Symantec™ Endpoint Protection 14.3 リリースノート

最終更新日: **2020 年 6 月**

Table of Contents

著作権に関する声明

Symantec Endpoint Protection 14.3 の新機能

このセクションでは、14.3 リリースの新機能を説明します。

保護機能

- サードパーティのアプリケーション開発者は、動的なスクリプトベースのマルウェアや従来とは異なるサイバー攻撃から顧客を保護することができます。 サードパーティアプリケーションは、Windows AMSI インターフェースを呼び出して、ユーザーが指定するスクリプトのスキャンを要求します。これは、Symantec Endpoint Protection クライアントにルーティングされます。 クライアントは、スクリプトの動作が悪意のあるものかどうかを示す判定で応答します。 動作が悪意のあるものでない場合、スクリプトの実行が進みます。 スクリプトの動作が悪意のあるものである場合、アプリケーションはそれを実行しません。 クライアントには、[検出結果] ダイアログボックスに「アクセス拒否」のステータスが表示されます。 サードパーティスクリプトの例には、Windows PowerShell、JavaScript、VBScript などがあります。 自動保護が有効になっている必要があります。 この機能は、Windows 10 以降のコンピュータで動作します。
  マルウェア対策スキャンインターフェース (AMSI) がマルウェアからの防御を支援する方法
  マルウェア対策スキャンインターフェース (AMSI)

Symantec Endpoint Protection Manager

- Symantec Endpoint Protection リモートコンソールでは、Java 8 ではなく Java 11 をサポートするようになりました。 リモートコンソールにアクセスするには、サポートされている Web ブラウザを開き、[アドレス] ボックスに次のアドレス「`http://SEPMServer:9090/symantec.html`」を入力し、新しいリモートコンソールパッケージをダウンロードします。 指示に従います。 以前のバージョンの Symantec Endpoint Protection Manager リモートコンソールはサポートされなくなりました。
  Symantec Endpoint Protection にログオン
- サイト上の Symantec Endpoint Protection Manager の 1 つをマスターログ記録サーバーとして設定して、ログを syslog サーバーに転送することができます。 マスターログ記録サーバーがオフラインになった場合、2 番目の管理サーバーがログを取得し、syslog サーバーにログを転送します。 マスターログ記録サーバーがオンラインに復帰すると、ログの転送を再開します。
  外部ログ記録用フェールオーバーサーバーの設定
- 統合ポリシーには、WSS トラフィックリダイレクトの新しいオプション、[LPS カスタム **PAC** ファイルを有効にする] があります。このオプションを使用すると、クライアント上の LPS サーバがホストしているデフォルトの PAC ファイルを、カスタム PAC ファイルと置き換えることができます。 カスタム PAC ファイルは、ループバックアダプタを応答準備しているローカルプロキシサーバーで動作しないサードパーティアプリケーションとの互換性の問題を解決します。

WSS トラフィックリダイレクトの設定

- Microsoft SQL Server 2019 データベースのサポート。
- ウイルス対策スキャンプロセスは、メインの非セキュリティサービスとは別のサービスを使用するようになりました。 この新しいスキャンプロセスは、より効率的なメモリ使用状況、継続的な保護、メインサービスの問題への依存関係の低下を提供します。
- データベーススキーマには、将来のリリースの機能の一部として新しい列が含まれます。(AGENT_SECURITY_LOG_1、AGENT_SECURITY_LOG_2、SEM_AGENT テーブル)
- Rest API には、/sepm/api/v1/computers API レスポンス JSON にコンピュータステータスレポートを呼び出してダウンロードするための次のフィールドがあります。quarantineStatus, quarantineCode, wssStatus, pskVersion。
- 次のサードパーティコンポーネントを新しいバージョンにアップグレードしました。Apache Tomcat、Boost C++ ライブラリ、cURL、Jackson-core、jackson-databind、Jakarta Activation、Java、logback、Microsoft JDBC Driver for SQL Server、OpenSC、OpenSSL、Spring Security、spring-framework、sqlite。
- クラウドコンソールに Symantec Endpoint Protection Manager ドメインを登録するには、まず Symantec Endpoint Security コンソールから登録トークンを取得する必要があります。 以前は、[クラウド] ページの [はじめに] をクリックして、登録トークンを取得していました。

クライアントおよびプラットフォームの更新

- Windows クライアントは、Windows 10 20H1 (Windows 10 バージョン 2004) をサポートします
- Linux クライアントは、Ubuntu 18.04、RHEL 8、CentOS 8 をサポートするようになりました。
- AppRemover ツールは、新しいバージョンに更新しました。AppRemover ツールは、Windows クライアントをインストールする前に、サードパーティ製アプリケーションを削除します。削除するアプリケーションについて詳しくは、「Endpoint Protection 14.3 でのサードパーティ製セキュリティソフトウェアの削除」を参照してください。

