Symantec™ Endpoint Protection における更新の計画とテストのためのベスト プラクティス - Japanese - Japan

September 2021

Table of Contents

著作権に関する声明

エンジンの更新と定義の更新を適用するためのベスト プラクティス

この文書について

対象読者

このドキュメントは、Symantec Endpoint Protection の更新を継続的に管理するシステム管理者を対象としています。このドキュメントでは、お客様が組織ですでに Symantec Endpoint Protection をインストールおよび設定していて、コンテンツの更新を行った経験がいくらかあることを前提としています。

範囲

このドキュメントでは、エンジンの更新と定義をすべてのクライアント コンピュータにロールアウトする前にそれらをテストするプロセスを推奨しています。このプロセスは大規模な企業組織においてより適切にスケーリングできますが、小規模な組織もこのプロセスに従うことができます。このドキュメントの目的は、障害とダウンタイムを最小限に抑えてコンテンツを更新できるようにすることです。このガイドの内容は主に Windows クライアントの更新に当てはまりますが、Mac クライアントと Linux クライアントのためにベスト プラクティスの一部を使用できます。

このドキュメントの使い方

このドキュメントでは、手順を完了するために必要な特定の概念またはタスク、あるいはタスクへのリンクについて説明します。このガイドは「Symantec Endpoint Protection インストール ガイドおよび管理者ガイド」と一緒に使用できます。

Symantec Endpoint Protection の更新の種類は?

Symantec Endpoint Protection はネットワークを保護するためにさまざまな種類の更新を使います。

デフォルトでは、Symantec Endpoint Protection は LiveUpdate を使用して以下のコンテンツを配信します。

- セキュリティ コンテンツ
  セキュリティ コンテンツには、アンチウイルスとマルウェアの定義、評価データ、侵入防止シグネチャ、動作ルール、新しいヒューリスティックなどが含まれます。セキュリティ チームは受信したデータとインテリジェンスからこのコンテンツを作成し、1 日に複数回更新します。
- エンジンの更新
  Symantec Endpoint Protection には、その機能の一部を実行するコンテンツエンジンがいくつか搭載されています。シマンテック社は、これらのエンジンの機能を更新して、Symantec Endpoint Protection の機能を強化し、新しい脅威に対応します。これらの更新は四半期ごとに自動的に行われ、セキュリティ コンテンツの更新と一緒に配信されます。これらのエンジンアップデートは、実稼働環境にロールアウトする前に必ずテスト環境で実行する必要があります。シマンテックは早期採用プログラムを提供しています。これにより、一般リリースで利用できる数週間前にエンジンの更新を受信してテストできます。次のサイトを参照してください。
  – 早期採用プログラム (EAP) を使用して Symantec Endpoint Protection クライアントでエンジンの更新をテストする
  – クライアントコンピュータで動作するエンジンと定義の確認
- クライアントのセキュリティパッチ
  クライアント パッチは、クライアント コード内に存在するセキュリティの脆弱性または機能の問題を解決します。新しい脆弱性や問題が判明すると、シマンテック社はそれらを修正するクライアント パッチを LiveUpdate を通じて提供します。次のサイトを参照してください。
  Windows クライアントへの Endpoint Protection クライアント パッチのインストール

以下のタイプの更新を Broadcom サポート ポータルからダウンロードします。

https://support.broadcom.com/

- 製品リリース
  管理サーバ ソフトウェアまたはクライアント ソフトウェアをアップグレードして新機能を提供し、既知の問題や回避策を解決します。一般的に、これらの更新は、オペレーティングシステムまたはハードウェアとの互換性の向上、性能問題の調整、製品エラーの修正を目的として作成されます。製品の更新は必要に応じてリリースされます。次のサイトを参照してください。
  – Endpoint Protection 14.x のアップグレードのベストプラクティス
  – Endpoint Protection のリリースタイプとバージョンについて

更新の計画に関するベスト プラクティス

クライアント コンピュータと小売りデバイスは重要な機能を実行することが多いので、更新をロールアウトするときには追加の注意が必要です。たとえば、エンジンの更新によって、停止エラー（ブルー スクリーン（BSOD）とも呼ばれます）、高い CPU 使用率、プロセスのハング、またはシステム全体の不安定化が生じる可能性があります。大規模な配備の前に、更新をテストするために適切に構成された厳格なプロセスに従うと、重要な本稼働システムでこれらの問題の多くを回避できます。

