SOPHOS
Security made simple.

# Sophos Anti-Virus for Unix

# 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

このマニュアルは、Sophos Anti-Virus for UNIX の使用方法や設定方法について説明しています。

Sophos Anti-Virus のインストール方法については、「*Sophos Anti-Virus for UNIX* スタートアップガイド」をご覧ください。

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

# 2 Sophos Anti-Virus for UNIX について

## 2.1 Sophos Anti-Virus とは

Sophos Anti-Virus は、UNIX 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) を検出し、対処します。UNIX を狙うすべてのウイルスを検出することはもちろん、UNIX コンピュータに潜む UNIX 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

Sophos Anti-Virus ではオンデマンド検索を実行できます。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実行することもできます。

## 2.3 Sophos Anti-Virus の使い方

Sophos Anti-Virus にはコマンドラインインターフェースが用意されており、Sophos Anti-Virus のすべての機能と設定はコマンドラインから操作できます。

> **注**
> 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。

このマニュアルは、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

ネットワーク上に Enterprise Console で一元管理していない UNIX コンピュータがある場合、Sophos Anti-Virus を設定する方法は次のとおりです。

- コンピュータのアップデート時に適用される環境設定ファイルを編集して、スケジュール検索、警告、ログ、アップデート機能を一元的に設定する。詳細は、補足: 追加ファイルベースの環境設定について (p. 15)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 コマンドライン インターフェースを使用して、オンデマンド検索を設定する。

Enterprise Console で一元管理せず、スタンドアロン (ソフォスから直接アップデートしている状態) で利用している UNIX コンピュータがある場合は、Sophos Anti-Virus の機能はすべて Sophos Anti-Virus コマンドライン インターフェースを使用して設定します。

Sophos Enterprise Console で UNIX コンピュータを一元管理している場合、Sophos Anti-Virus を設定する方法は次のとおりです。

- Enterprise Console からスケジュール検索、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 Enterprise Console ヘルプを参照してください。

  **注**
  これらの機能には、Enterprise Console では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 UNIX コンピュータのローカル環境で Sophos Anti-Virus コマンドライン インターフェースを使用して設定してください。このように設定したパラメータは Enterprise Console では無視されます。

- 各 UNIX コンピュータのローカル環境で Sophos Anti-Virus コマンドライン インターフェースを使用してオンデマンド検索を設定する。

**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を併用することはできません。

# 3 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実行することもできます。

オンデマンド検索のスケジュールを設定するには、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。

## 3.1 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。

### 3.1.1 コンピュータのオンデマンド検索の実行

Sophos Anti-Virus をインストールしたら、直ちにコンピュータ全体のウイルス検索を実施することを推奨します。これを行うには、オンデマンド検索を実行します。

> **注**
> この操作は、特にサーバーの場合、他のコンピュータへのウイルス拡散リスクを最小化するために重要となります。

- コンピュータのオンデマンド検索を実行するには、次のように入力します。
  ```
  savscan /
  ```

### 3.1.2 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。

### 3.1.3 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。

## 3.2 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
```

## 3.2.1 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はなく、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。

## 3.2.2 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。

## 3.2.3 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。

## 3.2.4 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。

- 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。

## 3.2.5 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`

## 3.2.6 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す。

- 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。

## 3.2.7 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`

## 3.2.8 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用して、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 オプションを使用し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
```

## 3.2.9 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`
  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。

# 4 ウイルスが検出された場合の動作

ウイルスが検出された場合、Sophos Anti-Virus はデフォルトで次のように動作します。

- 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. 12)を参照)。
- Enterprise Console によって集中管理されている場合、Enterprise Console に警告を送信する。
- root@localhost にメール警告を送信する。

デフォルトで Sophos Anti-Virus は、警告も表示します。

## オンデマンド検索

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 Sophos Anti-Virus は、コマンドラインの警告を表示します。検出されたウイルスは、>>> と ウイルスまたはウイルスフラグメントで始まる行で報告されます。

```
SAVScan ウイルス検出ユーティリティ
バージョン 4.69.0 [Linux/Intel]
ウイ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.aspx, Email 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. 9)を参照してください。

 

# 5 ウイルスのクリーンアップ

## 5.1 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。

## 5.2 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. 10)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。

### 5.2.1 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`

### 5.2.2 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。

# 5.3 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。

## 5.3.1 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. 9)を参照してください。)

## 5.3.2 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. 9)を参照してください。)

### 5.3.3 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。

### 5.3.4 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。

## 5.4 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問い合わせてください。

# 6 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。

Syslog に記録されている情報の詳細は、補足: Syslog メッセージ (p. 29)を参照してください。

- Sophos Anti-Virus ログを表示するには、コマンドプロンプトで 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
  ```

