

**SOPHOS**

Security made simple.

# Sophos Anti-Virus for Linux 環境設定ガイド

製品バージョン: 9



# 目次

1	このガイドについて.....	5
2	Sophos Anti-Virus for Linux について.....	6
2.1	Sophos Anti-Virus とは.....	6
2.2	Sophos Anti-Virus の保護機能.....	6
2.3	Sophos Anti-Virus の使い方.....	6
2.4	Sophos Anti-Virus の設定方法.....	6
3	オンアクセス検索.....	8
3.1	オンアクセス検索が有効になっていることを確認する.....	8
3.2	コンピュータの起動時にオンアクセス検索が自動で開始することを確認する.....	8
3.3	オンアクセス検索を開始する.....	8
3.4	オンアクセス検索を停止する.....	9
4	オンデマンド検索.....	10
4.1	オンデマンド検索を実行する.....	10
4.2	オンデマンド検索を設定する.....	11
5	ウイルスが検出された場合の動作.....	14
6	ウイルスのクリーンアップ.....	16
6.1	クリーンアップ情報を入手する.....	16
6.2	感染ファイルを隔離する.....	16
6.3	感染ファイルをクリーンアップする.....	17
6.4	ウイルスの副作用から復旧する.....	18
7	Sophos Anti-Virus ログの表示.....	19
8	Sophos Anti-Virus の即時アップデート.....	20
9	カーネル対応について.....	21
9.1	最新のカーネルへの対応について.....	21
9.2	カスタマイズされたカーネルへの対応について.....	21
10	スケジュール検索の設定.....	22
10.1	ファイルから読み込んでスケジュール検索を追加する.....	22
10.2	標準入力からスケジュール検索を追加する.....	22
10.3	特定のスケジュール検索をファイルに出力する.....	23
10.4	すべてのスケジュール検索の名前をファイルに出力する.....	23
10.5	特定のスケジュール検索を標準出力する.....	23

10.6	すべてのスケジュール検索の名前を標準出力する.....	23
10.7	ファイルから読み込んでスケジュール検索を更新する.....	24
10.8	標準入力からスケジュール検索を更新する.....	24
10.9	スケジュール検索のログを表示する.....	25
10.10	スケジュール検索を削除する.....	25
10.11	すべてのスケジュール検索を削除する.....	25
11	警告の設定.....	26
11.1	デスクトップ・ポップアップ警告を設定する.....	26
11.2	コマンドライン警告を設定する.....	27
11.3	メール警告を設定する.....	27
12	ログの設定.....	30
13	アップデートの設定.....	31
13.1	用語の解説.....	31
13.2	savsetup 設定コマンド.....	31
13.3	コンピュータの自動アップデートの設定内容を確認する.....	32
13.4	アップデートサーバーを設定する.....	32
13.5	複数のアップデートクライアントのアップデートを設定する .....	33
13.6	1台のアップデートクライアントのアップデートを設定する.....	34
14	Sophos Live Protection の設定.....	35
14.1	Sophos Live Protection の設定を確認する.....	35
14.2	Sophos Live Protection を有効/無効に切り替える.....	35
15	オンアクセス検索の設定.....	36
15.1	オンアクセス検索のファイル割り込み方法を変更する.....	36
15.2	検索の対象からファイルとディレクトリを除外する.....	36
15.3	検索の対象からファイルシステムの種類を除外する.....	38
15.4	アーカイブファイル内を検索する.....	38
15.5	感染ファイルをクリーンアップする.....	38
16	追加ファイルベースの環境設定について.....	40
16.1	追加ファイルベースの環境設定について.....	40
16.2	追加ファイルベースの環境設定を使用する.....	41
16.3	追加ファイルベースの環境設定を更新する.....	44
16.4	環境設定レイヤーについて.....	44
16.5	savconfig 設定コマンド.....	45
17	トラブルシューティング.....	47
17.1	コマンドを実行できない.....	47
17.2	除外の設定内容が適用されていない.....	47

17.3 「マニュアル ... は登録されていません」といった内容のシステムエラーが表示される.....	48
17.4 ディスク容量が足りなくなる.....	49
17.5 オンデマンド検索のスピードが遅い.....	49
17.6 オンデマンド検索済みのファイルがすべてアーカイバでバックアップされる.....	50
17.7 ウイルスがクリーンアップされない.....	50
17.8 ウイルス フラグメントが報告される.....	51
17.9 ディスクにアクセスできない.....	52
18 補足: オンデマンド検索のリターンコード.....	53
18.1 拡張リターンコード.....	53
19 補足:使用情報をソフォスに送信する機能の設定.....	55
20 補足:RMS の再起動の設定.....	56
21 用語集.....	57
22 テクニカルサポート.....	59
23 ご利用条件.....	60

# 1 このガイドについて

このガイドは、Sophos Anti-Virus for Linux の使用方法や設定方法について説明しています。  
インストールに関しては以下をご確認ください。

Sophos Central から一元管理を行う形態で Sophos Anti-Virus をインストールするには、  
Sophos Central にログインして「ダウンロード」ページを開き、表示される手順に従って  
ください。

Sophos Enterprise Console から一元管理を行う形態で Sophos Anti-Virus をインストールす  
る方法については、「**Sophos Enterprise Console スタートアップガイド Linux/UNIX 版**」  
を参照してください。

社内ネットワークに接続している/接続していない Linux マシンに、一元管理を行わない  
Sophos Anti-Virus をインストールまたはアンインストールする方法については、「**Sophos  
Anti-Virus for Linux スタートアップガイド**」を参照してください。

ソフォスの製品ドキュメントは次のサイトから入手可能です。  
<http://www.sophos.com/ja-jp/support/documentation.aspx>

**重要:** このガイドでの設定情報は Sophos Linux Security にも適用されます。

## 2 Sophos Anti-Virus for Linux について

### 2.1 Sophos Anti-Virus とは

Sophos Anti-Virus は、Linux コンピュータ上のウイルス (ワームやトロイの木馬を含む) を検出・処理するソフトウェアです。Linux を狙うすべてのウイルスを検出することはもちろん、Linux コンピュータに潜む Linux 以外のコンピュータを狙うウイルスもすべて検出できます。Sophos Anti-Virus はコンピュータの検索を実行してウイルスを検出します。

### 2.2 Sophos Anti-Virus の保護機能

オンアクセス検索は最もよく使うウイルス対策機能です。ファイルを開く、コピー、あるいは保存するときに Sophos Anti-Virus で検索が実行され、安全な場合のみファイルへのアクセスが許可されます。

これに加え、Sophos Anti-Virus にはオンデマンド検索機能も備わっています。オンデマンド検索は、ユーザーが手動で開始する検索です。ファイルを個別に検索するのはもちろんのこと、ユーザーが読み取り権限を持つすべてのローカルファイルを検索することもできます。オンデマンド検索は手動で実行することもできれば、スケジュールを設定して指定した日時にも実行することもできます。

### 2.3 Sophos Anti-Virus の使い方

すべての操作はコマンドラインインターフェース (CLI) から実行します。

オンデマンド検索の実行に使用される `savscan` 以外のコマンドを実行するには、`root` としてコンピュータにログオンする必要があります。

このガイドは、デフォルトのインストールディレクトリ `/opt/sophos-av` に Sophos Anti-Virus をインストールしていることを前提に書かれています。ここで説明するコマンドのパスは、このディレクトリを基準にしています。

### 2.4 Sophos Anti-Virus の設定方法

Sophos Anti-Virus を設定する方法は、ソフォスの管理ソフト (Sophos Enterprise Console または Sophos Central) を使用するかどうかによって異なります。

#### Enterprise Console または Sophos Central の管理下にあるコンピュータ

Linux コンピュータが Enterprise Console または Sophos Central で管理されている場合は、次のように Sophos Anti-Virus を設定します。

- 管理コンソールから**オンアクセス検索、スケジュール検索、警告、ログ、およびアップデート**機能を一元的に設定する。詳細は管理コンソールのヘルプを参照してください。

**注:** これらの機能の中には管理コンソールから一元的に設定できないパラメータもあります。コンソールから設定できないパラメータは、各 Linux コンピュータのローカル環境で Sophos Anti-Virus CLI を使用して設定してください。管理コンソールではこれらの設定は無視されます。

**注:** Sophos Central で管理される 64ビット版の Linux サーバーを使用している場合は、[Sophos Linux Security スタートアップガイド](#)を参照してください。

- 各 Linux コンピュータのローカル環境で、Sophos Anti-Virus CLI を使用して**オンデマンド検索**を設定する。

## Enterprise Console または Sophos Central の管理下でない、ネットワーク上のコンピュータ

Linux コンピュータがネットワーク上にあり、Enterprise Console または Sophos Central の管理下**でない**場合は、次のように Sophos Anti-Virus を設定します。

- コンピュータのアップデート元である環境設定ファイルを編集して、**オンアクセス検索、スケジュール検索、警告、ログ、アップデート**を一元的に設定する。[補足:追加ファイルベースの環境設定について](#) (p. 40) を参照してください。
- 各コンピュータのローカル環境で、Sophos Anti-Virus CLI を使用して**オンデマンド検索**を設定する。

**注:** 追加ファイルベースの環境設定は、テクニカルサポートから指示があった場合や、ソフォスの管理コンソールを使用できない場合のみに使用してください。管理コンソールベースの環境設定と追加ファイルベースの環境設定を併用することはできません。

## Enterprise Console または Sophos Central の管理下でない、スタンドアロン コンピュータ

Enterprise Console や Sophos Central で**管理していない** Linux コンピュータをスタンドアロンで (ソフォスから直接アップデートしている状態) 利用している場合は、すべての Sophos Anti-Virus の機能を CLI から設定します。

## 3 オンアクセス検索

オンアクセス検索はウイルス感染を未然に防ぐもっとも一般的な方法です。ファイルを開く、コピー、あるいは保存するときに Sophos Anti-Virus で検索が実行され、安全な場合のみファイルへのアクセスが許可されます。

### 3.1 オンアクセス検索が有効になっていることを確認する

- オンアクセス検索の状態を確認するには、次のコマンドを実行します。  
`/opt/sophos-av/bin/savdstatus`

### 3.2 コンピュータの起動時にオンアクセス検索が自動で開始することを確認する

この手順を実行するには、対象のコンピュータに root としてログインする必要があります。

1. システム起動時に `savd` が自動的に起動されるか確認するには次のように入力します。  
`chkconfig --list`

**注:** 使用している Linux ディストリビューションでこのコマンドを使用できない場合は、適切なユーティリティを使用して、システム起動時に起動するよう設定されているサービスを確認してください。

表示されたリストに、`sav-protect` に対して `2:on`、`3:on`、`4:on`、および `5:on` のエントリがある場合、オンアクセス検索はシステム起動時に自動的に起動します。

そうでない場合は、次のように入力してください。

```
/opt/sophos-av/bin/savdctl enableOnBoot savd
```

2. `savd` とともにオンアクセス検索が自動的に起動されるかを確認するには次のように入力します。

```
/opt/sophos-av/bin/savconfig query EnableOnStart
```

コマンドで `true` が返されると、`savd` とともにオンアクセス検索がシステム起動時に自動的に起動されます。

そうでない場合は、次のように入力してください。

```
/opt/sophos-av/bin/savconfig set EnableOnStart true
```

### 3.3 オンアクセス検索を開始する

オンアクセス検索を開始するには、次のいずれかの手順を実行してください。

- 次のように入力します。  
`/opt/sophos-av/bin/savdctl enable`

- 適切なツールを使用して、インストールされたサービス sav-protect を起動します。たとえば、次のように入力します。  
`/etc/init.d/sav-protect start`  
または  
`service sav-protect start`

## 3.4 オンアクセス検索を停止する

**重要:** オンアクセス検索を停止すると、ファイルにアクセスした際、Sophos Anti-Virus によるウイルス検索が実行されなくなります。このため、使用しているコンピュータおよびそれに接続する他のコンピュータが感染する可能性が高くなります。

- オンアクセス検索を停止するには次のように入力します。  
`/opt/sophos-av/bin/savdctl disable`

## 4 オンデマンド検索

**オンデマンド検索**は、ユーザーが手動で開始する検索です。ファイルを個別に検索するのはもちろんのこと、ユーザーが読み取り権限を持つすべてのローカルファイルを検索することもできます。オンデマンド検索は手動で実行することもできれば、スケジュールを設定して指定した日時にも実行することもできます。

オンデマンド検索をスケジュール設定するには、`crontab`コマンドを使用します。詳細は、[ソフォスのサポートデータベースの文章 12176](#)を参照してください。

### 4.1 オンデマンド検索を実行する

オンデマンド検索を実行するコマンドは、`savscan` です。

#### 4.1.1 コンピュータを検索する

- コンピュータの検索を実行するには次のように入力します。  
`savscan /`

#### 4.1.2 特定のディレクトリまたはファイルを検索する

- 特定のディレクトリやファイルを検索するには、検索の対象となるパスを指定します。たとえば、次のように入力します。  
`savscan /usr/mydirectory/myfile`  
ディレクトリやファイルは一度に複数指定できます。

