ユーザ ガイド
改訂 1.0

VirusScan® for Mac

バージョン 8.6

McAfee®
System Protection

信頼のセキュリティ

McAfee®

著作権と商標

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、ウェブシールドは米国法人 McAfee, Inc. またはその関係会社の登録商標です。McAfee ブランドの製品は赤を基調としています。本書中のその他の登録商標及び商標はそれぞれその所有者に帰属します。

ライセンス情報

使用許諾契約

お客様へ : お客様がお買い求めになっ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。お買い求めになったライセンス タイプがご不明の場合には、担当営業またはライセンス付与管理部門にご相談になるか、製品に付随する購入関係書類もしくは購入手続きにおいて別途受領された書類をご参照ください。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。

帰属

本製品には下記のソフトウェアおよびテクノロジーが含まれている場合があります。

• OpenSSL Toolkit で使用するために OpenSSL Project によって開発されたソフトウェア (http://www.openssl.org/)。• Eric A. Young によって作成された暗号化ソフトウェア、および Tim J. Hudson によって作成されたソフトウェア。• GNU General Public License (GPL) あるいは、プログラムもしくはその一部の複製、変更、再頒布およびソースコードへのアクセスを許諾するフリーソフトウェア ライセンスで使用 (または再ライセンス) が許可されるソフトウェア プログラム。GPL では、ソフトウェアを実行可能なバイナリ 形式で配布する場合に、そのソースコードも一緒に提供することが定められています。本製品に GPL で配布されているソフトウェアが含まれている場合、そのソースコードが製品 CD に収録されています。フリーソフトウェア ライセンスにより、弊社が製品の使用許諾契約で規定している範囲を超えてソフトウェア プログラムの使用、複製、または変更を許諾しなければならない場合、これらの権利が本資料に記載されている権限または制約より優先されるものとします。• Henry Spencer によって作成されたソフトウェア。Copyright 1992, 1993, 1994, 1997 Henry Spencer.• Robert Nordier によって作成されたソフトウェア。Copyright© 1996-7 Robert Nordier.• Douglas W. Sauder によって作成されたソフトウェア。• Apache Software Foundation (http://www.apache.org/) によって開発されたソフトウェア。A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.• International Components for Unicode ("ICU") Copyright ©1995-2002 International Business Machines Corporation and others.• CrystalClear Software, Inc. によって開発されたソフトウェア。Copyright ©2000 CrystalClear Software, Inc. • • Outside In® Viewer Technology ©1992-2001 Stellent Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellent Chicago, Inc. • • Software copyrighted by The Regents of the University of California, © 1996, 1989, 1998-2000. • • Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., © 2003. • © 1995-2003. • Software copyrighted by Michael A. Chase, © 1999-2000. • Software copyrighted by Neil Winton, ©1995-1996. • Software copyrighted by RSA Data Security, Inc., © 1990-1992. • Software copyrighted by Sean M. Burke, © 1999, 2000. • Software copyrighted by Martijn Koster, © 1995. • Software copyrighted by Brad Appleton, © 1996-1999. • Software copyrighted by Michael G. Schwern, ©2001. • Software copyrighted by Graham Barr, © 1998. • Software copyrighted by Larry Wall and Clark Cooper, © 1998-2000. • Software copyrighted by Frodo Looijaard, © 1997. • Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org.• Software copyrighted by Beman Dawes, © 1994-1999, 2002. • • Software copyrighted by Simone Bordet & Marco Cravero, © 2002. • Software copyrighted by Stephen Purcell, © 2001. • Software developed by the Indiana University Extreme! 研究室 (http://www.extreme.indiana.edu/) によって開発されたソフトウェア。• Software copyrighted by International Business Machines Corporation and others, © 1995-2003. • Software developed by the University of California, Berkeley and its contributors.• mod_ssl プロジェクト (http://www.modssl.org/) で使用するために Ralf S. Engelschall <rse@engelschall.com> によって開発されたソフトウェア。• Software copyrighted by Kevlin Henney, © 2000-2002. • Software copyrighted by Peter Dimov and Multi Media Ltd. © 2001, 2002. • Software copyrighted by David Abrahams, © 2001, 2002. See http://www.boost.org/libs/bind/bind.html for documentation. • Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. • Software copyrighted by Boost.org, © 1999-2002. • Software copyrighted by Nicolai M. Josuttis, © 1999. • Software copyrighted by Jeremy Siek, © 1999-2001. • Software copyrighted by Daryle Walker, © 2001. • Software copyrighted by Chuck Allison and Jeremy Siek, © 2001, 2002. • Software copyrighted by Samuel Krempp, © 2001. See http://www.boost.org for updates, documentation, and revision history.• Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. • Software copyrighted by Cadenza New Zealand Ltd., © 2000. • Software copyrighted by Jens Maurer, ©2000, 2001. • Software copyrighted by Jaakko Järvi (jaakko.jarvi@cs.utu.fi), ©1999, 2000. • Software copyrighted by Ronald Garcia, © 2002. • Software copyrighted by David Abrahams, Jeremy Siek, and Daryle Walker, ©1999-2001. • Software copyrighted by Stephen Cleary (shammah@voyager.net), ©2000. • Software copyrighted by Housemarque Oy <http://www.housemarque.com>, © 2001. • Software copyrighted by Paul Moore, © 1999. • Software copyrighted by Dr. John Maddock, © 1998-2002. • Software copyrighted by Greg Colvin and Beman Dawes, © 1998, 1999. • Software copyrighted by Peter Dimov, © 2001, 2002. • Software copyrighted by Jeremy Siek and John R. Bandela, © 2001. • Software copyrighted by Joerg Walter and Mathias Koch, © 2000-2002. • Software copyrighted by Carnegie Mellon University © 1989, 1991, 1992. • Software copyrighted by Cambridge Broadband Ltd., © 2001-2003. • Software copyrighted by Sparta, Inc., © 2003-2004. • Software copyrighted by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications, © 2004. • Software copyrighted by Simon Josefsson, © 2003. • Software copyrighted by Thomas Jacob, © 2003-2004. • Software copyrighted by Advanced Software Engineering Limited, © 2004. • Software copyrighted by Todd C. Miller, © 1998. • Software copyrighted by The Regents of the University of California, © 1990, 1993, Chris Torek によってバークレー校に寄与されたソフトウェアに由来するコード。

目次

1 VirusScan for Mac の紹介

このマニュアルの内容

このマニュアルには、VirusScan for Mac 8.6 を使用して、コンピュータをウイルスから保護するための以下の情報が記載されています。

- 製品の概要
- 製品機能の説明
- このリリースのすべての新機能についての説明
- ソフトウェアの詳細なインストール手順
- ソフトウェアの詳細な設定と配備の手順
- タスク実行の手順
- トラブルシューティング情報
- ePolicy Orchestrator 3.6 (パッチ 2)、3.6.1、4.0 との統合

VirusScan とは

VirusScan for Mac は、ウイルスやトロイの木馬などの悪質なコードから Macintosh コンピュータを保護するウイルス対策アプリケーションです。VirusScan には、オンデマンド スキャン、Apple Mail のスキャン、eUpdate のスケジュール設定、オンライン ヘルプ、オンアクセス スキャン、ドラッグ アンド ドロップ スキャンなどの機能が備わっています。さらに、クリック 1 つでオンラインのウイルス情報ライブラリにアクセスでき、新しい脅威に関するすべての最新情報をいつでも入手できます。

VirusScan を使用すると、他のコンピュータ (Macintosh コンピュータ、Windows コンピュータ、UNIX コンピュータなど) や、外部マウント ボリューム (USB デバイス、Firewire デバイス、CD/DVD など) に潜むウイルスからシステムを保護できます。

VirusScan のこのバージョンでは、Mac OS X 10.5 (Leopard) オペレーティング システム用のウイルス対策もサポートします。

VirusScan の特長

VirusScan は、Macintosh、Windows、UNIX のあらゆるファイル タイプ (圧縮ファイル、OLE 複合ドキュメントを含む) のファイル内に存在するプログラム ウイルス、マクロ ウイルス、トロイの木馬を検出し、駆除します。

VirusScan では、各ファイル、ファイル ディレクトリ、ドライブ全体、Apple Mail メッセージ、または CD や .DMG ファイル、ネットワーク マウント ファイル、USB デバイス (ペン ドライブ、iPod、カメラ) などの外部マウント ボリュームをスキャンします。高度なヒューリスティック スキャンにより、未知のマクロ ウイルスやプログラム ウイルスが検出されます。

このリリースの新機能

- Mac OS X Leopard (10.5) のサポート
- オンアクセス スキャンのパフォーマンスの最適化
- オンデマンド スキャンのパフォーマンスの最適化
- ePolicy Orchestrator 4.0 のサポート
- 差分 DAT アップデート
- 5200 スキャン エンジンのサポート

VirusScan の機能

VirusScan では、以前のバージョンから受け継がれている強力な機能に新しい保護機能とツールが追加され、ご使用のコンピュータ システムを確実に保護することが可能となりました。オンライン ヘルプ システムには、トラブルシューティング情報とタスクの手順についての説明が記載されています。

VirusScan コンソール

VirusScan コンソールでは、わかりやすいインターフェースで VirusScan を設定できます。

コンソールを使用すると、オンデマンド スキャナの設定や、ドロップ ゾーン (スキャン対象のファイルをドラッグ アンド ドロップする、VirusScan コンソール内の領域) を使用したオンデマンド スキャンの実行をすることができます。「**アイテムをドロップするかここをクリック**」をクリックして、「**スキャンおよび駆除するファイルまたはフォルダを選択**」ダイアログ ボックスを開き、オンデマンド スキャンおよび駆除を実行するファイルまたはフォルダを選択します。

また、VirusScan コンソールからオンアクセス スキャナの設定や有効化を行ったり、eUpdate を使用したウイルス定義の自動アップデートを有効にできます。

VirusScan コンソールにアクセスするには、コンピュータの「**アプリケーション**」フォルダにある「**VirusScan**」アイコンをダブルクリックします。

オンデマンド スキャナ

オンデマンド スキャナを使用すると、選択したファイルをコンソールにドラッグ アンド ドロップすることで、いつでもスキャンを開始できます。「**アイテムをドロップするかここをクリック**」をクリックして、「**スキャンおよび駆除するファイルまたはフォルダを選択**」ダイアログ ボックスを開き、スキャンや駆除を実行するファイルまたはフォルダを選択します。

オンデマンド スキャナでは、複数のファイル、ディレクトリ、またはボリュームを選択できます。スキャンの結果はレポート内に表示され、保存や印刷が可能です。スキャン対象や、感染ファイルに対する処理を設定できます。ウイルスが検出されると、メッセージが表示され、処理アクションの情報を記載したログが生成されます。

オンデマンド スキャナを使用するには、スキャンするファイルをドラッグし、「**VirusScan**」アイコンまたはコンソールのドロップ ゾーンにドロップします。

オンアクセス スキャナ

オンアクセス スキャナは、使用されるすべてのファイルを継続的に監視して、ウイルスなどの不審なプログラムが存在するかどうかを監視します。スキャンは、ユーザまたはシステム プロセスによってファイルがディスクから読み取られた場合や、ディスクに書き込まれる場合、もしくはその両方で毎回自動的に実行されます。

オンアクセス スキャナを使用すると、複数のファイル、ディレクトリ、ボリューム (ネットワークに接続しているリモート コンピュータ上のボリュームを含む) に対して、継続的にポリシーが施行されます。スキャン対象や、感染ファイルに対する処理を設定できます。ウイルスまたはその他の悪質なコードが検出されると、**Reporter** のポップアップ ウィンドウが表示されます。

オンアクセス スキャナは、VirusScan コンソールから有効にします。

VirusScan Schedule Editor

VirusScan Schedule Editor では、自動スキャンのスケジュールや、オンラインで入手可能なウイルス定義 (DAT) ファイルの自動アップデートのスケジュールを設定できます。スキャンとアップデートのスケジュールは、**VirusScan Schedule Editor** コンソールで設定できます。自動スキャンとアップデートのスケジュールは、日単位、週単位、または月単位の頻度で設定できます。VirusScan Schedule Editor にアクセスするには、以下のいずれかのタスクを行います。

- VirusScan コンソールで「**スケジューラ**」  をクリックします。
- メイン メニューの「**表示**」から「**スケジュール タスク**」を選択します。
- VirusScan Schedule Editor を `/Applications/Utilities` フォルダから直接開きます。

eUpdate

eUpdate では、DAT ファイルとウイルス対策エンジンをアップデートできます。eUpdate を使用すると、最新のウイルス情報とスキャン機能でウイルス対策ソフトウェアを継続的にアップデートできます。インターネットに接続している場合、eUpdate は新しいアップデートをチェックし、入手可能な新しいアップデートが存在する場合はウイルス定義をアップデートします。また、VirusScan Schedule Editor を使用して、eUpdate がアップデートをチェックするスケジュールを独自に設定することもできます。

eUpdate を手動で起動するには、VirusScan コンソールで「**eUpdate**」タブをクリックし、「**開始**」ボタンをクリックします。eUpdate は FTP プロトコルを使用してサポートされます。

ePolicy Orchestrator による管理

VirusScan を McAfee ePolicy Orchestrator 3.6 (パッチ 2)、3.6.1、4.0 と統合すると、管理された環境でこのソフトウェアを使用できます。ePolicy Orchestrator ソフトウェアを使用すると、McAfee System Protection Solutions を一元管理することができます。管理者は、1 台のコンソールから企業全体のコンピュータに対して、不正システムや未対応システムのリスクの軽減、最新の保護対策の維持、保護ポリシーの設定および施行、セキュリティ状態の監視を行うことができます。ePolicy Orchestrator を使用すると、ネットワークを介して他のシステム上の VirusScan for Mac を設定できます。各システムの「**環境設定**」ウィンドウから個別に設定する必要はありません。

ePolicy Orchestrator を使用しない場合でも、スタンドアロン製品として VirusScan のすべての機能を使用することができます。

ePolicy Orchestrator に関連する機能は、ePolicy Orchestrator と Non-Windows Agent をインストールし、企業環境で VirusScan の管理を行うように設定している場合にのみ使用できます。

対象読者

このマニュアルの情報は、社内のウイルス対策およびセキュリティ プログラムを担当するネットワーク管理者を対象としています。

表記規則

このマニュアルでは、次の表記規則を使用します。

太字

オプション、メニュー、ボタン、ダイアログ ボックスの名前など、インターフェースのすべての用語に使用します。

例：
適切なアカウント情報を「**ユーザ名**」と「**パスワード**」に入力します。

Courier

フォルダやプログラムのパス、ユーザがそのまま入力するテキスト（システム プロンプト でのコマンド など）に使用します。

例：
プログラムのデフォルトの場所は次のとおりです。

```
/Applications/Utilities
```

クライアント コンピュータ上で次のコマンドを実行します。

```
scan --help
```

青字

Web アドレス (URL) やリンクに使用します。

例：
McAfee の Web サイトを参照してください。

http://www.mcafee.com

< 用語 >

総称的な用語を表すために不等号括弧を使用します。

例：
コンソール ツリーで、< サーバ > を右クリックします。

注意： 同一のコマンドを実行するための別の方法など、補足的な情報を示します。

ヒント： ウイルス対策やパフォーマンスの改善などを効果的に行うために McAfee が提案または推奨する内容を示します。

警告： ユーザ、コンピュータ システム、企業、ソフト ウェアのインスト ール、またはデータを保護するための重要なアド バイスを示します。

危険: ハード ウェアを取り扱う場合にけがや事故を防ぐための重要なアド バイスを示します。

製品情報の入手

特に注記がない場合、製品マニュアルは製品 CD または McAfee ダウンロード サイトから Adobe Acrobat .PDF ファイル形式で入手することができます。

一般的なマニュアル

ユーザ ガイド ― 製品の紹介と機能の説明、ソフトウェアのインストールと設定方法、通常の操作やメンテナンスについての詳しい手順が記載されています。このマニュアルには、ePolicy Orchestrator による VirusScan の管理機能の紹介や、企業環境でのソフトウェアのインストール、設定および管理方法が記載されています。このマニュアル(『VirusScan ユーザ ガイド』) は、製品パッケージの「**マニュアル**」フォルダから .PDF 形式で入手できます。

ヘルプ ― ソフトウェア アプリケーションからアクセスするヘルプ。高度で詳細な情報が記載されています。

VirusScan for Mac リリース ノート ― このファイルには、製品の機能、マニュアルに記載されていない最新の追加や変更点、製品リリースに関する既知の動作や問題、インストール プロセスについての説明などが記載されています。このファイルは、製品パッケージの「**マニュアル**」フォルダから入手できます。

