SOPHOS

Cybersecurity made simple.

Sophos Anti-Virus for Linux

環境設定ガイド

目次

(2020/07/20)

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 による管理型の Sophos Anti-Virus をインストールする場合は、Sophos Central にサインインして「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 による管理型の Sophos Anti-Virus をインストールする場合は、「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。

非管理型の Sophos Anti-Virus を、社内ネットワーク上の Linux コンピュータや、スタンドアロンの Linux コンピュータに、インストールまたはアンインストールする場合は、「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

Sophos Central による管理版インストール

Sophos Central の管理下にある 32ビット版の Linux サーバーを使用している場合は、「Sophos Anti-Virus for Linux スタートアップガイド」を参照してください。

Sophos Central の管理下にある 64ビット版の Linux サーバーを使用している場合は、「Sophos Anti-Virus for Linux 10 スタートアップガイド」を参照してください。

注意
このガイドに記載されている設定に関する情報は、Sophos Anti-Virus for Linux 10 にも適用されます。

2 Sophos Anti-Virus for Linux について

2.1 Sophos Anti-Virus for Linux とは

Sophos Anti-Virus for Linux 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のはもちろんのこと、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、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。単一のファイルから、ユーザーが読み取り権限を持つコンピュータ上のすべてのファイルにいたるまで、さまざまな項目に対して検索を実行できます。オンデマンド検索は、手動で実行することも、スケジュール設定した日時に実行することもできます。

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。単一のファイルから、ユーザーが読み取り権限を持つコンピュータ上のすべてのファイルにいたるまで、さまざまな項目に対して検索を実行できます。オンデマンド検索は、手動で実行することも、スケジュール設定した日時に実行することもできます。

2.3 Sophos Anti-Virus の使用方法

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 for Linux の設定内容

Sophos Anti-Virus for Linux の設定内容は、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。

Sophos 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 Sophos Enterprise Console または Sophos Central の管理下にある場合は、次のように Sophos Anti-Virus for Linux 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 の 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 の管理下にある 64ビット版の Linux サーバーを使用している場合は、「Sophos Anti-Virus for Linux バージョン 10 スタートアップガイド」を参照してください。

- 各 Linux コンピュータで Sophos Anti-Virus for Linux の CLI を使用して、オンデマンド検索を設定する。

Sophos Enterprise Console または Sophos Central の管理下にないネットワーク上のコンピュータ

Sophos Enterprise Console または Sophos Central の管理下にないネットワーク上の Linux コンピュータは、各コンピュータで Sophos Anti-Virus for Linux の CLI を使用してオンデマンド検索をローカル設定します。

Sophos Enterprise Console または Sophos Central の管理下にないスタンドアロンコンピュータ

Sophos Enterprise Console や Sophos Central の管理下にない 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 for Linux 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、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、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。

オンアクセス検索はデフォルトで有効になっています。必要に応じてオンアクセス検索の状態を確認し、無効になっている場合は開始することができます。

注
ここで説明するコマンドを使うには、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 for Linux をインストールしていることを前提に書かれています。この前提に該当しない場合は、お使いのインストールディレクトリに置き換えてコマンドを実行してください。

3.1 オンアクセス検索が有効になっていることの確認

- 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の確認

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 と共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 オンアクセス検索の開始

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 オンアクセス検索の停止

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。単一のファイルから、ユーザーが読み取り権限を持つコンピュータ上のすべてのファイルにいたるまで、さまざまな項目に対して検索を実行できます。オンデマンド検索は、手動で実行することも、スケジュール設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。

4.1 オンデマンド検索の実行

オンデマンド検索を実行するコマンドは、savscan です。

4.1.1 コンピュータの検索

- 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 /

注
また、Sophos Enterprise Console を使用して、1台または複数台のコンピュータに対してシステムのフル検索を実行することもできます。詳細は、Sophos Enterprise Console のヘルプを参照してください。

4.1.2 特定のディレクトリやファイルの検索

- 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 ファイルシステムの検索

- 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 ブートセクタの検索

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 オンデマンド検索の設定

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の検索

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。Sophos Anti-Virus で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。

4.2.2 特定の種類のファイルの検索

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。Sophos Anti-Virus で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の検索

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の検索

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。

4.2.5 リモートコンピュータの検索

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の無効化

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。

4.2.7 ブートファイルシステムのみを検索

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の設定

-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 Sophos Anti-Virus 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の検索

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。

5 ウイルスが検出された場合の動作

オンアクセス検索、オンデマンド検索にかかわらず、Sophos Anti-Virus でウイルスが検出されると、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. 15)を参照)。
- Sophos Enterprise Console の管理下にある場合、Sophos Enterprise Console に警告を送信する。
- root@localhost にメール警告が送信される。

