リリース ガイド

VirusScan

V4.5.1

McAfee SECURITY

目次

まえがき 5

このガイドについて 5

対象読者 5

詳細情報 6

日本ネットワークアソシエイツ株式会社 7

第 1 章　このリリースの新機能 9

新機能 10

感染しやすいファイルのみのスキャン 10

passive FTP の使用 12

スキャン エンジンと .DAT ファイルのアップデート 13

Network Associates アップデート サイトのミラーリング 14

自動アップデートの設定 16

アップデートまたはアップグレード後のプログラムの実行 18

ネットワーク ドライブ スキャンのスケジューリング 19

第 2 章　インストール 21

概要 21

システム要件 23

インストールの前に 23

ソフトウェアのインストール 25

ソフトウェアの変更と削除 30

設定の保存 31

コンピュータの再起動が必要な場合 32

第 3 章　.DAT ファイルのアップデート 35

概要 35

自動アップデートの設定 37

自動アップデートの開始 37

アップデート サイトの定義 39

アップデートの詳細設定オプションの選択 44

アップデートの記録 45

第 4 章 Network Associates アップデート サイトのミラーリング 47
概要 47
ミラーリングの設定 48
Mirror ユーティリティの開始 49
Mirror サイトの定義 50
宛先フォルダの定義 53
ミラーリングの記録 54

索引 55

まえがき

このガイドについて

このガイドでは、McAfee VirusScan バージョン 4.5 以降の VirusScan 製品に行われた主な変更点について説明します。このガイドは、以下のマニュアルと一緒にお読みください。マニュアルの入手方法については、6 ページの「関連マニュアル」の「詳細情報」を参照してください。

マニュアル	内容
ePolicy Orchestrator 管理者ガイド	McAfee ePolicy Orchestrator による製品の配備
VirusScan ウイルス対策ソフトウェア v4.5 コンフィグレーションガイド（ePolicy Orchestrator 用）	McAfee ePolicy Orchestrator による VirusScan 製品の設定
VirusScan ウイルス対策ソフトウェア v4.5 ユーザーズガイド	VirusScan 製品の設定と使用方法
VirusScan ウイルス対策ソフトウェア v4.5 管理者ガイド	ネットワーク環境での VirusScan の管理
VirusScan v4.5 の README.TXT	VirusScan 4.5 に関する重要な情報と既知の問題

対象読者

このガイドの対象読者は次のとおりです。

- 企業のウイルス対策製品を担当しているネットワーク管理者
- ワークステーションのウイルス定義（.DAT）ファイルをアップデートするユーザ。または、ウイルスの検出オプションを設定するユーザ。

このリリースで追加された Mirror ユーティリティに関する記述は、管理者のみを対象にしています。通常、ワークステーション ユーザがこの機能を使用することはありません。

詳細情報

ヘルプ	VirusScan 製品のヘルプ機能を使用すると、より詳しい情報を得ることができます。ヘルプを起動するには、VirusScan コンソールの［ヘルプ］メニューを使用します。
README.TXT	このマニュアルは製品に同梱されています。製品に対する最新の変更点、現在のリリースで見つかっている問題点、また現在のリリースで解決されている問題点などが記載されています。
CONTACT.TXT	弊社の連絡先に関する情報が記載されています。
関連マニュアル	このガイドは、VirusScan 4.5 とそのサービス パックに付属の次のマニュアルを補足するものです。 • *管理者ガイド* • *ユーザーズ ガイド* • *コンフィグレーションガイド（ePolicy Orchestrator 用）* • README.TXT ファイル 承認番号をお持ちの方は、以前にリリースされたマニュアルを次の Web サイトからダウンロードできます。 http://www.nai.com/japan/download/licensed.asp 承認番号をお持ちでない方、あるいは最新の承認番号がご不明な方は、弊社カスタマ サービスまでご連絡ください。

日本ネットワークアソシエイツ株式会社

■東京

東京都渋谷区道玄坂一丁目 1 2-1 渋谷マークシティ ウェスト 20 階

TEL 03-5428-1100（代表）

■西日本営業所

大阪府大阪市北区堂島 2 丁目 2 番 2 号　近鉄堂島ビル 18 階

■福岡営業所

福岡市博多区博多駅東 1- 10- 27 アスティア博多ビル 8 F

このリリースの新機能 1

このリリースでは、VirusScan に 5 つの新機能が追加されました。新機能の内容と詳細情報については、以下のリストを参照してください。

新機能

- 感染しやすいファイルのみのスキャン （10 ページ）
- passive FTP の使用 （12 ページ）
- スキャン エンジンと .DAT ファイルのアップデート （13 ページ）
- Network Associates アップデート サイトのミラーリング （14 ページ）
- 自動アップデートの設定 （16 ページ）
- アップデートまたはアップグレード後のプログラムの実行 （18 ページ）
- ネットワーク ドライブ スキャンのスケジューリング （19 ページ）

新機能

感染しやすいファイルのみのスキャン

前のリリース

スキャナですべてのファイル タイプをスキャンするか、ユーザ定義リストで指定した拡張子のファイルだけをスキャンするのか設定できました。拡張子の指定は［**指定した拡張子のみ**］ボタンで設定できました。

現在のリリース

- 新しいオプションである［**デフォルト ファイル**］を選択すると、McAfee AVERT（Anti-Virus Emergency Response Team）が感染しやすいタイプとして定義しているファイルだけをスキャンすることができます。感染しやすいファイル タイプのリストは、最新のウイルス定義ファイル（.DAT）に含まれています。デフォルトでは、このオプションが選択されています。
- このリリースでは、拡張子のユーザ定義リストは**ユーザ指定ファイル**という名前に変更されています。

利点

すべてのファイルをスキャンすると、完全なウイルス対策を行うことができますが、ウイルス スキャンにかかる時間が非常に長くなります。

- ユーザ定義リストにあるファイル タイプだけをスキャンすると、ウイルスに感染しにくいファイルをスキャンの対象外にすることができます。
- デフォルトのファイルをスキャンすると、現在流行しているウイルスに感染しやすいファイルだけがスキャンされます。これは、非常に経済的で、効果的なオプションです。

操作方法

オンアクセス スキャン :

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan コンソール**］の順に選択します。
2. ［**Vshield**］をダブルクリックして、インストールされたスキャン モジュールの［**状態**］ページを開きます。通常、［**システム スキャン状態**］ページが最初に開きます。
3. ［**プロパティ**］をクリックして、インストールされたスキャン モジュールのプロパティ ページを開きます。通常、［**システム スキャン プロパティ**］ページが最初に開き、［**スキャン**］タブが表示されます。

オンデマンド スキャン :

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan**］または［**VirusScan コンソール**］の順に選択します。
2. コンソールに表示されたスキャン タスクをダブルクリックします。［**マイコンピュータのスキャン**］と［**C: ドライブのスキャン**］の 2 つのスキャン タスクが表示されます。

passive FTP の使用

前のリリース

FTP 経由でファイルをダウンロードするには、active FTP を使用する必要がありました。

現在のリリース

自動アップデート、自動アップグレード、新規の Mirror ユーティリティでは、passive FTP がデフォルトの設定になっています。この概要については 14 ページを、詳細については第 4 章 の 47 ページ以降を参照してください。active FTP が必要な状況では、［**PASSIVE FTP を使用する**］の選択が解除できます。

利点

- ファイアウォールやプロキシを使用する環境では、クライアントがコマンド セッションとデータ セッションの両方を開始するので、passive FTP は効果的です。これにより、ファイアウォールまたはプロキシとクライアント / サーバとの通信を減らすことができます。
- ネットワークによっては active FTP しか使用できない場合があります。この環境では、クライアントがコマンド セッションを開始し、サーバがデータ セッションを開始します。このような場合には、passive FTP オプションの選択を解除することができます。active FTP による転送は、ファイアウォールまたはプロキシを経由して行われます。

操作方法

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan コンソール**］の順に選択します。
2. ［**.DAT の自動アップデート**］をダブルクリックして、［**タスク プロパティ**］ダイアログ ボックスを開きます。
3. ［**設定**］をクリックして、［**自動アップデート**］ページを開きます。
4. ［**追加**］をクリックして新しいダウンロード サイトを設定するか、［**編集**］をクリックして既存のサイトを編集します。

スキャン エンジンと .DAT ファイルのアップデート

前のリリース

自動アップデートでは、Network Associates FTP サイトから .DAT ファイルだけがダウンロードされ、インストールされました。スキャン エンジンのアップグレードは、正規版の製品のアップグレードとして、またはエンジンの部分的なリリースに対するアップグレードして実行できました。また、McAfee Super DAT ユーティリティでもアップグレードが可能でした。

現在のリリース

自動アップデートを設定するときに、［**最新のスキャン エンジンが存在する場合は更新する**］が選択できます。この機能を実行するときに、ユーザが SuperDAT のエンジン アップグレード機能を開始する必要はありません。

利点

- .DAT ファイルをアップデートするときに、スキャン エンジンも最新の状態にすることができます。
- エンジンのアップグレードに、特別なユーティリティは必要ありません。
- 最新のリリースが発表されるまで待たなくても、最新のエンジンを入手することができます。
- 自動アップデートでは、現在使用されている .DAT とエンジンよりも新しい .DAT とエンジンがダウンロードされるので、通信コストを節約することができます。

操作方法

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan コンソール**］の順に選択します。
2. ［**.DAT の自動アップデート**］をダブルクリックして、［**タスク プロパティ**］ダイアログ ボックスを開きます。
3. ［**設定**］をクリックして、［**自動アップデート**］ページを開きます。
4. アップデート サイトを作成するか、［**アップデート サイト**］ページに表示されたサイトから選択します。デフォルトでは、Network Associates のダウンロード サイトが表示されています。このリストには、最大 16 までのサイトが追加できます。
5. ［**拡張アップデート オプション**］タブを選択します。［**拡張アップデート オプション**］の下に新規オプションが表示されます。