エンジン、定義、製品リリースの更新を計画するうえで、以下のベスト プラクティスを使用してください。

> **NOTE**
>
> 一般的には、クライアントのセキュリティ パッチをテストする必要があります。ただし、それらのインストールは常に行う必要があります。

- 更新の影響を評価する
  以下の基準を使って、更新をインストールする必要があるかどうかを評価してください。
  – 更新は適切なもので、既存の問題を解決する。
  – 更新はコンピュータに害を及ぼす可能性がある他の問題を引き起こさない。
  – 更新を有効にするために特定の機能が有効または無効になっているなど、更新に関連する依存関係がある。
  – 更新の順序によって潜在的な問題が発生する可能性がある。特定の手順では、更新が適用される前に一連のイベントや更新が行われることを示したり推奨したりする場合があります。
- 適切な更新のみを適用する
  必要に応じて、製品またはセキュリティ コンテンツの更新を適用してください。最初に、クライアント コンピュータを最新のコンテンツで更新する必要がある頻度を決定する必要があります。たとえば、物理的な攻撃だけでなくネットワークベースの攻撃の対象となる一般に公開されたキオスクまたは ATM は、多層的なセキュリティに守られたネットワークの奥に配置されたデバイスよりも頻繁に更新が必要になる可能性があります。
  リリース ノートと修正ノートをお読みください。リリース ノートには、各リリースの新機能の項目と既知の問題が含まれています。修正ノートには、解決した既知の問題の一覧が含まれています。次のサイトを参照してください。
  – Symantec Endpoint Protection（SEP）14.x のすべてのリリースの新機能
  – Symantec Endpoint Protection と Endpoint Security のバージョン、システム要件、リリース日、メモ、修正
- 関連するチームと調整して実稼働環境のダウンタイムの予定を決める
  ドメインまたはポリシー管理者といった他のチームと調整を行って、新しい製品リリースを実装してください。製品のインストールまたはエンジンの更新が、最小限の人に影響する時間に行われることを確認してください。
- 最初にテスト コンピュータに更新をインストールする
  実稼働環境で重要なソフトウェアやネットワーク通信と更新の相互作用がどのように発生する可能性があるのかを評価するために、実稼働でないコンピュータのごく一部でコンテンツをテストしてください。このラボ環境で問題が発生した場合は、問題を修正して再度テストができます。シマンテック社の早期採用プログラムに登録すると、一般リリースで更新が提供される数週間前にエンジンの更新を受信してテストできます。次のサイトを参照してください。
  早期採用プログラム（EAP）を使用して Symantec Endpoint Protection クライアントでエンジンの更新をテストする
- アンインストール計画を作成する
  可能な場合は、必要に応じてアンインストールできるようにして、製品の更新をインストールする必要があります。

Windows Embedded を使う小売りシステムの場合は、会社のゴールド イメージに最新の保護が適用されていることを確認してください。次のサイトを参照してください。

Image Configuration Editor（ICE）を使用して Windows Embedded に Endpoint Protection を配備する方法

- ドメインとサイト間で一貫性を保つ
  一般的に、すべてのドメインとサイトで更新を一貫してインストールする必要があります。ドメイン間で更新のレベルに一貫性がないと、ドメイン間の同期や複製に関連する問題が発生する可能性があります。同期していないドメインが原因のエラーを見つけるのは困難です。
- **Symantec Endpoint Protection** ソフトウェアのバックアップを行う
  開始する前に、重要なシステムのバックアップを行ってください。Symantec Endpoint Protection Manager とクライアント コンピュータ間の接続性を復元する必要がある場合に備えて、Symantec Endpoint Protection のディザスタ リカバリのベスト プラクティスを確認してください。次のサイトを参照してください。
  Endpoint Protection のディザスタリカバリのベストプラクティス
- バックアウト計画を用意する
  バックアウト計画を用意すると、更新またはインストールが失敗した場合に、クライアント コンピュータを元の状態に戻すことができます。計画の手順は明確にする必要があり、それらをテストしておく必要もあります。バックアウト計画は、バックアップからの復元のようなシンプルなものにすることもできますし、長い手動の手順を多数含めることもできます。
- 計画された更新についてユーザに告知する
  計画された更新についてユーザに告知すると、ユーザは画面に表示される通知に備えることができます。
- **2** つ前のバージョンの更新よりも古い状態にしない
  メンテナンス計画の一環として製品のアップグレードの予定を立てて、2 つ前のバージョンのアップグレードよりも古い状態にならないようにしてください。場合によっては、最新のアップグレードでサポートされていない古いオペレーティング システムのクライアント コンピュータをアップグレードしたくないことがあります。ただし、これらのクライアントは最近の修正や機能を受信しない場合があります。
- 重要でないコンピュータを最初に対象にする
  ラボ環境ですべてのテストが成功した後、可能な場合は、最初に重要でないクライアント コンピュータへの配備から始めてください。その後、更新が実稼働環境で 10 日間から 14 日間運用されたら、プライマリ サーバに取り掛かってください。
- 電子メール通知の購読
  通知エイリアスに登録すると、エンジンの最新の更新と製品リリースに関するシマンテック社からの電子メールを受信できます。次のサイトを参照してください。
  先を見越した製品の警告と記事の購読

