Symantec™ Endpoint Protection 14.3 RU3 for Linux クライアント ガイド - Japanese - Japan

September 2021

Table of Contents

著作権に関する声明

Broadcom、パルスロゴ、Connecting everything、および Symantec は、Broadcom の商標です。

Copyright ©2021 Broadcom. All Rights Reserved.

「Broadcom」または「ブロードコム」という用語は、Broadcom Inc. またはその関連会社を示します。詳しくは、www.broadcom.com を参照してください。

Broadcom は、品質、機能、設計を改善するため、ここに記載された製品やデータを予告なく変更する権利を留保します。Broadcom は、提供する情報の正確さと信頼性に細心の注意を払っています。ただし、Broadcom はこの情報の適用または使用、もしくはここに記載された製品や回路の適用または使用から生じる一切の責任を負わないものとし、また特許権やその他の権利に対するライセンスを付与しません。

Symantec Endpoint Protection での Linux デバイスの保護

Symantec Agent for Linux について

Symantec Agent for Linux は、マルウェアの脅威、リスク、脆弱性から Linux デバイスを保護します。Linux デバイスを既知や未知のマルウェアからプロアクティブに保護します。

マルウェア対策機能は、ウイルス、スパイウェア、ランサムウェアなどの悪質なソフトウェアから Linux デバイスを保護するマルウェア対策（AMD）と、アプリケーションの起動時に悪質な脅威を検出する **Auto-Protect**（AP）で構成されます。

シマンテック社では、リアルタイム保護を確実に行うために、Auto-Protect を有効にすることを推奨しています。検出されたマルウェアはいずれもすぐに検疫されます。Auto-Protect を無効にした場合でも、オンデマンド スキャンを使ってマルウェアを検出できます。

Linux エージェントを始めましょう

Symantec Agent for Linux のシステム必要条件

このセクションでは、最新バージョンのシステム要件を説明します。

Symantec Endpoint Protection の以前のバージョンのシステム要件や、これらのシステム要件の最新版については、次の Web ページを参照してください。

Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件

Table 1: Symantec Agent for Linux のシステム必要条件

コンポーネント	必要条件
ハードウェア	• Intel Pentium 4 (2 GHz) 以上のプロセッサ • 500 MB の空き RAM（4 GB の RAM を推奨） • `/var`、`/opt`、および `/tmp` が同じファイルシステム/ボリュームを共有する場合、2 GB のディスク空き容量 • 異なるボリュームにある場合、各 `/var`、`/opt`、および `/tmp` に 500 MB のディスク空き容量
オペレーティングシステム	• Amazon Linux 2 • CentOS 6、7、8 • Debian 9、10 • Oracle Enterprise Linux 6、7、8 • Red Hat Enterprise Linux 6、7、8 • SuSE Linux Enterprise Server 12.x、15.x • Ubuntu 14.04 LTS、16.04 LTS、18.04 LTS、20.04 LTS サポート対象のオペレーティングシステムカーネルのリストについては、「Symantec Endpoint Protection でサポートされる Linux のカーネル」を参照してください。
その他の環境条件	• Glibc 2.6 より前の glibc を実行するオペレーティングシステムはサポートされません。 • net-tools または iproute2 Symantec Endpoint Protection は、コンピュータの既存のインストール内容に応じて、次の 2 つのツールのうちのいずれかを使います。 • OpenSSL 1.0.2k-fips 以降

Symantec Linux エージェントまたは Linux 用 Symantec Endpoint Protection クライアントのインストール

(14.3 RU1 以降の場合)

Linux デバイスに Symantec Linux エージェントを直接インストールします。Linux エージェントを Symantec Endpoint Protection Manager からリモートで配備することはできません。

Symantec Linux エージェントをインストールするには、Symantec Endpoint Protection Manager でインストール パッケージを作成し、インストール パッケージを Linux デバイスに転送してから、インストーラを実行します。インストーラは、新しいエージェントを設定し、それを Symantec Endpoint Protection Manager に登録します。

