SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

環境設定ガイド: Enterprise Console ユーザー向け

目次

1 このガイドについて

このガイドでは、Sophos for Virtual Environments の設定方法について説明します。

ここでは、Sophos Enterprise Console を使用してセキュリティソフトウェアを保護していることを想定しています。

注
Sophos Central を使用している場合は、Sophos Central 版の環境設定ガイドを参照してください。

2 ポリシーの設定

Sophos for Virtual Environments は、Sophos Enterprise Console ポリシーを使用して設定します。

Sophos Enterprise Console のグループに Sophos Security VM を追加すると、ゲスト VM を保護およびアップデートするポリシーが適用されます。

デフォルト設定は、保護機能とシステムパフォーマンスのバランスが考慮されているため、この設定の使用を推奨します。ただし、次のポリシーの設定内容は変更することができます。

- ウイルス対策および HIPS
- アップデート

これ以外の Sophos Enterprise Console ポリシーは、Security VM に適用されません。

注
特定の Security VM によって保護されるゲスト VM は、その Security VM と同じポリシーを使用します。一部のゲスト VM に異なるポリシーを適用するには、そのようなゲスト VM を、別の Sophos Enterprise Console グループにある別の Security VM に移動します。そして、そのグループに別のポリシーを適用します。ゲスト VM の移動方法については、「Sophos for Virtual Environments スタートアップガイド：Enterprise Console ユーザー向け」を参照してください。

各 Security VM の管理下にあるゲスト VM の一覧を表示するには、保護されているゲスト VM の表示 (p. 10)を参照してください。

2.1 ウイルス対策および HIPS ポリシー

Security VM は、デフォルトで次の操作を実行します。

- ゲスト VM からアクセスされたファイルを検索する。
- 感染ファイルへのアクセスをブロックする。
- 検出された脅威を自動クリーンアップする。

ウイルス対策および HIPS ポリシーの設定には、Security VM に適用されないものもあります。このセクションでは、適用され、一括設定可能な検索オプションについて説明しています。

設定の詳細は、Sophos Enterprise Console ヘルプを参照してください。

オンアクセス検索

オンアクセス検索の設定の対応状況は次の表を参照してください。動作監視には対応していません。

Sophos Enterprise Console で、オンアクセス検索の設定ページを開く方法は次のとおりです。

1. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
2. 変更するポリシーをダブルクリックします。
3. 「**ウイルス対策および HIPS ポリシー**」ダイアログで、「**オンアクセス検索**」パネルを参照します。「**オンアクセス検索を有効にする**」の横にある「**環境設定**」をクリックします。

「**オンアクセス検索の設定**」ダイアログが表示されます。

各タブで設定できるオプションは次のとおりです。

検索	設定可能？	説明
ファイル検索のタイミング: 読み取ったとき/ファイル名を変更したとき/書き込んだとき	いいえ	1つまたは複数のオプションが有効に設定されている場合、Security VM は 3つのすべてのシナリオで検索を行います。 3つのオプションがすべて無効に設定されている場合、システムは保護されていない状態になります。
アドウェアや不要と思われるアプリケーション/疑わしいファイルの検索	いいえ	
ブートセクタが感染しているドライブへのアクセスを許可する	いいえ	
圧縮ファイル内を検索する (非推奨)	はい	
システムメモリを検索する	いいえ	

拡張子	設定可能？
すべてのファイルを検索する (非推奨)	はい
実行ファイルなど感染の可能性があるファイルのみを検索する	はい
追加で検索するファイル拡張子	はい
拡張子のないファイルも検索する	はい
検索の対象からファイルの種類を除外する	はい

除外	設定可能？	説明
「**Windows での除外**」タブ	はい	フォルダを除外するには、ドライブ文字やネットワーク共有フォルダ名を含むフルパスを指定する必要があります (例: C:¥Tools¥logs¥、¥¥Server¥Tools¥logs¥)。 詳細は、Sophos Enterprise Console ヘルプのウイルス対策および HIPS ポリシーの設定に関するセクションを参照してください。
「**Mac での除外**」タブ	いいえ	
「**Linux/UNIX での除外**」タブ	いいえ	

