** を選択してから、**[無効にする]** をクリックします。

2 EICAR Web サイトから EICAR テスト ファイルをダウンロードします。

   a http://www.eicar.org/ にアクセスします。

   b **[The AntiVirus testfile eicar.com]** リンクをクリックします。

c ページの下部にスクロールします。**[Download]** の下に、次の 4 つのリンクが表示されます。

eicar.com には、McAfee VirusScan がウイルスとして検出するテキスト行が含まれています。

eicar.com.txt (オプション) は同じファイルですが、1 つめのリンクからダウンロードできないユーザのために異なるファイル名が付けられています。このファイルをダウンロードした後、ファイル名を「eicar.com」に変更してください。

eicar_com.zip は、ZIP 圧縮ファイル (WinZip™ アーカイブ ファイル) 内にあるテスト ウイルスのコピーです。

eicarcom2.zip は ZIP 圧縮ファイル内にあるテスト ウイルスのコピーですが、この圧縮ファイル自体が ZIP 圧縮ファイル内にあります。

d 各リンクをクリックしてファイルをダウンロードします。各リンクに **[ファイルのダウンロード]** ダイアログ ボックスが表示されます。

e **[保存]**、**[新しいフォルダの作成]** ボタンの順にクリックし、次にフォルダを**「VSO Scan Folder」**という名前に変更します。

f **[VSO Scan Folder]** をダブルクリックした後、それぞれの **[名前をつけて保存]** ダイアログ ボックスでもう一度 **[保存]** をクリックします。

3 ファイルのダウンロードが終了したら、Internet Explorer を閉じます。

4 ActiveShield を有効にします。マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[有効にする]** をクリックします。

スキャンをテストするには

1 マカフィー・アイコンを右クリックして **[VirusScan]** を選択してから、**[ウイルスをスキャンする]** をクリックします。

2 ダイアログ ボックスの左ペインのディレクトリ ツリーを使用して、ファイルを保存した **[VSO Scan Folder]** フォルダに移動します。

a C ドライブのアイコンの横にある **[+]** 記号をクリックします。

b **[VSO Scan Folder]** をクリックしてハイライトします (フォルダの横にある **[+]** 記号はクリックしないでください)。

これで、スキャンはこのフォルダのウイルスのみをチェックするように設定されます。ファイルをハードディスク ドライブの無作為な場所に置くと、スキャンの性能の高さを確認できます。

3 **[ウイルスをスキャンする]** ダイアログ ボックスの **[スキャン オプション]** 領域で、すべてのオプションが選択されていることを確認します。

4 ダイアログ ボックスの右下にある **[スキャン]** をクリックします。

McAfee VirusScan により **[VSO Scan Folder]** がスキャンされます。このフォルダに保存した EICAR テスト ファイルが **[感染しているファイルの一覧]** に表示されます。表示された場合、スキャンは正常に動作しています。

感染したファイルの削除または隔離を試行して、スキャンによるウイルスの処理の方法を確認できます。詳細については、31 ページの「ウイルスまたは怪しいプログラムが検出された場合」を参照してください。

McAfee SecurityCenter を使用する

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

- コンピュータのセキュリティ分析を行う
- 1 つのアイコンから McAfee のすべてのサービスを起動、管理、設定する
- 最新のウイルス情報と最新の製品情報を表示する
- FAQ (よくある質問) やアカウントの詳細に簡単にアクセスする

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

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

コンピュータにインストールされている McAfee アプリケーションのうち 1 つまたは複数が無効になっている場合は、マカフィー・アイコンは黒色 に変わります。

McAfee SecurityCenter を開くには

1. マカフィー・アイコン を右クリックします。
2. **[SecurityCenter を開く]** をクリックします。

McAfee VirusScan の機能にアクセスするには

1. マカフィー・アイコン を右クリックします。
2. **[VirusScan]** をポイントし、使用する McAfee VirusScan の機能をクリックします。

McAfee VirusScan を使用する 2

ActiveShield を使用する

ActiveShield を起動 (コンピュータのメモリにロード) して有効にすると、常にコンピュータをウイルスから保護できます。ユーザやコンピュータがファイルにアクセスすると、ActiveShield によってそれらのファイルがスキャンされます。感染したファイルが検出されると、ウイルスの駆除が自動的に実行されます。ActiveShield でウイルスを駆除できない場合は、そのファイルを隔離または削除できます。

ActiveShield を有効または無効にする

インストール後、コンピュータを再起動すると、ActiveShield は起動され (コンピュータのメモリにロードされ)、有効になります (Windows システム トレイに赤色のアイコン が表示されます)。

ActiveShield が停止している (ロードされていない) 場合や無効になっている場合 (黒色のアイコン  が表示されます)、手動で実行したり、Windows の起動時に自動的に起動するように設定したりできます。

ActiveShield を有効にする

マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[有効にする]** をクリックします。マカフィー・アイコンが赤  に変わります。

Windows の起動時に ActiveShield を起動するよう設定されている場合は、コンピュータがウイルスから保護されていることを示すメッセージが表示されます。そのように設定されていない場合は、Windows の起動時に ActiveShield を起動するためのダイアログ ボックスが表示されます (14 ページの図 2-1)。

ActiveShield を無効にする

ActiveShield をこの Windows セッションでのみ無効にするには

1. マカフィー・アイコンを右クリックして **[VirusScan]** を選択してから、**[無効にする]** をクリックします。
2. **[はい]** をクリックして確認します。

   マカフィー・アイコンは黒  に変わります。

Windows の起動時に ActiveShield が起動するように設定されている場合は、コンピュータを再起動すると、ウイルスからの保護が再び有効になります。

ActiveShield のオプションを設定する

ActiveShield の起動およびスキャンのオプションは、McAfee VirusScan の **[オプション]** ダイアログ ボックス (図 2-1) の **[ActiveShield]** タブで変更できます。このダイアログ ボックスは、Windows のシステム トレイにあるマカフィー・アイコン からアクセスできます。

図 2-1 ActiveShield のオプション

ActiveShield を起動する

インストール後、コンピュータを再起動すると、ActiveShield は起動され (コンピュータのメモリにロードされ)、有効になります (赤の が表示されます)。

ActiveShield が停止している場合 (黒の が表示されます) は、Windows 起動時に自動的に起動するように設定できます (推奨)。

> **注**
> McAfee VirusScan の更新中、新しいファイルをインストールするために、**更新ウィザード**によって一時的に ActiveShield が終了する場合があります。**更新ウィザード**で **[完了]** をクリックすると、ActiveShield は再び起動します。

Windows の起動時に ActiveShield を自動的に起動するには

1 マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。

McAfee VirusScan の **[オプション]** ダイアログ ボックス (14 ページの図 2-1) が表示されます。

2 **[Windows の起動時に ActiveShield を起動する (推奨)]** チェックボックスをオンにし、**[適用]** をクリックして変更を保存します。