削除済みの機能

- [リスクの重大度] と [リスクの種類] フィールドに次の通知は表示されなくなりました： [リスクアウトブレーク]、[単一リスクイベント]、[新種のリスクを検出しました]。

Symantec Endpoint Protection のすべてのリリースの新機能

既知の問題と回避策

このセクションの項目は、このリリースの Symantec Endpoint Protection に該当します。

Table 1: アップグレードの問題

問題	説明と解決策
FIPS モードを有効にすると、SQL Server のバージョン 2017 からバージョン 2019 へのアップグレードに失敗する [14.3]	以下のエラーが表示される場合があります。「次のエラーが発生しました。 拡張機能のインストール中にエラーが発生しました。エラーメッセージ: AppContainer の作成に失敗。エラーメッセージ「なし」状態。 この実装は、Windows プラットフォームの FIPS で検証された暗号化アルゴリズムの一部ではありません。」 これは、FIPS 対応の Symantec Endpoint Protection Manager 14.3 を使用し、Microsoft SQL Server 2017 から 2019 にアップグレードした場合に発生します。 [SEP-61473] この問題を回避するには、オペレーティングシステムレベルで FIPS を無効にします。 1. `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools` で、[ローカルセキュリティポリシー] > [ローカルポリシー] > [セキュリティオプション] をクリックし、[システム暗号化] を無効にし、暗号化、ハッシュ、およびサイニングに **FIPS** 準拠のアルゴリズムを使用します 2. SQL Server バージョン 2017 からバージョン 2019 にアップグレードします。 3. SQL Server を正常にアップグレードした後、FIPS を再度有効にします。 FIPS モードを有効にすると、2017 から 2019 への SQL アップグレードが失敗する
14.2 以降へのアップグレード時に、カスタム名が使用されているとファイアウォールポリシーを更新できない場合がある	Symantec Endpoint Protection 14.2 以降へのアップグレードでは、いくつかのデフォルト名を変更していた場合、ファイアウォールポリシーに IPv6 の変更が組み込まれません。このデフォルト名には、デフォルトポリシーの名前とデフォルトルールの名前が含まれます。 アップグレード時にルールを更新できない場合、IPv6 のオプションは表示されません。 アップグレード後に作成する新しいポリシーまたはルールには影響がありません。 可能な場合は、変更された名前をデフォルトに戻します。 または、デフォルトポリシーに追加したカスタムルールが IPv6 通信を遮断しないことを確認します。 追加するすべての新しいポリシーまたはルールについて、同じことを確認します。

Table 2: Symantec Endpoint Protection Manager の問題

問題	説明と解決策
ハイブリッド管理オプションとプロキシサーバーを使用する場合は、Symantec Endpoint Security の追加 URL をホワイトリストに登録する [14.2.2.1 以降]	Broadcom による Symantec Enterprise Security の買収にともない、14.2.2.1 でのクライアントからクラウドへの通信用 URL が変更しました。 [CDM-42467] 以下の状況では、クライアントをバージョンビルド 14.2.5569.2100 以降にアップグレードする必要があります • オンプレミス Symantec Endpoint Protection Manager ドメインがクラウドコンソールに登録されているときに、Symantec Endpoint Security を使用してクライアントおよびポリシーを管理している • プロキシサーバーを使用している。 完全なクラウド管理エージェントまたはハイブリッド管理エージェントのいずれかの URL をホワイトリストに登録するには、Symantec Endpoint Security で URL をホワイトリストに登録します。 1. Symantec Endpoint Security で、[エンドポイント] > [ポリシー] > [ポリシー名] ホワイトリストポリシーに移動する。 2. ホワイトリストポリシーで、[ドメイン別除外] の横の、[追加] を選択し、以下の URL を 1 つずつ追加して、[追加] を選択する。 `us.spoc.securitycloud.symantec.com` `eu.spoc.securitycloud.symantec.com` (ヨーロッパにデバイスがある場合は追加)。 今後のバージョンでクライアントを引き続き管理する場合は、spoc.norton.com を保持します。 3. [ポリシーの保存] を選択してから [はい] を選択し、ポリシーを更新して既存のグループに適用する。 「Symantec Endpoint Security のホワイトリストに登録する URL」を参照してください。 「クラウド管理の Symantec Agents を 2020 年 5 月 4 日までにバージョン 14.2 RU2 MP1 以降にアップグレードする」を参照してください。
Symantec Endpoint Protection Manager リモートコンソールは、32 ビット Windows プラットフォームをサポートしません [14.3]	14.3 以降、32 ビットバージョンの Windows を実行している場合、Symantec Endpoint Protection Manager リモートコンソールにログオンできません。 Oracle Java SE Runtime Environment は、32 ビットバージョンの Microsoft Windows をサポートしなくなりました。 [SEP-61106] 以下のメッセージが表示された場合は、ローカルで Symantec Endpoint Protection Manager にログオンします。 「このバージョンの C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe は、実行中の Windows のバージョンと互換性がありません。 お使いのコンピュータのシステム情報を確認してから、ソフトウェア発行者にお問い合わせください。」 Symantec Endpoint Protection Manager にログオン
Symantec Endpoint Protection Manager をインストールするときに、「Microsoft Visual C++ ランタイムのインストールに失敗しました」というエラーが表示される [14.3]	Symantec Endpoint Protection Manager を Windows 2012 R2 にインストールしているときに、以下のエラーが表示される場合があります。「Microsoft Visual C++ ランタイムのインストールに失敗しました」 [SEP-60396] この問題を回避するには、Windows をアクティブ化して、Windows 更新プログラムをインストールします。 Windows 更新プログラムでは、Visual C++ 2017 再頒布可能パッケージをインストールします。これは、Windows 2012 R2 に Symantec Endpoint Protection Manager 14.3 をインストールするための前提条件です。