# 7 Sophos Anti-Virus の即時アップデート

自動アップデートを有効に設定している場合、Sophos Anti-Virus は自動的にアップデートを行います。ただし、次の自動アップデートを待たずに Sophos Anti-Virus を即座にアップデートすることも可能です。

- Sophos Anti-Virus を即座にアップデートするには、アップデートを行うコンピュータ上で次を入力します。
  `/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。

# 8 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 |

## 8.1 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 |
| 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 |

# 9 補足: 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。

## 9.1 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。

### 9.1.1 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を併用することはできません。

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. 4)を参照) を除く、すべての Sophos Anti-Virus の機能を設定できます。

### 9.1.2 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。

# 9.2 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。

## 9.2.1 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。

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

## 9.2.2 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. 19)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. 19)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
   ```

## 9.2.3 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/extrafiles-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/
   ```

 

### 9.2.4 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/extrafiles
   ```

   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。
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
   ```

## 9.3 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ー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/
   extrafiles/ --signing-key= /root/certificates/extrafiles-signing.key --
   signing-certificate=/root/certificates/extrafiles-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
   ```

# 9.4 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。

# 9.5 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
```

## 9.5.1 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 corpconfig.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
```

## 9.5.2 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。

## 9.5.3 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。

## 9.5.4 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。

# 10 補足: 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 を使用し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 のみから削除や更新を行うことができます。

## 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. 22) 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. update オペレーションと NamedScans パラメータを付けて savconfig コマンドを実行して、Sophos Anti-Virus で設定されているスケジュール検索を更新します。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. update オペレーションと NamedScans パラメータを付けて savconfig コマンドを実行して、Sophos Anti-Virus で設定されているスケジュール検索を更新します。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. 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。

# 10.9 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。

Syslog に記録されている情報の詳細は、補足: Syslog メッセージ (p. 29)を参照してください。

- Sophos Anti-Virus ログを表示するには、コマンドプロンプトで 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
  ```

# 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 補足: メール警告の設定

**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コンソールベースや追加ファイルベース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メール警告が送信されるよう Sophos Anti-Virus を設定できます。メール警告は英語または日本語で送信できます。

## 11.1 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`

## 11.2 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 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。

## 11.4 メール受信者を指定する

Sophos Anti-Virus ではデフォルトで root@localhost にメール警告が送信されます。

- 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
  ```

# 11.5 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
  ```

# 11.6 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
  ```

# 11.7 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
  ```

# 11.8 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 補足: 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 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 補足: Syslog メッセージ

Sophos Anti-Virus ログは、syslog に次の 3種類のメッセージを記録します。

- `ACTION-REQUIRED`: 対処が必要なメッセージです。
- `ERROR`: 検索中に発生したエラーの詳細が表示されます。
- `INFO`: 検索処理に関する情報が表示されます。

メッセージは深刻度の降順に表示されます。

## 対処が必要なメッセージ

次のメッセージが表示された場合は、対処が必要です。

| Syslog メッセージ | 説明 | メッセージ ID | 注 |
|---|---|---|---|
| 「脅威データが最新版でないので、アップデートしてください。」 | 脅威データが最新版でないので、アップデートしてください。 | `VIRUS-DATA-OLD` | アップデート元が、ソフォスからアップデートを取得していないことを意味します。ソフォスから適時にアップデートが配布されるよう調査する必要があります。 |
| 「Sophos Anti-Virus はアップデートするよう設定されていません。」 | Sophos Anti-Virus はアップデートするよう設定されていません。 | `NO-UPDATE-CONFIGURATION` | ソフォスからアップデートを取得している場合のみに、Sophos Anti-Virus は継続した保護を提供できます。このコンピュータはアップデートするよう設定されていません。 |
| 「ソフォスからの直接アップデートがサポートされていないため、ソフォスからアップデートしていません。」 | ソフォスからの直接アップデートがサポートされていないため、ソフォスからアップデートしていません。 | `NO-UPDATE-FROM-SOPHOS` | 古いメッセージなので、表示されることはありません。 |
| 「オンデマンド検索中、脅威が %s: %s で検出されました。(ファイルはまだ感染しています。)」 | Sophos Anti-Virus はオンデマンド検索中に脅威を検出しました。ファイルはまだ感染しています。 | `NOTIFY-ONDEMAND-THREAT-INFECTED` | ログインしてファイルを削除するか、savscan を使用して駆除を試みる必要があります。 |

| Syslog メッセージ | 説明 | メッセージ ID | 注 |
|---|---|---|---|
| 「オンデマンド検索中、脅威が %s: %s で検出されました。(ファイルは隔離されました。)」 | Sophos Anti-Virus はオンデマンド検索中に脅威を検出しました。ファイルはまだ感染しています。実行ファイルでないため、root 権限で検索を実行した場合、通常のユーザーがファイルにアクセスすることはできません。 | NOTIFY-ONDEMAND-THREAT-QUARANTINED | ログインしてファイルを削除するか、savscan を使用して駆除を試みる必要があります。 |