ライセンス ― McAfee 使用許諾契約書 (.PDF 形式)。製品に対して購入可能なライセンスのすべての種類が記載されています。使用許諾契約では、ライセンス製品の使用に関する一般的な条件が定義されています。よくお読みください。製品をインストールすると、ライセンス条件に同意したことになります。McAfee ソフトウェアの使用許諾契約は、製品パッケージの「**マニュアル**」フォルダから入手できます。

製品内のリンク

製品の「ヘルプ」メニューには、有用なリソースへのリンクがあります。

- VirusScan のヘルプ
- サンプルの送信
- テクニカル サポート
- ウイルス情報ライブラリ

VirusScan のヘルプ

このリンクからオンライン ヘルプのトピックにアクセスできます。

サンプルの送信

このリンクから、感染の可能性のあるファイルを分析用に弊社に送信できます。必要に応じて、解決方法やリアルタイムの修正方法など、ファイルに関する情報が提供されます。

テクニカル サポート

このリンクから、McAfee Technical Support Web サイトにアクセスし、製品マニュアル、FAQ、トラブルシューティングのヒントなどを参照できます。

ウイルス情報ライブラリ

「ウイルス情報ライブラリ」リンクから、McAfee® Avert® Labs のウイルス情報ライブラリにアクセスできます。この Web サイトには、ウイルスの発生源、システムへの感染経路、削除方法などの詳細な情報があります。

ウイルス情報ライブラリには、本物のウイルスに関する情報のほか、電子メールで受信するウイルス警告のように、ウイルスのデマに関する有益な情報があります。Virtual Card For You と SULFNBK が有名ですが、他にも多くのデマ情報があります。善意と思われるウイルス警告を受信した場合は、そのメッセージを周囲に送信する前に、デマ情報ページをご確認ください。

ウイルス情報ライブラリにアクセスするには

1 VirusScan を開きます。

2 「**ヘルプ**」メニューから、「**ウイルス情報ライブラリ**」を選択します。

連絡先

スレット センター : McAfee Avert® Labs http://www.mcafee.com/us/threat_center/default.asp

Avert Labs スレット ライブラリ
http://www.nai.com/japan/virusinfo/vlatest.asp\n

Avert Labs WebImmune およびサンプルの提出先
(ログオンするには有効な認証情報が必要です)
https://www.webimmune.net/default.asp

Avert Labs DAT 通知サービス
http://vil.nai.com/vil/signup_DAT_notification.aspx

ダウンロード サイト http://www.mcafee.com/us/downloads/

製品のアップグレード (有効な承認番号が必要です)

セキュリティ アップデート (DAT、エンジン)

HotFix およびパッチ リリース

- **セキュリティの脆弱性用** (公開版)
- **製品用** (ServicePortal アカウントおよび有効な承認番号が必要です)

製品の評価

McAfee ベータ プログラム

テクニカル サポート http://www.mcafee.com/us/support/

ナレッジベース検索
http://knowledge.mcafee.com/

McAfee Technical Support ServicePortal (ログオンするには有効な認証情報が必要です)
https://mysupport.mcafee.com/eservice_enu/start.swe

カスタマ サービス

ホームページ
http://www.mcafee.com/us/support/index.html
http://www.mcafee.com/us/about/contact/index.html

電話 ― 米国、カナダ、ラテン アメリカ (無料ダイアル):
+1-888-VIRUS NO または **+1-888-847-8766** 月曜日～金曜日、
午前 8 時～午後 8 時 (中部標準時)

プロフェッショナル サービス

大企業のお客様 : http://www.mcafee.com/us/enterprise/services/index.html

中堅・中小企業のお客様 : http://www.mcafee.com/us/small/services/index.html

2 VirusScan for Mac のインストール

ここでは、VirusScan ソフトウェアのインストールに関して、以下の内容について詳しく説明します。

システム要件

VirusScan for Mac ソフトウェアをインストールするには、PowerPC または Intel ベースの Mac コンピュータ、Mac OS X Tiger (10.4.6 以降) または Mac OS X Leopard (10.5) オペレーティング システム、512 MB (以上) の RAM、45 MB 以上の空きディスク容量が必要です。

ePolicy Orchestrator の要件

VirusScan は ePolicy Orchestrator バージョン 3.6 (パッチ 2)、3.6.1、4.0 と統合されます。ただし、ePolicy Orchestrator を使用しない場合でも、スタンドアロン製品として VirusScan for Mac を使用できることにご注意ください。

ePolicy Orchestrator に関連する機能は、ePolicy Orchestrator と Non-Windows Agent をインストールし、企業環境で VirusScan の管理を行うように設定している場合にのみ使用できます。

VirusScan をインストールする

VirusScan for Mac は、標準インストール (グラフィカル インターフェース) またはコマンド ラインからのインストール (サイレント インストール) のいずれかの方法でインストールできます。製品をインストールすると、製品パッケージの「**マニュアル**」フォルダから ReadMe ファイルを参照できます。このファイルには、既知の問題、オンライン リソース、その他の便利な情報が記載されています。

VirusScan では、eUpdate 機能を使用して Web サイトへの接続や、新しい DAT ファイルのダウンロードをすることができます。eUpdate や VirusScan のその他の機能の詳細については、17 ページの「基本操作」を参照してください。

この製品をインストールするには管理者権限が必要です。

標準インストール

VirusScan は、製品 CD、もしくは弊社 Web サイトからダウンロードして一時フォルダに保存したインストール .ZIP ファイルの VirusScan インストール ファイルを使用してインストールすることができます。

VirusScan をインストールするには

1 **VirusScan.pkg** ファイルをダブルクリックして、インストーラを起動します。

2 画面に表示された手順に従ってソフトウェアをインストールします。

3 使用許諾契約を読み、同意します。使用許諾契約に同意しないと、インストールを続行できません。

4 「**インストール**」をクリックしてインストールを実行します。「**認証**」ダイアログボックスが表示されます。

5 ユーザ名と管理者用パスワードを入力して、「**OK**」をクリックします。インストールが完了すると、メッセージが表示されます。「**閉じる**」をクリックします。

VirusScan for Mac インストーラにより、ご使用のコンピュータの `Applications` フォルダ内に VirusScan アプリケーションがインストールされ `Application/Utilities` フォルダ内に VirusScan Schedule Editor アプリケーションがインストールされます。

VirusScan for Mac 8.6 のインストール後は (以前のバージョンとは異なり)、コンピュータを再起動する必要はありません。

コマンド ラインからのインスト ール (サイレント インスト ール)

1 製品 CD または弊社 Web サイトからダウンロードしたインストール .ZIP ファイルで、**VirusScan.pkg** ファイルを検索し、一時フォルダに保存します。

2 「**Terminal**」ウィンドウを開き、作業フォルダを **VirusScan.pkg** ファイルが配置されているフォルダに変更します。

3 「**Terminal**」ウィンドウで次のように実行します。

```
sudo installer -pkg VirusScan.pkg -target /
```

4 システム パスワードの入力を求めるメッセージが表示された場合は、システム パスワードを入力します。

5 インストールが完了すると、メッセージが表示されます。「**Terminal**」ウィンドウを閉じます。

アップグレード インストール

VirusScan の以前のバージョン (8.0 や 8.5) から VirusScan for Mac v8.6 にアップグレードできます。アップグレード後、以前のバージョンから現在のバージョン (v8.6) に環境設定が移行されます。

インストールをテストする

EICAR (European Institute of Computer Anti-Virus Research) 標準ウイルス対策テストファイルを使用すると、VirusScan のテストを実行できます。このファイルは、世界中のウイルス対策ソフトウェア メーカーが共同で開発した標準規格です。ユーザはこれを使用してウイルス対策ソフトウェアを検証することができます。

インストールをテストするには

1 EICAR.ORG Web サイト (http://www.eicar.org) にアクセスし、ウイルス対策テストファイルである Eicar.zip をダウンロードします。

2 ダウンロードした ZIP ファイルに対して、オンデマンド スキャナを実行します。VirusScan は、EICAR テスト ファイルでの検出結果についてレポートします。

このファイルはウイルスではありません。ウイルス対策ソフトウェアのテストを行うためのファイルです。他のユーザがウイルスと間違えないように、ソフトウェアのテストが終了したらこのファイルは削除できます。

テストが正常に終了したら、VirusScan ソフトウェアを起動する準備は完了です。

VirusScan をアンインストールする

VirusScan は、製品 CD、もしくは弊社 Web サイトからダウンロードして一時フォルダに保存したインストール .ZIP ファイルに含まれるアンインストール ファイル (**VirusScan Uninstall.command**) を使用してアンインストールできます。アンインストール コマンドを Terminal から実行することもできます。

VirusScan をアンインストールするには

1 次のいずれかを実行します。

- 「**VirusScan Uninstall.command**」アイコンをダブルクリックします。
- 「**VirusScan Uninstall.command**」アイコンをドラッグして「**Terminal**」ウィンドウにドロップし、**Enter** キーを押します。
- 「**Terminal**」ウィンドウで、ディレクトリを `/usr/local/vscanx` に変更してから、**VirusScan Uninstall.command** を実行します。

「**Terminal**」アプリケーションを開くには、`/Applications/Utilities` に配置されているアプリケーションをダブルクリックします。

「**Terminal**」ウィンドウに管理者用パスワードの入力を求めるメッセージが表示されます。

2 管理者用パスワードを入力して、**Enter** キーを押します。

管理者用パスワードは、「**Terminal**」ウィンドウには表示されません。

アンインストール プロセスが正常に完了すると、コンピュータから VirusScan ソフトウェアが削除されたことを通知するメッセージが「**Terminal**」ウィンドウに表示されます。

3 基本操作

この章では、VirusScan の基本操作と、コンピュータをウイルスから保護する方法について説明します。内容は、次のとおりです。

VirusScan コンソールを使用する

VirusScan コンソールでは、オンデマンド スキャンとオンアクセス スキャンを実行および設定できます。また、McAfee ウイルス情報ライブラリへの接続、eUpdate の実行、ウイルス スキャン レポートの印刷や保存を行うこともできます。

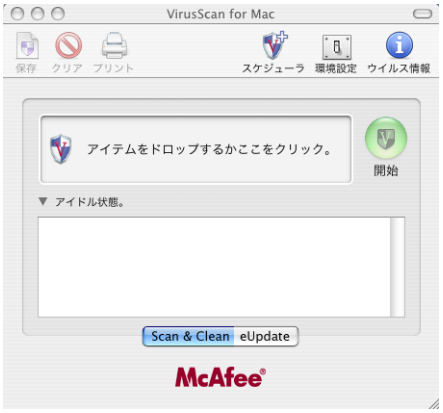
さらに、VirusScan コンソールには、オンデマンド スキャンで使用するドラッグ アンド ドロップ ペインがあります。コンソールの中央ペインにファイルをドラッグし、ドラッグ アンド ドロップ ペインにドロップして「**開始**」ボタンをクリックすると、オンデマンド スキャンをいつでも開始できます。1 つのファイルのスキャン終了後に、別のファイルを追加すると、最初のスキャン項目が上書きされます。

VirusScan コンソール

VirusScan コンソールには、以下を始めとする Macintosh の標準コンポーネントおよび特別なウイルス対策コンポーネントが表示されます。

- タイトル バーには、現在実行されているプログラムの名前が表示されます。
- 閉じる、最小化、最大化、表示 / 非表示のツール バー ボタンは、インターフェースのサイズ変更や表示 / 非表示の切り替えに使用します。

図 3-1 VirusScan コンソール



ツール バー

ツール バーには、次のボタンが表示されます。

ウイルス スキャン レポートをリッチ テキスト (.RTF) 形式で保存します。

ステータス パネルに現在表示されているレポートをクリアします。

現在のレポートを印刷します。

スキャン タスクや eUpdate タスクのスケジュールを設定できます。

「**環境設定**」ダイアログ ボックスを開き、次の操作を実行できます。

- オンデマンド スキャナの環境設定を指定します。
- オンアクセス スキャナの環境設定を指定します。
- ウイルスが検出されたときに実行するアクションを設定します。
- 結果をファイルにログ記録します。
- eUpdate サーバの設定を指定します。
- 除外リストを設定します。
- ウイルス定義のアップデートを自動的に確認します。

デフォルトのブラウザを起動し、McAfee ウイルス情報ライブラリを表示します。

メニュー バー

メニュー バーには、すべての画面に共通の標準ドロップダウン メニューが表示されます。「**ファイル**」、「**編集**」、「**表示**」、「**ウィンドウ**」、および「**ヘルプ**」があります。

スキャナを設定する

オンデマンド スキャナとオンアクセス スキャナの設定は、「**環境設定**」ダイアログ ボックスから指定できます。このダイアログ ボックスには、オンデマンド スキャナ用とオンアクセス スキャナ用の 2 種類のバージョンがあります。どちらのスキャナでも全般的な環境設定は同じですが、高度なスキャン オプションはスキャナ固有です。

スキャナの環境設定は、すべてのユーザに適用されるグローバル設定です。

環境設定は指定すると自動的に保存されます。

環境設定を変更するには管理者権限が必要です。

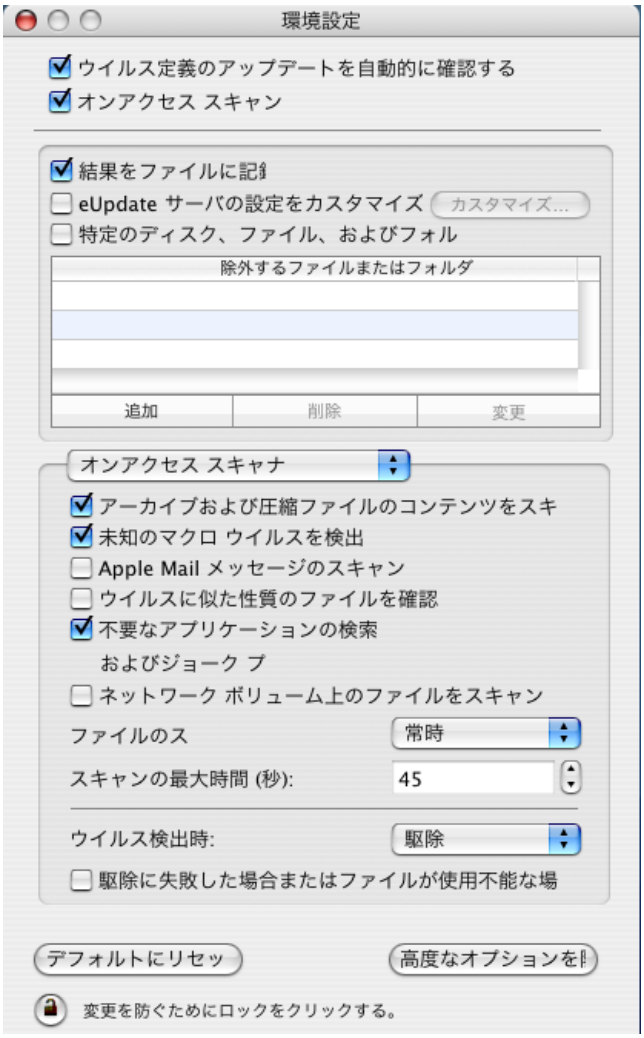
全般的な環境設定を指定する

全般的な環境設定は、オンデマンド スキャナとオンアクセス スキャナの両方に適用されます。どちらのスキャナにも同じ環境設定が用意されています。

全般的な環境設定を指定するには

1 ツール バーで「**環境設定**」 をクリックして、「**環境設定**」ダイアログ ボックスを表示します。このダイアログ ボックスの上部パネルに、オンデマンド スキャナとオンアクセス スキャナの両方に適用される全般的な環境設定オプションが表示されます。

図 3-2 全般的な環境設定



2 オンデマンド スキャナとオンアクセス スキャナに適用する、スキャンの全般的な環境設定を指定します。表 3-1 に、指定できる全般的な環境設定を示します。

表 3-1 オンデマンド スキャナとオンアクセス スキャナの全般的な環境設定

ウイルス定義のアップデートを自動的に確認する	自動 eUpdate を有効 / 無効にします。
オンアクセス スキャン	オンアクセス スキャンを有効 / 無効にします。
結果をファイルに記録	ファイルへの結果の記録を有効 / 無効にします。
eUpdate サーバの設定をカスタマイズ	ユーザ名とパスワードでアップデート サーバを管理します。「**カスタマイズ**」をクリックして、eUpdate の FTP 設定を変更します。
特定のディスク、ファイル、およびフォルダを除外	スキャンから除外する対象を設定します。これを選択しないと、除外設定はできません。 除外項目を追加するには ■ 「**除外するファイルまたはフォルダ**」リストで「**追加**」をクリックします。「**開く**」ダイアログ ボックスからファイルまたはフォルダを選択します。 除外項目を削除するには ■ 「**除外するファイルまたはフォルダ**」リストからファイルまたはフォルダを選択します。「**削除**」をクリックします。 除外項目を変更するには ■ 「**除外されたファイルまたはフォルダ**」リストからファイルまたはフォルダを選択します。「**変更**」をクリックします。「**開く**」ダイアログ ボックスが表示されます。既存の除外項目と置き換えるファイルまたはフォルダを選択します。

3 必要に応じて高度な環境設定を指定します。高度な環境設定は、「**環境設定**」ダイアログ ボックスの下部ペインに表示されます。オンデマンド スキャナ用とオンアクセス スキャナ用に、別々の環境設定を指定できます。詳細については、22 ページの「オンデマンド スキャナを設定する」と 24 ページの「オンアクセス スキャナを設定する」を参照してください。

4 環境設定が変更されないようにするには「**ロック**」をクリックします。

5 「**環境設定**」ダイアログ ボックスの左上端にある「**閉じる**」をクリックします。

オンデマンド スキャナを設定する

オンデマンド スキャナを使用すると、いつでもスキャンを開始できます。オンデマンド スキャナの高度な環境設定は、「環境設定」ダイアログの下部ペインに表示されるオプションを使用して指定します。

オンデマンド スキャナを設定するには

1 ツール バーで「**環境設定**」 をクリックして、「**環境設定**」ダイアログ ボックスを表示します。

2 ダイアログ ボックスの右下端にある「**高度なオプション**」をクリックして、高度な環境設定を表示します。

3 ドロップダウン メニューから「**オンデマンド スキャナ**」を選択し (まだ選択されていない場合)、オンデマンド スキャン用のダイアログ ボックスを表示します。

.