3 **[OK]** をクリックして確認し、再度 **[OK]** をクリックします。

ActiveShield を停止する

警告

ActiveShield を停止すると、コンピュータはウイルスから保護されません。ActiveShield を停止する必要がある場合は、McAfee VirusScan を更新する場合を除いて、コンピュータがインターネットに接続していないことを確認してください。

Windows 起動時に ActiveShield を起動しないようにするには

1 マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。

McAfee VirusScan の **[オプション]** ダイアログ ボックス (14 ページの図 2-1) が表示されます。

2 **[Windows の起動時に ActiveShield を起動する (推奨)]** チェックボックスをオフにし、**[適用]** をクリックして変更を保存します。

3 **[OK]** をクリックして確認し、再度 **[OK]** をクリックします。

E メールと添付ファイルをスキャンする

デフォルト (標準の設定) では、E メール スキャンとウイルス自動駆除は、**[E メールと添付ファイルをスキャンする]** オプション (14 ページの図 2-1) と **[ウイルスに感染した添付ファイルからウイルスを自動的に駆除する (推奨)]** オプション (18 ページの図 2-2) で有効にすることができます。

この 2 つのオプションを有効にすると、受信 (POP3) と送信 (SMTP) の E メール メッセージと添付ファイルが自動的にスキャンされ、感染している E メールと添付ファイルに対しウイルス駆除が実行されます。これには、以下のような代表的な E メール クライアントが対象になります。

- Microsoft Outlook Express 4.0 以降
- Microsoft Outlook 97 以降
- Netscape Messenger 4.0 以降
- Netscape Mail 6.0 以降
- Eudora Light 3.0 以降
- Eudora Pro 4.0 以降
- Eudora 5.0 以降
- Pegasus 4.0 以降

注

E メール スキャンは、Web ベースの E メール クライアント、IMAP、AOL、POP3 SSL、および Lotus Notes ではサポートされていません。ただし、E メールの添付ファイルは、ファイルを開いたときにスキャンされます。

[E メールと添付ファイルをスキャンする] オプションを無効にすると、[E メール スキャン] オプション (18 ページの図 2-2) と [ワーム ストッパー] のオプション (23 ページの図 2-5) は、自動的に無効になります。送信 E メールのスキャンを無効にすると、[ワーム ストッパー] のオプションは自動的に無効になります。

[E メール スキャン] オプションを変更した場合は、変更を完了させるために E メール プログラムを再起動する必要があります。

受信 E メール

受信した E メール メッセージまたは添付ファイルがウイルスに感染している場合、ActiveShield により以下の手順が実行されます。

- 感染した E メールからウイルスを駆除する
- ウイルス駆除が不可能な E メールを隔離または削除する
- ウイルス駆除のために実行されたアクションに関する情報を含むアラート ファイルを、受信した E メールに追加する

送信 E メール

送信する E メール メッセージまたは添付ファイルがウイルスに感染している場合、ActiveShield により以下の手順が実行されます。

- 感染した E メールからウイルスを駆除する
- ウイルス駆除ができない E メールを隔離または削除する

注

送信 E メールのスキャン エラーに関する詳細については、オンライン ヘルプを参照してください。

デフォルト（標準設定）では、**[送信 E メール スキャンのステータス ウィンドウの表示]** はオフになっています。ステータス ウィンドウはエラーが生じた場合のみ表示されます。

E メール スキャンを無効にする

デフォルト (標準の設定) では、ActiveShield は受信 E メールと送信 E メールの両方をスキャンします。より高度な制御をするためには、以下の手順に従って、受信 E メールのみまたは送信 E メールをスキャンするように ActiveShield を設定します。

受信 E メールまたは送信 E メールのスキャンを無効にするには

1. マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。
2. **[詳細設定]** をクリックし、次に **[E メール スキャン]** タブ (図 2-2) を選択します。
3. **[E メールの受信メッセージ]** または **[E メールの送信メッセージ]** の選択を解除して、**[OK]** をクリックします。

ユーザの接続時にのみ E メールの送受信がおこなわれるように設定されている場合にウイルス自動駆除を無効にすると、感染ファイルからのウイルス駆除を促すダイアログ ボックスが表示されます。ウイルス自動駆除を無効にするには、次の手順に従います。アラートへの応答に関する詳細は、25 ページの「感染した E メールを管理する」を参照してください。

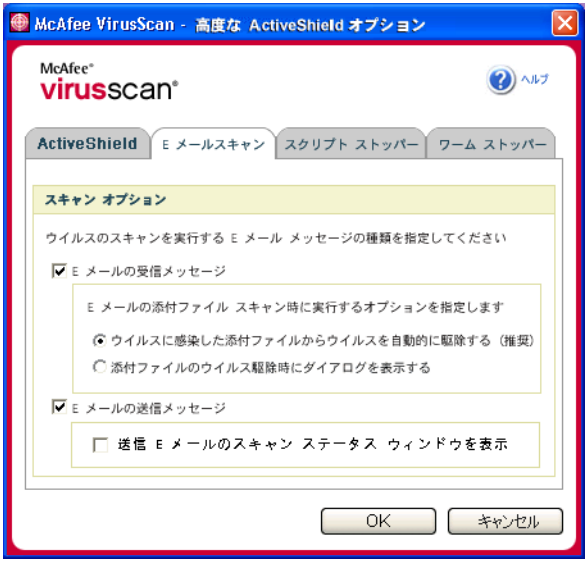


図 2-2 E メール スキャンのオプション

E メールのウイルス自動駆除を無効にする

感染した E メールのウイルス自動駆除を無効にするには

1. マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。
2. **[詳細設定]** をクリックし、次に **[E メール スキャン]** タブ (図 2-2) を選択します。
3. **[添付ファイルのウイルス駆除時にダイアログを表示する]** を選択してから、**[OK]** をクリックします。

インスタント メッセージ スキャンを有効にする

デフォルト (標準の設定) では、インスタント メッセージの添付ファイルのスキャンは、**[インスタント メッセージ スキャンを有効にする]** オプション (14 ページの図 2-1) で有効にできます。

このオプションを有効にすると、受信したインスタント メッセージの添付ファイルが自動的にスキャンされ、感染している添付ファイルに対しウイルス駆除が実行されます。これには、次のような代表的なインスタント メッセージ クライアントが対象となります。

- MSN メッセンジャー 6.0 以上
- Yahoo メッセンジャー 4.1 以上
- AOL インスタント メッセンジャー 2.1 以降

注

セキュリティ上の理由から、インスタント メッセージの添付ファイルのウイルス自動駆除を無効にすることはできません。

受信したインスタント メッセージの添付ファイルがウイルスに感染している場合、McAfee VirusScan によって以下の手順が実行されます。

- 感染したメッセージからウイルスを駆除する
- ウイルス駆除ができないメッセージの隔離または削除を要求するメッセージを表示する

すべてのファイルをスキャンする

ActiveShield でデフォルト (標準の設定) の **[すべてのファイル (推奨)]** オプションを使用するように設定すると、コンピュータでファイルを使用する際にはすべての種類のファイルがスキャンされます。このオプションを使用すると、最も徹底したスキャンが実行されます。

