Symantec™ Endpoint Protection 14.3 RU3 リリース ノート - Japanese - Japan

Updated: September 17, 2021

Table of Contents

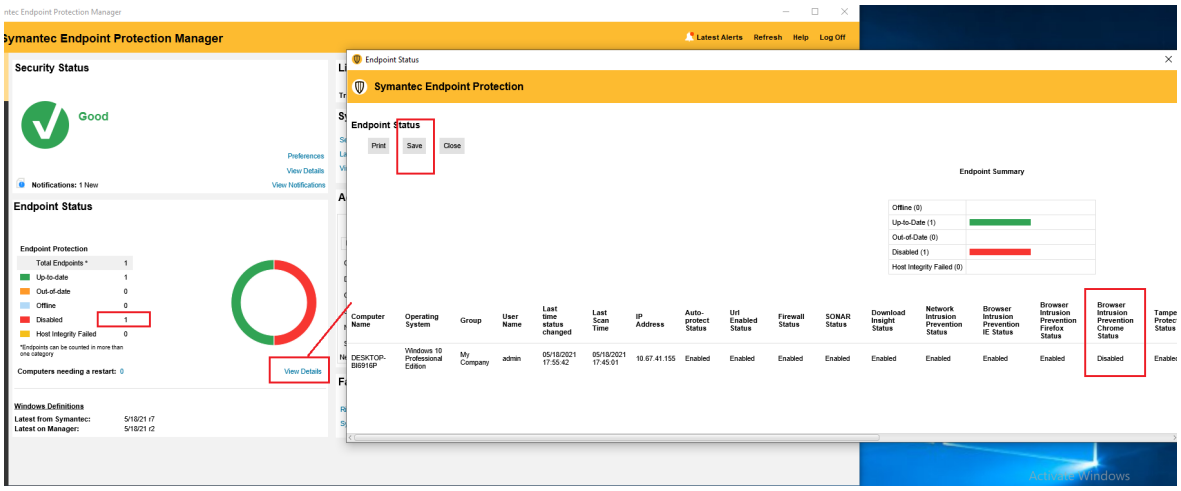
著作権に関する声明

Symantec Endpoint Protection 14.3 RU3 の新機能

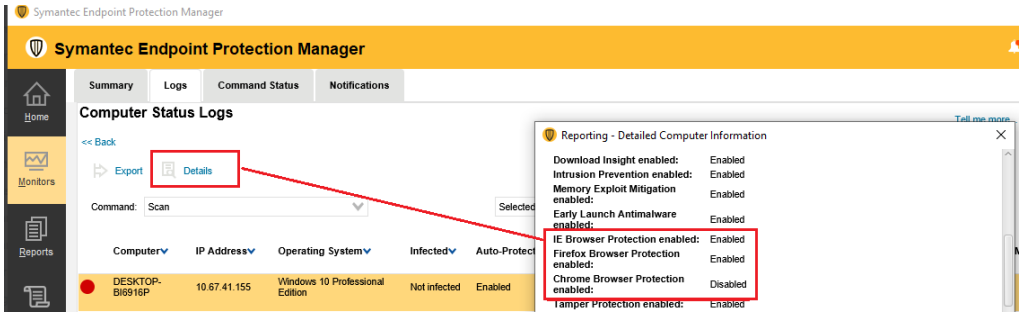
このセクションでは、このリリースの新機能を説明します。

保護機能

- Living-off-the-Land ツールに対する保護が強化されました。詳細については、「Symantec Endpoint Protection によるランサムウェアの脅威と Living-off-the-Land 戦術からの保護」を参照してください。
- REvil などの既知のランサムウェアの脅威に対する保護が強化され、新たな脅威に対応できるように検査技術が拡張されました。ターゲット攻撃に共通する疑わしいビヘイビアを検出し、暗号化が実行される前にファイルやプロセスをロックダウンします。
- 機械学習とクラウド分析によって Linux 上の脅威防止が強化されました。この機能を活用するには、[ウイルスとスパイウェアの対策ポリシー] で、[Linux の設定] > [グローバル スキャン オプション] をクリックします。
- シマンテックは、Auto-Protect による新しい検出機能をより迅速にリリースできるようになりました。
- ブラウザ拡張機能のレポートが拡張され、Symantec Endpoint Protection Manager で保護が無効になっているコンピュータやコンテンツが古いコンピュータが識別されるようになりました。
  - [クライアント] ページ > [クライアント] タブ > [保護技術] ビューに、ブラウザ拡張機能が有効であるかどうかが表示されます。クライアントを選択し、[プロパティの編集] > [クライアント] タブをクリックします。[ブラウザ **IE** の有効な状態]、[ブラウザ **FF** の有効な状態]、および [ブラウザ **Chrome** の有効な状態] フィールドに、[有効]、[無効]、または [Not **reporting**（レポートなし）] 状態のいずれかが表示されます。[ブラウザ拡張機能定義] には、定義のバージョン番号が表示されます。
  - [ホーム] ページの [エンドポイントの状態] で、[無効] 状態のクライアントを選択して [詳細] をクリックします。レポートで、有効または無効になっているブラウザ拡張機能を表示します。



  - ブラウザ拡張機能が無効なクライアントを表示する拡張レポート。[ホーム] ページの [お気に入りレポート] の下にある [Symantec **Endpoint Protection** の週次状態] レポートに、どのクライアントの拡張機能が有効または無効になっているかが表示されます。