## エラーメッセージ

検索処理中に発生したエラーの詳細が表示されます。対処が必要な場合、その方法も表示されます。

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「発生したインシデントの数が多すぎます。%s件のインシデント通知が破棄されました。」 | 発生したインシデントの数が多すぎます。%s件のインシデント通知が破棄されました。<br>savd に過剰な数の通知が送信されたため、一部の通知が破棄されたことを意味します。 | MESSAGES_DROPPED %s |
| 「リスポーン限度を超えました。これ以上検索プロセッサは開始されません。」 | リスポーン限度を超えました。これ以上検索プロセッサは開始されません。<br>savscand の起動に失敗したため、savd による savscand プロセスの作成が停止されました。問題が解決したら savd を再起動してください。 | RESPAWN-LIMIT |
| 「検索プロセッサのリスポーンを抑制しています。」 | savscand プロセスがすぐに強制終了してしまうため、savd は savscand プロセスの起動を制御しています。 | RESPAWN-THROTTLE |
| 「以前の Sophos Anti-Virus デーモンのインスタンスが、正常に終了しませんでした。」 | 前回 Sophos Anti-Virus は正常に終了しませんでした。<br>何も対処する必要はありません。 | SAVD-CLEANUP |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「検索プロセッサを強制的に終了しました。」 | Sophos Anti-Virus スキャナは終了しました。<br>Savd は savscand を強制終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-KILLED |
| 「検索プロセッサを強制的に終了しました。」 | Sophos Anti-Virus スキャナは終了しました。<br>Savd は savscand を強制終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-KILLED-PID |
| 「検索プロセッサは、次のシグナルを表示して予期せず終了しました: %s。」 | Sophos Anti-Virus スキャナは終了しました。<br>シグナルを受信したため savscand は終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-SIGNAL |
| 「検索プロセッサは、次のシグナルを表示して起動中に終了しました: %s。」 | Sophos Anti-Virus スキャナは開始しませんでした。<br>起動中にシグナルを受信したため savscand は終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-STARTUP-SIGNAL |
| 「検索プロセッサは、次のステータスコードを表示して起動中に終了しました: %s。」 | Sophos Anti-Virus スキャナは開始しませんでした。<br>起動中に savscand は終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-STARTUP-STATUS |
| 「検索プロセッサは、次のステータスコードを表示して予期せず終了しました: %s。」 | Sophos Anti-Virus スキャナは予期せず終了しました。<br>savscand は予期せず終了しました。この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-STATUS |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「検索プロセッサを終了しました。」 | Sophos Anti-Virus スキャナは終了しました。<br>Savd は savscand を終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-TERMED |
| 「検索プロセッサを終了しました。」 | Sophos Anti-Virus スキャナは終了しました。<br>Savd は savscand を終了しました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | SCANNER-DIED-TERMED-PID |
| 「ハートビートメッセージが送信されなかったため、検索プロセッサは停止されます。」 | Sophos Anti-Virus は、ハートビートメッセージを送信せずに停止しました。<br>savscand は、ハートビートメッセージを送信せずにタイムアウトしました。Savd によって終了されました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | TIMEOUT-SCANNER-HEARTBEAT |
| 「検索プロセッサは、起動時にタイムアウトしました。」 | Sophos Anti-Virus は起動せずにタイムアウトしました。<br>savscand は、起動せずにタイムアウトしました。Savd によって終了されました。<br>この問題が頻繁に発生しない限り、何も対処する必要はありません。 | TIMEOUT-SCANNER-STARTUP |
| 「オンデマンド検索中、脅威が %s: %s で検出されました。(ファイルは削除されました。)」 | Sophos Anti-Virus はオンデマンド検索中に脅威を検出しました。ファイルは削除されました。 | NOTIFY-ONDEMAND-THREAT-DELETED |
| 「オンデマンド検索中、脅威が %s: %s で検出されました。(ファイルは駆除されました。)」 | Sophos Anti-Virus はオンデマンド検索中に脅威を検出しました。ファイルは駆除されました。 | NOTIFY-ONDEMAND-THREAT-DISINFECTED |
| 「オンデマンド検索がユーザーによって中止されました。」 | Sophos Anti-Virus 検索がユーザーによって停止されました。 | SAVSCAN-ABORTED |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「スケジュール検索 ¥"%s¥" に失敗しました。エラー %s (%s) が発生しました。」 | エラーが発生して、Sophos Anti-Virus スケジュール検索に失敗しました。<br>次回に予定されているスケジュール検索で、検索が再試行されます。 | SCHEDULED-SCAN-FAILED |
| 「スケジュール検索 ¥"%s¥" に失敗しました: マウントを解析できませんでした。」 | マウントを解析できなかったため、Sophos Anti-Virus スケジュール検索 に失敗しました。<br>この問題が引き続き発生する場合は、ソフォスのサポートにお問い合わせください。「マウント」の出力を確認してください。 | SCHEDULED-SCAN-FAILED-MOUNT-PARSING |
| 「スケジュール検索 ¥"%s¥" に失敗しました: 脅威データ (%s) をロードできません。」 | 脅威データを読み込み中、Sophos Anti-Virus スケジュール検索に失敗しました。<br>引き続き検索に失敗しない限り、対処は必要はありません。 | SCHEDULED-SCAN-FAILED-VDL-LOAD-ERROR |
| 「脅威データ (%s) をロードできません。」 | 脅威データを読み込み中、Sophos Anti-Virus は失敗しました。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。 | SAVI_VDL_LOAD_ERROR |
| 「どのアップデート元からも複製することができませんでした。」 | Sophos Anti-Virus はアップデートに失敗した。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、プライマリアップデートの設定が正しいことを確認してください。 | ALL_UPDATE_SOURCES_FAILED |
| 「'%s' のダウンロードに失敗しました: 認証が無効です。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、プライマリアップデートの設定が正しいことを確認してください。 | BAD-BACKUP-AUTHENTICATION |