クリーンアップ	サポート対象？	注
ウイルス/スパイウェアのクリーンアップ	はい	クリーンアップに失敗した場合の別の対処方法は適用されません。Security VM は、感染ファイルへのアクセスを常に拒否します。
疑わしいファイルのクリーンアップ	いいえ	

設定やその選択方法の詳細は、Sophos Enterprise Console ヘルプを参照してください。

スケジュール検索

スケジュール検索の設定または編集方法は次のとおりです。

- 「**ウイルス対策および HIPS ポリシー**」ダイアログで、「**スケジュール検索**」パネルを参照します。
- 「**追加**」または「**編集**」をクリックします。

また、「**拡張子・除外**」をクリックして、別の種類のファイルを検索対象に指定したり、特定の種類のファイルを検索から除外したりすることもできます。

スケジュール検索の設定の対応状況は次の表を参照してください。**「追加」/「編集」 > 「スケジュール検索の設定」**。

スケジュール検索の設定	設定可能？	説明
ローカルハードディスク	はい	
フロッピーディスク、リムーバブルドライブ	はい	
CD ドライブ	はい	
検索のタイミング	はい	Security VM は、スケジュール設定した日時に検索を実行しますが、システムパフォーマンスへの影響を最小限に抑えるため、デフォルトで2台のゲスト VM のみに対して同時に検索を実行できます。

「追加」/「編集」 > 「スケジュール検索の設定」 > 「環境設定」 > 「検索・クリーンアップ設定」

検索とクリーンアップ	設定可能？	説明
「**検索**」タブ		
アドウェアや不要と思われるアプリケーション/疑わしいファイル/ルートキットの検索	いいえ	

検索とクリーンアップ	設定可能？	説明
圧縮ファイル内を検索する	はい	
システムメモリを検索する	いいえ	システムメモリはデフォルトで検索されます。このオプションを設定することはできません。
低いプライオリティで検索を実行する	いいえ	
「**クリーンアップ**」タブ		
ウイルス/スパイウェアのクリーンアップ	はい	Security VM は、フロッピーディスクドライブ、CD ドライブや ネットワークの場所を自動クリーンアップしません。 クリーンアップが実行されない場合の対処方法は適用されません。Security VM は、クリーンアップが実行されなかった場合、常にログにイベントを記録します。
アドウェアや不要と思われるアプリケーションのクリーンアップ	いいえ	
疑わしいファイルのクリーンアップ	いいえ	

「拡張子・除外」「スケジュール検索用の拡張子・除外」。

拡張子と除外	設定可能？	説明
「**拡張子**」タブ		
すべてのファイルを検索する (非推奨)	はい	
実行ファイルなど感染の可能性があるファイルのみを検索する	はい	
追加で検索するファイル拡張子	はい	
拡張子のないファイルも検索する	はい	
検索の対象からファイルの種類を除外する	はい	
「**除外**」タブ		

拡張子と除外	設定可能？	説明
「**Windows での除外**」タブ	はい	検索からフォルダを除外するには、ドライブ文字やネットワーク共有フォルダ名を含むフルパスを指定する必要があります (例: C:¥Tools¥logs¥、¥¥Server¥Tools¥logs¥)。 詳細は、Sophos Enterprise Console ヘルプを参照してください。
「**Mac での除外**」タブ	いいえ	
「**Linux/UNIX での除外**」タブ	いいえ	

Sophos Live Protection

SophosLabs のデータベースに登録されている最新のマルウェア情報を照会して、疑わしいファイルをチェックします。

オプション	設定可能？
Live Protection を有効にする	はい
オンデマンド検索での Live Protection を有効にする	はい
サンプルファイルをソフォスに自動送信する	いいえ