> **NOTE**
> Symantec Linux エージェント 14.3 RU1 以降は、管理外クライアントとして実行できません。すべての管理タスクは、Symantec Endpoint Protection Manager またはクラウド コンソールで実行する必要があります。

14.3 RU1 以降の場合： **Symantec Linux** エージェントをインストールする方法

1. Symantec Endpoint Protection Manager で、インストールパッケージを作成してダウンロードします。
2. ネットワーク共有、USB デバイス、または他の共有できる場所にパッケージを配置します。
   Linux エージェントをインストールするデバイスが隔離されたネットワークにあるか、インターネットにアクセスできない場合は、ローカル リポジトリを設定します。次のサイトを参照してください。
   ローカル リポジトリの作成
3. 以下のいずれかの方法で Linux エージェントをインストールします。

パッケージを Linux デバイスに転送した場合	1. フォルダの場所に移動し、以下のコマンドを実行して **LinuxInstaller** ファイルを実行可能にします。
	`chmod u+x LinuxInstaller`
	2. 以下のコマンドを実行してエージェントをインストールします。
	`./LinuxInstaller`

ローカル リポジトリを設定した場合	1. 以下のコマンドを実行します。
	`./LinuxInstaller – --local-repo <LOCAL Repository URL>`
	次に例を示します。
	`./LinuxInstaller – --local-repo https://your-domain.com/sep_linux_agent/14_3RU3`

   root としてコマンドを実行する必要があります。
   インストールオプションのリストを表示するには、`./LinuxInstaller -h` を実行します。
4. インストールを検証するには、`/usr/lib/symantec` に移動し、`./status.sh` を実行して、モジュールがロード済みでデーモンが実行されていることを確認します。

```
./status.sh
Symantec Agent for Linux Version: 14.3.450.1000
Checking Symantec Agent for Linux (SEPM) status..
Daemon status:
cafagent running
sisamdagent running
sisidsagent running
sisipsagent running
Module status:
sisevt loaded
sisap loaded
```

`communication status` はクラウド管理のクライアントでのみ利用可能です。

14.3 MP1 以前の場合

管理外または管理下の Symantec Endpoint Protection クライアントを直接 Linux コンピュータにインストールします。Linux クライアントを Symantec Endpoint Protection Manager からリモートで配備することはできません。インストールの手順は、クライアントが対象外または対象下に関係なくほぼ同じです。

管理下クライアントは、Symantec Endpoint Protection Manager で作成するインストールパッケージを使ってのみインストールできます。管理外クライアントは、クライアント/サーバーの通信設定を Linux クライアントにインポートすることでいつでも管理下クライアントに変換できます。

Linux オペレーティングシステムのカーネルがコンパイル済み自動保護カーネルモジュールと互換性がない場合、インストーラは互換性のある自動保護カーネルモジュールのコンパイルを試みます。自動コンパイルプロセスは、必要に応じて自動的に起動します。ただし、インストーラは互換性のある自動保護カーネルモジュールをコンパイルできないことがあります。その場合、自動保護はインストールされますが、無効になります。 詳細については、次を参照してください。

Symantec Endpoint Protection でサポートされる Linux のカーネル

NOTE

Linux コンピュータで Symantec Endpoint Protection クライアントをインストールするにはスーパーユーザーの権限が必要です。この手順では、`sudo` を使って権限の昇格を説明します。

14.3 MP1 以前の場合： **Linux** 用 **Symantec Endpoint Protection** クライアントをインストールする方法

1. 作成したインストールパッケージを Linux コンピュータにコピーします。パッケージは .zip ファイルです。
2. Linux コンピュータで、ターミナルアプリケーションウィンドウを開きます。
3. 次のコマンドを使ってインストールディレクトリに移動します。

   ```
   cd /directory/
   ```

   ここで、 directory は .zip ファイルをコピーしたディレクトの名前です。
4. 次のコマンドを使って、.zip ファイルの内容を `tmp` というディレクトリに抽出します。

   ```
   unzip "InstallPackage" -d sepfiles
   ```

   ここで、`InstallPackage` は .zip ファイルの完全名、`sepfiles` は抽出処理によりインストールファイルが配置されるデスティネーションフォルダを表します。

