ProScan
ANTIVIRUS

ProScan® File Scanner バージョン6.0.4

# 管理者ガイド

promark
株式会社プロマーク
2018年12月　第9版

# 目次

# 第1章 ProScan® Filescanner の概要

**ProScan® Filescanner** （以降、**Filescanner**と表記）は、コマンドライン上で指定したファイルに対してウイルス チェックを行います。Linux、FreeBSDのいずれかのOSにおいてサーバのファイルシステム上のファイルに対して定期ファイルスキャン(ウイルス検査/駆除)を実施する事ができます。

この製品の機能は次のとおりです。

- マウントされているすべてのファイルシステムのウイルス チェックを行います 。
- Filescannerはコマンドラインから手動で実行するか、標準の**cron**ユーティリティを使用してスケジューリングを設定しての定期的な起動が可能です。
- 感染ファイル、感染の疑いがあるファイル、パスワードで保護されているファイル、エラーのためウイルス チェックできないファイルを検知します。
- サーバーのファイルシステムで検知された感染オブジェクト、感染の疑いがあるオブジェクトをすべて検疫ディレクトリに移動します。ウイルスを駆除したファイル、パスワードで保護されているファイル、エラーのためウイルス チェックできないファイルも検疫場所に移動できます。.
- 感染オブジェクトや感染の疑いがあるオブジェクトを含んだファイルの情報を、管理者に通知します。
- Filescannerのモジュール、エンジン、ウイルス データベースを更新することができます。更新ファイルは、株式会社プロマークの更新用サーバーからダウンロードされ自動で反映されます。

  このウイルス データベースは、感染オブジェクトの検知に使用します。ウイルス チェックを行うと、ウイルス データベースの内容に基づいて、各ファイルがウイルスに感染していないかどうか分析すると同時に、ウイルス固有のコードと各ファイルのコードを比較します。

  

  新種のウイルスは毎日のように発生します。ウイルス データベースを毎日更新し、常に最新の状態にしておくことをお勧めします。

## 1.1. Filescannerのモジュール

Filescannerは以下の３つのモジュールから構成されています。

- **savapi**

  ウイルスチェックエンジンです。proscanfsはsavapiとのソケット接続によりウイルスデータベースを検索して、ファイルシステムのチェックを行います。

- **proscanfs**

  ファイルスキャナです。ローカルファイルシステムのファイルをスキャンします。オンデマンドで呼び出して使用します。

- **proscanup**

  ウイルスパターンデータベースの更新及びモジュールの更新を行います。弊社サイトに接続し、更新ファイルがあればダウンロードし、アップデートを行います。

## 1.2. ライセンス ポリシー

Filescannerは、次の項目を条件としたライセンスを用意しています。

- **製品使用期間** (通常は購入日から1年間)

## 1.3. ハードウェアとソフトウェアの要件

**Filescanner**を使用するには、次の要件を満たすシステムが必要です。

・ハードウェア要件：

- Intel Pentiumまたはそれと同等の性能を持つプロセッサ、およSPARCプロセッサ
- 1GB以上のRAM
- 512MB以上の空き容量

・ソフトウェア要件：

- 次のいずれかのOS：
  - glibc-2.4以上を有するx86_64アーキテクチャのLinux
  - FreeBSD 64bit バージョン10.3以降

## 1.4. 配布キット

Filescannerは、弊社の販売代理店経由または弊社よりご購入いただけます。

基本的にはダウンロード販売のみで、お客様にダウンロードして頂き、ご自身でインストールして頂きます。ダウンロードサイト（http://www.promark-inc.com/proscan/download.html）からのパッケージは標準で1ヶ月（30日）間の評価ライセンスを同梱しています。評価の後、正規ライセンスキーをご購入頂き製品版と同様にご利用いただけます。(評価中の機能制限はございません。)

正規ライセンスご購入後は以下のものを弊社よりお送りいたします。

- 管理者ガイド
- ライセンス キー
- ライセンス証書
- ソフトウェア使用権許諾契約書

### 1.4.1. ライセンス契約

本ライセンス契約 (LA) は、お客様 (個人または法人) と製造元 (株式会社プロマーク) との間で、お客様が購入したウイルス対策製品の使用条件について締結するものです。

ライセンス契約の条件を必ずお読み下さい。

本契約の条件に同意しない場合は、㈱プロマークから本ソフトウェア製品のライセンスが供与されません。

ソフトウェアのインストールを行うと、お客様は本契約条件に同意したとみなされます。

## 1.5. ご購入ユーザー様用のヘルプ デスク

プロマークでは、本ソフトウエアをご購入頂いた方にProScan®を最大限に活用いただけるようさまざまなサービス パッケージを用意しております。

ご購入頂いた方は、契約期間中、次のサービスをご利用いただけます。

- インターネット経由での日単位のウイルス データベース更新
- 製品アップグレード サービス
- ソフトウェアのインストール、構成、および使用法に関するEメールでのサポート
- プロマークの新製品および新種のコンピュータ ウイルスに関する情報の入手 (弊社のニュースレターの

購読をお申し込みの場合のみ)

弊社は、OSや弊社製品以外の各種技術の操作や使用法についてはお答えできません。

## 1.6. 本書の表記について

本書では、重要な部分を強調するために、次の表記を使用しています。

| 表記 | 意味 |
|---|---|
| **太字** | メニュー名、コマンド、ウィンドウ名、ダイアログ ボックスの要素など |
|  メモ | 補足情報、注意事項など |
|  注意 | きわめて重要な情報 |
|  **操作手順**<br>1. ステップ1<br>2. … | 実行すべきアクション |
|  **課題** | このプログラムを使用するタスクの例 |
|  **解決方法** | タスクを解決するための手順 |
| [**スイッチ**] — スイッチの機能 | コマンド ライン スイッチ |
| `Info message text` | 構成ファイルのテキスト、およびProScan®で表示される情報メール |

# 第2章　Filescannerについて

Unix（Linux/FreeBSD）システム上にインストールされます。コマンドの一つとしてインストールされますが、ライセンスやパターンファイルの関係で、専用のディレクトリにインストールされます。

- **コマンド形式のため、スクリプトやcronからウイルススキャンを実行できます。**
- **cronでコマンドを自動的に実行すると定期的にウイルスチェックを行うことが可能です。**

次に、Filescannerの動作アルゴリズムを理解できるよう、その内部アーキテクチャについて解説します。

## 2.1. Filescannerの内部アーキテクチャ

Filescannerを使用するには、その動作アルゴリズムを理解しておくことが重要です。

ここでは、Filescannerの内部アーキテクチャについて解説します。サーバーのファイル システムのウイルス チェックはきわめてシンプルです。

Filescannerは、サーバーのファイルシステムのウイルス チェックを行うことだけを目的として開発されています。ファイルの入出力時にウイルススキャンを実行する機能は備えていません。Filescannerは、インストールすると、ファイルサーバのファイルシステムの定期的（cronによる）なウイルス検査、およびコマンドラインによる手動でのウイルス検査を実施できます。

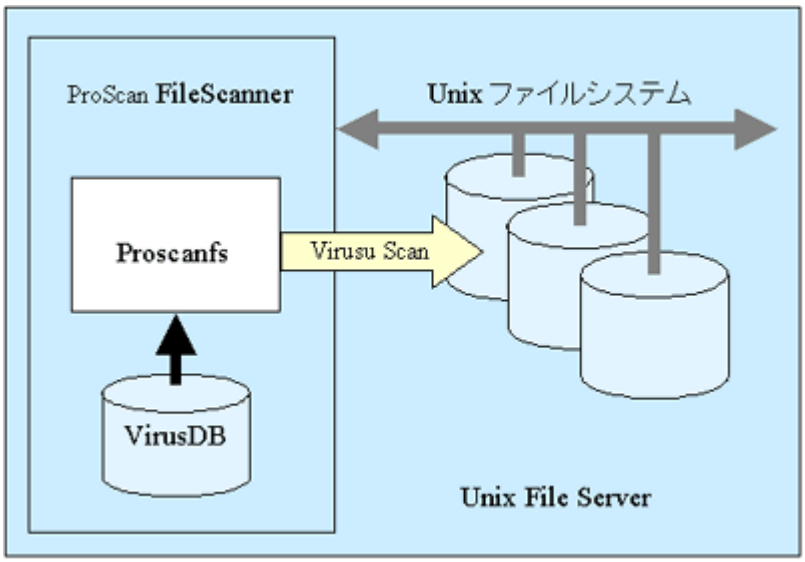


**図1　Filescannerの内部アーキテクチャ**

# 第3章　Filescannerをインストールする

Filescannerのインストールを始める前に、次の手順でシステムを準備してください。

- システムがFilescannerのハードウェア要件とソフトウェア要件を満たしているかどうか確認します。（第1章1.3. ハードウェアとソフトウェアの要件）wgetなどのアプリケーションがインストールされていない場合は、インストールを事前に行ってください。インストールしないと、アップデート機能を利用できません。
- インターネット接続を設定します。Proxy経由で接続する方は、Proxyサーバの情報を控えておいてください。
- **root**ユーザー、またはUID (universal identifier) がゼロであるユーザーとしてシステムにログインします。

インストール前に以下の内容をチェックしておいてください。

| | |
|---|---|
| 通知メールの送信者アドレス | |
| wgetのパス | |
| 正規ライセンスのパス | |
| Registration Code | |

## 3.1. 一般的なインストール

ここで説明するインストール方法は、主にLinux OSを想定しています。

Filescannerのパッケージは、OS種別ごとのアーカイブ形式になっています。このアーカイブの中はディレクトリ ツリー構造になっており、パッケージ ファイル群とインストール スクリプト**install.sh** (以降、「**インストーラ**」と表記) が格納されています。このインストーラでインストールを実行します。