#### 4.1.3 ファイルシステムを検索する

- 特定のファイルシステムをウイルス検索するには、ファイルシステム名を指定します。たとえば、次のように入力します。  
`savscan /home`  
ファイルシステム名は一度に複数指定できます。

#### 4.1.4 ブートセクタを検索する

**注:** この手順は、Linux および FreeBSD のみで実行できます。

ブートセクタを検索するには、スーパーユーザーとしてログインしてください。これによって、ディスクデバイスにアクセスするための十分な権限が与えられます。

論理ドライブまたは物理ドライブのブートセクタを検索できます。

- 特定の論理ドライブのブートセクタを検索するには、次のように入力します。  
`savscan -bs=ドライブ名, ドライブ名, ...`

ここで **ドライブ名** は、 /dev/fd0、 /dev/hda1 などのドライブ名です。

- すべての論理ドライブのブートセクタを検索するには、次のように入力します。  
**savscan -bs**
- コンピュータ上のすべての固定物理ドライブのマスターブートレコードを検索するには、次のように入力します。  
**savscan -mbr**

## 4.2 オンデマンド検索を設定する

このセクションで、コマンドに **パス名** と表示されている場合、検索を実行するパスを指します。

オンデマンド検索で使用できるオプションの一覧を表示するには次のように入力します。

```
man savscan
```

### 4.2.1 すべての種類のファイルを検索する

Sophos Anti-Virus では、デフォルトで実行ファイルのみ検索されます。デフォルトで検索されるファイルの一覧を表示するには、 **savscan -vv** と入力します。

- デフォルトで検索されるファイルだけでなく、すべての種類のファイルをウイルス検索するには、 **-all** オプションを付けます。次のように入力します。

```
savscan パス名 -all
```

**注:** これによって、検索により時間がかかったり、サーバーのパフォーマンスが低下したり、ウイルスの誤警告の原因になったりすることがあります。

### 4.2.2 特定の種類のファイルを検索する

Sophos Anti-Virus では、デフォルトで実行ファイルのみ検索されます。デフォルトで検索されるファイルの一覧を表示するには、 **savscan -vv** と入力します。

- 特定の種類のファイルを検索するには、 **-ext** オプションで、適切な拡張子を指定します。たとえば、 **.txt** という拡張子の付いたファイルを検索するには次のように入力します。

```
savscan パス名 -ext=txt
```

- 特定の種類のファイルを検索から除外するには、 **-next** オプションで、適切な拡張子を指定します。

**注:** ファイルの種類を複数指定するには、拡張子をカンマで区切って指定してください。

### 4.2.3 すべての種類のアーカイブファイル内を検索する

Sophos Anti-Virus では、すべての種類のアーカイブファイル内をウイルス検索するように設定できます。アーカイブファイルの種類の一覧を表示するには、 **savscan -vv** と入力します。

**注:** 脅威検出エンジンは、圧縮されていない状態で 8GB までの圧縮ファイルのみを検索します。これはエンジンが対応している POSIX ustar アーカイブフォーマットで 8GB 以上のファイルを扱えないためです。

- 全種類のアーカイブファイルをウイルス検索するには、**-archive** オプションを使用します。次のように入力します。

```
savscan パス名 -archive
```

ZIP ファイルに含まれる TAR 形式のアーカイブなど、入れ子になっているアーカイブファイルは再帰的に検索されます。

構造が複雑なアーカイブファイルが多数ある場合、検索の実行速度が遅くなることがあります。無人のスケジュール検索を設定する際は注意してください。

#### 4.2.4 特定の種類のアーカイブファイル内を検索する

Sophos Anti-Virus では、ウイルス検索を実行するアーカイブファイルの種類を設定できません。アーカイブファイルの種類の一覧を表示するには、**savscan -vv** と入力します。

**注:** 脅威検出エンジンは、圧縮されていない状態で 8GB までの圧縮ファイルのみを検索します。これはエンジンが対応している POSIX ustar アーカイブフォーマットで 8GB 以上のファイルを扱えないためです。

- 特定の種類のアーカイブファイル内を検索するには、一覧に表示されるオプションを使用します。たとえば、TAR および ZIP アーカイブファイル内を検索するには次のように入力します。

```
savscan パス名 -tar -zip
```

ZIP ファイルに含まれる TAR 形式のアーカイブなど、入れ子になっているアーカイブファイルは再帰的に検索されます。

構造が複雑なアーカイブファイルが多数ある場合、検索の実行速度が遅くなることがあります。無人のスケジュール検索を設定する際は注意してください。

#### 4.2.5 リモートコンピュータを検索する

Sophos Anti-Virus では、デフォルトでリモートコンピュータ上のアイテムはウイルス検索されません (つまり、リモートのマウントポイントは検索されません)。

- リモートコンピュータを検索するには、**--no-stay-on-machine** オプションを使用します。次のように入力します。

```
savscan パス名 --no-stay-on-machine
```

#### 4.2.6 シンボリックリンクの検索を無効にする

Sophos Anti-Virus では、デフォルトでシンボリックリンクの参照先がウイルス検索されません。

- シンボリックリンクが参照しているアイテムの検索を無効にするには、**--no-follow-symlinks** オプションを使用します。次のように入力します。

```
savscan パス名 --no-follow-symlinks
```

アイテムの検索を一度に限定する場合は、**--backtrack-protection** オプションを使用してください。

#### 4.2.7 ブートファイルシステムのみを検索する

Sophos Anti-Virus では、ブートファイルシステム以外の項目をウイルス検索しないように設定できます (つまり、マウントポイントはトラバースしません)。

- ブートファイルシステムだけ検索するには、**--stay-on-filesystem** オプションを使用します。次のように入力します。

```
savscan パス名 --stay-on-filesystem
```

#### 4.2.8 検索の対象から除外するアイテムを設定する

**-exclude** というオプションを使って、Sophos Anti-Virus の検索対象から特定の項目 (ファイル、ディレクトリ、ファイルシステム) を除外するように設定できます。Sophos Anti-Virus は、コマンドを実行する際にオプションの後に入力された項目すべてを除外します。たとえば、fred と harry というアイテムを検索し、tom と peter というアイテムを検索しないようにするには、次のように入力します。

```
savscan fred harry -exclude tom peter
```

特定のディレクトリの配下にあるファイルやディレクトリを検索の対象から除外することもできます。たとえば、games というディレクトリ (そのすべてのサブディレクトリおよびファイルを含む) を除く「Fred」のホームディレクトリすべてを検索するには次のように入力します。

```
savscan /home/fred -exclude /home/fred/games
```

また、**-include** オプションを使って特定のアイテムを検索の対象に含めることもできます。たとえば、fred、harry、および bill を検索し、tom および peter を検索しないようにするには次のように入力します。

```
savscan fred harry -exclude tom peter -include bill
```

#### 4.2.9 UNIX で実行ファイルと定義されているファイルを検索する

Sophos Anti-Virus では、UNIX で実行ファイルとして定義されているファイルはデフォルトで検索されません。

- UNIX の実行ファイルを検索するには、**--examine-x-bit** オプションを使用します。次のように入力します。

```
savscan パス名 --examine-x-bit
```

この際、Sophos Anti-Virus で定義されている実行ファイル拡張子が付いているファイルも検索されます。このファイル拡張子の一覧を表示するには、**savscan -vv** と入力します。

## 5 ウイルスが検出された場合の動作

Sophos Anti-Virus でウイルスが検出されると、オンアクセス検索、オンデマンド検索にかかわらず、デフォルトで次の処理が行われます。

- syslog および Sophos Anti-Virus ログにイベントを記録する ([Sophos Anti-Virus ログの表示](#) (p. 19) を参照)。
- Enterprise Console で一元管理されている場合、Enterprise Console に警告を送信する。
- root@localhost にメール警告が送信される。

デフォルトで Sophos Anti-Virus は警告も表示します。ウイルスがオンアクセス検索で検出されたか、オンデマンドで検出されたかによって次のような警告が表示されます。

### オンアクセス検索

オンアクセス検索でウイルスが検出されると、Sophos Anti-Virus によってファイルへのアクセスが遮断され、デフォルトで次のようなポップアップがデスクトップに表示されます。



デスクトップのポップアップ警告が表示されない場合は、かわりにコマンドラインの警告が表示されます。

ウイルスのクリーンアップの詳細は、[ウイルスのクリーンアップ](#) (p. 16) を参照してください。

### オンデマンド検索

Sophos Anti-Virus のオンデマンド検索でウイルスが検出されると、デフォルトでコマンドラインの警告が表示されます。検出されたウイルスは、>>> と ウィルスまたはウィルスフラグメントで始まる行で報告されます。

```
SAVScan ウィルス検出ユーティリティ  
バージョン 4.69.0 [Linux/Intel]  
ウィルスデータバージョン 4.69
```

```
2871136種類のウイルス、トロイの木馬、ワームを検出します。
Copyright (c) 1989-2012 Sophos Limited. All rights reserved.
システム時刻 13:43:32、システム日付 2012年 9月 22日
IDE ディレクトリ: /opt/sophos-av/lib/sav
以下の IDE ファイルを使用しています: nyrate-d.ide
.....
以下の IDE ファイルを使用しています: injec-lz.ide
```

#### クイック検索

```
>>> ウイルス `EICAR-AV-Test` がファイル /usr/mydirectory/eicar.src で
検出されました。
```

2秒間で 33個のファイルを検索しました。

1個のウイルスが発見されました。

1個のファイル (33個中) が感染しています。

解析用として感染ファイルのサンプルをソフォスまでお送りください。

お問い合わせ先: [www.sophos.com/ja-jp](http://www.sophos.com/ja-jp), Email [support@sophos.co.jp](mailto:support@sophos.co.jp)

検索が終了しました。

ウイルスのクリーンアップの詳細は、[ウイルスのクリーンアップ](#) (p. 16) を参照してください。

## 6 ウイルスのクリーンアップ

### 6.1 クリーンアップ情報を入手する

ウイルスが検出された場合は、ソフォスの Web サイトからクリーンアップに関する情報やアドバイスを参照できます。

クリーンアップ情報を入手する方法は次のとおりです。

1. セキュリティ解析ページ  
(<http://www.sophos.com/ja-jp/threat-center/threat-analyses/viruses-and-spyware.aspx>) を開きます。
2. Sophos Anti-Virus で検出されたウイルスの名前を入力して解析情報を検索します。

### 6.2 感染ファイルを隔離する

オンデマンド検索で感染ファイルを隔離エリアに移動するように設定し、アクセスを防止することができます。ファイルは所有者とパーミッションを変更することで隔離されます。

**注:** ファイルの隔離と駆除 ([感染ファイルをクリーンアップする](#) (p. 17) を参照) の両方を有効に設定すると、駆除に失敗した場合のみに、Sophos Anti-Virus で感染アイテムの隔離が実行されます。

このセクションで、コマンドに**パス名**と表示されている場合、検索を実行するパスを指します。

#### 6.2.1 隔離を指定する

- 隔離を指定するには、**--quarantine** オプションを使用します。次のように入力します。  
**savscan パス名 --quarantine**

#### 6.2.2 感染ファイルに適用するファイルの所有者やパーミッションを設定する

デフォルトで Sophos Anti-Virus は次のように動作します。

- 所有者のユーザーを Sophos Anti-Virus を起動しているユーザーに変更する。
- 所有者のグループを Sophos Anti-Virus を起動しているユーザーが所属するグループに変更する。
- パーミッションを **-r-----** (0400) に変更する。

Sophos Anti-Virus で感染ファイルに適用される所有者のユーザーやグループ、およびファイルのパーミッションの設定は、必要に応じて変更することができます。変更するには次のパラメータを使用します。

```
uid=nnn
user=ユーザー名
gid=nnn
group=グループ名
mode=ppp
```

所有者のユーザー、またはグループに対して複数のパラメータを指定することはできません。たとえば、**uid** と **user** パラメータを同時に使用することはできません。

値を指定していないパラメータには、先程のデフォルト値が適用されます。

たとえば、次のように入力します。

```
savscan fred --quarantine:user=virus,group=virus,mode=0400
```

この場合、感染ファイルの所有者であるユーザーは「virus」に、所有者であるグループは「virus」に、ファイルのパーミッションは `-r-----` に変更されます。ファイル所有者のユーザーは「virus」、グループは「virus」に設定されますが、ユーザー「virus」だけがファイルにアクセス(読み込みのみ)できるようになります。これ以外のユーザー (rootを除く) はファイルに対していかなる操作も行えません。

所有者とパーミッションを設定するには、スーパーユーザーとしてログインしていなければならない場合があります。

## 6.3 感染ファイルをクリーンアップする

オンデマンド検索を実行したときに、感染ファイルをクリーンアップ (駆除または削除) することができます。Sophos Anti-Virus で感染アイテムに対して実行されるアクションは、すべて検索サマリーおよび Sophos Anti-Virus ログに記録されます。デフォルトでクリーンアップは無効になっています。

このセクションで、コマンドに**パス名**と表示されている場合、検索を実行するパスを指します。

### 6.3.1 特定の感染ファイルを駆除する

- 特定の感染ファイルを駆除するには、**-di** オプションを付けて、次のように入力します。

```
savscan パス名 -di
```

Sophos Anti-Virus で駆除が実行される前に確認メッセージが表示されます。

**注:** 感染したドキュメントを駆除しても、ウイルスによるドキュメントの変更箇所は修復されません。(ウイルスの副作用に関する詳細をソフォスWebサイトで参照するには、[クリーンアップ情報を入手する](#) (p. 16) を参照してください。)