詳細情報

第 3 章、「.DAT ファイルのアップデート」の 35 ページ以降

Network Associates アップデート サイトのミラーリング

前のリリース

- ネットワーク管理者が、［**後で使用するためにアップデート ファイルを保存する**］を選択して、アップデート ファイルのソース サイトにネットワーク上の場所を指定することができました。
- アップデートを設定したコンピュータ上の .DAT ファイルがアップデートされた後で、その .DAT ファイルがある Network Associates FTP サイトの内容が、指定したネットワーク上の場所にコピーされました。
- ネットワーク上の場所は、仮想レプリカまたは Network Associates の Mirror サイトになりました。

現在のリリース

- 現在のリリースでは、Network Associates アップデート サイトのミラーリングを行うインタフェースと機能が追加されました。デザインが似ている一連の設定ページと新しい［**自動アップデート**］ページを使用して、ミラーリング機能がセットアップできます。
- VirusScan を ePolicy Orchestrator でインストールする場合には、Mirror ユーティリティはデフォルトでインストールされます。
- VirusScan をインストール ウィザードでインストールする場合には、カスタム インストールを選択して、［**Mirror Task**］を選択すると、ミラーリング機能がインストールされます。

  注 : カスタム インストールで Mirror Task を選択するには、ツリー ビューの VirusScan コンソールから自動アップデートを選択します。その下にある［**Mirror Task**］アイコンをクリックして、［**この機能をローカルハードディスクにインストールします**］を選択します。カスタム インストールの詳細については、27 ページを参照してください。

利点

- ネットワーク上のコンピュータがインターネットにアクセスできるかどうかに関係なく、コンピュータをアップデートすることができます。
- Network Associates FTP サーバより近くにあるサーバにアクセスするので、ワークステーションへのダウンロードを高速に行うことができます。

操作方法

この機能は VirusScan コンソールまたは ePolicy Orchestrator から実行できます。

VirusScan:

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan コンソール**］の順に選択します。
2. ［**VirusScan コンソール**］ウィンドウで［**Mirror**］をダブルクリックして、［**タスク プロパティ**］ダイアログ ボックスを開きます。
3. ［**設定**］をクリックして、［**VirusScan Mirror サイト**］ページを開きます。［**ソース サイト**］タブが表示されます。
4. ［**追加**］をクリックして、［**Mirror オプション**］ページを開きます。
5. ダウンロードに使用するミラー サーバのサイトと Network Associates FTP ダウンロード サイトを定義します。
6. ［**宛先**］タブを選択して、Network Associates FTP ダウンロード サイトのコンテンツをダウンロードするミラー サーバのフォルダ パスを指定します。

ePolicy Orchestrator:

1. ePolicy Orchestrator スケジューラを開きます。
2. ［**タスクの種類**］フィールドで［**自動アップデートのミラー サイト**］を選択します。

詳細情報

第 4 章、「Network Associates アップデート サイトのミラーリング」の 47 ページ以降

ヒント：コマンド ライン、ログイン スクリプト、またはバッチ ファイルで新しいコマンド ライン スイッチ /BATCH を使用すると、自動アップデート、自動アップグレード、Mirror ユーティリティが実行できます。タスクの進行状況を示すダイアログ ボックスが表示されます。状況を示す最後のダイアログ ボックスは、タスクが完了して 2 秒後に自動的に消えます。このスイッチの構文は、定義しているタスクの条件によって異なります。

```
MCUPDATE /TASK UPDATE /BATCH
MCUPDATE /TASK UPGRADE /BATCH
MCUPDATE /TASK MIRROR /BATCH
```

自動アップデートの設定

前のリリース

- アップデート ファイルをダウンロードするサイトを最大 8 つまで指定できました。
- リモート ネットワーク コンピュータから FTP 経由でアップデート ファイルを転送することも、ローカル ネットワーク コンピュータからファイルをコピーすることもできました。
- アップデート ファイルを取得しても、アップデートを実行せずに後で使用するために保存することもできました。この方法では、Network Associates ダウンロード サイトの仮想的なレプリカが作成できました。
- アップデートが正常に終了した後にシステムを再起動するように設定することができました。

現在のリリース

- 新しいインタフェースでは、［**自動アップデート**］ページが表示されます。これは、新しい Mirror ユーティリティのデザインに良く似ています。
- アップデート ファイルをダウンロードするサイトは最大 16 まで指定できます。
- アップデート ファイルは、FTP を経由してアクセス可能な任意のコンピュータから取得することができます。また、ローカル コンピュータの共有フォルダからファイルをコピーしたり、自動アップデートを設定したコンピュータからコピーすることもできます。
- Mirror ユーティリティが追加されたため、後で使用するためにアップデート ファイルを取得するオプションは破棄されました。
- アップデート後にシステムを再起動する必要はありません。
- このリリースでは、.DAT ファイルのアップデート時にスキャン エンジンもアップグレードできます。この機能の詳細については、13 ページの「スキャン エンジンと .DAT ファイルのアップデート」を参照してください。
- 最新のリリースでは、.DAT ファイルの転送に passive FTP が使用できます。この機能の詳細については、12 ページの「passive FTP の使用」を参照してください。

利点

- 自動アップデートの設定インタフェース、関連機能、ミラーリングによって、以前のインタフェースよりも使いやすさが向上しました。
- 指定できるダウンロード サイトの数が増えました。
- アップデート後にコンピュータを再起動する必要はありません。
- .DAT ファイルのアップデート時に新しいスキャン エンジンもダウンロードできます。
- ファイル転送に passive FTP が使用できます。

操作方法

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan コンソール**］の順に選択します。
2. ［**コンソール**］ウィンドウで［**.DAT の自動アップデート**］を選択して、［**タスク プロパティ**］ダイアログ ボックスを開きます。
3. ［**設定**］をクリックして、［**自動アップデート**］ページを開きます。［**アップデート サイト**］タブが表示されます。
4. ［**追加**］をクリックして、［**サイト オプション**］ページを開きます。
5. 最新のウイルス定義ファイル（.DAT) を取得するネットワーク コンピュータにサイトを定義します。［**OK**］をクリックして［**アップデート サイト**］ページに戻ります。
6. ［**拡張アップデート オプション**］タブを選択して、詳細設定オプションを指定します。

詳細情報

第 3 章、「.DAT ファイルのアップデート」の 35 ページ以降

アップデートまたはアップグレード後のプログラムの実行

前のリリース

- アップデートの完了後すぐにプログラムを実行することができました。
- アップグレードの完了後すぐに、プログラムを実行することはできませんでした。

現在のリリース

- デフォルトでは、アップデートの状況に関係なく、プログラムが実行されます。このリリースでは、正常にアップデートされた後に起動するプログラムを指定することができます。
- アップグレードの状況に関係なく、アップグレード後に実行するプログラムが選択できます。

利点

- アップデートまたはアップグレード後に実行するプログラムが指定できます。
- アップデートまたはアップグレードが正常に終了した場合にのみ実行するプログラムを指定することができます。

  注 : 自動アップデートまたは自動アップグレード後に実行するプログラムを選択する場合、プログラムの実行時にユーザがシステムにログオンしていなければなりません。ユーザがログオンしていないと、プログラムは実行されません。このため、特定の権限しかないユーザは、システム アカウントの権限が取得できなくなります。ログオンしているユーザがいない場合には、システム アカウントによってシステムが制御されます。

操作方法

1. [**スタート**] > [**プログラム**] > [**Network Associates**] > [**VirusScan コンソール**] の順に選択します。
2. [**コンソール**] ウィンドウで [**.DAT の自動アップデート**] (または [**製品の自動アップグレード**]) を選択して、[**タスク プロパティ**] ダイアログ ボックスを開きます。
3. [**設定**] をクリックして、選択したタスクのプロパティ ページを開きます。
4. [**追加**] をクリックして、[**サイト オプション**] ページを開きます。
5. アップデート ファイルまたはアップグレード ファイルを取得するコンピュータのあるサイトを定義します。
6. [**拡張アップデート オプション**] タブを選択して、詳細設定オプションを指定します。

ネットワーク ドライブ スキャンのスケジューリング

前のリリース

オンデマンド スキャナには、Windows NT または Windows 2000 環境でネットワーク ドライブをスキャンする機能がありません。スケジュールされたタスクを実行するには、スキャンの実行時にユーザがログオンする必要がありました。また、タスクを設定したユーザがログオンしていないと、スキャンが失敗しました。

現在のリリース

現在のリリースでは、スケジュールされたスキャンに特定のユーザ アカウントを関連付けることができます。スケジュールされた時刻になると、スキャナはこのアカウントを使用して、スキャンを実行します。

利点

- Windows NT および Windows 2000 環境でリモート スキャンがスケジュールできます。
- 現在ログオンしているアカウントを指定することも、スキャン対象のドメインで適切な権限のある別のアカウントを指定することもできます（ePolicy Orchestrator では使用できません)。

操作方法

1. ［**スタート**］>［**プログラム**］>［**Network Associates**］>［**VirusScan コンソール**］の順に選択します。
2. オンデマンド スキャン タスクを選択します。［**マイコンピュータのスキャン**］と［**C: ドライブのスキャン**］がデフォルトのスキャン タスクです。［**タスク プロパティ**］ダイアログ ボックスが開きます。
3. ［**スケジュール**］タブを選択します。
4. ［**詳細設定**］をクリックして［**ログオン アカウント**］ダイアログ ボックスを開きます。

インストール 2

概要

この章では、インストール ウィザードを使用して 1 台のコンピュータに VirusScan バージョン 4.5.1 をインストールする方法を説明します。この章の内容は次のとおりです。

- VirusScan のシステム要件
- 標準インストールとカスタム インストール
- Network Associates アップデート サイトをネットワーク コンピュータ上にミラーリングする機能
- インストール後のコンポーネントの追加と削除
- ワークステーションからの製品の削除
- 前のリリースの VirusScan の設定を保存しておく方法
- コンピュータの再起動が必要な場合