図 3-3 オンデマンド スキャナの環境設定

4 オンデマンド スキャナの高度な環境設定を指定します。表 3-2 に、指定できる環境設定を示します。

表 3-2 オンデマンド スキャナの高度な環境設定

アーカイブおよび圧縮ファイルのコンテンツをスキャン	選択したスキャナが、アーカイブやその他の圧縮ファイルの内容もスキャンするように設定します。オンデマンド スキャナではデフォルトでオンになっています。
未知のマクロ ウイルスを検出	感染の可能性のあるマクロ (未知のウイルス) をファイルが含んでいる場合、そのマクロもスキャンされ、駆除の一環として、駆除または削除されます。
Apple Mail メッセージのスキャン	オンデマンド スキャナによる Apple Mail メッセージの感染のチェックを有効 / 無効にします。
ウイルスに似た性質のファイルを確認	ウイルスやワームに似た特徴を持ち、未知のウイルスを含んでいる恐れがあるファイルを検出するチェックを、オンデマンド スキャナで有効 / 無効にします。
不要なアプリケーションおよびジョーク プログラムの検索	不正なプログラムやジョーク プログラムのチェックを、オンデマンド スキャナで有効/無効にします。
ウイルス検出時 : ■ 駆除 ■ 削除 ■ 通知	オンデマンド スキャナの基本アクションを選択します。
駆除に失敗した場合またはファイルが使用不能な場合に削除	オンデマンド スキャナで実行する 2 番目のアクションを選択します。この機能は基本アクションが「**駆除**」に設定されている場合にのみ有効です。

5 環境設定が変更されないようにするには「**ロック**」をクリックします。

6 「**環境設定**」ダイアログ ボックスの左上端にある「**閉じる**」をクリックします。

オンアクセス スキャナを設定する

オンアクセス スキャナは、使用されるすべてのファイルを継続的に監視して、ウイルスなどの不審なプログラムが存在するかどうかを監視します。オンアクセス スキャナは、スキャナの環境設定に応じて、ディスクからファイルが読み取られた場合、ディスクにファイルが書き込まれた場合、もしくはその両方でスキャンを実行します。

オンアクセス スキャナの高度な環境設定は、「環境設定」ダイアログの下部ペインに表示されるオプションを使用して指定します。

オンアクセス スキャナを設定するには

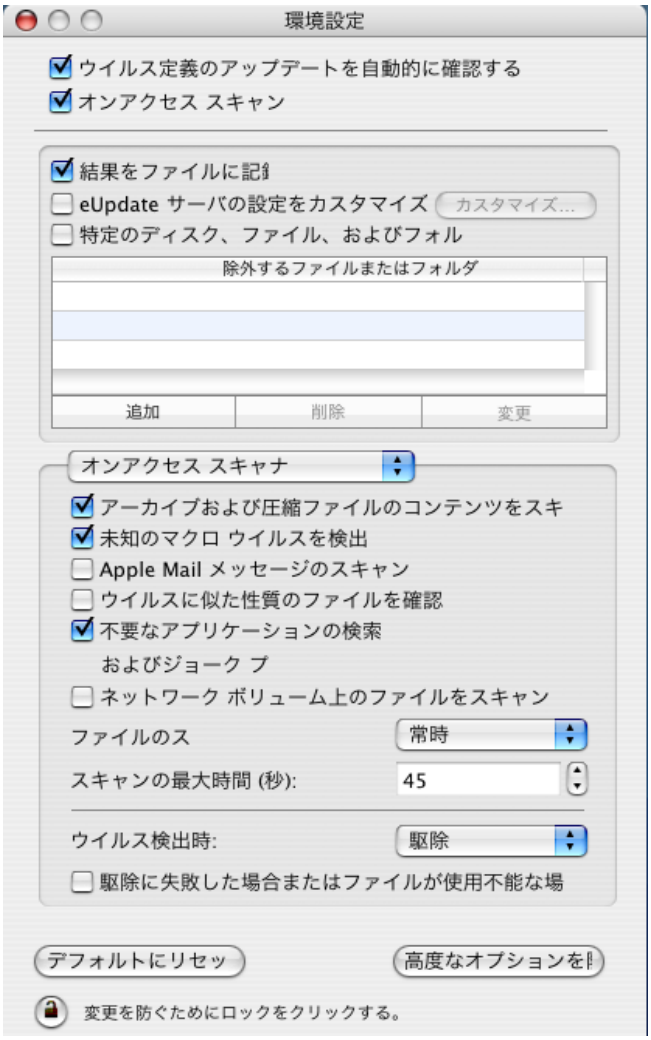
1 ツール バーで「**環境設定**」をクリックして、「**環境設定**」ダイアログ ボックスを表示します。

2 ダイアログ ボックスの右下端にある「**高度なオプション**」をクリックして、高度な環境設定を表示します。

3 ドロップダウン メニューから「**オンアクセス スキャナ**」を選択し (まだ選択されていない場合)、オンアクセス スキャン用のダイアログ ボックスを表示します。

.

図 3-4 オンアクセス スキャナの環境設定



4 オンアクセス スキャナの環境設定を指定します。表 3-3 に、指定できる環境設定を示します。

表 3-3 オンアクセス スキャンの高度な環境設定

アーカイブおよび圧縮ファイルのコンテンツをスキャン	選択したスキャナが、アーカイブやその他の圧縮ファイルの内容もスキャンするように設定します。オンアクセス スキャナではデフォルトでオンになっています。オンアクセス スキャナは stuffit アーカイブ内をスキャンしない点に注意してください。
未知のマクロ ウイルスを検出	感染の可能性のあるマクロ (未知のウイルス) をファイルが含んでいる場合、そのマクロもスキャンされ、駆除の一環として、駆除または削除されます。
Apple Mail メッセージのスキャン	オンアクセス スキャナによる Apple Mail メッセージの感染のチェックを有効 / 無効にします。
ウイルスに似た性質のファイルを確認	ウイルスやワームに似た特徴を持ち、未知のウイルスを含んでいる恐れがあるファイルを検出するチェックを、オンアクセス スキャナで有効 / 無効にします。
不要なアプリケーションおよびジョークプログラムの検索	不正なプログラムやジョーク プログラムのチェックを、オンアクセス スキャナで有効/無効にします。
ネットワーク ボリューム上のファイルをスキャン	ネットワーク ボリュームからアクセスされるファイルをスキャナでスキャンするかどうかを設定します。
ファイルのスキャン : ■ 常時 ■ 読み取り時 ■ 書き込み時	ファイルがディスクから読み取られたとき、ディスクに書き込まれたとき、またはその両方で、オンアクセス スキャナがファイルをスキャンするかどうかを指定します。
スキャンの最大時間	スキャンで 1 つのファイルをスキャンする最大時間 (秒) です (圧縮ファイルは 1 つのファイルとして扱われません。この時間制限は最終的に個々のファイルに適用され、上位レベルのコンテナ ファイルには適用されません)。
ウイルス検出時 : ■ 駆除 ■ 削除 ■ 通知	オンアクセス スキャナの基本アクションを選択します。
駆除に失敗した場合またはファイルが使用不能な場合に削除	選択したスキャナで実行する 2 番目のアクションとして選択します。この機能は基本アクションが「**駆除**」に設定されている場合にのみ有効です。

5 環境設定が変更されないようにするには「**ロック**」をクリックします。

6 「**環境設定**」ダイアログ ボックスの左上端にある「**閉じる**」をクリックします。

オンデマンド スキャナを使用する

オンデマンド スキャナを使用すると、次の方法でいつでもスキャンを開始できます。

- Dock の「**VirusScan**」アイコン、Finder の「**VirusScan**」アイコン、またはコンソールのドラッグ アンド ドロップ ペインにファイルをドラッグ アンド ドロップする。
- 「**スキャンおよび駆除するファイルまたはフォルダを選択**」ダイアログ ボックスを使用する。

ファイルやディレクトリは複数選択できます。結果はレポート ウィンドウにまとめて表示されます。

オンデマンド スキャンを実行するには

1 VirusScan コンソールを開きます。

2 スキャンするファイル、フォルダ、ボリュームを、メイン コンソールのドラッグ アンド ドロップ ペインにドラッグ アンド ドロップします。複数のファイルを選択するには、次のいずれかの操作を行います。

   - **Shift** キーを押しながら必要なファイルをすべて選択します。
   - ドラッグ アンド ドロップ ペインをクリックします。ファイル選択画面が表示されます。スキャンするファイル、ファイル グループ、ディレクトリ、ボリュームを選択し、「**場所の選択**」をクリックします。
   - ファイル、フォルダ、ボリュームを、**Finder** ビューで Dock の「**VirusScan**」アイコンにドラッグします。

3 コンソールで「**開始**」をクリックして、スキャンを開始します。

ステータス ラインに、スキャン中のファイルの名前およびスキャンのステータスが表示されます。ステータス ラインの横にある**矢印**は、**レポート** ウィンドウの表示 / 非表示を切り替えます。**レポート** ウィンドウはデフォルトで非表示になっています。

スキャン レポートが**レポート** ウィンドウに表示されます。レポートには、スキャンの時刻、スキャンされたファイル数、実行されたアクションが表示されます。コンソールには、スキャンのステータスがドラッグ アンド ドロップ ペインとレポート パネルの間に 1 行で表示されます。スキャン実行時以外には、ステータス パネルに「**アイドル**」と表示されます。

オンアクセス スキャナを使用する

オンアクセス スキャナを使用すると、複数のファイル、ディレクトリ、およびボリューム (ネットワークに接続しているリモート コンピュータ上のボリュームを含む) に対して、継続的かつ自動的にポリシーが実行されます。オンアクセス スキャナは、有効にするだけで実行されます。

オンアクセス スキャンを有効にするには

1 VirusScan コンソールを開きます。

2 ツール バーで「**環境設定**」 をクリックして、「**環境設定**」ダイアログ ボックスを表示します。

3 「**オンアクセス スキャン**」チェックボックスをオンにして、オンアクセス スキャンを有効にします。

ウイルスまたはその他の悪質なコードが検出されると、**Reporter** のポップアップ ウィンドウが表示されます。

DAT ファイルをアップデートする

eUpdate は、インターネット接続を介して eUpdate サーバに自動的に接続し (デフォルトでは毎日)、新しい DAT ファイルをチェックします。アップデートは、プロキシ サーバを迂回できます。eUpdate でアップデートをチェックするスケジュールは、**VirusScan Schedule Editor** を使用して設定できます。

自動的に実行するようにスケジュール設定された eUpdate とオンデマンド スキャンは、同時に実行できます。

アップデートが必要な理由

最新のウイルスの脅威からシステムを保護するには、DAT ファイルとエンジンを定期的にアップデートして、ウイルス対策ソフトウェアを常に最新の状態に維持する必要があります。

- 新しいウイルスやワームは、頻繁に発生しています。弊社ではアップデートした DAT ファイルを定期的にリリースすることにより、VirusScan でこのような新しいウイルスやワームを検出できるようにしています。
- ウイルス スキャン エンジンがアップグレードされる場合があります。これにより、VirusScan で最新のウイルス検出技術を使用できます。

eUpdate のしくみ

eUpdate では、インターネットに接続中に新しい DAT ファイルやアップグレードを取得して、ご使用のウイルス対策ソフトウェアに適用することができます。アップデートがある場合は、VirusScan は自動的にアップデートをダウンロードおよびインストールしようとします。アップデートを実行せずに 1 日が経過すると、VirusScan は自動的にアップデートをダウンロードします。これにより、システムを常に最新の状態に保つことができます。

eUpdate を設定する

DAT ファイルは、FTP サーバからアップデートできます。eUpdate を使用して DAT ファイルをアップデートするために、弊社では FTP サーバを提供しています。

弊社の FTP サーバ

デフォルトでは、VirusScan は弊社の FTP サーバにアクセスして最新の DAT ファイルをダウンロードするように設定されています。VirusScan をインストールすると、インターネットに接続している間に VirusScan が自動的にこの FTP サーバに接続し、DAT ファイルをダウンロードしてアップデートします。

内部 FTP サーバを設定する

ネットワーク上の Macintosh コンピュータ用に内部 FTP の eUpdate リポジトリを使用するには、内部 FTP eUpdate サーバを設定する必要があります。この場合、弊社の FTP サーバ (`ftp://ftp.mcafee.com/commonupdater`) から、設定した内部 FTP サーバに、DAT ファイルを毎日ダウンロードする必要があります。

内部 FTP サーバを設定するには

1 `ftp://ftp.mcafee.com/commonupdater` から DAT ファイルをダウンロードします。

2 FTP eUpdate サーバ上のフォルダにダウンロードした DAT ファイルをコピーします。

「環境設定」から FTP サーバにアクセスするには

1 VirusScan コンソールを開き、「**eUpdate サーバ設定**」ダイアログ ボックスで設定を変更します。

2 ツール バーで「**環境設定**」をクリックします。「**環境設定**」ダイアログ ボックスが表示されます。「**eUpdate サーバの設定をカスタマイズ**」オプションを選択します。

3 「**カスタマイズ**」ボタンをクリックします。「**eUpdate サーバ設定**」ダイアログ ボックスが表示されます。

4 「**サーバの URL**」に、内部 FTP サーバの URL を入力します。

5 「**ディレクトリ**」に、DAT ファイルをダウンロードした場所を入力します。

6 「**OK**」をクリックします。

例 :

1 内部 FTP サーバの最上位のディレクトリの下に、"commonupdater" という名前のディレクトリを作成します。

2 `ftp://ftp.mcafee.com/commonupdater` を開きます。

3 以下のファイルを、`ftp://ftp.mcafee.com/commonupdater/` から `<内部 FTP サーバ>/commonupdater/` にダウンロードします。

- oem.ini
- .gem ファイルすべて
- gdeltaavv.ini

4 `ftp://ftp.mcafee.com/commonupdater/current/VSCANDAT1000/DAT/0000/avvdat-xxxx.zip` を `<内部 FTP サーバ>/commonupdater/current/VSCANDAT1000/DAT/0000/` にダウンロードします。

5 ウイルス定義は毎日アップデートされます。今後、ローカル アップデート リポジトリを常に最新の状態に維持するには、手順 1 から 4 を毎日繰り返す必要があります。

プロキシ サーバを使用した eUpdate の実行方法

WebProxy (HTTP) プロキシの設定がサポートされています。Max OS X でこれらのプロキシを設定する方法については、Apple のマニュアルを参照してください。