### 6.3.2 コンピュータ上のすべての感染ファイルを駆除する

- コンピュータ上の感染ファイルすべてを駆除するには、次のように入力します。

```
savscan / -di
```

Sophos Anti-Virus で駆除が実行される前に確認メッセージが表示されます。

**注:** 感染したドキュメントを駆除しても、ウイルスによるドキュメントの変更箇所は修復されません。(ウイルスの副作用に関する詳細をソフォスWebサイトで参照するには、[クリーンアップ情報を入手する](#) (p. 16) を参照してください。)

### 6.3.3 特定の感染ファイルを削除する

- 特定の感染ファイルを削除するには、**-remove** オプションを付けて、次のように入力します。

```
savscan パス名 -remove
```

Sophos Anti-Virus で削除が実行される前に確認メッセージが表示されます。

### 6.3.4 コンピュータ上のすべての感染ファイルを削除する

- コンピュータ上の感染ファイルすべてを削除するには、次のように入力します。

```
savscan / -remove
```

Sophos Anti-Virus で削除が実行される前に確認メッセージが表示されます。

### 6.3.5 感染ブートセクタを駆除する

**注:** この手順は、Linux および FreeBSD のみで実行できます。

- 感染ブートセクタを駆除するには、**-di** 駆除オプションおよび**-bs** ブートセクタオプションを指定してください。たとえば、次のように入力します。

```
savscan -bs=/dev/fd0 -di
```

ここで `/dev/fd0` は、感染ブートセクタのあるドライブ名です。

Sophos Anti-Virus で駆除が実行される前に確認メッセージが表示されます。

## 6.4 ウイルスの副作用から復旧する

ウイルスの副作用からの復旧方法は、その感染経路によって異なります。対処が必要となる副作用を残さないウイルスもありますが、一方では、コンピュータの復旧にハードディスクの復元を要するなど、深刻な副作用を伴うウイルスも存在します。

また、データに少しずつ変化を加えていくウイルスもあり、この種のデータ破壊は発見が非常に困難な場合もあります。ウイルスの駆除後は、必ずソフォスWebサイトのウイルス解析を参照し、注意深くドキュメントを確認してください。

適切なバックアップは必須です。感染前のバックアップがない場合は、将来の感染に備え、今後作成するようにしてください。

ウイルスによって破壊されたディスクからデータを復旧できる場合もあります。ソフォスでは、一部のウイルスの破壊活動から復旧するためのユーティリティを提供しています。ソフォス テクニカルサポートにお問い合わせください。

## 7 Sophos Anti-Virus ログの表示

Sophos Anti-Virus では、検索アクティビティの詳細が Sophos Anti-Virus ログと syslog に記録されます。このほかにもウイルスやエラーのイベントが Sophos Anti-Virus ログに記録されます。

- Sophos Anti-Virus ログを表示するには、`savlog` コマンドを実行します。このコマンドを使用して、様々なオプションを付けて特定のメッセージの出力を制限したり、表示内容を調整したりすることができます。

たとえば、日時の形式を UTC/ISO 8601 に指定し、過去 24 時間に Sophos Anti-Virus ログに記録されたすべてのメッセージを表示するには次のように入力します。

```
/opt/sophos-av/bin/savlog --today --utc
```

- `savlog` コマンドのすべてのオプションを表示するには次のように入力します。

```
man savlog
```

## 8 Sophos Anti-Virus の即時アップデート

Sophos Anti-Virus の自動アップデートが有効に設定されている場合は、継続して自動的にアップデートが実施されます。また、次回の自動アップデートを待たずに、Sophos Anti-Virus を今すぐアップデートすることもできます。

- Sophos Anti-Virus を今すぐアップデートするには、アップデートするコンピュータで次のように入力します。  
`/opt/sophos-av/bin/savupdate`

**注:** また、各コンピュータを今すぐ一括アップデートするには、Sophos Enterprise Console を使用します。

## 9 カーネル対応について

**注:** このセクションは、オンアクセス検索の割り込み方法として Talpa を使用している場合のみ参照してください。詳細は[オンアクセス検索のファイル割り込み方法を変更する](#) (p.36) を参照してください。

### 9.1 最新のカーネルへの対応について

Sophos Anti-Virus が対応している Linux ベンダーが Linux カーネルのアップデート版をリリースした場合、ソフォスではそれに対応するため、Sophos カーネル インターフェース モジュール (Talpa) のアップデート版をリリースしています。対応するアップデート版 Talpa を適用する前に Linux カーネルのアップデート版を適用すると、Sophos Anti-Virus では、Talpa のコンパイルがローカルで実行されます。これに失敗すると、Sophos Anti-Virus は、割り込み方法として代わりに Fanotify を使用しようとしています。Fanotify も使用できない場合、オンアクセス検索は停止され、エラーが報告されます。

この問題を避けるには、Linux カーネルのアップデート版を適用する前に、該当する Talpa のアップデート版がリリースされていることを確認するようにしてください。対応している Linux ディストリビューションおよびアップデート版の一覧は、ソフォスのサポートデータベースの文章 14377 を参照してください

(<http://www.sophos.com/ja-jp/support/knowledgebase/14377.aspx>)。該当する Talpa のアップデート版が表示されている場合は、ダウンロード可能なことを意味します。Sophos Anti-Virus の自動アップデートを有効に設定した場合、アップデート版は自動的にダウンロードされます。または、次回の自動アップデートを待たずに、Sophos Anti-Virus を今すぐアップデートするには、次のように入力してください。

```
/opt/sophos-av/bin/savupdate
```

終了後、Linux カーネルのアップデート版を適用できます。

### 9.2 カスタマイズされたカーネルへの対応について

Linux カーネルをカスタマイズした場合、このマニュアルで説明するアップデートの設定方法は適用できません。詳細は、ソフォス サポートデータベースの文章 13503 を参照してください (<http://www.sophos.com/ja-jp/support/knowledgebase/13503.aspx>)。

## 10 スケジュール検索の設定

Sophos Anti-Virus では、1つ以上のスケジュール検索の設定を保存することができます。

**注:** Enterprise Console を使って追加したスケジュール検索には「SEC:」ではじまる検索名が付けられます。これらの検索は Enterprise Console だけから削除したり更新できます。

### 10.1 ファイルから読み込んでスケジュール検索を追加する

1. 新しいスケジュール検索の設定にあたり、あらかじめ検索が定義されているテンプレートを利用するには `/opt/sophos-av/doc/namedscan.example.en` を開きます。  
最初から検索を設定する場合は、新しいテキストファイルを開きます。
2. テンプレートにあるパラメータの一覧を参照して、検索対象、検索日時、およびその他のオプションを設定します。  
スケジュール検索を実行するには、最低 1つの日付と時刻を指定する必要があります。
3. テンプレートを上書きしないように、任意の別の場所にファイルを保存します。
4. スケジュール検索を Sophos Anti-Virus に追加するには、**add** オペレーションと **NamedScans** パラメータを付けて `savconfig` コマンドを実行します。検索名と検索の設定ファイルが保存されている場所を指定します。

たとえば、`/home/fred/DailyScan` に保存されている `Daily` という名前の検索を保存するには次のように入力します。

```
/opt/sophos-av/bin/savconfig add NamedScans Daily  
/home/fred/DailyScan
```

### 10.2 標準入力からスケジュール検索を追加する

1. スケジュール検索を Sophos Anti-Virus に追加するには、**add** オペレーションと **NamedScans** パラメータを付けて `savconfig` コマンドを実行します。この際に、検索名を指定し、標準入力から設定が読み込まれることを表すためにハイフンを入力します。  
たとえば、`Daily` という名前でスケジュール検索を追加するには次のように入力します。  
`/opt/sophos-av/bin/savconfig add NamedScans Daily -`  
「ENTER」キーを押した後で、スケジュール検索の設定内容を入力してください。
2. あらかじめ検索が定義されているテンプレートのパラメータの一覧を参照して、検索対象、検索日時やその他のオプションを設定します。テンプレートの保存場所は、`/opt/sophos-av/doc/namedscan.example.ja` です。各パラメータと値を入力して、「ENTER」キーを押します。設定が必要な数だけ繰り返します。  
スケジュール検索を実行するには、最低 1つの日付と時刻を指定する必要があります。
3. CTRL+D を押して設定を完了します。

## 10.3 特定のスケジュール検索をファイルに出力する

- Sophos Anti-Virus で設定されているスケジュール検索をファイルに出力するには、`query` オプションと **NamedScans** パラメータを付けて `savconfig` を実行します。この際に、検索名と検索を出力するパスを指定します。

たとえば、`/home/fred/DailyScan` というファイルに `Daily` という名前の検索を出力するには次のように入力します。

```
/opt/sophos-av/bin/savconfig query NamedScans Daily >
/home/fred/DailyScan
```

## 10.4 すべてのスケジュール検索の名前をファイルに出力する

- Sophos Anti-Virus で設定されているすべてのスケジュール検索 (Enterprise Console で設定された検索も含む) の名前を 1つのファイルに出力するには、**query** オプションと **NamedScans** パラメータを付けて `savconfig` を実行します。この際に、検索名を出力する場所を指定します。

たとえば、`/home/fred/AllScans` というファイルにすべてのスケジュール検索の検索名を出力するには次のように入力します。

```
/opt/sophos-av/bin/savconfig query NamedScans > /home/fred/AllScans
```

**注:** Enterprise Console で管理されるコンピュータの場合、常に `SEC:FullSystemScan` という名称の検索が定義されています。

## 10.5 特定のスケジュール検索を標準出力する

- Sophos Anti-Virus で設定されているスケジュール検索を標準出力に個別に出力するには、**query** オプションと **NamedScans** パラメータを付けて `savconfig` を実行します。この際に検索名を指定します。

たとえば、標準出力に `Daily` という名前のスケジュール検索を出力するには次のように入力します。

```
/opt/sophos-av/bin/savconfig query NamedScans Daily
```

## 10.6 すべてのスケジュール検索の名前を標準出力する

- Sophos Anti-Virus で設定されているすべてのスケジュール検索 (Enterprise Console で設定された検索も含む) の名前を標準出力に出力するには、**query** オプションと **NamedScans** パラメータを付けて `savconfig` を実行します。

たとえば、標準出力にすべてのスケジュール検索の検索名を出力するには次のように入力します。

```
/opt/sophos-av/bin/savconfig query NamedScans
```

**注:** Enterprise Console で管理されるコンピュータの場合、常に SEC:FullSystemScan という名称の検索が定義されています。

## 10.7 ファイルから読み込んでスケジュール検索を更新する

**注:** Enterprise Console を使用して追加したスケジュール検索を更新することはできません。

1. 更新するスケジュール検索の設定ファイルを開きます。  
検索がファイルとして出力されていない場合は、[特定のスケジュール検索をファイルに出力する](#) (p. 23) の説明に従ってファイルに出力してください。
2. 検索が定義されているテンプレートのパラメータの一覧を参照し、必要に応じて設定内容を修正します。テンプレートの保存場所は、`/opt/sophos-av/doc/namedscan.example.ja` です。なお、既存の設定内容を維持するために、更新する項目だけでなく、すべての項目を指定する必要があります。
3. ファイルを保存します。
4. Sophos Anti-Virus で設定されているスケジュール検索を更新するには、**update** オペレーションと **NamedScans** パラメータを付けて `savconfig` コマンドを実行します。検索名と検索の設定ファイルが保存されている場所を指定します。

たとえば、`/home/fred/DailyScan` に保存されている `Daily` という名前の検索を更新するには次のように入力します。

```
/opt/sophos-av/bin/savconfig update NamedScans Daily  
/home/fred/DailyScan
```

## 10.8 標準入力からスケジュール検索を更新する

**注:** Enterprise Console を使用して追加したスケジュール検索を更新することはできません。

1. Sophos Anti-Virus で設定されているスケジュール検索を更新するには、**update** オペレーションと **NamedScans** パラメータを付けて `savconfig` コマンドを実行します。この際に、検索名を指定し、標準入力から設定が読み込まれることを表すためにハイフンを入力します。

たとえば、`Daily` というスケジュール検索を更新するには次のように入力します。

```
/opt/sophos-av/bin/savconfig update NamedScans Daily -
```

「ENTER」キーを押した後で、スケジュール検索の設定内容を入力してください。

2. あらかじめ検索が定義されているテンプレートのパラメータの一覧を参照して、検索対象、検索日時やその他のオプションを設定します。テンプレートの保存場所は、`/opt/sophos-av/doc/namedscan.example.ja` です。各パラメータと値を入力して、「ENTER」キーを押します。設定が必要な数だけ繰り返します。なお、既存の設定内容を維持するために、更新する項目だけでなく、すべての項目を指定する必要があります。  
スケジュール検索を実行するには、最低 1つの日付と時刻を指定する必要があります。
3. CTRL+D を押して設定を完了します。