Web Protection

対応していません。

承認

アドウェアや他の不要と思われるアプリケーション (PUA) の承認・検出には対応していません。

メッセージング

メールメッセージのみに対応しています。

2.1.1 検索対象のファイル拡張子

デフォルトで検索されるファイル拡張子は次の表のとおりです。

386 3gr add ani asp aspx asx bat cab chm class cmd com cpl dbx dex dll dmd doc docm	docx dot drv eml exe fas flt fon fot hlp ht? hta html i13 ifs inf ini jar jpeg jpg	jpz js jse lnk lsp mnl mod mpd mpp mpt mso mui nws o ocx ov? pdf pdr php pif	pl pot pps ppt pptm pptx prc ps1 psm1 rtf scr sh shb shs src swf sys tif tiff vb?	vlx vs? vxd wbk wma wmf wsf xl? xlsm xlsx xsn zip zipx

Security VM に適用されているウイルス対策および HIPS ポリシーで「**圧縮ファイル内を検索する**」オプションが有効化されている場合、デフォルトで次の拡張子も検索されます。

7z 7zip ??_ a arj bin bz2 gz hqx hxs	lha lzh rar rpm tar taz tbz tbz2 tgz uue z

拡張子を検索の対象に追加したり、検索から除外したりする場合は、Sophos Enterprise Console ヘルプのウイルス対策および HIPS ポリシーの設定に関するセクションを参照してください。

2.2 アップデートポリシー

Sophos Enterprise Console アップデートポリシーの設定すべてが Security VM に適用されます。

詳細は、Sophos Enterprise Console ヘルプの「**コンピュータのアップデート > アップデートポリシーを設定する**」を参照してください。

3 Security VM が保護されていることの確認

ここでは、ゲスト VM が保護されているかどうかを確認する方法について説明します。次の内容を実行できます。

- ゲスト VM での保護機能の設定の確認。
- ゲスト VM でのリアルタイム検索のテスト。
- リアルタイム検索のトラブルシューティング。

3.1 保護機能の設定の確認

ゲスト VM が保護されているかどうかを確認する方法は次のとおりです。

1. ゲスト VM へ移動し、スタートメニューで「**セキュリティとメンテナンス**」を検索します。このオプションが見つからない場合は、「**アクションセンター**」を検索します。

   重要
   どちらのオプションも見つからない場合、ゲスト VM に Windows セキュリティ センターは搭載されていません。リアルタイム検索の確認 (p. 8)に記載されている手順に従って、ゲスト VM が保護されていることを確認してください。

2. 「**セキュリティ**」の横のドロップダウン矢印をクリックします。Sophos for Virtual Environments が有効になっていることが表示されます。

   注
   有効になっていない場合は、オンアクセス検索のトラブルシューティング (p. 9)を参照してください。

3.2 リアルタイム検索の確認

リアルタイム検索は最もよく使われる脅威対策機能です。ファイルを開く、書き込み、移動、名前変更する際に、Security VM 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。プログラムの実行時には、実行ファイルやプログラムが読み込むその他のファイルに対して、Security VM が検索を実行します。

重要
Security VM で保護するゲスト VM に、Sophos Endpoint for Windows がインストールされていないことを確認してください。

ファイルアクセス時に Security VM が検索を実行していることを確認する方法は次のとおりです。

1. http://2016.eicar.org/86-0-Intended-use.html を参照して、EICAR テスト用文字列を使用します。EICAR テスト用文字列を新規ファイルにコピーします。そのファイルに拡張子 .com を持つファイル名を付け、いずれか 1台のゲスト VM に保存します。
2. そのゲスト VM からこのファイルへのアクセスを試みます。
3. Sophos Enterprise Console 画面の右下にあるコンピュータリストで、「**ステータス**」をクリックします。
4. コンピュータのリストから Security VM を探します。
   - 自動クリーンアップを有効化している場合は、Security VM をダブルクリックし、「**コンピュータの詳細**」を開きます。「履歴」セクションに、EICAR が検出され、クリーンアップされたことが表示されます。
   - 自動クリーンアップを有効化していない場合は、「**警告とエラー**」カラムに警告が表示されます。Security VM を右クリックします。「**警告とエラーの対処**」に、EICAR が検出されたが、クリーンアップされていないことが表示されます。