また、eUpdate を機能させるには、FTP サーバ上で匿名アクセスを有効にする必要があります。

VirusScan では、プロキシ サーバ認証はサポートされていません。

VirusScan Schedule Editor を使用する

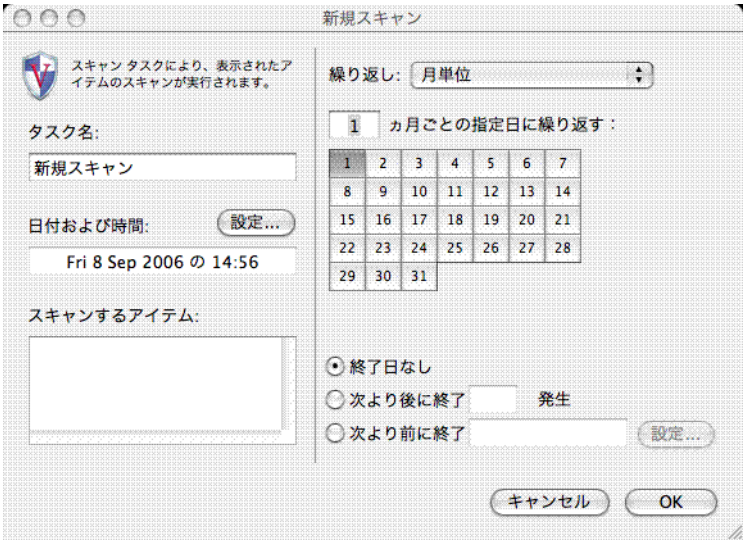
VirusScan Schedule Editor では、ファイルやフォルダの一定のグループに対して繰り返し実行するスキャンのスケジュールを設定できます。スキャンは、日単位、週単位、月単位でスケジュール設定できます。

スキャンのスケジュールを設定するには

1 VirusScan コンソールで「**スケジューラ**」をクリックします。または、「**表示**」メニューから「**スケジュール タスク**」を選択します。「**VirusScan Schedule Editor**」ダイアログ ボックスが表示されます。

2 「**新規スキャン タスク**」 をクリックします。「**名称未設定**」ダイアログ ボックスが表示されます。

図 3-5「 新規スキャン」ダイアログ ボックス



3 タスクに名前を付けます。スケジュールを設定するスキャンの内容を示す名前にしてください。

4 「**設定**」をクリックして、スケジュール設定するスキャンの「**日付および時間**」を指定します。

5 スキャンするアイテムを選択します。次の方法で選択できます。

- 項目を「**スキャンするアイテム**」ペインにドラッグ アンド ドロップします。
- 「**スキャンするアイテム**」ペインをクリックします。「**アイテムの選択**」ダイアログ ボックスが表示されます。スキャンするファイルをすべて選択したら、「**選択**」をクリックします。

6 「**繰り返し**」を選択します。次のいずれかを選択してください。

- **日単位** : スキャンを実行する日を入力します (複数入力可)。
- **週単位** : スキャンを実行する曜日を選択します (複数選択可)。
- **月単位** : スキャンを実行する月と日を選択します (複数選択可)。
- **なし** : スキャンを再実行しない場合は、このオプションを選択します。

7 スケジュールを終了するタイミングを指定し、「**OK**」をクリックします。

VirusScan Schedule Editor のスケジュール設定されたスキャンと eUpdate のリストに、新しいスキャン タスクが追加されます。スケジュール タスクを有効または無効にするには、タスク項目の横のチェックボックスを選択します。

スケジュール タスクが実行されるときにコンピュータの電源がオフになっている場合、VirusScan では、コンピュータの電源を再度入れてもそのタスクは実行されません。

eUpdate のスケジュールを設定する

VirusScan Schedule Editor では、コンピュータの DAT ファイルとウイルス スキャン エンジンのアップデートを繰り返し実行するようにスケジュールを設定することができます。この機能は、FTP を通してサポートされます。

eUpdate は、独自の設定でアップデート ファイルを確認するようプログラムされていますが、確認頻度を増やしたり、既存のスケジュールを変更することも可能です。

eUpdate のスケジュールを設定するには

1 「**表示**」メニューから「**スケジュール タスク**」を選択します。「**VirusScan Schedule Editor**」ダイアログ ボックスが表示されます。

2 「**新規 eUpdate タスク**」をクリックします。  「 **名称未設定**」ウィンドウが表示されます。

図 3-6「 新規 eUpdate」ダイアログ ボックス

3 タスク名を入力します。スケジュールに設定するタスクの内容が分かる名前にすることをお勧めします。

4 「**設定**」をクリックして、アップデートを実行する「**日付および時間**」を指定します。

5 「**繰り返し**」を選択します。次のいずれかを選択してください。

- **日単位** : eUpdate を実行する日を入力します (複数入力可)。
- **週単位** : eUpdate を実行する曜日を選択します (複数選択可)。
- **月単位** : 自動アップデートを実行する月と日を選択します (複数選択可)。
- **なし** : 自動アップデートを再実行しない場合は、このオプションを選択します。

6 終了日を選択し、「**OK**」をクリックします。

VirusScan Schedule Editor のスケジュール設定されたスキャンと eUpdate のリストに、新しい eUpdate タスクが追加されます。eUpdate タスクを有効 / 無効にするには、タスク項目の横の該当するチェックボックスを選択します。アップデート ファイルが利用可能になると、eUpdate が自動的に開始されます。

スケジュール未設定の eUpdate を開始するには

1 VirusScan コンソールを開きます。

2 「**eUpdate**」タブをクリックして、eUpdate ペインに切り替えます。

3 「**開始**」をクリックして、ダウンロードできる新しいウイルス定義があるかどうかチェックします。

4 ePolicy Orchestrator 3.6 との統合

概説

ここでは、McAfee ePolicy Orchestrator® 管理ソフトウェアのバージョン 3.6 と 3.6.1 を使用して、VirusScan for Mac を設定する方法について説明します。このマニュアルの情報を効果的に活用するには、ePolicy Orchestrator について把握しておく必要があります。詳細については、『ePolicy Orchestrator 製品ガイド』を参照してください。ePolicy Orchestrator ソフトウェアを使用すると、弊社のウイルス対策製品を一元管理することができます。企業環境で、ウイルス対策ポリシーの管理、ウイルス イベントとウイルス活動のレポートの表示を行うことが可能になります。ePolicy Orchestrator を使用すると、ネットワークを介して他のシステム上の VirusScan for Mac を設定できます。各システムを個別に設定する必要はありません。

ここでは次の内容について説明します。

- ePolicy Orchestrator サーバに ePolicy Orchestrator エージェント設定を追加する。
- 対象のシステムにウイルス対策ポリシーを設定して、以下の VirusScan for Mac 機能を設定する。
  - VirusScan for Mac の全体的な動作を設定する全般ポリシー
  - eUpdate サーバのポリシー
  - オンデマンド スキャナのポリシー
  - オンアクセス スキャナのポリシー
- Macintosh コンピュータ用に ePolicy Orchestrator エージェント機能を設定する。
  - エージェントの通信間隔
  - ポリシーの施行間隔
  - イベント転送
  - ログ .

このマニュアルでは、ePolicy Orchestrator のインストール方法や使用方法の詳細については説明していません。『ePolicy Orchestrator 製品ガイド』を参照してください。

ePolicy Orchestrator を使用して VirusScan for Mac を管理するための必要事項

ePolicy Orchestrator を使用して VirusScan for Mac を管理する前に、以下を行う必要があります。

- ePolicy Orchestrator ソフトウェア リポジトリ内に VirusScan for Mac 用の適切な Network Associate Package (.NAP) ファイルをチェックインする。
- ePolicy Orchestrator リポジトリに Non-Windows Agent (NWA) ファイルをチェックインする。

> NWA (Non- Windows Agent) は、ePolicy Orchestrator Agent for Mac OS X とも呼ばれます。

- ご使用の Macintosh コンピュータに ePolicy Orchestrator エージェントをインストールする。

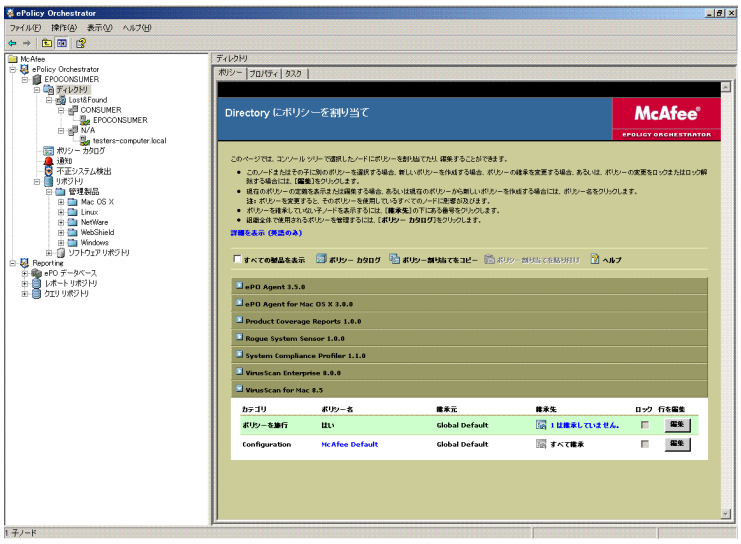
ePolicy Orchestrator コンソールの紹介

ePolicy Orchestrator 製品とその機能とのインターフェースは MMC (Microsoft Management Console) です。ここでは、ePolicy Orchestrator を通して管理する VirusScan for Mac ウイルス対策製品の登録と設定を行います。このコンソールでは、標準の MMC 機能が使用されています。

コンソールは、上下左右のペインに分かれています。

- コンソール ツリーは、コンソールのナビゲーション ペインです。この部分には、ユーザが ePolicy Orchestrator を使用して管理できるサーバ、ワークステーション、アプライアンスが表示されます。
- コンソールの右側には詳細ペインが表示されます。コンソール ツリーで選択したアイテムに応じて、詳細ペインは上部詳細ペインと下部詳細ペインに分割されます。

図 4-1 ePolicy Orchestrator コンソール



サーバに初めてログオンすると、コンソールが開き、左側のペインの**コンソール ルート**がハイライト 表示されます。

コンソールの状態は、コンソール ツリーや詳細ペインで選択したアイテムによって変わります。

ePolicy Orchestrator の使用方法の詳細については、『ePolicy Orchestrator 製品ガイド』を参照してください。

インストール

概説

Non-Windows Agent は ePolicy Orchestrator の分散コンポーネントであり、これをネットワーク上の各 Macintosh コンピュータにインストールする必要があります。エージェントは、ePolicy Orchestrator のサーバとリポジトリの間で情報を収集して送信し、ネットワークを介して VirusScan のインストール環境を管理します。エージェントやポリシーの設定内容によって、各環境での通信方法やアップデート方法は異なります。

システム要件

エージェントは、以下のいずれかの Macintosh プラットフォーム上の、Apple Macintosh OS X オペレーティング システムのバージョン 10.4.6 (以降) にインストールできます。

- G3
- G4
- G5
- SMP (デュアル プロセッサ)
- Intel ベースの Macintosh コンピュータ

VirusScan 管理用の NAP ファイルをチェックインする

ePolicy Orchestrator を通して VirusScan を管理するには、まず、この製品の .NAP ファイルを ePolicy Orchestrator サーバ上のソフトウェア リポジトリに追加する必要があります。.NAP ファイルには、VirusScan ポリシー ページが含まれており、ユーザはそこから、ePolicy Orchestrator エージェントを通して、クライアント コンピュータに配備する製品設定を制御することができます。

弊社では、ePolicy Orchestrator でサポートされるすべてのウイルス対策およびセキュリティ製品の .NAP ファイルをリリースしています。特定の製品の .NAP ファイルは、製品の他のインストール ファイルとセットになっています。これらのファイルは製品 CD に含まれています。弊社 Web サイトからインストール ファイルをダウンロードした場合は、製品の .ZIP ファイルに含まれています。VirusScan 用の .NAP ファイルは、製品 CD または製品の .ZIP ファイルの **ePolicy Orchestrator Server Components** サブフォルダに格納されています。.NAP ファイル名は、NWA-MAC300.NAP のように、製品名コード、バージョン番号、.NAP 拡張子で構成されています。

ポリシー ページはマスタ リポジトリには追加されず、ePolicy Orchestrator サーバに格納されます。このため、NAP ファイルが分散リポジトリに複製されたり、Macintosh コンピュータにアップデートされることはありません。

Macintosh 用 Non-Windows Agent NAP ファイル (NWA-MAC300.NAP) を追加する

Macintosh 用 Non-Windows Agent .NAP ファイルを ePolicy Orchestrator サーバにチェックインするには

1 製品 CD または弊社 Web サイトからダウンロードしたインストール .ZIP ファイルで **NWA-MAC300.NAP** ファイルを探し、ePolicy Orchestrator サーバからアクセス可能な一時フォルダに保存します。

2 管理者権限で ePolicy Orchestrator サーバにログオンします。

3 ePolicy Orchestrator コンソール ツリーで、「**リポジトリ**」を右クリックし、「**リポジトリの設定**」を選択します。「**ソフトウェア リポジトリの設定**」ウィザードが表示されます。

または、ePolicy Orchestrator のコンソール ツリーで「**リポジトリ**」をダブルクリックしてから、詳細ペインで「**NAP のチェックイン**」をクリックします。

4 「**新しく管理対象のソフトウェアを追加する**」を選択して、「**次へ**」をクリックします。

5 「**ソフトウェア パッケージの選択**」ダイアログ ボックスで、36 ページの手順 1 で一時フォルダに保存した **NWA-MAC300.NAP** ファイルを検索して選択します。

6 「**開く**」をクリックすると、選択した .NAP ファイルを ePolicy Orchestrator が読み込みます。

VirusScan for Mac NAP ファイル (Virex.nap) を追加する

Virex.nap ファイルを ePolicy Orchestrator サーバに追加するには

1 製品 CD または弊社 Web サイトからダウンロードしたインストール .ZIP ファイルで **Virex.nap** ファイルを探し、ePolicy Orchestrator サーバからアクセス可能な一時フォルダに保存します。

2 管理者権限で ePolicy Orchestrator サーバにログオンします。

3 ePolicy Orchestrator コンソール ツリーで、「**リポジトリ**」を右クリックし、「**リポジトリの設定**」を選択します。「**ソフトウェア リポジトリの設定**」ウィザードが表示されます。

4 「**新しく管理対象のソフトウェアを追加する**」を選択して、「**次へ**」をクリックします。

5 「**ソフトウェア パッケージの選択**」ダイアログ ボックスで、36 ページの手順 1 で一時フォルダに保存した **Virex.nap** ファイルを検索して選択します。

6 「**開く**」をクリックすると、選択した .NAP ファイルを ePolicy Orchestrator が読み込みます。

VirusScan for Mac レポート用 NAP ファイル (virexExt.nap) を追加する

virexExt.nap ファイルを ePolicy Orchestrator サーバに追加するには

1 製品 CD または弊社 Web サイトからダウンロードしたインストール .ZIP ファイルで **virexExt.nap** ファイルを探し、ePolicy Orchestrator サーバからアクセス可能な一時フォルダに保存します。

2 管理者権限で ePolicy Orchestrator サーバにログオンします。

3 ePolicy Orchestrator コンソール ツリーで、「**リポジトリ**」を右クリックし、「**リポジトリの設定**」を選択します。「**ソフトウェア リポジトリの設定**」ウィザードが表示されます。

4 「**レポートを追加する**」を選択して、「**次へ**」をクリックします。

5 「**ソフトウェア パッケージの選択**」ダイアログ ボックスで、「VirusScan for Mac レポート用 NAP ファイル (virexExt.nap) を追加する」の手順 1 で一時フォルダに保存した **virexExt.nap** ファイルを検索して選択します。「**開く**」をクリックすると、レポート用 .NAP ファイルを ePolicy Orchestrator がリポジトリに読み込みます。

.NAP ファイルのすべての読み込みが完了すると、詳細ペインのポリシー リストにエージェントが表示されます。

Macintosh コンピュータ用 ePolicy Orchestrator エージェントをインストールする

Macintosh コンピュータ用の ePolicy Orchestrator エージェントは、標準インスト ール (グラフィカル インターフェース) またはコマンド ラインからのインスト ール (サイレント インスト ール) のいずれかの方法でインスト ールできます。エージェントは `/Library/NETAepoagt` ディレクトリにインスト ールされます。また、設定に関連するデータは `/Library/NETASSOC` ディレクトリにインスト ールされます。

ePolicy Orchestrator エージェントのインストール ディレクトリは変更できません。

標準インストール

1 製品 CD または弊社 Web サイトからダウンロードしたインストール .ZIP ファイルで、**nwa.dmg** ファイルを探し、一時フォルダに保存します。