注 : このガイドでは、McAfee ePolicy Orchestrator で VirusScan の配備と設定を行う方法については触れていません。詳細については、『*ePolicy Orchestrator 管理者ガイド*』と『*VirusScan ウイルス対策ソフトウェア v4.5 コンフィグレーションガイド (ePolicy Orchestrator 用)*』を参照してください。これらのマニュアルは製品 CD または McAfee ダウンロード サイトで入手できます。

また、このガイドでは次の情報についても触れていません。詳細については、『*VirusScan v4.5 管理者ガイド*』を参照してください。

- コマンドライン オプションによる製品のインストール
- McAfee Management Edition による製品のインストール
- 次の他社製ユーティリティによる製品のインストール
  - SMS スクリプト
  - Windows NT ログオン スクリプト
  - Tivoli IT Director

> **重要 :** 他社製の製品またはスクリプトで VirusScan をインストールするときに、ミラーリング機能もインストールする方法については、23 ページの「インストールの前に」を参照してください。

- エマージェンシー ディスク作成ユーティリティの使用方法
- インストールのテスト

システム要件

VirusScan は、次の要件を満たす IBM PC または PC 互換のコンピュータにインストールして実行することができます。

- Intel Pentium クラスまたは同等のプロセッサを搭載しているコンピュータ。Intel Pentium プロセッサまたは 166MHz. 以上の Celeron プロセッサをお勧めします。
- CD-ROM ドライブ（CD からプログラムをインストールする場合）
- ソフトウェアのインストール用に 55MB 以上のハードディスク空き容量。インストール後に最適なパフォーマンスを得るには、十分な空き容量が必要です。
- 16 MB 以上の RAM。OS のパフォーマンスを最適にするには、Microsoft 社のガイドラインを参照して、RAM の要件を確認してください。
- Microsoft Windows 95、Windows 98、Windows NT 4.0 SP 4 以降、Windows 2000 Professional、または Windows ME
- Microsoft Internet Explorer v4.0.1 以降

このバージョンの VirusScan は、VirusScan 4.0.3 または 4.0.3a からアップグレードすることができます。4.0.3 より前のバージョンまたは VirusScan TC バージョン 6 からはアップグレードできません。これらのバージョンからアップグレードするには、インストールされているバージョンを削除してから VirusScan 4.5.1 をインストールしてください。

インストールの前に

- このリリースでは、最新の .DAT ファイルのある Network Associates FTP サイトをミラーリングすることができます。詳細については、第 4 章を参照してください。
  - VirusScan を ePolicy Orchestrator でインストールする場合には、デフォルトで Mirror ユーティリティがインストールされます。
  - インストール ウィザードで VirusScan をインストールするときに、ミラーリング機能もインストールする場合には、カスタム インストールを実行して［**Mirror Task**］を選択する必要があります。［カスタム インストール］ページで［**Mirror Task**］を検索するには、ツリー ビューの VirusScan コンソールを展開して、自動アップデートを表示します。［**Mirror Task**］アイコンをクリックして、［**この機能をローカル ハードドライブにインストールする**］を選択します。カスタム インストールの詳細については、27 ページを参照してください。

- VirusScan インストーラには、VirusScan v4.5 や他社製のウイルス対策製品など、コンピュータにインストールされているウイルス対策製品を削除するアンインストール機能が付いています。
  - サイレント モードでインストールすると、このアンインストール機能によって、コンピュータにインストールされているウイルス対策製品がすべて削除されます。
  - SETUP.EXE で製品をインストールする場合には、インストールされているウイルス対策製品が検出されると、システムから削除するかどうかを確認するプロンプトが表示されます。
  - VirusScan 4.0.3 または VirusScan 4.5 がインストールされている場合は、これらの製品の削除に同意しないと、VirusScan 4.5.1 がインストールできません。
  - VirusScan TC の場合には、インストールが失敗します。
  - 弊社以外のウイルス対策製品がインストールされている場合、削除に同意しなくても VirusScan 4.5.1 はインストールされます。ただし、同じシステムに複数のウイルス対策製品が存在してしまうため、致命的な障害が起きる可能性があります。別のウイルス対策製品が存在するシステムに VirusScan 4.5.1 をインストールした場合には、弊社のサポートの対象外になります。
  - VirusScan v5 などのリテール版がインストールされていると、エラーが発生して Dr Watson が起動したり、アンインストールに失敗する場合があります。リテール版の製品は、VirusScan をインストールする前に［**アプリケーションの追加と削除**］機能で削除するようにしてください。
  - ウイルス対策製品が削除されるときには、その製品固有の削除プロセスが実行されます。削除が終了すると、コンピュータが自動的に再起動します。
  - 多くの場合、VirusScan はインストールされている言語に関係なく削除されます。ただし、McAfee and Dr Solomon のバージョン 4.0.1 と 4.0.2 、あるいは他社製品の場合、英語版以外のバージョンは削除されません。
  - 英語以外のバージョンまたはは他社製品がアンインストーラで削除されない場合には、VirusScan 4.5.1 をインストールする前に、［**アプリケーションの追加と削除**］機能を使用して、インストールされている製品を削除するようにしてください。
  - VirusScan 4.5.0 がインストールされている場合には、製品は削除されずにアップグレードされます。
  - VirusScan 4.0.3 の場合には、製品が削除される前に、スキャン設定のコピーが作成されます。インストール プロセスの後半で、いくつかのスキャン設定を保存して、VirusScan 4.5.1 に適用することができます。

- インストールを開始すると、Microsoft Windows Installer（MSI）v1.1 ユーティリティが実行されているかどうかチェックされます。このユーティリティがないと、インストールはできません。Windows 2000 Professional には正しいバージョンの MSI が含まれています。前のバージョンの MSI がコンピュータにインストールされていると、正しいバージョンの MSI が自動的にインストールされます。
- インストール中にコンピュータの再起動が必要になる場合があります。コンピュータの再起動が必要になる状況については、32 ページの「コンピュータの再起動が必要な場合」を参照してください。

ソフトウェアのインストール

1. インストールでのソフトウェアの競合を回避するため、システムで実行されているアプリケーションをすべて終了してください。

   注 : Windows NT Workstation v4.0 または Windows 2000 Professional の場合には、管理者権限が必要です。他のオペレーティング システムの場合には、管理者の認証情報を使用してログオンしてください。

2. 次のいずれかの方法でインストール ウィザードを開始します。

   CD から :

   a. コンピュータの CD-ROM ドライブに CD を挿入します。

   b. ［**McAfee VirusScan インストール**］ウィンドウが表示されたら、［**インストール**］をクリックして、インストールを開始します。

      ［**McAfee VirusScan インストール**］ウィンドウが表示されない場合には、CD の SETUP.EXE をダブルクリックします。

   ダウンロードした ZIP アーカイブから :

   a. ハードディスク上に一時フォルダを作成します。

   b. WinZip、PKZIP、などのユーティリティを使用して、VirusScan インストール ファイルを一時フォルダに解凍します。

   c. 一時フォルダにある SETUP.EXE をダブルクリックして、インストール ウィザードを開始します。

3. インストール ユーティリティが製品情報、リリース ガイド、README.TXT ファイルを表示します。この README.TXT には、機能の紹介、このバージョンの VirusScan での既知の問題が記載されています。［**次へ >**］をクリックして、使用許諾契約を表示します。

4. 使用許諾契約をよく読んでください。VirusScan をインストールするには、使用許諾契約に同意する必要があります。[**ライセンス契約に同意します**] を選択し、[**次へ >**] をクリックして次に進みます。

   - 前のバージョンがインストールされていなければ、[**セキュリティ レベルを選択してください**] ウィンドウが開きます。手順 6 に進んでください。
   - VirusScan 4.5 または VirusScan 4.0.3 がインストールされていると、[**以前のバージョンが見つかりました**] ウィンドウが開きます。ここで、前の製品の設定を保存することができます。詳細については、31 ページの「設定の保存」を参照してください。

5. [**次へ >**] をクリックして、先に進みます。Windows NT または Windows 2000 を使用している場合には、[**セキュリティ レベルを選択してください**] ウィンドウが開きます。
6. インストール後に VirusScan に適用されるセキュリティ レベルを選択します。

   - [**標準のセキュリティ レベル**] を選択すると、ログオンしているすべてのユーザが、タスクの開始、停止、設定、定義を行うことができます。
   - [**高度なセキュリティ レベル**] を選択すると、管理者権限のあるユーザしかこれらのアクションを実行することができません。

   オプションを選択したら [**次へ >**] をクリックして、[**インストールの種類**] ウィンドウを開きます。

7. インストールの種類を選択します。

   - [**標準インストール**] を選択して [**次へ >**] をクリックすると、次の機能がインストールされます。
     - VirusScan（オンデマンド スキャン）コンポーネントとアプリケーションの拡張機能。ハードディスク上のオブジェクトを右クリックして、スキャンを開始することができます。
     - VirusScan コンソール。すべてのコンポーネントの設定ユーティリティが実行できます。
     - VShield システム スキャン（オンアクセス スキャン）モジュール .
     - E-Mail スキャン。メール メッセージと添付ファイルをスキャンします。
     - インターネット スキャン。ダウンロード スキャン（悪意のある Java アプレットや ActiveX コントロールから保護します）とインターネット フィルター（危険なインターネット サイトへのアクセスをブロックします）の 2 つのモジュールがあります。

– ウイルス送信ユーティリティ。解析のため、感染の疑いのあるファイルを McAfee A.V.E.R.T（Anti-Virus Emergency Response Team）に送信できます。

– VirusScan コマンドライン スキャナ。MS-DOS プロンプト、［**コマンド プロンプト**］ウィンドウ、MS-DOS 保護モードでスキャンを実行するスキャナです。

注 : VirusScan コンポーネントの詳細については、『*VirusScan 4.5 ユーザーズ ガイド*』の「VirusScan を構成するコンポーネント」を参照してください。