パッケージは、tar+gzパッケージ形式となっています。

サーバーへのFilescannerのインストールは、次の手順で行われます。

1. ProScan@Filescannerインストールに必要なディレクトリを作成します。
2. パッケージ ファイルをサーバーにコピーします。(必要な設定は対話形式で行われます)
3. レジストレーションコードの設定を行います。(正規ライセンスを持っている場合のみ)
4. ライセンスキーファイルの設定を行います。(正規ライセンスを持っている場合のみ)
5. Crontabに自動アップデート設定を行います。
6. パターンファイルの更新をします。

次に、インストール手順について説明します。

### 3.1.1. インストールを開始する

**サーバーにFilescannerをインストールするには、次の手順で行ってください。**

1. アーカイブ形式のパッケージを、サーバーのファイル システム上のディレクトリにコピーします。
2. **tar zxvf <archive name>**コマンドを使用してアーカイブをアンパックします。配布パッケージが配置されているディレクトリ ツリー、およびインストーラがアーカイブから展開されます。
3. 展開したディレクトリに移動し、インストール スクリプト**install.sh**を実行します。

インストール例：

# **./install.sh**

*** ProScan Anti-Virus for Filescanner 6.0.4 Installer started.
*** Installer version 3.0.6, Copyright (C) Promark Inc. 2004-2018

このメッセージが読めますか？(Do you read this japanese message?)[y/n] **y**
日本語モードでインストールします

*** LICENSEファイルをよくお読みになり同意される方のみインストールを続行してください
ライセンスに同意しますか？[y/n] **y**
ライセンスに同意していただきありがとうございました。インストールを続行します

ProScan for Filescanner のインストール方法を選択してください

1. ProScan for Filescanner フルインストール
2. ProScan for Filescanner モジュールアップデート

処理を番号で選んでください[1,2,3] **1**

インストールディレクトリチェック完了

ProScanディレクトリチェック完了

結果通知メールの送信者アドレスを設定して下さい
アドレス：**name@xxx.xx.xx**
wgetのパスをフルパスで指定して下さい[/usr/bin/wget]

ProScan for Filescanner モジュールコピー完了
Registration Codeを持っていますか？[y/n] **n**
評価用Registration codeを設定しました。

正規のKeyファイルをインストールしますか？[y/skip] **skip**
試用版のKeyをインストールしました

アップデートサイトに接続し最新パターンファイルのロードを行います
Proxyサーバ経由ですか？[y/n] **n**
ProScan Updater starting...
ProScan Updater for Filescanner Ver.6.0.4.0
All Rights Reserved,Copyright(C) 2003-2018 Promark Inc.
License check OK
HTTP Proxy Server not defined
Trying update from server http://update.promark-inc.com:80/FS604/PSHB21.lst
Downloading file PSHB21.lst, Please wait...
Success: Get Update list(PSHB21.lst)
Downloading Post-update file, Please wait...
No post update file
Antivir update from update.promark-inc.com server ....
command: /usr/lib/AntiVir/avupdate --config=/etc/avira/avupdate_fs.conf output...
--------------------
Updating, please wait...
（途中省略）
Update finished successfully
--------------------
ProScan updater exited

アップデートを自動で行うためにcronに設定します

ProScan for Filescanner インストールは完了しました

## 3.1.2. Registration Codeの設定

インストール中に、Registration Codeの設定を促すプロンプトが現れます。既に、Codeをお持ちの場合はそのCodeを登録してください。登録したコードはファイル(**/var/opt/filescan/keys/regist.code:**Linuxの場合)に格納されます。Filescanner起動時にはこのコードとライセンスキーファイルのコードがマッチするか検査されます。

評価版ご使用時には設定不要です。（評価版にはfilescan4.keyのみkeyディレクトリに入っています）

Registration Codeは弊社において、お客様のライセンス情報を管理する上で非常に重要なものです。紛失したり、他のプロダクトではご利用なさらないようよろしくお願いいたします。

## 3.1.3. ライセンス キーのインストール

Filescannerは起動時に、設定ファイルに書かれたディレクトリにライセンス キー (filescan3.keyというファイル) があるかどうか検索します。ライセンス キーは、Filescannerの実行に不可欠なファイルです。このファイルがライセンスの種類を判別し、プログラムの使用をユーザーに許可します。ライセンス キーをインストールしなければ、Filescannerを使用できません。

ライセンスを取得済みの場合は、[y]とタイプし、続いてライセンスキーファイルのフルパスを指定します。もし、ファイルが見つからない場合は、評価ライセンスでインストールを続行します。

評価時やライセンス購入後まだ、ライセンスキーファイルを入手していない場合には、内蔵している30日間評価ライセンスが自動で利用されます。その場合は、”n“ をタイプしてパスの指定をスキップし、インストールを続行します。

後日ライセンス キーを受け取ったら、Filescannerの構成ファイルの**LicensePath**パラメータ(付録-A.2を参照) で指定されているキー格納用ディレクトリにコピーして下さい。

ライセンス キーは検知されたものの、有効でない場合は、インストールしてもFilescannerはご使用できません。

## 3.1.5. ウイルス データベースをインストール・更新する

インストール時、ウイルス データベースのダウンロードを必ず実施します。ウイルスデータベースがないとFilescannerは動作しません。必ず最新のウイルスデータベースをダウンロードしてからご利用ください。ウイルスの検知と感染オブジェクトの修復は、このウイルス データベースのレコードに基づいて実行されます。各レコードには、現時点で認識しているウイルスの説明とそのウイルスに感染したファイルの修復方法が記録されています。（インストール方法がフルインストールの場合、自動で行われます）

Filescannerインストーラはインストールが完了すると、cronにウイルスデータベースアップデートの自動起動設定を行います。デフォルトでは1時間に1回の割合でアップデートサイトに接続を行います。プロマークのアップデートサイトには最低でも1日1回パターンファイルの更新が行われています。

ウイルス データベースは毎時更新することをお勧めします。新種のウイルスは毎日のように発生するため、データベースを常に最新の状態にしておくことが重要です。ウイルス データベースの更新については、第5章 5.1を参照してください。

### 3.1.6. インストールを完了する

ここまでの手順を完了すると、それを通知するメッセージがコンソールに出力されます。パッケージの構成ファイルには、Filescannerプログラムの起動に必要な設定情報がすべて含まれています。次のパラメータは、プログラムのインストール時に設定されます。

- Filescannerが動作するホストの名前
- ウイルス データベースの保存先ディレクトリ
- ライセンス キーの格納ディレクトリ
- proscanavモジュールとともに使用されるソケット ファイル
- 一時ファイルの配置ディレクトリ
- 結果通知メールの送信アドレス

その他のパラメータにはデフォルトで既定値が設定されます (第4章4.1を参照)。ただし、管理者はFilescannerの使用を開始する前に、管理者は一部の設定値を変更する必要があります。Filescannerの使用を開始する前に設定が必要なすべきパラメータについては、第4章を参照してください。

ウイルス データベースのダウンロードなど、何らかの一部のインストール手順を ステップをスキップした場合 (たとえば、ウイルス データベースをダウンロードできなかった場合等)は、後でそのステップだけを実行できます。

## 3.2. root以外のユーザが利用する場合の設定

ファイルサーバの運用状況によっては、root以外のユーザが自身のディレクトリをスキャンしたい場合があります。一般ユーザでもスキャンを実施することができるようになりました。ここでは、そのためのセットアップ方法について説明します。
パッケージのインストールは、rootにて通常のインストールを行って下さい。その後、以下の手順により、別ユーザでの利用を可能として下さい。

ライセンスはサーバ単位に与えられますので、複数ユーザで利用することも可能です。

### 3.2.1. コンフィグファイルを用意する

ファイルスキャン用のコンフィグファイルを用意します。もちろん、デフォルトで使用しているコンフィグファイルをそのまま利用しても構いませんが、ログファイルやソケットファイルの置き場所によっては専用のコンフィグファイルを用意しておいた方が便利な場合があります。起動ユーザが書き込み可能なディレクトリ、ファイルが必要ですので、それに合わせたコンフィグファイルとして下さい。起動時に生成されるファイルは以下のパラメータで指定されます。

| セクション | パラメータ | 内容 |
|---|---|---|
| path | LocalSocketPath | エンジンとの通信用ソケットファイルを格納するディレクトリ。エンジンの起動パラメータと合わせる必要がある。 |
| | TempPath | 一時ファイルを生成するディレクトリ。 |
| | CheckStartTimeFile | ファイルのタイムスタンプを確認するための開始時間を記録するファイルを指定。 |
| aveserver | ReportFileName | エンジンのログファイルを指定。 |
| | ConfigFileName | エンジン起動時のパラメータファイルを指定。 |
| scanner.options | SaveDirectory | アラート時のアクションでsave、moveを指定した場合の保存先ディレクトリを指定。 |
| scanner.report | ReportFileName | スキャンログの格納ファイル名。 |

もし、予めスキャンエンジンを起動しておかないモードで利用する場合には、この他、エンジン起動時のコン

フィグファイルを用意します。そして、そのファイル名はConfigFileNameで指定可能なようにします。ここで指定したファイルが存在しない場合には、デフォルトの値が自動的に設定されますので、スキャンエンジンの起動には問題がありません。

上記、コンフィグファイルに指定したディレクトリならびにファイルを起動ユーザが読み書きできるモードで準備しておきます。

### 3.2.2. エンジンの起動方法

エンジンの起動は、事前に行っておくか、スキャン時に自動で起動する方法があります。

【事前に起動する場合】

以下のコマンドで起動します。

```
/usr/lib/AntoVir/savapi --config=config_file_path --socket-file=socket_file_path
```

config_file_pathで指定するファイルはConfigFileNameと同じにします。socket_file_pathに指定するソケットファイル名は、LocalSocketPathで指定したディレクトリと".savapi4_UID.0"というファイル名になります。
例えば、UID=500のユーザがLocalSocketPathに/home/user_dir/runを設定していれば以下のようになります。

```
/home/usr_dir/run/.savapi4_500.0
```