ActiveShield ですべてのファイルの種類をスキャンするよう設定するには

1. マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。
2. **[詳細設定]** をクリックし、次に **[ActiveShield]** タブ (20 ページの図 2-3) を選択します。
3. **[すべてのファイル (推奨)]** をクリックし、次に **[OK]** をクリックします。

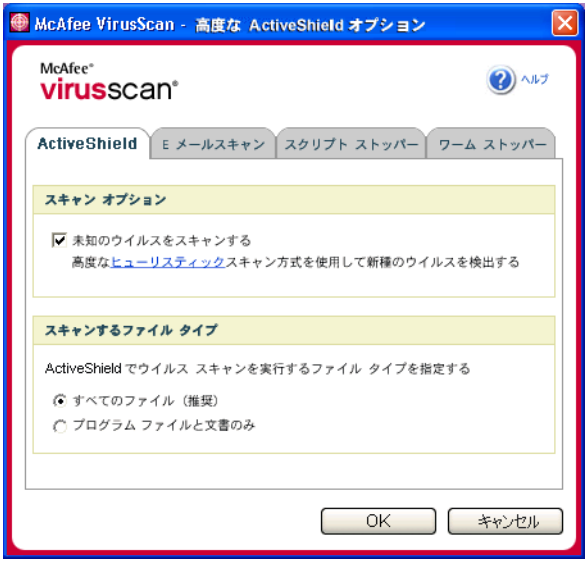


図 2-3 高度な ActiveShield オプション

プログラム ファイルと文書のみをスキャンする

ActiveShield で **[プログラム ファイルと文書のみ]** オプションに設定すると、プログラム ファイルと文書がスキャンされますが、コンピュータで使用されるその他のファイルはスキャンされません。最新のウイルス定義ファイル (DAT ファイル) によって、ActiveShield がスキャンするファイルの種類が決定されます。プログラム ファイルと文書のみをスキャンするように ActiveShield を設定するには、次の手順に従います。

1 マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。

2 **[詳細設定]** をクリックし、次に **[ActiveShield]** タブ (図 2-3) を選択します。

3 **[プログラム ファイルと文書のみ]** をクリックしてから、**[OK]** をクリックします。

未知のウイルスをスキャンする

デフォルト (標準の設定) の **[未知のウイルスをスキャンする (推奨)]** オプションを使用すると、ファイルと既知のウイルスのシグネチャを一致させる高度なヒューリスティック スキャン方式が使用され、かつファイル内の未確認ウイルスの兆候がないかチェックされます。

未知のウイルスをスキャンするように ActiveShield を設定するには

1 マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。

2 **[詳細設定]** をクリックし、次に **[ActiveShield]** タブ (図 2-3) を選択します。

3 **[未知のウイルスをスキャンする (推奨)]** をクリックし、**[OK]** をクリックします。

スクリプトとワームをスキャンする

McAfee VirusScan はコンピュータを監視して、脅威となり得る不審な動作が存在するかどうかをチェックします。McAfee VirusScan がウイルスを駆除するのに対し、スクリプト ストッパー™ とワーム ストッパー™ はウイルス、ワーム、トロイの木馬がさらに伝染することを防ぎます。

スクリプト ストッパーとワーム ストッパーの保護メカニズムは、悪質な動作を検出して、警告およびブロックします。不審な動作には、以下のようなアクションがあります。

- ファイルを作成、コピー、削除したり、Windows レジストリを開いたりするスクリプトを実行する
- アドレス帳に保存されているアドレスの大多数に E メールを転送しようとする
- 複数の E メール メッセージを頻繁に転送しようとする

[詳細設定] ダイアログ ボックスで、デフォルト (標準の設定) の **[スクリプト ストッパーを有効にする (推奨)]** オプションと **[ワーム ストッパーを有効にする (推奨)]** オプションを使用するように ActiveShield を設定した場合、スクリプト ストッパーと ワーム ストッパーは、スクリプトの実行と E メールの動作に不審なパターンがないか監視します。指定した期間内に、E メールまたは E メールの受信者の数が指定した数を超えるとアラートが表示されます。

スクリプトとワームのような悪意ある動作をスキャンするよう設定するように ActiveShield を設定するには

1. マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。
2. **[詳細設定]** をクリックし、次に **[スクリプト ストッパー]** タブを選択します。
3. **[スクリプト ストッパーを有効にする (推奨)]** (22 ページの図 2-4) を選択します。

図 2-4 スクリプト ストッパーのオプション

4 **[ワーム ストッパー]** タブをクリックして、**[ワーム ストッパーを有効にする (推奨)]** を選択し、次に **[OK]** を選択します (23 ページの図 2-5)。

デフォルト (標準の設定) では、以下の詳細オプションが有効になっています。

- パターンを照合して不審な動作を検出する
- E メールが 40 人以上の受信者に送信されたときにアラートを表示する
- 30 秒間に 5 通以上の E メールが送信されたときにアラートを表示する

注

送信済み E メールの監視に適用される受信者数または秒数を変更すると、正しく検出できなくなることがあります。**[いいえ]** をクリックしてデフォルト設定 (標準の設定) をそのまま使用することをお勧めします。デフォルト設定 (標準の設定) を変更する場合は **[はい]** をクリックします。

このオプションは、潜在的なワームが初めて検出されると、自動的に有効になります (25 ページの「潜在的なワームを管理する」を参照してください)。

- 不審な送信 E メールを自動的にブロックする

図 2-5 ワーム ストッパーのオプション

ActiveShield がウイルスを検出した場合

ActiveShield によりウイルスが検出されると、図 2-6 のようなウイルス アラートが表示されます。ほとんどのウイルス、トロイの木馬、およびワームに対しては、ActiveShield によって自動駆除が実行されます。次に、感染しているファイルや E メール、不審なスクリプト、および潜在的なワームへの対処法や、感染ファイルをマカフィー AVERT の調査ラボへ報告するかどうかを選択できます。

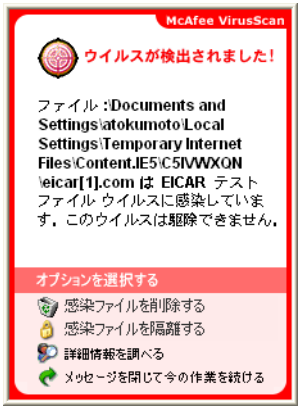


図 2-6 ウイルス アラート

感染ファイルを管理する

1 ActiveShield でファイルからウイルスを駆除できる場合、アラートの内容を詳しく調べたり無視することができます。

- **[詳細情報を調べる]** をクリックすると、感染したファイルの名前、場所、およびウイルス名が表示されます。
- アラートを無視して閉じる場合は、**[メッセージを閉じて今の作業を続ける]** をクリックします。