製品 CD では、**nwa.dmg** は **ePO Components.ZIP** ファイル内の **ePO Agent** フォルダにあります。

2 **nwa.dmg** ファイルをダブルクリックします。以下のファイルが表示されます。

- NWA.pkg
- cmdinstall

3 **NWA.pkg** ファイルをダブルクリックします。「**ようこそ ePO Agent for Mac OS X インストールへ**」ウィンドウが表示されます。

4 「**続ける**」をクリックします。「**大切な情報**」ウィンドウが表示されます。ここには、エージェントの機能、製品リリースに関する既知の動作や問題などの説明が表示されます。

5 「**続ける**」をクリックします。「**ソフトウェア使用許諾契約**」ウィンドウが表示されます。

使用許諾契約を読み、同意します。この使用許諾契約に同意しないと、インストールを続行できません。

6 「**続ける**」をクリックします。「**インストール先を選択**」ウィンドウが表示されます。ePolicy Orchestrator エージェントをインストールするボリュームを選択し、「**続ける**」をクリックします。

7 「**簡易インストール**」ウィンドウが開きます。

エージェントをインストール / 再インストールするか、アップグレードするかによって、2 種類の ウィンドウがあります。初めてエージェントをインストールする場合や、以前にインストールした ePolicy Orchestrator エージェントをアンインストールした後に再インストールする場合、このウィンドウには、「**インストール**」ボタンが表示されます。ePolicy Orchestrator エージェントのこれまでのバージョンをアップグレードする場合、このウィンドウには、「**アップグレード**」ボタンが表示されます。

8 「**インストール**」または「**アップグレード**」をクリックして、次に進みます。

9 認証情報の入力を求めるプロンプトが表示されます。パスワードを入力して、「**OK**」をクリックします。「**ソフトウェアをインストール**」ウィンドウが表示されます。

このプロセス中に、**ePO Agent Configurator** の認証情報の入力を求めるプロンプトが表示されます。パスワードを入力して、「**OK**」をクリックします。「**ePO Agent Configurator**」ダイアログ ボックスが表示されます。

10 「**ePO Server の IP アドレス**」と「**ePO Server のポート番号**」に値を入力します。「**適用**」をクリックします。「**ソフトウェアをインストール**」ウィンドウが表示されます。

11 「**再起動**」をクリックしてインストール プロセスを完了します。

サイレント インストール (コマンド ライン)

1 製品 CD または弊社 Web サイトからダウンロードしたインストール .ZIP ファイルで、**nwa.dmg ファイル**を探し、一時フォルダに保存します。

製品 CD では、**nwa.dmg** は **ePO Components.ZIP** ファイル内の **ePO Agent** フォルダにあります。

2 **nwa.dmg** ファイルをダブルクリックします。以下のファイルが表示されます。

- NWA.pkg
- cmdinstall

3 「**Terminal**」ウィンドウを開き、作業ディレクトリを `/Volumes/NAINWA` に変更します。

このコマンドを実行するには、管理者権限が必要です。

4 「**Terminal**」ウィンドウで次のように実行します。

```
sudo ./cmdinstall <ePO Sever の IP アドレス>:<ePO Server のポート番号>
```

5 サイレント インストールが終了すると、「**Terminal**」ウィンドウに次のように表示されます。

図 4-2「 Terminal」ウィンドウ ー インスト ール / アップグレード の終了

```
installer[661]:                         It took 3.385372 seconds to run preupgrade script for ePO Agent for Mac OS X
installer[661]:                         It took 0.445282 seconds to Write files
installer[661]:                         It took 3.174604 seconds to run postupgrade script for ePO Agent for Mac OS X
installer[661]:                         It took 0.098582 seconds to Assembling receipt
installer[661]:
installer[661]: Summary Information
installer[661]: Type           Elapsed time (sec)
installer[661]:          patch           0.000117
installer[661]:           zero           0.010520
installer[661]:         script           6.559976
installer[661]:        extract           0.445282
installer[661]:         config           0.065356
installer[661]:        receipt           0.433727
installer[661]:           disk           1.006918
installer[661]:        install           7.509475
installer[661]:
installer[661]: Starting installation:
installer[661]: Finalizing installation.
#
installer:     Finishing Installation
installer[661]: Registering applications
installer[661]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
#
installer:
#
installer: The software was successfully installed.....
installer: The upgrade was successful.
installer: The install recommends restarting now.
Cleaning /tmp/NAINWA.mpnlThby
iMac-Mactel-2:/Volumes/NAINWA shreyas$
```

これで、ePolicy Orchestrator Agent for Mac OS X のインストール / アップグレードは正常に終了しました。

VirusScan for Mac のインストール

Macintosh コンピュータ上でのこの製品のインストールの詳細については、13 ページの「VirusScan for Mac のインストール」を参照してください。

アンインストール

VirusScan for Mac を ePolicy Orchestrator サーバから削除する

ePolicy Orchestrator サーバから VirusScan for Mac .NAP ファイルをアンインストールできます。

VirusScan for Mac NAP ファイルを削除するには

1 対象の ePolicy Orchestrator データベース サーバにログオンします。

2 コンソール ツリーの「**リポジトリ**」、「**管理製品**」、「**MAC OS X**」の下で、「**VirusScan for Mac**」を選択します。

3 「**VirusScan for Mac**」を右クリックし、「**削除**」を選択して ePolicy Orchestrator サーバから VirusScan .NAP ファイルをアンインストールします。

ePolicy Orchestrator Agent for Mac OS X を ePolicy Orchestrator サーバから削除する

ePolicy Orchestrator Agent for MAC OS X を、チェックイン後に ePolicy Orchestrator サーバから削除することはできません。

ePolicy Orchestrator エージェントを VirusScan for Mac から削除する

Macintosh コンピュータから ePolicy Orchestrator エージェントをアンインストールできます。

コマンド ラインを使用して ePolicy Orchestrator エージェントをアンインストールするには

1 管理者権限でログインします。

2 `/Library/NETAepoagt` ディレクトリに移動します。

3 `cmduninst` を実行します。

ePolicy Orchestrator でポリシーを設定する

ePolicy Orchestrator コンソールでは、コンピュータ グループ全体や単一のコンピュータに対してポリシーを施行することができます。個々のコンピュータで行われた設定は、これらのポリシーで上書きされます。

ポリシーを設定する前に、VirusScan for Mac のポリシーを変更するコンピュータ グループを選択してください。VirusScan for Mac のポリシーは、ePolicy Orchestrator コンソールの詳細ペインに表示されるページやタブで変更することができます。これらのページは、VirusScan for Mac のユーザ インターフェースから直接アクセスできるページとほとんど同じです。

該当するポリシーを変更して、対象のコンピュータまたはコンピュータ グループに対して変更を保存すると、ePolicy Orchestrator エージェントを介して新しい設定を配備できるようになります。

ePolicy Orchestrator で VirusScan for Mac のポリシーを変更するには

1 対象の ePolicy Orchestrator サーバにログオンします。

2 コンソール ツリーの「**ePolicy Orchestrator**」の <**サーバ**> の下にある「**ディレクトリ**」で、ポリシーの対象となるサイト、グループ、単一のコンピュータ、またはディレクトリ全体を選択します。詳細ペインに「**ポリシー**」タブ、「**プロパティ**」タブ、および「**タスク**」タブが表示されます。

3 詳細ペインで「**ポリシー**」タブを選択し、「**VirusScan for Mac 8.6**」を展開します。「**ポリシー**を**施行**」と「**VirusScan ポリシー**」が「**VirusScan for Mac 8.6**」エントリの下に表示されます。

4 「**ポリシー名**」の下で、デフォルトのポリシー設定を表示する「**カテゴリ**」に対して「**McAfee デフォルト**」をクリックします。

選択した「**カテゴリ**」に対して、「**McAfee デフォルト**」のポリシー設定を変更することはできません。選択したカテゴリを設定するには、選択した「**カテゴリ**」の新しいポリシーを作成する必要があります。

カテゴリのポリシーを新規作成するには

1 ePolicy Orchestrator 詳細ペインで、「**VirusScan for Mac 8.6**」エントリの 1 つの「**カテゴリ**」で、「**編集**」をクリックします。

2 「**ポリシー名**」ドロップダウン リストをクリックして、「**新規ポリシー**」を選択します。「**ポリシーの新規作成**」ダイアログ ボックスが表示されます。

ポリシー オプションの新規作成

次のポリシー オプションを複製	選択した「**カテゴリ**」のポリシーの複製を作成します。ドロップダウン リストからポリシーを選択します。
すべてのタブを継承するポリシーを作成	すべてのポリシー タブ設定を継承する新しいポリシーを作成します。
新規ポリシー名	「**カテゴリ**」に対して作成する新しいポリシーの名前を入力します。

3 作成するポリシーで必要に応じてオプションを設定し、「**OK**」をクリックして、ポリシーを新規作成します。

4 「**適用**」をクリックして設定を保存します。

既存のポリシーを編集するには

1 ePolicy Orchestrator 詳細ペインの「**VirusScan for Mac 8.6**」のエントリで、選択した「**カテゴリ**」の  をクリックします。

2 必要に応じてオプションを設定し、「**適用**」をクリックしてポリシーを保存します。

ポリシーを施行するには

1 ePolicy Orchestrator の VirusScan for Mac のエントリで、「**ポリシーの施行**」の「**編集**」をクリックします。

2 「**ポリシー名**」ドロップダウン リストをクリックして、「**はい**」を選択します。

3 「**適用**」をクリックして、設定したポリシーを施行します。

「全般」タブ

「**全般**」タブでは、VirusScan for Mac の機能全般を制御する全般ポリシーを設定できます。制御できる機能には、ウイルス定義のアップデートの自動確認、オンアクセス スキャンの実行、スキャン結果のログ記録、特定のディスク、ファイルおよびフォルダの除外リストの作成などがあります。

以下の全般ポリシーを設定することができます。

ウイルス定義のアップデートを自動的に確認する	自動 eUpdate を有効 / 無効にします。
オンアクセス スキャン	オンアクセス スキャンを有効 / 無効にします。
結果をファイルに記録	ファイルへの結果の記録を有効 / 無効にします。
特定のディスク、ファイル、およびフォルダを除外	ここにリストされた項目をスキャンから除外します。このオプションが選択されていない場合は、スキャナは除外リストを無視します。 除外項目の追加 : ■ 「**追加**」をクリックすると、「**スキャン項目の追加 -- Web ページ**」ダイアログが表示されます。除外対象のファイル、ディレクトリ、またはディスクの完全なパスを入力して、「**OK**」をクリックします。除外する項目が「**除外リスト**」に表示されます。 除外項目の削除 : ■ 「**除外リスト**」で除外する項目を選択して、「**削除**」をクリックします。 除外項目の編集 : ■ 「**除外リスト**」で除外する項目を選択して、「**編集**」をクリックします。

「eUpdate」タブ

「**eUpdate**」タブでは、DAT とウイルス スキャン エンジンのアップデート設定をカスタマイズできます。eUpdate を使用すると、最新のウイルス情報とスキャン機能でウイルス対策ソフトウェアを継続的にアップデートできます。DAT ファイルとエンジン ファイルのアップデートには、FTP を使用できます。

eUpdate の設定をカスタマイズする

DAT ファイルとエンジン ファイルをアップデートするには、アップデート ファイルの転送元のサーバの詳細を指定する必要があります。

サーバの URL	DAT とエンジンのアップデートをダウンロードするサーバの URL
ポート番号	FTP に使用するポート番号
ユーザ名	各自のユーザ名
パスワード	各自のパスワード
アカウント	FTP アカウント
ディレクトリ	DAT ファイルとエンジン ファイルの格納先へのパス

「オンアクセス スキャナ」タブ

オンアクセス スキャナ」タブでは、現在使用されているすべてのファイルに対して、ウイルスなどの不審なプログラムが存在するかどうかを検査するスキャンを実行できます。スキャンは、ユーザまたはシステム プロセスによってファイルがディスクから読み取られた場合や、ディスクに書き込まれる場合、もしくはその両方で毎回実行されます。オンアクセス スキャナを使用すると、複数のファイル、ディレクトリ、ボリューム (ネットワークに接続しているリモート コンピュータ上のボリュームを含む) に対して、継続的にポリシーを施行できます。スキャン対象や、感染ファイルに対する処理を設定できます。ウイルスまたはその他の悪質なコードが検出されると、Macintosh コンピュータの **Reporter** ポップアップ ウィンドウにメッセージが表示されます。

以下のオンアクセス スキャナ ポリシーを設定できます。

アーカイブおよび圧縮ファイルのコンテンツをスキャン	スキャナが、アーカイブやその他の圧縮ファイルの内容もスキャンするように設定します。オンアクセス スキャナではデフォルトで**オフ**になっています。オンアクセス スキャナは stuffit アーカイブ内をスキャンしない点に注意してください。
未知のマクロ ウイルスを検出	感染の可能性のあるマクロ (未知のウイルス) をファイルが含んでいる場合、そのマクロもスキャンされ、駆除の一環として、駆除または削除されます。
Apple Mail メッセージのスキャン	Apple Mail メッセージをスキャンするようにスキャナを設定します。
ウイルスに似た性質のファイルを確認	ウイルスやワームに似た特徴を持ち、未知のウイルスを含んでいる恐れがあるファイルを検出するヒューリスティクスを、有効 / 無効にします。
不要なアプリケーションおよびジョーク プログラムの検索	不正なプログラムやジョーク プログラムをチェックするスキャナを有効 / 無効にします。
ネットワーク ボリューム上のファイルをスキャン	ネットワーク ボリューム上にあるファイルをスキャンするようにスキャナを設定します。
ファイルのスキャン : ■ 常時 ■ 読み取り時 ■ 書き込み時	ファイルがディスクから読み取られたとき、ディスクに書き込まれたとき、またはその両方で、スキャナがファイルをスキャンするかどうかを指定します。デフォルトでは、「**常時**」に設定され、ファイルがディスクから読み取られたときと、ディスクに書き込まれたときにスキャンされます。
ウイルス検出時 : ■ 駆除 ■ 削除 ■ 通知	ウイルスの検出時の、オンアクセス スキャナの基本アクションを選択します。
駆除に失敗した場合またはファイルが使用不能な場合に削除	ウイルスの検出時にスキャナで実行する 2 番目のアクションを選択します。この機能は基本アクションが「**駆除**」に設定されている場合にのみ有効です。
スキャンの最大時間	スキャンで 1 つのファイルをスキャンする最大時間 (秒) です。(圧縮ファイルは 1 つのファイルとして扱われません。この時間制限は最終的に個々のファイルに適用され、上位レベルのコンテナ ファイルには適用されません。)

「オンデマンド スキャナ」タブ

「オンデマンド スキャナ」タブでは、選択したファイルをコンソールにドラッグ アンド ドロップするか、「**ファイルを開く**」ダイアログ ボックスから、いつでもスキャンを実行できます。オンデマンド スキャナでは、複数のファイル、ディレクトリ、ボリュームを選択できます。スキャンの結果はレポート内に表示され、保存や印刷が可能です。スキャン対象や、感染ファイルに対する処理を設定できます。ウイルスが検出されると、メッセージが表示され、処理アクションの情報を記載したログが生成されます。

以下のオンデマンド スキャナ ポリシーを設定できます。

アーカイブおよび圧縮ファイルのコンテンツをスキャン	スキャナが、アーカイブやその他の圧縮ファイルの内容もスキャンするように設定します。オンデマンド スキャナではデフォルトで**オン**になっています。
未知のマクロ ウイルスを検出	感染の可能性のあるマクロ (未知のウイルス) をファイルが含んでいる場合、そのマクロもスキャンされ、駆除の一環として、駆除または削除されます。
Apple Mail メッセージのスキャン	Apple Mail メッセージをスキャンするようにスキャナを設定します。
ウイルスに似た性質のファイルを確認	ウイルスやワームに似た特徴を持ち、未知のウイルスを含んでいる恐れがあるファイルを検出するヒューリスティクスを、有効 / 無効にします。
不要なアプリケーションおよびジョーク プログラムの検索	不正なプログラムやジョーク プログラムをチェックするスキャナを有効 / 無効にします。
ウイルス検出時 : ■ 駆除 ■ 削除 ■ 通知	ウイルスの検出時のスキャナの基本アクションを選択します。
駆除に失敗した場合またはファイルが使用不能な場合に削除	ウイルスの検出時に選択されたスキャナで実行する 2 番目のアクションを選択します。この機能は基本アクションが「**駆除**」に設定されている場合にのみ有効です。