Windows クライアントでリリースする前のエンジン更新のテスト

Symantec Endpoint Protection には、その機能の一部を実行するエンジンがいくつか含まれています。これらのエンジンは、バイナリファイル (.dll または .exe) であり、セキュリティ定義と共に提供されます。シマンテック社は、これらのエンジンの機能を更新して、Symantec Endpoint Protection の機能を強化し、新しい脅威に対応します。

シマンテック社は 1 日に数回ウイルス定義を更新しますが、エンジンコンテンツの更新は四半期単位です。エンジンは LiveUpdate を使用して更新されます。

実稼働環境にエンジン コンテンツをロールアウトする前に、コンテンツをダウンロードしてテストできる特別なサーバが用意されています。これらの更新は早期採用サーバー (EAS) でリリースされます。一般リリースで LiveUpdate 公開サーバーからエンジンが入手できるようになる数週間前に、エンジンの更新がリリースされます。

EAS を使用してエンジンの更新をダウンロードして、ラボ環境で試し、シマンテック社まで、発生した競合をお知らせください。このプロセスにより、シマンテック社は、一般リリース前にこの競合を修正できます。

エンジンの更新をテストするには、次の手順を使用します。

ステップ **1:** コンテンツを受信するテストコンピュータのグループを作成する

エンジンの互換性の最も正確なテストには、実際の作業を行う実働システムを利用します。次の基準を使用して EAS コンテンツを受信するクライアントコンピュータのセットを選択して、永続的なテストグループを作成します。

- 環境内の重要なシステムのさまざまな種類を識別します。これらのシステムは、ハードウェア、ソフトウェア、機能によって、互いに異なる場合があります。たとえば、デスクトップのゴールデンイメージ (マスターイメージ)、POS システム、Web サーバーなどの小売りシステムを、テストする他の重要なシステムから識別する可能性があります。
- 一部のソフトウェアの競合は断続的にのみ現れるため、各種類に対して複数のシステムを使用します。通常使用していて、代表的な作業負荷を実行するソフトウェアがインストールされている実働システムを選択します。
- 早期リリースコンテンツを受信するテストクライアントコンピュータを、テストしない実働コンピュータに似せて設定します。テストクライアントと非テストクライアントの両方が、同じ Symantec Endpoint Protection 機能をインストールして、同じポリシーを使用する必要があります。

EAS によるテストに実働コンピュータを使用したくない場合、ラボベースのシステムを使用できます。この場合、テストでシステムの機能を実行して負荷をシミュレーションする自動化のコーディングを行うと便利です。

クライアントコンピュータが少数の場合、必要なのは Symantec Endpoint Protection Manager 1 つと Windows クライアント用の Symantec Endpoint Protection 1 つです。

ステップ **2:** 早期採用サーバーからプレリリースコンテンツを受信するテストコンピュータを設定する

テストグループについては、次の手順を実行して、シマンテック社の早期採用サーバーからコンテンツをダウンロードするように LiveUpdate を設定します。

シマンテック社の早期採用 **LiveUpdate** サーバーからコンテンツをダウンロードするサイトを設定するには

1. コンソールで、[管理] > [サーバー] の順に選択します。
2. [サーバー] で、[ローカルサイト] を右クリックして [サイトプロパティを編集] をクリックします。
3. [LiveUpdate 更新元サーバー] で、[ダウンロード元サーバーの編集] をクリックします。
4. [LiveUpdate サーバー] ダイアログボックスで、[プレリリースのコンテンツに **Symantec LiveUpdate** サーバーを使用] をクリックして、[OK] > [OK] とクリックします。