2 ActiveShield でファイルからウイルスを駆除できない場合、**[感染ファイルを隔離する]** をクリックすると、感染ファイルや不審なファイルを暗号化し、適切な操作を実行できるようになるまで一時的に隔離ディレクトリに隔離できます。

確認メッセージが表示され、コンピュータのウイルス チェックの実行を促します。**[スキャン]** をクリックすると、隔離処理が完了します。

3 ActiveShield でファイルを隔離できない場合、**[感染ファイルを削除する]** をクリックすると、ファイルを削除できます。

感染した E メールを管理する

1 E メールのウイルス自動駆除が無効になっている場合、詳細をチェックして E メールからウイルスを駆除できます。

   a **[詳細情報を調べる]** をクリックすると、感染したファイルの名前、ウイルスの名前、感染の状態、送信者、および件名が表示されます。

   b **[感染した添付ファイルからウイルスを駆除する]** をクリックします。

2 ActiveShield で E メールからウイルスを駆除できない場合、**[感染ファイルを隔離する]** をクリックすると、感染ファイルや不審なファイルを暗号化し、適切な操作を実行できるようになるまで一時的に隔離ディレクトリに隔離できます。

   確認メッセージが表示され、コンピュータのウイルス チェックの実行を促します。**[スキャン]** をクリックすると、隔離処理が完了します。

3 ActiveShield で E メールを隔離できない場合、**[感染ファイルを削除する]** をクリックして、ファイルを削除します。

不審なスクリプトを管理する

1 ActiveShield により不審なスクリプトが検出された場合、危険性等についての詳細をチェックして、不審なスクリプトを停止できます。

   a **[詳細情報を調べる]** をクリックすると、不審なスクリプトの名前、場所、および動作の詳細を表示できます。

   b **[このスクリプトを停止する]** をクリックすると、不要なスクリプトの実行を回避できます。

2 スクリプトが安全であることが確実な場合、スクリプトを実行できます。

   a **[今回このスクリプトを許可する]** をクリックすると、単一ファイル内のすべてのスクリプトを一回実行できます。

   b アラートを無視してスクリプトを実行する場合は、**[メッセージを閉じて今の作業を続ける]** をクリックします。

潜在的なワームを管理する

1 ActiveShield により潜在的なワームが検出された場合、ユーザは詳細をチェックして、不要な E メールの動作を停止できます。

   a **[詳細情報を調べる]** をクリックすると、感染した E メール メッセージの受信者リスト、件名、メッセージ本文、不審な動作の詳細を表示できます。

   b **[この E メールを停止する]** をクリックすると、不審な E メールの送信を回避して、メッセージ キューから削除できます。

2 E メールの動作が安全であることが確実な場合、**[メッセージを閉じて今の作業を続ける]** をクリックすると、アラートを無視して E メールを送信できます。

コンピュータのウイルスをスキャンする

スキャン機能を使用すると、ハード ドライブ、フロッピー ディスク、個々のファイルやフォルダからウイルスや不要なプログラムを検出できます。感染したファイルが検出されると、不審なプログラムでない限り、ウイルス駆除が自動的に実行されます。ウイルスを駆除できない場合は、そのファイルを隔離または削除できます。

ウイルスを手動でスキャンする

コンピュータをスキャンするには

1 マカフィー・アイコンを右クリックして **[VirusScan]** を選択してから、**[ウイルスをスキャンする]** をクリックします。

[ウイルスをスキャンする] ダイアログ ボックスが表示されます (図 2-7)。

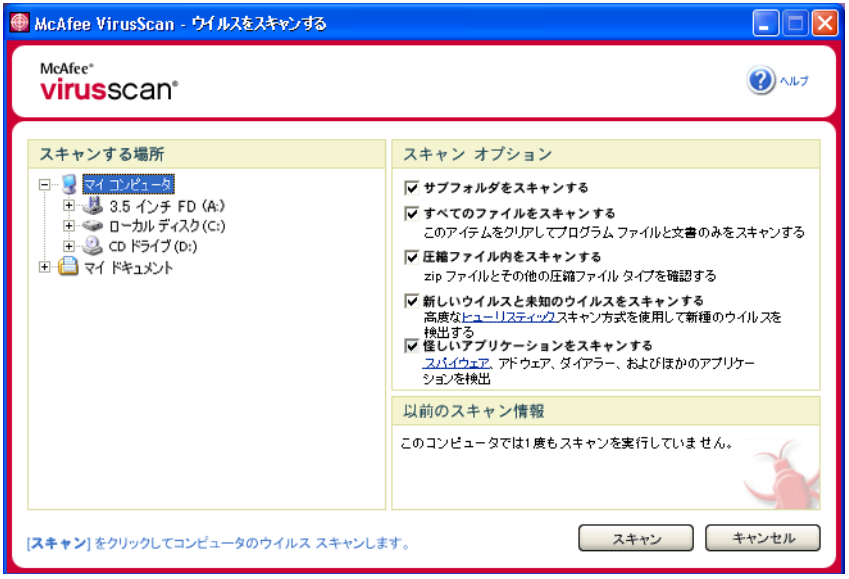


図 2-7 ウイルスをスキャンする

2 スキャンするドライブ、フォルダ、またはファイルをクリックします。

3 **[スキャン オプション]** を選択します。徹底的なスキャンを実行するため、デフォルト (標準の設定) ではすべての **[スキャン オプション]** のすべてのオプションが選択されています (図 2-7)。

- **[サブフォルダをスキャンする]** — このオプションを使用すると、サブフォルダ内のファイルもスキャンされます。このチェックボックスをオフにすると、フォルダまたはドライブを開いたときに表示されるファイルのみがチェックされます。

例 :**[サブフォルダをスキャンする]** チェックボックスをオフにすると、図 2-8 にあるファイルのみがスキャンされます。フォルダやその中身はスキャンされません。フォルダとそこに保存されているファイルをスキャンするには、チェックボックスをオンのままにしておく必要があります。