問題	説明と解決策
Windows の WinHTTP で、TLS 1.1 および TLS 1.2 をデフォルトのセキュアプロトコルとして有効にするための更新 [14.3]	クラウドコンソールに登録されている Symantec Endpoint Protection Manager バージョン 14.3 にアップグレードまたはインストールした後、管理サーバーは、クラウドにログを正常にアップロードしなくなります。 アップローダーに、以下のエラーが表示される場合があります。 `<SEVERE> WinHttpSendRequest: 12175: A security error occurred` この問題は、TLS 1.1 および 1.2 のサポートを提供する Microsoft update がないことが原因で発生します。 この問題を解決するには、Microsoft update: KB3140245 をインストールします。 詳細については、次を参照してください。 Windows の WinHTTP で、TLS 1.1 および TLS 1.2 をデフォルトのセキュアプロトコルとして有効にするための更新
クライアントが Endpoint Threat Defense for AD 用に更新されたポリシーを受信した後も、Symantec Endpoint Protection Manager に「配備が進行中」と引き続き表示される [14.2 RU1 MP1 以降]	これは正常な動作です。 Endpoint Threat Defense for AD 3.3 ポリシーは、バージョン 14.2 RU1 MP1 以降のクライアントでのみサポートされます。 Symantec Endpoint Threat Defense for Active Directory 3.3 のポリシーをグループに適用します。 このグループには、Symantec Endpoint Protection 14.2 RU1 以前のバージョンを実行するクライアントが含まれています。 これらのクライアントはポリシーを予期したとおりに受信して適用しますが、Symantec Endpoint Protection Manager で状態に「配備が進行中」のメッセージが引き続き表示されます。

Table 3: Windows、Mac、Linux クライアントの問題

問題	説明と解決策
最初に SHA-2 サポートをインストールしないと、Symantec Endpoint Protection 14.3 Windows クライアントのインストールに失敗することがある [14.3]	レガシーオペレーティングシステムのバージョン (Windows 7 RTM または SP1、Windows Server 2008 R2 または R2 SP1 または R2 SP2) を実行している場合、2019 年 7 月以降にリリースされた Windows アップデートをインストールするには、デバイスに SHA-2 コードサイニングサポートをインストールする必要があります。 SHA-2 をサポートしていない場合、Windows クライアントのインストールに失敗することがあります。 クライアントを初めてインストールする場合でも、以前のリリースから自動的にアップグレードする場合でも、インストールが失敗することがあります。 [SEP-61175/61403] Microsoft が適用した SHA-2 コードサイニングサポートを取得するには、以下を参照してください。 Windows および WSUS の 2019 SHA-2 コードサイニングサポートの要件 SHA-2 サポートがインストールされていない場合、Symantec Endpoint Protection 14.3 Windows クライアントのインストールに失敗することがある
Windows 10 1803 で UWF が有効な場合、Symantec Endpoint Protection Windows クライアントが動作しない [14.3]	統合書き込みフィルタ (UWF) が有効で、Windows クライアントがインストールされているドライブを保護しているときに、Symantec Endpoint Protection クライアントを Windows 10 RS4 1803 32 ビットオペレーティングシステムで実行する場合、クライアントは正常に動作しません。 この Windows オペレーティングシステムには、Windows クライアントを実行できない UWF 障害が含まれています。 この問題を回避する方法。 • 障害が含まれていない別のオペレーティングシステムバージョンにアップグレードする。 • UWF を無効にする。UWF が有効な Windows 10 1803 にインストールすると、Endpoint Protection が誤動作を起こすを参照してください。
WSS トラフィックリダイレクトが有効な Mac クライアントで LiveUpdate にカスタムプロキシ設定を適用できない [14.2 RU1 MP1 以降]	Symantec Endpoint Protection 14.2 RU1 MP1 の管理対象 Mac クライアントで、外部通信設定を通じて LiveUpdate にカスタムプロキシ設定を使用するように設定しました。 しかし、Symantec Endpoint Protection Manager ポリシーを使用して Mac クライアントの WSS トラフィックリダイレクト (WTR) を有効にすると、LiveUpdate トラフィックにカスタムプロキシ設定が適用されていないことに気付きました。 代わりに、LiveUpdate は直接接続を試行しています。 この問題を回避するには、WSS トラフィックリダイレクトが無効になっているときにのみ、LiveUpdate でカスタムプロキシ設定を使用します。

