SOPHOS

Cybersecurity made simple.

Sophos for Virtual Environments

環境設定ガイド: Sophos Central ユーザー向け

目次

(2019/03/26)

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 Central 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。

Sophos Enterprise Console を使用している場合は、Sophos Enterprise Console ユーザー向け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 Central ポリシーを使用して設定します。

ポリシータイプが「脅威対策」のポリシーのみを使用できますが、必要に応じて複数のポリシーを作成できます。

デフォルトで Sophos Central は、デフォルトの脅威対策ポリシーをすべての Security VM に適用します。そして、そのポリシーの設定内容は、ゲスト VM に対しても使用されます。

次の項目が実行されます。

- 既知マルウェアの検出。
- ソフォスのクラウドデータベースを参照して、ソフォスが把握している最新のマルウェアを検出。
- 脅威の定義が特定されていない新規のマルウェアもプロアクティブに検出。
- マルウェアの自動クリーンアップ。

関連タスク

ポリシーの作成/編集 (p. 2)
Sophos for Virtual Environments は、Sophos Central ポリシーを使用して設定します。

関連資料

ポリシー設定 (p. 2)
Security VM で設定可能なオプションは次のとおりです。

2.1 ポリシーの作成/編集

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

ポリシータイプが「脅威対策」のポリシーのみを使用できますが、必要に応じて複数のポリシーを作成できます。

脅威対策ポリシーを作成/編集する方法は次のとおりです。

1. Sophos Central を開き、「**サーバープロテクション > ポリシー**」を選択します。
2. 「**脅威対策**」ポリシーをクリックするか、「**ポリシーの追加**」をクリックして新しいポリシーを作成します。
3. 「**サーバー**」タブで、このポリシーを適用する Security VM を選択します。
4. 「**設定**」タブで、必要な設定を選択します。

2.2 ポリシー設定

Security VM で設定可能なオプションは次のとおりです。

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 を使用する	はい
マルウェアのサンプルを SophosLabs に自動送信する	いいえ

リアルタイム検索

「**リアルタイム検索**」のオプションは次のとおりです。

オプション	設定可能？
有効、無効	はい
検索対象: ローカル、検索対象: ローカルおよびリモート	はい
ファイルを読み込んだとき	いいえ
ファイルに書き込んだとき	いいえ

リアルタイム検索 - インターネット

「**リアルタイム検索 - インターネット**」のオプションは次のとおりです。

オプション	設定可能？
進行中のダウンロードをスキャンする	いいえ
悪意のある Web サイトへのアクセスをブロックする	いいえ
レピュテーションの低いファイルを検出する	いいえ

修復

「**修復**」のオプションは次のとおりです。

オプション	設定可能？
マルウェアを自動クリーンアップする	はい

リアルタイム検索 - オプション

「**リアルタイム検索 - オプション**」のオプションは次のとおりです。

オプション	設定可能？
既知のアプリケーションを自動的に検索の対象から除外する	いいえ

オプション	設定可能？
悪意のある動作を検知する (HIPS)	いいえ

スケジュール検索

「**スケジュール検索**」のオプションは次のとおりです。

オプション	設定可能？
スケジュール検索を有効にする	はい

ランタイム保護

「**ランタイム保護**」のオプションは次のとおりです。

オプション	設定可能？
C & C サーバーに送信されるネットワークトラフィックを検出する	いいえ
ランサムウェアから文書ファイルを保護する (CryptoGuard)	いいえ
Sophos Security Heartbeat を有効にする	いいえ

検索除外

「**検索除外**」のオプションは次のとおりです。

オプション	設定可能？
グローバル検索除外 設定は、「**設定 > グローバル検索除外**」で編集できます。	はい
ポリシーごとの検索除外 (Windows および Linux)	はい
ポリシーごとの Heartbeat 除外 (Windows のみ)	いいえ
DNS サーバーの除外 (Windows のみ)	いいえ

デスクトップ通知

「**デスクトップ通知**」のオプションは次のとおりです。

オプション	設定可能？
脅威対策のデスクトップ通知を有効にする	いいえ

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. 6)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、リアルタイム検索のトラブルシューティング (p. 7)を参照してください。

3.2 リアルタイム検索の確認

Security VM でリアルタイム検索が動作することを確認します。

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。

ファイルのアクセス時に 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。
2. 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。
3. 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。
4. Sophos Central にサインインします。
   - 自動クリーンアップを有効化している場合は、「**サーバー**」ページで Security VM をクリックして、詳細ページを表示します。「**イベント**」タブに、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**」ページを表示します。Security VM に警告が表示されているのが確認できます。EICAR が検出されましたが、クリーンアップされていません。

EICAR が検出されない場合は、リアルタイム検索のトラブルシューティング (p. 7)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 リアルタイム検索のトラブルシューティング