EICAR が検出されない場合は、オンアクセス検索のトラブルシューティング (p. 9)を参照してください。EICAR がクリーンアップされない場合は、削除してください。

3.3 オンアクセス検索のトラブルシューティング

オンアクセス検索が機能していない場合の対処方法は次のとおりです。

1. Security VM が属するグループに、オンアクセス検索の有効化を指定するウイルス対策ポリシーが適用されていることを確認します。
   a) Sophos Enterprise Console の「**グループ**」で、Security VM が属するグループを右クリックし、「**グループポリシーの詳細の表示/編集**」を選択します。どの「ウイルス対策および HIPS」ポリシーが適用されているかを確認します。
   b) 「**ポリシー**」で、「**ウイルス対策および HIPS**」をダブルクリックします。
   c) Security VM を含むグループに適用されているポリシーをダブルクリックします。
   d) 「**オンアクセス検索**」で、「**オンアクセス検索を有効にする**」チェックボックスが選択されていることを確認します。「**OK**」をクリックします。
   e) コンピュータリストで Security VM を右クリックして、「**ポリシーの適用**」を選択します。次に、「**グループのウイルス対策および HIPS ポリシー**」を選択します。
   f) Security VM のステータスがポリシーに準拠していることを確認します。
2. ゲスト VM が保護されていることを確認します。Security VM のホストに移動し、ログファイルを確認します。
3. Windows セキュリティ センターで、ゲスト VM が Sophos for Virtual Environments で保護されていることを確認します。
4. マイクロソフトの更新プログラムが要求する再起動が保留されていないことを確認します。保留にされていると、Sophos Guest VM Agent のインストールが完了しない原因となることがあります。
5. 他のウイルス対策製品がインストールされていないことを確認します。セキュリティセンターが搭載されていないサーバー OS では、Windows Defender が有効になっていないことを確認します。他のウイルス対策製品が稼動しているゲスト VM は、Sophos for Virtual Environments で保護できないことに留意してください。
6. 依然としてオンアクセス検索が機能しない場合は、ソフォス テクニカルサポートへお問い合わせください。

4 保護されているゲスト VM の表示

Security VM で保護されているゲスト VM すべてを表示することができます。

1. Security VM を参照します。この際、Windows エクスプローラを使用し、IP アドレスを入力してください。
2. 「**Logs**」という共有フォルダをダブルクリックします。
3. メッセージが表示されたら、認証情報を入力します。
   - ユーザー名は、「sophos」です。
   - パスワードは、Security VM をインストールした際に設定したアクセス用パスワードです。
4. **ProtectedGVMs.log** を開き、保護されているゲスト VM を表示します。

注
ProtectedGVMs.log は、Security VM がゲスト VM の保護を開始するまで表示されません。

5 ゲスト VM の検索

Sophos for Virtual Environments では、ファイルを開いたときや閉じたときなど、ファイルのアクセス時に常に検索が実行されます (お使いのポリシーでオンアクセス検索が有効になっている場合)。

また、Security VM の管理下のすべてのゲスト VM に対してフル検索を実行することも可能です。検索は即時または指定した日時に実行できます。

システムのフル検索では、脅威は検出されますが、クリーンアップは実行されません。

注
Security VM が Sophos Enterprise Console の「**グループ外のコンピュータ**」に属している場合、検索を実行することはできません。ポリシーが適用されているグループに追加する必要があります。

注
Security VM では、ハイパーバイザーに過剰な負荷がかからないように、各ゲスト VM の検索のタイミングが調整されます。デフォルトで 2台のゲスト VM に対して同時に検索を実行します。検索を実行するゲスト VM の台数が多い場合は、終了するまで時間がかかることがあります。

- すべてのゲスト VM に対して、即時にフル検索を実行する方法は次のとおりです。
  a) Sophos Enterprise Console を開き、コンピュータのリストから対象の Security VM を参照します。
  b) Security VM を右クリックして、「**システムのフル検索**」を選択します。