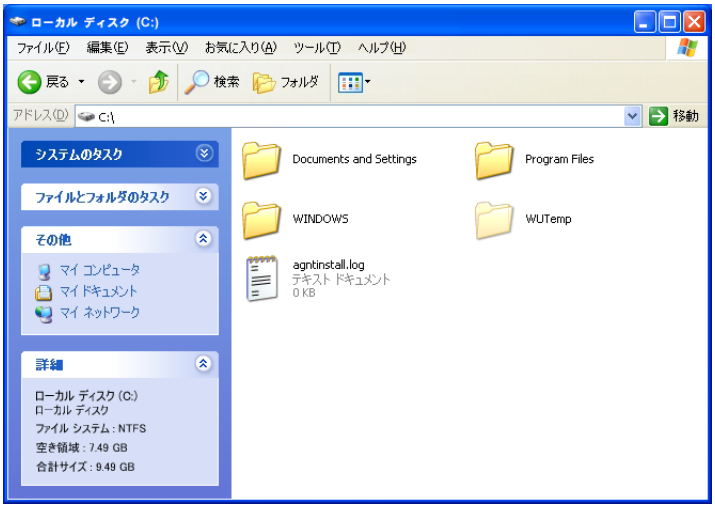


図 2-8 ローカル ディスクの内容

- **[すべてのファイルをスキャンする]** — このオプションを使用すると、すべての種類のファイルが完全にスキャンされます。このチェックボックスをオフにすると、プログラム ファイルと文書のみがスキャンされるため、スキャンの所要時間を短縮できます。
- **[圧縮ファイルをスキャンする]** — このオプションを使用すると、ZIP などの圧縮ファイル内にある隠れた感染ファイルを検出できます。このチェックボックスをオフにすると、圧縮ファイル内にあるファイルや圧縮ファイルのチェックは行われません。

  ウイルス作成者はウイルスを ZIP ファイルに埋め込み、その ZIP ファイルをさらに別の ZIP ファイルに入れて、ウイルス対策スキャナの目をすりぬけようとします。このオプションを選択しておくと、これらのウイルスを検出できます。
- **[未知のウイルスをスキャンする]** — このオプションを使用すると、対処法が存在しない場合がある最新のウイルスが検出されます。このオプションでは、ファイルと既知のウイルスのシグネチャを一致させる高度なヒューリスティック スキャン方式が使用され、かつファイル内の未確認ウイルスの兆候がないかチェックされます。

  このスキャン方式では、ウイルスを含むファイルとして識別するための一般的なファイル特性も検出します。これにより、誤った結果が表示される可能性を最小限に抑えることができます。ただし、ヒューリスティック スキャンでウイルスが検出された場合、ウイルスが含まれているとわかっているファイルを扱う場合と同様に、慎重にファイルを扱う必要があります。

このオプションでは最も徹底したスキャンが行われ、一般的に通常のスキャンよりも時間がかかります。

- **[怪しいアプリケーションをスキャンする]** — このオプションでは、ユーザがコンピュータへのインストールを意図していないスパイウェア、アドウェア、ダイアラ、その他のプログラムを検出できます。

注

最も徹底したスキャンを実行するには、すべてのオプションを選択したままにします。その場合、選択したドライブやフォルダ内のすべてのファイルが効率よくスキャンされます。スキャン完了までに十分に時間を用意してください。ハード ディスク ドライブが大きいほど、またファイルの数が多いほど、スキャンにかかる時間は長くなります。

4 **[スキャン]** をクリックしてファイルのスキャンを開始します。

スキャンが完了すると、スキャンしたファイルの数、検出したファイルの数、不審なプログラムの数、自動的に駆除されたファイルの数が [スキャンの概要] に表示されます。

5 **[OK]** をクリックして概要の画面を閉じます。検出されたファイルのリストが **[ウイルスをスキャンする]** ダイアログ ボックスに表示されます (図 2-9)。

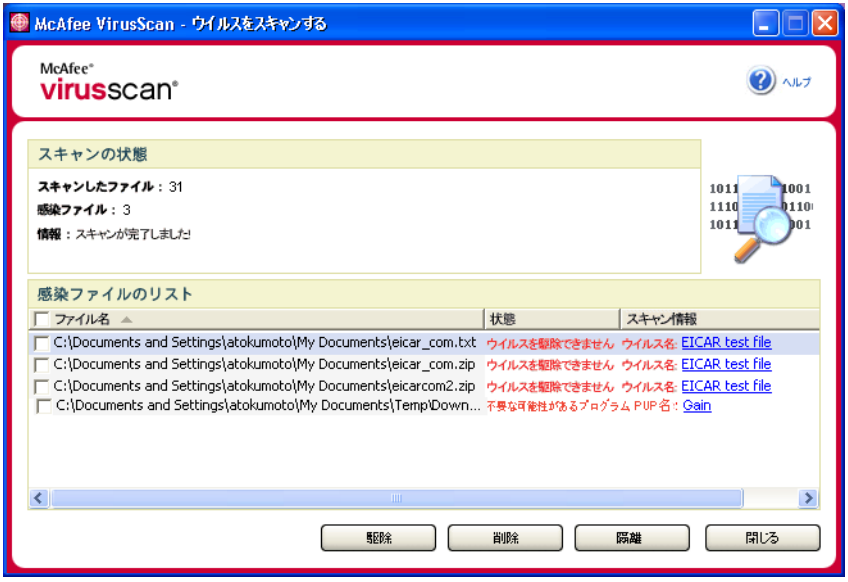


図 2-9 スキャンの結果

注

スキャンでは、圧縮ファイル (zip、cab など) は 1 つのファイルとして **[スキャンしたファイル]** 数に加算されます。また、前回のスキャン以降にインターネットの一時ファイルを削除した場合は、スキャンしたファイル数が変わる場合があります。

6 ウイルスや怪しいプログラムが検出されなかった場合は、**[戻る]** をクリックして別のフォルダまたはドライブをスキャンするか、**[閉じる]** をクリックしてダイアログボックスを閉じます。詳細は、31 ページの「ウイルスまたは怪しいプログラムが検出された場合」を参照してください。

Windows エクスプローラからウイルスをスキャンする

Windows エクスプローラ内からショートカット メニューを使用して、選択したファイル、フォルダ、またはドライブをスキャンできます。

Windows エクスプローラでファイルをスキャンするには

1 Windows エクスプローラを開きます。

2 スキャンするドライブ、フォルダ、ファイルを右クリックし、次に **[ウイルスをスキャンする]** をクリックします。

[ウイルスをスキャンする] ダイアログ ボックスが表示され、ファイルのスキャンが開始されます。徹底的なスキャンを実行するため、デフォルト (標準の設定) では **[スキャン オプション]** のすべてのオプションが選択されています (26 ページの図 2-7)。

Microsoft Outlook からウイルスをスキャンする

Microsoft Outlook 97 以降では、選択したメッセージ ストアやそのサブフォルダ、メールボックス フォルダ、または添付ファイルを含む E メール メッセージのウイルスや怪しいプログラムを、ツールバーのアイコンからスキャンできます。

Microsoft Outlook で E メールをスキャンするには

1 Microsoft Outlook を開きます。

2 スキャンするメッセージ ストア、フォルダ、または添付ファイルを含む E メールをクリックし、次にツールバーで、E メール スキャンのアイコン  をクリックします。

E メールのスキャナが開き、ファイルのスキャンが開始されます。徹底的なスキャンを実行するため、デフォルト (標準の設定) ではすべての**スキャン オプション**が選択されています (26 ページの図 2-7)。

