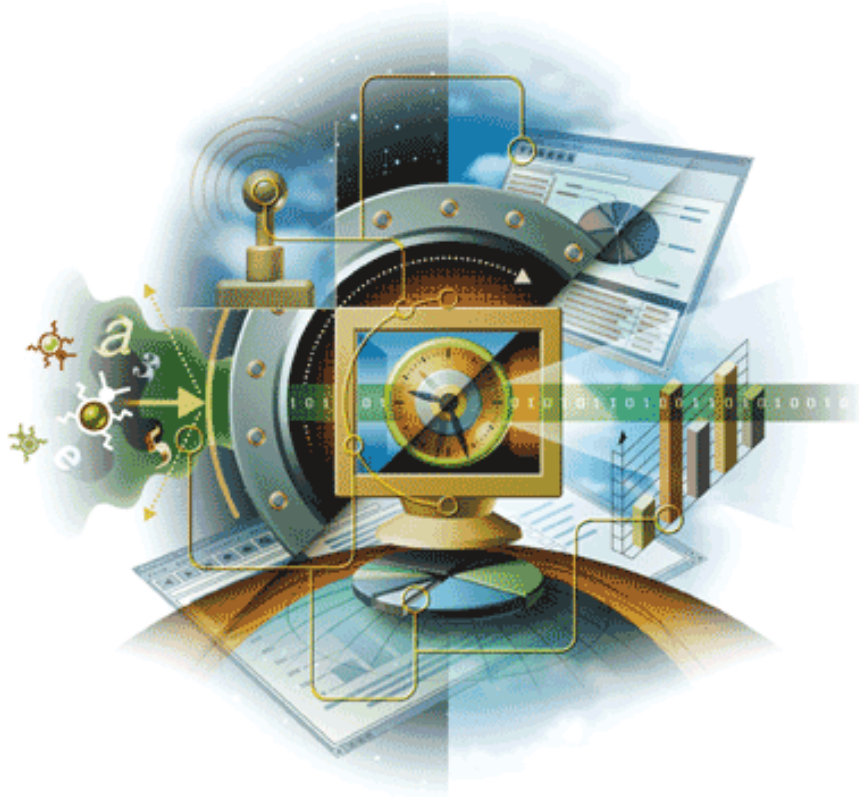


**Virex®**

バージョン 7.6

ePolicy Orchestrator 用



**McAfee®**  
System Protection

業界トップの侵入防止ソリューション

## 著作権

Copyright © 2004-2005 McAfee, Inc. All Rights Reserved.

このマニュアルのいかなる部分も、McAfee, Inc. またはその代理店または関連会社の書面による許可なしに、形態、方法を問わず、複製、送信、転載、検索システムへの保存、および他言語に翻訳することを禁じます。許諾を得る際には、下記の McAfee 法務部門まで書面にてご連絡ください。5000 Headquarters Drive, Plano, Texas 75024 もしくは +1-972-963-8000

## 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

### ライセンス条項

お客様へ：お客様がお買い求めになられたライセンスに従い、該当する契約書（許諾されたソフトウェアの使用につき一般条項を定めるものです、以下「本契約」といいます）をよくお読みください。お買い求めになられたライセンス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若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、弊社が製品のライセンス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。本ソフトウェアの使用許諾条件については、[www.apache.org/licenses/LICENSE-2.0.txt](http://www.apache.org/licenses/LICENSE-2.0.txt) を参照。◆ 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. ◆ FEAD® Optimizer technology, Copyright Netop Systems AG, Berlin, Germany。◆ Outside In® Viewer Technology © 1992-2001 Stellant Chicago, Inc. and/or Outside In® HTML Export, © 2001 Stellant Chicago, Inc. ◆ Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, © 1998, 1999, 2000。◆ Software copyrighted by Expat maintainers。◆ Software copyrighted by The Regents of the University of California, © 1989。◆ Software copyrighted by Gunnar Ritter。◆ Software copyrighted by Sun Microsystems®, Inc. © 2003。◆ Software copyrighted by Gisle Aas. © 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 Looijgaard, © 1997。◆ Software copyrighted by the Python Software Foundation, Copyright © 2001, 2002, 2003。本ソフトウェアの使用許諾条件については、[www.python.org](http://www.python.org) を参照。◆ Software copyrighted by Beman Dawes, © 1994-1999, 2002。◆ Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame。◆ Software copyrighted by Simone Bordet & Marco Cravero, © 2002。◆ Software copyrighted by Stephen Purcell, © 2001。◆ インディアナ大学 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。◆ カリフォルニア大学バークレー校によって開発されたソフトウェア。◆ 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](mailto: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。詳細については、<http://www.boost.org/libs/bind/bind.html> を参照。◆ 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。アップデート、ドキュメント、改訂履歴については、<http://www.boost.org> を参照。◆ Software copyrighted by Doug Gregor ([gregod@cs.rpi.edu](mailto: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](mailto: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](mailto: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。

# 目次

<b>1</b>	<b>はじめに</b>	<b>5</b>
	このマニュアルの内容	5
	ePolicy Orchestrator を使用して Virex を管理するための前提条件	6
	ePolicy Orchestrator コンソールの紹介	6
	対象読者	7
	表記規則	7
	詳細情報	8
	製品情報の入手	8
	製品内のリンク	9
	製品サービス	10
	連絡先	11
<b>2</b>	<b>インストール</b>	<b>13</b>
	はじめに	13
	システム要件	13
	Virex 7.6 管理用に ePolicy Orchestrator コンソールを設定する	13
	Virex 7.6 管理用の NAP ファイルをチェックインする	14
	Macintosh システム用エージェントをインストールする	18
	エージェントのインストール ディレクトリ	18
	エージェントをインストールする	18
	Virex 7.6 をインストールする	24
	アンインストール	24
	ePolicy Orchestrator サーバから Virex NAP を削除する	24
	ePolicy Orchestrator サーバから ePolicy Orchestrator エージェントを 削除する	24
	Mac OS X から ePolicy Orchestrator エージェントを削除する	25
<b>3</b>	<b>Virex 7.6 用の ePolicy Orchestrator ポリシーの設定</b>	<b>27</b>
	ePolicy Orchestrator でポリシーを設定する	27
	全般	29
	eUpdate	30
	アクティブ スキャナ	32
	バックグラウンド スキャナ	33
	マウント ボリューム スキャナ	34
	オンデマンド スキャナ	35
	スキャンと eUpdate のスケジュールを設定する	36
	スケジュール タスクについて	36
	eUpdate	40
	ePolicy Orchestrator サーバのプロパティを表示する	42
<b>4</b>	<b>リモートからのエージェントの制御</b>	<b>43</b>
	エージェントのプロパティを表示する	43
	ePolicy Orchestrator エージェントにポリシーを施行する	44
	エージェント オプション	45
	イベント	45
	サーバイベントを表示する	48
	ログに記録する	49

<b>5</b>	<b>レポート</b>	<b>51</b>
	レポート .....	51
	レポートを設定する .....	52
	<b>用語集</b>	<b>53</b>
	<b>索引</b>	<b>57</b>

# 1 はじめに

## このマニュアルの内容

このマニュアルでは、McAfee® ePolicy Orchestrator® 管理ソフトウェアのバージョン 3.0.2 以降を使用して、Virex 7.6 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、弊社のウィルス対策製品を一元管理することができます。企業規模でウィルス対策ポリシーを管理したり、ウィルス対策イベントとウィルス活動のレポートを表示することが可能となります。ePolicy Orchestrator を使用すると、ネットワーク上に存在するシステムの Virex 7.6 を設定できます。Virex の「**環境設定**」ダイアログ ボックスからそれぞれ個別に設定する必要はありません。

このマニュアル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ィルス対策ポリシーを設定して、次の Virex 機能を設定する。
  - Virex 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
  - アクティブ スキャナのポリシー
  - バックグラウンド スキャナのポリシー
  - マウント ボリューム スキャナのポリシー
  - オンデマンド スキャナのポリシー
- ePO Agent for Mac OS X 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。これらの情報については、『ePolicy Orchestrator 製品ガイド』を参照してください。

## ePolicy Orchestrator を使用して Virex を管理するための前提条件

ePolicy Orchestrator ソフトウェアから Virex の設定を行うようにするには、次の内容を実行する必要があります。

- ePolicy Orchestrator ソフトウェア リポジトリに Virex 7.6 NAP ファイルをチェックインする。
- ePolicy Orchestrator に Non Windows Agent<sup>1</sup> ファイルをチェックインする。
- Macintosh システムに Virex 7.6 をインストールする。
- Macintosh システムに 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 とのインタフェースは MMC (Microsoft Management Console) です。ここでは、ePolicy Orchestrator から管理する Virex ウィルス対策製品の登録と設定を行います。

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項目によって変わります。このコンソールでは、標準の MMC 機能が使用されています。

ウィンドウ上部のメニューの下で、コンソールは 2 つのペインに分かれています。

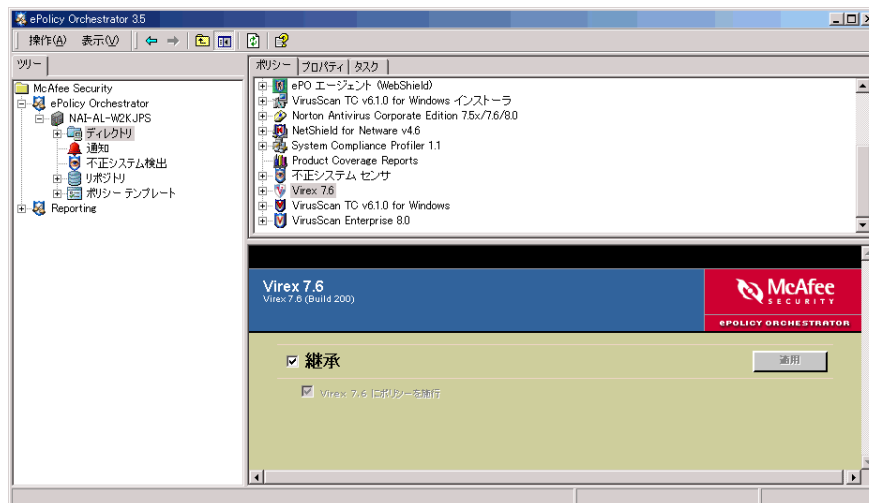


図 1-1 ePolicy Orchestrator コンソール

- コンソールの左側には**コンソール ツリー**が表示されます。この部分には、管理対象のサーバ、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 ツリーで選択した項目に応じて、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。

<sup>1</sup> Non Windows Agent (NWA) は、ePO Agent for Mac OS X ともいいます。

## 対象読者

このマニュアルの情報は、社内のウィルス対策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。

<b>太字</b>	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、ユーザインタフェースのすべての用語に使用します。 <b>例：</b> 対象のアカウント情報を「 <b>ユーザ名</b> 」と「 <b>パスワード</b> 」に入力します。
Courier	フォルダやプログラムのパス、Web アドレス (URL)、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。 <b>例：</b> プログラムのデフォルトの場所は次のとおりです。 C:\Program Files\McAfee\EPO\3.5.0 弊社の Web サイトを参照してください。 <a href="http://www.mcafee.com">http://www.mcafee.com</a> 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。 C:\SETUP.EXE
斜体	製品マニュアル名や、マニュアル内のトピック ( 見出し )、新しい用語の紹介、または語句を強調するために使用します。 <b>例：</b> 詳細については、『Virex 7.6 製品ガイド』を参照してください。
< 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。 <b>例：</b> コンソール ツリーの「 <b>ePolicy Orchestrator</b> 」の下位にある「< サーバ >」を右クリックします。
	<b>注意：</b> 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。
	<b>ヒント：</b> ウィ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弊社が提案または推奨する内容を示します。
	<b>警告：</b> 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。
	<b>危険：</b> 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。
	<b>新機能：</b> このリリースの新しい機能またはオプションを示します。