  - [保護コンテンツのバージョン] クイック レポートには、Chrome ブラウザ拡張機能の定義が最後に更新された日時が表示されます。[レポート] > [クイック レポート] > [コンピュータの状態] レポートの種類 > [保護コンテンツのバージョン] レポートをクリックし、[レポートの作成] をクリックします。[セキュリティ状態の概略] レポートをクリックして、ブラウザ拡張機能が無効であるか誤動作しているクライアントの数を確認します。
  - コンピュータの状態ログに、[IE ブラウザ保護有効]、[Firefox ブラウザ保護有効]、[Chrome ブラウザ保護有効] の列が表示されます。[監視] ページで、[ログ] > [コンピュータの状態] ログ > [ログの表示] をクリックします。[ログ] タブで、[ブラウザ拡張機能定義] のリビジョン番号の [詳細] をクリックします。この情報を使用して、ブラウザ拡張機能のコンテンツがクライアントにダウンロードされていることを確認します。



– クライアントのシステム ログには、Chrome ブラウザ拡張機能が有効または無効になったとき、インストールまたはアンインストールされたとき、削除されたときにイベントが表示されます。
ブラウザ拡張機能を Symantec Endpoint Protection と統合して悪質な Web サイトから保護する

Symantec Endpoint Protection Manager の更新

- Symantec Endpoint Protection Manager で Windows Server 2022 がサポートされました。
- 場所の認識の設定があるクライアント アップグレード ポリシーを使用することで、Windows クライアントをより柔軟にアップグレードできます。このポリシーを使用すると、アップグレードを任意の曜日に実行し、複数日にわたって配布し、スケジュールどおりにアップグレードが開始しなかった場合に再試行することもできます。
クライアント アップグレード ポリシーを使用したクライアント ソフトウェアのアップグレード
LiveUpdate から Symantec Endpoint Protection Manager へのコンテンツのダウンロード
- 古いコンテンツがあることをクライアントが検出すると、Windows クライアントは定期的に更新をチェックして継続的な保護を提供します。定義が見つからない場合、クライアントは 30 分ごとにイベントをログに記録します。レガシー クライアントは、設定された回数だけ修復を試みた後に、その日の修復を停止してログにエラーを記録します。この設定を制御するには、[ウイルスとスパイウェアの対策ポリシー] > [その他] > [通知] タブ > [Symantec **Endpoint Protection** で警告を表示する前に修復を試みる回数] オプションを使用します。
- 次のサードパーティ コンポーネントがアップグレードまたは追加されました： AjaxSwing、Apache HTTP Server、libcurl、libxml2、OpenJDK、OpenSSL、および PHP。