シマンテック社の早期採用 **LiveUpdate** サーバーでプレリリースを使用する管理下クライアントを設定するには

1. コンソールで、新しい LiveUpdate 設定ポリシーを開いて、[ポリシー] > [LiveUpdate] とクリックします。
2. [Windows の設定] で、[サーバーの設定] > [LiveUpdate サーバーを使う] > [プレリリースのコンテンツに **Symantec LiveUpdate** サーバーを使用] とクリックします。
3. [OK] をクリックして、ポリシーをテストグループに割り当てます。

LiveUpdate 設定ポリシーが EAS からコンテンツを取得するかぎり、テストクライアントはコンテンツのプレリリースバージョンを受信し続けます。

> **NOTE**
>
> テストしないグループについては、LiveUpdate 設定ポリシーを通常使用している LiveUpdate サーバーに設定します。一般リリースのエンジンが入手できるようになったら、クライアントコンピュータの受信設定に応じて、すべてのクライアントコンピュータが LiveUpdate コンテンツを受信します。

詳細については、次を参照してください。

- 社内の LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定
- 外部 LiveUpdate サーバーからコンテンツをダウンロードするためのクライアントの設定

ステップ 3： 特定のエンジン バージョンに対してテスト コンピュータと非テスト コンピュータを設定する

次のように複数の LiveUpdate コンテンツポリシーを設定します。

- テストグループは、セキュリティ定義とエンジンの最新バージョンを受信します。このグループは、プレリリースのエンジンバージョンを含む今後すべてのコンテンツリビジョンをダウンロードします。
- 非テストグループは、エンジンの既存の安全なバージョンを受信します。
  エンジンのバージョンでロックすることもできます。このオプションでは、クライアントは特定のエンジンに関連付けられている最新のセキュリティ定義を受信し続けますが、エンジンの最新のバージョンは受信しません。次のサイトを参照してください。
  Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す
  テストグループがプレリリースコンテンツで普通に機能することを確認したら、非テストグループで次に使用するエンジンバージョンを手動で選択します。

ステップ **4:** 新しいエンジンのリリースに関する通知を設定する（省略可能）

LiveUpdate が Symantec Endpoint Protection Manager にダウンロードする予定のエンジンリリースの通知を取得するには、次のいずれかを実行します。

- 新しいコンテンツが Symantec Endpoint Protection Manager にダウンロードされたとき用の通知を追加します。新しいコンテンツの通知には、新しいエンジン リリースとセキュリティ定義の情報が含まれます。エンジンのバージョンによってコンテンツリビジョンを指定する 1 つ以上の LiveUpdate コンテンツポリシーが入手可能なエンジンの更新により ロックされている場合にのみ、通知を受信します。
  通知を表示するには、[ホーム] ページの [セキュリティの状態] ペインで、[通知の表示] をクリックします。

  NOTE

  EAS での更新の頻度は正規の LiveUpdate サーバーと同じです。これらの通知の受信頻度が高すぎると感じる場合、通知が表示されないように設定します。

  詳細については、次を参照してください。
  管理者通知の設定
- プレミアム サポートのお客様は、ここでカスタマ サブスクリプション ポータルにログオンできます。次のサイトを参照してください。
  プレミアム サポートのお客様が警告と通知にサインアップする方法

ステップ **5:** エンジンコンテンツがリリースされた後、テストコンピュータを監視する

シマンテック社がエンジンの更新を EAS に公開した後、このコンテンツを受信するように設定したコンピュータの監視を開始します。次の項目を監視します。

- テストコンピュータがエンジンの更新のプレリリースバージョンを実行することを確認します。次のサイトを参照してください。
  クライアントコンピュータで動作するエンジンと定義の確認
- Microsoft System Center Operations Manager などのツールを使用するサーバーとその他の重要なインフラ上での稼働時間と利用可能なリソース。
- クライアントコンピュータで動作するアプリケーションが、想定通り動作し続けることを確認します。
- Symantec Endpoint Protection クライアントの状態が、管理サーバーに接続されたまま保護されていることを確認します。次のサイトを参照してください。
  クライアントが管理サーバーに接続され、保護されているかどうかの確認