- ［**カスタム インストール**］を選択して［**次へ >**］をクリックすると、［**カスタム インストール**］ウィンドウが開きます（図 2-1）。

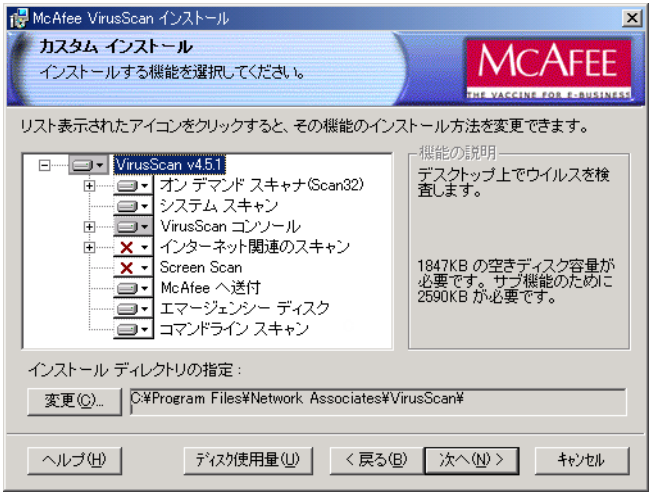

図 2-1. インストール ウィザード（［カスタム インストール］ウィンドウ）

［**カスタム インストール**］ウィンドウでは、インストールしないコンポーネントを選択したり、Mirror ユーティリティを追加することができます。このユーティリティを使用すると、Network Associates FTP サイトのミラーリングを行うことができます。また、このウィンドウでは、スクリーン セーバーの起動時にスキャンを実行するスクリーン スキャンを追加したり、エマージェンシー ディスク ユーティリティが追加できます。このユーティリティは、ウィルスに感染していない環境でコンピュータを起動するためのフロッピー ディスクを作成します。

a. 追加または除外するコンポーネントを指定します。

- コンポーネントを追加するには、名前の横の  をクリックして、次の項目を選択します。
  この機能をローカル ハードディスクにインストールします
- コンポーネントとそれに関連するすべてのモジュールをインストールするには、次の項目を選択します。
  この機能とすべてのサブ機能をローカル ハードディスクにインストールします
  このオプションは、コンポーネントに関連するモジュールがある場合に使用できます。
- コンポーネントを削除するには、名前の横の  をクリックして、次の項目を選択します。
  インストールしません

注 : VirusScan セットアップ ユーティリティでは、上の項目以外のメニューはサポートしていません。VirusScan コンポーネントはネットワーク経由では実行できません。また、VirusScan には、必要なときにインストールできるコンポーネントはありません。

b. インストール先に別のディスクやディレクトリを指定することができます。[**変更**] をクリックして、使用するドライブまたはディレクトリを指定します。

c. [**ディスク使用量**] をクリックすると、ローカル ディスクの空き容量と VirusScan に必要な容量が表示されます。空き容量の少ないドライブは強調表示されます。

8. 選択が完了したら、[**次へ >**] をクリックして [**インストール**] を選択し、ファイルのコピーを開始します。

9. インストールが完了したら、[**McAfee VirusScan 設定**] ウィンドウで選択を行います。次のいずれかを選択します。

   - **起動時にブート レコードをスキャン**
     Windows 95 または Windows 98 の場合、これを選択すると、システムの起動時にディスクのブートセクタがスキャンされるように、AUTOEXEC.BAT ファイルが修正されます。
   - **エマージェンシー ディスクを作成**
     カスタム インストールで [**エマージェンシー ディスクを作成**] を選択すると、インストールの完了時にエマージェンシー ディスクが作成できます。

- **インストール後にデフォルトのウイルス検査を実行**
  インストールの完了後、オンデマンド スキャナがローカル ドライブ上のファイルをスキャンします。

10. 選択が終了したら、[**次へ >**] をクリックします。スキャナがシステム メモリを自動的に検査し、[**ウイルス定義ファイルのアップデート**] ウィンドウが開きます。
11. アップデート オプションを選択します。

    - **自動アップデートを今すぐ実行**。このオプションを選択すると、自動アップデートのデフォルトの設定に従って、Network Associates FTP サイトから最新の差分 .DAT ファイルがダウンロードされます。アップデート サイトをネットワーク上に設定していない場合や、プロキシ サーバの設定を行う必要がない場合には、このオプションを選択してください。これにより、最新の .DAT ファイルでスキャンを実行することができます。

      このオプションを選択して [**次へ >**] をクリックすると、自動アップデートが開始し、必要に応じて .DAT ファイルがアップデートされます。

    - **自動アップデートを今すぐ設定**。このオプションを選択すると、[自動アップデート] ダイアログボックスが開き、ファイルをダウンロードするアップデート サイトを追加したり、設定することができます。ネットワーク上のサーバから最新の .DAT ファイルをダウンロードする場合や、McAfee Web サイトへのアクセス方法を変更する場合（ファイアウォールやプロキシ サーバの設定）には、このオプションを選択してください。

      このオプションを選択して [**次へ**] をクリックすると、[自動アップデート] ページが表示されます。自動アップデートの設定方法については、第 3 章、「.DAT ファイルのアップデート」の 35 ページ以降を参照してください。

    - **後でアップデート**。このオプションを選択すると、アップデート操作がスキップされます。最新の .DAT ファイルを後でダウンロードするように自動アップデートを設定し、スケジュールすることができます。タスクのスケジュール方法については、『*VirusScan v4.5 ユーザーズ ガイド*』の第 6 章、「スケジュール タスクの作成と設定」を参照してください。

12. [**次へ >**] をクリックすると、インストールの最後のウィンドウが表示されます。インストールが完了すると、VirusScan が自動的に開始します。

ソフトウェアの変更と削除

VirusScan が使用しているバージョンの Microsoft Windows Installer では、ローカル ワークステーションにインストールされた VirusScan の変更と削除が実行できます。

VirusScan の変更や削除を行うには、次の手順に従ってください。

1. ［**スタート**］メニューの［**設定**］から［**コントロール パネル**］を選択します。
2. ［**アプリケーションの追加と削除**］をダブルクリックします。
3. リストから **"McAfee VirusScan"** を選択して［**追加と削除**］をクリックします。ウィザードが起動します。

   注 : Windows 2000 Professional の場合には、プログラムの追加と削除に別々のボタンが用意されています。［**削除**］を選択すると、プログラムの削除がすぐに開始します。

4. ［**次へ >**］をクリックします。［**プログラムのメンテナンス**］ウィンドウで、次のいずれかのオプションを選択します。
   - ［**変更**］。VirusScan コンポーネントを個別に追加または削除します。［カスタム インストール］ウィンドウが開き、追加または削除するコンポーネントを選択することができます。
   - ［**削除**］。コンピュータから完全に削除します。

設定の保存

インストールで VirusScan 4.0.3 が検出されると、［**以前のバージョンが見つかりました**］ウィンドウが表示されます。ここで、前のバージョンの設定を保存することができます。保存できる設定は次のとおりです。

結果	バージョン 4.0.3 の設定	バージョン 4.5 の設定
保存	オンアクセス スキャンの設定 **注 :** これらの設定は保存され、VirusScan 4.5.1 システム スキャン モジュールで使用されますが、他のモジュールには適用されません。	• ユーザが指定したスキャン対象の拡張子リスト • オンデマンド スキャンの設定 • オンアクセス スキャンの設定 • 定義されたスキャン タスク • アラート オプション
保存されない	• 製造元が設定したスキャン対象の拡張子リスト • ユーザが指定したログ ファイルの名前またはパス名 • ユーザが指定したインストール場所 • アップデートまたはアップグレードで使用される URL または FTP • アラート オプション • オンデマンド スキャンの設定 • 定義されたスキャン タスク	• 製造元が設定したスキャン対象の拡張子リスト • ユーザが指定したログ ファイルの名前またはパス名 • ユーザが指定したインストール場所 • アップデートまたはアップグレードで使用される URL または FTP

コンピュータの再起動が必要な場合

通常、このリリースの VirusScan はインストール後すぐに使用することができます。コンピュータの再起動は必要ありません。ただし、Microsoft Installer（MSI）がファイルの置換や初期化を必要としたり、インストールされている前のバージョンの McAfee 製品を削除しないと VirusScan が正常に実行できない場合があります。この要件は、サポートされる Windows プラットフォームによって異なります。このような場合、インストール中またはインストール後にシステムの再起動が要求されます（MSI ファイルがインストールされた場合には、インストール中に要求されます）。

- ヒント：再起動が必要になると、次のレジストリ キーに値 “1” が設定されます。

```
HKEY_LOCAL_MACHINE
  SOFTWARE
    Network Associates
      TVD
        VirusScan
           RebootNeeded
```

コンピュータの再起動が必要になる場合は次のとおりです。

状況	Windows 95/98/ME	Windows NT/2000
前のバージョンの VirusScan と互換性のない製品は、コンピュータにインストールされていない	Novell Client32 for NetWare がインストールされていなければ、再起動は不要です。	再起動が必要
前のバージョンの VirusScan がコンピュータにインストールされている	再起動が必要	再起動が必要
互換性のない製品がコンピュータにインストールされている	再起動が必要であれば、プロンプトが表示されます。	再起動が必要であれば、プロンプトが表示されます。
Microsoft Installer（MSI）v1.0 がコンピュータにインストールされている	MSI ファイルがインストールされると再起動が要求されます。再起動後、インストールが継続します。	MSI ファイルがインストールされると再起動が要求されます。再起動後、インストールが継続します。
Microsoft Installer v1.11 がコンピュータにインストールされている	Windows 98 SE またはドライバか .DLL ファイルが使用されている場合を除いて、再起動は不要です。	再起動は不要です。
DAT ファイル アップデート	再起動は不要です。	再起動は不要です。