| Syslog メッセージ | 説明 | メッセージ ID |
| --- | --- | --- |
| 「'%s' のダウンロードに失敗しました: プロキシの認証が無効です。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、プライマリアップデートの設定が正しいことを確認してください。 | BAD-BACKUP-PROXY-AUTHENTICATION |
| 「'%s' のダウンロードに失敗しました: ファイルが存在しません。」 | Sophos Anti-Virus はアップデートできません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、プライマリアップデートの設定が正しいことを確認してください。 | BAD-BACKUP-URL |
| 「'%s' のダウンロードに失敗しました: 認証が無効です。ExtraFilesUsername および ExtraFilesPassword を確認してください。」 | Sophos Anti-Virus は ExtraFiles のダウンロードに失敗しました。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、ExtraFilesUsername および ExtraFilesPassword が正しいことを確認してください。 | BAD-EXTRAFILES-AUTHENTICATION |
| 「'%s' のダウンロードに失敗しました: プロキシの認証が無効です。<br>ExtraFilesProxyUsername および ExtraFilesProxyPassword を確認してください。」 | Sophos Anti-Virus は ExtraFiles のダウンロードに失敗しました。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、ExtraFilesProxyUsername および ExtraFilesProxyPassword が正しいことを確認してください。 | BAD-EXTRAFILES-PROXY-AUTHENTICATION |

| Syslog メッセージ | 説明 | メッセージ ID |
| --- | --- | --- |
| 「'%s' のダウンロードに失敗しました: ファイルが存在しません。<br>`ExtraFilesSourcePath` を確認してください。」 | Sophos Anti-Virus は `ExtraFiles` のダウンロードに失敗しました。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、ExtraFilesSourcePath が正しいことを確認してください。 | `BAD-EXTRAFILES-URL` |
| 「'%s' のダウンロードに失敗しました: 認証が無効です。<br>`PrimaryUpdateUsername` および `PrimaryUpdatePassword` を確認してください。」 | Sophos Anti-Virus は、プライマリアップデート元で認証できません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、`PrimaryUpdateUsername` および `PrimaryUpdatePassword` が正しいことを確認してください。 | `BAD-PRIMARY-AUTHENTICATION` |
| 「'%s' のダウンロードに失敗しました: プロキシの認証が無効です。<br>`PrimaryUpdateProxyUsername` および `PrimaryUpdateProxyPassword` が正しいことを確認してください。」 | Sophos Anti-Virus は、プライマリアップデート元プロキシで認証できません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、次の内容を確認してください。<br>`PrimaryUpdateProxyUsername` および `PrimaryUpdateProxyPassword` が正しいことを確認してください。 | `BAD-PRIMARY-PROXY-AUTHENTICATION` |