  ヒント
  または、「**アクション**」メニューから「**システムのフル検索**」を選択します。

- 指定した日時にすべてのゲスト VM のフル検索を実行する方法は次のとおりです。
  a) Sophos Enterprise Consoleに進んでください。
  b) スケジュール検索を作成します。この手順については、Sophos Enterprise Console ヘルプの「ウイルス対策および HIPS ポリシーの設定」に関するセクションを参照してください。
- 検索を実行した後に検索結果の詳細を表示する方法は以下のとおりです。
  a) Sophos Enterprise Console 画面の右下にあるコンピュータリストで、Security VM をダブルクリックして「**コンピュータの詳細**」を表示します。

6 検出された脅威の確認方法

脅威やその対処方法について詳細を調べるには、次の手順を実行します。

1. Sophos Enterprise Console 画面の右下にあるコンピュータリストで、Security VM をダブルクリックして「**コンピュータの詳細**」を表示します。
   「**履歴**」セクションで、「**検出したアイテム数**」が表示されます。脅威名が「**名前**」に表示され、該当するゲスト VM およびファイルが「**詳細**」に表示されます。
2. 脅威名をクリックします。
   ソフォス Web サイトが表示され、ここから各項目に関する解析情報や、対処の方法を参照できます。

7 脅威のクリーンアップ

Security VM は、脅威を自動クリーンアップできます。なお、手動でクリーンアップすることもできます。

7.1 自動クリーンアップ

Security VM は、検出された脅威を自動的にクリーンアップすることができます。

注
CD やその他の読み取り専用ファイルシステム、リモート ファイル システムに対して、自動クリーンアップを実行することはできません。

自動クリーンアップ実行後の動作

脅威が検出され自動的にクリーンアップされると、Sophos Enterprise Console では次の内容が実行されます。

- 脅威がブロックされたことが表示される (「**コンピュータの詳細**」の「履歴」セクションを参照)。
- 脅威名、およびクリーンアップが可能かどうかを表示する警告が表示される。
- クリーンアップに成功すると警告が削除される。失敗した場合は、「クリーンアップできません」と表示される。

クリーンアップを完了させるためには、ゲスト VM の再起動が必要な場合があります。この場合、「コンピュータの再起動が必要です」という警告が該当する Security VM に対して表示されます。警告を発しているゲスト VM を確認するには、Security VM をダブルクリックして「**コンピュータの詳細**」を開き、「**未対処の警告とエラー**」に表示される警告の詳細を確認します。

7.2 手動クリーンアップ

脅威は手動でクリーンアップできます。

脅威をクリーンアップした後は、Sophos Enterprise Console で警告を消去する必要があります。

7.2.1 ゲスト VM のクリーンアップ

手動でクリーンアップするには、ゲスト VM を復元します。復元を行うと、現在の状態が失われることに注意してください。次のいずれか 1つの手順を実行してください。

- 感染したゲスト VM を感染する前のスナップショットに戻す。
- 感染したゲスト VM を削除してテンプレートから再度クローンを作成する。

必要なソフォスツールがテンプレートイメージにインストールされていることを確認してください (詳細は「Sophos for Virtual Environments スタートアップガイド: Enterprise Console ユーザー向け」を参照)。

どちらの方法でも対処後、フル検索を実行してゲスト VM が感染していないことを確認します。

7.2.2 Sophos Enterprise Console の警告の消去

感染したゲスト VM がクリーンアップされたことが確認できたら、次のようにして Sophos Enterprise Console で警告を消去します。

1. Sophos Enterprise Console の画面の右下にあるコンピュータリストで、Security VM を右クリックして、「**警告とエラーの対処**」を選択します。
2. 「**警告とエラーの対処**」の「**警告**」タブで、警告を選択し、「**消去**」をクリックします。

警告は、Sophos Enterprise Console に表示されなくなります。

8 警告

このセクションでは、脅威の検出、クリーンアップ時に Security VM によって送信される警告について説明します。

脅威警告

Security VM がゲスト VM で脅威を検出すると、Sophos Enterprise Console に警告が表示されます。

- ダッシュボードに警告が表示されます。
- コンピュータリストの「**ステータス**」タブの「**警告とエラー**」で、Security VM に対して赤い警告アイコンが表示されます。