さらに、ポリシーを変更した後にクライアントを実行するか、スキャンを実行して、想定通りコンピュータが機能することを確認します。

予想外の動作に気付くか、エンジンの更新とのソフトウェアの競合が存在すると感じる場合、サポートに連絡してください。通常、段階的ロールアウトの開始前にソフトウェアの競合があることを確認した場合、シマンテック社は、公開のスケジュールを再設定して、お客様と共に問題を修正します。その後、シマンテック社は、更新されたエンジンを EAS に再公開します。

Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す

デフォルトでは、LiveUpdate サーバーから管理サーバーにダウンロードされるコンテンツの最新バージョンは、Windows クライアントに自動的にダウンロードされます。LiveUpdate コンテンツポリシーは、クライアントが調べてインストールできるコンテンツの種類を指定します。

ただし、次の場合、古いバージョンのコンテンツをダウンロードする必要があります。

- 定義またはエンジンの最新のセットによって、クライアントコンピュータでソフトウェアの競合が発生している。
- コンテンツを実働環境にリリースする前に、制御グループで新しいエンジンをテストする時間が必要である。

NOTE

この機能は特に注意して使ってください。コンテンツの種類のチェックマークをはずすことは、クライアントでその機能が最新の状態に維持されないことを意味します。この結果、クライアントを潜在的により大きいリスクにさらす可能性があります。

コンテンツの種類を [リビジョンを選択する] に設定してから、Symantec Endpoint Protection クライアントをクラウド管理下クライアントに変換する場合、コンテンツはクライアントで更新されません。この問題を回避するには、クライアントを変換する前にコンテンツ オプションを [利用可能な最新のものを使う] に設定します。

Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す方法

1. コンソールで、[ポリシー] > [LiveUpdate] とクリックして、LiveUpdate コンテンツポリシーを開きます。
2. [Windows の設定] の下で、[セキュリティ定義] をクリックします。

   Mac クライアントまたは Linux クライアントのコンテンツはロールバックできません。
3. 特定のバージョンにコンテンツをロールバックするには、次のオプションのいずれかをクリックします。
   - [リビジョンを選択する] > [編集] をクリックし、リビジョン番号を選択します。
     このオプションは、1 つの特定のセキュリティ定義セットにクライアントをロックします。クライアントは新しいセキュリティ定義を受信しません。
   - [エンジンのバージョンを選択してください] > [編集] をクリックし、エンジンのバージョンを選択します。
     このオプションは、特定の 1 つのエンジンのバージョンにクライアントをロックしますが、そのエンジンに関連付けられている最新のセキュリティ定義を引き続き配布します。環境で現在のエンジンが動作することが判明していて、新しいエンジンのリリース前に異なるグループでテストする必要がある場合、エンジンのバージョンを選択します。または、クライアントがそのコンテンツの種類の最新のエンジンバージョンと定義を受信し続けられるように、[利用可能な最新を使う] をクリックします。
4. [OK] をクリックします。

   コンテンツの更新で、クライアントコンピュータを再起動する必要はありません。
5. トラブルシューティングの問題を解決した後、[Windows の設定] で、コンテンツの各種類に対して [セキュリティ定義] > [利用可能な最新を使う] をクリックします。

詳しい情報

- Windows クライアントでリリースする前のエンジン更新のテスト
- LiveUpdate から Symantec Endpoint Protection Manager へのコンテンツのダウンロード

早期採用プログラム（EAP）を使用して **Symantec Endpoint Protection** クライアントでエンジンの更新をテストする

このセクションでは、環境内のエンジンのコンテンツをテストおよび管理するために、早期採用プログラム（EAP）に参加する方法について説明します。このプログラムは Windows クライアント向けです。

早期採用プログラムはすべてのお客様が対象で、予定されているエンジンのコンテンツのリリースに関するサポート通知の受信にサインアップする PCS のお客様であるかどうかは関係ありません。PCS のお客様でない場合でも、エンジンのリリース後に環境でエンジンをテストできます。

概要

早期採用プログラムでは、更新されるエンジンに関する情報とすべてのお客様に対するエンジンのリリース スケジュールを含むプレリリース通知が送られます。コンテンツが LiveUpdate によって一般に提供される前に、早期採用システム（EAS）を通じて、別の公開された場所にある Symantec LiveUpdate server からエンジンのプレリリース コンテンツを入手できます。

エンジンをダウンロードして、ラボ環境で試し、発生した競合をシマンテック社に知らせることができます。このプロセスにより、シマンテック社は、一般リリース前にこの競合を修正できます。