| Syslog メッセージ | 説明 | メッセージ ID |
| --- | --- | --- |
| 「'%s' のダウンロードに失敗しました: ファイルが存在しません。<br>`PrimaryUpdateSourcePath` を確認してください。」 | Sophos Anti-Virus は、プライマリアップデート元に接続できません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、次の内容を確認してください。<br>PrimaryUpdateSourcePath が正しいことを確認してください。 | `BAD-PRIMARY-URL` |
| 「'%s' のダウンロードに失敗しました: 認証が無効です。<br>`SecondaryUpdateUsername` および `SecondaryUpdatePassword` を確認してください。」 | Sophos Anti-Virus は、セカンダリアップデート元で認証できません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、`SecondaryUpdateUsername` および`SecondaryUpdatePassword` が正しいことを確認してください。 | `BAD-SECONDARY-AUTHENTICATION` |
| 「'%s' のダウンロードに失敗しました: プロキシの認証が無効です。<br>`SecondaryUpdateProxyUsername` および `SecondaryUpdateProxyPassword` が正しいことを確認してください。」 | Sophos Anti-Virus は、プライマリアップデート元プロキシで認証できません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、次の内容を確認してください。<br>`SecondaryUpdateProxyUsername` および `SecondaryUpdateProxyPassword` が正しいことを確認してください。 | `BAD-SECONDARY-PROXY-AUTHENTICATION` |