状況	Windows 95/98/ME	Windows NT/2000
McAfee SuperDAT ユーティリティによるスキャン エンジンのアップデート	再起動は不要です。	再起動は不要です。
次のレジストリ キーが Windows NT システムに存在しない HKLM\SYSTEM\CurrentControlSet\Services\NaiFiltr	N/A	Windows NT の場合には再起動が必要 Windows 2000 には適用されません

* 通常、再起動は VirusScan バージョン 4.0.1、4.0.2、4.0.3 の削除後や MSI 1.0 のインストール後に要求されますが、コマンドラインからインストールする場合に、次のプロパティを使用すると、再起動をしないように設定することができます。

```
FORCEINSTALL = True
```

コマンドライン オプションを使用した VirusScan のインストール方法については、『VirusScan 4.5.0 *管理者ガイド*』を参照してください。

.DAT ファイルのアップデート 3

概要

この章では、ネットワーク経由で最新のウイルス定義ファイル（.DAT ファイル）をコンピュータにダウンロードする方法の変更点について説明します。一般に、この設定手順は、Windows Server のネイティブ環境または ePolicy Orchestrator 環境のインタフェースを使用する場合に適用されます。ただし、ePolicy Orchestrator 環境には、［**参照**］または［**デフォルト**］ボタンに関する記述は適用されません。

注 : この章の内容は、VirusScan バージョン 4.5 マニュアルの次のセクションにある手順を改訂したものです。

- 『*ユーザーズ ガイド*』の第 7 章、「DAT の自動アップデートの理解」と「DAT の自動アップデートの設定」
- 『*管理者ガイド*』の第 6 章、「DAT の自動アップデートの理解」と「DAT の自動アップデートの設定」
- 『*コンフィグレーション ガイド（ePolicy Orchestrator 用）*』の第 9 章、「ウイルス定義ファイルのアップデート」と「アップデート オプションの詳細設定」

ウイルス定義ファイルは Network Associates FTP サイト（ftp.nai.com/virusdefs/4.x）にあります。このサイトには、3 種類の .DAT ファイルが用意されています。

- **通常の .DAT ファイル**。DAT-XXXX.ZIP（または DAT-XXXX.TAR）というラベルが付いています。XXXX は .DAT ファイルのバージョンです。
- **SuperDAT ファイル**。SDATXXXX.EXE というラベルが付いています。SuperDAT は .DAT ファイルを XXXX というバージョンの .DAT ファイルにアップデートするユーティリティです。現在使用しているスキャン エンジンよりも新しいエンジンが Network Associates サイトにある場合には、スキャン エンジンもアップグレードされます。
- **差分 .DAT ファイル**。XXXXXXXX.UPD というラベルが付いています。差分 .DAT ファイルは、現在使用されている .DAT ファイルが提供されてから最新の .DAT ファイルが提供されるまでのファイルです。最初の 4 桁の X は現在コンピュータで使用されている .DAT のバージョンを表します。次の 4 桁の X は、最新の .DAT ファイルのバージョンを表します。

FTP サイトにも 2 つの *.INI ファイルがあります。自動アップデートは、これらのファイルを参照し、アップデートが必要な範囲と、コンピュータの自動アップデートの設定に基づいて、有効なアップデート パターンを選択します。次のアップデート パターンがあります。

- スキャン エンジンはアップグレードせずに、使用中の .DAT ファイルをすべて置換する
- すべての .DAT ファイルを置換し、スキャン エンジンもアップグレードする
- 最新の状態にするために必要な差分変更のみを組み込む

次の *.INI ファイルがあります。

- **UPDATE.INI**。Network Associates FTP サイトで利用できる最新の .DAT ファイルとスキャン エンジンが記述されています。自動アップデートは、このファイルを参照して、アップデートの対象と使用可能なファイルを識別します。
- **DELTA.INI**。使用中のファイルを最新の状態にするために必要な差分 .DAT ファイルが記述されています。

.DAT の自動アップデート ユーティリティは、必要なファイルをダウンロードし、オンアクセス スキャナを停止して最新のファイルをインストールします。インストール後、オンアクセス スキャナが再開し、スキャナは最新のファイルを使用します。

このリリースでは、Network Associates FTP サイトのミラーリングを行うインタフェースが追加されました。このミラーリング機能については、第 4 章、「Network Associates アップデート サイトのミラーリング」の 47 ページ以降を参照してください。

ネットワーク上に Mirror サイトを作成するには、次の操作が必要になります。

- 自動アップデートとミラーリング タスクを**設定**します。タスクの設定順序は重要ではありません。
- 適切な時間帯に自動アップデートとミラーリングが実行されるように、**スケジュール**します。自動アップデートで最新の .DAT ファイルが選択されるようにするには、*ミラーリングを先に実行し、その完了後に自動アップデートを実行するようにし*てください。

自動アップデートの設定

自動アップデートの設定には 4 つのプロセスがあります。

- 「自動アップデートの開始」。詳細については、以下の情報を参照してください。
- 「アップデート サイトの定義」。詳細については、39 ページを参照してください。
- 「アップデートの詳細設定オプションの選択」。詳細については、44 ページを参照してください。
- 「アップデートの記録」。詳細については、45 ページを参照してください。

---

ePolicy Orchestrator ユーザへの注： アップデート、アップグレード、または Mirror タスクを設定して ePolicy Orchestrator で配備するときに、配備先のワークステーションに同じタスクの設定があると、古い設定は上書きされます。たとえば、自動アップグレード、自動アップデート、または Mirror タスクを定期的に実行するように設定して、すぐに実行するアップデート、アップグレード、または Mirror タスクを設定して配備すると（または前のタスクと異なる優先順位を設定して配備すると）、クライアント マシンにある古い設定は新しい設定で上書きされます。古い設定を復元するには、そのタスクを再度設定して配備する必要があります。

自動アップデートの開始

［**自動アップデート**］ページは、VirusScan コンソールまたは ePolicy Orchestrator のどちらを使用しても表示することができます。外観は異なりますが、同じ機能が実行できます。

VirusScan コンソールから表示する場合

1. ［**スタート**］メニューから VirusScan コンソールを起動します。
2. ［**.DAT の自動アップデート**］をダブルクリックして、［**タスク プロパティ**］ダイアログ ボックスを開きます。
3. ［**設定**］をクリックして、［**自動アップデート**］ページ（38 ページの図 3-1）を開きます。

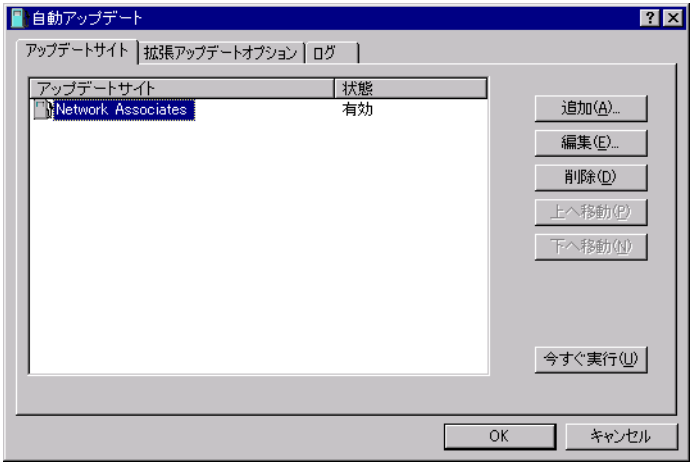

図 3-1. 自動アップデート（[アップデートサイト] タブ）

ePolicy Orchestrator を使用する場合

1. 上部詳細ペインで［**VirusScan 4.5.1 設定**］を選択します。
2. ePolicy Orchestrator ディレクトリ ツリーで、アップデート タスクを設定する対象を選択します。
3. ディレクトリ ツリーで対象を右クリックして、［**タスクのスケジュール**］を選択し、スケジューラを開きます。
4. ［**タスク**］タブを選択して、設定するアクティビティを定義します。
5. ［**名前**］フィールドに、作成するアップデート タスクの名前を入力します。
6. ［**ソフトウェア**］フィールドで、タスクを設定するソフトウェアを選択します。
7. ［**タスクの種類**］フィールドで、［**VirusScan 4.5.1 自動アップデート**］を選択して、［**設定**］をクリックし、［**自動アップデート**］ページを開きます。

アップデート サイトの定義

.DAT ファイルとスキャン エンジンをダウンロード元は、最大 16 まで指定することができます。

1. ［**追加**］をクリックして、［**サイト オプション**］ページ（図 3-2）を開きます。

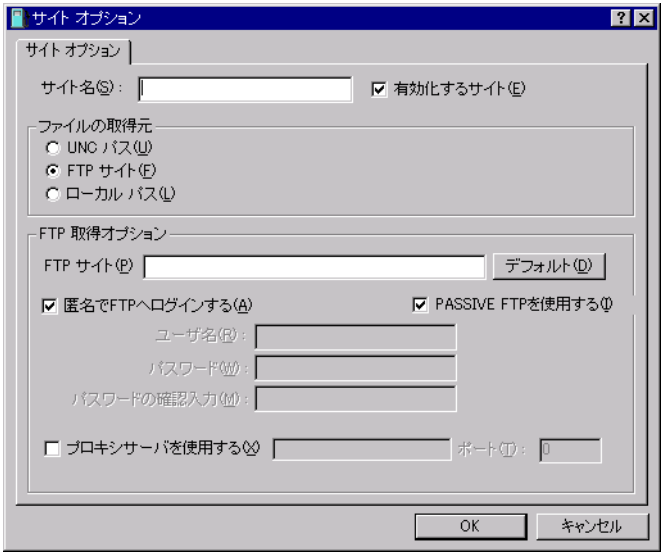

図 3-2. 自動アップデート（サイト オプション）

2. ファイルの取得方法を選択します。詳細については、次のページを参照してください。

   - 「FTP サイトの設定」の 40 ページ以降
   - 「UNC パスの設定」の 42 ページ以降
   - 43 ページの「ローカル パスの設定」

自動アップデートを実行すると、[**アップデート サイト**] ページに表示される順序でサイトがアクセスされます。

重要 : 通常、リストに表示されるアップデート サイトは Network Associates FTP サイトのレプリカになります。このレプリカはミラーリング機能で作成できます。この機能を使用すると、ミラー ユーティリティで指定した場所からサーバにファイルをダウンロードすることができます。この機能の概要については第 4 章、「Network Associates アップデート サイトのミラーリング」を、詳細については 53 ページの手順 1 を参照してください。