## 詳細情報

弊社では、長年の経験に基づき、お客様の満足を第一に考えて製品を開発しています。弊社のテクニカル サポート チームでは、重要なプロジェクトを成功させるために、高度な技術者による状況に応じた解決策やサポートを提供し、すべてのお客様が満足できるようなサービスをお届けしています。また、業界トップの情報システムおよびセキュリティ調査を提供する McAfee Research では、革新的な開発と技術の向上を率先して行っています。

製品の詳細については、次のセクションを参照してください。

- 製品情報の入手
- 製品内のリンク
- 製品サービス
- 連絡先

## 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 または弊社ダウンロード 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。

**製品ガイド** — 製品の紹介と機能の説明、ソフトウェアの詳細な設定手順、配備方法、繰り返し実行するタスク、および操作手順について記載されています。

- *Virex 7.6 製品ガイド*

**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。

**コンフィグレーション ガイド** — *ePolicy Orchestrator* 用。ePolicy Orchestrator 管理ソフトウェアを介して Virex の配備や管理を行う方法が記載されています。

**リリース情報**<sup>^</sup> — *ReadMe*。製品情報、解決された問題、既知の問題、製品または製品マニュアルに対する最新の変更点が記載されています。

**Contact**<sup>^</sup> — 連絡先が記載されています。

**License** — ライセンス約款。製品に対して購入することのできるライセンスのすべての種類が記載されています。ライセンス約款では、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。

---

\* 製品 CD に同梱されている冊子のマニュアル。注意：一部の言語のマニュアルは、.PDF ファイルでのみ提供されます。

<sup>^</sup> ソフトウェア アプリケーションおよび製品 CD に含まれているテキストファイル。

## 製品内のリンク

製品には有用なリソースへのリンクがあります。

- オンライン ヘルプ
- ウィルス情報ライブラリ
- ePolicy Orchestrator のテクニカル サポート
- Minimum Escalation Resource Tool
- AVERT Web Immune
- McAfee Security ホームページ

### オンライン 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。



製品に組み込まれているヘルプ システム (ソフトウェア上で「ヘルプ」メニューをクリックしてアクセス) が正常に表示されない場合は、ご使用のバージョンの Microsoft® Internet Explorer では、ActiveX コントロールが正常に動作しない可能性があります。ヘルプ ファイルを表示するためには、ActiveX コントロールが必要となります。最新バージョンの Internet Explorer をインストールしてください。

### ウィルス情報ライブラリ

「**ウィルス情報**」から弊社の AVERT (Anti-virus & Vulnerability Emergency Response Team) ウィ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、ウィルスの発生源、システムへの感染方法、削除方法などの詳細な情報があります。

ウィルス情報ライブラリには、本物のウィルス以外にも、電子メールで受信するウィルス警告など、ウィ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。善意と思われるウィ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。

ウィルス情報ライブラリにアクセスするには、次の手順に従います。

- 1 ePolicy Orchestrator を開きます。
- 2 「**開始ページ**」から「**ウィルス情報**」を選択します。

### ePolicy Orchestrator のテクニカル サポート

「**テクニカル サポート**」から弊社テクニカル サポートの Web サイトにアクセスできます。このサイトでは、よくある質問 (FAQ) やマニュアルを参照したり、指示に従って検索を行うことができます。

- 1 ePolicy Orchestrator を開きます。
- 2 「**開始ページ**」から「**ePolicy Orchestrator のテクニカル サポート**」をクリックします。

### Minimum Escalation Resource Tool

「**Minimum Escalation Resource Tool**」から弊社テクニカル サポートの Web サイトにアクセスできます。登録にはログインが必要となります。

- 1 ePolicy Orchestrator を開きます。
- 2 「**開始ページ**」から「**Minimum Escalation Resource Tool**」をクリックします。

### AVERT Web Immune

「**AVERT Web Immune**」から Avert Web Immune の Web サイトにアクセスすることができます。

- 1 ePolicy Orchestrator を開きます。
- 2 「**開始ページ**」から「**AVERT Web Immune**」をクリックします。

### McAfee Security ホームページ

「**McAfee Security ホームページ**」から弊社 Web サイトにアクセスできます。

- 1 ePolicy Orchestrator を開きます。
- 2 「**開始ページ**」から「**McAfee Security ホームページ**」をクリックします。

## 製品サービス

次のサービスを利用して、弊社製品に関する必要な情報を入手することができます。

- ベータ版プログラム
- HotFix およびパッチ
- 製品のサポート終了期限

### ベータ版プログラム

ベータ版プログラムでは、弊社製品が市場にリリースされる前に、既存の製品の新機能を確認したり、新製品を試すことができます。このプログラムを利用すると、アップデートや新機能を安全な環境で事前にテストすることができます。また、製品の新機能について提案したり、弊社のエンジニアと直接やり取りすることもできます。

詳細については、次を参照してください。

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

### HotFix およびパッチ

HotFix およびパッチは、製品の主要リリースの間にアップデート ファイル、ドライバ、実行ファイルなどと一緒にリリースされます。最新の HotFix およびパッチは、次のリンクから入手できます。

<http://www.mcafeesecurity.com/us/downloads/updates/hotfixes.asp>

### 製品のサポート終了期限

ウィルスやその他の不審なソフトウェアから保護するためには、ウィルス対策ソフトウェアを常に最新の状態にしておく必要があります。ウィルス定義 (DAT) ファイルを定期的にアップデートすることは非常に重要です。弊社では、常に効果的なウィルス対策機能を提供するために、DAT ファイルとウィルススキャン エンジンに頻繁に更新しています。したがって、新しいバージョンがリリースされたら、エンジンをアップデートしてください。古いエンジンでは、新たに出現したウィルスが検知できない場合があります。

新しいエンジンがリリースされると、既存のエンジンのサポート終了期限が報告されます。弊社製品のサポート終了期限のポリシー、およびサポート対象のエンジンや製品の詳細については、次を参照してください。

[http://www.mcafeesecurity.com/us/products/mcafee/end\\_of\\_life.htm](http://www.mcafeesecurity.com/us/products/mcafee/end_of_life.htm)

## 連絡先

弊社は、お客様のご意見、ご要望に基づいて、製品およびサービスを提供いたしております。弊社製品およびマニュアルで使用されている用語、表現につきまして、お気づきの点がございましたら、下記の宛先まで電子メールにてお知らせください。

B2BLoc\_JP@mcafee.com

連絡先については、この製品に付属の CONTACT ファイルをご覧ください。



## 2 インストール

---

### はじめに

エージェントは、ePolicy Orchestrator の分散コンポーネントで、ネットワーク上の各 Macintosh コンピュータにインストールされます。ePolicy Orchestrator サーバ、リポジトリ、管理対象の Virex 7.6 間で、ネットワークを介して情報の収集や送信を行います。エージェントやポリシーの設定内容によって、エージェント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、次の Macintosh オペレーティング システムにインストールできます。

- MAC OS 10.2.6
- MAC OS 10.2.8
- MAC OS 10.3.x

また、次の Macintosh プラットフォームで動作します。

- G3
- G4
- G5

---

### Virex 7.6 管理用に ePolicy Orchestrator コンソールを設定する

コンピュータに ePolicy Orchestrator エージェントが完全にインストールされている場合、容易にレポートを作成することができます。レポートの設定を行うには、次の内容を実行します。

- クライアント コンピュータのユーザ インタフェースから、ePolicy Orchestrator Configurator の IP アドレスとポートが設定されているかどうかを確認します。

## Virex 7.6 管理用の NAP ファイルをチェックインする

NAP ファイルとは、Network Associate Package ファイルのことです。このファイル拡張子は、ePolicy Orchestrator で管理するためにソフトウェア リポジトリにインストールした、弊社のソフトウェア プログラム ファイルを識別するために使用されます。ePolicy Orchestrator サーバをインストールすると、ご使用のバージョンの ePolicy Orchestrator のリリース時にサポートされていた主要な製品のポリシー ページセットも一緒にインストールされます。Virex 7.6 を管理するには、まず、この製品の NAP ファイルをソフトウェア リポジトリに追加する必要があります。

### リポジトリに追加する Virex 7.6 の \*.NAP ファイルの場所

弊社では、ePolicy Orchestrator でサポートされるすべてのウィ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、製品のほかのインストール 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。Virex 7.6 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、.NAP 拡張子、製品名コード、およびバージョン番号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 (NWA) の .NAP ファイルを追加する

**ePolicy Orchestrator サーバに Macintosh 用 Non-Windows Agent の NAP ファイルを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 NAP ファイルを検索し、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。

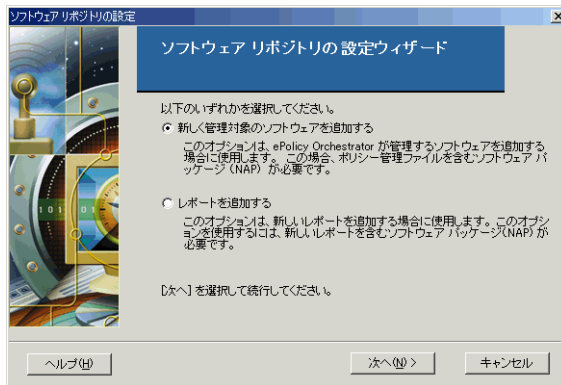


図 2-1 「ソフトウェア リポジトリの設定」ウィザード



ePolicy Orchestrator コンソール ツリーで「リポジトリ」をダブルクリックし、右側の詳細ペインで「NAP のチェックイン」リンクをクリックしても、「ソフトウェア リポジトリの設定」ウィザードを表示することができます。

- 4 「ソフトウェア リポジトリの設定」ウィザードで「新しく管理対象のソフトウェアを追加する」を選択し、「次へ」をクリックします。

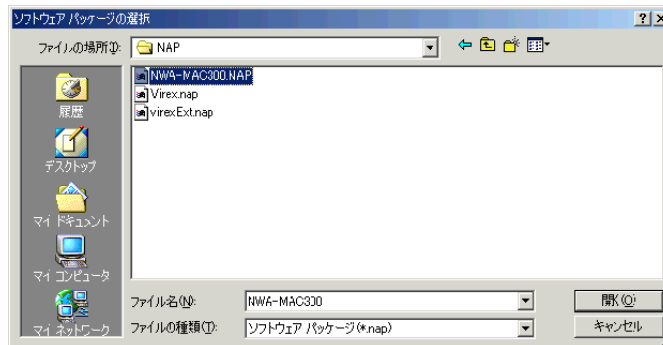


図 2-2 「ソフトウェア パッケージの選択」ダイアログ ボックス

- 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、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、NAP ファイルが読み込まれます。

## Virex の .NAP ファイルを追加する

ePolicy Orchestrator サーバに Virex の .NAP ファイルを追加するには

- 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 NAP ファイルを検索し、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。

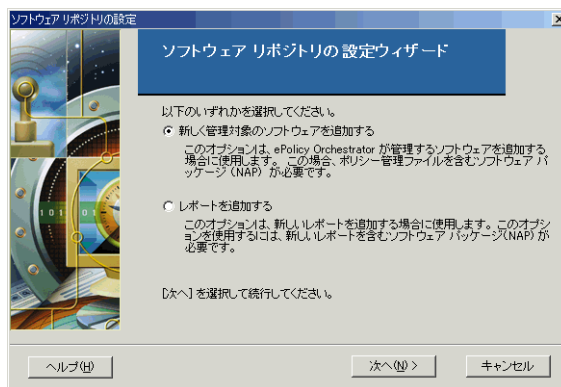


図 2-3 「ソフトウェア リポジトリの設定」ウィザード



ePolicy Orchestrator コンソール ツリーで「リポジトリ」をダブルクリックし、右側の詳細ペインで「NAP のチェックイン」リンクをクリックしても、「ソフトウェア リポジトリの設定」ウィザードを表示することができます。