また、オンアクセス検索、オンデマンド検索のどちらでウイルスが検出されたかによって、デフォルトで、Sophos Anti-Virus に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. 12)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。
```

6 ウイルスのクリーンアップ

6.1 クリーンアップ情報の入手

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 感染ファイルの隔離

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 (感染ファイルのクリーンアップ (p. 13)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 隔離の設定

- 隔離を設定するには、--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とパーミッションの設定

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、次のようになります。

savscan fred --quarantine:user=virus,group=virus,mode=0400 と入力すると、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 感染ファイルのクリーンアップ

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の駆除

- 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の入手 (p. 12)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の駆除

- 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の入手 (p. 12)を参照してください。)

6.3.3 特定の感染ファイルの削除

- 特定の感染ファイルを削除するには、-remove 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 -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の削除

- 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 感染ブートセクタの駆除

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の復旧

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。

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 の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

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。

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の変更 (p. 31)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 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
Sophos 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 Sophos 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

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 標準入力からのスケジュール検索の追加

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、Sophos Anti-Virus 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のファイル出力

- 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名のファイル出力

- Sophos Anti-Virus で設定されているすべてのスケジュール検索 (Sophos 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
Sophos 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の標準出力

- 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名の標準出力

- Sophos Anti-Virus で設定されているすべてのスケジュール検索 (Sophos 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
Sophos 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

注
Sophos 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のファイル出力 (p. 19) 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

注
Sophos 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、Sophos Anti-Virus 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. 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、およびその他のオプションを設定します。/opt/sophos-av/doc/namedscan.example.en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 スケジュール検索のログの表示

- 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」とうい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 スケジュール検索の削除

注
Sophos 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の削除

注
Sophos 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: 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 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 Anti-Virus では、ウイルスを検出したときや、検索エラーやその他のエラーが発生したときに警告が送信されるよう設定することができます。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・ポップアップ警告の設定

11.1.1 デスクトップ・ポップアップ警告の無効化

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の指定

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で表示されます。

- 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 'システム管理者に問い合わせてください'

11.2 コマンドライン警告の設定

11.2.1 コマンドラインの警告の無効化

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の指定

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で表示されます。

- 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 'システム管理者に問い合わせてください'

11.3 メール警告の設定

11.3.1 メール警告の無効化

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 アドレスの指定

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 言語の指定

警告メッセージ本文は、デフォルトで英語表記です。

- 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 メール受信者の指定

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) の設定

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) の設定

- 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の指定

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 'IT 部門にお問い合わせください。'

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の指定

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 SendErrorEmail 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 'IT 部門にお問い合わせください。'

11.3.9 オンデマンド検索のメール警告の無効化

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の指定

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 'IT 部門にお問い合わせください。'

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 Sophos 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、検索のアクティビティは 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: 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、Sophos 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 Sophos Enterprise Console のヘルプを参照してください。

13.1 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ているコンピュータです。他のコンピュータのアップデート元としては使用する必要はありません。

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。

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の確認

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の設定

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 がインストールされているコンピュータを使用します。

注
アップデートするクライアントに 64ビットのコンピュータが含まれる場合、アップデートサーバーは 64ビットである必要があります。アップデートサーバーが 32ビットの場合、64ビットのアップデート版はダウンロードされないため、64ビットのクライアントがアップデートされません。

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) 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。

   b) 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 1台のアップデートクライアントをアップデートサーバーからアップデートするように設定

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方法は次のとおりです。

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. 「**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. 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。
4. 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。
5. 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。

14 補足: 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 Sophos 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。

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 の設定の確認

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 の有効/無効の切り替え

- 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 補足: 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 Sophos 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。

15.1 オンアクセス検索のファイル割り込み方法の変更

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 ファイルとディレクトリの検索除外

ファイルとディレクトリを除外する方法には次の 2とおりあります。

- 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コードの指定 (p. 32)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の使用

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 Sophos 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。

- 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
  a) /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の使用

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 Sophos 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。

- 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コードの指定

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 ファイルシステムの種類の検索除外

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の検索

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 感染ファイルのクリーンアップ

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 の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 は最初にファイルを駆除しようと試みます。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の駆除

- 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の入手 (p. 12)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 感染ファイルの削除

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があります。

- 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 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. 41)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 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

16.3 「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。

16.4 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、Sophos Anti-Virus の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。

16.5 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。詳細については、特定のディレクトリやファイルの検索 (p. 6) を参照してください。

16.6 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。

16.7 ウイルスがクリーンアップされない

現象

- Sophos Anti-Virus でウイルスのクリーンアップが実行されない。
- 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。

- 検出されたウイルスが 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。

16.8 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の駆除 (p. 13)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。

16.9 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、ディスクをコンピュータから取り出してください。

17 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

17.1 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

18 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

19 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 に追加します。

20 用語集

ブートセクタ感染型ウイルス

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。

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。

オンアクセス検索

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。

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。アクセスするには認証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。アクセスするには認証情報が必要な場合があります。

Sophos Live Protection

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 がインストールされており、他のコンピュータのアップデート元ではないコンピュータ。

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。

21 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わせ。https://secure2.sophos.com/ja-jp/support/open-a-support-case.aspx

22 利用条件

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

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

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

libcap

Unless otherwise *explicitly* stated, the following text describes the licensed conditions under which the contents of this libcap release may be used and distributed:

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

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.
2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License (v2.0 - see below), in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED "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(S) 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.

OpenSSL

OpenSSL copyright

LICENSE ISSUES

==========

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 © 1998–2017 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 (C) 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 Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared 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

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 rouines 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 licence 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 licence [including the GNU Public Licence.]

protobuf

This license applies to all parts of Protocol Buffers except the following:

- Atomicops support for generic gcc, located in src/google/protobuf/stubs/atomicops_internals_generic_gcc.h. This file is copyrighted by Red Hat Inc.

- Atomicops support for AIX/POWER, located in src/google/protobuf/stubs/atomicops_internals_power.h. This file is copyrighted by Bloomberg Finance LP.

Copyright 2014, 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)

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

Copyright (C) 1995-2017 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 Mark Adler

jloup@gzip.org madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://tools.ietf.org/html/rfc1950 (zlib format), rfc1951 (deflate format) and rfc1952 (gzip format).