## 10.9 スケジュール検索のログを表示する

- スケジュール検索のログを表示するには、コマンド `savlog` とオプション **namedscan** を使用します。この際に検索名を指定します。

たとえば、「Daily」という名前の検索のログを表示するには次のように入力します。

```
/opt/sophos-av/bin/savlog --namedscan=Daily
```

## 10.10 スケジュール検索を削除する

**注:** Enterprise Console を使用して追加したスケジュール検索を削除することはできません。

- Sophos Anti-Virus で設定されているスケジュール検索を個別に削除するには、**remove** オプションと **NamedScans** パラメータを付けて `savconfig` を実行します。この際に検索名を指定します。

たとえば、Daily というスケジュール検索を削除するには次のように入力します。

```
/opt/sophos-av/bin/savconfig remove NamedScans Daily
```

## 10.11 すべてのスケジュール検索を削除する

**注:** Enterprise Console を使用して追加したスケジュール検索を削除することはできません。

- Sophos Anti-Virus で設定されているすべてのスケジュール検索を削除するには次のように入力します。

```
/opt/sophos-av/bin/savconfig delete NamedScans
```

# 11 警告の設定

**注:** ネットワーク上のコンピュータを個別に構成する場合は、そのコンピュータに Enterprise Console や追加ファイルの新しい環境設定がダウンロードされると、構成した環境設定が上書きされることがありますので注意してください。

ウイルス検出時や、検索エラーやその他のエラーが発生した時に警告が送信されるよう Sophos Anti-Virus を設定できます。警告の送信方法は次のとおりです。

- デスクトップ・ポップアップ (オンアクセス検索のみ)
- コマンドライン (オンアクセス検索のみ)
- メール (オンアクセス検索、オンデマンド検索)

デスクトップ・ポップアップ警告とコマンドライン警告は、警告を発したコンピュータで指定した言語によって表示されます。メール警告は英語または日本語で送信できます。

## 11.1 デスクトップ・ポップアップ警告を設定する

### 11.1.1 デスクトップ・ポップアップ警告を無効にする

デフォルトで、デスクトップ・ポップアップ警告は有効になっています。

- デスクトップ・ポップアップ警告を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set UIpopupNotification disabled`
- デスクトップ・ポップアップ警告とコマンドラインの警告の両方を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set UINotifier disabled`

### 11.1.2 カスタムメッセージを指定する

すべてのコマンドラインの警告とデスクトップ・ポップアップに追加されるカスタムメッセージを指定できます。

**注:** メインの警告メッセージは異なる言語で表示 (システム設定によって変わります) できますが、カスタムテキストは指定した元の言語のまま表示されます。

- カスタムメッセージを指定するには、**UIContactMessage** パラメータを使用します。たとえば、次のように入力します。  
`/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

## 11.2 コマンドライン警告を設定する

### 11.2.1 コマンドラインの警告を無効にする

デフォルトで、コマンドラインの警告は有効になっています。

- コマンドラインの警告を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set UIttyNotification disabled`
- デスクトップ・ポップアップ警告とコマンドラインの警告の両方を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set UINotifier disabled`

### 11.2.2 カスタムメッセージを指定する

すべてのコマンドラインの警告とデスクトップ・ポップアップに追加されるカスタムメッセージを指定できます。

**注:** メインの警告メッセージは異なる言語で表示 (システム設定によって変わります) できますが、カスタムテキストは指定した元の言語のまま表示されます。

- カスタムメッセージを指定するには、**UIContactMessage** パラメータを使用します。たとえば、次のように入力します。  
`/opt/sophos-av/bin/savconfig set UIContactMessage 'Contact IT'`

## 11.3 メール警告を設定する

### 11.3.1 メール警告を無効にする

デフォルトで、メール警告は有効になっています。

- メール警告を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set EmailNotifier disabled`

### 11.3.2 SMTP サーバーのホスト名や IP アドレスを指定する

デフォルトで、ホスト名および SMTP サーバーのポートは localhost:25 に設定されています。

- SMTP サーバーのホスト名や IP アドレスを指定するには、**EmailServer** を使用します。たとえば、次のように入力します。  
`/opt/sophos-av/bin/savconfig set EmailServer 171.17.31.184`

### 11.3.3 言語を指定する

警告メッセージ本文で使用される言語は、デフォルトで英語です。

- 警告メッセージ本文で使用される言語を指定するには、**EmailLanguage** パラメータを使用します。現在、使用できる値は、「**English**」または「**Japanese**」のみです。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig set EmailLanguage Japanese
```

**注:** ここで指定する言語設定は、警告メッセージ本文のみに適用されます。各メール警告で、警告メッセージに加えて表示されるカスタムメッセージには適用されません。

### 11.3.4 メール受信者を指定する

デフォルトでメール警告は root@localhost に送信されます。

- メール警告の受信者のリストにアドレスを追加するには、**add** オペレーションとともに **Email** パラメータを使用します。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig add Email admin@localhost
```

**注:** 受信者は一度に複数指定できます。受信者名を空白で区切って入力してください。

- リストからアドレスを削除するには、**remove** オペレーションとともに **Email** パラメータを使用します。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig remove Email admin@localhost
```

**重要:** このコマンドでは **root@localhost** は削除できません。これを実行するには、以下のコマンドで一覧をすべて上書きしてください。

```
/opt/sophos-av/bin/savconfig set Email <メールアドレス>
```

### 11.3.5 送信元メールアドレス (Sender) を設定する

デフォルトでメール警告は root@localhost から送信されます。

- 送信元メールアドレス (Sender) を指定するには、**EmailSender** というパラメータを使用します。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig set EmailSender admin@localhost
```

### 11.3.6 返信先メールアドレス (ReplyTo) を設定する

- 返信先メールアドレス (ReplyTo) を指定するには、**EmailReplyTo** というパラメータを使用します。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig set EmailReplyTo admin@localhost
```

### 11.3.7 オンアクセス検索でウイルスが検出されたときの処理方法を指定する

オンアクセス検索でウイルスが検出されると、Sophos Anti-Virus はデフォルトでメール警告を送信します。各コマンドラインの警告には、警告メッセージ本文に加えて、英語のカス

タムメッセージが含まれます。カスタムメッセージの内容を変更することはできますが、日本語で表示することはできません。

- オンアクセス検索のウイルス検出時に行うメール警告の送信を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set SendThreatEmail disabled`
- カスタムメッセージを指定するには、**ThreatMessage** パラメータを使用します。たとえば、次のように入力します。  
`/opt/sophos-av/bin/savconfig set ThreatMessage 'Contact IT'`

### 11.3.8 オンアクセス検索エラーが発生したときの処理方法を指定する

オンアクセス検索エラーが発生すると、デフォルトで Sophos Anti-Virus からメール警告が送信されます。各コマンドラインの警告には、警告メッセージ本文に加えて、英語のカスタムメッセージが含まれます。カスタムメッセージの内容を変更することはできますが、日本語で表示することはできません。

- オンアクセス検索の検索エラー発生時に行うメール警告の送信を無効にするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set SendErrorMessage disabled`
- カスタムメッセージを指定するには、**ScanErrorMessage** パラメータを使用します。たとえば、次のように入力します。  
`/opt/sophos-av/bin/savconfig set ScanErrorMessage 'Contact IT'`

### 11.3.9 オンデマンド検索のメール警告を無効にする

デフォルトで Sophos Anti-Virus では、ウイルスが検出された場合に限って、検索のサマリーがメール送信されます。

- ウイルス検出時にオンデマンド検索のサマリーがメール送信されないようにするには、次のように入力します。  
`/opt/sophos-av/bin/savconfig set EmailDemandSummaryIfThreat disabled`

### 11.3.10 ログにイベントが記録されたときの処理方法を指定する

Sophos Anti-Virus では、Sophos Anti-Virus ログにイベントが記録されると、デフォルトでメール警告が送信されます。各警告には、警告メッセージ本文に加えて、英語のカスタムメッセージが含まれます。カスタムメッセージの内容を変更することはできますが、日本語で表示することはできません。

- カスタムメッセージを指定するには、**LogMessage** パラメータを使用します。たとえば、次のように入力します。  
`/opt/sophos-av/bin/savconfig set LogMessage 'Contact IT'`

## 12 ログの設定

**注:** ネットワーク上のコンピュータを個別に構成する場合は、そのコンピュータに Enterprise Console や追加ファイルの新しい環境設定がダウンロードされると、構成した環境設定が上書きされることがありますので注意してください。

デフォルトで、検索の活動内容は Sophos Anti-Virus ログに出力されます (パス: `/opt/sophos-av/log/savd.log`)。ログのサイズが 1MB に達すると、同じディレクトリに自動的にバックアップされ、新しいログファイルが作成されます。

- デフォルトのログの最大サイズを表示するには、次のように入力してください。  
`/opt/sophos-av/bin/savconfig -s query LogMaxSizeMB`
- ログの最大サイズを指定するには、**LogMaxSizeMB** パラメータを使用してください。たとえば、ログの最大サイズを 50MB に指定するには次のように入力します。  
`/opt/sophos-av/bin/savconfig set LogMaxSizeMB 50`

## 13 アップデートの設定

**重要:** Sophos Enterprise Console を使って Sophos Anti-Virus を管理する場合は、Enterprise Console でアップデートの設定を行う必要があります。操作方法については、このセクションではなく Enterprise Console ヘルプを参照してください。

### 13.1 用語の解説

#### アップデートサーバー

**アップデートサーバー**は、Sophos Anti-Virus for Linux がインストールされたコンピュータで、他のコンピュータのアップデート元として使用されます。他のコンピュータは、ネットワークにおける Sophos Anti-Virus のデプロイ方法により、アップデートサーバーまたはアップデートクライアントとなります。

#### アップデートクライアント

**アップデートクライアント**は、Sophos Anti-Virus がインストールされたコンピュータですが、他のコンピュータのアップデート元としては使用されません。

#### プライマリアップデート元

**プライマリアップデート元**は、コンピュータがアップデート版を取得するために通常アクセスする場所です。アクセスにはアカウント情報が必要な場合があります。

#### セカンダリアップデート元

**セカンダリアップデート元**は、コンピュータがアップデート版を取得する際、プライマリアップデート元にアクセスできない場合に、アクセスする場所です。アクセスにはアカウント情報が必要な場合があります。

### 13.2 savsetup 設定コマンド

savsetup はアップデートを設定するためのコマンドです。このコマンドは、これ以降のセクションで説明する特定のタスクを実行するときだけ使用してください。

savconfig と比較して、アクセスできるパラメータに限りがありますが、使用はより簡単です。起動すると、パラメータの値を入力するよう表示されるので、値を選択するか、直接入力します。savsetup を起動するには次のように入力します。

```
/opt/sophos-av/bin/savsetup
```

## 13.3 コンピュータの自動アップデートの設定内容を確認する

1. 確認するコンピュータで次のコマンドを実行します。  
`/opt/sophos-av/bin/savsetup`  
 savsetup コマンドを入力後、画面に選択肢が表示されます。
2. 「**自動アップデートの環境設定**」を選択します。  
 savsetup コマンドを入力後、画面に選択肢が表示されます。
3. 「**アップデートの環境設定を表示する**」を選択して、現在の設定内容を表示します。

## 13.4 アップデートサーバーを設定する

アップデートサーバー (ネットワークに接続しているコンピュータのアップデート元) には、スタンドアロンの Sophos Anti-Virus for Linux がインストールされているコンピュータを使用します。

1. アップデートサーバーで次のように入力します。  
`/opt/sophos-av/bin/savsetup`  
 savsetup コマンドを入力後、画面に選択肢が表示されます。
2. 選択肢から1つ選択し、画面の指示にしたがって、アップデートサーバーを設定します。  
 アップデートの設定をする際、ソフォスからアップデートする場合、お持ちのライセンスに記載されているユーザー名とパスワードを入力します。アップデートサーバーからアップデートする場合、アップデートサーバーの設定内容により、HTTP アドレスまたは UNC パスのどちらかを指定できます。
3. 他の Sophos Anti-Virus クライアントのアップデート元に指定する方法は次のとおりです。
  - a) アップデートサーバーを設定し、アップデートクライアントで必要となる (状況によっては不要) 追加ファイルをダウンロードします。アップデートサーバーで次のように入力します。  
`/opt/sophos-av/bin/savconfig set PrimaryUpdateAllDistros true`
  - b) アップデートを強制実行し、アップデートサーバーに追加ファイルをダウンロードします。アップデートサーバーで次のように入力します。  
`/opt/sophos-av/bin/savupdate --force`
  - c) ローカル キャッシュ ディレクトリ (/opt/sophos-av/update/cache/) を、ファイルシステム上の別の場所にコピーします。  
 この操作は、スクリプトを使用して自動化できます。
  - d) この場所を HTTP、SMB、NFS または他の方法で、他のネットワークコンピュータに公開します。  
 この場所が CID (セントラル インストール ディレクトリ) となり、ここからクライアントはアップデート版をダウンロードします。

## 13.5 複数のアップデートクライアントのアップデートを設定する

ここでは追加ファイルベースの環境設定内のアップデート用パラメータを更新する手順について説明します。パラメータを更新すると、次のアップデート時にアップデートクライアントに環境設定がダウンロードされます。

このセクションでは追加ファイルベースの環境設定が作成済みであることを前提としています。作成が済んでいない場合は、[補足: 追加ファイルベースの環境設定について](#) (p. 40) を参照してください。

**注:** ここでは、複数のアップデートクライアントが**プライマリ**アップデートソースからアップデートする場合の設定方法を説明します。**セカンダリ**アップデートソースからのアップデートを設定する場合は、*Primary*を*Secondary*と置き換えて、同様の手順を実施します。たとえば、**PrimaryUpdateSourcePath**を**SecondaryUpdateSourcePath**に置き換えてください。

複数のアップデートクライアントのアップデートを設定する方法は、次のとおりです。

- 追加ファイルベースの環境設定が保存されているコンピュータで、**PrimaryUpdateSourcePath**パラメータを使用して、アップデート元アドレスを **sophos:** または CID (セントラル インストール ディレクトリ) のいずれかの場所に設定します。CID からアップデートする場合は、アップデートサーバーの設定内容により、HTTP アドレスまたはUNCパスのどちらかを指定できます。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定ファイルのパス -c set PrimaryUpdateSourcePath 'http://www.mywebcid.com/cid'
```