- 4 「ソフトウェア リポジトリの設定」ウィザードで「新しく管理対象のソフトウェアを追加する」を選択し、「次へ」をクリックします。

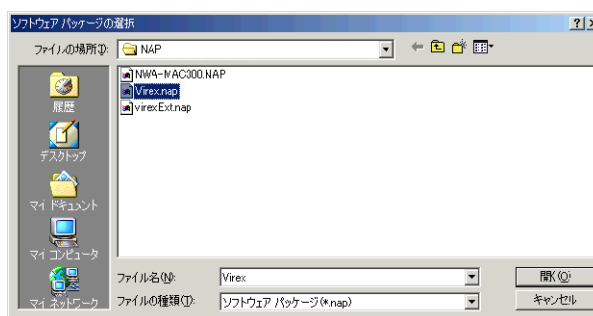


図 2-4 「ソフトウェア パッケージの選択」ダイアログ ボックス

- 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、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、NAP ファイルが読み込まれます。

## レポート用の .NAP ファイルを追加する

ePolicy Orchestrator サーバにレポート用の .NAP ファイルを追加するには

- 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 NAP ファイルを検索し、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。

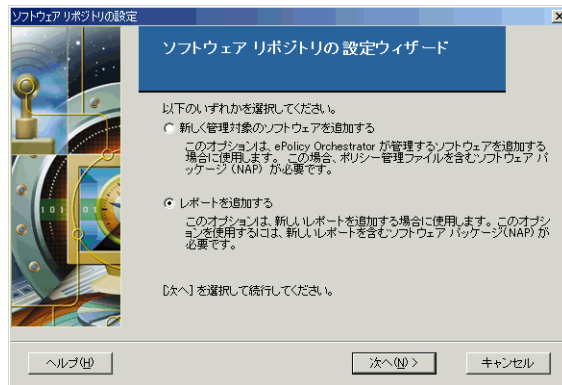


図 2-5 「ソフトウェア リポジトリの設定」ウィザード



ePolicy Orchestrator コンソール ツリーで「リポジトリ」をダブルクリックし、右側の詳細ペインで「NAP のチェックイン」リンクをクリックしても、「ソフトウェア リポジトリの設定」ウィザードを表示することができます。

- 4 「ソフトウェア リポジトリの設定」ウィザードで「レポートを追加する」を選択し、「次へ」をクリックします。

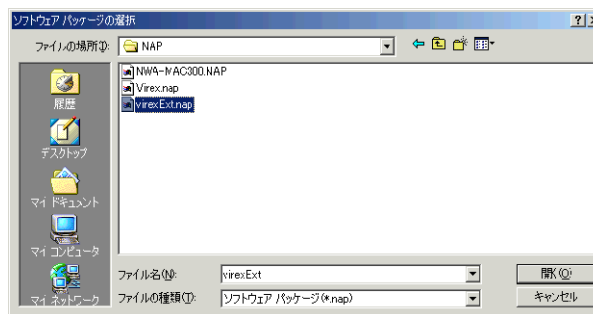


図 2-6 「ソフトウェア パッケージの選択」ダイアログ ボックス

- 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、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、レポート用の NAP ファイルが読み込まれます。

NAP ファイルの読み込みが完了すると、上部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。



図 2-7 「ポリシー」 タブ

## Macintosh システム用エージェントをインストールする

### エージェントのインストール ディレクトリ

エージェントは /Library/NETAepoagt 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 にインストールされます。



Macintosh OS X 用 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。

### エージェントをインストールする

Macintosh 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。

#### 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** を検索し、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** をダブルクリックします。次のファイルが解凍されます。

- NWA.pkg
- cmdinstall

- 3 **NWA.pkg** 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。



図 2-8 ePO エージェントのインストール ウィンドウ – 紹介

- 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。

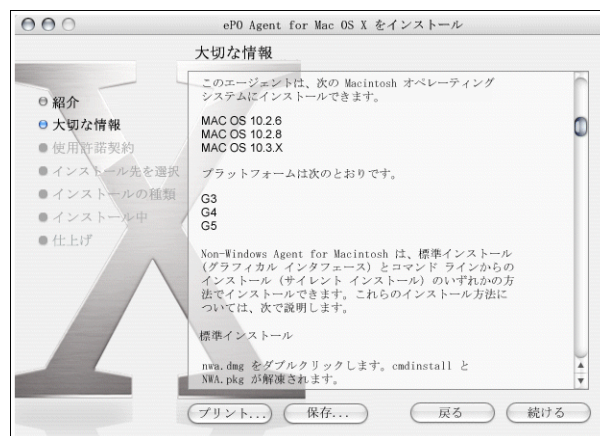


図 2-9 ePO エージェントのインストール ウィンドウ – 大切な情報

5 「続ける」をクリックします。「使用許諾契約」ウィンドウが表示されます。

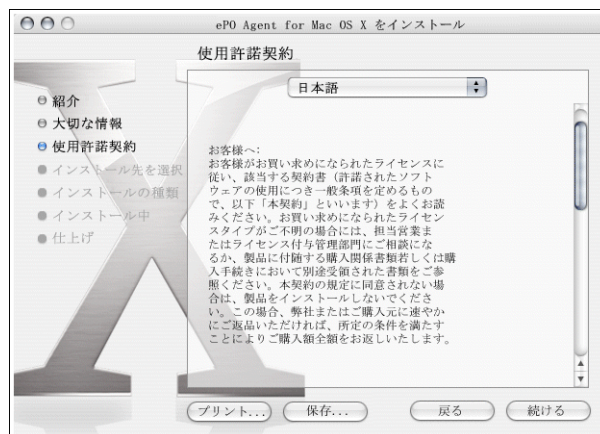


図 2-10 ePO エージェントのインストール ウィンドウ – 使用許諾契約



使用許諾契約をよく読みください。使用許諾契約に同意しないと、インストールは続行できません。

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。

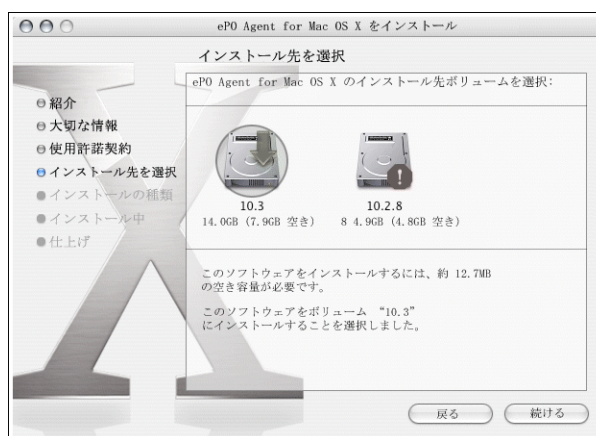


図 2-11 ePO エージェントのインストール ウィンドウ – インストール先を選択

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。「簡易インストール」ウィンドウが表示されます。

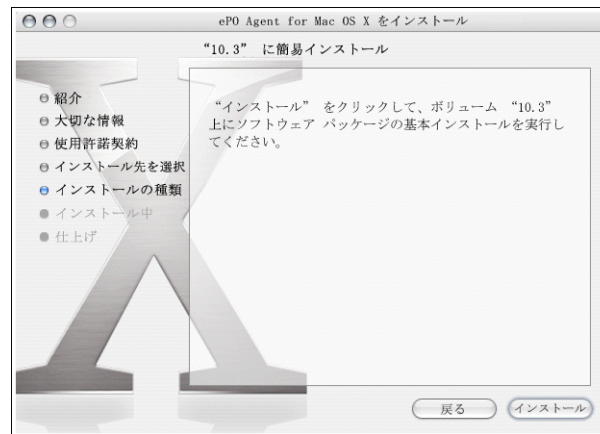


図 2-12 ePO エージェントのインストール ウィザード – 新規インストール



次の場合には、「簡易インストール」ウィンドウに「インストール」ボタンが表示されます。

- エージェントを初めてインストールする場合。
- 以前のバージョンの ePolicy Orchestrator エージェントをアンインストールしたあとに、このエージェントをインストールする場合。

ePolicy Orchestrator エージェントをアップグレードする場合は、次のウィンドウが表示されます。

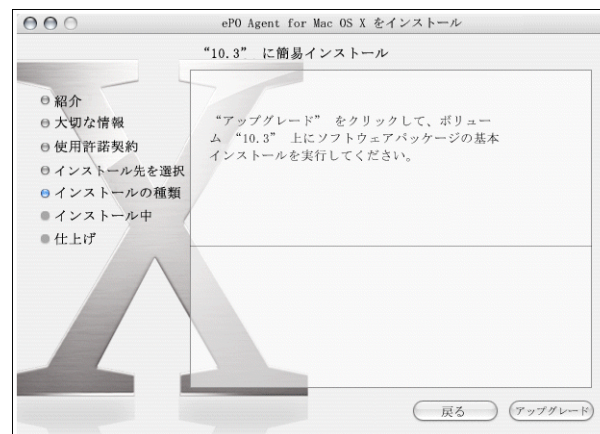


図 2-13 ePO エージェントのインストール ウィンドウ – アップグレード インストール

- 7 「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。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。

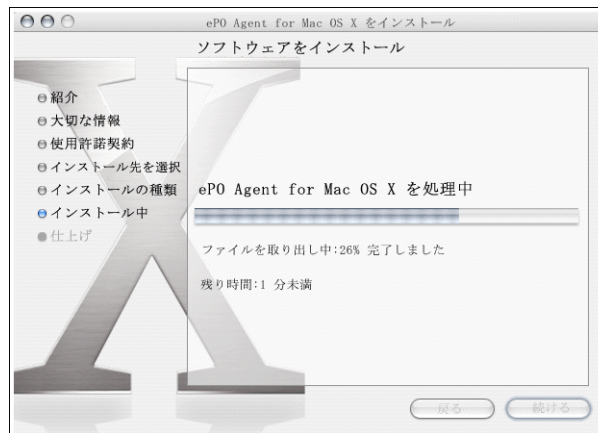


図 2-14 ePO エージェントのインストール ウィンドウ – ソフトウェアをインストール

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。

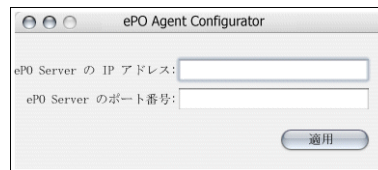


図 2-15 「ePO Agent Configurator」ダイアログ ボックス

- 8 「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。

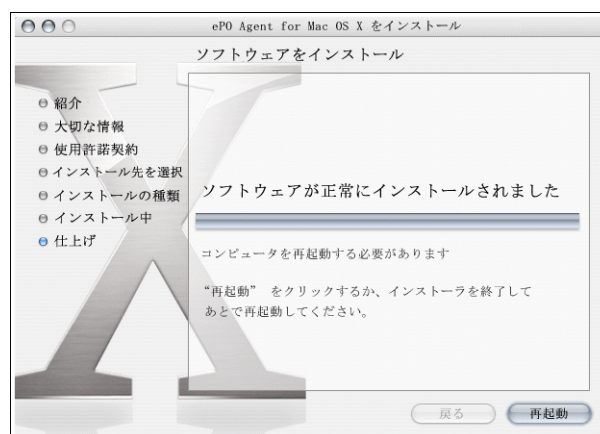


図 2-16 ePO エージェントのインストール ウィンドウ – ソフトウェアをインストール

- 9 「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** を検索し、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** をダブルクリックします。次のファイルが解凍されます。

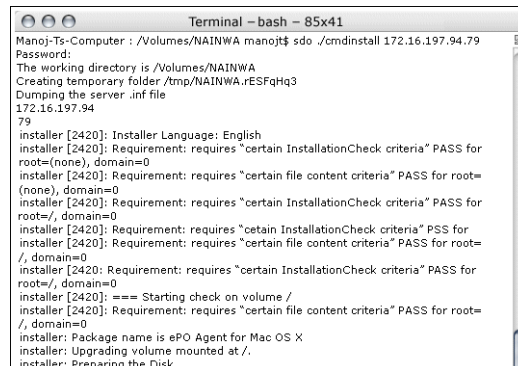
- NWA.pkg
- cmdinstall

- 3 「**Terminal**」ウィンドウを開き、作業ディレクトリを **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。