問題	説明と解決策
強化が有効な状態で Microsoft Edge が PDF のダウンロードを予期せず許可する [14.2 RU1 MP1 以降]	Symantec Endpoint Protection クライアントでアプリケーション強化が有効な状態で Microsoft Edge ブラウザを使用すると、予期せず PDF ファイルをダウンロードできてしまいます。 PDF ファイルのダウンロードの禁止は、他のブラウザでは想定どおりに機能します。 この問題は今後のリリースで修正される予定です。

Symantec Enterprise Protection が正式に Broadcom の一員になったという発表に伴い、シマンテックはマニュアルを Broadcom Symantec Security Tech Docs Portal に移行しました。

Endpoint Protection のマニュアルを見つけるには、 [Symantec **Security** Software] タブをクリックし、 [Endpoint **Security and** Management] > [Endpoint Protection] をクリックします。

Table 4: マニュアルの問題

問題	説明と解決策
操作方法の記事の有効期限が切れている。	Symantec Endpoint Protection Manager ヘルプのトピックと重複していた操作方法の記事は、Endpoint Protection サイトに再公開され、URL が変更しました。 記事を検索するには、 [検索フィールド] を使用します。
PDF ファイル	Symantec は DOC 記事にすべての PDF ファイルを掲載していました。 これらのページは有効期限が切れました。 PDF ファイルの最新バージョンのリリースを検索するには、「関連ドキュメント」ページに移動します。 今後、Broadcom はレガシー PDF ファイルや翻訳した PDF ファイルを追加していく予定です。

解決済みの問題は、「Symantec Endpoint Protection 14.3 の新しい修正とコンポーネント」を参照してください

Symantec Endpoint Protection のシステム要件 (SEP)

一般に、次のシステム必要条件は、これらがサポートされるオペレーティングシステムのものと同じです。

NOTE
Symantec Endpoint Protection Manager の以前のバージョンでは、新しいバージョンのクライアントを正しく管理できない場合があります。 コンテンツの更新やクライアント管理に問題が発生することがあります。 たとえば、Symantec Endpoint Protection Manager 14.0.1 以前では、バージョン 14.2 クライアントをそのバージョン固有の名称で正しく指定することができません。 Symantec Endpoint Protection Manager 14 MP2 以前のバージョンでは、14.0.1 以降のクライアントバージョンをバージョン固有の名称で正しく指定することができません。

以下の表に、Symantec Endpoint Protection のソフトウェア要件とハードウェア要件を示します。

Table 5: Symantec Endpoint Protection Manager (SEPM) ソフトウェアのシステム必要条件

コンポーネント	必要条件
オペレーティングシステム	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **Note:** デスクトップオペレーティングシステムはサポートされません。 **Note:** Windows Server Core エディションはサポートされません。 Windows Server Core は Symantec Endpoint Protection Manager が動作するために必要な Internet Explorer を搭載していません。
Web ブラウザ	次のブラウザは、Symantec Endpoint Protection Manager に Web コンソールでアクセスする場合や、Symantec Endpoint Protection Manager のヘルプを表示する場合に使用できます。 • Microsoft Edge 注: 32 ビット版の Windows 10 は、Edge ブラウザ上での Web コンソールアクセスをサポートしません。 • Microsoft Internet Explorer 11 • Mozilla Firefox 5.x から 68.x • Google Chrome 75.x

コンポーネント	必要条件
データベース	**Symantec Endpoint Protection Manager** には組み込み型データベースが付属しています。 代わりに、Microsoft **SQL Server** の次のいずれかのバージョンのデータベースを使うこともできます。 • SQL Server 2008、SP4 • SQL Server 2008 R2、SP3 • SQL Server 2012、RTM - SP4 • SQL Server 2014、RTM - SP3 • SQL Server 2016、RTM、SP1、SP2 • SQL Server 2017、RTM • SQL Server 2019, RTM (14.3 時点) **Note:** SQL Server Express エディションのデータベースはサポートされません。Amazon RDS でホストされている SQL Server データベースがサポートされています (14.0.1 MP2 時点)。 **Note:** Symantec Endpoint Protection で SQL Server データベースを使用しており、環境で TLS 1.2 のみが使用されている場合は、その SQL Server で TLS 1.2 がサポートされることを確認してください。 SQL Server にパッチを適用する必要がある場合があります。 この推奨事項は SQL Server 2008、2012、2014 に適用されます。TLS 1.2 をサポートする SQL Server のパッチを適用しないと、Symantec Endpoint Protection 12.1 から 14 にアップグレードするときに問題が発生する可能性があります。 **Note:** Microsoft SQL Server 用の TLS 1.2 のサポート
その他の環境条件	IPv6 ネットワーク純粋に IPv4 スタックもをインストールし、無効になっています。 IPv4 スタックがアンインストールされ、Symantec Endpoint Protection Manager は機能しません。;"