| Syslog メッセージ | 説明 | メッセージ ID |
| --- | --- | --- |
| 「'%s' のダウンロードに失敗しました: ファイルが存在しません。<br>SecondaryUpdate SourcePath を確認してください。」 | Sophos Anti-Virus は、プライマリアップデート元に接続できません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続き失敗する場合は、次の内容を確認してください。<br>SecondaryUpdate SourcePath が正しいことを確認してください。 | BAD-SECONDARY-URL |
| 「認証証明書が %s に見つかりませんでした」 | 検証証明書が存在しないため、Sophos Anti-Virus はアップデートしませんでした。<br>引き続きメッセージが表示される場合は、Sophos Anti-Virus をアンインストールしてから再インストールしてください。 | CERTIFICATE_NOT_FOUND |
| 「サーバー %s への接続がタイムアウトしました」 | 指定されたアドレスにあるアップデートサーバーに接続中、savupdate はタイムアウトしました。 | CONNECTION-TIMEOUT |
| 「アップグレード後」の Savupdate 制御スクリプトで、エラーが発生しました。エラーコード: %s」 | アップグレード後のカスタムスクリプトでエラーが発生しました。カスタムスクリプトを修正するか削除してください。Sophos Anti-Virus はアップデートされませんでした。 | CONTROL_SCRIPT<br>_AFTER_UPGRADE_ABORT |
| 「「アップグレード前」の Savupdate 制御スクリプトによって、アップグレードが中止されました。エラーコード: %s」 | アップグレード前のカスタムスクリプトでエラーが発生しました。カスタムスクリプトを修正するか削除してください。Sophos Anti-Virus はアップデートされませんでした。 | CONTROL_SCRIPT_<br>BEFORE_UPGRADE_ABORT |
| 「%s から複製することができませんでした。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、アップデートの設定を確認してください。 | FAILED-TO-UPDATE-FROM |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「マニフェストファイル '%s' の認証に失敗しました。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、次の操作を実行してください。<br>CID からアップデートしている場合は、アップデート元を再構築してください。<br>ソフォスからアップデートしている場合は、Sophos Anti-Virus を再インストールしてください。 | FAILED_VERIFY_MANIFEST |
| 「アップデートに失敗しました: %s のチェックサム (%s から取得) が無効です。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、次の操作を実行してください。<br>CID からアップデートしている場合は、アップデート元を再構築してください。<br>ソフォスからアップデートしている場合は、Sophos Anti-Virus を再インストールしてください。 | INVALID-CHECKSUM-FROM |
| 「キャッシュディレクトリ '%s' のコンテンツの認証に失敗しました。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、次の操作を実行してください。<br>CID からアップデートしている場合は、アップデート元を再構築してください。<br>ソフォスからアップデートしている場合は、Sophos Anti-Virus を再インストールしてください。 | MSG_COMPOUNDSINK<br>_VALIDATE_FAIL |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「Sophos Anti-Virus のアップデートに失敗しました。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、他のログメッセージを参照して、適切な対処を実行してください。 | MSG_RTC_UPDATE_FAIL |
| 「アップデートに失敗しました。有効な環境設定が見つかりませんでした。」 | Sophos Anti-Virus はアップデートできません。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、アップデートの設定を確認してください。 | NO_VALID<br>_CONFIGURATION_FOUND |
| 「プライマリアップデート元からのアップデートに失敗しました。セカンダリアップデート元に接続しています。」 | プライマリ設定を使用できなかったため、Sophos Anti-Virus はセカンダリ設定を使用してアップデートしました。<br>プライマリアップデート設定、およびプライマリサーバーを使用できるかを確認してください。 | SECONDARY-REPORT-AS-ERROR |
| 次のバージョンにアップデートしました - SAV: %s[エンジン: %s[データ: %s]」 | Sophos Anti-Virus はアップデートしました。<br>対処は必要はありません。 | UPDATED_TO_VERSION %s %s %s |
| 「%s のアップデート参照先で、適切な製品が見つかりませんでした。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、Sophos Anti-Virus を再インストールしてください。 | UPDATE_FAILURE<br>_PRODUCT_UNAVAILABLE |
| 「アップデート参照先の証明書チェーンが無効です。アップデート元アドレスは %s です。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、Sophos Anti-Virus を再インストールしてください。 | UPDATE_FAILURE_SDDS<br>_BAD_CERTIFICATE_CHAIN |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「アップデート参照先の証明書を認証できませんでした。アップデート元アドレスは %s です。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、Sophos Anti-Virus を再インストールしてください。 | UPDATE_FAILURE_SDDS<br>_SIGNING_ERROR |
| 「補助のアップデート参照先がが見つかりませんでした。アップデート元アドレスは %s です。」 | Sophos Anti-Virus はアップデートしませんでした。補助のアップデート参照先を見つけることができません。<br>設定を確認してください。 | UPDATE_FAILURE_SUPPLEMENT<br>_WAREHOUSE_UNAVAILABLE |
| 「次のバージョンをアップデート中です - SAV: %s[エンジン: %s[データ: %s]。」 | Sophos Anti-Virus はアップデートしています。<br>対処は必要はありません。 | UPDATING_FROM_VERSION |
| 「メイン環境設定を使用できません。バックアップ環境設定を使用します。」 | Sophos Anti-Virus は、バックアップ設定を使用してアップデートしました。プライマリアップデートの設定が正しく設定されていることを確認してください。 | USING_BACKUP<br>_CONFIGURATION |
| 「「%s」ポリシーを使用できません。代わりに「%s」ポリシーを使用します。」 | Sophos Anti-Virus は、アップデート参照先にない SDDS タグからアップデートする設定になっています。`PrimaryUpdatePolicy` が正しく設定されていることを確認してください。 | Unable to follow %s policy[following %s instead |
| 「パッケージディレクトリ '%s' のコンテンツの認証に失敗しました。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、Sophos Anti-Virus を再インストールしてください。 | VERIFICATION_FAILED |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「%s でシグネチャの検証が見つかりません。」 | Sophos Anti-Virus はアップデートしませんでした。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きアップデートに失敗する場合は、Sophos Anti-Virus を再インストールしてください。 | VERSIG_MISSING |
| 「magent (%s) は、次のシグナルを表示して予期せず終了しました: %s。」 | シグナルを受信したため magent は終了しました。sophosmgmtd は自動的に magent を再起動します。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きメッセージが表示される場合は、ソフォステクニカルサポートまでお問い合わせください。 | MAGENT-DIED-SIGNAL |
| 「magent (%s) は、エラー (%s) を表示して終了しました。」 | magent は予期せず終了しました。sophosmgmtd は自動的に magent を再起動します。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きメッセージが表示される場合は、ソフォステクニカルサポートまでお問い合わせください。 | MAGENT-EXIT-ERROR |
| 「mrouter (%s) は、次のシグナルを表示して予期せず終了しました: %s。」 | シグナルを受信したため mrouter は終了しました。sophosmgmtd は自動的に mrouter を再起動します。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きメッセージが表示される場合は、ソフォステクニカルサポートまでお問い合わせください。 | MROUTER-DIED-SIGNAL |
| 「mrouter (%s) は、エラー (%s) を表示して終了しました。」 | mrouter は予期せず終了しました。sophosmgmtd は自動的に mrouter を再起動します。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きメッセージが表示される場合は、ソフォステクニカルサポートまでお問い合わせください。 | MROUTER-EXIT-ERROR |