   デスティネーションフォルダが存在しない場合は、抽出処理によって作成されます。
5. 次のコマンドを使って `sepfiles` に移動します。

   ```
   cd sepfiles
   ```
6. `install.sh` の実行ファイルの権限を正しく設定するには、次のコマンドを使います。

   ```
   chmod u+x install.sh
   ```
7. 次のコマンドで、組み込みスクリプトを使って Symantec Endpoint Protection をインストールします。

   ```
   sudo ./install.sh -i
   ```

   パスワードの入力を求めるメッセージが表示されたらパスワードを入力します。

   このスクリプトは Symantec Endpoint Protection コンポーネントのインストールを開始します。デフォルトのインストールディレクトリは次のとおりです:

   ```
   /opt/Symantec/symantec_antivirus
   ```

   ライブアップデートのデフォルトの作業ディレクトリは次のとおりです。

   ```
   /opt/Symantec/LiveUpdate/tmp
   ```

   コマンドプロンプトが返されるとインストールの完了です。インストールを完了するためにコンピュータを再起動する必要はありません。

14.3 MP1 以前の場合

クライアントインストールを検証するには、Symantec Endpoint Protection の黄色のシールドをクリックまたは右クリックし、[**Symantec Endpoint Protection** を開く] をクリックします。黄色のシールドの位置は Linux のバージョンによって異なります。クライアントユーザーインターフェースにプログラムバージョン、ウイルス定義、サーバー接続状態、管理に関する情報が表示されます。

詳しい情報

- Symantec Endpoint Protection for Linux クライアントの自動コンパイルについて
- Linux クライアントの GUI について
- Linux クライアントへのクライアントとサーバーの通信設定のインポート
- クライアントインストールの準備
- Redhat ベースのディストリビューションの Symantec Endpoint Protection 14.x のインストール

Linux エージェントを始めましょう

Symantec Endpoint Protection Manager 管理者によって Linux エージェントの設定が許可されていることがあります。

Table 2: Linux エージェントを開始する手順 (14.3 **RU1** 以降の場合)

手順	タスク	説明
1	Symantec Agent for Linux をインストールします。	管理者から管理下クライアント用のインストールパッケージが提供されるか、インストールパッケージをダウンロードするためのリンクが電子メールで送信されます。次のサイトを参照してください。 Symantec Linux エージェントまたは Linux 用 Symantec Endpoint Protection クライアントのインストール
2	Linux エージェントが Symantec Endpoint Protection Manager またはクラウドコンソールと通信していることを確認します。	Symantec Endpoint Protection Manager またはクラウドコンソールとの接続を確認するには、以下のコマンドを実行します。 `/usr/lib/symantec/status.sh`
手順 3	Auto-Protect が動作していることを確認します。	Auto-Protect の状態を確認するには、次のコマンドを実行します。 `cat /proc/sisap/status`
手順 4	定義が最新であることを確認します。	LiveUpdate 定義は次の場所にあります。 `/opt/Symantec/sdcssagent/AMD/sef/definitions/`

Table 3: Linux クライアントを開始する手順 (14.3 MP1 以前)