脅威が自動的にクリーンアップされると、Sophos Enterprise Console の脅威警告は消去されます。

警告の対象となるゲスト VM を表示するには、コンピュータのリストで Security VM をダブルクリックします。「**コンピュータの詳細**」の「**未対処の警告とエラ**」で、警告の詳細を参照します。ゲスト VM の詳細が表示され、脅威のパスが次のようにして表示されます。

MachineName(IP アドレス)/C:¥threat.exe

ユーザーがファイルを開こうとしたときに、Security VM が脅威を検出した場合、ファイルにアクセスできないという内容のメッセージがゲスト VM にも表示されることがあります。この動作はファイルを開く際に使用したアプリケーションによって異なります。

クリーンアップ後の警告

脅威がクリーンアップされると、Sophos Enterprise Console の警告は消去されます。

クリーンアップも Sophos Enterprise Console にレポートされます。レポートを表示するには、コンピュータのリストに表示されている Security VM をダブルクリックし、「**コンピュータの詳細**」を開き、「**履歴**」を参照します。

脅威が部分的に削除されたが、クリーンアップの完了にはゲスト VM の再起動が必要な場合は、「コンピュータの再起動が必要です」という警告が表示されます。

9 ログ

ログは、ゲスト VM で表示できます。

ゲスト VM で、ログは Windows のアプリケーション イベント ログに書き込まれます。ログは、「**アプリケーションとサービス ログ > Sophos > SVE**」にあります。

Security VM でログを収集して、共有ログディレクトリから取得することできます。次の手順を実行します。

1. Security VM のコンソールを開きます。
2. ログオンします。
   - ユーザー名は、「sophos」です。
   - パスワードは、Security VM をインストールした際に設定したアクセス用パスワードです。
3. 次のコマンドを入力します。sudo /opt/sophox/logcollector/diagnose
4. メッセージが表示されたら、アクセス用パスワードを入力します。(終了するまで数分かかることがあります)。
5. これで、¥¥<SVM の IP アドレス>¥logs¥logs.tgz にある収集されたログを Windows エクスプローラで参照できます。メッセージが表示されたら、認証情報を入力します。
   - ユーザー名は、「sophos」です。
   - パスワードは、Security VM をインストールした際に設定したアクセス用パスワードです。

Sophos Enterprise Console のログについては、Sophos Enterprise Console ヘルプを参照してください。

10 Security VM のアンインストール

アンインストール後も、 必ずゲスト VM が継続的に保護されるようにしてから、アンインストールを開始します。アンインストールする Security VM がインストールされているホストに移動し、保護されているゲスト VM を表示します (保護されているゲスト VM の表示 (p. 10)を参照)。表示されたゲスト VM を同様のポリシー設定が適用されている別の Security VM に移動します。

Security VM をアンインストールするには、 Security VM を削除します。

ゲスト VM を移動する方法は次のとおりです。

1. Guest VM Agent をアンインストールします (Guest VM Agent のアンインストールを参照)。
2. 新しい Security VM の IP アドレスを使用して Guest VM Agent を再インストールします。

ゲスト VM の移動が完了したら、Security VM を削除します。次の手順を実行します。

3. ハイパーバイザーに移動します。
4. Security VM をパワーオフします。
5. 仮想マシンを削除します。

11 Guest VM Agent のアンインストール

Guest VM Agent は、コントロールパネルからアンインストールできます。

1. ゲスト VM で、「**コントロールパネル**」を開きます。
2. 「**プログラムと機能**」をクリックします。
3. 次の機能を選択して「**アンインストール**」をクリックします。
   - Sophos for Virtual Environments
   - Sophos Guest VM Scanning Service
   - Sophos Virus Removal Tool