【自動で起動する場合】

ファイルスキャナは、自分で利用できるスキャンエンジンがない場合には自動的にスキャンエンジンを起動します。その際の、起動パラメータは【事前に起動する場合】と全く同じです。

自動的に起動することを行いたくない場合には`filescan.conf`の`[aveserver]`セクションに`AVEAutoStart=no`と設定してください。

### 3.2.3. ファイルスキャン時の注意

ファイルスキャンは、rootで行う場合と同じですが、読取パーミッションのないファイルをスキャンすることはできません。

# 第4章　インストール後の設定作業

インストール実行中、Filescannerのインストール先システムを解析し、一部の構成パラメータを自動的に設定します。その他の構成パラメータには、ウイルス チェック プログラムの動作に最適なデフォルト設定が割り当てられます (第 4 章4.1を参照)。

ここでは、Filescannerのデフォルト設定について説明します。また、Filescannerの使用に必要な構成について詳しく説明します。

## 4.1. Filescannerのデフォルト設定を使用する

Filescannerのパラメータは、すべて**filescan.conf**ファイルにあります。**filescan.conf**はデフォルトの構成ファイルです。

独自の構成ファイルを作成し、そのファイルを現在の作業に使用したり、デフォルトの構成ファイルとして指定することもできます。

ここでは、このファイルのデフォルトのパラメータについて詳しく説明します。この章の説明を読めば、自社の現在の条件下で最大の性能を引き出すためにFilescannerの構成変更が必要かどうか判断できます (構成変更については、第6章を参照ください)。

**サーバーのファイル システムをウイルスから保護するための設定**

デフォルトでは、コマンド ライン スイッチを指定せずにproscanfsモジュールを起動すると、サーバーのファイル システムのウイルス チェックが行われます。

感染ファイル、感染の疑いがあるファイルを検知すると、それを通知するメッセージをコンソールとレポート ファイルに出力します。(設定による)

デフォルトの設定では、検知した感染ファイルの削除を行いません。

## 4.2. ウイルス データベースをインストール・更新する

手動でウイルス データベースを更新するには、**proscanup**モジュールを実行します。コマンド ラインで次のように入力します。

```
/opt/filescan/bin/proscanup -V
```

ウイルス データベースがプロマークの更新用サーバーからダウンロードされ、構成ファイルで指定されている専用のディレクトリに格納されます。

ウイルス データベースは毎日更新することをお勧めします。新種のウイルスは毎日のように発生するため、ウイルス データベースを常に最新の状態にしておくことが重要です。ウイルス データベースの更新については、第5章5.1.1～5.1.2を参照してください。

# 第5章　Filescanner機能概要

Filescannerを使用すると、以下のような機能がご使用できます。

1. Filescannerのアップデートが行なわれます。
2. サーバーのファイルシステムへのウイルス侵入を防ぎます。
3. ライセンス管理を行い、適切な処理を行います。

大きく３つの処理にわけて説明します。

この章で説明する処理に関しては､インストール後の設定作業を完了していることを前提とします (第4章を参照)。

## 5.1. Filescannerのアップデート

Filescannerは本体のモジュール、AVエンジン、ウイルスデータベースの更新を行うことが可能です。

ProScanモジュールはプロマークの更新用サーバーからダウンロードできます。更新用サーバーのURLを次に示します。

http://update.promark-inc.com
http://update.promark-inc.com:8001

AVエンジン､ウイルス データベースの更新用サーバはエンジン開発元のドイツAvira社より直接ダウンロードします。更新用サーバのURLを以下に示します。

https://professional.avira-update.com/update
https://professional.avira-update.net/update

これらのサーバーのアドレスは、設定ファイルに記述されています。（UpdateHostまたはSavapiUpdateHost）

設定ファイルには複数のアップデートサーバを指定することが可能です。
ウイルス データベースの更新は、**proscanup**モジュールが実行します。

**proscanup**モジュールの設定は、**filescan.conf**構成ファイルの [**updater.***] オプションですべて行えます (付録-A.2を参照)。

複雑なLANを組んでいる場合は、最新のウイルス データベースを毎日ダウンロードして所定のネットワーク ディレクトリに格納し、クライアント コンピュータがそのディレクトリからダウンロードできるようにネットワークを設定することをお勧めします。

ウイルス データベースの更新は、**cron**を使用して実行するか (第5章5.1.1を参照)、またはコマンド ラインから実行します (第5章5.1.2を参照)。

インストーラは自動でcron設定を行います。crontabに既に別のプログラムを登録している場合には、それらがきちんと登録されているか確認してください。（インストーラが書き換えて止めていないように。インストーラはインストール時にバックアップを/tmp/crontab.filescanとして残しています。）

また、環境によっては直接ダウンロードサイトに接続できない場合も考えられますので、HTTP Proxyを経由したダウンロードも可能となっております。ProScanでは、モジュールとパターンファイルで別々のダウンロード方法を採用しておりますが、どちらもHTTPによるダウンロードとなっております。モジュールに関してはwgetプログラムによりダウンロードを行いますので、wgetの設定方法はwgetのマニュアルもあわせてご覧ください。

### 5.1.1. アップデート設定

Filescannerのアップデート設定は**filescan.conf**構成ファイルの [**updater.options**] セクションで、適切な値を設定します。次に例を示します。各パラメータ値の詳細は付録Aを参照してください。

```
[updater.options]
KeepSilent=yes
```

```
ReloadApplication=yes
ShowExternalCmdOutput=no
UpdateHost=proscan.promark-inc.com
UpdatePort=80
UpdateProtocol=http
SavapiUpdateHost=https://professional.avira-update.com/update,
    https://professional.avira-update.net/update


[updater.report]
ReportFileName=/var/opt/filescan/log/updater.log
```

## 5.1.2. cronによる自動アップデート方法

cronプログラムを使用すると、Filescannerの更新をスケジューリングできます。インストール時にインストール時刻の分をcronの設定とし、1時間に1回その時刻になるとproscanupが起動します。

1. filescan.confの設定を行います。
2. cronプロセスの動作ルールを設定するためのファイルを開きます（**crontab -e**）。
3. 次の行を入力します。

```
0 * * * * /opt/filescan/bin/proscanup -V
```

4. cronによる実行が行われると結果をメールで知らせます。

インストール時に設定した場合には、上記作業は不要です。インストール時の時刻設定は、アップデートが集中しないように、インストール時の時刻の分を設定しています。(例：10:23にインストールを行えば毎時23分にproscanupが起動されるように設定されます。)

## 5.1.3. コマンドラインからアップデートする方法

Filescannerの更新処理は、コマンド ラインからいつでも実行できます。コマンド ラインで次のように入力します。コマンドラインパラメータについては付録A.5を参照してください。

```
proscanup -V
```

## 5.1.4. モジュールの自動反映について

Filescannerはモジュールの自動更新機能も備えています。アップデートコマンドが実行されると、プロマークのアップデートサイトに接続し、モジュールリストを取得します。このリストの内容に従い、現在のモジュールが古い場合に、新規モジュールをダウンロードし入れ替えることが可能です。この機能を利用するとProScanを常に最新版の状態に保つことができます。

※現在、この機能は停止しております。

自動反映手順

1.アップデートサイトに接続
2.モジュールリストを取得（PSHB21.lst等のプロダクトコードのついたリスト）
3.現在のモジュールのバージョンとリストのバージョンを比較
4.リストのバージョンが新しい場合に、ダウンロードを行う（newディレクトリにダウンロード）
5.ReloadApplication=yesの場合にモジュールの自動反映を行う

（自動反映を行う際に、現状のモジュールのバックアップをoldディレクトリに退避、新しいモジュールのサイズ、実行可能かチェックを行い、正しい場合のみ反映を行う仕組みになっています。）

## 5.2. ファイル システムのウイルス チェックについて

サーバーのファイル システムをウイルスから保護するには、**proscanfs**モジュールを使用します。**proscanfs**はサーバーのファイルに対してウイルス チェックを行い、感染ファイルや感染の疑いがあるファイルを検知すると、設定に従って処理します。オブジェクトの処理としては、ログやサーバー コンソールへの出力、管理者への通知などのような情報提供と、ウイルスの駆除、オブジェクトの検疫場所への移動、感染オブジェクトの除去などのオブジェクト変更があります。

**proscanfs**モジュール関連の設定は、構成ファイル**filescan.conf**の [**scanner.***] オプションですべて行えます (付録A.2を参照)。

サーバーのファイル システムのウイルス チェックは、コマンド ラインから手動で実行するか、標準の**cron**ユーティリティを使用してスケジューリングを設定します。ウイルス チェックは、サーバーのすべてのファイル システムに対して実行することも、特定のディレクトリやファイルだけをチェックすることもできます。

次にサーバーのファイル システムをウイルスから保護するための典型的な作業について、詳しく説明します。

サーバー全体のウイルス チェックを行うと、大量のリソースを消費し、ウイルス チェックの実行中、サーバーのパフォーマンスが低下することに留意してください。ウイルス チェックとほかのプロセスを同時に実行することはお勧めできません。サーバー全体ではなく、特定のディレクトリに対してウイルス チェックを行うとこの問題を回避できます。

### 5.2.1. 指定ファイルのスキャンを行う

特定のファイルに対してウイルススキャンを行うには、コマンドラインから以下のコマンドを投入してファイルをスキャンします。

```
/opt/filescan/bin/proscanfs /home/hoge.doc
```