手順	タスク	説明
1	Linux クライアントをインストールします。	Symantec Endpoint Protection Manager 管理者から管理下クライアント用のインストールパッケージが提供されるか、インストールパッケージをダウンロードするためのリンクが電子メールで送信されます。 Symantec Endpoint Protection Manager と通信しない管理外クライアントをアンインストールすることもできます。一次コンピュータのユーザーは、クライアントコンピュータの管理、ソフトウェアの更新、定義の更新を行う必要があります。管理外クライアントを管理下クライアントに変換できます。次のサイトを参照してください。 Symantec Linux エージェントまたは Linux 用 Symantec Endpoint Protection クライアントのインストール
2	Linux クライアントが Symantec Endpoint Protection Manager と通信していることを確認します。	Symantec Endpoint Protection のシールドをダブルクリックします。クライアントが Symantec Endpoint Protection Manager と正常に通信している場合は、 [管理] の [サーバー] の横にサーバー情報が表示されます。 [オフライン] と表示される場合は、Symantec Endpoint Protection Manager 管理者に連絡してください。 [自己管理] と表示される場合は、クライアントが管理外です。 シールドアイコンは管理状態と通信状態を両方とも示します。
手順 3	Auto-Protect が動作していることを確認します。	Symantec Endpoint Protection のシールドをダブルクリックします。 [状態] の [自動保護] の横に Auto-Protect の状態が表示されます。 次のコマンドラインインターフェースで Auto-Protect の状態を確認することもできます。 `sav info -a`
手順 4	定義が最新であることを確認します。	インストールが完了すると、LiveUpdate が自動的に起動します。Symantec Endpoint Protection シールドをダブルクリックしたときに、定義が更新されていることを確認できます。 [定義] に定義日が表示されます。デフォルトでは、LiveUpdate for the Linux クライアントは 4 時間おきに実行されます。 定義が最新でない可能性がある場合は、 [LiveUpdate] をクリックして LiveUpdate manually を手動で実行できます。次のコマンドラインインターフェースを使って LiveUpdate を実行することもできます。 `sav liveupdate -u`
手順 5	スキャンを実行します。	デフォルトでは、管理下の Linux クライアントは、毎日午前 12 時 30 分にすべてのファイルとフォルダをスキャンします。ただし、以下のコマンドラインインターフェースを使って手動スキャンを開始できます。 sav manualscan -s <パス名> **Note:** 手動スキャンを開始するコマンドを実行するには、スーパーユーザーの権限が必要です。

詳しい情報

Symantec Endpoint Protection for Linux によく寄せられる質問 (SEP for Linux FAQ)

Symantec Linux エージェントのアップグレード

(14.3 RU1 以降の場合)

バージョン 14.3 RU1 以降では、Linux クライアント インストーラは、レガシー Linux クライアント (14.3 RU1 より前) を検出してアンインストールし、新規インストールを実行します。古い設定は保持されません。

Symantec Linux エージェントをアップグレードする方法

1. Symantec Endpoint Protection Manager で、インストールパッケージを作成してダウンロードします。
   クライアントインストールパッケージのエクスポート

2. ダウンロードしたパッケージを Linux デバイスにコピーします。
3. フォルダの場所に移動し、以下のコマンドを実行して **LinuxInstaller** ファイルを実行可能にします。

   ```
   chmod u+x LinuxInstaller
   ```

4. 以下のコマンドを実行して、既存のエージェントをアンインストールし、Symantec Linux エージェントを再インストールします。

   ```
   ./LinuxInstaller
   ```

   root としてコマンドを実行します。

5. インストールを検証するには、`/usr/lib/symantec` に移動し、`./status.sh` スクリプトを実行して、モジュールがロード済みでデーモンが実行されていることを確認します。

   ```
   ./status.sh
   Symantec Agent for Linux Version: 14.3.450.1000
   Checking Symantec Agent for Linux (SEPM) status..
   Daemon status:
   cafagent running
   sisamdagent running
   sisidsagent running
   sisipsagent running
   Module status:
   sisevt loaded
   sisap loaded
   ```

Symantec Linux エージェントのカーネル モジュールの更新

Symantec Linux エージェントは、Symantec Endpoint Protection Manager から管理する場合、またはクラウド コンソールから管理する場合も、同じクライアントです。

(14.3 RU1 以降の場合)

新しい Linux カーネルの更新がリリースされるたびに、新しいカーネルをサポートするために、そのプラットフォームの Symantec Linux エージェントを更新する必要があります。プロセスをより効率化するために、Linux エージェントのカーネル モジュールを Linux リポジトリを使用して更新できるようになりました。

> **NOTE**
> エージェントがシマンテック リポジトリ サーバ (https://linux-repo.us.securitycloud.symantec.com/) に接続してカーネル モジュールの更新をダウンロードできることを確認してください。

RHEL、Amazon Linux、Oracle Linux、または CentOS システムで `yum update` コマンドを実行するたびに、このコマンドは新しいエージェント パッケージも検索します。更新が利用可能な場合は、最新のカーネル モジュールがダウンロードされ、エージェントは自動的に更新されます。カーネル モジュールが更新された後、更新を有効にするためにインスタンスを再起動する必要があります。