12 補足: 移行するゲスト VM を保護する Security VM の追加

移行するゲスト VM を保護する Security VM は、随時、追加することができます。

今後さらに Sophos Security VM を作成する予定がある場合は、追加する予定の Sophos Security VM 用に IP アドレスを予約するようにしてください。そして、以下で説明するファイルのマスター版を作成し、該当する IP アドレスを事前に入力しておきます。ファイルには、現在ある Sophos Security VM、および今後追加する Sophos Security VM の IP アドレスすべてを入力します。そして、Sophos Security VM を作成するたびに、このファイルをそこにコピーします。

重要
ここでの手順は、追加する Security VM と既存の Security VM で実行する必要があります。

1. Security VM のコンソールを開きます。
2. ログオンします。

   ユーザー名は、「sophos」です。

   パスワードは、Security VM をインストールした際に設定したアクセス用パスワードです。
3. 次のコマンドを実行して環境設定ファイル additional_svms.txt を開き、編集します。sudo vi /opt/sophos-svms/etc/additional_svms.txt
4. 移行するゲスト VM を保護できる Security VM の IP アドレスを追加または削除します。IP アドレスは、区切り文字なしで、1行に 1つ指定します。

   a) 「i」を押して、vi の編集モードに切り替えます。

   b) IP アドレスは、区切り文字なしで、1行に 1つ指定します。例:

      1.2.3.4
      5.6.7.8

   c) 現在ログインしている Security VM の IP アドレスを入力する必要はありません。

   d) 「Esc」を押して、vi のコマンドモードに戻ります。

   e) 「:wq」を押して、ファイルを保存して閉じます。
5. SVM ログ (/var/log/ssvm.log) を参照して、追加する Security VM のリストの処理中にエラーが発生したかどうかを確認します。

   エラーがない場合は、接続されているゲスト VM すべてに更新されたリストが送信され、新たに追加された Security VM から保護を受けられるようになります。

13 補足: Security VM への CPU の追加

1台のホストに多数のゲスト VM がある場合は、すべての仮想マシンが起動時に使用するファイルをスキャンするのに十分なプロセッサを、Security VM に割り当てる必要があります。

割り当てを行うには、Security VM に使用できる CPU の数を増やします。この設定は、いつでも行うことができます。

注
Security VM を Sophos Enterprise Console のコンピュータのグループに追加した後に、CPU を追加する場合は、必ず Security VM にグループポリシーが適用されてから追加します。

負荷のタイプにもよりますが、CPU を追加することによってシステム全体のパフォーマンスが向上することもあります。

VMware ESXi での CPU の追加

CPU を追加する方法は次のとおりです。

1. Security VM をパワーオフします。
2. vSphere Client で、Security VM を選択します。
3. 「**設定の編集 > ハードウェア > CPU**」の順に選択します。CPU の数を指定します。

Microsoft Hyper-V での CPU の追加

CPU を追加する方法は次のとおりです。

1. 「**スタート**」ボタンをクリックして「**管理ツール**」を選択し、「**Hyper-V マネージャー**」をクリックします。
2. 結果パネルの「**仮想マシン**」で、Security VM を選択します。
3. 「**操作**」パネルで、VM 名の下の「**設定**」をクリックします。
4. 「**プロセッサ**」をクリックし、割り当てるプロセッサ数を指定します。

14 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わせ。 https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

15 利用条件

サードパーティライセンス

本製品の使用に関連するサードパーティライセンスについては、Sophos Security VM の次のフォルダを参照してください。/usr/share/doc

一部のソフトウェアプログラムは、特に複製、変更または特定のプログラム、あるいはその一部の頒布、およびソースコードへのアクセスを許可する、GNU 一般公衆利用許諾契約書 (GNU General Public License、あるいは単に GPL)、または同様のフリーソフトウェア使用許諾契約に基づいてユーザーの使用が許諾 (またはサブライセンス) されています。GPL に基づき使用が許諾され、実行可能なバイナリ形式で頒布されるいかなるソフトウェアも GPL によりソースコードの開示が義務付けられています。本製品と共に配布されるこのようなソフトウェアのソースコードを入手するには、サポートデータベースの文章 124427 に記載されている手順に従ってください。