スキャンの結果は以下のように表示されます。

```
/opt/filescan/bin/proscanfs /home/hoge.doc
ProScan now starting!
ProScan File scanner Ver.6.0.4.1 starting...
All Rights Reserved,Copyright(C) 2003-2018 Promark Inc.

scan results --------------------
 directories :       0
       files :       1
      alerts :       0
   scan time : 00:00:00
--------------------------------
```

1つのファイルを処理したことを示しています。
また、mbox形式のメールファイルをスキャンすると以下のようになります。

```
# /opt/filescan/bin/proscanfs /var/spool/mail/test
ProScan now starting!
ProScan File scanner Ver.6.0.4.1 starting...
All Rights Reserved,Copyright(C) 2003-2018 Promark Inc.

File: /var/spool/mail/test
Date: 2014/05/15 15:05:01    Size: 1,640,186 byte
Result: infected! >>> Mailbox_[From: MAILER-DAEMON@proscan.promark-inc.com (Mail Deliv
System)][Subject:Undelivered Mail Returned to Sender].mim --> file2.mim --> eicarcom2.
eicar_com.zip --> eicar.com <<< Eicar-Test-Signatur

scan results --------------------
 directories :       0
       files :       1
      alerts :       1
   scan time : 00:00:07
--------------------------------
```

## 5.2.2. ディレクトリをスキャンする

proscanfsの r オプションを使うと、ディレクトリは再帰スキャンが可能となります。 r オプションを付けてディレクトリのスキャンを行うと、ディレクトリ配下のファイルもスキャンし、ディレクトリがあればさらにそのディレクトリ配下をスキャンしていきます。（再帰スキャン）

以下、実行例です。

```
# /opt/filescan/bin/proscanfs -r /home/test
ProScan now starting!
ProScan File scanner Ver.6.0.4.1 starting...
All Rights Reserved,Copyright(C) 2003-2018 Promark Inc.

File: /home/test/1074743081-RAV8116
Date: 2004/01/22 13:09:43    Size: 379,372 byte
Result: infected! >>> pop3wGTtTO.mail --> LOVE.zip --> LOVE-LETTER-FOR-YOU.TXT.vbs <<<
VBS/LoveLetter.D

File: /home/test/54MO2h028638
Date: 2004/04/21 16:19:23    Size: 41,813 byte
Result: infected! >>> file0.mim --> file1.txt <<< Worm/NetSky.P.Expl

File: /home/test/virus/body_virus.txt
Date: 2004/03/28 22:32:35    Size: 445 byte
Result: infected! >>> file0.txt <<< Eicar-Test-Signatur

File: /home/test/mbox
Date: 2004/05/12 15:11:40    Size: 3,852,615 byte
Result: infected! >>> Mailbox_[From: MAILER-DAEMON@proscan.promark-inc.com (Mail Delivery
System)][Subject:Undelivered Mail Returned to Sender].mim --> file2.mim --> eicarcom2.zip
--> eicar_com.zip <<< ...

File: /home/test/NetSky.D.mail
Date: 2004/03/03 23:56:50    Size: 25,536 byte
Result: infected! >>> virus-20040302-012631-42056-02-4.gz -->
virus-20040302-012631-42056-02-4 --> file2.mim --> document_excel.pif <<<
Worm/Netsky.D.Dam

File: /home/test/Netsky.D.error.mail
Date: 2004/03/04 00:15:43    Size: 31,102 byte
Result: infected! >>> file2.mim --> document_excel.pif <<< Worm/Netsky.D.Dam

scan results --------------------
 directories :      251
       files :     4994
      alerts :        6
   scan time : 00:03:14
------------------------------
```

## 5.2.3. その他のファイルスキャン機能

ローカルファイルシステムのスキャンには、さまざまな付加機能があります。それらの機能について一覧でまとめて以下に示します。詳細については第6章で説明します。

| 機能 | コマンドラインスイッチ | 内容 |
|---|---|---|
| リンク先チェック | s/S | シンボリックリンク先のファイルもチェックするかどうか指定します。デフォルトではチェックします。 |
| 対象外ファイル指定 | E | スキャン対象外にするファイルをPosix準拠の正規表現で記述します。複数指定はコロン(:)で区切ってください。 |
| 対象ファイル指定 | I | スキャン対象とするファイルをPosix準拠の正規表現で記述します。複数指定はコロン(:)で区切ってください。 |
| 対象オブジェクト指定 | m | 対象となるオブジェクトを指定します。 |
| アクション指定 | C/D/M | オブジェクトにマッチした場合の処理を指定します。Cはチェックのみ、Dは削除、Mは指定ディレクトリに移動します。 |

| | | |
|---|---|---|
| 結果出力 | o <filename> | 結果の出力先を指定します。 |
| メール送付 | a <addoress> | 結果をメールで送付します。設定によりアラートが発生した場合のみメールを送付することも可能です。(デフォルト動作) |
| ログファイル指定 | l <filename> | ログファイル名を指定します。デフォルトはFilescanner.logです。 |
| ログレベル指定 | L <level> | ログの出力レベルを指定します。 |
| レポートレベル指定 | n <level> | コンソールに出力するレベルを指定します。 |

現バージョンではサイズが2GB以上のファイルに対してもスキャンが可能です。また、アーカイブファイルの場合にスキャンするファイル数の制限をかけられますので、ファイル数が多くスキャンに時間がかかるような場合には、この制限を付けてスキャンを実施、ファイル数の多いアーカイブを別途スキャンするような運用を行うことをお勧めします。

## 5.3. ライセンス キーを管理する

ライセンス キーは、Filescannerの使用権をお客様に供与するものです。ライセンス キーには、ライセンスの種別、有効期限、保護対象ドメイン数またはユーザ数の上限 (ライセンス種別によって異なる)、販売店の情報など、お客様が購入したライセンスに関する必須情報がすべて記述されています。

ライセンスを供与されたお客様は、契約期間中、Filescannerのほかに次のサービスをご利用いただけます。

・E-Mailによるテクニカル サポート

・毎日のウイルス データベース更新

・製品のパッチ プログラム入手

・新バージョンへのアップグレード

・新種のウイルスに関する最新情報の入手

ライセンスが失効すると、これらのサービスを自動的に利用できなくなります。サーバーのファイル システムのウイルス チェックは引き続き実行できますが、ウイルス データベースを更新する機能が利用できなくなるため、ライセンス失効時点のデータベースしか使用できません。

ライセンス キーに保存されている情報を定期的に確認し、有効期限を常に把握しておいてください。

ライセンスを確認するには、filescanner.logに記録される情報を見てください。

### 5.3.1. ライセンスを更新する

Filescannerのライセンスを更新すれば、ウイルス データベースの更新をはじめとするFilescannerの機能をすべて引き続きご利用いただけます。

ライセンス期間は、ご購入時に選択したライセンスの種別によって異なります。

**Filescanner のライセンスを更新するには：**

ご購入元に連絡し、Filescannerのライセンス更新料をお支払いください。

または

プロマークに直接連絡してライセンスを更新します。販売部門 (sales@promark-inc.com) 宛にEメールを送信してください。

購入したライセンス キーはインストールする必要があります。インストールするには、キー格納用ディレクトリにライセンス キーをコピーし、サーバーを再起動します。キー格納用ディレクトリとは、構成ファイルの**LicensePath**パラメータで指定したディレクトリのことです。filescan.keyを置き換えることで新たに1年間利用が可能となります。

# 第6章　詳細設定

## 6.1. サーバーのファイル システムのウイルス チェック機能を設定する

サーバーのファイル システムのウイルス チェックを行うパラメータは、次の設定項目でグループ分けされています。

- ウイルス チェックの対象範囲 (第6章6.1.1を参照)
- ファイルのウイルス チェック・駆除のモード (第6章6.1.2を参照)
- ファイルに適用するアクション (第6章6.1.3を参照)
- 処理結果レポートの生成 （第6章6.4を参照)

次に、これらの各グループについて説明します。

### 6.1.1. ウイルス チェックの対象範囲

ウイルス チェックの対象範囲は、次の３つの要素に分けられます。

- **ウイルス チェック パス** — ウイルス チェックを行うディレクトリとファイル
- **ウイルス チェック対象外オブジェクト** — ウイルスチェック対象外となるファイル名
- **ウイルス チェック対象オブジェクト** — ウイルスチェックを行うファイル

デフォルトでは、ファイル システムでチェック可能なオブジェクトがすべて対象となります。

サーバーのすべてのファイル システムをチェックするには、コマンド ラインでルートファイル システム「/」を指定します。但し、これはシステムに大きな負荷を与えます。

ウイルス チェック パスを指定するには、次のいずれかの方法を使用します。

- モジュールを起動する際、完全パスまたは相対パスを使用して、ディレクトリやファイルを指定します。複数のディレクトリやファイルを指定する場合は、空白で区切ります。
- パスの一部をウイルス チェック対象から除外するには、構成ファイル**filescan.conf**内で、ウイルス チェック対象から除外するファイル マスクとディレクトリ マスクを指定します ([**scanner.options**] セクションの**Exclude**パラメータ)。
- 逆に、指定パスのみチェックする場合には、**Include**パラメータでそのファイルまたはディレクトリを指定します。
- ディレクトリに対する再帰的ウイルス チェックを有効にします。有効にするには、[**scanner.options**] セクションの**Recursion**パラメータを変更するか、またはコマンド ラインで**-r**キーの設定を変更します。

### 6.1.2. ファイルのウイルス チェックと駆除のモード

感染ファイルの発見時のアクションは、サーバのファイルシステムをウイルスから守る上で重要な設定項目です。

```
[scanner.object]
MatchAction=none
```

このオプションは、デフォルトでは”none”になっており、ウイルス チェックでウイルス、感染の疑いがあるファイル、暗号化アーカイブの検出のみ行います。通知は、コンソールとレポートにメッセージを出力するという形で行われます (第6章を参照)。