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：

- Windows クライアントは、Windows Server 2022 と Windows 10 Embedded でサポートされています。バージョン 14.3 RU3 は、すべての Windows 11 および Windows 11 Embedded のプレリリース バージョンでテスト済みであり、これらのバージョンと互換性があります。
- Symantec Endpoint Protection Manager ドメインがクラウドに登録されている場合、トラブルシューティング ページにクラウド コンソールで管理されているポリシーの名前が表示されます。このページにアクセスするには、[ヘルプ] > [トラブルシューティング] > [Hybrid **Management**（ハイブリッド管理）] をクリックします。
- デバッグ ログ： [ヘルプ] > [トラブルシューティング] > [デバッグ ログ] パネルでクライアントの `debug.log` を有効にする場合は、`cve.log` も有効にします。デバッグ ログの変更を有効にするために、クライアントを再起動したり次のコマンドを実行したりする必要はありません： `smc -stop` または `smc -start`。クライアントのデバッグ ログは、クライアントと Symantec Endpoint Protection Manger の通信の問題やクライアント機能の問題のトラブルシューティングに役立ちます。通信ログ（`cve.log` および `cve-actions.log`）は、**C:\ProgramData\Symantec\Symantec Endpoint Protection\CurrentVersion\Data\Logs** にあります。
Endpoint Protection クライアント用の SymDiag の詳細デバッグログオプション
14.2 以降での Endpoint Protection 通信モジュールのログ記録の設定

Mac クライアント：

NOTE
Mac 用 Symantec Endpoint Protection クライアントの 14.3 RU3 のリリースは、2021 年 10 月に予定されています。

- macOS 12 のサポートが追加されました。
- Mac クライアント インストーラのサイズが 100 MB に削減されました。
- 「リスクを伴う」警報の数が削減され、最適化されました。
- パフォーマンスを向上させるために、複数のスキャンを同時に実行できなくなりました。スキャンが実行中の場合、他のスキャンはキューに登録されます。
- バージョン 14.3 RU3 以降、Mac クライアント インストーラで以前のバージョンのクライアントをインストールすることはできません。

Linux エージェント

- Linux エージェントのコマンド ライン ツール (sav) が拡張され、バージョンの表示、LiveUpdate の実行、スキャンの開始と停止のオプションが追加されました。詳細については、次を参照してください。
  コマンド ライン ツール (sav) を使用した Linux エージェントの管理
- Linux の SEPM 管理対象コンピュータで TCP がサポートされました。
- 問題が修正されました。
- [クライアント] ページ > [クライアント] タブ > [外部通信] の [専用サーバが利用可能でないときは、シマンテック社のサーバを使用する] オプションの警告が削除されました。12.1.5 クライアントはサポートされなくなりました。

マニュアルの変更

- Symantec Endpoint Protection Manager API は、以下の場所にある PDF ファイルで説明されています。
  Endpoint Security REST API のマニュアル

詳細については、次を参照してください。

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

Symantec Endpoint Protection（SEP）の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。

NOTE

「問題」列には、問題が見つかったときのバージョン番号が示されています。たとえば、[14.3 RU1] は、バージョン 14.3 RU1 以降に問題が当てはまるという意味です。これらの問題が修正された場合は、修正メモに表示されます。次のサイトを参照してください。