## 情報メッセージ

検索処理に関する情報が表示されます。

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「Sophos Anti-Virus デーモンが開始されました。」 | Sophos Anti-Virus が開始されました。 | SAVD-STARTED |
| 「Sophos Anti-Virus デーモンが停止されました。」 | Sophos Anti-Virus が停止されました。 | SAVD-STOPPED |
| 「SAV Interface を起動中、エラー %s が返されました: %s。」 | エラーが発生したため、Sophos Anti-Virus インターフェースが開きませんでした。 | SAVI_LOAD_ERROR |
| 「検索プロセッサが稼動しています。」 | Sophos Anti-Virus スキャナが稼働しています。 | SCANNER-RUNNING |
| 「検索プロセッサが停止されました。」 | Sophos Anti-Virus スキャナが停止しました。 | SCANNER-SHUTDOWN |
| 「次のシグナルにより検索プロセッサをシャットダウンします: %s。」 | シグナルを受信したため savscand は終了しました。sophosmgmtd は自動的に savscand を再起動します。<br>このメッセージが引き続き表示されない限り、対処は必要はありません。引き続きメッセージが表示される場合は、ソフォステクニカルサポートまでお問い合わせください。 | SCANNER-SHUTDOWN-WITH-SIGNAL |
| 「%s の駆除に失敗しました: 駆除の処理回数が多すぎます。」 | Sophos Anti-Virus オンデマンドスキャナはファイルを駆除しませんでした。<br>このファイルを削除してください。 | NOTIFY-ONDEMAND-MAX-DISINFECT-ERROR |
| 「%s を開けませんでした。」 | Sophos Anti-Virus オンデマンドスキャナはファイルを開くことができません。これは、ネットワークファイルなど、スキャナが開くことができないファイルを検索する場合に発生することがあります。そのようなファイルは未検索であることに注意してください。 | NOTIFY-ONDEMAND-OPEN-ERROR |

| Syslog メッセージ | 説明 | メッセージ ID |
|---|---|---|
| 「指定されたパス %s を検索できませんでした。」 | Sophos Anti-Virus スケジュール検索は、指定されたパスを検索できませんでした。スケジュール検索が正しく設定されていることを確認してください。 | NOTIFY-ONDEMAND-SPECIFIED-PATH-ERROR |
| 「オンデマンド検索の詳細: 検索マスターブートレコード数: %s[検索ブートレコード数: %s[検索ファイル数: %s[エラー数: %s[検出脅威数: %s、検出した感染ファイル数: %s。」 | Sophos Anti-Virus オンデマンド検索が終了しました。これは結果のサマリーです。 | SAVSCAN-DETAILS |
| 「オンデマンド検索が終了しました。」 | Sophos Anti-Virus オンデマンド検索が終了しました。 | SAVSCAN-FINISHED |
| 「オンデマンド検索が開始しました。」 | Sophos Anti-Virus オンデマンド検索が開始しました。 | SAVSCAN-START |
| 「スケジュール検索 ¥"%s¥" が開始しました」 | Sophos Anti-Virus スケジュール検索 が開始しました。 | SCHEDULED-SCAN-BEGIN |
| 「スケジュール検索 ¥"%s¥" の完了: 検索マスターブートレコード数: %s[検索ブートレコード数: %s[検索ファイル数: %s[エラー数: %s[検出脅威数: %s、検出した感染ファイル数: %s。」 | Sophos Anti-Virus スケジュール検索が終了しました。これは結果のサマリーです。 | SCHEDULED-SCAN-DETAILS |
| 「%s からの Sophos Anti-Virus Sophos Anti-Virus のアップデートに成功しました」 | Sophos Anti-Virus のアップデートに成功しました。 | SUCCESSFULLY_<br>UPDATED_FROM |

# 14 補足: アップデートの設定

**重要**
Sophos Enterprise Console を使用して 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。

## 14.1 用語の定義

### アップデートサーバー

アップデートサーバーは、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

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。アクセスするには認証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