ウイルス チェックを完了すると、すべてのファイルに次のいずれかのステータスが割り当てられます。

- **Ok —** このファイルでウイルスは検知されませんでした。
- **Infected —** このファイルはウイルスに感染しています。

・**Suspicious —** このファイルのコードは、未知のウイルスのコードに類似しています。

・**Error—** 何らかの原因で正しくスキャンできませんでした。

・**Protected —** このファイルはパスワードで保護されています。

### 6.1.3. ファイルに適用するアクション

ファイルに適用できるアクションは、そのステータス (第6章6.4.1参照) によって異なります。デフォルトでは、一定のステータスのファイルの感染が検知された場合にのみ通知が行われます。このような通知メッセージは、コンソールとレポートに出力されます。

なお、ステータスが**Infected**、**Suspicious**、**Protected**および**Error**のファイルに対しては、次のアクションを設定できます。

・**特定のディレクトリに移動する —** 特定のステータスのファイルをあらかじめ設定したディレクトリに移動します。これらのファイルは、パス名、属性そのままで移動されます。(**move**)

・ファイル システムから**ファイルを削除する**。(**delete**)

・チェックのみで**何もしない**。(**none**)

ファイルに適用するアクションを選択するには、次のいずれかの方法を使用します。

・デフォルトのアクションは、構成ファイル**filescan.conf**の [**scanner.object**] セクションで設定します（詳細については付録A.2を参照してください）。

・代替構成ファイルでアクションを設定し、モジュール起動時にその代替構成ファイルを指定します。

モジュール起動時にコマンド ラインで構成ファイルを指定しなかった場合は、**filescan.conf**で指定したパラメータが使用されます。**filescan.conf**をモジュール起動時に明示的に指定する必要はありません。

・現在のセッションに適用するアクションを設定するには、proscanfsモジュール起動時に、コマンド ラインのキーを使用します (付録A.3を参照)。

### 6.1.4. 更新ファイルのみチェックするモード

ファイルの更新時間を調べ前回チェック時より更新されたファイルのみスキャンすることが可能です。そのモードを利用する場合には構成ファイル**filescan.conf**の**[scanner.options]**セクションの**UpdateOnly**パラメータを**yes**に設定してください。前回のチェック時刻は同じく構成ファイルの**[path]**セクションの**CheckStartTimeFile**パラメータに設定されたファイルに記録されています。
このモードを利用することにより、チェック時間の短縮が図れます。

但し、この機能は簡易的なものなのでファイルの更新タイミングによっては再度チェックされる場合もあります。

## 6.2. savapiプロセスの動作

これまでに説明してきたとおり、ファイルシステムののウイルス チェックは、proscanfsモジュールが行います。

savapi（スキャンエンジン）は、proscanfsの起動時に利用可能なエンジンがなければ自動的に呼び出され、処理が終了すると自動的に終了します。（起動済の場合は、起動されているエンジンを流用します。）起動させたくない場合には「AVEAutoStart=no」を設定してください。

root以外のユーザが自身のUIDで実行するような場合には、以下の方法で起動して下さい。

`/usr/lib/AntiVir/savapi --config=`*config_file_path* `--socket-file=`*socket_file_path*

*socket_file_path*の書式は「格納ディレクトリのパス`/.savapi4_`*UID*`.0`」となります。

## 6.3. 日付と時刻の表現形式を変更する

Filescannerの実行時、各モジュールに関するレポートが生成され、それと同時に管理者にさまざまな情報が通知されます。これらの情報には必ず、その情報の生成日時が付加されます。

デフォルトでは、strftime規格に準拠した次の日時形式が使用されます。

%H:%M:%S — 日付の表示形式

%d/%m/%y — 時刻の表示形式

管理者は、日時の表現形式を変更できます。変更するには、構成ファイル**filescan.conf**の **[locale]** セクションで行います。設定可能な形式は次のとおりです。

%I:%M:%S %P — 12時間表示の時刻形式 **(TimeFormat**パラメータ**)**
%y/%m/%dおよび%m/%d/%y — 日付の形式 **(DateFormat**パラメータ**)**

## 6.4. Filescannerのレポート生成パラメータ

Filescannerの各モジュール動作結果はすべてレポートに記録され、そのレポートがファイルに出力されます。

サーバーのファイル システムに対するウイルス チェックの結果は、コンソールにも出力されます。デフォルトでは、コンソールとレポートに同じ情報が出力されます。コンソールとレポートに出力する情報を変更するには、追加設定を行う必要があります。詳細については、第 6 章6.4.3を参照してください。

出力される情報は、レポートレベルで変更できます。Filescannerはレベルをビットの重み付けであらわします。論理和をとることで出力させたい情報を選択することが可能です。

次の表に、レポート情報レベルのリストを示します。

| レベル | Webminでのレベル名 | 意味 |
|---|---|---|
| 0 | | 0 を指定すると何も出力されなくなります。 |
| +1 | エラー関連 | エラー（アクションを実行できないためにプログラムが停止する）に関する情報のみ出力。 |
| +2 | コンフィグ関連 | filescan。Confファイル読み込み時の処理を出力。 |
| +4 | ライセンス関連 | ライセンスに関わる情報を出力。 |
| +8 | ファイルスキャン関連 | ファイルのスキャンに関する情報を出力。 |
| +16 | AVエンジン関連 | ウイルス チェック関連メッセージを出力。 |

| | | |
|---|---|---|
| +64 | メール送信関連 | 結果メール送信関連の情報を出力。 |
| +128 | アップデート関連 | アップデートに関連する情報を出力。（proscanup） |
| +8192 | デバッグ情報 | デバッグに関する情報を出力。 |

レベル１～４は各モジュール共通です。128はproscanupが出力します。proscanfsが出力するメッセージは上記とは別にコントロールされます。

上記の情報レベルに従って出力される情報は、一般に次の形式で表示されます。

```
[date time]-[pid] STRING
```

パラメータの説明：

[*date time*] — システムによって生成されるパラメータ。このパラメータは、日付と時刻（管理者が設定した形式）とレポート情報レベル（レベルの先頭の文字）で構成されます。

日付と時刻の形式は、構成ファイル**filescan.conf**の **[locale]** セクションで変更できます。

[*pid*]－プロセスIDです。

*STRING* — レポートの行。形式はメールの種類によって異なります。メッセージの種類は次のとおりです。

- ウイルス チェックに関するメッセージ (6.5.1を参照)
- その他のメッセージ (モジュールの起動、ウイルス データベースの読み込み、リターン コードなど。6.4.2を参照)
- コンソールに出力されるメッセージ (6.4.3を参照)

それぞれのメッセージの種類と形式については、後述します。

## 6.4.1. ウイルス チェックに関するメッセージの形式

ウイルス チェックに関するメッセージは、各種モジュールとproscanfsとproscanavに対してのみ生成されます。

ウイルス チェックに関するメッセージは次のとおりです。

・スキャン結果メッセージ

```
scan result: result
```

・感染時のサブメッセージ

```
>>> archive_file_name <<< virus_name
```

パラメータの説明：

*result* – ウイルスのチェック実行後に、ファイルに割り当てられるステータス。このパラメータの種類については、後述の表に示します。

*archive_file_name* — チェックしたファイル名です。圧縮アーカイブの場合には展開後のファイル名が ”-->” に続いて表示されます。Infectedの場合のみ表示されます。

*virus_name* — ウイルスの名前。Infectedの場合のみ表示されます。

| 結果(result) | 意味 |
|---|---|
| ok | このファイルは感染していません。 |
| infected | このファイルは1つ以上のウイルスに感染しています。 |
| suspicius | このファイルは、未知のウイルスに感染している疑いがあります。 |
| error | エラーが発生したため、このファイルのウイルス チェックを実行できません (例：破損しているアーカイブなど)。 |

| | |
|---|---|
| protected | このファイルは暗号化されているため、ウイルス チェックできません。 |
| other | 上記以外の理由でチェックできません。 |
| not scan | システム的なエラーでウイルスチェックできません。 |

## 6.4.2. その他のメッセージの形式

ウイルス チェックに関するメッセージ以外にも、モジュールの起動やライセンス キーの読み込みなどの情報を示すメッセージが生成されます。これらのメッセージの形式は次のとおりです。

- モジュールの起動およびウイルス データベースに関するメッセージ
- 読み込んだライセンス キーに関するメッセージ
- ファイルに適用したアクションに関するメッセージ

## 6.4.3. コンソールに出力されるメッセージの形式

メッセージをコンソールに出力できるのは、**proscanfs**と**proscanup**です。

**proscanfs**モジュールの起動時にコマンド ラインで**-q**キーを使用するかどうかによって、**proscanfs**モジュールでコンソールに情報を出力するかどうかが決まります。このキーを指定すると、コンソールに情報が出力されません。**proscanup**モジュールの動作に関するメールをコンソールに出力するには、構成ファイルで**KeepSilent=no**と指定するか、**-V**オプションを使用します。

**proscanfs**モジュールのコンソールに出力される情報の内容は、変更できます。変更するには、構成ファイル(**filescan.conf**または代替構成ファイル) に [**display**] セクションを追加します。詳細については、付録A.2を参照してください。

このセクションでは、アーカイブのオブジェクトに対するウイルス チェック情報、およびモジュールの処理の進行状況を表示するかどうかを設定できます。

ウイルス チェック レポートの情報レベルを変更するには、[**display**] セクションを追加したうえで、コマンドラインで**–L <option>**キーを指定します。

## 6.4.4. レポートファイルのローテートについて

各種レポートファイルは、運用中にどんどん肥大化しますので、Filescannerではローテートスクリプトを標準で提供しています。インストール時に${ProScan binディレクトリ}/contrib/rotate_log.shというスクリプトがインストールされますのでこれを**cron**で1日1回（または、サイトの状況に合わせて1週間に1回等適当な間隔で）起動するように設定して下さい。スクリプトは4世代までバックアップを持つようになっています。（それ以上をご希望の方は各自で修正してください。）