**sophos:** からアップデートする場合は、次のように入力します。

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定ファイルのパス -c set PrimaryUpdateSourcePath 'sophos:'
```
- アップデート元へのアクセスにユーザー認証が必要な場合は、**PrimaryUpdateUsername** および **PrimaryUpdatePassword** パラメータを使用して、ユーザー名とパスワードをそれぞれ指定してください。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定のパス -c set PrimaryUpdateUsername 'fred'
```

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定のパス -c set PrimaryUpdatePassword 'j23rjjfwj'
```

3. プロキシ経由でアップデート元にアクセスしている場合は、**PrimaryUpdateProxyAddress**、**PrimaryUpdateProxyUsername** および **PrimaryUpdateProxyPassword** パラメータを使用して、プロキシサーバーのアドレス、ユーザー名およびパスワードをそれぞれ指定してください。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定のパス -c set
PrimaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
```

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定のパス -c set
PrimaryUpdateProxyUsername 'penelope'
```

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定のパス -c set
PrimaryUpdateProxyPassword 'fj202jrjf'
```

4. オフライン環境設定ファイルのパラメータを設定し終わったら、addextra というコマンドを使用してライブ環境設定ファイルを更新します。構文は次のとおりです。

```
/opt/sophos-av/update/addextra オフライン環境設定ファイルのパスライブ環境
設定ファイルのパス --signing-key=署名鍵ファイルのパス
--signing-certificate=署名証明書ファイルのパス
```

たとえば次のように入力します。

```
/opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg
/var/www/extrafiles/ --signing-key=
/root/certificates/extrafiles-signing.key
--signing-certificate=/root/certificates/extrafiles-signing.crt
```

以上で各アップデートクライアントに対する環境設定が更新され、次のアップデート時に各コンピュータにダウンロードされます。

## 13.6 1台のアップデートクライアントのアップデートを設定する

1. 設定するコンピュータで次のように入力します。

```
/opt/sophos-av/bin/savsetup
```

savsetup コマンドを入力後、画面に選択肢が表示されます。

2. 選択肢から 1つ選択し、画面の指示にしたがって、アップデートクライアントを設定します。

アップデートの設定をする際、ソフォスからアップデートする場合、お持ちのライセンスに記載されているユーザー名とパスワードを入力します。CID からアップデートする場合、アップデートサーバーの設定内容により、HTTP アドレスまたは UNC パスのどちらかを指定できます。

## 14 Sophos Live Protection の設定

**注:** ネットワーク上のコンピュータを個別に構成する場合は、そのコンピュータに Enterprise Console や追加ファイルの新しい環境設定がダウンロードされると、構成した環境設定が上書きされることがありますので注意してください。

Sophos Live Protection は、不正な疑いのあるファイルが脅威であるかどうかを判断する、クラウド型の検出機能です。脅威を検知すると、Sophos Anti-Virus のクリーンアップ機能に設定されているアクションが直ちに実行されます。

Sophos Live Protection は、誤検知のリスクを抑えつつ、新種マルウェアの検出率を大幅に向上します。最新の情報が保存されるソフォスのマルウェアデータベースをリアルタイムに参照することで、新しい脅威にすばやく対応できます。新種マルウェアとして検出された場合、ソフォスから脅威定義ファイルのアップデート版を数秒内に受信できます。

エンドポイントコンピュータのウイルス検索機能で疑わしいファイルが検出された場合で、ローカルの脅威定義ファイル (IDE ファイル) を使っても、ファイルが感染していないか、あるいは悪質なものか詳細な判定ができないときは、チェックサムやその他の属性など、特定のファイルデータがソフォスに送信され、詳細な解析が行われます。

オンラインベースのチェックでは、疑わしいファイルがソフォスラボのデータベースと照合されます。ファイルが未感染または悪質であると判断された場合、結果がローカルコンピュータに返信され、ファイルのステータスが自動的に更新されます。

### 14.1 Sophos Live Protection の設定を確認する

Sophos Anti-Virus を新規インストールした場合、Sophos Live Protection はデフォルトで有効に設定されます。以前のバージョンの Sophos Anti-Virus をアップグレードした場合は、無効に設定されます。

- Sophos Live Protection の設定状態を確認するには次のように入力します。  
`/opt/sophos-av/bin/savconfig query LiveProtection`

### 14.2 Sophos Live Protection を有効/無効に切り替える

- Sophos Live Protection を有効にするには、次のように入力してください。  
`/opt/sophos-av/bin/savconfig set LiveProtection true`
- Sophos Live Protection を無効にするには、次のように入力してください。  
`/opt/sophos-av/bin/savconfig set LiveProtection false`

## 15 オンアクセス検索の設定

**注:** ネットワーク上のコンピュータを個別に構成する場合は、そのコンピュータに Enterprise Console や追加ファイルの新しい環境設定がダウンロードされると、構成した環境設定が上書きされることがありますので注意してください。

### 15.1 オンアクセス検索のファイル割り込み方法を変更する

Talpa に対応していない Linux カーネルのバージョンへアップグレードした場合、オンアクセス検索のファイル割り込み方法として Fanotify を使用できます。

**重要:** Sophos Anti-Virus での Fanotify の使用は、ベータ版機能であり、完全対応はしていません。

- オンアクセス検索のファイル割り込み方法として、Fanotify を使用する場合は、次のように入力します。

```
/opt/sophos-av/bin/savconfig set DisableFanotify false
```

### 15.2 検索の対象からファイルとディレクトリを除外する

ファイルとディレクトリを除外する方法には次の 2 とおあります。

- ファイル名やディレクトリ名を使用する
- ワールドカード文字を使用する

UTF-8 以外の文字セットでエンコードされているファイル名やディレクトリ名を除外するには、[ディレクトリ名とファイル名の文字エンコードを指定する](#) (p. 37) を参照してください。

#### 15.2.1 ファイル名やディレクトリ名を使用する

**注:** ネットワーク上のコンピュータを個別に構成する場合は、そのコンピュータに Enterprise Console や追加ファイルの新しい環境設定がダウンロードされると、構成した環境設定が上書きされることがありますので注意してください。

- 特定のディレクトリやファイルを除外するには、**ExcludeFilePaths** パラメータを使って **add** コマンドを実行してください。スラッシュを使用してディレクトリを指定します。たとえば、`/tmp/report` ファイルを、除外するファイル名やディレクトリ名のリストに追加するには、次のように入力します。

```
/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report
```

`/tmp/report/` ディレクトリを、除外するファイル名やディレクトリ名のリストに追加するには、次のように入力します。

```
/opt/sophos-av/bin/savconfig add ExcludeFilePaths /tmp/report/
```

- リストから除外アイテムを削除するには、**ExcludeFilePaths** パラメータを使って **remove** コマンドを実行してください。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig remove ExcludeFilePaths /tmp/report
```

## 15.2.2 ワイルドカード文字を使用する

**注:** ネットワーク上のコンピュータを個別に構成する場合は、そのコンピュータに Enterprise Console や追加ファイルの新しい環境設定がダウンロードされると、構成した環境設定が上書きされることがありますので注意してください。

- ワイルドカード文字を使用してファイル名やディレクトリ名を除外するには、**ExcludeFileOnGlob** パラメータを使って **add** コマンドを実行してください。有効なワイルドカード文字は、「\*」(0文字以上の任意の文字列と一致)、および「?」(任意の1文字と一致)です。たとえば、/tmp ディレクトリにあるテキストファイルを、除外するファイル名やディレクトリ名のリストに追加するには、次のように入力します。

```
/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/*.txt'
```

**注:** **ExcludeFileOnGlob to** を使ってディレクトリを検索の対象から除外する場合は、ワイルドカード「\*」をパスの最後に付け加える必要があります。たとえば次のように入力します。

```
/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob '/tmp/report/*'
```

- 指定する文字列を上のような引用符で囲まない場合は、Linux はワイルドカードを展開してその時点で該当するファイルのリストを Sophos Anti-Virus に渡します。この方法は、既存のファイルのみを除外し、以後作成されるファイルは検索されるように設定する場合に便利です。たとえば、/tmp ディレクトリにある既存のテキストファイルのみを、除外するファイル名やディレクトリ名のリストに追加するには、次のように入力します。

```
/opt/sophos-av/bin/savconfig add ExcludeFileOnGlob /tmp/*.txt
```

- リストから除外アイテムを削除するには、**ExcludeFileOnGlob** パラメータを使って **remove** コマンドを実行してください。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig remove ExcludeFileOnGlob  
'/tmp/notes.txt'
```

## 15.2.3 ディレクトリ名とファイル名の文字エンコードを指定する

Linux では、指定した文字コード (例: UTF-8、EUC\_jp) で、ディレクトリやファイルに名前を付けることができます。一方、Sophos Anti-Virus は、UTF-8 形式のみで除外アイテムを保存します。したがって、UTF-8 以外でエンコードされているファイル名やディレクトリ名を検索の対象から除外するには、除外を UTF-8 で指定した後、**ExclusionEncodings** パラメータを使ってエンコーディングを指定してください。これによって、除外するディレクトリやファイルの名前は、指定したエンコーディングによって評価され、一致した場合、ディレクトリやファイルはすべて除外されます。これは、**ExcludeFilePaths** パラメータと **ExcludeFileOnGlob** パラメータを使用して指定された除外に適用されます。デフォルトで、UTF-8、EUC\_jp、および ISO-8859-1 (Latin-1) が指定されています。

たとえば、EUC\_cn でエンコードされている名前のディレクトリとファイルを除外するには、**ExcludeFilePaths** パラメータや **ExcludeFileOnGlob** パラメータを使ってディレクト

リ名やファイル名を指定します。そして、次のようにして、EUC\_cnをエンコーディングの一覧に追加します。

```
/opt/sophos-av/bin/savconfig add ExclusionEncodings EUC_cn
```

これで、Sophos Anti-Virus は、指定されたディレクトリ名やファイル名すべてを、UTF-8、EUC\_jp、ISO-8859-1 (Latin-1)、および EUC\_cn で評価します。その後、名前が一致するディレクトリとファイルすべてを除外します。

## 15.3 検索の対象からファイルシステムの種類を除外する

デフォルトで、ファイルシステムの種類すべてが検索されます。

- ファイルシステムの種類を除外するには、**ExcludeFilesystems** パラメータを使って **add** コマンドを実行してください。有効なファイルシステムの種類は、**/proc/filesystems** ファイルに一覧が記載されています。たとえば、nfsをファイルシステムの種類の除外リストに追加するには、次のように入力してください。

```
/opt/sophos-av/bin/savconfig add ExcludeFilesystems nfs
```

- リストから除外アイテムを削除するには、**ExcludeFilesystems** パラメータを使って **remove** コマンドを実行してください。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig remove ExcludeFilesystems nfs
```

## 15.4 アーカイブファイル内を検索する

デフォルトで、アーカイブファイル内のオンアクセス検索は無効になっています。ただし、このようなファイルを一度に多数扱う必要があり、ウイルスを検出しなかった場合のリスクが大きいと判断できる場合は、このオプションを有効にしてください。この具体例としては、アーカイブファイルを重要な取引先にメール送信する場合などがあります。

**注:** 次の理由からこのオプションを無効にすることを推奨します。

- アーカイブファイル内を検索すると、検索速度が著しく低下します。
- このオプションの設定内容に関係なく、アーカイブファイルから展開したファイルを開くと、ファイルに対して検索が実行されます。

**注:** 脅威検出エンジンは、圧縮されていない状態で 8GB までの圧縮ファイルのみを検索します。これはエンジンが対応している POSIX ustar アーカイブフォーマットで 8GB 以上のファイルを扱えないためです。

- アーカイブファイル内の検索を**有効**にするには、次のように入力してください。

```
/opt/sophos-av/bin/savconfig set ScanArchives enabled
```

- アーカイブファイル内の検索を**無効**にするには、次のように入力してください。