ウイルスを自動的にスキャンする

ユーザまたはユーザのコンピュータがファイルにアクセスすると、McAfee VirusScan はファイルをスキャンしますが、Windows スケジューラで自動スキャンをスケジュール設定して、特定の間隔でコンピュータのウイルスや不審なプログラムを完全にチェックすることもできます。

スキャンのスケジュールを設定するには

1 マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。

McAfee VirusScan の **[オプション]** ダイアログ ボックスが表示されます。

2 **[スケジュール スキャン]** タブをクリックします (30 ページの図 2-10)。

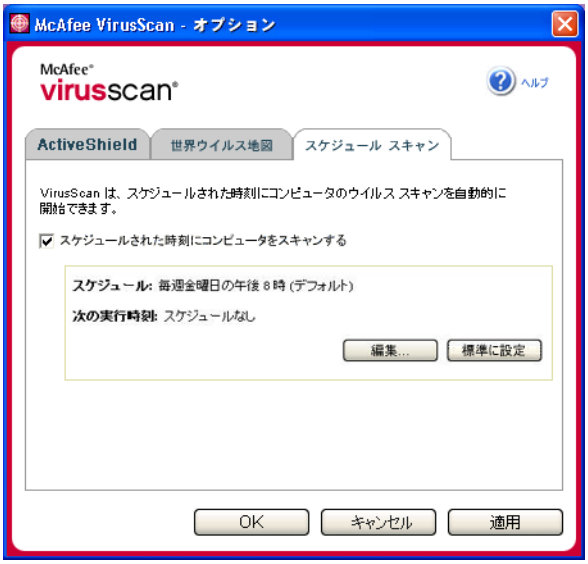


図 2-10 スケジュール スキャン オプション

3 **[スケジュールされた時刻にコンピュータをスキャンする]** チェックボックスを選択し、自動スキャンを有効にします。

4 自動スキャンのスケジュールを指定します。

- デフォルト (標準の設定) のスケジュール (毎週金曜日の午後 8 時) を使用するには、**[OK]** をクリックします。
- スケジュールを編集するには

  a. **[編集]** をクリックします。

  b. コンピュータをスキャンする頻度を **[タスクのスケジュール]** リストで選択し、その下の動的エリアでその他のオプションを選択します。

[日単位] — スキャンの間隔を日数で指定します。

[週単位] (デフォルト (標準の設定)) — スキャンの間隔を週数で指定し、曜日も指定します。

[月単位] — スキャンを実行する日を指定します。スキャンを実行する月を指定する場合は、**[実行する月の選択]** をクリックし、**[OK]** をクリックします。

[1 回のみ] — スキャンを実行する日付を指定します。

注
以下の Windows スケジューラのオプションはサポートされません。**[システム起動時]**、**[アイドル時]**、**[複数のスケジュールを表示する]**。有効なオプションを選択しないと、最後にサポートされたスケジュールがそのまま有効になります。

c. コンピュータをスキャンする時刻を **[開始時刻]** ボックスで選択します。

d. 詳細なオプションを選択するには、**[詳細設定]** をクリックします。

[スケジュール オプションの詳細設定] ダイアログ ボックスが表示されます。

i. 開始日、終了日、期間、終了時刻、およびスキャンがまだ実行中の場合に指定した時刻でタスクを停止するかどうかを指定します。

ii. **[OK]** をクリックして変更を保存し、ダイアログ ボックスを閉じます。または、**[キャンセル]** をクリックします。

5 **[OK]** をクリックして変更を保存し、ダイアログ ボックスを閉じます。または、**[キャンセル]** をクリックします。

6 スケジュールをデフォルト (標準の設定) に戻すには、**[標準に設定]** をクリックします。それ以外の場合は、**[OK]** をクリックします。

ウイルスまたは怪しいプログラムが検出された場合

ほとんどのウイルス、トロイの木馬、およびワームに対しては、ウイルス駆除が自動的に実行されます。次に、検出されたファイルの対処法や、ファイルをマカフィー AVERT の調査ラボへ報告するかどうかを選択できます。怪しいプログラムを検出した場合は、手動でプログラムを駆除、隔離、または削除できます (AVERT 送信は使用できません)。

ウイルスや怪しいプログラムを管理するには

1 ファイルが **[検出されたファイル]** の一覧に表示されている場合は、そのファイルの横にあるチェックボックスをオンにします。

注
一覧に複数のファイルが表示される場合は、**[ファイル名]** リストの先頭にあるチェックボックスをオンにすると、すべてのファイルに同じ操作を実行することができます。**[スキャン情報]** リストのファイル名をクリックして、ウイルス情報ページから詳細を表示することもできます。

2 ファイルが怪しいプログラムを含んでいる場合は、**[駆除]** をクリックして、駆除を試行します。

3 スキャンでファイルからウイルスを駆除できない場合、**[隔離]** をクリックすると、感染ファイルや不審なファイルを暗号化し、適切な操作を実行できるようになるまで一時的に隔離ディレクトリに隔離できます (詳細については、33 ページの「隔離ファイルを管理する」を参照してください)。

4 スキャンによってファイルを隔離できない場合は、次のいずれかの操作を実行できます。

- **[削除]** をクリックしてファイルを削除します。
- これ以上操作を実行せずにダイアログ ボックスを閉じるには、**[キャンセル]** をクリックします。

スキャンでファイルを駆除または検出できない場合、ウイルスを手動で削除する方法については、ウイルス情報ページ (http://www.mcafeesecurity.com/japan/security/) を参照してください。

検出されたファイルによってインターネットに接続できない場合やコンピュータをまったく使用できない場合は、システム修復ディスクを使用してコンピュータを起動してください。検出されたファイルによってコンピュータが使用不能になっている場合は、通常、システム修復ディスクでコンピュータを起動できます。詳細については、35 ページの「システム修復ディスクを作成する」を参照してください。

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

隔離ファイルを管理する

隔離機能を使用すると、感染ファイルや不審なファイルを暗号化し、適切な操作を実行できるようになるまで一時的に隔離ディレクトリに隔離できます。隔離されたファイルは、ウイルスを駆除した後、元の場所に復元できます。

隔離ファイルを管理するには

1 マカフィー・アイコンを右クリックして、**[VirusScan]** を選択してから **[隔離ファイルの管理]** をクリックします。

隔離ファイルの一覧が表示されます (図 2-11)。

図 2-11 隔離ファイルの管理

2 駆除するファイルの横にあるチェックボックスをオンにします。

注

一覧に複数のファイルが表示された場合は、**[ファイル名]** リストの横にあるチェックボックスをオンにして、すべてのファイルに同じ処理を実行することができます。**[状態]** リストのウイルス名をクリックして、ウイルス情報ページから詳細を表示することもできます。