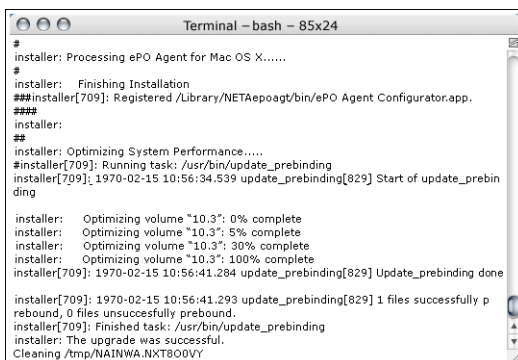
- 4 「**Terminal**」ウィンドウで、**sudo ./cmdinstall <ePO サーバの IP アドレス>:<ePO サーバのポート>** を実行します。



```
Terminal - bash - 85x41
Manoj-Ts-Computer : /Volumes/NAINWA manojts$ sudo ./cmdinstall 172.16.197.94 79
Password:
The working directory is /Volumes/NAINWA
Creating temporary folder /tmp/NAINWA.rESFqHq3
Dumping the server .inf file
172.16.197.94
79
installer [2420]: Installer Language: English
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for root=(none), domain=0
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=(none), domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for root=/, domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for installer [2420]: Requirement: requires "certain file content criteria" PASS for root=/, domain=0
installer [2420]: Requirement: requires "certain InstallationCheck criteria" PASS for root=/, domain=0
installer [2420]: == Starting check on volume /
installer [2420]: Requirement: requires "certain file content criteria" PASS for root=/, domain=0
installer: Package name is ePO Agent for Mac OS X
installer: Upgrading volume mounted at /.
installer: Preparing the Disk.....
```

図 2-17 「Terminal」ウィンドウ - 開始

- 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。



```
Terminal - bash - 85x24
#
installer: Processing ePO Agent for Mac OS X.....
#
installer: Finishing Installation
###installer[709]: Registered /Library/NETAepoagt/bin/ePO Agent Configurator.app.
###
installer:
##
installer: Optimizing System Performance.....
#installer[709]: Running task: /usr/bin/update_prebinding
installer[709]: 1970-02-15 10:56:34.539 update_prebinding[829] Start of update_prebinding
installer: Optimizing volume "10.3": 0% complete
installer: Optimizing volume "10.3": 5% complete
installer: Optimizing volume "10.3": 30% complete
installer: Optimizing volume "10.3": 100% complete
installer[709]: 1970-02-15 10:56:41.284 update_prebinding[829] Update_prebinding done
installer[709]: 1970-02-15 10:56:41.293 update_prebinding[829] 1 files successfully prebound, 0 files unsuccessfully prebound.
installer[709]: Finished task: /usr/bin/update_prebinding
installer: The upgrade was successful.
Cleaning /tmp/NAINWA.NXT8O0VY
```

図 2-18 「Terminal」ウィンドウ - インストール/アップグレードの終了

- 6 これで、**ePO Agent for Mac OS X** のインストール/アップグレードは完了です。

## Virex 7.6 をインストールする



Macintosh システムでの Virex 7.6 ソフトウェアのインストールについては、『Virex 7.6 製品ガイド』を参照してください。

## アンインストール

### ePolicy Orchestrator サーバから Virex NAP を削除する

ePolicy Orchestrator サーバから Virex NAP をアンインストールできます。

Virex NAP を削除するには

- 1 対象の ePolicy Orchestrator データベース サーバにログインします。
- 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、「Virex」を選択します。

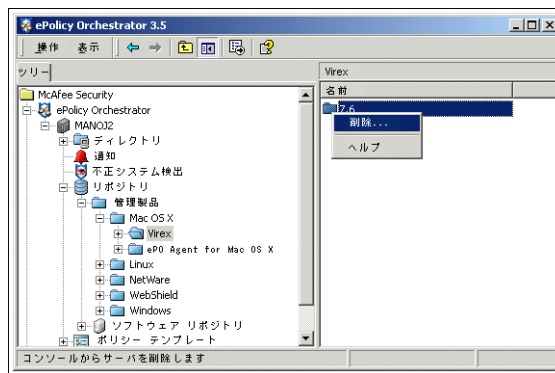


図 2-19 Virex NAP — 削除

- 3 「Virex」を右クリックし、「削除」を選択して ePolicy Orchestrator サーバから Virex NAP をアンインストールします。

### ePolicy Orchestrator サーバから ePolicy Orchestrator エージェントを削除する



ePO Agent for MAC OS X は、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。

## Mac OS X から ePolicy Orchestrator エージェントを削除する

コマンドラインを使用して、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する場合

- 1 root ユーザとしてログインします。



デフォルトでは、Macintosh システムの root ユーザは無効になっています。無効になっている場合は有効にしてください。ユーザとしてログインした場合は、「Terminal」ウィンドウを開き、**su**、root パスワードの順に入力して、root ユーザとしてログインします。

- 2 /Library/NETAepoagt に移動します。
- 3 cmduninst を実行します。



# 3

## Virex 7.6 用の ePolicy Orchestrator ポリシーの設定

この章では、ePolicy Orchestrator から Virex のポリシーを施行する方法について説明します。主な手順は次のとおりです。

- ePolicy Orchestrator で、コンピュータの名前と適用する Virex のポリシーを選択します。たとえば、コンピュータ A と B にウィルス スキャンを実行するとします。この場合、さまざまなポリシーを設定して、個々のコンピュータやコンピュータグループにそれぞれ適用することができます。
- ePolicy Orchestrator に対して、コンピュータ上でこれらのポリシーを施行するように指示します。エージェントはサーバと通信して新しいポリシーの有無を確認します。新しいポリシーは各コンピュータで施行されます。Virex の「**環境設定**」ダイアログ ボックスで以前に設定されたポリシーは無視されます。

---

### 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。ポリシーおよび施行方法については、『*ePolicy Orchestrator 製品ガイド*』を参照してください。

ポリシーを設定する前に、Virex のポリシーを変更するコンピュータ グループをコンソール ツリーで選択してください。Virex 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 Virex の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 Virex のユーザ インタフェースから直接アクセスできるページやダイアログ ボックスとほぼ同じです。Virex 7.6 の設定オプションの詳細については、『*Virex 製品ガイド*』を参照してください。

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。29 ページの「[ポリシーを施行する](#)」を参照してください。

#### ePolicy Orchestrator で Virex のポリシーを変更するには

- 1 対象の ePolicy Orchestrator サーバにログインします。
- 2 コンソール ツリーの「**ePolicy Orchestrator**」、「<サーバ>」の下にある「**ディレクトリ**」で、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。上部詳細ペインに「**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 上部詳細ペインで「**ポリシー**」タブを選択し、「**Virex**」を展開します。Virex エントリの下に単一のエントリが表示されます。

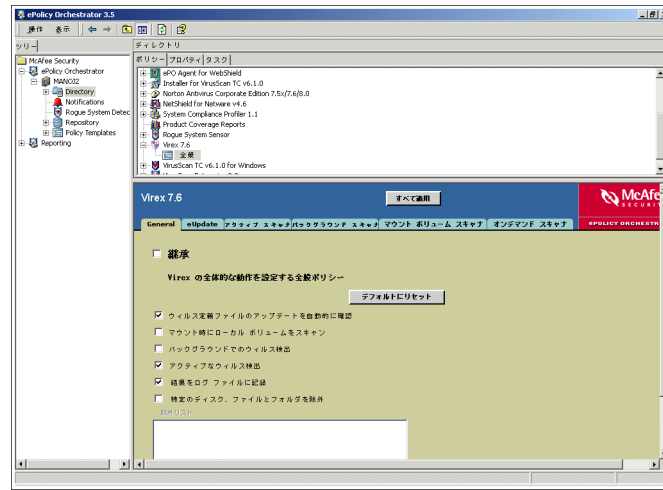


図 3-1 ePolicy Orchestrator コンソール – Virex

下部詳細ペインに、次のような Virex インタフェース内の設定オプションが表示されます。

- 全般
  - eUpdate
  - アクティブ スキャナ
  - バックグラウンド スキャナ
  - マウント ボリューム スキャナ
  - オンデマンド スキャナ
- 4 下部詳細ペインで、上記のいずれかのオプションを選択します。たとえば、「**全般**」を選択します。
- 5 「**全般**」タブで「**継承**」の選択を解除します。
- 6 必要なオプションを設定します。



これらのページは Virex 内のページと同じです。詳細については、『Virex 7.6 製品ガイド』を参照してください。

- 7 「**適用**」をクリックして変更を保存します。ポリシーの設定を続行したあとに、「**すべて適用**」をクリックしてすべての設定を保存することもできます。

## ポリシーを施行する

ポリシーを設定したら、Virex がインストールされているコンピュータに施行する必要があります。

- 1 コンソール ツリーの「**ディレクトリ**」で、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。
- 2 上部詳細ペインの「**ポリシー**」タブで、「**Virex**」を選択します。下部詳細ペインに **Virex** のページが表示されます。
- 3 「**継承**」の選択を解除します。
- 4 「**Virex 7.6 にポリシーを施行**」を選択します。
- 5 「**適用**」をクリックして変更を保存します。

ePolicy Orchestrator ソフトウェアにより、設定したポリシーが Virex コンピュータの ePolicy Orchestrator エージェントに適用されます。

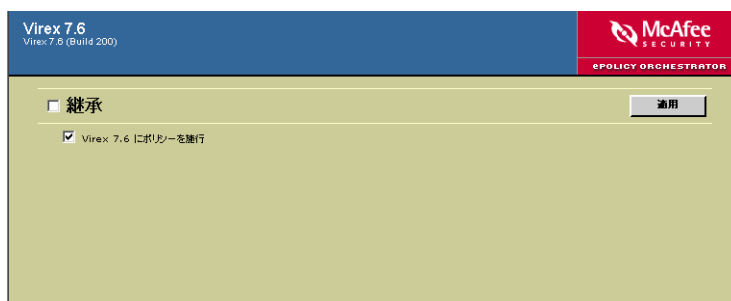


図 3-2 Virex 7.6 にポリシーを施行

## 全般

「**全般**」タブでは、Virex 7.6 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、ウィルス定義のアップデートの自動確認、マウント時のローカルボリュームのスキャン、スキャン結果のログ記録、バックグラウンドでのウィルス検出、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。

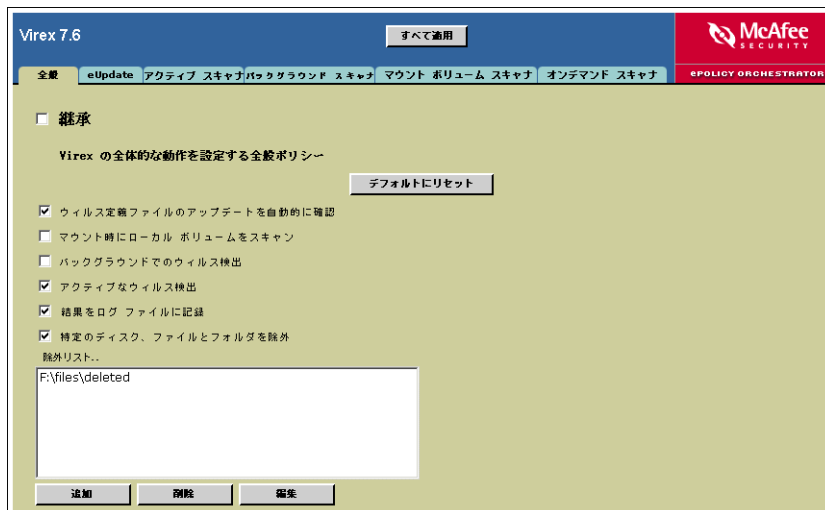


図 3-3 「全般」タブ

## 全般ポリシーの説明

ウィルス定義ファイルのアップデートを自動的に確認	自動 eUpdate を有効 / 無効にします。
マウント時にローカル ボリュームをスキャン	マウント ボリューム スキャナを有効 / 無効にします。
バックグラウンドでのウィルス検出	バックグラウンド スキャナを有効 / 無効にします。
アクティブなウィルス検出	アクティブ スキャナを有効 / 無効にします。
結果をログ 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、ファイルとフォルダを除外	<p>スキャンから除外する対象を設定します。除外する項目は、VShieldExclude.txt と呼ばれるテキスト ファイルにリストとして保存されます。これを選択しないと、除外を設定できません。</p> <p>除外項目の追加</p> <ul style="list-style-type: none"> <li>■ 「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。</li> </ul> <p>除外項目の削除</p> <ul style="list-style-type: none"> <li>■ 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。</li> </ul> <p>除外項目の編集</p> <ul style="list-style-type: none"> <li>■ 除外リストで除外する項目を選択し、「編集」をクリックして除外対象を変更します。</li> </ul>