```
/opt/sophos-av/bin/savconfig set ScanArchives disabled
```

## 15.5 感染ファイルをクリーンアップする

オンアクセス検索を実行したときに、感染ファイルをクリーンアップ (駆除または削除) するよう設定することができます。デフォルトでクリーンアップは無効になっています。

感染ファイルに対処するために Sophos Anti-Virus で実行されるアクションは、すべて Sophos Anti-Virus ログに記録されます。

**注:** 駆除と削除の両方を有効に設定することができますが、この設定は推奨しません。このように設定した場合、Sophos Anti-Virus では最初にファイルの駆除が実行されます。駆除に失敗すると、削除が行われます。

**注:** Sophos Anti-Virus では、ファイルを「開いたとき」に検索が実行された場合は、駆除や削除を実行することができます。「開いたとき」はファイルをコピー、移動、開いたときに該当します)。ただし、ファイルを「閉じたとき」に検索が実行された場合は、駆除や削除を行うことができません。「閉じたとき」はファイルを保存したときや作成したときに該当します。各 Linux コンピュータで「開いたとき」に実行される検索は、一元的に無効化できないこと、さらには次回ファイルにアクセスした際に駆除や削除が行われることから、通常の使用でこの動作が問題になることはありません。

### 15.5.1 感染ファイルと感染ブートセクタを駆除する

- オンアクセス検索での感染ファイルと感染ブートセクタの自動駆除を**有効**にするには、次のように入力します。

```
/opt/sophos-av/bin/savconfig add AutomaticAction disinfect
```

**重要:** Sophos Anti-Virus で駆除が実行される前に確認メッセージは表示されません。

**注:** 感染したドキュメントを駆除しても、ウイルスによるドキュメントの変更箇所は修復されません。(ウイルスの副作用に関する詳細をソフォス Web サイトで参照するには、[クリーンアップ情報を入手する](#) (p. 16) を参照してください。)

- オンアクセス検索での感染ファイルとブートセクタの自動駆除を**無効**にするには、次のように入力します。

```
/opt/sophos-av/bin/savconfig remove AutomaticAction disinfect
```

### 15.5.2 感染ファイルを削除する

**重要:** このオプションは、ソフォス テクニカルサポートより指示があった場合のみに使用してください。感染ファイルがメールボックスの際、Sophos Anti-Virus によってメールボックス全体が削除されてしまう場合もあります。

- オンアクセス検索での感染ファイルの自動削除を**有効**にするには、次のように入力します。

```
/opt/sophos-av/bin/savconfig add AutomaticAction delete
```

**重要:** Sophos Anti-Virus で削除が実行される前に確認メッセージは表示されません。

- オンアクセス検索での感染ファイルの自動削除を**無効**にするには、次のように入力します。

```
/opt/sophos-av/bin/savconfig remove AutomaticAction delete
```

## 16 追加ファイルベースの環境設定について

ここでは、追加ファイルベースの環境設定で Sophos Anti-Virus を設定する方法について説明します。

### 16.1 追加ファイルベースの環境設定について

ここでは、追加ファイルベースの環境設定の概要について説明します。

#### 16.1.1 追加ファイルベースの環境設定とは？

追加ファイルベースの環境設定は、Sophos Anti-Virus の設定方法の 1 つです。Sophos Enterprise Console を使用せずに行う環境設定で、Windows コンピュータを必要としません。

この方法は、Enterprise Console を使用できない場合のみに使用してください。

**注: Enterprise Console ベースの環境設定と追加ファイルベースの環境設定は同時に使用できません。**

追加ファイルベースの環境設定では、オンデマンド検索 ([オンデマンド検索を設定する](#) (p. 11) を参照) を除く、すべての Sophos Anti-Virus の機能を設定できます。

#### 16.1.2 追加ファイルベースの環境設定の使用方法

追加ファイルベースの環境設定を含むファイルを作成します。このファイルはオフラインなため、他のコンピュータからアクセスすることはできません。

他のコンピュータを設定する準備ができたなら、このオフラインファイルを、エンドポイントコンピュータからアクセス可能な場所にあるライブ環境設定ファイルにコピーします。アップデート時にライブファイルから設定内容を取得するよう、各エンドポイントコンピュータを構成します。

各エンドポイントコンピュータを再構成するには、オフライン環境設定ファイルをアップデートし、ライブ環境設定ファイルに再度コピーします。

**注:**

- 環境設定ファイルの安全を確保するため、以下のセクションの説明に従って、セキュリティ証明書を作成し、使用する必要があります。
- ユーザーが各自のコンピュータで設定を変更することを防ぐため、一部またはすべての設定内容をロックできます。

追加ファイルベースの環境設定ファイルの作成・使用方法は、次のセクションを参照してください。

## 16.2 追加ファイルベースの環境設定を使用する

追加ファイルベースの環境設定を使用する方法は次のとおりです。

- サーバーでセキュリティ証明書を作成する。
- 追加ファイルベースの環境設定を作成する。
- エンドポイントコンピュータに root 証明書をインストールする。
- 追加ファイルベースの環境設定を使用するよう、エンドポイントコンピュータを設定する。

### 16.2.1 サーバーでセキュリティ証明書を作成する

セキュリティ証明書を作成する方法は次のとおりです。

**注:** 証明書の生成に OpenSSL を使用している場合は、OpenSSL 0.9.8 以降を稼働している必要があります。

1. 証明書の作成に使用するスクリプトを取得します。スクリプトは、[ソフォスのサポートデータベースの文章 119602](#) から入手できます。
2. スクリプトを実行して、証明書のセットを作成します。たとえば、次のように入力します。

```
./create_certificates.sh /root/certificates
```

証明書の保存場所として、上記以外のディレクトリも指定できますが、安全な場所を指定するようにしてください。

3. 画面の指示に従って、root 鍵のパスワードを入力し、確認入力します。
4. 画面の指示に従って、署名鍵のパスワードを入力し、確認入力します。
5. 証明書がこのディレクトリにあることを確認します。次のように入力します。

```
ls /root/certificates/
```

次のようなファイルが表示されるはずですが。

```
extrafiles-root-ca.crt extrafiles-root-ca.key extrafiles-signing.cnf  
extrafiles-signing.crt extrafiles-signing.key
```

## 16.2.2 追加ファイルベースの環境設定を作成する

1. 追加ファイルベースの環境設定を保存するコンピュータで、`savconfig` コマンドを使用してオフライン環境設定ファイルを作成し、ファイル内のパラメータ値を設定します。構文は次のとおりです。

```
/opt/sophos-av/bin/savconfig -f オフライン環境設定のパス -c オペレーション パラメータ 値
```

各値の説明

- 「**-f オフライン環境設定のパス**」でファイル名を含むオフライン環境設定ファイルのパスを指定します。「`savconfig`」がファイルを作成します。
- **-c**: オフラインファイルのコーポレートレイヤーへのアクセスを指定するオプション (レイヤーの詳細は、[環境設定レイヤーについて](#) (p. 44) を参照してください)。
- **オペレーション**: `set`、`update`、`add`、`remove`、または `delete` オプション。
- **パラメータ**: 設定するパラメータ。
- **値**: パラメータの設定値。

たとえば、`/rootconfig/` ディレクトリに `OfflineConfig.cfg` というファイルを作成し、メール警告を無効に設定するには、次のように入力します。

```
/opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c set EmailNotifier Disabled
```

`savconfig` の使用方法の詳細は、[savconfig 設定コマンド](#) (p. 45) を参照してください。

2. パラメータの値を表示するには、**query** オペレーションを使用します。特定のパラメータや、すべてのパラメータの設定を表示することができます。たとえば、設定したパラメータすべての設定値を表示するには次のように入力します。

```
/opt/sophos-av/bin/savconfig -f /root/config/OfflineConfig.cfg -c query
```

3. オフライン環境設定ファイルのパラメータを設定し終わったら、ライブ環境設定ファイルを保存するための Web 共有または共有ディレクトリを作成します。
4. `addextra` というコマンドを使用してライブ環境設定ファイルを作成します。構文は次のとおりです。

```
/opt/sophos-av/update/addextra オフライン環境設定ファイルのパスライブ環境設定ファイルのパス --signing-key=署名鍵ファイルのパス --signing-certificate=署名証明書ファイルのパス
```

たとえば次のように入力します。

```
/opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /var/www/extrafiles/ --signing-key=/root/certificates/extrafiles-signing.key --signing-certificate=/root/certificates/extrafiles-signing.crt
```

## 16.2.3 エンドポイントコンピュータに root 証明書をインストールする

各エンドポイントコンピュータに root 証明書をインストールする必要があります。

1. 証明書を作成したコンピュータ (または証明書のコピー先コンピュータ) で、root 証明書用のディレクトリを新規作成します。次のように入力します。

```
mkdir rootcert
cd rootcert/
```

2. root 証明書を新しいディレクトリにコピーします。次のように入力します。

```
cp /root/certificates/extrfiles-root-ca.crt .
```

3. 新しいディレクトリを共有ディレクトリにコピーします。
4. 各エンドポイントコンピュータで、共有ディレクトリをマウントします。
5. 証明書をインストールします。構文は次のとおりです。

```
/opt/sophos-av/update/addextra_certs --install= ルート証明書の共有ディレクトリ
```

例:

```
/opt/sophos-av/update/addextra_certs --install= /mnt/rootcert/
```

## 16.2.4 追加ファイルベースの環境設定を使用するよう、エンドポイントコンピュータを設定する

環境設定ファイルをダウンロードして使用できるよう、エンドポイントコンピュータを設定する方法は次のとおりです。

1. ライブ環境設定ファイルが共有ディレクトリにある場合は、各クライアントマシンでそのディレクトリをマウントします。
2. 各エンドポイントコンピュータで、ライブ環境設定ファイルのパスを指定します。たとえば、次のように入力します。

```
/opt/sophos-av/bin/savconfig set ExtraFilesSourcePath
http://www.example.com/extrfiles
```

以上で各クライアントマシンに対する新しい環境設定が作成され、次回アップデート時に各コンピュータにダウンロードされます。

3. 今すぐアップデートを実行するには、次のように入力します。

```
/opt/sophos-av/bin/savupdate
```

## 16.3 追加ファイルベースの環境設定を更新する

1. 追加ファイルベースの環境設定が保存されているコンピュータで、`savconfig` コマンドを使用してオフライン環境設定ファイルを更新し、ファイル内のパラメータ値を設定します。

オフライン環境設定ファイルを作成したときと同じ構文を使用できます。

たとえば、`/opt/sophos-av` ディレクトリにある `OfflineConfig.cfg` というファイルを更新し、メール警告を有効化するには次のように入力します。

```
/opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg
-c set EmailNotifier Enabled
```

2. パラメータの値を表示するには、**query** オペレーションを使用します。特定のパラメータや、すべてのパラメータの設定を表示することができます。たとえば、設定したパラメータすべての設定値を表示するには次のように入力します。

```
/opt/sophos-av/bin/savconfig -f /opt/sophos-av/OfflineConfig.cfg
-c query
```

3. オフライン環境設定ファイルのパラメータを設定し終わったら、`addextra` というコマンドを使用してライブ環境設定ファイルを更新します。構文は次のとおりです。

```
/opt/sophos-av/update/addextra オフライン環境設定ファイルのパス ライブ環境設定ファイルのパス
--signing-key=署名鍵ファイルのパス
--signing-certificate=署名証明書ファイルのパス
```

例:

```
/opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg
/var/www/extrfiles/ --signing-key=
/root/certificates/extrfiles-signing.key
--signing-certificate=/root/certificates/extrfiles-signing.crt
```

以上で各クライアントマシンに対する環境設定が更新され、次回のアップデート時に各コンピュータにダウンロードされます。

4. 今すぐアップデートを実行するには、次のように入力します。

```
/opt/sophos-av/bin/savupdate
```

## 16.4 環境設定レイヤーについて

各エンドポイントの Sophos Anti-Virus にはオンデマンド検索を除く Sophos Anti-Virus のすべての機能が設定されているローカル環境設定ファイルがあります。

各ローカル環境設定ファイルには複数のレイヤーがあります。

- ソフォス: はじめからローカルの環境設定ファイルに存在するレイヤー。このレイヤーにはソフォスだけが変更できる製品出荷時の設定が含まれています。
- コーポレート: 追加ファイルベースの環境設定で構成すると作成されるレイヤー。
- ユーザー: ローカルで設定を行うと作成されるレイヤー。このコンピュータの Sophos Anti-Virus のみに適用される設定が含まれています。

複数のレイヤーに同じパラメータを設定できるようにするため、各レイヤーでは同じパラメータを使用します。ただし、Sophos Anti-Virus では、次のレイヤーの優先順位に従ってパラメータがチェックされます。

- デフォルトで、コーポレートレイヤーは、ユーザーレイヤーをオーバーライドする。
- コーポレート/ユーザーレイヤーは、ソフォスレイヤーをオーバーライドする。

たとえば、ユーザーレイヤーおよびコーポレートレイヤーで、それぞれパラメータを設定した場合、コーポレートレイヤーで設定されている値が使用されます。ただし、コーポレートレイヤーのパラメータ値を個別にロック解除し、その値をオーバーライドすることもできます。

追加ファイルベースの環境設定ファイルからローカルの環境設定ファイルを更新した場合は、追加ファイルベースの環境設定ファイルのコーポレートレイヤーでローカルファイル内のコーポレートレイヤーが上書きされます。

## 16.5 savconfig 設定コマンド

savconfig はオンデマンド検索以外の Sophos Anti-Virus の機能すべてを設定するためのコマンドです。コマンドのパスは `/opt/sophos-av/bin` です。このコマンドを使用して Sophos Anti-Virus の特定の機能を設定する方法は、次の項以降を参照してください。この項では、コマンドの構文について説明します。

savconfig の構文は次のとおりです。

**savconfig** **[オプション]** ... **[オペレーション]** **[パラメータ]** **[値]** ...

オプション、オペレーション、およびパラメータの一覧を表示するには次のように入力します。