以下、crontabへの設定例です。1日1回午前0時にローテートを行う場合。

```
0 0 * * * /opt/filescan/contrib/rotate_log.sh > /dev/null 2>&1
```

# 第7章　設定例

この章では、実際の業務で行うことを想定した設定を例に課題と解決方法として説明します。ここではfilescan.confを直接書き換える方法について説明します。

## 7.1. ファイル システムのウイルス チェックを行う

サーバーのファイル システムをウイルスから保護するには、**proscanfs**モジュールを使用します。**proscanfs**はサーバーのファイルに対してウイルス チェックを行い、感染ファイルや感染の疑いがあるファイルを検知すると、設定に従って処理します。オブジェクトの処理としては、ログやサーバー コンソールへの出力、管理者への通知などのような情報提供と、ウイルスの駆除、オブジェクトの検疫場所への移動、感染オブジェクトの除去などのオブジェクト変更があります。

**proscanfs**モジュール関連の設定は、構成ファイル**filescan.conf**の [**scanner.***] オプションですべて行えます (付録A.2を参照)。

サーバーのファイル システムのウイルス チェックは、コマンド ラインから手動で実行するか、標準の**cron**ユーティリティを使用してスケジューリングを設定します。ウイルス チェックは、サーバーのすべてのファイル システムに対して実行することも、特定のディレクトリやファイルだけをチェックすることもできます。

次にサーバーのファイル システムをウイルスから保護するための典型的な作業について、詳しく説明します。

サーバー全体のウイルス チェックを行うと、大量のリソースを消費し、ウイルス チェックの実行中、サーバーのパフォーマンスが低下することに留意してください。ウイルス チェックとほかのプロセスを同時に実行することはお勧めできません。サーバー全体ではなく、特定のディレクトリに対してウイルス チェックを行うとこの問題を回避できます。

### 7.1.1. コマンド ラインからディレクトリのウイルス チェックを行う

Filescannerは、サーバーの特定のディレクトリに対してウイルス チェックを行えます。

課題：**/home/user**ディレクトリのウイルス チェックを再帰的に行い、ウイルス感染ファイルを検知した場合は除去します。

/home/userディレクトリ内にあるファイルを再帰的に検査（ディレクトリがあればその中身も）チェックします。

処理結果をメールでadmin@proscan.comに送付します。

解決方法：コマンド ラインで次のように入力します。

```
#proscanfs -r -M -a admin@proscan.com -L 15 -q /home/user
```

ディレクトリの構成によっては、シンボリックリンクの関係で再帰的なチェックで無限ループに陥る場合があります。そのような場合を防ぐために、**MaxCheckLevel**パラメータを用意しています。ディレクトリの深度がこの値に達するとそれ以上の再帰チェックを止めます。（デフォルトは50です。50以上の深さのディレクトリをチェックする場合には、この値を大きくしてください。）

## 7.1.2. ディレクトリの毎日のウイルス チェックをスケジューリングする

UNIX OSでは、Filescannerなどスケジューリングされたプログラムは、cronユーティリティで実行します。

課題：毎日0:00に、構成ファイル**/etc/opt/filescan/scanhome.conf**で指定されているウイルス チェック パラメータを使用して**/home**ディレクトリのウイルス チェックを行います。

解決方法：次の手順で行ってください。

1. **/etc/opt/filescan/scanhome.conf**という構成ファイルを新規作成し、必要なウイルス チェック関連パラメータを指定します (第 6 章6.1を参照)。

2. cronプロセスの動作ルールを設定するためのファイルを開き (**crontab -e**)、次のように入力します。

```
* 0 * * * /opt/filescan/bin/proscanfs -c /etc/opt/filescan/scanhome.conf
/home
```

## 7.1.3. オブジェクトを別のディレクトリ (検疫場所) に移動する

Filescannerでは、サーバーのファイル システムで検知されたすべての感染オブジェクトを特別なディレクトリに移動するように設定できます。

この機能は、ディレクトリのウイルス チェック中に重要なデータを保存したファイルの感染が検知された場合場合などに利用できます。これは、ウイルスを駆除するとデータの一部が失われるおそれがあるためです。このような場合には、感染オブジェクトをいったん特別なディレクトリに隔離します。

サーバーのファイル システムに検疫ディレクトリを常に配置しておく場合は、構成ファイルのExcludeパラメータでそのディレクトリの完全パスを指定すると、そのディレクトリがウイルス チェックの対象から除外されます。

課題：**/tmp/download** 配下のすべてのファイルをウイルス チェックし、感染オブジェクトを完全パスの情報と共に**/tmp/infected**ディレクトリに移動します。このとき、反復的なウイルス チェックは無効にします。さらに、感染オブジェクト、感染の疑いのあるオブジェクト、および破損したオブジェクトの情報を、レポート ファイルに出力します。

解決方法：次の手順で行ってください。

1. オブジェクトを検疫場所に移動するようFilescannerを設定します。設定するには、/etc/opt/filescan/filescan.conf設定ファイルで、**[scanner.object]** セクションの SaveDirectory パラメータに、次の行をセットします。

```
SaveDirectory=/tmp/infected
```

2. **ディレクトリ再帰検査**、**シンボリックリンク先検査**を無効にし、**アクション**を**移動**に設定します。これを行うには以下の操作を行います。

```
[scanner.options]
Recursion=no
Symlink=no

[scanner.object]
SaveDirectory=/tmp/infected
MatchAction=move
ScanLevel=1
```

3. コマンド ラインで次のように入力します。

```
#proscanfs /tmp/download
```

または

コマンド ラインで次のように入力します。

```
#proscanfs -m 1 -M -d /tmp/infected /tmp/download
```

Filescannerの検査時の移動は、パス情報を持ったまま指定ディレクトリ先に移動します。ファイルの属性情報もそのままです。

# 第8章　よく寄せられる質問

ここでは、Filescannerのインストール、設定、および使用法に関する質問とその回答を示します。

**質問：**Filescanner は、Linuxのディストリビューション上で動作しますか。

Filescannerは、RedHat、Debianの各ディストリビューション上でテスト済みです。パッケージは、これらのOS用に作成されています。
サポートしているOSのバージョンについては、第1章1.3を参照してください。

ご使用のディストリビューションがサポート対象のOSと完全な互換性を保持している場合(たとえば、ASPLinuxはRedHat Linuxと互換性がある)、重大な問題が発生する可能性はきわめて低いと言えます。

Filescannerは、プロマークのサポート対象リストに掲載されていないディストリビューション上では、正しく動作しない可能性があります。正しく動作しない場合、一般にその原因はOSの特性にあります。たとえば、ご使用のディストリビューションで別のバージョンのライブラリが使用されていたり、システム初期化スクリプトが異なる場所に配置されている可能性があります。このような場合、プロマークのテクニカル サポート サービスではサポートできません。

**質問：**tgz形式またはtar+gz形式のアーカイブを展開するには、どうすればよいですか。

.tgzまたは.tar.gz形式のアーカイブを展開するには、次のコマンドを使用します。

```
tar zxvf <archive_name>
```

詳細については、man (1)の**tar**プログラムの説明を参照してください。

**質問：**なぜキー ファイルが必要なのですか。キー ファイルがなくてもFilescannerは動作しますか。

ライセンス キーがなければ、Filescannerは動作しません。
Filescannerのご購入を検討中の方には、一時キー ファイル (試用版キー) を提供しています。一時キー ファイルの有効期間は30日です。この期間が過ぎると、キーは無効になります。

**質問：**製品ライセンスが失効するとどうなりますか。

失効しても、Filescannerを引き続きご利用になれます。ただし、ウイルス データベース更新機能は使用できません。つまり、古いデータベースを使用してのみ、感染ファイルを検出できます。proscanupモジュールを使用してプロマークのWebサイトから最新のウイルス データベースをダウンロードきなくなります。proscanupを使用せずにダウンロードしたウイルス データベースをFilescannerで使用することはできません。
したがって、新種のウイルスからファイルを保護することはできなくなります。

**質問：**ウイルス データベースを1時間1回更新するよう、crondを設定しています。しかし、proscanupがWgetプログラムを検知しません。なお、コマンド ラインから起動したときには、何の問題もありませんでした。

ここで重要な点は、crondユーティリティは独自の環境変数を使用するということです。この場合、Wgetプログラムへのパスが PATHパラメータの中で指定されていない可能性があります。
Wgetへのパスを追加するには、**/etc/crontab**ファイルのPATH環境変数を変更します。

**質問：**Filescannerが動作しません。どうすればよいですか。
まず、その問題への対策がこのマニュアル (特にこの章) またはWebサイトに記載されているかどうかを確認します。
また、Filescannerの購入元にサポートを依頼するか、弊社のテクニカル サポート サービス

(support@promark-inc.com) 宛にEメールを送信することもできます。
できるだけ早く回答を入手できるようにするため、次の点を守ってください。