## eUpdate

「eUpdate」タブでは、DAT ファイルとウィルス 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、最新のウィルス情報とスキャン機能でウィルス対策ソフトウェアを確実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 または HTTP を使用できます。

Virex 7.6

すべて適用

McAfee SECURITY ePOLICY ORCHESTRATOR

全般 eUpdate アクティブ スキャン バックグラウンド スキャン マウント ボリューム スキャン オンデマンド スキャン

☐ 継承

eUpdate サーバのポリシー

☒ eUpdate の設定をカスタマイズ

デフォルトにリセット

☒ FTP

サーバの URL: ftp.nai.com

ポート番号: 21

ユーザ名: User

パスワード: \*\*\*\*\*

アカウント:

ディレクトリ: /virusdefs/mac/virex7/

☐ HTTP

サーバの URL:

ユーザ名:

パスワード:

図 3-4 「eUpdate」タブ

## eUpdate の設定をカスタマイズする

### Virex の eUpdate の設定

#### FTP

FTP (File Transfer Protocol) は、インターネット上でのファイルの送受信に利用される方法です。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、コンピュータにファイルを転送する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 を指定します。
ポート番号	FTP に使用するポート番号を指定します。
ユーザ名	ユーザ名を入力します。
パスワード	パスワードを入力します。
アカウント	FTP アカウントを入力します。
ディレクトリ	DAT ファイルとエンジン ファイルの格納場所へのパスを指定します。

#### HTTP

HTTP (Hypertext Transfer Protocol) は、テキスト、画像、音楽、ビデオなどのマルチメディア ファイルの転送に利用されるルール セットです。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、コンピュータにファイルを転送するサーバの URL 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 を指定します。
ユーザ名	ユーザ名を入力します。
パスワード	パスワードを入力します。

## アクティブ スキャナ

Virex のアクティブ スキャナ機能は、ネットワーク接続やインターネットを経由するウィルスからハード ディスクを絶えず保護します。アクティブ スキャナが常に起動していれば、コンピュータをウィルス感染の危険から確実に保護できます。

アクティブ スキャナは、ハード ドライブ (すべてのパーティション) やすべてのリムーバブルドライブにファイルが書き込まれると、スキャンを開始します。コンピュータの起動時に起動し、シャットダウンされるまで終了することはありません。このスキャナはデフォルトで実行されます。スキャン対象とウィルス感染ファイルの処理方法は設定することができます。

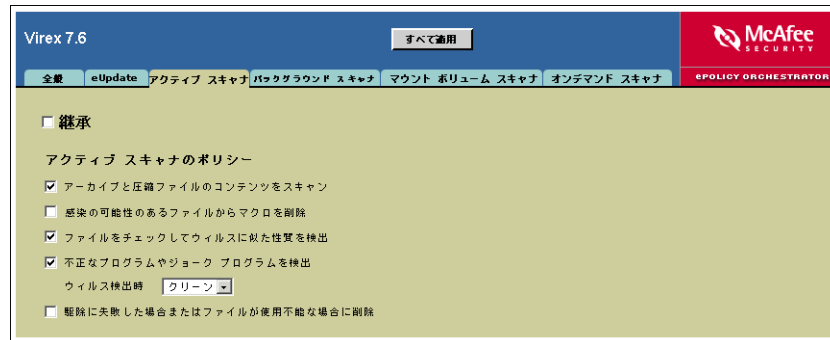


図 3-5 「アクティブ スキャナ」タブ

### アクティブ スキャナ ポリシーの説明

アーカイブと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。バックグラウンド スキャナおよびオンデマンド スキャナではデフォルトでオンになっています。
感染の可能性のあるファイルからマクロを削除	感染ファイルが検出されると、クリーニング時にそのファイルからすべてのマクロが削除されます。
ファイルをチェックしてウィルスに似た性質を検出	ウィルスやワームに似た特徴があり、未知のウィルスが含まれている可能性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。バックグラウンド スキャナではデフォルトでオンになっています。
不正なプログラムやジョーク プログラムを検出	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。
ウィルス検出時 :	スキャナの基本アクションを選択します。
<ul style="list-style-type: none"> <li>■ クリーン</li> <li>■ 削除</li> <li>■ 通知</li> </ul>	
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	選択したスキャナの 2 次的なアクションを選択します。この機能は基本アクションが「クリーン」に設定されている場合にのみ有効です。

## バックグラウンド スキャナ

バックグラウンド スキャナは、システム上にあるすべてのファイルを常にスキャンする機能です。このスキャナでは、システム上のファイルを絶えずスキャンし、ウイルスに感染したファイルを検出することによってコンピュータを保護します。このスキャンは少ないメモリで実行できるので、コンピュータのパフォーマンスが低下することはありません。スキャン対象とウイルス感染ファイルの処理方法は設定することができます。

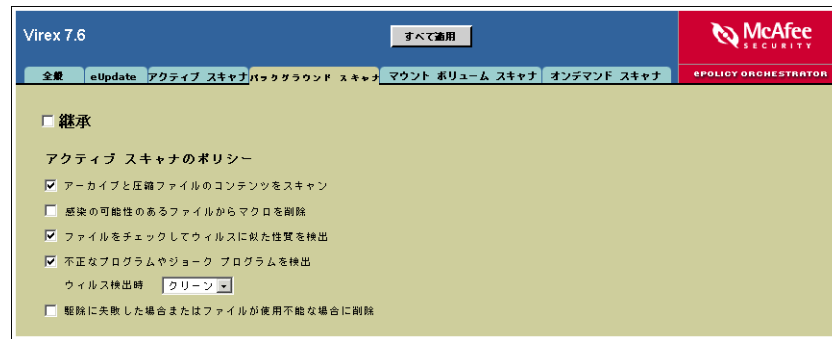


図 3-6 「バックグラウンド スキャナ」タブ

### バックグラウンド スキャナ ポリシーの説明

アーカイブと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。バックグラウンド スキャナおよびオンデマンド スキャナではデフォルトでオンになっています。
感染の可能性のあるファイルからマクロを削除	感染ファイルが検出されると、クリーニング時にそのファイルからすべてのマクロが削除されます。
ファイルをチェックしてウイルスに似た性質を検出	ウイルスやワームに似た特徴があり、未知のウイルスが含まれている可能性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。バックグラウンド スキャナではデフォルトでオンになっています。
不正なプログラムやジョーク プログラムを検出	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。
ウィルス検出時 :	スキャナの基本アクションを選択します。
<ul style="list-style-type: none"> <li>■ クリーン</li> <li>■ 削除</li> <li>■ 通知</li> </ul>	
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	選択したスキャナの 2 次的なアクションを選択します。この機能は基本アクションが「クリーン」に設定されている場合にのみ有効です。

## マウント ボリューム スキャナ

マウント ボリューム スキャナは、CD やカメラなどのボリュームがローカルにマウントされたときにスキャンを開始します。このスキャナを使用すると、システムにマウントする前に大容量のボリュームやデバイスをスキャンして、感染しているデバイスを事前に検出することができます。これにより、危険なウイルスへの感染を防ぐことができます。この機能は Zip ドライブ、CD、DVD、OS X .DMG ファイルのような、ローカルで挿入や取り出しが可能なメディアに対してのみ使用できます。ペンドライブやカメラなどの USB カード デバイスや、iPod などの Firewire デバイスのスキャンも実行できます。ネットワーク接続されているリモート マシンのボリュームはスキャンされません。スキャナはバックグラウンドで実行され、ユーザに対しメッセージを表示します。

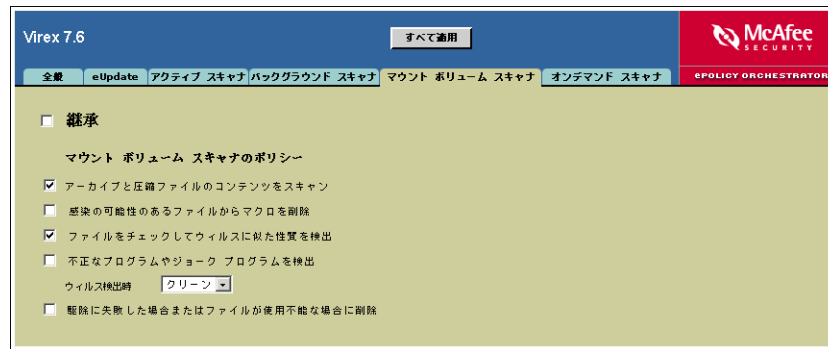


図 3-7 マウント ボリューム スキャナ

### マウント ボリューム スキャナ ポリシーの説明

アーカイブと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。
感染の可能性のあるファイルからマクロを削除	感染ファイルが検出されると、クリーニング時にそのファイルからすべてのマクロが削除されます。
ファイルをチェックしてウイルスに似た性質を検出	ウイルスやワームに似た特徴があり、未知のウイルスが含まれている可能性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。
不正なプログラムやジョーク プログラムを検出	不正なプログラムやジョーク プログラムをスキャナでチェックするかどうかを有効 / 無効にします。
ウイルス検出時:	スキャナの基本アクションを選択します。
■ クリーン	
■ 削除	
■ 通知	
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	選択したスキャナの 2 次的なアクションを選択します。この機能は基本アクションが「クリーン」に設定されている場合にのみ有効です。



マウント ボリューム スキャナはデフォルトでは実行されません。

## 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、「開く」ダイアログ ボックスを使用して、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、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。スキャン対象とウィルス感染ファイルの処理方法は設定することができます。また、アクティブ スキャナ、バックグラウンド スキャナ、マウント ボリューム スキャナのすべてで使用される除外リストを設定することもできます。ウィルスが検出されると、ユーザにメッセージが表示され、処理アクションの情報が記録されたログが生成されます。

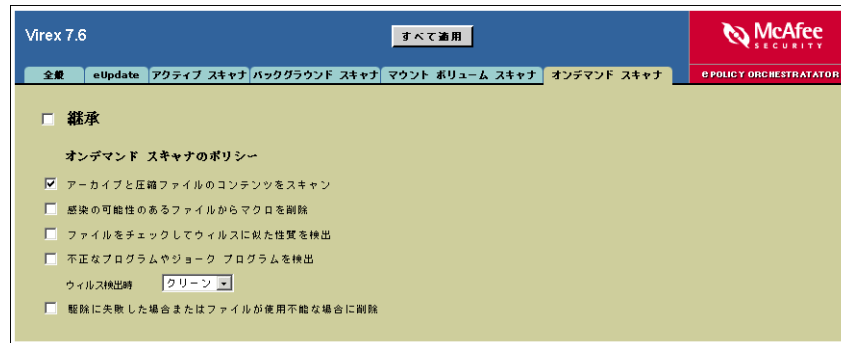


図 3-8 「オンデマンド スキャナ」タブ

### オンデマンド スキャナ ポリシーの説明

アーカイブと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。
感染の可能性のあるファイルからマクロを削除	感染ファイルが検出されると、クリーニング時にそのファイルからすべてのマクロが削除されます。
ファイルをチェックしてウィルスに似た性質を検出	ウィルスやワームに似た特徴があり、未知のウィルスが含まれている可能性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。
不正なプログラムやジョーク プログラムを検出	不正なプログラムやジョーク プログラムをスキャナでチェックするかどうかを有効 / 無効にします。
ウィルス検出時 :	スキャナの基本アクションを選択します。
<ul style="list-style-type: none"> <li>■ クリーン</li> <li>■ 削除</li> <li>■ 通知</li> </ul>	
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	選択したスキャナの 2 次的なアクションを選択します。この機能は基本アクションが「クリーン」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