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

アップグレードの問題

Table 1: アップグレードに関する既知の問題

問題	説明と解決策
「Symantec Endpoint Protection バージョン 14.3 RU2 for Win64bit は最新のパッケージです。削除できません。」というエラー メッセージが表示される。[14.3 RU2]	Symantec Endpoint Protection Manager に複数のビルドのパッケージが表示された場合、クライアント インストール パッケージを削除できません。14.3 RU2 以降、LiveUpdate はビルド番号が異なる複数のクライアント インストール パッケージをダウンロードできます。これは、[管理] ページ > [インストール パッケージ] > [クライアント インストール パッケージ] のテーブルに表示されます。[SEP-72531]
14.3 RU2 の [現在インストールされている言語がサポートされていない場合は英語にアップグレードする] オプションを使用して、サポート対象外の言語のクライアントを英語にアップグレードする場合、自動更新に失敗する。[14.3 RU2]	この問題は、14.3 RU1 MP1 以前で、サポート対象の言語からサポート対象外の言語に手動でアップグレードしたクライアントで発生します (日本語のオペレーティング システムでチェコ語のクライアントを日本語のクライアントにアップグレードするなど)。そして、[現在インストールされている言語がサポートされていない場合は英語にアップグレードする] オプションを使用して、14.3 RU2 でサポート対象外の言語を英語にアップグレードします。[SEP-72490] この問題は、クライアント言語がサポートされているオペレーティング システムの言語 (この場合は日本語) を使っている場合に発生します。自動更新は英語ではなくサポート対象言語を使います。 この問題を回避するには、自動更新を再試行し、[現在インストールされている言語がサポートされていない場合は英語にアップグレードする] オプションをオフにします。
14.3 RU2 Symantec Endpoint Protection Manager（SEPM）からクライアント インストール パッケージをエクスポートするときに、「クライアント インストール パッケージにコンテンツが含まれていません。」という警告メッセージが表示される。[14.3 RU2]	この問題は、パッケージのエクスポートに使用している Symantec Endpoint Protection Manager とコンソールの間の通信が中断された場合に発生します。次のサイトを参照してください。 Endpoint Protection Manager からインストール パッケージをエクスポートするときに、「クライアント インストール パッケージにコンテンツが含まれていません。」という警告メッセージが表示される。
最新のクライアント インストール パッケージを古いバージョンの Symantec Endpoint Protection Manager にインポートするとエラーが表示される。[14.3 RU2]	Symantec Endpoint Protection 14.3 RU2 クライアントは、14.3 RU1 MP1 以前の Symantec Endpoint Protection Manager では管理できません。[SEP-72292]

問題	説明と解決策
Symantec Endpoint Protection Manager を 14.3 RU2 にアップグレードした後、php-cgi.exe がクラッシュしてイベント ビューアにエラーが記録される [14.3 RU2]	この問題は、バージョン 17.4.1.1 の Microsoft ODBC Driver for SQL Server で発生します。[SEP-70385] この問題を回避するには、以下の URL からバージョン 17.7.2 の Microsoft ODBC Driver for SQL Server を Windows にダウンロードしてインストールします。 https://docs.microsoft.com/en-us/sql/connect/odbc/windows/release-notes-odbc-sql-server-windows?view=sql-server-ver15 詳細については、次を参照してください。 14.3 RU2 へのアップグレード後に Endpoint Protection Manager で php-cgi.exe がクラッシュする
Symantec Endpoint Protection Manager 14.3 RU2 へのアップグレード後に、「クライアント コンピュータの名前を変更しました」という通知が表示される場合がある [14.3 RU2]	Symantec Endpoint Protection Manager の古いバージョンから 14.3 RU2 にアップグレードした後に、管理者が「クライアント コンピュータの名前を変更しました」という通知を受け取る場合があります。この問題は Mac クライアントにのみ当てはまります。次のサイトを参照してください。 Symantec Endpoint Protection Manager 14.3 RU2 へのアップグレード後に「クライアント コンピュータの名前を変更しました」という通知が表示される場合がある
Symantec Endpoint Protection Manager のダーク ネットワークでは、LiveUpdate がアップグレード中に実行しないので、古いクライアント侵入検出システム (CIDS) コンテンツを新しいクライアントにダウンロードする [14.3 RU1]	14.3 RU1 Symantec Endpoint Protection Manager がインターネットまたは LiveUpdate Administrator (LUA) サーバにアクセスできない場合、古い互換性のないコンテンツをキャッシュに保持します。この古いコンテンツは通常、新しいクライアントに配信されます。管理サーバのキャッシュのコンテンツを更新するには、認証済みウイルス定義と CIDS .jdb ファイルを手動でダウンロードします。[SEP-69125] 新しいクライアントが古いコンテンツを取得しないようにするには、新しいクライアントをインストールする前、または古いクライアントをアップグレードする前に、CIDS .jdb ファイルを SEPM に手動でインストールします。次のサイトを参照してください。 .jdb ファイルをダウンロードして Endpoint Protection Manager の定義を更新する
ネットワーク インターフェース カードが無効な場合、Symantec Endpoint Protection Manager (SEPM) にログオンできません [14.3 RU1]	Symantec Endpoint Protection Manager をインストールした後、コンソールにログオンできず、次のエラー メッセージが表示されます。 ######## ### この問題は、SEPM をインストールしたときにコンピュータのネットワーク インターフェース カードが無効になっている場合に発生する可能性があり、これによりサーバ証明書が生成されなくなります。[SEP-67040] SEPM が無効なネットワーク インターフェース カードでインストールされたかどうかを調べるには、サーバ証明書を確認します。次のサイトを参照してください。 NIC が有効になっていないサーバにインストールされた場合、SEPM ログイン時に予期しないサーバ エラーが発生する
SEPM をアンインストールし、オプションを使用してデフォルトのデータベースを削除して SQL Server Express インスタンスを残すと、「###### ########################## # 」というエラーが表示される [14.3 RU1]	Symantec Endpoint Protection Manager をアンインストールし、[DB のみを削除して **SEPM** とインストールされた **SQL Server Express** インスタンスを残す] オプションを選択すると、「###### ########################## 」というエラーが表示される場合があります。この問題は、デフォルト ユーザ DBA の認証情報を追加した後に発生し、ユーザ権限に関連している可能性があります。[SEP-68670] この問題を回避するには、SEPM setup.exe ファイルを実行してアンインストールし、アンインストール中に [**DB** のみを削除して **SEPM** とインストールされた **SQL Server Express** インスタンスを残す] オプションをクリックします。