クライアントコンピュータが少数の場合、必要なのは Symantec Endpoint Protection Manager 1 つと Windows クライアント用の Symantec Endpoint Protection 1 つです。

エンジンの更新がリリースされる頻度

エンジンのコンテンツは、LiveUpdate 公開サーバで段階的にリリースされる前に、2 週間 EAS に公開されます。エンジンの更新はおおよそ四半期ごとにリリースされ、セキュリティ コンテンツの更新と一緒にリリースされます。新しいエンジンのリリースは、LiveUpdate の標準設定で提供されます。次のサイトを参照してください。

- クライアントコンピュータで動作するエンジンと定義の確認
- Endpoint Protection のコンテンツの段階的なロールアウトについて

ステップ 1： エンジンのリリースに関する通知を要求する

PCS の警告および通知サービスの一環として、予定されているエンジンのコンテンツのリリースに関する通知を受信します。PCS のお客様は、お客様向けのサブスクリプション ポータルにログオンして、希望する伝達手段を設定できます。次のサイトを参照してください。

プレミアム サポートのお客様が警告と通知にサインアップする方法

ステップ 2： コンテンツを受信するコンピュータを特定する

EAS のコンテンツを受信する適切なエンドポイントのセットを選択してください。環境内の重要なシステムのさまざまな種類を識別します。これらのシステムは、ハードウェア、ソフトウェア、または機能によって互いに区別される場合があります。たとえば、デスクトップのゴールデンイメージ (マスターイメージ)、POS システム、Web サーバーなどの小売りシステムを、テストする他の重要なシステムから識別する可能性があります。

エンジンの互換性の最も正確なテストには、実際の作業を行う実働システムを利用します。EAS の対象として識別するシステムの種類ごとに、EAS のコンテンツを受信する特定のエンドポイントをいくつか選択してください。本稼働システムを使用することにより、これらのシステムにインストールされたソフトウェアが実際の方法で実行され、サーバに典型的な負荷がかかることになります。一部のソフトウェアの競合は断続的にしか現れないため、各種類のシステムを複数使用する必要があります。

この目的のために実稼働エンドポイントを使用したくない場合は、ラボベースのシステムを EAS と一緒に使用できます。その場合、テストでシステムの機能を実行する自動化のコーディングを行って負荷のシミュレーションを行うと便利です。

ステップ 3： **EAS** からコンテンツを受信するエンドポイントを設定する

シマンテック社の早期採用サーバ（EAS）からコンテンツを受信する必要があるクライアント コンピュータを特定した後、以下のタスクを実行してください。

1. EAS からコンテンツをダウンロードするサイトを設定します。
2. デフォルトの管理サーバを使う管理下クライアントを設定します。
   このタスクは、クライアントがデフォルトの Symantec LiveUpdate server を使用するように設定されている場合にのみ実行します。
3. LiveUpdate Administrator からコンテンツを受信する管理外クライアントを設定します。
   一時的に改変対策を無効にしてホスト ファイルをコピーします。
4. （省略可能）LiveUpdate Administrator で Symantec Endpoint Protection Manager と管理外 Symantec Endpoint Protection クライアントのコンテンツを管理する場合は、専用の LiveUpdate Administrator を設定します。

これらのタスクについて詳しくは、以下を参照してください。

早期採用システムを利用して新しい Endpoint Protection エンジンのプレビューを行う

EAS サーバからコンテンツを受信するクライアント コンピュータが、それ以外の点ではテストに現状含まれていない実稼働コンピュータのように設定されていることを確認してください。テストクライアントと非テストクライアントの両方が、同じ Symantec Endpoint Protection 機能をインストールして、同じポリシーを使用する必要があります。

ステップ 4： エンジンのコンテンツがリリースされた場合にクライアント コンピュータの監視とテストを行う

シマンテック社が新しいエンジンを EAS に公開した後、このコンテンツを受信するように設定したコンピュータの監視を開始してください。次の項目を監視します。

- Microsoft System Center Operations Manager などのツールを使用するサーバーとその他の重要なインフラ上での稼働時間と利用可能なリソース。
- クライアントコンピュータで動作するアプリケーションが、想定通り動作し続けることを確認します。
- Symantec Endpoint Protection クライアントの状態が、管理サーバーに接続されたまま保護されていることを確認します。次のサイトを参照してください。
  クライアントが管理サーバーに接続され、保護されているかどうかの確認