スキャンと eUpdate のスケジュールを設定する

VirusScan for Mac のウイルス スキャンでは、DAT ファイルの情報に基づいて、ウイルスの検知と駆除が行われます。次々と出現する新しいウイルスへの対策機能を提供するため、弊社では新しい DAT ファイルを定期的にリリースしています。確実なウイルス対策機能を施すため、ePolicy Orchestrator を使用して、VirusScan for Mac に最新の DAT ファイルの取得場所を通知すること、既存の DAT ファイルのアップデートのスケジュールを設定すること、オンデマンド スキャンを実行することなどが可能です。

ePolicy Orchestrator を使用すると、VirusScan for Mac ソフトウェアに対して次のようなタスクのスケジュールを設定することができます。

- オンデマンド スキャン
- eUpdate

コンピュータによるタスクの実行時間は、ローカル時間または GMT (グリニッジ標準時間) のいずれかで設定できます。ただし、ePolicy Orchestrator では、スケジュール タスクの進行状況を監視することはできません。サーバのログ ファイルを定期的に参照して、スケジュール タスクが正常に実行されたかどうかを確認するようにしてください。

オンデマンド スキャン

VirusScan for Mac を使用すると、ファイルに対してオンデマンド スキャンを実行して、コンピュータ上のすべてのファイルに、ウイルスやトロイの木馬、その他の悪質なコードが含まれていないかどうかを検査できます。作成できるオンデマンド スキャン スケジュールの数に制限はありません。スキャンのスケジュールを、定期的に実行されるように設定するだけでなく、ユーザが任意に実行することもできます。自動的に実行したくないスケジュールを無効することもできます。

タスクを新規作成する

1 上部詳細ペインで「**タスク**」タブをクリックします。 ペイン内で右クリックして、「**スケジュール タスク**」オプションを選択します。

2 「**新規タスク名**」フィールドにタスクの名前を入力し、作成するタスクを選択します。

3 「**タスクの種類**」ドロップダウン リストで、「**ODS**」を選択します。「**OK**」をクリックします。

作成したタスクが「**タスク**」タブに表示されます。

タスクを編集する

1 タスクを右クリックして、「**タスクの編集**」オプションを選択します。

2 「**設定**」をクリックします。「**場所**」ページが表示されるので、スケジュール設定するスキャンの対象とするファイルとディレクトリを指定します。

次のファイルとディレクトリをスキャンの対象にする	スキャン対象項目を設定します。 対象項目の追加方法 : ■ 「**追加**」をクリックすると、「**スキャン項目の追加 -- Web ページ**」ダイアログが表示されます。対象とするファイル、ディレクトリ、またはディスクの完全なパスを入力して、「**OK**」をクリックします。対象とする項目が「**対象リスト**」に表示されます。 対象項目の削除方法 : ■ 「**対象リスト**」で対象項目を選択して、「**削除**」をクリックします。 対象項目の編集方法 : ■ 「**対象リスト**」で対象項目を選択して、「**編集**」をクリックします。「**スキャン項目の追加 -- Web ページ**」ダイアログが表示されたら、スキャン対象とするファイルまたはディレクトリの完全なパスを変更して、「**OK**」をクリックします。

スケジュールの設定

3 「**スケジュールの設定**」ペインでの設定を有効にするために、「**継承**」の選択を解除します。

有効 (スケジュール タスクが指定した時刻に実行されます)	選択すると指定した時刻にタスクが実行されます。
次の時間実行されていたタスクを停止	タスクがキャンセルされるまでの最大実行時間を時間と分単位で指定します。

4 「**スケジュール**」タブをクリックすると、以下のオプションが表示されます。

スケジュール タスク	ドロップダウン リストから以下の可能なタスクの種類のいずれかを選択します。 ■ 日単位 ■ 週単位 ■ 月単位 ■ 一回のみ ■ システム起動時 ■ すぐに実行
開始時刻 ■ UTC 時間 ■ ローカル時間	スケジュール タスクの開始時刻を指定します。クライアント コンピュータのシステム時間に基づいて、定期的な間隔でタスクを実行するには、「ローカル時間」オプションを選択します。これは、オンデマンド スキャンなど、プロセッサに負荷のかかるタスクのスケジュールを営業時間外に設定する場合に有用です。 「UTC 時間」オプションを選択すると、UTC (世界協定時、GMT ともいう) に基づいてタスクが実行されます。このオプションを選択すると、Macintosh システムのローカル システム時間にかかわらず、すべての Macintosh クライアントで同時にタスクが実行されます。

指定時間内でランダムに実行	特定の開始時刻でタスクを実行せずに、指定した時刻以降にランダムにタスクを実行します。ランダムに実行するには、時間と分を指定します。
開始されなかったタスクを実行	Macintosh コンピュータのシャットダウンなどが原因で、スケジュール設定された開始時刻に実行されなかったタスクを実行します。このオプションを選択すると、Macintosh コンピュータが次に使用可能となったときにタスクが実行されます。
開始されなかったタスクの待機時間	「**スケジュールの詳細設定**」ダイアログ ボックスで「**詳細設定**」をクリックします。このオプションを選択すると、開始されなかったタスクを実行する場合、Macintosh コンピュータが使用可能となってからタスクが開始されるまでの待機時間を設定することができます。
開始日 / 終了日	「**スケジュールの詳細設定**」ダイアログ ボックスで「**詳細設定**」をクリックします。数日間や数週間などの特定の期間にタスクを実行する場合は、開始日と終了日を入力します。
タスクを繰り返す	「**スケジュールの詳細設定**」ダイアログ ボックスで「**詳細設定**」をクリックします。同じ日に何度もタスクを実行する場合、このオプションを選択します。「**タスクを繰り返す**」にチェック マークを付けて、繰り返す間隔を設定します。 通常、数多くの新しいウイルスが出現している場合など、1 日に何度もクライアント アップデート タスクを実行する必要がある場合に、このオプションを選択します。週単位や月単位などの間隔でタスクを繰り返すこともできます。
スケジュール タスク : 日単位	スケジュール タスクを実行する間隔を指定します。1 日や数日の間隔を指定できます。1 を選択した場合、スケジュール タスクは 1 日おきに実行されます。

タスクを削除する

- 「**タスク**」タブでタスクを右クリックして、「**削除**」を選択します。

eUpdate

ウイルス対策ソフトウェアは、DAT ファイルとウイルス スキャン エンジンが最新の状態でなければ、十分なウイルス対策を行うことはできません。DAT ファイルは、毎日アップデートすることをお勧めします。また、McAfee Avert Labs Web サイトで、新しい DAT ファイルがリリースされていないかを定期的に確認してください。現在のドメインに複数のサーバ (すべて VirusScan for Mac を実行) が存在する場合は、1 台のサーバに最新の DAT ファイルをダウンロードし、このサーバから他のサーバがファイルをコピーするように設定できます。サーバで実行されているオペレーティング システムにかかわらず、複数のオペレーティング システム用にファイルをダウンロードすることができます。

DAT ファイルの場所を指定する

DAT ファイルのダウンロード元の場所は「**eUpdate**」タブで指定できます。

eUpdate タスクを作成する

1 コンソール ツリーの「**ePolicy Orchestrator**」の下で、「**ディレクトリ**」または対象のサイト、グループ、ホストを右クリックし、「**スケジュール タスク**」を選択します。「**スケジュール タスク**」ダイアログ ボックスが開きます。

2 「**新規タスク名**」に名前を入力します。

3 「**ソフトウェア / タスクの種類**」リストから「**VirusScan for Mac 8.6 ー アップデート**」を選択します。

4 「**OK**」をクリックしてタスクを作成します。

eUpdate タスクを設定する

eUpdate タスクを新規作成してから、必要に応じてタスクを設定できます。

1 上部詳細ペインの「**タスク**」タブで、タスクを右クリックして「**タスクの編集**」を選択します。「**ePolicy Orchestrator スケジューラ**」ダイアログ ボックスが開きます。

2 「**設定**」をクリックして、「**タスク**」タブと「**スケジュール**」タブの両方で必要に応じてオプションを編集します。

3 「**継承**」の選択を解除します。

4 「**eUpdate を実行**」を選択してから、「**継承**」を選択します。

5 「**OK**」をクリックして「**ePolicy Orchestrator スケジューラ**」ダイアログ ボックスに戻ります。

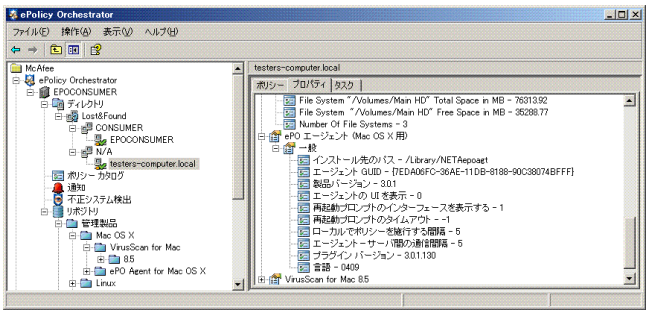
ePolicy Orchestrator のプロパティを表示する

ePolicy Orchestrator サーバから、各種システム プロパティを表示することができます。

プロパティを表示するには

1 コンソール ツリーで、設定を表示するサーバを選択します。

図 4-3 システム プロパティ



2 上部詳細ペインで「**プロパティ**」タブをクリックします。

3 「**プロパティ**」タブで、**VirusScan for Mac** ツリー表示を展開して各種プロパティを表示します。

4 詳細を表示するには、プロパティの横にある **+** 記号をクリックします。

レポート

ePolicy Orchestrator コンソールでは、VirusScan for Mac ホストによる感染の処理方法を表示するレポートの参照や、ホスト上の設定の確認をすることができます。また、特定の ePolicy Orchestrator データベースで、Non-Windows Agent によって送信されたデータを使用してレポートを作成することもできます。「**レポート入力情報を設定してください**」ダイアログ ボックスおよび「**レポート データ フィルタ**」ダイアログ ボックスでの設定は、今後の使用のために保存することができます。

VirusScan for Mac のレポートはすべて、「**ウイルス対策**」の見出しの下にあります。

ePolicy Orchestrator レポートの機能

- ディレクトリ フィルタを設定して、表示したい情報のみを収集できます。このフィルタを設定すると、ePolicy Orchestrator コンソール ツリーからレポートの対象とするサイトやグループを選択できます。
- 論理演算子を使用してデータ フィルタを設定して、レポートに含めるデータに適用するフィルタを正確に定義することができます。
- データベース内の情報をもとにグラフィック レポートを生成して、必要に応じてレポートをフィルタリングできます。レポートを印刷することや、他のソフトウェアで使用するためにエクスポートすることができます。
- コンピュータ、イベント、インストールのクエリを実行できます。

レポートを実行するには

1 対象の ePolicy Orchestrator データベース サーバにログオンします。

2 コンソール ツリーの「**レポート**」、「**ePO データベース**」、<**データベース サーバ**>、「**レポート**」、<**レポート グループ**> の下で、実行する VirusScan for Mac レポートを選択します。

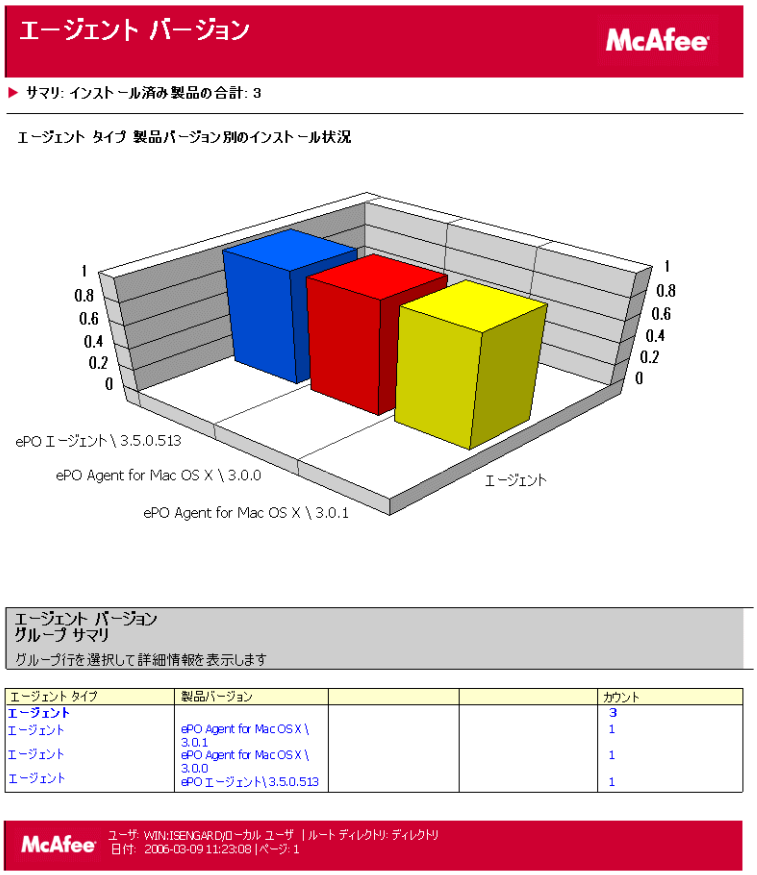
- 「**現在の保護レベル**」ダイアログ ボックスが表示された場合は、レポートを実行するウイルス定義ファイルまたはウイルス スキャン エンジンのバージョンを指定します。
- 「**レポート入力情報を設定してください**」ダイアログ ボックスが表示された場合は、表示されたタブで選択を行います。タブには、「**ルール**」、「**レイアウト**」、「**データのグループ**」、「**データの範囲**」、「**保存された設定**」の各タブがあります。

選択したレポートによって表示されるタブは異なります。表示されるすべての設定タブの詳細ついては、『ePolicy Orchestrator 製品ガイド』を参照してください。

3 生成するレポート (例えば、「**エージェント バージョン**」) を選択し、「**レポート データ フィルタ**」ダイアログ ボックスでデータ フィルタを設定します。「**OK**」をクリックします。

4 エージェント バージョンのレポートが生成されます。

図 4-4 レポート のサンプル ― エージェント バージョン



レポートを設定する

レポートに表示されるデータを制御する方法は複数あります。企業のウイルス対策およびセキュリティ プログラムに対応させるために、Macintosh クライアント コンピュータにインストールする必要のあるウイルス定義ファイル、ウイルス スキャン エンジン、およびサポートされている製品のバージョン番号を定義することができます。または、製品の基準を選択してレポート結果を制限することもできます (例えば、コンピュータ名、オペレーティング システム、ウイルス名、または感染ファイルに対して実行されたアクションなど)。

レポート結果が表示されると、このデータに対してさまざまなタスクを実行することができます。必要に応じてレポート データの詳細を表示できます (例えば、VirusScan for Mac の対応バージョンがインストールされていない Macintosh クライアント コンピュータを識別できます)。レポートによっては、サブレポートと呼ばれる他のレポートへのリンクが含まれています。サブレポートには現在のレポートに関連するデータが表示されます。レポートの印刷や、HTML、Microsoft Excel などの各種ファイル形式でレポート データをエクスポートすることもできます。

5 ePolicy Orchestrator 4.0 との統合

概説

ここでは、McAfee ePolicy Orchestrator 管理ソフトウェアのバージョン 4.0 を使用して、VirusScan を設定する方法について説明します。ここでの情報を効果的に活用するには、ePolicy Orchestrator 4.0 について把握しておく必要があります。

ePolicy Orchestrator 4.0 により、ご使用のセキュリティ製品とその製品を使用するシステムに対して、ポリシーの一元化した管理と施行をする、拡張が容易なプラットフォームが使用できます。この一元管理を通して、包括的なレポート機能や、製品配備機能も使用することができます。

このマニュアルでは、ePolicy Orchestrator のインストール方法や使用方法の詳細については説明していません。『ePolicy Orchestrator v4.0 製品ガイド』を参照してください。

拡張機能

VirusScan 拡張機能は、ePolicy Orchestrator 4.0 にあらかじめインストールされています。VirusScan 拡張機能ファイルを、ユーザがインストール、削除、管理することができます。拡張機能ファイルは、ZIP ファイル形式であり、製品やコンポーネントを ePolicy Orchestrator 4.0 で管理する前に、インストールしておく必要があります。

VirusScan 拡張機能をアンインストールした場合、拡張機能は、「**Program Files**」、「**McAfee**」、「**ePolicyOrchestrator**」、「**Extensions**」にあります。

VirusScan には、次の 2 つの拡張機能ファイルがあります。

- **VSCANMAC8600.ZIP**
- **VIREXREPORTS.ZIP**

VirusScan ポリシー拡張機能ファイルをインストールするには

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**設定**」、「**拡張機能**」、「**拡張機能のインストール**」を順にクリックします。「**拡張機能のインストール**」ダイアログ ボックスが表示されます。