Table 6: Symantec Endpoint Protection Manager ハードウェアのシステム必要条件

コンポーネント	必要条件
CPU	Intel Pentium デュアルコアまたは同等以上 (8 コア以上を推奨) **Note:** Intel Itanium IA-64 プロセッサはサポートされません。
物理 RAM	2 GB 以上の RAM 空き容量 (8 GB 以上を推奨)。 **Note:** Symantec Endpoint Protection Manager サーバーには、すでにインストールされている他のアプリケーションの RAM 要件によって RAM の追加が必要な場合があります。たとえば、Symantec Endpoint Protection Manager サーバーに Microsoft SQL Server がインストールされている場合、サーバーには少なくとも 8 GB が使用可能である必要があります。
表示	1024 x 768 以上
システムドライブにインストールする場合はハードディスクドライブ	埋め込みデータベースまたはローカル **SQL Server** データベースを使用する場合: • 管理サーバーとデータベース用に最小 40 GB 利用可能であること (200 GB を推奨) リモート **SQL Server** データベースを使用する場合: • 管理サーバー用に最小 40 GB 利用可能であること (100 GB を推奨) • データベースのリモートサーバー用に追加のディスク容量が利用可能であること
代替ドライブにインストールする場合はハードディスクドライブ	埋め込みデータベースまたはローカル **SQL Server** データベースを使用する場合: • システムドライブには 15 GB 以上の空き容量が必要 (100 GB を推奨) • インストールドライブには 25 GB 以上の空き容量が必要 (100 GB を推奨) リモート **SQL Server** データベースを使用する場合: • システムドライブには 15 GB 以上の空き容量が必要 (100 GB を推奨) • インストールドライブには 25 GB 以上の空き容量が必要 (100 GB を推奨) • データベースのリモートサーバー用に追加のディスク容量が利用可能であること

SQL Server データベースを使用する場合は、利用可能なディスク容量を追加しなければならないことがあります。 追加容量のサイズと場所は、SQL Server で使用するドライブ、データベース保守の要件、その他のデータベースの設定によって異なります。

Table 7: Symantec Endpoint Protection for Windows クライアントソフトウェアのシステム必要条件

コンポーネント	必要条件
オペレーティングシステム（デスクトップ）	• Windows 7（32 ビット、64 ビット、RTM、SP1） • Windows Embedded 7 Standard、POSReady、Enterprise (32 ビット、64 ビット) • Windows 8 (32 ビット、64 ビット) • Windows Embedded 8 Standard (32 ビット、64 ビット) • Windows To Go を含む Windows 8.1 (32 ビット、64 ビット) • Windows 8.1 (2014 年 4 月更新) (32 ビット、64 ビット) • Windows 8.1 (2014 年 8 月更新) (32 ビット、64 ビット) • Windows Embedded 8.1 Pro、Industry Pro、Industry Enterprise (32 ビット、64 ビット) • Windows 10 (バージョン 1507) (32 ビット、64 ビット)、Windows 10 Enterprise 2015 LTSB を含む • Windows 10 November Update (バージョン 1511) (32 ビット、64 ビット) • Windows 10 Anniversary Update (バージョン 1607) (32 ビット、64 ビット)、Windows 10 Enterprise 2016 LTSB を含む • Windows 10 Creators Update (バージョン 1703) (32 ビット、64 ビット) • Windows 10 Fall Creators Update (バージョン 1709) (32 ビット、64 ビット) • Windows 10 April 2018 Update (バージョン 1803) (32 ビット、64 ビット) • Windows 10 October 2018 Update（バージョン 1809）（32 ビット、64 ビット）、Windows 10 Enterprise 2019 LTSC を含む • Windows 10 May 2019 Update（バージョン 1903）（32 ビット、64 ビット） • Windows 10 November 2019 Update (バージョン 1909) (32 ビット、64 ビット) (14.2 RU1 以降) • Windows 10 20H1 (Windows 10 バージョン 2004) (14.3 時点)
オペレーティングシステム（サーバー）	• Windows Server 2008 R2 • Windows Small Business Server 2011 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2012 R2 (2014 年 4 月更新) • Windows Server 2012 R2 (2014 年 8 月更新) • Windows Server 2016 • Windows Server 2019 • Windows Server, version 1803 (サーバーコア) (14.2 以降) • Windows Server、バージョン 1809（サーバーコア） • Windows Server, version 1903 (サーバーコア) (14.2 RU1 以降) • Windows Server, version 1909 (サーバーコア) (14.2 RU1 以降)
ブラウザの侵入防止	ブラウザ侵入防止のサポートは CIDS（Client Intrusion Detection System）エンジンのバージョンに基づきます。 「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」を参照してください。