FTP サイトの設定

1. 定義するサイトの名前を入力し、[**有効化するサイト**] をオンにします。
2. FTP サーバの名前とファイルを保存するディレクトリの名前を入力します。
   - デフォルトでは、Network Associates FTP ダウンロード サイトが選択されています。
   - 会社のネットワークなど、別の FTP サイトを使用するには、そのサイトの URL を入力します。たとえば、`ftp.myserver/install` と入力します。
   - ダウンロード元を Network Associates FTP サイトに戻すには、[**デフォルト**] をクリックします。
3. ユーザの認証情報を入力します。
   - FTP サイトで匿名ログインが許可されている場合には（Network Associates FTP サイトなど）、[**匿名で FTP にログインする**] をクリックします。
   - FTP サイトでログイン認証が必要な場合には、[**匿名で FTP にログインする**] をオフにして、サーバ アクセスに必要な**ユーザ名**と**パスワード**を入力します。入力したパスワードは、8 つのアスタリスクで表示されます。
4. passive FTP または active FTP を選択します。
   - デフォルトは passive FTP です。この FTP では、クライアントがコマンド セッションとデータ セッションの両方を開始します。したがって、active FTP とは異なり、ファイアウォールが転送に介入しません。
   - active FTP 接続を使用するには、このチェックボックスをオフにします。

5. プロキシ情報を指定します。

   - プロキシ サーバが必要なネットワークの場合には［**プロキシ サーバを使用する**］をオンにして、プロキシ サーバの名前とポート番号を入力します。
   - プロキシ ソフトウェアを使用する場合には、最新のバージョン（サービスパックも含む）を使用してください。

6. 設定が完了したら［**OK**］をクリックします。

UNC パスの設定

1. 定義するサイトの名前を入力し、［**有効化するサイト**］をオンにします。
2. UNC の表記法（¥¥servername¥path）に従って、アップデート サイトのパス名を入力するか、［**参照**］をクリックして、ネットワーク上の共有ファイルを指定します。
3. ユーザの認証情報を入力します。
   - デフォルトでは、UNC サイトへのアクセスには、現在ログオンしているユーザのアカウントが使用されます。
   - UNC サイトが NullSessionShare の場合には、現在ログオンしているすべてのユーザがそのサイトにアクセスできます。NullSessionShare については、43 ページの「**重要**」を参照してください。
   - UNC サイトへのアクセスに特別な権限が必要な場合には、その権限のあるユーザ アカウントを使用してください。Windows 95 および Windows 98 では、現在ログオンしているユーザに共有フォルダに対する “ 読み取り ” 権限が必要です。
   - アップデートの実行時に指定したユーザがログオンしていないと、**ローカル システム アカウント**で自動アップデートが実行されます。UNC 共有フォルダが NullSessionShare でなければ、アップデートは失敗します。NullSessionShare については、43 ページの「**重要**」を参照してください。
4. 設定が完了したら［**OK**］をクリックします。

ローカル パスの設定

1. 定義するサイトの名前を入力し、［**有効化するサイト**］をオンにします。
2. ローカル フォルダのパス（たとえば C:¥DATS¥）を入力するか、［**参照**］をクリックしてアップデート ファイルの保存先を選択します。
3. 設定が完了したら［**OK**］をクリックします。

重要 : NullSessionShare の使用方法

アクセス時にログインの認証情報が不要な共有フォルダにアップデート ファイルを置く場合には、ネットワーク セキュリティを維持できるように十分に配慮する必要があります。共有フォルダは NullSessionShare と指定してください。ネットワーク上に NullSessionShare を作成する方法については、他のマニュアルを参照してください。

結果的に NullSessionShare がセキュリティ ホールになる可能性があるため、Windows NTFS システムにある次のセキュリティ機能を使用するようにしてください。

- クライアントには共有フォルダに対する “読み取り” と “検索” 権限のみを許可する。
- 共有フォルダのあるサーバには、“ 書き込み ” 権限を許可する。
- 共有フォルダで受け入れ可能なメッセージ数を設定する。
- NTFS 監査機能を使用する。

アップデートの詳細設定オプションの選択

アップデートにはいくつかの詳細設定があります。

1. ［**拡張アップデート オプション**］タブ（図 3-3）で詳細設定オプションを指定します。

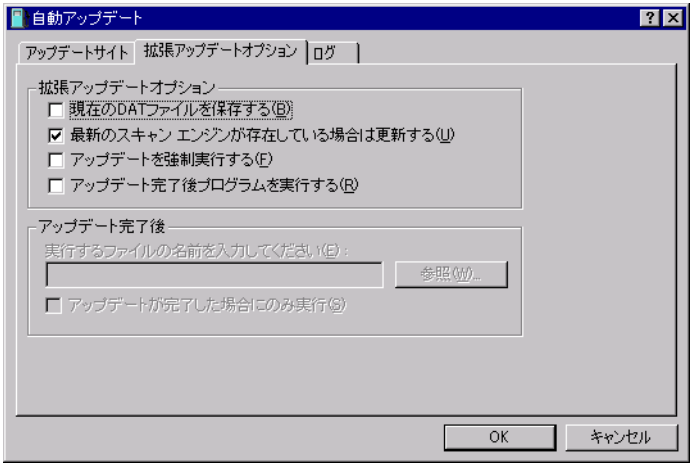

図 3-3. 自動アップデート
（[拡張アップデート オプション］ タブ）

2. 次のいずれかの機能を選択します。

   - **現在の .DAT ファイルを保存する。**現在使用中の .DAT ファイルの拡張子を **.SAV** に変更してから、新規ファイルをインストールします。
   - **最新のスキャン エンジンが存在している場合は更新する。**最新のスキャン エンジンがある場合には、既存のスキャン エンジンと置換します。
   - **アップデートを強制実行する。**このチェックボックスは、次の場合にオンにします。
     - 現在の .DAT ファイルを前のバージョンに戻す場合。新しい .DAT ファイルが正常に機能しない場合に、一時的な処置としてこのアクションを実行することができます。
     - 特定のワークステーションにある最新の .DAT ファイルが壊れていたり、CLEAN.DAT など必要なファイルが削除されたために正常に動作しない場合。

ヒント : エンジンはアップグレードせずに .DAT ファイルだけを強制的にアップデートするには、［**アップデートを強制実行する**］をオンにして、［**最新のスキャン エンジンが存在している場合は更新する**］をオフにします。

- **アップデート完了後プログラムを実行する。**自動アップデートの終了後に別のプログラムを開始します。
  - 実行するプログラムのパス名を入力するか、［参照］をクリックしてプログラムを検索します。
  - アップデートに失敗したときにプログラムを実行しないようにするには、［**アップデートが完了した場合にのみ実行**］をオンにします。

重要 : 現在ログオンしているユーザが実行できないプログラムは指定できません。現在ログオンしているユーザがプログラム ファイルのあるフォルダにアクセスできない場合や、ログオンしているユーザがいない場合には、プログラムは実行されません。

アップデートの記録

アップデート イベントを記録するログ ファイルをセットアップすることができます。

1. ［**ログ**］タブ（図 3-4）でロギング機能を設定します。

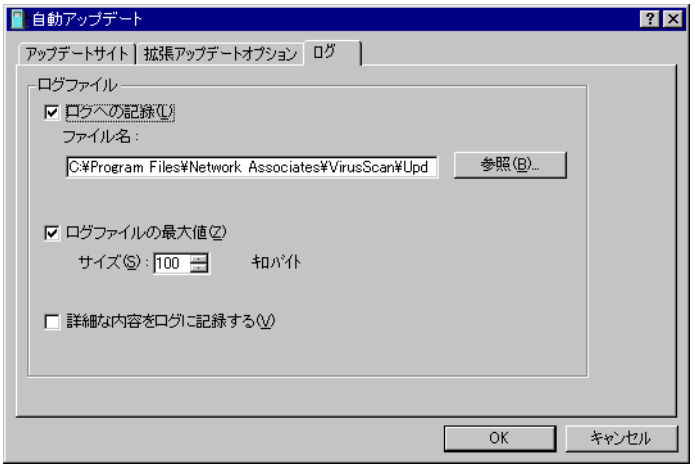

図 3-4. 自動アップデート（[ログ] タブ）

2. ［**ログへの記録**］が選択され、ロギング機能が有効になっているかどうか確認します。
   - ログ ファイルの名前は UPDATE.TXT です。デフォルトのパスは次のとおりです。

     ```
     <drive>:¥Program Files¥Network
     Associates¥VirusScan¥
     ```

   - 必要であれば、別の名前またはパスが入力できます。
3. ログ ファイルのサイズを指定します。
   - ログ ファイルの最大サイズは 999 KB です。10KB から 999KB までの値を入力してください。
   - ログ ファイルのデータが、ログ ファイルに設定した制限を超えると、新しい情報を記録するため、古い順から 20% のログ テキストが削除されます。ログ ファイルのサイズに制限を設定しないと、ログ ファイルの存在するドライブのすべての空き容量を使用してしまう危険性があります。
4. ロギングの範囲を指定します。
   - ［**詳細な内容をログに記録する**］をオンにすると、操作の詳細が記録されます。
   - タスクの開始と終了だけを記録するには、このチェックボックスをオフにします。
5. ログ オプションの設定が完了したら［**OK**］をクリックします。

Network Associates アップデート サイトのミラーリング 4

概要

この章では、Network Associates FTP アップデート サイトのミラー イメージを社内のネットワーク内に作成する方法について説明します。この機能は、このリリースで追加された機能です。一般に、Mirror サイトのセットアップは、ネットワーク管理者の責任で行われます。エンドユーザは自動アップデートの設定は行いますが、通常、ミラーリング タスクの設定は行いません。