さらに、ポリシーを変更した後にクライアントを実行するか、スキャンを実行して、想定通りコンピュータが機能することを確認します。

予期していない動作に気付いた場合、または新しいエンジンの更新によるソフトウェアの競合が存在すると思われる場合は、サポートにお問い合わせください。 ほとんどの場合、段階的ロールアウトの開始前にソフトウェアの競合があることが確認されると、シマンテック社は、公開のスケジュールを再設定して、お客様と共に問題を修正してから、更新されたエンジンを EAS に公開します。必要な場合は、LiveUpdate コンテンツ ポリシーで、エンジンの更新がリリースされる前にリビジョンをロックするよう設定して、環境のその他の部分に伝播されないようにすることもできます。競合が解決したら、最新の利用可能なオプションを使うように LiveUpdate コンテンツ ポリシーを忘れずに変更し直してください。次のサイトを参照してください。

Symantec Endpoint Protection のセキュリティ更新の古いバージョンに戻す

ステップ 5： 通常の **LiveUpdate** サーバからコンテンツを受信するようにエンドポイントを設定する

早期採用プログラムを使ってエンジンをテストしたら、LiveUpdate サーバのアドレスを通常使用するサーバにリダイレクトしてください。一般リリースのエンジンが入手できるようになったら、クライアントコンピュータの受信設定に応じて、すべてのクライアントコンピュータが LiveUpdate コンテンツを受信します。

通常は、新しいエンジンを適用するためにクライアント コンピュータを再起動する必要はありません。

シマンテック社では一般的に、新しいエンジンの更新ごとにリリース ノートは提供していません。

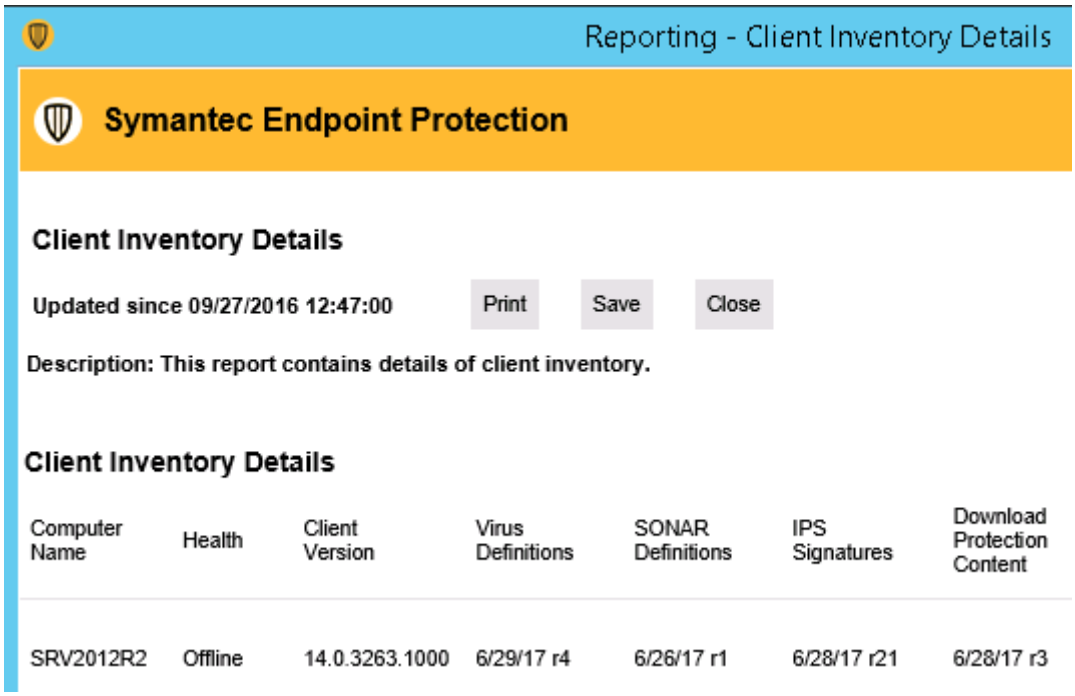
クライアントコンピュータで動作するエンジンと定義の確認

管理サーバーとクライアントで、クライアントが実行するエンジンのバージョン番号と定義を見つけます。更新したエンジンを含むコンテンツの日付とリビジョン番号を比較します。新しいエンジンを所有するクライアントと更新が必要なクライアントをすぐに判断できます。