Table 8: Symantec Endpoint Protection for Windows クライアントハードウェアのシステム必要条件

コンポーネント	必要条件
プロセッサ (物理コンピュータ用)	• 32 ビット CPU: 最低限 2 GHz Intel Pentium 4 または同等 (Intel Pentium 4 または同等を推奨) • 64 ビット CPU: 最小 2 GHz Pentium 4 で x86-64 をサポートまたは同等 **Note:** Itanium CPU はサポートされません。
プロセッサ (仮想コンピュータ用)	1 つの仮想ソケットと、ソケットごとに 1 つの 1 GHz 以上のコア (1 つの仮想ソケットと、ソケットごとに 2 つの 2 GHz のコアを推奨) **Note:** ハイパーバイザリソースの予約を有効にする必要があります。
物理 RAM	1 GB (2 GB を推奨)、またはオペレーティングシステムの必要に応じてそれ以上
表示	800 x 600 以上
ハードディスクドライブ	ディスク容量の必要条件は、インストールするクライアントの種類、インストール先のドライブ、プログラムデータファイルの保存先によって異なります。 プログラムデータフォルダは通常、システムドライブのデフォルトの場所 (C:\ProgramData) に配置されています。 選択したインストールドライブに関係なく、システムドライブには利用可能なディスク容量が常に必要です。 ハードディスクドライブのシステム必要条件: • 「システムドライブにインストールする場合にSymantec Endpoint Protection for Windows クライアントで利用可能なハードディスクドライブのシステム必要条件」に、Symantec Endpoint Protection をシステムドライブにインストールした場合のハードディスクドライブのシステムの必要条件を示します。 • 「代替ドライブにインストールする場合に Symantec Endpoint Protection for Windows クライアントで利用可能なハードディスクドライブのシステム必要条件」に、Symantec Endpoint Protection を代替ドライブにインストールした場合のハードディスクドライブのシステムの必要条件を示します。 **Note:** 必要なディスク空き領域は NTFS ファイルシステムに基づきます。 コンテンツの更新とログ用の追加容量も必要です。

Table 9: システムドライブにインストールする場合に **Symantec Endpoint Protection for Windows** クライアントで利用可能なハードディスクドライブのシステム必要条件

クライアントの種類	必要条件
標準	システムドライブ上にプログラムデータフォルダが置かれている場合: • 395 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合: • システムドライブ: 180 MB • 代替インストールドライブ: 350 MB
Embedded/VDI	システムドライブ上にプログラムデータフォルダが置かれている場合: • 245 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合: • システムドライブ: 180 MB • 代替インストールドライブ: 200 MB
ダークネットワーク	システムドライブ上にプログラムデータフォルダが置かれている場合: • 545 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合: • システムドライブ: 180 MB • 代替インストールドライブ: 500 MB

* インストール中は、さらに 135 MB が必要です。

Table 10: 代替ドライブにインストールする場合に **Symantec Endpoint Protection for Windows** クライアントで利用可能なハードディスクドライブのシステム必要条件

クライアントの種類	必要条件
標準	システムドライブ上にプログラムデータフォルダが置かれている場合: • システムドライブ: 380 MB • 代替インストールドライブ: 15 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合:** • システムドライブ: 30 MB • プログラムデータドライブ: 350 MB • 代替インストールドライブ: 150 MB
Embedded/VDI	システムドライブ上にプログラムデータフォルダが置かれている場合: • システムドライブ: 230 MB • 代替インストールドライブ: 15 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合:** • システムドライブ: 30 MB • プログラムデータドライブ: 200 MB • 代替インストールドライブ: 150 MB
ダークネットワーク	システムドライブ上にプログラムデータフォルダが置かれている場合: • システムドライブ: 530 MB • 代替インストールドライブ: 15 MB* 代替ドライブ上にプログラムデータフォルダが置かれている場合:** • システムドライブ: 30 MB • プログラムデータドライブ: 500 MB • 代替インストールドライブ: 150 MB

* インストール中は、さらに 135 MB が必要です。

** プログラムデータフォルダが代替インストールドライブと同じである場合は、プログラムデータドライブに 15 MB を加算して合計を算出します。 ただし、インストール中は、完全に利用可能な 150 MB の容量が代替インストールドライブ上に必要になります。

Table 11: Windows Embedded の **Symantec Endpoint Protection** クライアントのシステム必要条件

コンポーネント	必要条件
CPU	1 GHz Intel Pentium
物理 RAM	256 MB **Note:** この図は Symantec Endpoint Protection 埋め込みクライアントのインストール用です。 EDR などの統合ソリューションから追加機能を実装する場合は、物理 RAM の追加が必要です。
ハードディスクドライブ	Symantec Endpoint Protection Embedded/VDI クライアントには、次のハードディスク空き容量が必要です。 • システムドライブにインストールした場合: 245 MB • 代替ドライブにインストールした場合: システムドライブ上に 230 MB、代替ドライブ上に 15 MB インストール中は、さらに 135 MB が必要です。 次の図では、プログラムデータフォルダがシステムドライブ上にあると想定しています。 詳細または他のクライアントの種類の必要条件については、Symantec Endpoint Protection for Windows クライアントのシステム必要条件を参照してください。