Virex のウイルス スキャンでは、ウイルス定義 (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に対抗するため、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。ePolicy Orchestrator を使用すると、Virex に最新の DAT ファイルの取得場所を通知したり、既存の DAT ファイルの上書きやオンデマンド スキャンを実行するスケジュールを設定することができます。

### スケジュール タスクについて

ePolicy Orchestrator を使用すると、Virex 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

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、タスクの進行状況を監視することはできません。サーバのログを定期的に参照するようにしてください。

### オンデマンド スキャン

Virex は、ファイルに対してオンデマンド スキャンを実行して、データベース内のすべてのファイルに問題のあるコンテンツが含まれていないかどうか検査します。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は、定期的に行われるように設定したり、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

#### タスクを新規作成するには

- 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、「タスクのスケジュール」オプションを選択します。

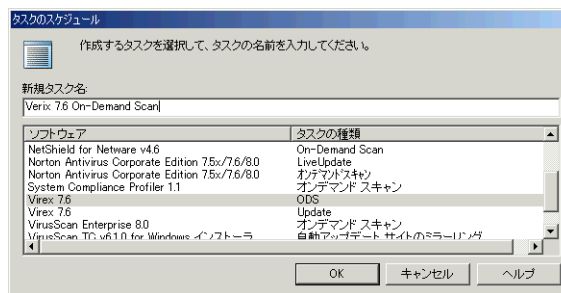


図 3-9 タスクのスケジュール

- 「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。「タスクの種類」ドロップダウン リストで、「オンデマンド スキャン」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。

ポリシー		プロパティ		タスク		
タスク名	最後に修正した	作成したノード	有効	スケジュールの	開始日	開始時刻
Deployment	ディレクトリ	ディレクトリ	はい	日単位	2005/02/02	00:00 日ーカ
Virex 7.6 On-Demand Scan	ディレクトリ	ディレクトリ	はい	日単位	2005/02/03	11:53:00 日ーカ
Update Virex 7.6	ディレクトリ	ディレクトリ	はい	日単位	2005/02/03	12:31:00 日ーカ

図 3-10 「タスク」タブ

## タスクを編集する

### タスクを編集するには

- 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。

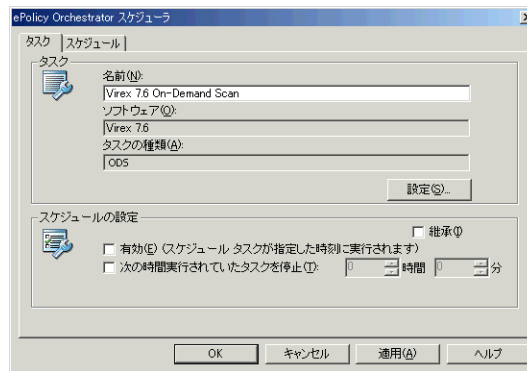


図 3-11 ePolicy Orchestrator スケジューラ – 「タスク」タブ

- 「**設定**」をクリックして、スキャン対象とするファイルとディレクトリを指定します。35 ページの「**オンデマンド スキャナ**」を参照してください。

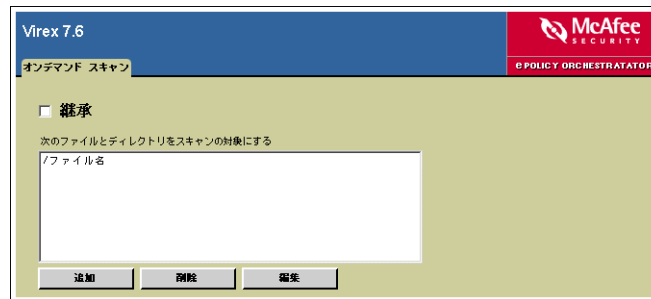


図 3-12 オンデマンド スキャン – ファイルとディレクトリの指定



「**スケジュールの設定**」ペインのタスク設定を有効にするには、「**継承**」の選択を解除して、「**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)**」を選択します。

次のファイルとディレクトリをスキャンの対象にする	<p>スキャン対象項目を設定します。</p> <p>対象項目の追加方法</p> <ul style="list-style-type: none"> <li>■ 「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<b>対象リスト</b>に表示されます。</li> </ul> <p>対象項目の削除方法</p> <ul style="list-style-type: none"> <li>■ <b>対象リスト</b>で対象項目を選択して、「削除」をクリックします。</li> </ul> <p>対象項目の編集方法</p> <ul style="list-style-type: none"> <li>■ <b>対象リスト</b>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。</li> </ul>
--------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

### スケジュールの設定

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。

### 「スケジュール」タブ

タスクのスケジュール設定には、多数のオプションがあります。

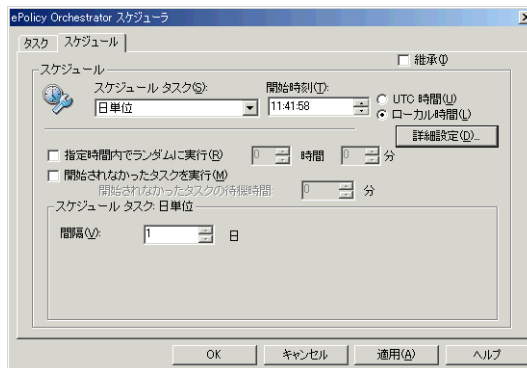


図 3-13 ePolicy Orchestrator スケジューラ — 「スケジュール」タブ

スケジュール タスク	<p>ドロップダウンからタスクの種類を選択します。次のオプションのいずれかを選択できます。</p> <ul style="list-style-type: none"> <li>■ 日単位</li> <li>■ 週単位</li> <li>■ 月単位</li> <li>■ 一回のみ</li> <li>■ システム起動時</li> <li>■ すぐに実行</li> </ul>
開始時刻 ■ UTC 時間 ■ ローカル時間	<p>スケジュール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。</p> <p>UTC 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。</p>
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	「 <b>スケジュールの詳細設定</b> 」ダイアログ ボックスで「 <b>詳細設定</b> 」をクリックします。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	「 <b>スケジュールの詳細設定</b> 」ダイアログ ボックスで「 <b>詳細設定</b> 」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	<p>「<b>スケジュールの詳細設定</b>」ダイアログ ボックスで「<b>詳細設定</b>」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。「<b>タスクを繰り返す</b>」にチェックマークを付けて、繰り返す間隔を設定します。</p> <p>通常、数多くの新しいウィルスが実環境に拡散している場合など、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。</p>
スケジュール タスク : 日単位	スケジュール タスクの間隔を日単位で指定します。1 を選択すると、1 日おきにタスクが実行されます。

## タスクを削除する

### タスクを削除するには

- 「**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

Virex は、スキャンの実行時にウィルス スキャン エンジンとウィルス定義 (DAT) ファイルを使用して、ウィルスの検知と駆除を行います。次々に出現する新しいウィルスに対抗するため、弊社では新しいウィルス定義ファイルを定期的にリリースしています。ウィルス対策ソフトウェアの DAT ファイルとスキャン エンジンが最新の状態でなければ、効果的なウィルス対策を行うことはできません。Virex の DAT ファイルは、少なくとも 1 週間に一度アップデートしてください。また、弊社 AVERT (Anti-Virus Emergency Response Team) の 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定期的に確認してください。Virex を実行しているドメインに複数のサーバが存在する場合は、1 台のサーバに最新の DAT ファイルをダウンロードし、このサーバからほかのサーバがファイルをコピーするように設定できます。サーバで稼動しているオペレーティング システムに関係なく、複数のオペレーティング システム用の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 ファイルの場所は「eUpdate」ページで指定します (31 ページを参照)。

### 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、「タスクのスケジュール」を選択します。「タスクのスケジュール」ダイアログ ボックスが開きます。

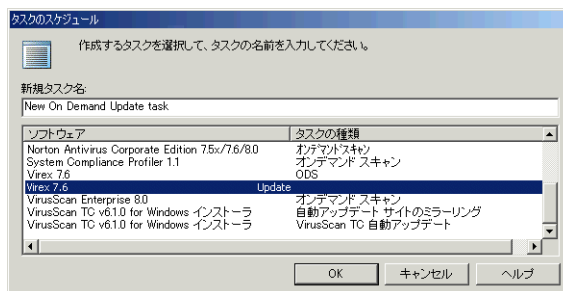


図 3-14 新規アップデート タスク

- 2 「タスクのスケジュール」ダイアログ ボックスで、「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「Virex 7.6 - 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 タスクを新規作成すると、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 「継承」の選択を解除します (37 ページを参照)。

- 3 「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。
- 4 Virex eUpdate タスクを削除する方法については、[39 ページ](#)を参照してください。

### eUpdate タスクを無効にする

- 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 「ePolicy Orchestrator スケジューラ」ダイアログボックスの「タスク」タブと「スケジュール」タブで、必要なオプションを編集し、完了したら「設定」ボタンをクリックします。Virex eUpdate の「タスクの設定」ページが開きます。

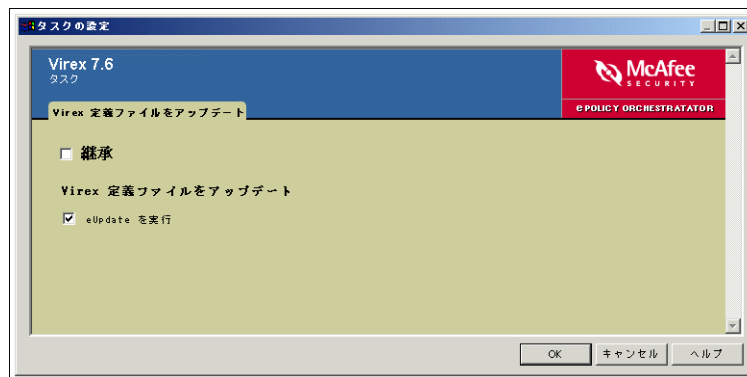


図 3-15 Virex 定義のアップデート – eUpdate を実行

- 3 Virex eUpdate の「タスクの設定」ページで「継承」の選択を解除します。
- 4 「eUpdate を実行」の選択を解除し、「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。
- 6 Virex eUpdate タスクを削除する方法については、[39 ページ](#)を参照してください。

## ePolicy Orchestrator サーバ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。

サーバのプロパティを表示するには

- 1 コンソール ツリーのディレクトリで、設定を表示するサーバを選択します。

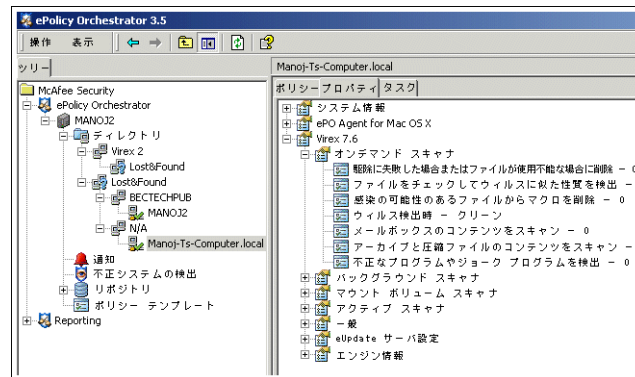


図 3-16 コンソール ツリーのディレクトリ

- 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、**Virex 7.6** 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。

# 4

## リモートからのエージェントの制御

---

### エージェントのプロパティを表示する

ePolicy Orchestrator コンソールを使用して、特定のコンピュータの現在のプロパティを表示することができます。これらのプロパティには、オペレーティング システム、ネットワークの IP アドレス、RAM、プロセッサの速度などの基本的なシステム情報が表示されます。また、コンピュータにインストールされているエージェント、McAfee ウィルス対策またはセキュリティ製品のプロパティも表示されます。

特に、トラブルシューティングを行う場合は、コンピュータのポリシーを確認して、コンソールで変更したポリシーが Macintosh クライアントで施行されているかどうかを確認すると役に立ちます。エージェントは、ASCI ごとにサーバにプロパティを送信するため、ePolicy Orchestrator コンソールから Macintosh クライアント コンピュータのシステム プロパティを確認することができます。