1. メールサブジェクトにサーバのOS、問題が発生したモジュールの名前、および問題の概要を記述します。たとえば、「**Linux、ディレクトリがスキャンできない**」等のように記述します。
2. Eメールをテキスト形式で作成します。HTML形式のメールは送信しないでください。
3. メール本文の先頭に、OSとFilescannerパッケージの正確なバージョン、およびキー ファイルの名前を記述します。
4. 問題を簡潔に説明します。サポート サービス要員はEメールを読むとき、ユーザーが抱えている問題について何も知りません。サポート サービス要員が問題を十分に理解し、その現象を再現しなければ、サポートを行えません。
5. 次のデータを1つのアーカイブにまとめ、テクニカル サポート サービスに送信します。
   - **/etc/opt/filescan**ディレクトリのファイル
   - メール システムのレポート ファイル
   - ウイルス チェック モジュールのレポート ファイル (例：**/var/opt/filescan/log/filescan.log**)
   - **ps -ax**コマンドを実行してコンソールに出力された情報
   - キー ファイル
6. ご使用のシステムが次の条件に当てはまるかどうかを、Eメールに記述してください。
   - SCSIコントローラ搭載の有無
   - 非常に古いプロセッサや最新のプロセッサの搭載の有無、または複数プロセッサ構成の有無
   - RAMの容量が64 MB以下または2 GB以上であるかどうか
7. 毎日の概算トラフィック量(MTAであれば)、およびサーバーの負荷が一時的に高くなる時間帯があるかどうかを記述します。

**質問：**コンソールに出力された情報をファイルに保存するには、どうすればよいですか。

Filescannerの動作中にコンソールに出力された情報を保存するには、構成ファイルで適切な設定を行うか (付録A.2を参照)、またはコマンド ラインで次のように入力します。

```
$ some_app > ./text_file 2>&1
```

パラメータの説明：

some_app — ファイルに保存したい、アプリケーション、標準出力、およびエラー メールの行。
text_file — 情報の保存先ファイルへの完全パス。
例：

```
$proscanup > ./updater.log 2>&1
```

上記の場合、proscanupモジュールの標準出力メールとエラー メールが、カレント ディレクトリ内のupdater.logファイルに出力されます。

**質問：**侵入者にウイルス データベースを改ざんされる可能性はありますか。

侵入者がプロマークのWebサイトからウイルス データベースをダウンロードし、ウイルス格納用ディレクトリにコピーする可能性はあります。ただし、そのウイルス データベースはFilescannerの実行時に使用されません。
ウイルス データベースにはそれぞれ一意の署名がなされており、ウイルス データベースを使用する際にFilescannerが検査します。署名が不正であるか、ウイルス データベースの日付がライセンスの失効日より遅い場合、そのウイルス データベースは使用されません。

**質問：**Proxy設定をしたのですが、アップデートできません。

アップデートできない理由は色々と考えられますが、Proxy経由で行う場合にはwgetのProxy設定が正しく行われているか確認してください。FilescannerでのProxy設定はwgetのProxy設定にはんえいされません。別途、設定する必要があります。

# 第9章　Filescannerをアンインストールする

Filescanner をアンインストールするには、次の条件を満たしている必要があります。

・superuser権限（**root**ユーザー、またはUID=0であるユーザー）を持っていること。Filescannerをアンインストールするときにこの権限がない場合は、**root**ユーザーとしてログオンする必要があります。

**サーバーからProScan®FSをアンインストールするには、パッケージを展開したディレクトリに移動し、コマンド ラインで次のように入力します。**

```
./uninstall.sh
```

コマンドを実行すると自動的にアンインストールされます。アンインストールが完了すると、メッセージがコンソールに出力されます。

# 付録A　Filescannerに関する補足情報

この付録では、インストールしたFilescannerパッケージのディレクトリ ツリー (A.1)、構成ファイルの内容 (A.2)、および各モジュールに関するコマンド ライン キーとリターン コード (A.3～A.6) について説明します。メール システムの構成ファイルとウイルス駆除のためのスクリプト ファイルの例を示します。

## A.1　製品ファイルの配置ディレクトリ

デフォルトのパスをそのまま使用してFilescannerをインストールすると、配布ファイルは次の場所に配置されます。（Linux、Solarisの場合）

**/usr/lib/AntiVir/** — AVエンジン（savapi）関連のディレクトリ
　　**savapi** — スキャンエンジン本体
**/etc/opt/filescan/** — Filescannerの構成ファイル、および設定情報を保存したその他のファイルが配置されるディレクトリ
　**filescan.conf** — 構成ファイル
**/opt/filescan/** — ウイルス チェック関連ファイルが配置されているメイン ディレクトリ。このディレクトリの下位には、次のディレクトリとファイルがあります。
　**/opt/filescan/bin/** — Filescanner の実行ファイルが配置されるディレクトリ
　　**proscanfs** — サーバーのファイル システムのウイルス チェックを行うモジュールの実行ファイル
　　**proscanup** — ウイルス データベースを更新するproscanupモジュールの実行ファイル
　　**proscan_avupdate.sh** — アップデート時のラッパースクリプト

**/var/opt/filescan/keys** — ライセンスキーが配置されるディレクトリ

FreeBSDの場合は、上記ディレクトリの/etc/opt/filescanを/etc/filescanに、/opt/filescanを/usr/local/filescanに、/var/opt/filescanを/var/filescanにそれぞれ置き換えて読んでください。以降も同じです。

## A.2　Filescannerの構成ファイル

デフォルトでは、Filescanner には**filescan.conf**という構成ファイルが付属しています。**filescan.conf**では、多数のプログラム動作パラメータが指定されています。ここでは、この構成ファイルのすべてのパラメータ セクションについて詳しく説明します。パラメータにデフォルト設定が用意されていれば、その値があらかじめ指定されています。

**[path]** セクションには、重要なファイルへのパスを定義するパラメータがあります。これらのファイルへのパスを正しく指定しなければ、Filescannerは動作しません。

**LicensePath=/var/opt/filescan/key** — ライセンス キーが保存されているディレクトリへの完全パス
**LocalSocketPath=/var/opt/filescan/run** — savapiプロセスに接続するために使用するローカル ソケットおよびPIDファイルを格納するディレクトリへの完全パス
**TempPath=/var/opt/proscan/tmp** — 一時ファイルを保存するディレクトリへの完全パス
**WgetPath=/usr/sbin/wget** — wgetコマンドへの完全パス（システムに合わせて設定）
**CheckStartTimeFile=/var/run/filescan.start.time** — スキャン開始時刻を記録するファイル

**[locale]** セクションには、メール通知の%SCANSTATUS%マクロを置き換えるテキストと日時の形式を指定するパラメータが含まれます。

**ProtectedMessage** — パスワードで保護されたオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
**SuspiciousMessage** — 疑わしいオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
**ErrorMessage** — スキャンに失敗したオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。
**InfectedMessage** — 感染したオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換える使用するテキストです。
**OtherMessage** — ウイルス チェックに失敗したオブジェクトを通知するメールの%SCANSTATUS%マク

ロを置き換えるテキストです。

**FilteredMessage —** ファイル名、タイプ、サイズ、件名に基づいてフィルタリングされたオブジェクトを通知するメールの%SCANSTATUS%マクロを置き換えるテキストです。

**TimeFormat=%H:%M:%S —** メール通知に表示される、strftime規格に準拠した時刻の形式 12時間表示 (am/pm) に変更するには、**%I:%M:%S %P**と指定します。

**DateFormat=%d/%m/%y —** メール通知に表示される、strftime規格に準拠した日付の形式。日付の形式は、**%y/%m/%d**または**%m/%d/%y**などに変更することもできます。

[**aveserver**] セクションでは、**savapi**モジュールの動作および処理レポートの生成に関するパラメータを指定します。

**ReportFileName=/var/opt/filescan/log/aveserver.log —** AVエンジンの処理結果を記録するレポート ファイルの名前。

**ReportLevel=1 —** レポートの情報レベル

**AVEAutoStart=yes —** savapiエンジンの自動起動を指定します。proscanfs実行時に有効なsavapiエンジンが起動していない場合に「yes」が指定されていると自動的に起動します。デフォルトは「yes」です。

[**scanner.options**] セクションでは、サーバーのファイル システムのウイルス チェックに関するパラメータを指定します。

**Recursion=yes —** ディレクトリを再帰的にチェックするモード。このモードを無効にするには、このパラメータを**no**に設定します。この設定が**no**になっているとディレクトリのチェックは行われません。

**Symlink=yes —** シンボリックリンク先のファイルをチェックするモード。このモードを無効にするには、このパラメータを**no**に設定します。

**SendMail=no —** 結果をメールで送信するモード。このモードを無効にするには、このパラメータを**no**に設定します。送信先アドレスは、**ReportAddress**で設定します。

**SendMailCondition=alert —**結果をメールで送信するモードを指定した場合に、結果によって送信をコントロールするための設定。アラートが発生した場合のみに送信する場合には「alert」を指定します。「all」を指定すると結果のいかんに関わらず、メールを送信します。デフォルトは「alert」です。

**ReportAddress=E-Mail address —** 結果をメールで送信するあて先。

**Subject=" ProScan File Scan Result" —** 結果メールのSubjectを指定。

**MaxScanTime=300 —** ファイルをスキャンするときのタイムアウト値。

**MaxRecursion=0 —** 多重圧縮の深度やMIMEコンテナの入れ子数の制限。0は無制限。

**MaxSize=0 —** 圧縮ファイルを展開できる最大ファイルサイズ。0は無制限。

**MaxRatio=150 —** 圧縮ファイルの伸張比（圧縮時と展開後のサイズ比）。0は無制限。

**MaxCount=0 —** アーカイブファイル内のスキャンファイルのリミット数。0は無制限。

**ReadTimeout=120 —** AVエンジンのソケットタイムアウト値。

**ArchiveScan=yes —** アーカイブファイルのスキャン指定。

**MailboxScan=yes —** メールボックスタイプファイルのスキャン指定。

**RepairFile=no —** マクロウイルス等、駆除可能なウイルスの駆除指定。

**MaxCheckLevel=50 —** ディレクトリの再帰スキャンの最大深度。

**SaveDirectory=Directory name —** 感染オブジェクトの移動先ディレクトリ。

**UpdateOnly=no —** 前回スキャン時から更新されたファイルのみスキャンする場合、yesを指定。デフォルトは「no」です。

[**scanner.object**] セクションでは、セクションでは、サーバーのファイル システムをウイルスから保護する際に各種の単独オブジェクトに適用するアクションを指定します。