リアルタイム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 に適用されているサーバーポリシーで、オンアクセス検索が有効化されていることを確認します。
   a) Sophos Central の「**サーバー**」ページで、該当する Security VM をクリックして詳細を参照します。
   b) 「**サマリー**」タブの「**サマリー**」にサーバーに適用されている脅威対策ポリシーが表示されます。ポリシー名をクリックします。
   c) ポリシーの「**リアルタイム検索**」セクションを参照します。「**検索対象**」が有効になっていることを確認します。
   d) Security VM 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。詳細は、保護されているゲスト VM の表示 (p. 8)を参照してください。
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 ゲスト VM の表示

すべてのゲスト VM の詳細は、次の方法で表示できます。

- 接続されているゲスト VM の表示 (p. 8)。これは Sophos Central で実行できます。
- 保護されているゲスト VM の表示 (p. 8)。

「接続されている」ゲスト VM には、ソフォス製品のエージェントがインストールされており、Security VM に接続できます。

通常、接続されているゲスト VM も保護されている状態にあります。ただし、エージェントをインストールしたばかりの場合や、問題が発生している場合は、脅威の検索が開始していないこともあります。

4.1 接続されているゲスト VM の表示

Security VM で保護されているゲスト VM すべてを次のようにして表示することができます。

1. Sophos Central にサインインします。
2. 「**サーバープロテクション > サーバー**」を開きます。
3. 一覧で、該当する Security VM を参照し、クリックして詳細を表示します。
4. 「**サマリー**」タブの「**仮想環境の状態**」の下で、「**接続されているゲスト VM**」を参照します。表示されている数値をクリックします。

   注
   パワーオン中のゲスト VM がまったくない場合や、エージェントのインストールが進行中の場合は、ゲスト VM は表示されません。

5. VM の名前と IP アドレスの一覧が表示されます。

   一覧で特定のゲスト VM を検索したり、デスクトップゲスト VM やサーバーゲスト VM をフィルタリング表示したりできます。

4.2 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

Security VM 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。

Security VM は、すべてのゲスト VM に対してフル検索を実行することもできます。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 では、ESXi ホスト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。このため、Security VM で管理されるすべてのゲスト VM の検索を実行すると、完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 Central にサインインします。
  b) 「**サーバー**」ページを開きます。
  c) 対象の Sophos Security VM を参照し、クリックして詳細ページを開きます。
  d) 左側のペインで「**今すぐ検索**」をクリックします。
- 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 Central にサインインします。
  b) 「**サーバー**」ページを開きます。
  c) 対象の Sophos Security VM を参照し、クリックして詳細ページを表示します。
  d) 「**サマリー**」タブで、「**サマリー**」の下から該当する「脅威対策ポリシー」を探します。ダブルクリックして編集します。
  e) ポリシーの「**スケジュール検索**」セクションに移動します。スケジュール検索を有効にし、検索を実行する日時を指定します。

6 脅威が検出された際に表示される警告

ゲスト VM のいずれかで脅威が検出されると、Security VM が次の操作を実行します。

- 脅威をブロックする。
- 検出された脅威の自動クリーンアップを実行する。
- 対処が必要な場合は、Sophos Central に警告を送信する。

注
Security VM は、すべてのゲスト VM のフル検索中に検出された脅威に対しては、自動クリーンアップを実行しません。

Sophos Central に表示される内容

Sophos Central:

- 脅威がブロックされたことが表示される。Security VM の詳細ページの「**イベント**」タブを参照してください。
- 「**警告**」ページに警告が表示される。脅威名、脅威のある VM の名前、およびクリーンアップが可能かどうかが表示されます。
- 自動クリーンアップに成功すると警告が削除される。

自動クリーンアップに失敗した場合や使用できない場合は、手動によるクリーンアップを促す警告が「**警告**」ページに表示されます。

クリーンアップの詳細は、脅威のクリーンアップ (p. 12)を参照してください。

ゲスト VM に表示される内容

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、ゲスト VM からのファイルアクセスはブロックされます。アクセスするために使用したアプリケーションで対応している場合、ファイルにアクセスできなくなったというメッセージがユーザーに表示されます。

7 脅威のクリーンアップ

このセクションでは手動および自動による脅威のクリーンアップについて説明します。

脅威とそのクリーンアップ方法の詳細は、Sophos Central にログオンして「**警告**」ページを開き、対象の脅威に関する警告を探して脅威名をクリックします。

自動クリーンアップ

Security VM は、検出した脅威を自動的にクリーンアップします。

注
CD や、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。

手動クリーンアップ

ゲスト VM は手動でクリーンアップすることができます。

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場合があることに注意してください (詳細は以下を参照)。

次のいずれか 1つの手順を実行してください。

- 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。現在の状態が失われます。
- ゲスト VM を感染する前のスナップショットに戻す。スナップショットを作成後の状態が失われます。

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。

8 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. 8)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。

9 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

10 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。

11 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。

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。

12 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

13 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。