```
man savconfig
```

### 16.5.1 オプション

オプションは1つまたは複数指定できます。主に各エンドポイントのローカル環境設定ファイル内の**レイヤー**を設定する際に使用します。コマンドはデフォルトでユーザーレイヤーにアクセスします。したがって、コーポレートレイヤーにアクセスする場合は、**-c** または **--corporate** オプションを使用してください。

また、ユーザーレイヤーの値をオーバーライドするため、デフォルトでコーポレートレイヤーのパラメータ値はロックされています。コーポレートレイヤーの設定のオーバーライドをユーザーに許可する場合は、**--nolock** オプションを使用してください。たとえば、**LogMaxSizeMB** の値を設定し、この値のオーバーライドを許可するには、次のように入力します。

```
/opt/sophos-av/bin/savconfig --nolock -f corpcnfig.cfg -c
LogMaxSizeMB 50
```

Enterprise Console を使用している場合、**--consoleav** オプションを使用すると、ウイルス対策ポリシー用パラメータの値だけが表示されます。次のように入力します。

```
/opt/sophos-av/bin/savconfig --consoleav query
```

また、**--consoleupdate** オプションを使用すると、Enterprise Console のアップデートポリシーの値だけが表示されます。次のように入力します。

```
/opt/sophos-av/bin/savconfig --consoleupdate query
```

## 16.5.2 オペレーション

オペレーションは1つだけ指定できます。オペレーションは、主に、パラメータへのアクセス方法を指定するために使用します。パラメータには、1つの値しか持つことができないものと、リストに数種類の値を持つことができるものがあります。オペレーションを使用すると、このようなリストに値を加えたり、リストから値を削除することができます。たとえば、**Email** というパラメータは、メール受信者の**リスト**です。

パラメータの値を表示するには、**query** オペレーションを使用します。たとえば、**EmailNotifier** というパラメータの値を表示するには次のように入力します。

```
/opt/sophos-av/bin/savconfig query EmailNotifier
```

Enterprise Console を使用している場合、savconfig のパラメータ値が返される際に、関連する Enterprise Console ポリシーと干渉するものは「Conflict」と表示されます。

## 16.5.3 パラメータ

パラメータは1つだけ指定できます。設定可能な基本的なパラメータの一覧を表示するには次のように入力します。

```
/opt/sophos-av/bin/savconfig -v
```

一部のパラメータには、2つ目のパラメータの指定が必要なものもあります。

## 16.5.4 値

パラメータには、1つまたは複数の値を指定できます。指定する値に空白が含まれる場合は、シングルクォーテーションで囲ってください。

## 17 トラブルシューティング

このセクションでは、Sophos Anti-Virus を使用しているときに生じる可能性のある問題の解決方法について説明します。

オンデマンド検索に関する Sophos Anti-Virus のリターンコードの詳細は、[補足: オンデマンド検索のリターンコード](#) (p. 53) を参照してください。

### 17.1 コマンドを実行できない

#### 現象

コンピュータで Sophos Anti-Virus コマンドを実行できない。

#### 原因

権限不足が原因である可能性があります。

#### 解決方法

root でコンピュータにログオンしてください。

### 17.2 除外の設定内容が適用されていない

#### 現象

これまでオンアクセス検索の対象から除外していたファイルを検索の対象に含めるよう Sophos Anti-Virus で指定しても、ファイルが引き続き除外されることがある。

#### 原因

以前検索されたファイルのキャッシュに、これまで除外されていたファイルがまだ含まれていることが原因である可能性があります。

#### 解決方法

使用しているオンアクセス検索の割り込み方法に従って、次のいずれかの手順を実行してください。

- Talpa を使用している場合は、キャッシュのフラッシュを試みてください。次のように入力します。

```
echo 'disable' > /proc/sys/talpa/intercept-filters/Cache/status
```

```
echo 'enable' > /proc/sys/talpa/intercept-filters/Cache/status
```

- Fanotify を使用している場合は、インストール済みの sav-protect サービスの再起動を試みてください。次のように入力します。

```
/etc/init.d/sav-protect restart
```

## 17.3 「マニュアル ... は登録されていません」といった内容のシステムエラーが表示される

### 現象

Sophos Anti-Virus の man ページを表示しようとする、「マニュアル ... は登録されていません」といった内容のメッセージがコンピュータに表示されます。

### 原因

環境変数 MANPATH に man ページのパスが通っていないことが原因である可能性があります。

### 解決方法

1. sh、ksh または bash シェルを実行している場合は、`/etc/profile` を開いて内容を編集します。

csh または tcsh シェルを実行している場合は、`/etc/login` を開いて内容を編集します。

**注:** ログインスクリプトやログインプロファイルがない場合は、コマンドプロンプトで次の手順を実行してください。この手順はコンピュータを再起動するたびに実行する必要があります。

2. 環境変数 MANPATH に `/usr/local/man` というディレクトリが追加されていることを確認します。

3. MANPATH にこのディレクトリがない場合は、次のように追加します。既存の設定には変更を加えないでください。

sh シェル、ksh シェル、または bash シェルを実行している場合は、以下を入力します。

```
MANPATH=$MANPATH:/usr/local/man
```

```
export MANPATH
```

csh シェルや tcsh シェルを実行している場合は、以下を入力します。

```
setenv MANPATH 値:/usr/local/man
```

ここで **値** は、既存の設定値です。

4. ログインスクリプトまたはログインプロファイルを保存します。

## 17.4 ディスク容量が足りなくなる

### 現象

Sophos Anti-Virus のディスク容量が足りなくなる (複雑なアーカイブファイルの検索を実行した場合など)。

### 原因

次のいずれかの原因が考えられます。

- アーカイブファイルを展開する際、Sophos Anti-Virus はファイルを /tmp ディレクトリに保存する。このディレクトリの容量が十分でない場合、ディスク容量が足りなくなることがあるため。
- Sophos Anti-Virus の容量がユーザーの容量制限 (quota) を越えた場合。

### 解決方法

次のいずれかの手順を実行してください。

- /tmp の容量を増やす。
- ユーザーの容量制限 (quota) を増加する。
- Sophos Anti-Virus で展開されるファイルの保存先ディレクトリを変更する。ディレクトリを変更するには、環境変数 SAV\_TMP を設定します。

## 17.5 オンデマンド検索のスピードが遅い

この問題は、次のいずれかが原因で発生することが考えられます。

### 現象

Sophos Anti-Virus のオンデマンド検索に非常に時間がかかる。

### 原因

次のいずれかの原因が考えられます。

- デフォルトで Sophos Anti-Virus は、クイックモード検索を行い、ウイルスが存在する可能性のある部分のみを検索する。フル検索が指定されている場合 (オプション `-f` を付けてコマンドを実行した場合)、ファイル全体が検索されるため。
- Sophos Anti-Virus のデフォルトの設定では、特定のファイルタイプのみが検索される。**すべての**ファイルを検索する設定になっていると、検索により時間がかかるため。

## 解決方法

適宜、次のいずれかを実行します。

- ソフォスのテクニカルサポートなどから指示があった場合を除き、フル検索の実行を避けてください。
- 特定の拡張子を持つファイルを検索するには、その拡張子を Sophos Anti-Virus がデフォルトで検索を実行するファイルタイプのリストに追加してください。詳細は、[特定の種類のファイルを検索する](#) (p. 11) を参照してください。

## 17.6 オンデマンド検索済みのファイルがすべてアーカイバでバックアップされる

### 現象

Sophos Anti-Virus でオンデマンド検索されたファイルすべてが、アーカイバで常にバックアップされる。

### 原因

これは、Sophos Anti-Virus がファイルのステータス変更時刻 (ctime) に変更を加えることにより発生します。デフォルトで Sophos Anti-Virus は、ファイルのアクセスタイム (atime) をウイルス検索前の時刻にリセットしようとはしますが、この影響により、i ノードのステータス変更時刻 (ctime) が変更されます。このため、ご使用のアーカイバが、ファイルの変更を **ctime** の値で判断している場合、Sophos Anti-Virus が検索したファイルすべてがバックアップされることとなります。

### 解決方法

**--no-reset-atime** オプションを使用して `savscan` コマンドを実行してください。

## 17.7 ウイルスがクリーンアップされない

### 現象

- Sophos Anti-Virus でウイルスをクリーンアップできない。
- Sophos Anti-Virus で「駆除に失敗しました」というメッセージが表示される。

### 原因

次のいずれかの原因が考えられます。

- 自動クリーンアップが有効になっていない。

- Sophos Anti-Virus で駆除できない種類のウイルスである。
- 感染ファイルが書き込み禁止のフロッピーディスクや CD などのリムーバブルメディアにある。
- 感染ファイルが NTFS ファイルシステム上にある。
- Sophos Anti-Virus でウイルスフラグメントが検出された場合。完全に一致するウイルスを見つけることができないためクリーンアップは行われません。

## 解決方法

適宜、次のいずれかを実行します。

- 自動クリーンアップを有効にする。
- 可能な場合、リムーバブルメディアへの書き込みを許可する。
- NTFS ファイルシステム上にあるファイルをローカルコンピュータで処理する。

## 17.8 ウィルスフラグメントが報告される

### 現象

Sophos Anti-Virus でウィルスのフラグメントが検出されたとレポートされることがある。

### 原因

これはファイルにウィルスのコードの一部と一致する部分があることを意味します。原因は次のいずれかです。

- 新種ウィルスの多くは既知のウィルスをもとにしたものなので、既知ウィルスの典型的なコードの一部が新種ウィルスに感染したファイルに発見されることがあります。
- 複製ルーチンにバグのあるウィルスが多いため、目的のファイルに正常に感染できない場合があります。このような場合、ウィルスの非アクティブな部分 (ウィルスの大部分の可能性あり) だけがホストファイルの中に現れることがあり、Sophos Anti-Virus はそれを検出します。
- システムのフル検索を実行すると、Sophos Anti-Virus で、データベースファイル内にウィルスのフラグメントがあると報告されることがある。

### 解決方法

1. 感染しているコンピュータの Sophos Anti-Virus をアップデートし、最新のウィルス定義ファイルを取得します。
2. ファイルの駆除を実行します ([特定の感染ファイルを駆除する](#) (p. 17) を参照)。
3. 依然としてウィルスのフラグメントが報告される場合は、ソフォステクニカルサポートに対処方法について問い合わせてください。

## 17.9 ディスクにアクセスできない

### 現象

リムーバブルディスクにあるファイルにアクセスできない。

### 原因

デフォルトで、Sophos Anti-Virus はブートセクタが感染しているリムーバブルディスクへのアクセスをブロックします。

### 解決方法

ブートセクタ感染型ウイルスに感染しているフロッピーディスクから、ファイルをコピーする場合などは、次のようにしてアクセスを許可します。

1. 次のように入力します。

```
/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat enabled
```

2. ディスクへのアクセス終了後は、次のように入力します。

```
/opt/sophos-av/bin/savconfig set AllowIfBootSectorThreat disabled
```

3. そして、コンピュータの再起動時に再感染することがないように、ディスクをコンピュータから取り出してください。

## 18 補足: オンデマンド検索のリターンコード

savscan は検索の結果を示すコードをシェルに返します。検索が完了した後に、次のような追加コマンドを実行すると、コードを表示できます。

```
echo $?
```

リターンコード	説明
0	エラー、ウイルスの検出ともになし
1	ユーザーが「Ctrl + C」を押して検索を中断した
2	エラーが発生したため検索が中断した
3	ウイルスが検出された

### 18.1 拡張リターンコード

**-eec** オプションを付けて savscan を実行すると、さらに詳細なコードがシェルに返されます。検索が完了した後に、次のような追加コマンドを実行すると、コードを表示できます。

```
echo $?
```

拡張リターンコード	説明
0	エラー、ウイルスの検出ともになし
8	続行可能なエラーが発生した
16	パスワードで保護されているファイルが見つかった (このファイルはスキャンされていない)
20	ウイルスを含むファイルが検出され駆除された

拡張リターンコード	説明
24	ウイルスを含むファイルが見つかり駆除されていない
28	メモリにウイルスが検出された
32	整合性チェックに失敗した
36	続行不可能なエラーが発生した
40	検索が中断した

## 19 補足:使用情報をソフォスに送信する機能の設定

Sophos Anti-Virus には、使用製品や OS の詳細に関する情報をソフォスに送信する機能があります。この機能は、製品を改善・強化してユーザーエクスペリエンスを向上させることを目標としています。

Sophos Anti-Virus をインストールすると、製品から使用情報を送信する機能はデフォルトで有効に設定されます。ソフォスでは、このオプションを有効に設定したままにしておくことをお願いしています。データの送信がセキュリティやコンピュータのパフォーマンスに影響を及ぼすことはありません。

- データは暗号化ファイルとして安全な場所に送信され、3カ月以内に削除されます。
- 週に一度、約 2KB のデータのみが送信されます。複数のマシンが同時に使用情報を送信する事態を回避するために、ランダムな間隔で送信されます。

この機能は、製品をインストールした後、いつでも無効にできます。

製品からの使用情報送信を無効にするには、次のように入力します。