コンポーネント	必要条件
組み込みオペレーティングシステム	• Windows Embedded Standard 7（32 ビットおよび 64 ビット） • Windows Embedded POSReady 7（32 ビットおよび 64 ビット） • Windows Embedded Enterprise 7（32 ビットおよび 64 ビット） • Windows Embedded 8 Standard (32 ビット、64 ビット) • Windows Embedded 8.1 Industry Pro（32 ビットおよび 64 ビット） • Windows Embedded 8.1 Industry Enterprise（32 ビットおよび 64 ビット） • Windows Embedded 8.1 Pro（32 ビットおよび 64 ビット）
必要な最小コンポーネント	• フィルターマネージャ（FltMgr.sys） • パフォーマンスデータヘルパー（pdh.dll） • Windows インストーラサービス
テンプレート	• Application Compatibility（デフォルト） • 電子看板 • Industrial Automation • IE、メディアプレーヤー、RDP • セットトップボックス • Thin Client Minimum Configuration テンプレートはサポートされていません。 Enhanced Write Filter（EWF）と Unified Write Filter（UWF）はサポートされません。 推奨される書き込みフィルタは、レジストリフィルタと共にインストールされる File Based Write Filter (FBWF) です。

Table 12: Symantec Endpoint Protection for Mac クライアントのシステム必要条件

コンポーネント	必要条件
CPU	64 ビットの Intel Core 2 Duo 以降
物理 RAM	2 GB の RAM
ハードディスクドライブ	インストールに 500 MB のハードディスク空き領域
表示	800 x 600
オペレーティングシステム	• macOS 10.13 • macOS 10.14 • macOS 10.15 から 10.15.5 macOS 10.14.5 以降では、kext 公証要件をサポートしています。「Endpoint Protection 14.2 RU1 と macOS 10.14.5 の kext notarization」を参照してください。 以前のリリースのサポート対象のオペレーティングシステムのリストについては、「Mac と Endpoint Protection クライアントの互換性」を参照してください。

Table 13: Symantec Endpoint Protection for Linux クライアント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 • 1 GB の RAM • 7 GB の空きディスク容量
オペレーティングシステム	• Amazon Linux • CentOS 6U3 - 6U9, 7 - 7U7, 8 (32 ビットと 64 ビット) • Debian 6.0.5 Squeeze、Debian 8 Jessie (32 ビットと 64 ビット) • Fedora 16, 17 (32 ビットおよび 64 ビット) • Oracle Linux （ OEL ） 6U2、6U4、6U5、6U8、7、7U1、7U2、7U3、7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4 (32 ビットと 64 ビット)、12 (64 ビット)、12 SP1 - 12 SP3 (64 ビット) • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4 (32 ビットと 64 ビット)、12 SP3 (64 ビット) • Ubuntu 12.04, 14.04, 16.04, 18.04 (14.3 時点)、32 ビットと 64 ビット 以前のリリースの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。
グラフィカルデスクトップ環境	次のグラフィカルデスクトップ環境を使用して Symantec Endpoint Protection for Linux クライアントを表示できます。 • KDE • Gnome • Unity

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。
	• 64 ビットコンピュータでの i686 ベース依存パッケージ
	Linux クライアントの実行可能ファイルの多くは 32 ビットプログラムです。 64 ビットのコンピュータでは、Linux クライアントをインストールする前に i686 ベースの依存パッケージをインストールする必要があります。
	i686 ベース依存パッケージをインストールしていない場合は、次のコマンドラインを使用してインストールできます。 このインストールでは、`sudo` を使用した次のコマンドが示すように、スーパーユーザー権限が必要です。
	– Red Hat ベースの配布: `sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686`
	– Debian ベースの配布: `sudo apt-get install ia32-libs`
	– Ubuntu ベースの配布:
	`sudo dpkg --add-architecture i386`
	`sudo apt-get update`
	`sudo apt-get install gcc-multilib libx11-6:i386`
	• 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。
	• 開発者ツール
	Auto-Protect カーネルモジュールの自動コンパイルおよび手動コンパイルプロセスでは、特定の開発者ツールをインストールする必要があります。 ここでの開発者ツールには、gcc、カーネルソース、ヘッダーファイルが含まれます。 インストールするツール、および特定の Linux バージョンに対しツールをインストールする方法について詳しくは、以下を参照してください。
	Endpoint Protection for Linux の Auto-Protect カーネルモジュールの手動コンパイル