または、**[追加]** をクリックし、隔離ファイルの一覧に追加する不審なファイルを選択してから、**[開く]** をクリックして隔離ファイルの一覧からそのファイルを選択します。

3 **[駆除]** をクリックします。

4 ファイルからウイルスが駆除されたら、**[復元]** をクリックしてファイルを元の場所に戻します。

5 McAfee VirusScan でウイルスを駆除できない場合は、**[削除]** をクリックしてファイルを削除します。

6 McAfee VirusScan でファイルからウイルスを駆除または削除できず、そのファイルが怪しいプログラムではない場合は、マカフィー・ウイルス緊急対策チーム (AVERT™) にファイルを送信し、調査を依頼できます。

   a 2 週間以上前のウイルス定義ファイルを使用している場合は更新してください。

   b 契約状況を確認します。

   c ファイルを選択し、**[送信]** をクリックして AVERT にファイルを送信します。

   McAfee VirusScan では、E メール アドレス、国、ソフトウェアのバージョン、オペレーティング システム、およびファイルの元の名前と場所を含む E メール メッセージの添付ファイルとして隔離ファイルが送信されます。1 日に 1 度、最大 1.5 MB のファイルを送信できます。

7 これ以上操作を実行せずにダイアログ ボックスを閉じるには、**[キャンセル]** をクリックします。

システム修復ディスクを作成する

システム修復ディスクは、コンピュータの起動を妨げているウイルスをスキャンするためのブート可能なフロッピー ディスクを作成するユーティリティです。

注
システム修復ディスクをダウンロードするには、インターネットに接続している必要があります。さらに、システム修復ディスクは、FAT (FAT 16 および FAT 32) ハード ドライブ パーティションを装備したコンピュータでのみ使用できます。システム修復ディスクは、NTFS パーティションには必要ありません。

注
HDD: 4 GB 以上は未対応となります。

注
本機能は各パソコン メーカが提供するマカフィー プリインストール版では提供されておりません。

システム修復ディスクを作成するには

1 ウイルスに感染していないコンピュータで、感染していないフロッピー ディスクを A ドライブに挿入します。コンピュータとフロッピー ディスクのどちらもウイルスに感染していないことを確認するため、スキャンを使用することをお勧めします (詳細については、26 ページの「ウイルスを手動でスキャンする」を参照してください)。

2 マカフィー・アイコンを右クリックして、**[VirusScan]** を選択してから **[システム修復ディスクの作成]** をクリックします。

[システム修復ディスクの作成] ダイアログ ボックスが表示されます (図 2-12)。

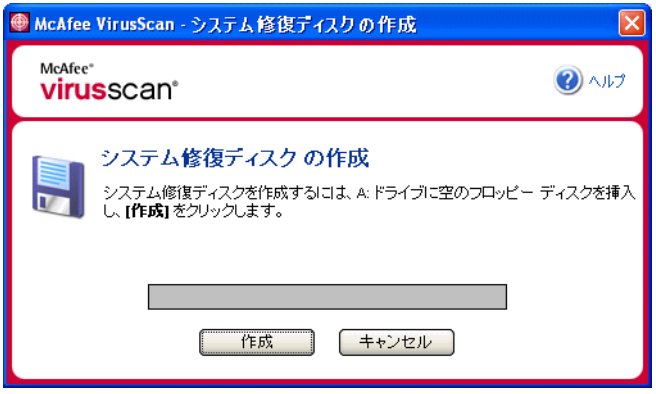


図 2-12 システム修復ディスクの作成

3 **[作成]** をクリックしてシステム修復ディスクを作成します。

初めてシステム修復ディスクを作成する場合、システム修復ディスクにイメージファイルをダウンロードする必要があることを伝えるメッセージが表示されます。コンポーネントを今すぐダウンロードする場合は **[OK]** をクリックし、後でダウンロードする場合は **[キャンセル]** をクリックします。

フロッピー ディスクの内容が失われることを知らせる警告メッセージが表示されます。

4 **[はい]** をクリックしてシステム修復ディスクの作成を続行します。

作成プロセスの状態が **[システム修復ディスクの作成]** ダイアログ ボックスに表示されます。

5 「システム修復ディスクが作成されました」というメッセージが表示されたら、**[OK]** をクリックして **[システム修復ディスクの作成]** ダイアログ ボックスを閉じます。

6 システム修復ディスクをドライブから取り出し、ライトプロテクトにして、安全な場所に保管します。

システム修復ディスクをライトプロテクトにする

システム修復ディスクをライトプロテクトにするには

1 フロッピー ディスクのラベル面を下向きにします (円形の金属面が見えるはずです)。

2 ライトプロテクトのつまみを探します。つまみをスライドさせて穴が見えるようにします。

システム修復ディスクを使用する

システム修復ディスクを使用するには

1 ウイルスに感染しているコンピュータの電源をオフにします。

2 システム修復ディスクをドライブに挿入します。

3 コンピュータの電源をオンにします。

複数のオプションが灰色のウィンドウに表示されます。

4 ファンクション キー (F2、F3 など) を押して、必要に応じた最適なオプションを選択します。

注
キーを押さなかった場合は、60 秒後に自動的にシステム修復ディスクが起動します。

システム修復ディスクを更新する

システム修復ディスクは定期的に更新することをお勧めします。システム修復ディスクを更新するには、新しいシステム修復ディスクを作成する場合と同じ手順に従います。

ウイルスを自動的にレポートする

ウイルス追跡情報を匿名で送信して、世界ウイルス地図に追加することができます。セキュリティ保護されているこの機能は、McAfee VirusScan のインストール時に **[世界ウイルス地図]** ダイアログ ボックスで登録するか、McAfee VirusScan の **[オプション]** ダイアログ ボックスにある **[世界ウイルス地図]** タブでいつでも自動的に登録できます。

世界ウイルス地図にレポートする

ウイルス情報を世界ウイルス地図に自動的にレポートするには

1 マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[オプション]** をクリックします。

McAfee VirusScan の **[オプション]** ダイアログ ボックスが表示されます。

2 **[世界ウイルス地図]** タブをクリックします (図 2-13)。

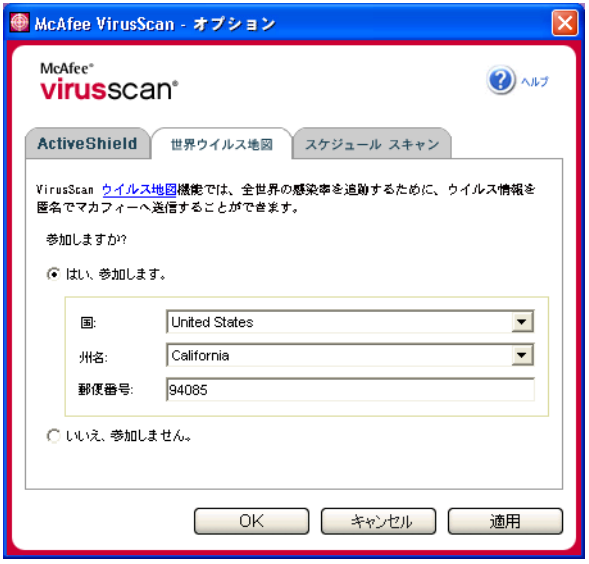


図 2-13 世界ウイルス地図のオプション

3 匿名でウイルス情報をマカフィーに送信し、全世界の感染率を表示する世界ウイルス地図に追加するには、デフォルト (標準の設定) の **[はい、参加します]** オプションを受け入れます。ウイルス情報の送信を行わない場合は、**[いいえ、参加しません]** を選択します。