または、インスタンスで以下のコマンドを実行して、エージェントのカーネル モジュールを更新できます。root 権限でターミナル ウィンドウを開き、`/usr/lib/symantec/` に移動し、以下のコマンドを実行します。

```
/usr/lib/symantec/installagent.sh --update-kmod
```

Ubuntu システム上のカーネル モジュールを更新する方法

1. ローカル パッケージ データベースをリフレッシュおよび更新するには、以下のコマンドを入力します。
   ```
   sudo apt-get clean
   sudo apt-get update
   ```
2. 最新のカーネル モジュールにアップグレードするには、以下のコマンドを入力します。
   ```
   /usr/lib/symantec/installagent.sh --update-kmod
   ```
   このアクションを実行するにはスーパーユーザ権限が必要です。

インターネット接続がない制限された環境でカーネル モジュールを更新する方法

1. 方法 1： 最新の KMOD パッケージをインターネット接続がないシステムに手動で転送し、LinuxInstaller に KMOD パッケージを適用して、LinuxInstaller を実行します。
   1. インターネットに接続されているシステムで、KMOD パッケージをダウンロードします。
      `./LinuxInstaller -d`
   2. アップグレードするエージェントに KMOD パッケージを手動でコピーして貼り付けます。
   3. 適用されたパッケージをリスト表示します。
      `./LinuxInstaller -l`
   4. LinuxInstaller に新しい KMOD パッケージを適用します。
      `tar czf - [KMOD-package-name] >> LinuxInstaller`
   5. 新しい KMOD パッケージが適用されたパッケージのリストに含まれていることを確認します。
      `./LinuxInstaller -l`
   6. インストーラを実行して、カーネル モジュールを更新します。
      `./LinuxInstaller -- --update-kmod`
2. 方法 2： ローカル リポジトリを設定し、エージェントがデフォルトのシマンテック リポジトリの代わりにローカル リポジトリを使用するようにレポジトリ設定を編集します。
   1. KMOD パッケージをホストするローカル リポジトリを設定します。
      ローカル リポジトリを作成する方法の詳細については、使用している各 Linux 配布のマニュアルを参照してください。
   2. クライアント コンピュータで、以下のコマンドを実行して、ローカル リポジトリを使用するようにリダイレクトします。
      `./LinuxInstaller --local-repo<localrepo_url>`
      URL の例： `--local-repo 'http://<repo_ip_or_hostname:<port_optional>/sep_linux'`
   3. KMOD を更新するには、以下を実行します。
      `./LinuxInstaller -- --update-kmod`

オペレーティング システムのカーネル モジュールを更新する場合は、Symantec Endpoint Protection クライアントの対応するカーネル モジュールの更新も更新する必要があります。互換性のあるカーネル モジュールがない場合、Symantec Endpoint Protection クライアントが正しく動作せず、一部の機能が無効になる可能性があります。

詳しい情報

Symantec Linux エージェントのインストール パッケージの作成とインストール

コマンド ライン ツール (sav) を使用した **Linux** クライアントの管理

Linux クライアント コマンド ライン ツールを使って、Linux クライアントを制御して確認できます。

コマンド ライン ツールを使用して Linux クライアントを管理するには、以下を参照してください。

(14.3 RU2 以降の場合)

Linux クライアント コマンド ライン ツールを使って、Linux クライアントを制御して確認できます。

コマンド ライン ツールを使用して **Linux** クライアントを管理する方法

1. Linux クライアント コンピュータで、以下の場所に移動します。
   `/opt/Symantec/sdcssagent/AMD/tools`
2. 以下のように sav コマンドを実行します。
   `./sav [options] command`