**ExcludeMask=mask1:mask2:...:maskN —** ウイルス チェック対象から除外するファイル マスク。デフォルトでは、すべてのファイルが対象となります。このパラメータを指定した場合には、チェック中にこのマスクにマッチするファイルはチェックされません。

**IncludeMask=mask1:mask2:...:maskN —** ウイルス チェック対象とするファイルのマスク。デフォルトでは、すべてのファイルが対象となります。このパラメータを指定した場合には、ここで指定したファイルだけがチェックされます。

**ScanLevel=15 —** アクション対象となるオブジェクトを指定します。スキャン時にこのパラメータで設定したオブジェクトは、**MatchAction**で指定された処理が実行されます。指定方法は以下の4種類を論理和で行います。（ビットの論理和です）デフォルトは15ですべてのオブジェクトが対象です。

・**0 —** 何もしません。チェックのみです。
・**1 —** ウイルス感染オブジェクト。
・**2 —** 暗号化オブジェクト。
・**4 —** 感染の疑いがあるオブジェクト。
・**8 —** スキャンに失敗したエラーオブジェクト。

**MacthAction=action —** 感染ファイルの検知時に実行するアクション。感染ファイルの修復モードが有効になっている場合、ウイルスを駆除できないオブジェクトにこのアクションが実行されます。アクションには、次の値のいずれかを設定できます。デフォルトは「none」です。
・**none —** 何もしません。チェックのみです。
・**move —** ファイルを**SaveDirectory**に反復的に (完全パスを付加して) 移動します。
・**delete —** ファイルを削除します。

[**scanner.report**] セクションでは、proscanfsモジュールの処理結果レポートの生成に関するパラメータを指定します。

**ReportFileName=/var/opt/filescan/log/Filescanner.log —** 処理結果を記録するレポート ファイルの名前
**ReportLevel=3 —** 処理結果のレポート内容を指定します。
・ 1 — エラー
・ 2 — スキャン結果
・ 4 — サマリ
・ 8 — 詳細

[**scanner.display**] セクションでは、モジュールの動作状況 (ウイルス データベース読み込み処理の進行状況およびウイルス チェック中のファイルに関する情報) をリアルタイムで出力するモードに関するパラメータを指定します。

**ShowLevel=255 —** ファイルチェック時の動作をコンソールに出力するレベルを設定します。
**OutputFileName=Filename —** 出力先を指定します。このパラメータが設定されていないとコンソールに出力されます。[scanner.report]の内容との違いは、スキャンしたファイル情報を出力します。

[**scanner.mailer**] セクションでは、**Filescanner**が処理したメールを配信するためのパラメータを指定します。

**NotifyFromAddress=proscan@localhost —** 結果通知の送信元アドレス
**ForwardMailer=smtp:localhost:100026** — MTAの設定

[**updater.options**] セクションでは、**proscanup**モジュールの動作に関するパラメータを指定します。

**ExtraWgetOptions —** Wgetパッケージの情報オプション
**KeepSilent=no —** proscanupモジュールの動作情報をコンソールに出力するモード。このモードを有効にするには、このパラメータをYesに設定します。
**UpdateHost=update.promark-inc.com —** 更新用サーバーのホスト名を設定します。カンマで区切って複数のサーバを指定することが可能です。
**UpdatePort=80 —** 更新用サーバーのポート番号を設定します。
**UpdatePlotocol=HTTP —** 更新用サーバーのプロトコルを設定します。
**ReloadApplication=yes —** ProScan®のモジュールが更新された場合に、モジュールを自動で反映するかどうかを指定します。このパラメータがyesに設定されていると自動で最新モジュールに入れ替わります。
**ShowExternalCmdOutput=no —** 外部プログラム (例：Wget) の情報をコンソールに出力するモード。このモードを有効にするには、このパラメータをyesに設定します。
**HTTPproxyServer=host_name —** Proxy経由でのアップデートを行う場合にProxyサーバのホスト名またはIPアドレスを指定します。
**HTTPproxyPort=8080 —** Proxyサーバのポートを指定します。
**SavapiUpdateHost=Avira社サイト —** savapi関連のアップデート先を指定します。
**ExtraWgetOptions=--no-check-certificate —** wgetに個別オプションを指定する場合に使用します。
**RetryTimes=5 —** 試行回数を指定します。（savapiアップデートに有効）
**RetryInterval=10 —** 試行間隔を秒数で指定します。（savapiアップデートに有効）

[**updater.report**] セクションでは、**proscanup**モジュール動作レポートの生成に関するパラメータを指定します。

**ReportFileName=/var/opt/filescan/log/updater.log —** モジュール処理結果を記録するレポート ファイルの名前

**ReportLevel=1 —** レポートの情報レベル

- 1 — 通常メッセージ
- 2 — 設定ファイル関連メッセージ
- 4 — ライセンス関連メッセージ
- 128 — デバッグメッセージ

## A.3 proscanfsモジュールに関するコマンド ライン キー

プログラムをコマンド ラインから起動する際、構成ファイルのパラメータを変更するには、コマンド ライン キーを使用します。以下に詳しく説明します。

| | | |
|---|---|---|
| ヘルプに関するオプション | | |
| **-h** | | proscanfsモジュールに関するヘルプをコンソールに出力します。 |
| **-v** | | プログラムのバージョンを表示します。 |
| 構成に関するオプション | | |
| **-c <file_path>** | | 代替構成ファイル**<file_path>**を使用します。 |
| ウイルス チェックに関するオプション | | |
| **-r/R** | | ディレクトリ再帰チェックの有効・無効を切り替えます。 |
| **-s/S** | | リンク先チェックの有効・無効を切り替えます。 |
| **-E <mask1:…>** | | 対象外ファイルを指定します。 |
| **-I <mask1:…>** | | 対象ファイルを指定します。 |
| **-m <objects>** | | 対象となるオブジェクトを指定します。 |
| | **1** | ウイルス感染ファイル |
| | **2** | 暗号化されているファイル |
| | **4** | ウイルスの感染が疑わしいファイル |
| | **8** | チェックでエラーとなったファイル |
| **-C** | | チェックのみの動作となります。 |
| **-D** | | 上記オブジェクトにマッチした場合にそのファイルを削除します。 |
| **-M** | | 上記オブジェクトにマッチした場合にそのファイルを移動します。 |
| | | ※オプションC, D, Mは排他関係にあります。 |
| **-d <path>** | | Mオプションが指定された場合の移動先を指定します。 |
| レポート生成に関するオプション | | |
| **–q** | | メッセージをコンソールに出力しません。 |
| **-o <fname>** | | 処理結果を出力するファイルの名前を設定します。ファイル名を設定しない場合、コンソールに出力されます。 |
| **-a <address>** | | 処理結果をメールで送付します。 |
| **-l <fname>** | | ログファイルを指定します。 |
| **-L <level>** | | ログに格納される情報を設定します。**<level>**に次の情報レベルを指定できます。 |
| | **1** | エラーメッセージを出力します。 |
| | **2** | スキャン内容を出力します。 |
| | **4** | 設定内容を出力します。 |
| | **8** | ファイル処理に関するメッセージを出力します。 |

**16** 詳細メッセージを出力します。

**-n <level>** コンソールに出力するウイルス チェック レポートの情報レベルを設定します。**<level>**に次の情報レベルを指定できます。

**1** サマリ表示します。

**2** 感染ファイルを表示します。

**256** 非感染ファイルも出力します。

## A.4 proscanfsモジュールのリターン コード

proscanfsモジュールの実行中に返されるコードは、次のとおりです。

**0** 正常終了しました。

**1** オプションが足りません。

**2** 不正なパラメータです。

**3** 設定ファイルが読み込めません。

**4** ログファイルがオープンできません。

**5** ライセンスが異常です。

**99** ファイルが指定されていません。

## A.5. proscanupモジュールに関するコマンド ライン キー

| | |
|---|---|
| ヘルプに関するオプション | |
| **-h** | **proscanup**モジュールに関するヘルプをコンソールに出力します。 |
| **-v** | プログラムのバージョンを表示します。 |
| アップデート処理時に使用されるオプション | |
| **-c <file_path>** | 代替構成ファイル**<file_path>**を使用します。 |
| **-U <URL>** | アップデートサーバのURLをhttp://update.hoge.domain:8080の形式で指定します。 |
| レポート生成に関するオプション | |
| **-l <file_path>** | モジュールの処理結果を**<file_path>**に記録します。 |
| **-r** | 設定ファイルの内容によらずモジュールの反映を行います。 |
| **-f** | モジュールの強制ダウンロードを行います。 |
| **-q** | メッセージをコンソールに出力しません。 |
| **-V** | メッセージをコンソールに出力します。 |

## A.6. proscanupモジュールのリターン コード

proscanupモジュールの実行中に返されるコードは、次のとおりです。

**0** 正常に処理が終了しました。

**0以外** 更新処理に失敗しました。

# 付録B　お問い合わせ先

ご質問やご意見がございましたら、代理店またはプロマークにご連絡ください。製品のインストールや管理について、どのようなことでもEメールにて承ります。お送りいただいたご意見やご提案は、弊社にて十分に検討いたします。

| | |
|---|---|
| テクニカル サポート | テクニカル サポートの詳細については、<br>http://**www.promark-inc.com/index.html**をご覧ください。 |
| その他、製品やサービスに関するお問い合わせ窓口 | 現在のところ電子メールによるお問い合わせのみです。<br>Eメール：**support@promark-inc.com** |

ProScan Anti-Virus for Filescanner
バージョン6.0.4

# 管理者ガイド　第9版

発行日　2018年12月1日
作成元　株式会社プロマーク

promark

株式会社プロマーク