クライアントが実行するエンジンのバージョンを確認するには

1. Symantec Endpoint Protection Manager コンソールで、[レポート] > [クイックレポート] タブをクリックします。
2. [レポートの種類] では [コンピュータの状態] を選択し、[レポートの選択] では [クライアントインベントリの詳細] をクリックします。
3. 時間範囲の選択は、[フィルタの保存] をクリックしてレポート名を指定し、[レポートの作成] をクリックします。

   レポートには、主要なコンテンツの種類すべての定義日とリビジョン番号が表示されます。必要に応じて、このレポートを .csv ファイルにエクスポートできます。



4. クライアントで、[ヘルプ] > [トラブルシューティング] > [バージョン] をクリックします。

次の方法で、AV エンジンと消去エンジンの更新がクライアントに正常に適用されていることを確認することもできます。次のサイトを参照してください。

- クライアント コンピュータから AV エンジン、IPS エンジン、および消去エンジンのバージョンを確認する方法
- コンピュータ状態のレポートとログについて

Symantec Endpoint Protection が実行するエンジンとは?

Endpoint Protection エンジンのリリースは、シマンテックセキュリティレスポンスチームが提供し更新しています。

Symantec Endpoint Protection は、Windows クライアントで以下のエンジン コンポーネントを使用します。

- ウイルス対策エンジン (AVE) (ウイルスとスパイウェアの対策)

この独自のスキャンエンジンにより、最新の脅威に対する高度なファイルベースの検出を実行します。ウイルス対策エンジンの新しいリリースでは、Symantec Endpoint Protection が使用するページプールメモリの容量が変更される場合があります。エンジンが使用するファイルは、シマンテック社によって署名されています。

- **BASH** エンジン (SONAR)
  ヒューリスティックとファイル評価データを使用してアプリケーションまたはファイルについての決定を行う、SONAR の動作エンジンです。
- **CIDS** (クライアント侵入検知システム) エンジン (侵入防止システム、メモリ エクスプロイト緩和機能)
  CIDS エンジンは、ネットワーク攻撃やブラウザ攻撃から保護するための IPS 定義を使用して機能します。ブラウザ侵入防止のサポートは、クライアントが使用する CIDS エンジンのバージョンに基づきます。メモリエクスプロイト緩和機能 (バージョン 14 の時点) でも CIDS エンジンを使用します。次のサイトを参照してください。
  Endpoint Protection のブラウザ侵入防止がサポートするブラウザのバージョン
- 消去エンジン (ウイルスとスパイウェアの対策)
  消去エンジンは、顧客のシステムで検出された脅威に対する修復と削除の機能 (修復機能) を提供するために使用します。また、消去エンジンは、起動時に実行されるドライバとアプリケーションが悪質ではないことを確認します。次のサイトを参照してください。
  消去 (Eraser) エンジンの更新が適用された後の Eraser の更新とアプリケーション テストについて
- 静的データスキャナ **(SDS)** エンジン
  このエンジンとその定義では、高度な機械学習 (AML) にエミュレータ、ITCS (Intelligent Threat Cloud Service)、CoreDef-3 定義エンジンをサポートします (バージョン 14 以降)。SDS エンジンは、指定したブートセクタ、パーティションテーブル、ファイル、またはプロセスメモリに脅威が含まれているか判断し、特定の条件で脅威を修復します。

リソースとリンク

以下の表に、このドキュメントに記載されているタスクを実行するための、ベスト プラクティスに関する詳細情報とその他の背景情報を確認できる記事を示します。

Table 1: シマンテック社の **Web** サイトの情報

情報の種類	**Web** サイトリンク
新しい製品リリースへのアップグレード	• Symantec Endpoint Protection (SEP) の最新リリースへのアップグレードおよび移行 • Endpoint Protection 14.x のアップグレードのベストプラクティス • クライアントソフトウェアをアップグレードする方法の選択
クライアントのセキュリティパッチの更新	• Windows クライアントへの Endpoint Protection クライアント パッチのインストール
LiveUpdate	• クライアント上のコンテンツを更新するための配布方法の選択 • クライアント上のコンテンツと定義を更新する方法 • グループ更新プロバイダ (GUP) のベスト プラクティス • Endpoint Protection Manager の LiveUpdate とコンテンツのトラブルシューティング
ベスト プラクティスの記事の一覧	• Symantec Endpoint Protection のベストプラクティス

詳細情報の入手方法


Symantec
A Division of Broadcom