Table 4: sav のオプション

オプション	説明	適用先
`-q`	静的	14.3 RU2 現在
`-h`	sav の利用可能なオプションとコマンドを表示します。	14.3 RU2 現在

Table 5: sav のコマンド

オプション	説明	適用先
`autoprotect -e`	Auto-Protect を有効にします。 Auto-Protect の状態を確認するには、以下のコマンドを実行します。 `[root@localhost tools]# cat /proc/sisap/status | grep -i MODE` 応答は以下のいずれかになります。 • `mode=ENA`（有効な場合） • `mode=DIS`（無効な場合）	14.3 RU2 現在
`autoprotect -d`	Auto-Protect を無効にします。	14.3 RU2 現在
`info -d`	デバイスで使用中の現在のウイルス定義とセキュリティ リスク定義のバージョンと日付を表示します。	14.3 RU3 以降
`info -e`	デバイスで使用中のスキャン エンジンのバージョンを表示します。	14.3 RU3 以降
`info -p`	デバイスで使用中の Symantec Agent のバージョンを表示します。	14.3 RU3 以降
`info -a`	デバイスの Auto-Protect の状態を表示します。	14.3 RU3 以降
`liveupdate -u`	LiveUpdate をすぐに実行します。	14.3 RU3 以降
`manage -i <file>`	*sylink.xml* ファイルを指定された場所にインポートします。	14.3 RU2 現在
`manualscan -s <### ### ###>`	手動スキャンを開始します。 <ファイル リスト> には、スキャンするファイルとディレクトリのリストを指定します。 このリストを指定するには、ファイルとディレクトリのリストを改行で区切って入力します。最後に CTRL-D のようなファイルの終わりを示す信号でリストを終了します。ディレクトリが指定されると、すべてのサブディレクトリもスキャンされます。ワイルドカード文字はサポートされます。 デフォルトでは、コマンド ライン インターフェースから開始される手動スキャンに追加できる項目の最大数は 100 です。**symcfg** を使用すると、VirusProtect6MaxInput の DWORD 値を変更して、この上限を増やすことができます。制限を完全に削除するには、VirusProtect6MaxInput の値を 0 に設定します。 ファイルのリストやディレクトリの代わりにハイフン（-）を指定した場合には、パス名のリストは標準入力から読み込まれます。改行で区切ったファイルまたはパス名のリストを生成するコマンドを使えます。非常に長い項目リストをこのコマンドに送信するとパフォーマンスが低下する可能性があります。シマンテック社は最大で数千項目にリストを制限することを推奨します。	14.3 RU3 以降
`manualscan -t`	進行中の手動スキャンを中止します。	14.3 RU3 以降

詳しい情報

Symantec Linux エージェントのトラブルシューティング

Symantec Linux エージェントのトラブルシューティング

以下の表に、Symantec Linux エージェント（14.3 RU1 以降）のトラブルシューティングに関するリソースを示します。

Table 6: Symantec Linux エージェントのトラブルシューティング方法

処理	説明
エージェントの状態の確認。	エージェントのバージョンおよび接続状態をチェックし、モジュールがロード済みでデーモンが実行されていることを確認するには、`/usr/lib/symantec` に移動し、以下のコマンドを実行します。 `./status.sh`
エージェントパッケージのバージョンの確認。	`/usr/lib/symantec` に移動し、以下のコマンドを実行します。 `./version.sh`

ログの表示。	Symantec Linux エージェントのログは、以下の場所で確認できます。
	• AMD ログ - スキャンに関連する情報を提供します。
	`/var/log/sdcsslog/amdlog`
	• CAF ログ - サーバーとの通信、登録、コマンド、イベントなど、エージェントの活動に関連する情報を提供します。
	`/var/log/sdcss-caflog/`
	• エージェントログ - エージェントの活動に関連する情報を提供します。
	`/var/log/sdcsslog/SISIDSEvents*.csv`
	• CVE ログ - Symantec Endpoint Protection Manager とエージェントの間の通信に関連する情報を提供します。
	`/var/log/sdcss-caflog/cve.log`