3 「**参照**」をクリックし、拡張ファイル **VSCANMAC8600.ZIP** を選択して、「**OK**」をクリックします。

VirusScan レポート拡張機能ファイルをインストールするには

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**設定**」、「**拡張機能**」、「**拡張機能のインストール**」を順にクリックします。「**拡張機能のインストール**」ダイアログ ボックスが表示されます。

3 「**参照**」をクリックし、拡張ファイル **VIREXREPORTS.ZIP** を選択して、「**OK**」をクリックします。

ePolicy Orchestrator 4.0 ダッシュボードの紹介

ダッシュボードは、検出に関する現在のデータを示す、あらかじめ設定されたモニタやユーザが選択したモニタの集合です。

ePolicy Orchestrator ダッシュボードは、名前を付けたダッシュボード モニタの集合から構成されます。ユーザ アカウントに割り当てられた許可に応じて、ユーザはダッシュボードの新規作成、既存のダッシュボードの管理、アクティブ ダッシュボードの選択、ダッシュボード環境設定の編集を行うことができます。

ダッシュボードを新規作成する

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**ダッシュボード**」、「**オプション**」、「**新規ダッシュボード**」を順にクリックします。「**新規ダッシュボード**」ページが開きます。

3 「**ダッシュボード名**」に入力し、「**ダッシュボード サイズ**」のドロップダウンから適宜選択します。

4 「**新規モニタ**」をクリックします。

5 「**クエリ**」で「**カテゴリ**」を選択し、VirusScan 関連のクエリを適宜、「**モニタ**」ドロップダウン メニューから選択します。

6 「**OK**」をクリックします。

7 残りのモニタに関して、手順 4 と 5 を繰り返します。

8 「**保存**」をクリックします。「**アクティブにする**」ダイアログ ボックスが表示されます。

9 「**はい**」をクリックして、新規作成したダッシュボードをアクティブ セットに追加します。

表 5-1 ダッシュボード オプション

オプション	説明
ダッシュボード名	選択したダッシュボードの名前を指定します。
ダッシュボード サイズ	選択したダッシュボードの大きさ (ダッシュボード モニタの数) を指定します。
作成者	選択したダッシュボードを作成したユーザ名を指定します。
最終変更	選択したダッシュボードに対して、最後に変更したユーザ名と日時を指定します。
編集	ダッシュボードの名前とサイズを変更できる「**ダッシュボードの編集**」ページを表示します。
削除	選択したダッシュボードを削除します。

表 5-1 ダッシュボード オプション

オプション	説明
複製	選択したダッシュボードのコピーを作成して、保存します。これによって、同様のダッシュボードを作成するのに、最初から作成せずに、コピーして編集することができます。
パブリックにする	選択したプライベート ダッシュボードをパブリック ダッシュボード リストに追加して、許可を受けたすべてのユーザがそのダッシュボードを、パブリック ダッシュボードとして使用できるようにします。
アクティブにする	選択したダッシュボードを「ダッシュボード」タブに追加して、簡単にアクセスできるようにします。

システム

ネットワーク内のすべてのシステムを、「**システム**」タブで管理することができます。ePolicy Orchestrator を使用して管理するすべてのシステムは、「**システム ツリー**」に含まれます。このツリーは、これらのシステム上のポリシーやタスクを管理する基本インターフェースです。「**システム ツリー**」では、これらのシステムを論理グループに編成やソートすることができます。

「**システム ツリー**」のルートは「**My Organization**」です。これには、サーバが場所を判定できないシステムを保管する「**Lost&Found**」グループが含まれます。「**システム ツリー**」のセグメント (システム) をユーザが作成して管理する方法に応じて、サーバは異なる特徴に基づいて、システムを「**システム ツリー**」内に配置します。

新しいシステムの追加方法については、『ePolicy Orchestrator 4.0 製品ガイド』を参照してください。

エージェント ウェークアップ コールを送信する

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**システム**」をクリックします。

3 「**システム ツリー**」内のグループを 1 つ選択します。

4 そのグループの対象とする「**コンピュータ名**」を選択します (複数選択可)。

5 「**高度なアクション**」、「**ウェークアップ エージェント**」を順にクリックします。「**ウェークアップ エージェント**」ページが開きます。

6 「**ウェークアップ コール タイプ**」、および ePolicy Orchestrator サーバが送信するウェークアップ コールにシステムが応答する「**ランダム**」時間 (0 から 60 分) を選択します。

7 エージェントの「**製品の全プロパティを取得**」を選択して、最後のエージェント ー サーバ間通信以降に変更されたプロパティのみを送信するのではなく、全プロパティを送信します。

8 「**OK**」をクリックします。

エージェント ウェークアップ コールのステータスを表示するには、「**サーバ タスク ログ**」に移動します。

ポリシー

「**システム ツリー**」では、ポリシーの作成、編集、削除、特定のグループ / システムへの割り当てを行うことができます。

ポリシーの新規作成

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**システム**」、「**システム ツリー**」を順にクリックし、対象とするグループを 1 つ選択します。

3 「**ポリシー**」で、ドロップダウンから対象とする「**製品**」を選択します。選択した製品が管理するポリシーのリストが、下部ペインに表示されます。

4 対象とするポリシー カテゴリを探し、「**割り当ての編集**」をクリックします。「**ポリシーの割り当て : My Organization**」、「**Lost& Found**」、**(選択したグループ)** のページが表示されます。

5 「**ポリシーの新規作成**」をクリックします。「**ポリシーの新規作成**」ダイアログ ボックスが表示されます。

6 「**McAfee デフォルト**」か「**マイ デフォルト**」を選択します。

「**McAfee デフォルト**」のポリシーは、読み取り専用であり、編集、名前の変更、削除をすることはできません。

7 「**新規ポリシー名**」に入力します。

8 「**OK**」をクリックしてから、「**保存**」をクリックします。

ポリシーを施行する

グループ内の複数の管理対象システムに対して、ポリシーを施行することができます。

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**システム**」、「**システム ツリー**」を順にクリックし、対象とするグループを 1 つ選択します。

3 対象とするシステムを選択します (複数選択可)。

4 「**ポリシーの割り当て**」をクリックします。「**<n> システムにポリシーを割り当て**」ページが開きます。

5 ドロップダウンから対象とする「**製品**」、「**カテゴリ**」、および「**ポリシー**」を選択してから、「**保存**」をクリックします。

6 対象とするシステムをもう一度選択します。

7 エージェント ウェークアップ コールを送信します。

エージェント ウェークアップ コールの送信手順については、55 ページの「エージェント ウェークアップ コールを送信する」を参照してください。

VirusScan ポリシーの作成や施行、レポートの表示は、VirusScan 拡張機能ファイルの追加後に可能になります。

クライアント タスク

ePolicy Orchestrator を使用すると、管理対象システムで実行されるクライアント タスクに対して、作成、スケジュールの設定、管理を行うことができます。クライアント タスクは、「**システム ツリー**」全体、特定のグループ、または個々のシステムに対して定義することができます。

ePolicy Orchestrator 4.0 を使用すると、VirusScan ソフトウェアに対して以下のようなタスクのスケジュールを設定することができます。

- eUpdate タスク
- オンデマンド スキャン タスク

ドロップダウンに表示されるクライアント タスクは、インストールされている拡張機能ファイルによって異なります。

eUpdate タスク

ウイルス対策ソフトウェアは、ウイルス対策定義 (DAT) とウイルス スキャン エンジンが最新の状態でなければ、十分な対策を行うことはできません。DAT ファイルは、毎日アップデートすることをお勧めします。また、弊社 AVERT (Anti-Virus Emergency Response Team) Web サイトで、新しい DAT ファイルがリリースされていないかを定期的に確認してください。

eUpdate タスクを新規作成する

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**システム**」、「**システム ツリー**」を順にクリックし、対象とするグループを 1 つ選択します。

3 「**クライアント タスク**」で、eUpdate タスクを作成する対象グループを「**システム ツリー**」から選択します。

4 「**タスクの作成**」をクリックします。「**クライアント タスク ビルダ**」ページが開きます。

5 「**説明**」の下で、作成する eUpdate タスクの「**名前**」と「**注記**」に (必要に応じて) 入力します。

6 タスクの「**タイプ**」として「**eUpdate タスク (VirusScan 8.6)**」を選択して、「**次へ**」をクリックします。

7 タスクのスケジュールを適宜設定し、「**次へ**」をクリックすると、その eUpdate タスクの「**サマリー**」が表示されます。ここには、タスクの「**名前**」、「**注記**」、「**製品**」、「**タイプ**」と、「**スケジュール**」の情報が表示されます。

8 「**保存**」をクリックします。

9 エージェント ウェークアップ コールを送信します。

エージェント ウェークアップ コールの送信手順については、55 ページの「エージェント ウェークアップ コールを送信する」を参照してください。

eUpdate タスクの説明 / スケジュールを変更するには「**編集**」をクリックし、削除するには「**削除**」をクリックします。

オンデマンド スキャン タスク

作成できるオンデマンド スキャン スケジュールの数に制限はありません。スキャンのスケジュールを定期的に実行されるように設定するだけでなく、ユーザが任意に実行することもできます。

オンデマンド スキャン タスクの作成

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**システム**」、「**システム ツリー**」、「**クライアント タスク**」を順にクリックします。

3 オンデマンド スキャン タスクを作成する対象グループを「**システム ツリー**」から選択します。

4 「**タスクの作成**」をクリックします。「**クライアント タスク ビルダ**」ページが開きます。

5 「**説明**」の下で、作成するオンデマンド スキャン タスクの「**名前**」と「**注記**」に (必要に応じて) 入力します。

6 タスクの「**タイプ**」として「**オンデマンド スキャン (VirusScan 8.6)**」を選択して、「**次へ**」をクリックします。

7 「**設定**」の下で、ドロップダウンからポリシーを選択します。

8 「**次へ**」をクリックして、タスクのスケジュールを適宜設定します。

9 「**次へ**」をクリックすると、オンデマンド スキャン タスクの「**サマリー**」が表示されます。ここには、タスクの「**名前**」、「**注記**」、「**製品**」、「**タイプ**」と、「**スケジュール**」の情報が表示されます。

10 「**保存**」をクリックします。

11 エージェント ウェークアップ コールを送信します。

エージェント ウェークアップ コールの送信手順については、55 ページの「エージェント ウェークアップ コールを送信する」を参照してください。

オンデマンド スキャン タスクの説明 / スケジュールを変更するには「**編集**」をクリックし、削除するには「**削除**」をクリックします。

アンインストール

製品拡張機能を削除する

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**設定**」、「**拡張機能**」を順にクリックします。

3 拡張機能ファイル **VirusScan** を選択し、「**削除**」をクリックします。

4 オプション「**強制削除、チェックやエラー処理をバイパス**」を選択します。

5 「**OK**」をクリックします。

レポート拡張機能を削除する

1 管理者用アカウントを使用して、対象の ePolicy Orchestrator サーバにログオンします。

2 「**設定**」、「**拡張機能**」を順にクリックします。

3 拡張機能ファイル **VirusScan Reports** を選択し、「**削除**」をクリックします。

4 オプション「**強制削除、チェックやエラー処理をバイパス**」を選択します。

5 「**OK**」をクリックします。

6 トラブルシューティング

この章では、VirusScan ソフトウェアのインストールまたは使用時に発生する可能性がある問題について解決方法を紹介します。

次の内容について説明します。

よく寄せられる質問

インストール

インストーラが機能しない

VirusScan をインスト ールするプラット フォームを確認してく ださい。Mac OS X バージョン 10.4.6 (以降) または Mac OS X Leopard バージョン 10.5 が実行されている、PowerPC または Intel ベースの Mac コンピュータである必要があり ます。512 MB 以上の RAM と 45 MB 以上の空きディスク容量が必要です。または、インスト ール中に既存のウイルス対策プログラムが検出された可能性も考えられます。その場合、VirusScan を正常にインスト ールするには、既存のプログラムを削除する必要があり ます。また、VirusScan を正常に動作さ せるには、BSD サブシステムをインスト ールする必要があり ます。

インストールされる VirusScan のファイルとその場所は？

VirusScan は `/Applications` にインスト ールされます。VirusScan Schedule Editor は `/Applications/Utilities` にインスト ールされます。VirusScan Reporter は `/Library/Application Support` にインスト ールされます。DAT ファイル、動的ライブラリ 、デーモンは、`/usr/local/vscanx` にインスト ールされます。

スキャン

特定のファイルのスキャンがスキップされる

スキップされるファイルが除外リストにあるかどうかを確認し、ある場合はリストから削除してください。また、特に指定しない限り、VirusScan ではアーカイブおよび圧縮ファイルはスキャンされません。

VirusScan のファイルのスキャン中に、別のファイルをスキャンするために、ドラッグ アンド ドロップしてしまった

スキャン中は、スキャン待機キューにファイルを追加することはできません。複数の項目をドラッグすると、それらは同時にスキャン待機キューに入ります。つまり、3 つのフォルダまたはファイルをドラッグ アンド ドロップした場合、スキャナは 3 つのスキャンを実行します。複数のファイルを含む 1 つのフォルダをドラッグすると、スキャナは 1 つのスキャンを実行します。

コンピュータのスキャンが定期的に実行されない

オンデマンド スキャンのスケジュールを設定していること、オンデマンド スキャンが有効になっていること、定期的に実行されるよう設定されていることを確認してください。

ウイルスと検出

Macintosh と Windows の両方のウイルスを検出できますか？

VirusScan は、Macintosh および Windows のすべての既知のウイルスおよびワームを検出します。

スキャン項目が表示されなくなった

VirusScan では、スキャンされ、感染が検出された最初の 20 万項目のみが表示されます。

ログ ファイルが途中で切れる

ログ ファイルのサイズは最大 512 KB です。ログ ファイルのサイズが 512 KB を超えると、ファイルの名前が **VirusScan.log.0** に変更され、新しく **VirusScan.log** が作成されます。最大で 2 つのログ ファイルのバックアップが保持されます。既存のログ ファイルのコピーを確保しておきたい場合は、新しいスキャンを開始する前に、それ以前のログ ファイルを保存しておくことをお勧めします。ログ ファイルを表示するには、「**ファイル**」で「**表示**」を選択します。

一般的な情報

「環境設定」の設定を元に戻したい

望まない設定を保存してしまった場合、「**環境設定**」ウィンドウの左下にある「**デフォルトにリセット**」をクリックすると、設定をデフォルトの状態にリセットできます。一度設定した環境設定を取り消すことはできません。「環境設定」メニューの設定は、変更後直ちに保存されます。変更を行う場合、あらかじめ現在の設定内容を控えておくことをお勧めします。

過去のアップデートを利用するには

eUpdate では、現在のまたは新しいアップデートのみをサポートしています。過去のアップデートを利用することはできません。

アップデートには Macintosh のウイルス定義も含まれていますか？

eUpdate には、Macintosh と Windows の両方のウイルス定義が含まれています。

ウイルス定義 (DAT ファイル) のバージョン番号および日付を確認したい

VirusScan アプリケーションのメニュー バーで、「VirusScan」メニューから「**VirusScan について**」を選択します。DAT バージョンの日付は、DAT ファイルの作成日のみを示します。

VirusScan での DAT ファイルの自動アップデートの頻度は？

eUpdate では、インターネットを介して新しいアップデートが毎日チェックされます。McAfee ウイルス情報ライブラリの Web サイトから、毎日手動でアップデートをダウンロードすることもできます。

eUpdate サーバに接続してスケジュール未設定の eUpdate を実行できない

インターネットに接続しているかどうか確認してください。eUpdate サーバがビジー状態である可能性も考えられます。

高度なトラブルシューティング

VirusScan のインストール後に、実行中のプロセスを表示したい

実行されるプロセスは、VShieldScanManager と VShieldScanner です。

eUpdate を使用せずにウイルス定義を手動でダウンロードしたい

VirusScan コンソールのツール バーで「**ウイルス情報**」をクリックします。デフォルトのブラウザが起動し、McAfee ウイルス情報ライブラリが表示されます。画面の左端にある「**ダウンロード**」リンクをクリックして、DAT ファイルをダウンロードします。

eUpdate サーバ設定をカスタマイズしたい

1 ツール バーで「**環境設定**」をクリックして、「環境設定」ダイアログ ボックスを表示します。

2 「**高度なオプション**」をクリックします。

3 「**eUpdate サーバの設定をカスタマイズ**」オプションを選択してから、「**カスタマイズ**」をクリックします。

4 eUpdate FTP サーバ設定を指定して、「**OK**」をクリックします。

5 「**閉じる**」をクリックします。

ログ ファイルの場所は？

表 6-1 にログ ファイルのリストを示します。

表 6-1 ログ ファイル

ログ ファイル	説明	場所
VirusScan.log	VirusScan の出力が記録されています。	このログ ファイルには、`/var/log/VirusScan.log` からアクセスできます。
log	ePolicy Orchestrator エージェントの出力が記録されています。	このログ ファイルには、`/Library/NETAepoagt/scratch/etc/log` からアクセスできます。