#### プロパティとポリシーの違いについて

ポリシーとは、エージェントまたは特定の製品に対して ePolicy Orchestrator サーバのポリシー ページで設定したルールのことです。エージェントが Macintosh クライアント コンピュータ上でポリシーを施行すると、施行されたポリシーはプロパティとなります。プロパティとは、Macintosh クライアント コンピュータに実際に影響を与える設定のことです。

### エージェントのプロパティを表示する

ディレクトリ内の選択したコンピュータに対してエージェントが収集したプロパティを表示するには

- 1 コンソール ツリーで、Virex がインストールされているコンピュータを選択します。

- 2 右上部詳細ペインで「プロパティ」タブをクリックし、選択したコンピュータのプロパティを表示します。

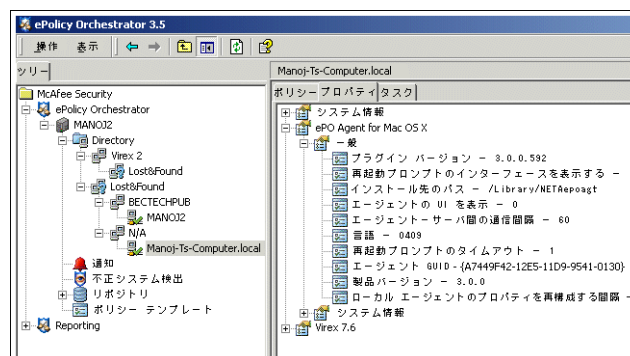


図 4-1 エージェント プロパティの表示

- 3 プロパティの種類を展開して、特定のプロパティの詳細を表示します。エージェントのプロパティは、「ePolicy Orchestrator エージェント」の下に表示されます。

## ePolicy Orchestrator エージェントにポリシーを施行する

ポリシーの設定が終了したら、ポリシーを施行して Virex ホスト上の ePolicy Orchestrator エージェントに適用します。

ePolicy Orchestrator コンソール ツリーで、ポリシーを施行するエージェントを選択します。

- 1 上部詳細ペインで、「ePO Agent for Mac OS X」を選択します。

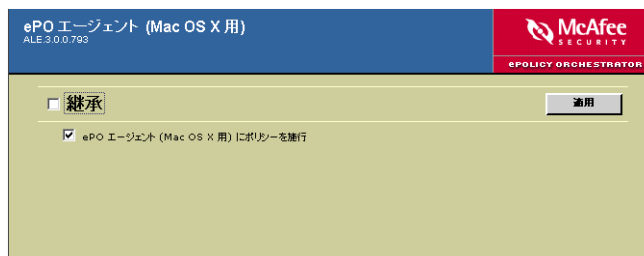


図 4-2 ePO エージェント (Mac OS X 用) にポリシーを施行する場合

- 2 「継承」の選択を解除します。
- 3 「ePO エージェント (Mac OS X 用) にポリシーを施行」を選択します。
- 4 「適用」をクリックして設定を保存します。ePolicy Orchestrator ソフトウェアにより、設定したポリシーは Virex ホスト上のエージェントに適用されます。

## エージェント オプション

エージェントは、ePolicy Orchestrator の分散コンポーネントで、ネットワーク上の各 Macintosh コンピュータにインストールされます。ePolicy Orchestrator サーバ、リポジトリ、管理対象クライアント コンピュータおよび製品間で、情報の収集や送信を行います。エージェントやポリシーの設定方法によって、エージェントの動作、通信およびアップデート方法は異なります。

### コンピュータのエージェント ポリシーを設定するには

- 1 ePolicy Orchestrator のコンソール ツリーで、Virex 用に追加したコンピュータを選択します。
- 2 上部詳細ペインの「ポリシー」タブで、「ePO Agent for Mac OS X」 エントリの下で「設定」を選択します。下部詳細ペインに「ポリシー」ページが表示されます。
- 3 「エージェントのオプション」タブで「継承」の選択を解除します。

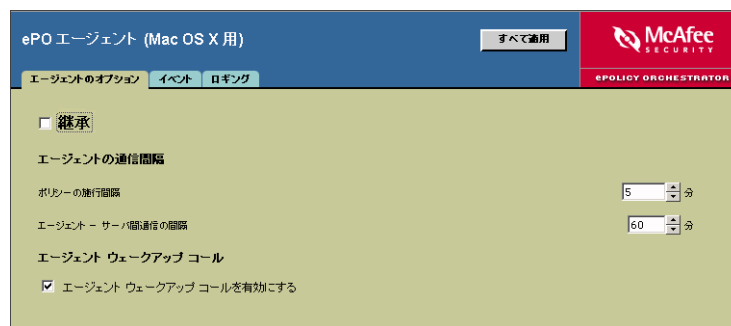


図 4-3 ePolicy Orchestrator — エージェントのオプション

- 4 「ポリシーの施行間隔」で、使用環境に適した間隔を分単位で選択します。デフォルトは 5 分です。5 分から 10,080 分 (1 週間) までの値を選択できます。
- 5 「エージェント-サーバ間通信の間隔」で、使用環境に適した間隔を分単位で選択します。デフォルトは 60 分です。5 分から 2,880 分 (2 日) までの値を選択できます。
- 6 ePolicy Orchestrator サーバからエージェントにウェイクアップ コールが送信されるようにするには、「エージェント ウェイクアップ コールを有効にする」を選択します。

## イベント

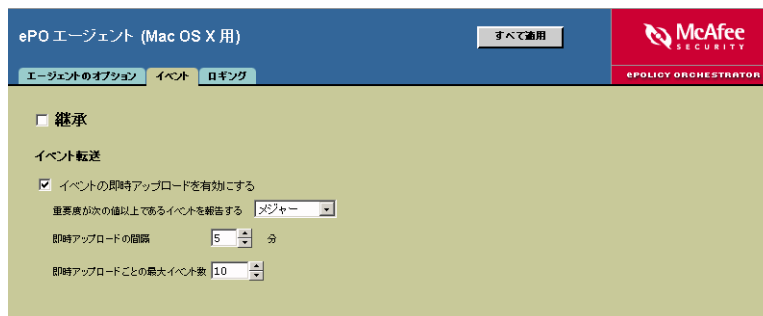
ePolicy Orchestrator サーバは、Non Windows Agent から通知を受け取ります。エージェントのポリシー ページで、ePolicy Orchestrator サーバに即座にイベントを送信するか、またはエージェント-サーバ間通信の間隔でイベントを送信するかを設定する必要があります。

イベントを即座に送信するように設定した場合、エージェントに設定された重大度以上のすべてのイベントがすぐに送信されます。

即座に送信するように設定しない場合、エージェントは、重大度に関係なく、エージェント-サーバ間通信の際にイベントを送信します。

**ePolicy Orchestrator エージェントのポリシーを設定するには**

- 1 対象の ePolicy Orchestrator サーバにログインします。
- 2 ディレクトリまたはサイト、グループ、コンピュータを選択し、上部詳細ペインで「**ポリシー**」タブを選択します。
- 3 上部詳細ペインで「**ePolicy Orchestrator Agent for Mac OS X**」、「**設定**」の順に選択します。
- 4 下部詳細ペインで「**イベント**」タブを選択します。

**図 4-4 「イベント」タブ**

- 5 「**継承**」の選択を解除します。

次のポリシー オプションを設定します。

**イベント転送**

「**イベントの即時アップロードを有効にする**」を選択すると、サーバに即座にイベントを転送するようにエージェントを設定できます。

このオプションの選択を解除すると、エージェントは次の ASCII でイベントを転送します。このオプションを選択した場合は、次の内容を指定する必要があります。

- サーバに送信するイベントの重大度を指定します。ここで設定した重大度以上のイベントがサーバに送信されます。重大度は、「**重大**」、「**メジャー**」、「**マイナー**」、「**警告**」、「**通知**」から選択できます。たとえば、マイナーを選択した場合、重大度がマイナー以上のイベントがサーバに転送されます。
  - 「**即時アップロードの間隔**」でイベント転送間隔を指定します。ここで指定した時間が、一番短いイベント転送間隔になります。たとえば、「5 分」を選択した場合、エージェントは最短で 5 分おきにサーバにイベントを送信します。
  - 「**即時アップロードごとの最大イベント数**」で同時に送信可能なイベントの最大数を指定します。イベント数がこの制限を超えると、残りのイベントは次のイベント転送間隔に送信されます。
- 6 「**すべて適用**」をクリックして変更を保存します。変更は次のエージェントーサーバ間通信で有効になります。

## データベースから古いイベントを定期的に削除する

データベースからイベントを定期的に削除すると、データベースのサイズを抑え、パフォーマンスを向上させることができます。イベントの多く（特に情報イベントやマイナー イベント）は、長期にわたって使用する必要はありません。ただし、データベースからイベントを削除する場合は、イベントの種類に関係なく、事前にデータベースをバックアップする必要があります。このデータベースをアーカイブに保管して、必要に応じてあとで履歴レポートに使用することができます。

ePolicy Orchestrator データベースからイベントを永久削除するには、次の手順に従います。

- 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 ツリーで「Reporting」、「ePO データベース」、「<データベースサーバ>」の下に「イベント」を選択します。詳細ペインに「フィルタリング」、「インポート」、「修復」、および「削除」タブが表示されます。

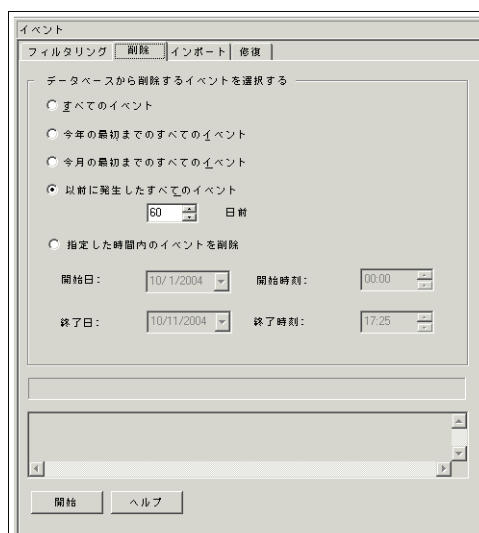


図 4-5 イベント — 「削除」タブ

- 3 「削除」タブをクリックします。
- 4 データベースから削除するイベントを選択します。
  - **すべてのイベント** — データベースからすべてのイベントが削除されます。
  - **今年の最初までのすべてのイベント** — 今年の最初までのすべてのイベントが削除されます。
  - **今月の最初までのすべてのイベント** — 今月の最初までのすべてのイベントが削除されます。
  - **以前に発生したすべてのイベント** — 指定した日付よりも古いイベントが削除されます。
  - **指定した時間内のイベントを削除** — 日付の範囲を指定することができます。この範囲に含まれるすべてのイベントが削除されます。
- 5 「開始」をクリックして、指定したイベントをデータベースから削除します。

## サーバ イベントを表示する

ePolicy Orchestrator コンソールでは、各 ePolicy Orchestrator サーバのすべての情報イベント、警告イベント、エラー イベントを参照、保存、印刷することができます。サーバのイベント ウィンドウでは、サーバで開始されたアクション ( エージェントのプッシュや、アップデートされた DAT ファイルのソース リポジトリからのプル など ) が正常に実行されたかどうかを確認することができます。

また、ePolicy Orchestrator データベースに保存するイベントを管理することもできます。ePolicy Orchestrator データベースのメンテナンスやデータベース内のイベントの管理については、『ePolicy Orchestrator 製品ガイド』を参照してください。

### ePolicy Orchestrator コンソールからサーバ イベントを参照、保存、印刷するには

- 1 対象の ePolicy Orchestrator サーバにログインします。
- 2 コンソール ツリーの ePolicy Orchestrator でサーバ ノードを選択し、詳細ペインの「全般」タブをクリックします。
- 3 「サーバ イベント」をクリックし、「サーバ イベント ビューア」ダイアログ ボックスを開きます。