ログを zip ファイルに収集。	`GetAgentInfo` スクリプトを使用して、すべてのログファイルを ZIP ファイルに収集し、カスタマサポートに送信できます。 1. Symantec Linux エージェント システムにログインします。 2. `/opt/Symantec/sdcssagent/IPS/tools/` に移動します。 3. root として `./getagentinfo.sh` を実行します。 4. `/tmp/` ディレクトリに ZIP ファイルが作成されます。 ファイル名は `20201208_184935_0001_CU_mihsan-rhel8.zip` のようになります。 `-out <directory>` を指定して、生成される ZIP ファイルの場所と名前を変更できます。
CVE ログレベルの変更。	デフォルトでは、CVE のログレベルは `info` です。 `/opt/Symantec/cafagent/bin/log4j.properties` ファイルで、ログ記録レベルを `debug` に変更できます。 ファイルを変更した後に、`cafagent` サービスを再起動する必要があります。

AMD ログレベルの変更。	デフォルトでは、AMD のログレベルは `info` です。
	`/opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini` ファイルで、ログレベルを `trace`、`warning`、または `error` に変更できます。
	Note: AntiMalware.ini ファイルを修正する前に、sisamdagent を停止します。
	`service sisamdagent stop`
	Note: ファイルを変更したら、サービスを再起動します。
	`service sisamdagent start`

Symantec Linux エージェントまたは Linux 用 Symantec Endpoint Protection クライアントのアンインストール

インストール時に取得したスクリプトとともに Symantec Endpoint Protection for Linux クライアントをアンインストールします。

NOTE

Linux コンピュータの Symantec Endpoint Protection クライアントをアンインストールするにはスーパーユーザー権限が必要です。この手順では、`sudo` を使って権限の昇格を説明します。

14.3 RU1 以降の場合： **Symantec Linux** エージェントをアンインストールする方法

1. Linux コンピュータで、ターミナルアプリケーションウィンドウを開きます。
2. 以下のディレクトリに移動します。
   `/usr/lib/symantec/`
3. 以下の組み込みスクリプトを実行して、Symantec Agent for Linux をアンインストールします。
   `./uninstall.sh`
4. アンインストールが完了して再起動プロンプトが表示されたら、コンピュータを再起動します。
   `uninstall.sh` スクリプトを実行すると、Symantec Agent for Linux のすべてのコンポーネント (`sdcss-caf`、`sdcss-sepagent`、および `sdcss-kmod`) が削除されます。

```
[root@localhost symantec]# ./uninstall.sh
Running ./uninstall.sh (PWD /usr/lib/symantec; version 2.2.4.41)
Uninstalling Symantec Agent for Linux (SEPM) ...
Removing packages sdcss-caf sdcss-sepagent sdcss-kmod sdcss-scripts
Symantec Agent for Linux (SEPM) uninstalled successfully.
A reboot is required to complete uninstallation.
Please reboot your machine at the earliest convenience.
```

14.3 MP1 以前の場合： **Linux** 用 **Symantec Endpoint Protection** クライアントをアンインストールする方法

1. Linux コンピュータで、ターミナルアプリケーションウィンドウを開きます。
2. 次のコマンドを実行して Symantec Endpoint Protection インストールフォルダにナビゲートします。

   ```
   cd /opt/Symantec/symantec_antivirus
   ```

   このパスはデフォルトのインストールパスです。
3. 組み込みスクリプトで次のコマンドを実行して Symantec Endpoint Protection をアンインストールします。

   ```
   sudo ./uninstall.sh
   ```

   パスワードの入力を求めるメッセージが表示されたらパスワードを入力します。

   このスクリプトは Symantec Endpoint Protection コンポーネントのアンインストールを開始します。
4. メッセージが表示されたら `Y` と入力して **Enter** キーを押します。

   コマンドプロンプトが返るとアンインストールは完了します。

   NOTE

   一部のオペレーティングシステムでは、`/opt` フォルダの唯一の内容が Symantec Endpoint Protection クライアントファイルの場合にはアンインストーラスクリプトは `/opt` も削除します。このフォルダを作成し直すには、`sudo mkdir /opt` コマンドを入力します。

パッケージマネージャまたはソフトウェアマネージャを使ってアンインストールするには、ご使用の Linux 配布版に固有のマニュアルを参照してください。


Symantec
A Division of Broadcom