コンピュータがプライマリアップデート元からアップデート版を取得できない場合に、代わりにアクセスする場所。アクセスするには認証情報が必要な場合があります。

## 14.2 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
```

## 14.3 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. 「**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。

## 14.4 アップデートサーバーにアクセスできない場合、直接ソフォスからアップデートするよう複数のアップデートクライアントを設定する

**注**
アップデートクライアント 1台の設定を変更する場合は、代わりにアップデートクライアント 1台がアップデートサーバーよりアップデートするよう設定する (p. 46)を参照してください。

アップデートサーバーで、CID にあるオフライン環境設定ファイルを更新して、その変更内容をライブ環境設定ファイルに適用すると、次回のアップデートからアップデートクライアントでダウンロードが実行されます。以下にある説明で、*offline-config-file-path* は、オフライン環境設定ファイルのパスです。また、*live-config-file-path* は、ライブ環境設定ファイルのパスです。

アップデートサーバーにアクセスできない場合、直接ソフォスからアップデートするよう複数のアップデートクライアントを設定する方法は次のとおりです。

1. SecondaryUpdateSourcePath パラメータを使用して、セカンダリアップデート元アドレスを `sophos:` に設定します。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 -c set
   SecondaryUpdateSourcePath 'sophos:'
   ```
2. SecondaryUpdateUsername パラメータを使用して、セカンダリアップデート元用ユーザー名に、使用許諾契約書にあるユーザー名を指定します。たとえば、次のように入力します。
   ```
   /opt/sophos-av/bin/savconfig -f オフライン環境設定ファイル -c set
   SecondaryUpdateUsername 'cust123'
   ```
3. SecondaryUpdatePassword パラメータを使用して、セカンダリアップデート元用パスワードに、使用許諾契約書にあるパスワードを指定します。たとえば、次のように入力します。
   ```
   /opt/sophos-av/bin/savconfig -f オフライン環境設定ファイル -c set
   SecondaryUpdatePassword 'j23rjjfwj'
   ```
4. プロキシ経由でインターネットにアクセスしている場合は、SecondaryUpdateProxyAddress、SecondaryUpdateProxyUsername および SecondaryUpdateProxyPassword 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ファイル -c set
   SecondaryUpdateProxyAddress 'http://www-cache.xyz.com:8080'
   /opt/sophos-av/bin/savconfig -f オフライン環境設定ファイル -c set
   SecondaryUpdateProxyUsername 'penelope'
   /opt/sophos-av/bin/savconfig -f オフライン環境設定ファイル -c set
   SecondaryUpdateProxyPassword 'fj202jrjf'
   ```

5. オフライン環境設定ファイルのパラー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のパス ライブ環境設定ファイルのパス

   たとえば次のように入力します。

   ```
   /opt/sophos-av/update/addextra /opt/sophos-av/OfflineConfig.cfg /opt/sophos-av/extrafiles/LiveConfig.cfg
   ```

# 14.5 アップデートクライアント 1台がアップデートサーバーよりアップデートするよう設定する

**注**
複数のアップデートクライアントの設定を変更する場合は、代わりに アップデートサーバーにアクセスできない場合、直接ソフォスからアップデートするよう複数のアップデートクライアントを設定する (p. 45)を参照してください。

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. プライマリ (またはセカンダリ) アップデート元を「自社サーバー」に設定するオプションを選択します。
   savsetup コマンドを入力後、アップデート元の詳細を入力する画面が表示されます。
3. 必要に応じ、アップデート元のアドレス、ユーザー名およびパスワードを入力します。
   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。

   savsetup プロキシ経由でアップデートサーバーにアクセスするかどうかを確認する画面が表示されます。
4. プロキシサーバーを使用している場合は、「Y」を押し、詳細を入力します。

# 15 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にしています。

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
```

# 16 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. 14)を参照してください。

## 16.1 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。

## 16.2 「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と、「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。

# 16.3 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。

# 16.4 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。詳細については、特定のディレクトリまたはファイルを検索する (p. 4) を参照してください。

# 16.5 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になります。

### 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。

## 16.6 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。

## 16.7 ウイルス フラグメントが報告される

### 現象

Sophos Anti-Virus でウイ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イ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。

- 新種ウイルスの多くは既知のウイルスをもとにしたものなので、既知ウイルスの典型的なコードの一部が新種ウイ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イルスが多いため、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、ウイルスの非アクティブな部分 (ウイ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イ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、最新のウイ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. 10)を参照)。
3. 依然としてウイ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 用語集

| | |
|---|---|
| セントラル インストール ディレクトリ (CID) | 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。 |
| 駆除 | 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。 |
| 追加ファイル | 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。 |
| オンデマンド検索 | ユーザー自身が開始する検索。オンデマンド検索機能で、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。 |
| プライマリアップデート元 | 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。 |
| スケジュール検索 | 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。 |
| セカンダリアップデート元 | 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。 |
| 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。 |
| 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。 |

# 18 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。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (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
- 製品ドキュメントのダウンロード。 www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合せ。https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

# 19 利用条件



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

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

## curl

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2014, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

## GNU General Public License

Some software programs are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or similar Free Software licenses which, among other rights, permit the user to copy, modify, and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires for any software licensed under the GPL, which is distributed to a user in an executable binary format, that the source code also be made available to those users. For any such software which is distributed along with this Sophos product, the source code is available by submitting a request to Sophos via email to savlinuxgpl@sophos.com. A copy of the GPL terms can be found at www.gnu.org/copyleft/gpl.html

## 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.

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.
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). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

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

This package is an SSL implementation written by Eric Young (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).

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)"

   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)"

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)

## 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

Original code by Lee Thomason (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

Mark Adler madler@alumni.caltech.edu

 

# 索引

## れ



## ろ



 