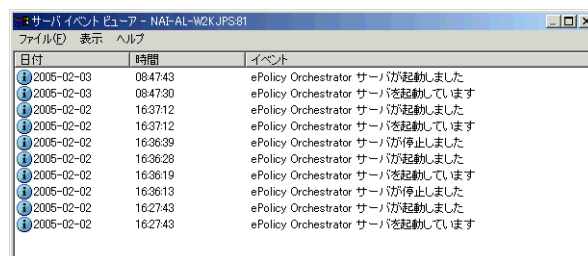


図 4-6 サーバ イベント ビューア

- 4 「表示」、「最新の情報に更新」の順に選択し、イベント リストを最新の状態にします。

### 特定のイベントの詳細を表示する

サーバ イベントの詳細を表示するには、該当するイベントをダブル クリックします。「サーバ イベントの詳細」ダイアログ ボックスが表示されます。

### ログ ファイルにイベントを保存する

すべてのサーバ イベントをサーバ ログ (.log) ファイルに保存するには、「ファイル」から「名前を付けて保存」を選択します。選択したサーバ イベントのみをサーバ ログ ファイルに保存するには、対象のイベントを選択し、「ファイル」から「名前を付けて保存」を選択します。「名前を付けて保存」ダイアログ ボックスで「選択したアイテムのみ」を選択します。

### サーバ イベントを印刷する

すべてのサーバ イベントをデフォルトのプリンタで印刷するには、「ファイル」メニューから「印刷」を選択します。選択したサーバ イベントのみをデフォルトのプリンタで印刷するには、対象のイベントを選択し、「ファイル」メニューから「印刷」を選択します。

## ログに記録する

Macintosh コンピュータ上のエージェントでは、通常の操作中にソフトウェア イベントが常に生成されます。これらのイベントには、エージェントがローカルでポリシーを施行した時間や、オンデマンド スキャンを開始した時間など、通常の操作に関する情報が含まれます。これらのイベントはエージェントによって記録され、ASCI ごとにサーバに送信されてデータベースに格納されます。大規模なネットワークに ePolicy Orchestrator を配備している場合は、1 時間に何千ものイベントが生成される可能性があります。

### ePolicy Orchestrator のログ ポリシーを設定するには

- 1 対象の ePolicy Orchestrator サーバにログインします。
- 2 ディレクトリまたはサイト、グループ、コンピュータを選択し、上部詳細ペインで「ポリシー」タブを選択します。
- 3 上部詳細ペインで「ePolicy Orchestrator Agent for Mac OS X」、「設定」の順に選択します。
- 4 下部詳細ペインで「ロギング」タブを選択します。

次のオプションを使用すると、エージェント アクティビティの記録方法に関するポリシーを設定することができます。

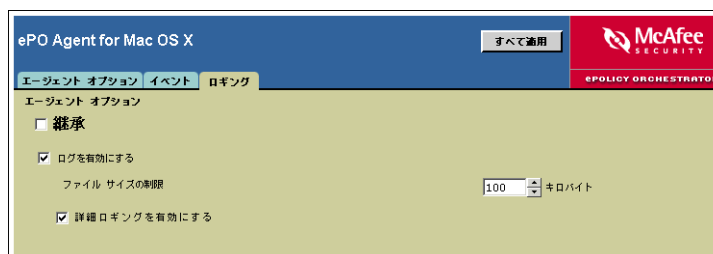


図 4-7 「ロギング」タブ

エージェント ログ ポリシー	プロパティの説明
ログを有効にする	エージェント ログを有効にするかどうかを選択します。このチェック ボックスを選択すると、 /Library/NETAepoagt/Scratch/etc/log への記録が有効になります。
詳細ロギングを有効にする	詳細なエージェント アクティビティ ログ (agent_<コンピュータ>.log) が有効になります。このログ ファイルは、サイズが非常に大きくなる可能性があります。詳細ロギングは有効にすることをお勧めします。有効にしないと、重大なエラーのみが記録されるため、特定の通信問題に対処できない場合があります。



# 5

## レポート

### レポート

ePolicy Orchestrator コンソールでは、Virex ホストによる感染の処理方法を表示するレポートを参照したり、ホスト上の設定を確認することができます。また、特定の ePolicy Orchestrator データベースで、Non Window 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**」および「**レポート データ フィルタ**」ダイアログ ボックスの設定は、今後の使用のために保存することができます。

#### 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、Policy 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。レポートは印刷したり、ほか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「Reporting」、「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>」の下で対象の Virex 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番号を指定します。
  - 「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」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。「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」タブの詳細については、『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 (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 レポートが生成されます。

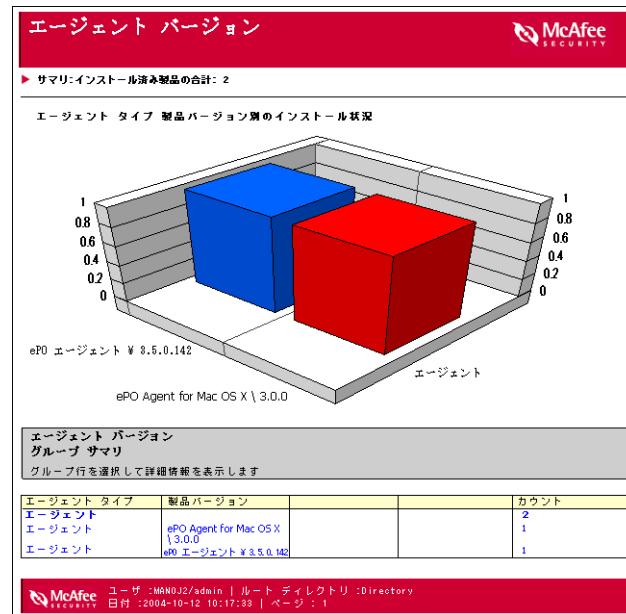


図 5-1 レポートのサンプル - エージェント バージョン

## 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。企業のウィ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ウィルス定義ファイルのバージョン番号、ウィルス スキャン エンジン、およびサポートされている製品を定義することができます。また、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 (たとえば、コンピュータ名、オペレーティング システム、ウィルス名、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。また、必要なレポート データの詳細を表示することもできます (たとえば、Virex 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)。一部のレポートには、サブレポートと呼ばれるほか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。レポートを印刷したり、HTML や Microsoft Excel などの各種ファイル形式でエクスポートすることもできます。



レポートの設定については、『ePolicy Orchestrator 製品ガイド』を参照してください。

# 用語集

## ASCI

エージェントーサーバ間通信の間隔を参照。

## DAT ファイル

ファイルに埋め込まれたウイルスやウイルス関連の不審なプログラムを検出および処理するために、ウイルス対策ソフトウェアがシグネチャ ファイルとして使用するウイルス定義ファイル。

*EXTRA.DAT* ファイル、差分 *DAT* ファイル、*SuperDAT* も参照。

## 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。また、ePolicy Orchestrator サーバと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* リモート コンソールも参照。

## 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* エージェント、*ePolicy Orchestrator* コンソールも参照。

## 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 サーバも参照。

## 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もあります。

## ePolicy Orchestrator リモート コンソール

ePolicy Orchestrator サーバから別のコンピュータにインストールした ePolicy Orchestrator ユーザ インタフェース。

*ePolicy Orchestrator* コンソールも参照。

## 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。

## 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。

## 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

ウィ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、電子メールやポケットベル、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。

*Alert Manager* も参照。

### イベント

エージェント-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。

### ウィルス

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できるプログラム。増殖したプログラムはさらに増殖します。

### 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があるファイル。

### 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-サーバ間通信を開始させる機能。

*SuperAgent* ウェークアップ コールも参照。

### エージェント-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通信が開始されます。

### エージェント-サーバ間通信の間隔 (ASCI)

定義済みのエージェントとサーバが通信を行う頻度。

### 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 コンピュータに配備する必要が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。

### エラー レポート ユーティリティ

システムに配備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。

### オンデマンド スキャン

選択されたファイルにウィルスなどの不審なプログラムが存在するかどうかを確認す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。

オンアクセス スキャンと比較。

### 下部詳細ペイン

コンソールの右下部詳細ペイン。上部詳細ペインの「**ポリシー**」タブにある製品の設定情報を表示します。

*詳細ペイン*と*上部詳細ペイン*も参照。

### 駆除、クリーン

ウィルス、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、ファイルからのウィルスの削除とファイルの修復、システム ファイル、.INI ファイルおよびレジストリからウィルスへの参照の削除、ウィルスが生成したプロセスの終了、ファイルに感染したマクロやスクリプトの削除、トロイの木馬やワームであるファイルの削除、駆除が実行されなかったファイルの名前の変更が含まれます。

### 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、ほか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、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場合は、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のインストールパッケージを送信することができます。

### 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

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。サイトにはグループやコンピュータを入れることができます。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。

### 詳細ペイン

ePolicy Orchestrator コンソールの右側のペイン。現在選択されているコンソール ツリー アイテムの詳細を表示します。選択したコンソール ツリー アイテムによって、詳細ペインが上部と下部に分かれる場合があります。

上部詳細ペインと 下部詳細ペインも参照。

### 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。

詳細ペインと 下部詳細ペインも参照。

### スキャン

ウィルスなどの不審なプログラムが存在するかどうかを確認するためのファイルの検査。

オンアクセス スキャンと オンデマンド スキャンを参照。

### 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

定義済みのイベント数に達した場合に、特定の重要度またはそれ以上のイベントを 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-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発生するようにスケジュールされたアクティビティ。オンデマンド スキャンなど 1 回限りのものと、アップデートなど繰り返しのものの両方があります。

ポリシーと比較。

**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。これらの管理を行うプライマリ インタフェースへリンクしています。

**バイナリ (セッアップ) ファイル**

セッアップ 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。

**配備**

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

**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備するためのマスタ リポジトリ内の場所。

アップデートの選択も参照。

**プロパティ**

エージェント-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。

**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備された 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、クライアント コンピュータ上でサポートされている製品やアップデートをインストールする場合に必要なファイルが保管されています。

**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、この間隔に帯域幅は必要ありません。

**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 ファイル**

McAfee ウィルス対策ソフトウェアのコンポーネントの動作に関する記録。ログ ファイルには、インストール中、スキャン中、アップデート タスク中に行われた処理が記録されます。

イベントも参照。

**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ィルス。

# 索引

## D

DAT ファイル  
場所の指定, 40

## E

ePolicy Orchestrator  
サーバのプロパティ, 42

eUpdate, 30  
FTP, 31  
HTTP, 31  
設定, 40  
作成, 40  
無効化, 41

## N

NAP ファイル  
NAP ファイルの場所, 14  
Non-Windows Agent の追加, 14  
Virex の NAP ファイルの  
追加, 16  
チェックイン, 14  
レポート用の NAP ファイルの  
追加, 17

## あ

アンインストール  
ePO エージェント (ePO サーバ  
から), 24  
ePO エージェント (Mac OS X  
から), 25  
Virex NAP (ePO サーバ  
から), 24

## い

イベント, 45  
イベントの削除, 47  
サーバ イベントの表示, 48

## う

ウィルス情報ライブラリ, 9

## え

エージェント  
インストール, 18  
コマンドライン, 23  
サイレント  
インストール, 23  
標準インストール, 18

オプション, 45  
システム要件, 13  
ディレクトリ, 18  
プロパティの表示, 43  
ポリシーの施行, 44

## こ

このマニュアルについて  
書体の表記規則と記号, 7  
このマニュアルの対象読者, 7

## さ

サーバ コンポーネント, 14

## し

詳細情報, 8  
情報の入手, 8  
製品内, 9  
連絡先, 11

## す

スキャンと eUpdate のスケジュール  
の設定, 36

## せ

製品内のリンク, 9  
製品の詳細情報, 8  
製品のマニュアル, 8

## た

タスク  
削除, 39  
編集, 37

## て

テクニカル サポート  
製品からのアクセス, 9

## ほ

ポリシーの設定  
ePolicy Orchestrator, 27  
アクティブ スキャナ, 32  
オンデマンド スキャナ, 35  
全般, 29  
バックグラウンド  
スキャナ, 33  
マウント ボリューム  
スキャナ, 34

## ま

マニュアル, 8

## よ

用語集, 53  
用語の定義 (用語集を参照)

## れ

レポート, 51  
設定, 52  
連絡先, 11

## ろ

ログ記録, 49