Symantec Endpoint Protection のすべてのバージョンのリリースノートとシステム要件

Symantec Endpoint Protection 14.x の最新バージョンへのサポート対象アップグレードパス

NOTE

通常、最新バージョンより前の Symantec Endpoint Protection バージョンでは、これより前のリストのすべてのバージョンがサポートされます。 ただし、特定のバージョンのリリースノートを参照して確認してください。

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

Symantec Endpoint Protection Manager および **Windows** クライアント

次のバージョンの Symantec Endpoint Protection Manager と Symantec Endpoint Protection の Windows クライアントは最新バージョンに直接アップグレードできます。

- 11.x と Small Business Edition 12.0 (Symantec Endpoint Protection クライアントのみ、サポート対象オペレーティングシステムの場合)
- 12.1.6 MP10 までの 12.1.x バージョン
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU2 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Mac クライアント

次のバージョンの Symantec Endpoint Protection for Mac クライアントは最新バージョンに直接アップグレードできます。

- 12.1.4 から 12.1.6 MP9 までのバージョン
  Mac クライアントはバージョン 12.1.6 MP10 では更新されませんでした。
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

NOTE

Symantec Endpoint Protection for Mac クライアントでは 14.0.1 MP2 の更新は実施されていません。

Linux クライアント

次のバージョンの Symantec Endpoint Protection for Linux クライアントは最新バージョンに直接アップグレードできます。

- 12.1.6 MP9 までの 12.1.x バージョン
  Linux クライアントはバージョン 12.1.6 MP10 では更新されませんでした。
- 14
- 14 MP1
- 14 MP2
- 14 RU1
- 14 RU1 MP1
- 14 RU2 MP1
- 14.2
- 14.2 MP1
- 14.2 RU1
- 14.2 RU1 MP1
- 14.2 RU2
- 14.2 RU2 MP1

Symantec AntiVirus for Linux 1.0.14 は、Symantec Endpoint Protection に直接移行できる唯一のバージョンです。 Symantec AntiVirus for Linux の他のすべてのバージョンは、最初にアンインストールする必要があります。 管理下クライアントは管理外クライアントに移行できません。

サポート対象外のアップグレードのパス

すべてのシマンテック製品から Symantec Endpoint Protection に移行できるわけではありません。 Symantec Endpoint Protection クライアントをインストールする前に次の製品をアンインストールする必要があります。

- サポート外のシマンテック製品 (Symantec AntiVirus と Symantec Client Security)
- シマンテック社のすべての ノートン ™ 製品
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- Symantec Endpoint Protection for Mac 12.1.4 より前のバージョン

Symantec Endpoint Protection Manager 11.0.x または Symantec Endpoint Protection Manager Small Business Edition 12.0.x を直接 Symantec Endpoint Protection Manager 14 の任意のバージョンにアップグレードすることはできません。 最初にこれらのバージョンをアンインストールするか、12.1.x にアップグレードしてから 14.x. にアップグレードしてください。

Symantec Endpoint Protection Manager 12.1.6 MP7 のデータベーススキーマのバージョンがバージョン 14 のデータベーススキーマより新しいため、12.1.6 MP7 を 14 にアップグレードできません。 その代わり、12.1.6 MP7 を 14 MP1 以降にアップグレードする必要があります。

14 MP1 (14.0.2332.0100) から 14 MP1 更新ビルド (14.0.2349.0100) へのアップグレードはサポートされません。

ダウングレードパスはサポートされません。 たとえば、Symantec Endpoint Protection 14.2.1.1 から 12.1.6 MP10 に移行する場合は、最初に Symantec Endpoint Protection 14.2.1.1 をアンインストールする必要があります。

ビルド番号はあるが、リリースバージョンに変換する方法がわからない場合は、次を参照してください。

- リリース済みの Symantec Endpoint Protection のバージョン情報
- Endpoint Protection のリリースタイプとバージョンについて

詳細情報の入手方法

「Endpoint Protection の情報」に、ベストプラクティス、トラブルシューティング情報、製品の使用に役立つその他のリソースを入手できる Web サイトを示します。

Table 14: Endpoint Protection Web サイトの情報

情報の種類	Web サイトリンク
体験版	アカウント担当者にお問い合わせください。
マニュアルとマニュアル更新	• 最新リリースの製品ガイド (英語) • 最新リリースの製品ガイド (その他の言語) • Symantec Endpoint Protection 14.x のすべてのバージョンの製品ガイド (英語) その他の言語:
テクニカルサポート	Endpoint Protection テクニカルサポート ナレッジベースの記事、製品リリースの詳細、更新、パッチ、サポートの問い合わせオプションが含まれます。
脅威の情報と更新	シマンテックセキュリティセンター
トレーニング	教育サービス トレーニングコース、eLibrary、その他のコンテンツにアクセスできます。
Symantec Connect フォーラム (英語)	Endpoint Protection


Symantec
A Division of Broadcom