```
/opt/sophos-av/bin/savconfig set DisableFeedback true
```

再び有効にするには、次のように入力します。

```
/opt/sophos-av/bin/savconfig set DisableFeedback false
```

## 20 補足:RMS の再起動の設定

サーバーとの通信を処理する RMS (Remote Management System) がクラッシュする、または正常に起動しない場合、アダプタによって RMS コンポーネントの mrouter および magent が再起動されます。

RMS を定期的に再起動する場合は、

**RestartIntervalHours=<時間>**

を \$INST/etc/sophosmgmtd.conf に追加してください。

## 21 用語集

<b>ブートセクタ感染型ウイルス</b>	ブート過程の初期段階を破壊するコンピュータウイルス。ブートセクタ感染型ウイルスは、マスターブートセクタかDOSブートセクタに感染します。
<b>セントラルインストールドイレクトリ (CID)</b>	ソフォス製品やアップデート版が配置されるフォルダ。ネットワーク上のコンピュータはこのフォルダからアップデートします。
<b>駆除</b>	駆除によってファイルやブートセクタからウイルスが除去されます。
<b>追加ファイル</b>	ネットワーク用の Sophos Anti-Virus の環境設定の保存先。コンピュータでアップデートが実行される際、ここから環境設定ファイルがダウンロードされます。
<b>オンアクセス検索</b>	最も基本的なウイルス対策機能。ファイルにアクセス(コピー、保存、移動、開くなど)した時点で、Sophos Anti-Virus が検索を実行し、感染していない場合のみアクセスを許可します。
<b>オンデマンド検索</b>	ユーザー自身が開始する検索。ファイルを個別に検索したり、コンピュータで読み取り権限のあるファイルすべてを検索するなど、さまざまなオンデマンド検索を実行できます。
<b>プライマリアップデート元</b>	コンピュータの通常のアップデート元。アクセスにはアカウント情報が必要な場合があります。
<b>スケジュール検索</b>	設定した日時に実行できる、コンピュータ全体または一部に対する検索。
<b>セカンダリアップデート元</b>	プライマリアップデート元にアクセスできない場合に、コンピュータがアクセスするアップデート元。アクセスにはアカウント情報が必要な場合があります。
<b>Sophos Live Protection</b>	オンラインベースのテクノロジーを使って、疑わしいファイルが脅威であるかを瞬時に解析する機能。Sophos Anti-Virus のクリーンアップ機能で設定されているアクションを実行します。

**アップデートクライアント** Sophos Anti-Virus をインストールしたコンピュータではあるが、他のコンピュータのアップデート元としては使用しないコンピュータ。

**アップデートサーバー** Sophos Anti-Virus がインストールされたコンピュータで、他のコンピュータのアップデート元として使用されるコンピュータ。他のコンピュータは、ネットワークにおける Sophos Anti-Virus のデプロイ方法により、アップデートサーバーまたはアップデートクライアントとなります。

**ウイルス** 自身を他のプログラムにコピーするコンピュータプログラム。コンピュータシステムを妨害したり、データを破壊したりすることがあります。ウイルスにはホストプログラムが必要で、起動されるまでコンピュータに感染することはありません。ウイルスには、自らをコピーしてネットワークへ増殖するものや、あるいはメールを介して自己を転送させるものがあります。「ウイルス」という用語は、ウイルス、ワーム、トロイの木馬の総称として使われることもあります。

## 22 テクニカルサポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- 「Sophos Community」ユーザーフォーラム (英語) (<http://community.sophos.com>) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。 [www.sophos.com/ja-jp/support.aspx](http://www.sophos.com/ja-jp/support.aspx)
- 製品ドキュメントのダウンロード。 [www.sophos.com/ja-jp/support/documentation.aspx](http://www.sophos.com/ja-jp/support/documentation.aspx)
- オンラインでのお問い合わせ。  
<https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx>

## 23 ご利用条件

Copyright © 2016 Sophos Limited. All rights reserved. この出版物の一部または全部を、電子的、機械的な方法、写真複製、録音、その他いかなる形や方法においても、使用許諾契約の条項に準じてドキュメントを複製することを許可されている、もしくは著作権所有者からの事前の書面による許可がある場合以外、無断に複製、復元できるシステムに保存、または送信することを禁じます。

Sophos、Sophos Anti-Virus および SafeGuard は、Sophos Limited、Sophos Group および Utimaco Safeware AG の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us know so we can promote your project in the [DOC software success stories](#).

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A [number of companies](#) around the world provide

commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let [me](#) know.

[Douglas C. Schmidt](#)

## GNU General Public License

一部のソフトウェアプログラムは、特に複製、変更または特定のプログラム、あるいはその一部の頒布、およびソースコードへのアクセスを許可する、GNU 一般公衆利用許諾契約書 (GNU General Public License、あるいは単に GPL)、または同様のフリーソフトウェア使用許諾契約に基づいてユーザーの使用が許諾 (またはサブライセンス) されています。GPL に基づき使用が許諾され、実行可能なバイナリ形式で頒布されるいかなるソフトウェアも GPL によりソースコードの開示が義務付けられています。このソフトウェアと共に頒布されるこのようなソフトウェアのソースコードの入手を希望する場合は、次のメールアドレスにてソフトウェアまでその旨をご連絡ください: [savlinuxgpl@sophos.com](mailto:savlinuxgpl@sophos.com)。GPL の利用規約は、次のリンク先をご覧ください: [www.gnu.org/copyleft/gpl.html](http://www.gnu.org/copyleft/gpl.html)。

## libmagic – file type detection

Copyright © Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994–2004 Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice immediately at the beginning of the file, without modification, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

## Medusa web server

Medusa was once distributed under a 'free for non-commercial use' license, but in May of 2000 Sam Rushing changed the license to be identical to the standard Python license at the time. The standard Python license has always applied to the core components of Medusa, this change just frees up the rest of the system, including the http server, ftp server, utilities, etc. Medusa is therefore under the following license:

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of Sam Rushing not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

SAM RUSHING DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SAM RUSHING BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Sam would like to take this opportunity to thank all of the folks who supported Medusa over the years by purchasing commercial licenses.

## OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

### **OpenSSL license**

Copyright © 1998-2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
 “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

#### Original SSLeay license

Copyright © 1995–1998 Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)) All rights reserved.

This package is an SSL implementation written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com)). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young ([eay@cryptsoft.com](mailto:eay@cryptsoft.com))”

The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com))”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

## Protocol Buffers (libprotobuf)

Copyright 2008, Google Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Code generated by the Protocol Buffer compiler is owned by the owner of the input file used when generating it. This code is not standalone and requires a support library to be linked with it. This support library is itself covered by the above license.

## pycrypto

Distribute and use freely; there are no restrictions on further dissemination and usage except those imposed by the laws of your country of residence. This software is provided "as is" without warranty of fitness for use or suitability for any purpose, express or implied. Use at your own risk or not at all.

Incorporating the code into commercial products is permitted; you do not have to make source available or contribute your changes back (though that would be nice).

– amk ([www.amk.ca](http://www.amk.ca))

## Python

### PYTHON SOFTWARE FOUNDATION LICENSE VERSION 2

1. This LICENSE AGREEMENT is between the Python Software Foundation ("PSF"), and the Individual or Organization ("Licensee") accessing and otherwise using this software ("Python") in source or binary form and its associated documentation.
2. Subject to the terms and conditions of this License Agreement, PSF hereby grants Licensee a nonexclusive, royalty-free, worldwide license to reproduce, analyze, test, perform and/or display publicly, prepare derivative works, distribute, and otherwise use Python alone or in any derivative version, provided, however, that PSF's License Agreement and PSF's notice of copyright, i.e., "Copyright © 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009 Python Software Foundation; All Rights Reserved" are retained in Python alone or in any derivative version prepared by Licensee.
3. In the event Licensee prepares a derivative work that is based on or incorporates Python or any part thereof, and wants to make the derivative work available to others as provided herein, then Licensee hereby agrees to include in any such work a brief summary of the changes made to Python.
4. PSF is making Python available to Licensee on an "AS IS" basis. PSF MAKES NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED. BY WAY OF EXAMPLE, BUT NOT LIMITATION, PSF MAKES NO AND DISCLAIMS ANY REPRESENTATION OR WARRANTY OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF PYTHON WILL NOT INFRINGE ANY THIRD PARTY RIGHTS.
5. PSF SHALL NOT BE LIABLE TO LICENSEE OR ANY OTHER USERS OF PYTHON FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES OR LOSS AS A RESULT OF MODIFYING, DISTRIBUTING, OR OTHERWISE USING PYTHON, OR ANY DERIVATIVE THEREOF, EVEN IF ADVISED OF THE POSSIBILITY THEREOF.
6. This License Agreement will automatically terminate upon a material breach of its terms and conditions.
7. Nothing in this License Agreement shall be deemed to create any relationship of agency, partnership, or joint venture between PSF and Licensee. This License Agreement does not grant permission to use PSF trademarks or trade name in a trademark sense to endorse or promote products or services of Licensee, or any third party.
8. By copying, installing or otherwise using Python, Licensee agrees to be bound by the terms and conditions of this License Agreement.

## TinyXML XML parser

[www.sourceforge.net/projects/tinyxml](http://www.sourceforge.net/projects/tinyxml)

Original code by Lee Thomason ([www.grinninglizard.com](http://www.grinninglizard.com))

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

## zlib data compression library

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org)

Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)

20161125

# 索引

## E

Enterprise Console [6](#)

## M

man ページが見つからない [48](#)

## S

savconfig [45](#)

savsetup [31](#)

Sophos Anti-Virus の設定 [6](#)

Sophos Anti-Virus ログ [30](#)

環境設定 [30](#)

Sophos Live Protection [35](#)

## U

UNIX 実行ファイル, オンデマンド検索 [13](#)

## あ

アーカイブファイル [11-12](#)

オンデマンド検索 [11-12](#)

アイテムの除外 [13, 36-37](#)

オンアクセス検索 [36](#)

オンデマンド検索 [13](#)

文字エンコード [37](#)

アップデート [20-21, 31](#)

カスタマイズされたカーネルへの対応 [21](#)

環境設定 [31](#)

最新のカーネルへの対応 [21](#)

即時 [20](#)

## う

ウイルス [14, 16, 18, 29, 50-51](#)

クリーンアップされない [50](#)

フラグメントのレポート [51](#)

解析 [16](#)

検出 [14, 29](#)

副作用 [18](#)

ウイルスの副作用 [18](#)

## え

エラーコード [53](#)

## お

オンアクセス検索 [8, 36](#)

Fanotify [36](#)

アイテムの除外 [36](#)

オンデマンド検索 [10-13, 22](#)

UNIX 実行ファイル [13](#)

アーカイブファイル [11-12](#)

アイテムの除外 [13](#)

コンピュータ [10](#)

シンボリックリンクの参照先 [12](#)

スケジュール検索 [22](#)

ディレクトリ [10](#)

ファイル [10](#)

ファイルシステム [10, 13](#)

ファイルの種類 [11, 13](#)

ブートセクタ [10](#)

リモートコンピュータ [12](#)

オンデマンド検索のスピードが遅い [49](#)

## か

カーネル [21](#)

カスタマイズ版 [21](#)

最新リリース [21](#)

カスタマイズされたカーネル [21](#)

## <

クリーンアップ情報 [16](#)

## こ

コマンドラインの警告 [14](#)

コマンドライン警告 [27](#)

コンピュータ, オンデマンド検索 [10](#)

## し

シンボリックリンクの参照先, オンデマンド検索 [12](#)

## す

スケジュール検索 [22](#)

## て

ディスク, アクセス [52](#)

ディスクへのアクセス [52](#)

ディスク容量不足 [49](#)

ディレクトリ, オンデマンド検索 [10](#)

デスクトップ・ポップアップ警告 [14](#), [26](#)

## ふ

ファイル, オンデマンド検索 [10](#)  
ファイルシステム, オンデマンド検索 [10](#), [13](#)  
ファイルの種類, オンデマンド検索 [11](#), [13](#)  
ブートセクタ [10](#), [18](#), [52](#)  
    オンデマンド検索 [10](#)  
    感染 [52](#)  
    駆除 [18](#)  
フラグメントのレポート, ウイルス [51](#)

## ま

マニュアル ... は登録されていません [48](#)

## め

メール警告 [27](#)

## り

リターンコード [53](#)  
リモートコンピュータ, オンデマンド検索 [12](#)

## れ

レイヤー, 環境設定ファイル [44](#)

## ろ

ログ, Sophos Anti-Virus [30](#)  
    環境設定 [30](#)