一般に、この設定手順は、Windows Server のネイティブ環境または ePolicy Orchestrator 環境のインタフェースを使用する場合に適用されます。ただし、ePolicy Orchestrator 環境では、［**参照**］または［**デフォルト**］ボタンに関する記述は適用されません。

重要 : ミラーリング機能を使用する場合には、セットアップ ウィザードで VirusScan をインストールするときにカスタム インストールを実行してください。カスタム インストールで［**Mirror Task**］を選択するには、ツリー ビューの VirsuScan コンソールを展開して、自動アップデートを表示します。［**Mirror Task**］アイコンをクリックして、［**この機能をローカルハードドライブにインストールします**］を選択します。カスタム インストールの詳細については、27 ページを参照してください。

各コンピュータが自由にインターネットにアクセスできるような比較的小規模なネットワーク環境では、各コンピュータから Network Associates FTP サイトに直接アクセスして、アップデート ファイルを取得することができます。しかし、インターネットにアクセスできないコンピュータがある場合、このような方法は*現実的ではありません*。また、多くのコンピュータがリモートの外部ソース（Network Associates FTP サイトなど）からファイルをダウンロードするような環境では、*効率的ではありません*。

このリリースの VirusScan では、比較的規模の大きいネットワーク環境（ePolicy Orchestrator で管理されるネットワークも含む）向けの機能が搭載されています。この機能を使用すると、企業のネットワーク上に 1 つ以上のサイトが作成できます。各サイトが、.DAT ファイルのある Network Associates FTP サイトのレプリカになります。これにより、ネットワーク上のコンピュータから Mirror サイトにアクセスしてファイルをダウンロードすること

ができます。この方法では、コンピュータがインターネットにアクセス可能かどうかに関係なく、ネットワーク上のコンピュータをアップデートすることができます。また、Network Associates FTP サーバよりも近くにあるサーバにアクセスすることで、アクセス時間やダウンロード時間を短縮することができます。

Mirror ユーティリティは、以前に自動アップデートで選択できた［**後で使用するためにアップデート ファイルを保存する**］オプションと同じ機能が実行できます。

ネットワーク上に Mirror サイトを作成するには、次の操作が必要になります。

- 自動アップデートとミラーリング タスクを設定します。タスクの設定順序は重要ではありません。
- 適切な時間帯に自動アップデートとミラーリングが実行されるようにスケジュールします。自動アップデートで最新の .DAT ファイルが選択されるようにするには、*ミラーリングを先に実行し、その完了後に自動アップデートを実行するようにしてください。*

ミラーリングの設定

ミラーリングの設定には 4 つのプロセスがあります。

- 「Mirror ユーティリティの開始」詳細については、以下の情報を参照してください。
- 「Mirror サイトの定義」。詳細については、50 ページを参照してください。
- 「宛先フォルダの定義」。詳細については、53 ページを参照してください。
- 「ミラーリングの記録」。詳細については、54 ページを参照してください。

注 : McAfee ePolicy Orchestrator でミラーリングを設定する方法については、37 ページの「注」を参照してください。

Mirror ユーティリティの開始

［**VirusScan Mirror サイト**］ページは VirusScan コンソールまたは ePolicy Orchestrator のいずれかから表示することができます。外観は異なりますが、どちらからページを表示しても、同じ機能が実行できます。

VirusScan コンソールから表示する場合

1. ［**スタート**］メニューから VirusScan コンソールを起動します。
2. ［**Mirror**］をダブルクリックして、［**タスク プロパティ**］ダイアログ ボックスを開きます。
3. ［**設定**］をクリックして、［**VirusScan Mirror サイト**］ページ（図 4-1）を開きます。

図 4-1. ミラーリング（[ソースサイト］タブ）

ePolicy Orchestrator を使用する場合

1. 上部詳細ペインで［**VirusScan 4.5.1 設定**］を選択します。
2. ePolicy Orchestrator ディレクトリ ツリーで、ミラーリング タスクを設定する対象を選択します。
3. ディレクトリ ツリーで対象を右クリックして、［**タスクのスケジュール**］を選択し、［**スケジューラ**］ダイアログボックスを開きます。
4. ［**タスク**］タブを選択して、設定するアクティビティを定義します。
5. ［**名前**］フィールドに、作成するミラーリング タスクの名前を入力します。

6. ［**ソフトウェア**］フィールドで、タスクを設定するソフトウェアを選択します。
7. ［**タスクの種類**］フィールドで、［**VirusScan 4.5.1 モニタ**］を選択して、［**設定**］をクリックし、［Mirror］ページを開きます。

Mirror サイトの定義

.DAT ファイルとスキャン エンジンをダウンロードする Mirror サイトは、最大 16 まで指定することができます。

1. ［**追加**］をクリックします。［**サイト オプション**］ページ（図 4-2）が開きます。

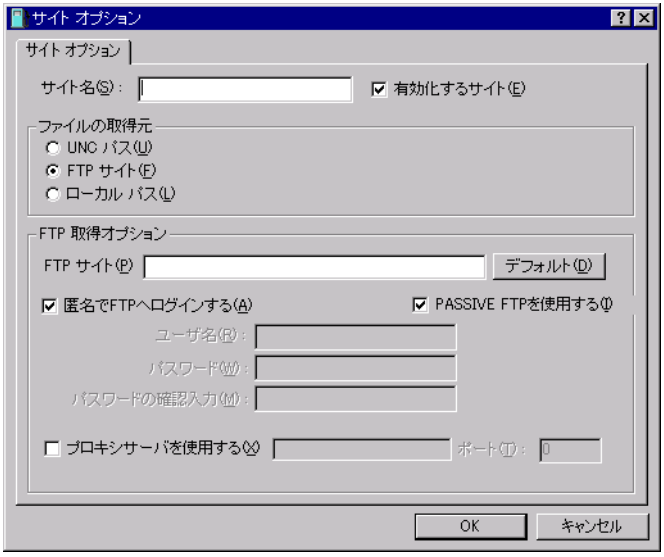

図 4-2. ミラーリング（サイト オプション）

2. ファイルの取得方法を選択します。詳細については、次のページを参照してください。
   - 「FTP サイトの設定」（51 ページ以降）
   - 「UNC パスの設定」（52 ページ以降）
   - 「ローカル パスの設定」（52 ページ）

   ミラーリングを実行すると、［**VirusScan Mirror サイト**］ページに表示される順序でサイトがアクセスされます。

FTP サイトの設定

1. 定義するサイトの名前を入力し、［**有効化するサイト**］をオンにします。
2. FTP サーバの名前とファイルを保存するディレクトリの名前を入力します。
   - デフォルトでは、Network Associates FTP ダウンロード サイトが選択されています。
   - 会社のネットワークなど、別の FTP サイトを使用するには、そのサイトの URL を入力します。たとえば、`ftp.myserver/install` と入力します。
   - ダウンロード元を Network Associates FTP サイトに戻すには、［**デフォルト**］をクリックします。
3. ユーザの認証情報を入力します。
   - FTP サイトで匿名ログインが許可されている場合には（NAI FTP サイトなど）、［**匿名で FTP へログインする**］をクリックします。
   - FTP サイトでログイン認証が必要な場合には、［**匿名で FTP へログインする**］をオフにして、サーバ アクセスに必要な**ユーザ名**と**パスワード**を入力します。入力したパスワードは、8 つのアスタリスクで表示されます。
4. passive FTP または active FTP を選択します。
   - デフォルトは passive FTP です。この FTP では、クライアントがコマンド セッションとデータ セッションの両方を開始します。したがって、active FTP とは異なり、ファイアウォールが転送に介入しません。
   - active FTP 接続を使用するには、このチェックボックスをオフにします。
5. プロキシ情報を指定します。
   - プロキシ サーバが必要なネットワークの場合には［**プロキシ サーバを使用する**］をオンにして、プロキシ サーバの名前とポート番号を入力します。
   - プロキシ ソフトウェアを使用する場合には、最新のバージョン（サービスパックも含む）を使用してください。
6. 設定が完了したら［**OK**］をクリックします。

UNC パスの設定

1. 定義するサイトの名前を入力し、［**有効化するサイト**］をオンにします。
2. UNC の表記法（¥¥servername¥path）に従って、アップデート ファイルのサイトのパス名を入力するか、［**参照**］をクリックして、ネットワーク上の共有ファイルを指定します。
3. ユーザの認証情報を入力します。
   - デフォルトでは、UNC サイトへのアクセスには、現在ログオンしているユーザ アカウントが使用されます。
   - UNC サイトが NullSessionShares の場合には、現在ログオンしているすべてのユーザがそのサイトにアクセスできます。NullSessionShares については、47 ページの「**重要**」を参照してください。
   - UNC サイトへのアクセスに特別な権限が必要な場合には、その権限のあるユーザ アカウントを使用してください。Windows 95 および Windows 98 では、現在ログオンしているユーザに共有フォルダに対する “ 読み取り ” 権限が必要です。
   - ミラーリングの実行時に、指定したユーザがログオンしていないと、**ローカル システム アカウント**でミラーリングが実行されます。UNC 共有フォルダが NullSessionShares でなければ、ミラーリングは失敗します。NullSessionShares については、47 ページの「**重要**」を参照してください。
4. 設定が完了したら［**OK**］をクリックします。

ローカル パスの設定

1. 定義するサイトの名前を入力し、［**有効化するサイト**］をオフにします。
2. ローカル フォルダのパス（たとえば C:¥DATS¥）を入力するか、［**参照**］をクリックしてアップデート ファイルを保存する場所を選択します。
3. 選択が完了したら［**OK**］をクリックします。