エラー メッセージ

表 6-2 に、VirusScan アプリケーションの実行時に表示される可能性のあるすべてのエラー メッセージと、その考えられる原因を示します。

表 6-2 エラー メッセージ ― VirusScan アプリケーション

エラー番号	メッセージ	考えられる原因
1	VirusScan エンジンの初期化に失敗しました (エラー x)。	エンジンまたは DAT ファイルが破損しているか、移動 / 削除されています。再インストールしてください。
2	レポートを保存できませんでした。 ディスクに空き容量がないか、書き込むデータがない可能性があります。	レポートを保存するために必要なディスクの空き容量がない可能性があります。空き容量を増やしてから、もう一度保存してください。
3	ウイルス情報ライブラリの URL を表示できませんでした。 ブラウザが正しくインストールされていない可能性があります。	ブラウザが正しくインストールされていることを確認してください。
4	アップデートのインストール中にエラーが発生し、eUpdate が完了しませんでした。	アップデートをインストールしようとしてエラーが発生しました。eUpdate プロセスを再起動して、やり直してください。
5	アップデートの展開中にエラーが発生し、eUpdate が完了しませんでした。	インストールするアップデートを展開しようとしてエラーが発生しました。eUpdate プロセスを再起動して、やり直してください。
6	アップデートのダウンロード中にエラーが発生し、eUpdate が完了しませんでした。	アップデートをダウンロードしようとしてエラーが発生しました。サーバが現在ビジー状態である可能性があります。数分待ってから eUpdate プロセスを再起動して、やり直してください。
7	このソフトウェア製品の有効期限が近づいています。適切なウイルス対策機能を維持するには、製品をできるだけ早くアップデートすることをお勧めします。	古いバージョンの VirusScan が使用されています。VirusScan の最新バージョンにアップグレードして、ウイルスに対する確実な保護を施すことをお勧めします。
8	このソフトウェア製品の有効期限が近づいています。有効期限を過ぎると、サポート適用外になります。適切なウイルス対策機能を維持するには、製品をできるだけ早くアップデートすることが重要です。	古いバージョンの VirusScan が使用されています。VirusScan の最新バージョンにアップグレードして、ウイルスに対する確実な保護を施すことをお勧めします。
9	このソフトウェア製品は、十分なウイルス対策を提供することができません。適切なウイルス対策機能を維持するには、製品のアップデートが必要です。	古いバージョンの VirusScan が使用されています。VirusScan の最新バージョンにアップグレードして、ウイルスに対する確実な保護を施すことをお勧めします。
10	この製品にインストールされたスキャンエンジンの有効期限が近づいています。適切なウイルス対策機能を維持するには、スキャン エンジンをできるだけ早くアップデートすることをお勧めします。	VirusScan で古いバージョンのエンジンが使用されています。できるだけ早く eUpdate タスクを実行して、ウイルスに対する確実な保護を施すことをお勧めします。

表 6-2 エラー メッセージ ー VirusScan アプリケーション

エラー番号	メッセージ	考えられる原因
11	この製品にインストールされたスキャン エンジンの有効期限が近づいています。有効期限を過ぎると、サポート適用外になります。適切なウイルス対策機能を維持するには、スキャン エンジンをできるだけ早くアップデートすることが重要です。	VirusScan で古いバージョンのエンジンが使用されています。できるだけ早く eUpdate タスクを実行して、ウイルスに対する確実な保護を施すことをお勧めします。
12	この製品にインストールされたスキャン エンジンは、十分なウイルス対策を提供することができません。適切なウイルス対策機能を提供するには、スキャン エンジンのアップデートが必要です。	VirusScan で古いバージョンのエンジンが使用されています。できるだけ早く eUpdate タスクを実行して、ウイルスに対する確実な保護を施すことをお勧めします。

用語集

DAT ファイル	ウイルスやファイルに埋め込まれた不審なプログラムをウイルス対策ソフトウェアに認識させるためのウイルス定義ファイル。
EICAR	European Institute of Computer Anti-Virus Research の略。EICAR は、ウイルス対策ソフトウェアが正常にインストールされ、動作するかどうかをテストするためのファイルを開発しました。
ePolicy Orchestrator エージェント	管理対象コンピュータのバックグラウンドでタスクを実行するプログラム。ePolicy Orchestrator サーバとそのコンピュータ上のウイルス対策およびセキュリティ製品間のすべての要求を仲介し、これらのタスクのステータスをサーバに報告します。
ePolicy Orchestrator コンソール	ePolicy Orchestrator ソフトウェアのユーザ インターフェース。管理対象コンピュータをリモートから制御および監視するために使用します。
ePolicy Orchestrator サーバ	ePolicy Orchestrator ソフトウェアのバックエンド コンポーネント。
ePolicy Orchestrator データベース	ePolicy Orchestrator サーバが ePolicy Orchestrator エージェントから受信したすべてのデータ、およびサーバ上のすべての設定情報が格納されるデータベース。
ePolicy Orchestrator データベース サーバ	ePolicy Orchestrator データベースを格納しているコンピュータ。ePolicy Orchestrator サーバがインストールされているコンピュータ、または別のコンピュータの可能性があります。
ePolicy Orchestrator リモート コンソール	ePolicy Orchestrator サーバとは別のコンピュータにインストールした ePolicy Orchestrator ユーザ インターフェース。
eUpdate	eUpdate を使用すると、DAT ファイルおよびウイルス スキャン エンジンをアップデートできます。インターネットに接続している場合は、毎日新しいアップデートが自動的にチェックされます。
Extra DAT ファイル	新種のウイルスや既存のウイルスの亜種が発生した際に作成される、補足的なウイルス定義ファイル。
FTP	File Transfer Protocol の略。インターネット上の 2 つのサイト間でファイルを移動するための一般的なプロトコルです。
HTTP	HyperText Transfer Protocol の略。インターネット上でファイルを移動するためのプロトコルです。一方に HTTP クライアント プログラム、他方に HTTP サーバ プログラムが必要です。
Lost&Found グループ	**ディレクトリ**内の適切な場所が見つからないコンピュータを一時的に保管するために使用されるグループ。
McAfee ウイルス情報ライブラリ	ウイルス情報ライブラリ (http://vil.nai.com/vil/default.aspx) には、ウイルスの発生元、コンピュータへの感染経路、駆除方法に関する詳細情報が記載されています。デマメールに関する情報も記載されています

UTC 時間	Coordinated Universal Time (協定世界時) の略。経度 0 度 (グリニッジ子午線) の時間を指します。
VirusScan Schedule Editor	ウイルス定義およびソフトウェアのアップデートのスケジュールを追加して設定できます。
VirusScan コンソール	VirusScan の一般的なユーザ インターフェース。このコンソールでは、オンデマンド スキャナの設定、オンアクセス スキャナの設定、オンデマンド スキャンの実行、eUpdate の開始などが実行できます。
アクティブでないエージェント	一定の期間 ePolicy Orchestrator サーバと通信していないエージェント。
アラート	ウイルス検出などのコンピュータのアクティビティに関するメッセージや通知。定義済みの設定に従い、電子メール、ポケットベル、電話などを介してシステム管理者やユーザに自動的に送信することができます。
イベント	エージェントーサーバ間通信で交換されたデータ。管理対象コンピュータに関する情報 (ハードウェアやソフトウェアなど)、および管理製品に関する情報 (特定のポリシー設定や製品のバージョン番号など) が含まれます。
ウイルス	ファイルやプログラムを変更したり破壊する悪質なコードを含むプログラム。ユーザによるわずかな操作で増殖したり、ユーザがまったく操作しなくても増殖する場合があります。増殖したプログラムもさらに増殖します。
エージェントインスト ール パッケージ	セットアップ プログラムなど、エージェントにインストールする必要のあるファイル。
エージェントウェークアップ コール	サーバ側からエージェントーサーバ間通信を開始させる機能。
エージェント モニタ	管理対象コンピュータ上で、オプションで表示されるエージェントのユーザ インターフェース。あらかじめ設定された間隔でエージェントが実行するタスクを即座に実行することができます。
エージェントーサーバ間通信	ePolicy Orchestrator エージェントと ePolicy Orchestrator サーバ間でのデータ交換を行うための通信。通常は、エージェント側からサーバに通信が開始されます。
エージェントーサーバ間通信の間隔 (ASCI)	あらかじめ設定されたエージェントとサーバ間での通信を行う頻度。
エージェントの言語パッケージ	英語以外の言語でエージェントのユーザ インターフェースを表示するために、クライアント コンピュータに配布する必要のあるファイルのセット。
エージェントの自動アップグレード	ePolicy Orchestrator サーバ上で最新バージョンが用意されると、自動的にエージェントのアップグレードを行うプログラム。
エラー レポートユーティリティ	システムに配布された弊社製品の障害を追跡し、記録するユーティリティ。記録された情報は、分析に使用することができます。
オンアクセス スキャナ	オンアクセス スキャナは、使用されるすべてのファイルを継続的に監視して、ウイルスなどの不審なプログラムが存在するかどうかを検査します。スキャンは、ファイルがディスクから読み取られた場合、ディスクに書き込まれた場合、もしくはその両方で毎回実行されます。複数のディレクトリやボリュームをスキャンできます。
オンアクセス スキャン	使用されるファイルに、ウイルスなどの悪質なコードが存在するかどうかを調べるための継続的な検査。スキャンは、ファイルがディスクから読み取られた場合、ディスクに書き込まれた場合、もしくはその両方で毎回実行されます。複数のディレクトリやボリュームをスキャンできます。

オンデマンド スキャナ
オンデマンド スキャナを使用すると、選択したファイルをコンソールにドラッグ アンド ドロップするか、ファイルを開くダイアログ ボックスから、いつでもスキャンを実行できます。複数のファイル、ディレクトリ、およびボリュームをスキャンできます。

オンデマンド スキャン
選択されたファイルにウイルスなどの不審なプログラムが存在するかどうかを調べるためのスケジュール設定された検査。即座に実行したり、スケジュールで設定した時刻や定期的な間隔で実行することができます。

駆除、クリーン
ウイルス、トロイの木馬、ワームを検出したときにスキャナが実行するアクションの 1 つ。駆除には、ファイルからのウイルスの削除とファイルの修復、システム ファイル、システム .INI ファイルおよびレジストリからのウイルスへの参照の削除、ウイルスが生成したプロセスの終了、ファイルを感染させたマクロや Microsoft Visual Basic スクリプトの削除、トロイの木馬やワームであるファイルの削除、駆除が実行できなかったファイルの名前の変更などがあります。

グループ
コンソール ツリーに表示されるエンティティの論理的な集合で、管理を容易にするためのまとまり。グループには、他のグループやコンピュータを含めることができます。グループに IP アドレスの範囲や IP サブネット マスクを割り当てて、コンピュータを IP アドレスでソートすることができます。Windows NT ドメインをインポートしてグループを作成すると、ドメイン内のインポートされたコンピュータすべてに、自動的にエージェント インストール パッケージを送信することができます。

グローバル管理者
読み取り、書き込み、削除の許可や、あらゆる操作に対する権限を持つユーザ。インストール全体に影響する操作を行うことができるのは、グローバル管理者のユーザ アカウントのみです。

警告の優先度
通知用のアラート メッセージに対してユーザが割り当てる値。
「**重大**」、「**メジャー**」、「**マイナー**」、「**警告**」、「**通知**」の優先度を設定できます。

継承
階層内の上位のアイテムに対して定義されている設定を下位のアイテムに適用すること。

コンソール ツリー
ePolicy Orchestrator コンソールの左側のペインにある「**ツリー**」タブの内容。ここには、コンソールで使用できるアイテムが表示されます。

コンソール ツリー アイテム
ePolicy Orchestrator コンソールのコンソール ツリーにある個々のアイコン。

サーバ イベント
Windows イベント ビューアによって記録される ePolicy Orchestrator サーバ上のアクティビティ。この情報は ePolicy Orchestrator データベースには格納されないため、レポート作成に使用することはできません。

サイト
コンソール ツリーに表示されるエンティティの論理的な集合で、管理を容易にするためのまとまり。サイトにはコンピュータのグループを含めることができます。また、IP アドレスの範囲、IP サブネット マスク、場所、部門などで編成することができます。

サイレント インスト ール
ソフトウェア パッケージをサイレント モードでコンピュータにインストールする方法。ユーザの操作を必要としません。

施行
クライアント コンピュータ上で、定義済みの設定を指定された間隔で適用すること。

ジョーク プログラム
アラームを発するなどしてユーザを困らせるプログラム。ただし、悪質なコードは含まれておらず、ファイルやデータに対する実質的な破壊活動や自己複製は行いません。

上部詳細ペイン
コンソールの右上部ペイン。「**ポリシー**」タブ、「**プロパティ**」タブ、「**タスク**」タブがあります。

スキャン
ウイルスなどの不審なプログラムが存在するかどうかを調べるためのファイルの検査。

スキャン タスク
単一のスキャン イベント。

即時イベント転送
あらかじめ設定されたイベント 数に達した場合に、特定の重要度以上のイベントを ePolicy Orchestrator サーバに即座に送信すること。この通信は、エージェント ー サーバ間通信以外で行われます。

タスク
特定の時刻や指定した間隔で行うようにスケジュールが設定されたアクティビティ。オンデマンド スキャンなどの 1 回限りのものと、アップデートなどの繰り返しのものの両方があります。ポリシーと比較してください。

チェックイン
マスタ リポジトリにファイルを追加するプロセス。

デーモン
コンピュータ システムが受信したサービス要求を処理する常駐するプログラム。デーモン プログラムは、これらの要求を他のプログラムまたはプロセスに転送します。

ディレクトリ
コンソール ツリーにある ePolicy Orchestrator で管理されるすべてのコンピュータの一覧。これらのコンピュータの管理を行うプライマリ インターフェースへリンクしています。

トロイの木馬
便利で有用な機能が含まれていると見せかけて、実際は有害なペイロードが含まれているプログラム。トロイの木馬は増殖しないので、厳密にはウイルスとは言えません。

配布
中央からクライアント コンピュータにセットアップ プログラムを配布してインストールすること。

バイナリ (セットアップ) ファイル
セットアップ プログラムなど、製品にインストールする必要のあるファイル。

ファイアウォール
コンピュータとネットワークまたはインターネットとの間のフィルタとして機能するプログラム。コンピュータに送られたすべてのトラフィック (受信トラフィック) およびコンピュータから送られるすべてのトラフィック (送信トラフィック) をスキャンできます。パケット レベルでトラフィックをスキャンし、ユーザが設定したルールに基づいてブロックまたは許可します。

ブランチ
任意のアップデートの異なるバージョンを保存および配布するためのマスタ リポジトリ内の場所。

分散ソフトウェア リポジトリ
帯域幅を有効に使用しながらクライアント コンピュータにアクセスできるようにネットワーク上に配布された Web サイトまたはコンピュータの集合。分散リポジトリには、サポートされている製品やそのアップデートをクライアント コンピュータにインストールするのに必要なファイルが保管されています。

プロパティ
エージェント ー サーバ間通信で交換されたデータ。管理対象コンピュータに関する情報 (ハードウェアやソフトウェアなど)、および管理製品に関する情報 (特定のポリシー設定や製品のバージョン番号など) が含まれます。

ポリシー
ePolicy Orchestrator で定義および管理可能な各製品の設定情報。

ポリシーの施行間隔
エージェントが ePolicy Orchestrator サーバから受信した設定を施行する頻度。これらの設定はローカルで施行されるため、ポリシーの施行の間隔を大きくとる必要はありません。

マクロ
ワープロ プログラムなどのプログラムでは、マクロとは一連のコマンドを保存したもので、単一のコマンドまたはキー操作で呼び出すことができます。

リポジトリ	製品の管理に使用するポリシー ページが格納されている場所。
ログ / ログ ファイル	McAfee ウイルス対策ソフトウェアのコンポーネントのアクティビティに関する記録。ログ ファイルには、インストール、スキャン タスク、アップデート タスクの実行中に行われた処理が記録されます。
ワーム	他のドライブ、システム、またはネットワーク上で自己複製することにより広がるウイルス。他のプログラムに寄生せずに、ファイルやプログラムを変更、インストール、破壊します。

索引

McAfee®

mcafee.com