4 米国内のユーザの場合、コンピュータを設置している場所の州を選択し、郵便番号を入力します。米国以外のユーザの場合、コンピュータを設置している国が McAfee VirusScan によって自動的に選択されます。

5 **[OK]** をクリックします。

世界ウイルス地図を表示する

世界ウイルス地図に参加しているかどうかにかかわらず、Windows のシステム トレイにあるマカフィー・アイコンをクリックすると、最新の全世界の感染率を表示することができます。

世界ウイルス地図を表示するには

- マカフィー・アイコンを右クリックし、**[VirusScan]** を選択してから **[世界ウイルス地図]** をクリックします。

  世界ウイルス地図の Web ページが表示されます (図 2-14)。

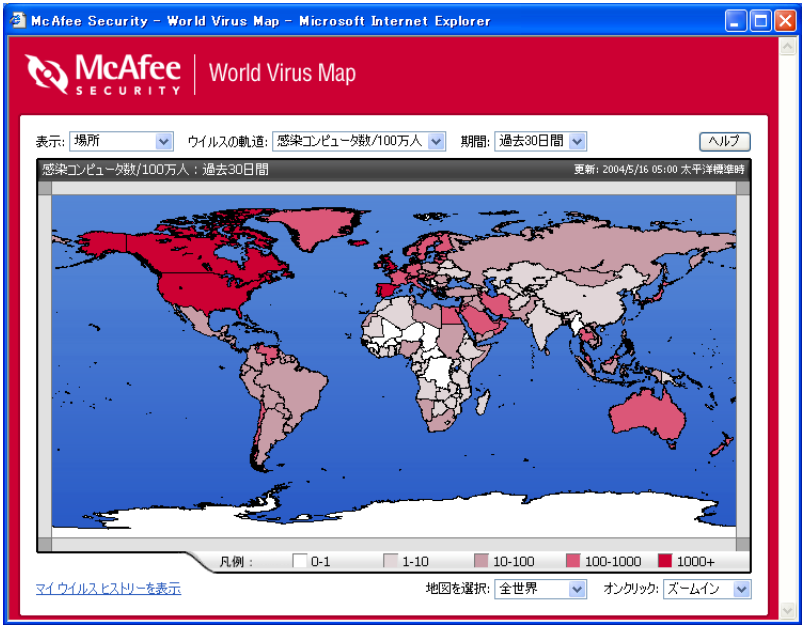


図 2-14 世界ウイルス地図

世界ウイルス地図には、デフォルト (標準の設定) では、過去 30 日間に全世界で感染したコンピュータの数と、レポートされたデータの最終更新日時が表示されます。感染したファイル数を表示できるようにマップ表示を変更したり、過去 7 日間または過去 24 時間以内の結果のみを表示するように時間間隔を変更したりすることができます。

ウイルス追跡セクションには、表示日付以降にレポートされたスキャンしたファイル数、感染したファイル数、感染したコンピュータ数の累積集計が一覧されます。

McAfee VirusScan を更新する

インターネットに接続している間は、McAfee VirusScan は 4 時間ごとに最新の更新を自動的にチェックしてダウンロードし、週ごとにウイルス定義の更新をインストールします。その際に、ユーザの作業が中断されることはありません。

ウイルス定義ファイルは約 100 KB であり、ダウンロードによるシステムのパフォーマンスへの影響はほとんどありません。

製品の更新がある場合、またはウイルスが大発生している場合は、アラートが表示されます。アラートが表示されたら、McAfee VirusScan を更新して、ウイルス発生の脅威を取り除くことができます。

更新を自動的に確認する

インターネットに接続している間は、McAfee SecurityCenter は 4 時間ごとにすべての McAfee サービスの更新を自動的にチェックし、アラートおよびサウンドによってユーザに通知します。デフォルト (標準の設定) では、McAfee SecurityCenter は必要な更新を自動的にダウンロードし、インストールします。

注
更新を完了するためにコンピュータを再起動するようメッセージが表示される場合があります。再起動する前に、必ず作業中のデータをすべて保存し、すべてのアプリケーションを閉じてください。

更新を手動で確認する

インターネットに接続している間は、4 時間ごとに更新の自動確認が行われますが、いつでも手動で更新の有無を確認できます。

更新を手動で確認するには

1. コンピュータがインターネットに接続されていることを確認します。
2. マカフィー・アイコンを右クリックし、**[更新]** をクリックします。

   [SecurityCenter の更新] ダイアログ ボックスが表示されます。
3. **[今すぐ確認する]** をクリックします。

   更新がある場合、McAfee VirusScan の **[更新]** ダイアログ ボックスが表示されます (40 ページの図 2-15 を参照)。**[更新]** をクリックして続行します。

   利用可能な更新がない場合、McAfee VirusScan が最新状態であることがダイアログ ボックスで通知されます。**[OK]** をクリックしてダイアログ ボックスを閉じます。

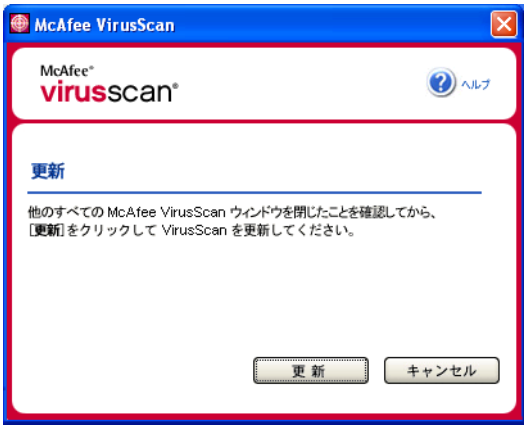


図 2-15 [更新] ダイアログ ボックス

4 ログオン メッセージが表示された場合は、Web サイトにログオンします。**更新ウィザード**により、自動的に更新がインストールされます。

5 更新のインストールが終了したら、**[完了]** をクリックします。

注
更新を完了するためにコンピュータを再起動するようメッセージが表示される場合があります。再起動する前に、必ず作業中のデータをすべて保存し、すべてのアプリケーションを閉じてください。

索引

う

か

く

け

こ

さ

し

す

せ

と

ふ

み

わ