宛先フォルダの定義

アップデート ファイルのあるフォルダのローカル パスを指定します。

1. ［**宛先**］タブ（図 4-3）を選択します。

図 4-3. VirusScan Mirror サイト（［宛先］タブ）

［宛先］タブでは、指定したサイト（［ソース サイト］ページに表示されます）から取得した .DAT ファイルを保存するローカル フォルダのパスを指定できます。ファイルが取得されるのは、次のいずれかの場合です。

- 宛先フォルダに存在しない新規ファイルがある。
- 宛先フォルダにあるファイルと同じ名前の新規ファイルがある。

2. この手順で、定義する各 Mirror サイトを設定します。

重要 : 宛先がローカル コンピュータでない場合には、ネットワーク上のドライブをマッピングする必要があります。マッピングされたネットワーク ドライブはユーザがシステムにログオンしていないと使用できません。したがって、タスクが開始するときに、ユーザがログオンしていないと、ミラーリング タスクは実行されません。

ミラーリングの記録

ミラーリング イベントを記録するログ ファイルをセットアップすることができます。

1. ［**ログ**］タブ（46 ページの図 3-4）を選択して、ロギング機能を設定します。
2. ［**ログへの記録**］が選択され、ロギング機能が有効になっているかどうか確認します。
   - ログ ファイルの名前は UPDATE.TXT です。デフォルトのパスは次のとおりです。

     ```
     <drive>:¥Program Files¥Network
     Associates¥VirusScan¥
     ```

   - 必要であれば、別の名前またはパスが入力できます。
3. ログ ファイルのサイズを指定します。
   - ログ ファイルの最大サイズは 999 KB です。10 KB から 999 KB までの値を入力してください。
   - ログ ファイルのデータが、ログ ファイルに設定した制限を超えると、新しい情報を記録するため、古い順から 20% のログ テキストが削除されます。ログ ファイルのサイズに制限を設定しないと、ログ ファイルの存在するドライブのすべての空き容量を使用してしまう危険性があります。
4. ロギングの範囲を指定します。
   - ［**詳細な内容をログに記録する**］を選択すると、操作の詳細が記録されます。
   - タスクの開始と終了だけを記録するには、このチェックボックスをオフにします。
5. ログ オプションの設定が完了したら［**OK**］をクリックします。

索引

記号

.DAT ファイル
- .ZIP ファイル， 35
- FTP サイトの Mirror サイト， 48
- Mirror サイトの作成， 47 ～ 54
- Network Associates ダウンロード サイト， 35
- SuperDAT， 35
- アップデート， 35
- 既存ファイルのバックアップ， 44
- 差分， 35
- 内容， 35
- 前のバージョンの復元， 44

.DAT ファイルのバックアップ， 44

A

active FTP の選択
- 自動アップデート， 40
- ミラーリング， 51

D

.DAT ファイル
- 強制アップデート， 44

DELTA.INI ファイル， 36

E

E-Mail スキャンのインストール， 26

ePolicy Orchestrator
- 自動アップデートの設定， 38
- ミラーリングの設定， 49

F

FTP
- .DAT アップデートに使用する Network Associates のサイト， 14
- .DAT アップデートの Network Associates サイト， 35, 48
- active の選択， 40, 51
- Network Associates サイト (デフォルト)
  - 自動アップデート， 39
  - ミラーリング， 50
- Network Associates ダウンロード サイトのミラーリング， 23, 47 ～ 54
- passive， 12, 40, 51
- アップグレード時に保存されない設定， 31
- アップデート ファイルのダウンロード， 16
- ダウンロード サイトへのログオン， 40, 51
- 匿名
  - 自動アップデート， 40
  - ミラーリング， 51
- 認証が必要な
  - 自動アップデート， 40
  - ミラーリング， 51
- ファイルの取得方法の設定， 40, 51

M

Mirror サイトの作成， 47 ～ 54

MSI (Microsoft Windows Installer)， 25

N

NTFS、NullSessionShare を保護するセキュリティ機能， 43
NullSessionShare， 42 〜 43

P

passive FTP、新機能， 12
passive FTP の選択
　自動アップデート， 40
　ミラーリング， 51

S

SETUP.EXE， 25
SuperDAT ファイル， 35

U

UNC
　アップグレード時に保存されない設定， 31
UNC (Universal Naming Convention)
　Mirror サイトからのアップデート ファイルの取得， 52
　NullSessionShare からのファイルの取得， 42
　共有ファイルからのアップデート ファイルの取得， 42
UPDATE.INI ファイル， 36

V

VirusScan 4.5.1 の機能
　Network Associates FTP サイトのミラーリング， 14
　passive FTP， 12
　アップデートまたはアップグレード後のプログラムの実行， 13, 18
　エンジンと .DAT ファイルのアップデート， 13
　感染しやすいファイルのみのスキャン， 10
　自動アップデートの設定， 16
　ネットワーク ドライブ スキャンのスケジューリング， 19
VirusScan コンソール
　［タスク プロパティ］の表示， 12
　オンアクセス スキャン， 11
　オンデマンド スキャン， 11
　自動アップデートの設定， 37
　説明， 26
　ミラーリングの設定， 49
VShield システム スキャンのインストール， 26

あ

アップグレード
　/BATCH スイッチ， 15
　完了後のプログラムの実行， 18
アップデート
　.DAT ファイル， 35
　/BATCH スイッチ， 15
　完了後のプログラムの実行， 18
　強制， 44
　サイトの設定， 38
　サイトの定義， 38
　スキャン エンジン， 44
　ログ オプション， 45
［宛先］タブ， 53
宛先フォルダ， 53
後でアップデート， 29
後で使用するためにアップデート ファイルを保存する
　ミラーリングの設定を参照

い

インストール
　概要， 21
インストール ウィザード， 25
インストール後のデフォルトのスキャン， 29
インストール時のコンピュータの再起動， 32
インストール時のシステムの再起動
　ソフトウェアのインストール， 32
インストールで使用する管理者権限， 25
インストールの種類
　カスタム インストール， 27
　標準インストール， 26
インストールの前に， 23
インストール要件， 23
インターネット スキャンのインストール， 26

う

ウイルス送信ユーティリティのインストール， 27

え

エマージェンシー ディスクの作成， 28
エンジンのアップデート， 44

お

オンアクセス スキャン， 11
オンデマンド スキャン， 11

か

［拡張アップデート オプション］タブ
　自動アップグレード， 18
　自動アップデート， 18, 44
カスタム インストール， 27
関連マニュアル， 6

き

強制アップデート オプション， 44

こ

コマンドライン /BATCH スイッチ， 15
コマンドライン スキャナのインストール， 27
コンポーネントのインストール
　VirusScan， 27

さ

［サイト オプション］ページ
　自動アップデート， 39 ～ 43
　ミラーリング， 50 ～ 52
差分 .DAT ファイル， 35

し

システム要件， 23
自動アップグレード
　/BATCH スイッチ， 15
　完了後のプログラムの実行， 18
　［プロパティ］ページ， 50
自動アップデートの設定， 37
　/BATCH スイッチ， 15
　ePolicy Orchestrator の使用， 38
　VirusScan コンソールの使用， 37
　アップデート後のプログラムの実行， 45
　アップデート サイト， 38
　詳細設定オプション， 44
　プロパティ ページの表示， 38
　ログ オプション， 45
自動アップデートを今すぐ実行， 29
自動アップデートを今すぐ設定， 29

使用許諾契約， 26
詳細情報， 6
詳細ログ
　自動アップデート， 46
　ミラーリング， 54
新機能。VirusScan 4.5.1 の機能を参照

す

スキャン
　エンジンのアップデート， 44
　オンアクセス， 11
　オンデマンド， 11
　感染しやすいファイル タイプ， 11
［スケジュール］タブ (［スケジューラ］ダイアログ ボックス)， 38 ～ 50

せ

設定
　自動アップデート。自動アップデートの設定を参照
　ミラーリング。ミラーリングの設定を参照
設定の保存， 31

そ

ソース サイトの設定， 38, 50
ソフトウェアのインストール， 25
　SETUP.EXE， 25
　インストール ウィザード， 25
　インストールの前に， 23
　システム要件， 23
　追加と削除， 30
　必要な管理者レベル， 25
　標準インストール， 26
ソフトウェアの削除， 30
ソフトウェアの変更， 30

た

ダウンロード サイトへの匿名ログオン
　自動アップデート， 40
　ミラーリング， 51
ダウンロードに使用するプロキシ サーバ
　自動アップデート， 41
　ミラーリング， 51
［タスク］タブ (［スケジューラ］ダイアログ ボックス)， 38, 49 ～ 50

は

ハードディスクの空き容量， 23
バッチ ファイルでの /BATCH スイッチの使用， 15

ひ

必要な Internet Explorer， 23
必要な RAM， 23
必要なオペレーティング システム， 23
標準インストール， 26

ふ

ファイルの取得に使用するローカル パス
　自動アップデート， 43
　ミラーリング， 52
ブート レコードのスキャン， 28
プログラム機能のインストール， 26
プロセッサ要件， 23
［プロパティ］ページ
　システム スキャン， 11
　自動アップグレード， 50
　自動アップデート， 38

ま

マニュアル
　関連， 6

み

ミラーリングの設定， 48
ePolicy Orchestrator の使用， 49
VirusScan コンソールの使用， 49
宛先， 53
詳細設定オプション， 53
ソース サイト， 50
ログ オプション， 54

ゆ

ユーザ認証情報
FTP 経由の自動アップデート， 40
FTP 経由のミラーリング， 51
NullSessionShare, 43
自動アップデートでの UNC パス， 42
ミラー サイトの UNC パス， 52

れ

レポート
自動アップデート， 45 ～ 46
ミラーリング， 54

ろ

ログイン スクリプトでの /BATCH スイッチの使用， 15
ログ オプション
自動アップデート， 45 ～ 46
詳細， 46, 54
ミラーリング， 54
［ログ］タブ， 46, 54
ログ ファイルのサイズ， 46, 54
ログ ファイルのサイズ制限
自動アップデート， 46
ミラーリング， 54