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。 詳細については、次を参照してください。 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。

Symantec Endpoint Protection Manager の問題

Table 2: Symantec Endpoint Protection Manager に関する既知の問題

問題	説明と解決策
Endpoint Protection （SEP） 14.2 RU1 MP1 以前のクライアントで、クライアント アップグレード ポリシーの [アップグレード スケジュール] 設定が適用されない [14.3 RU3]	詳細については、次を参照してください。 Endpoint Protection 14.3 RU1 MP1 以前のクライアントがクライアント アップグレード ポリシーに従っていない [SEP-72814]
一部の EDR イベントがクライアントに表示されない [14.3 RU1]	Symantec Endpoint Protection クライアントは、Symantec EDR の Windows 用イベント追跡 (ETW) イベントを収集するために、Windows 10 ビルド 14393 以降を実行している必要があります。[SEP-67175]

問題	説明と解決策
Network Traffic Redirection（Web とクラウドのアクセス保護）機能にいくつかの制限事項がある [14.3 RU1]	• Symantec Web Security Service は、IPv6 ではなく IPv4 で提供されます。[SEP-68700] • トンネルリダイレクト方式 – Windows 10 x64 バージョン 1703 以降 (半期サービスチャネル) でのみ実行されます。この方法では、他の Windows オペレーティングシステムまたは Mac クライアントはサポートされていません。[SEP-67927] – HVCI 対応の Windows 10 64 ビットデバイスはサポートされていません。[SEP-67648] – Symantec Endpoint Protection クライアントからのアウトバウンドトラフィックは、クライアントのファイアウォールまたは URL 評価ルールのいずれかによって評価される前に、WSS にリダイレクトされます。代わりに、そのトラフィックは WSS ファイアウォールおよび URL に対して評価されます。たとえば、SEP クライアント ファイアウォール ルールが google.com を遮断し、WSS のルールが google.com を許可する場合、クライアントは google.com へのアクセスをユーザに許可します。クライアントへのインバウンド ローカル トラフィックは引き続き Symantec Endpoint Protection ファイアウォールによって処理されます。[SEP-67488] – WSS キャプティブ ポータルはトンネル方式では使用できません。クライアントはチャレンジ資格情報を無視します。今後のリリースでは、WSS エージェント内の SAML 認証はキャプティブ ポータルに置き換わり、Symantec Endpoint Protection クライアントで使用可能になります。 – クライアント コンピュータがトンネル方式を使用して WSS に接続して仮想マシンをホストする場合、各ゲスト ユーザは WSS ポータルで提供された SSL 証明書をインストールする必要があります。 – ホームディレクトリや Active Directory 認証のようなローカルネットワークへのトラフィックはリダイレクトされません。 – Microsoft DirectAccess VPN とは互換性がありません。 このトンネル方式は、現在のところ早期採用リリース機能です。
14.2.x から 14.3 MP1 以降へのアップグレード後のクライアント登録エントリの重複 [14.3 RU1]	Symantec endpoint Protection クライアントを 14.2.x から 14.3 MP1 以降にアップグレードすると、Symantec Endpoint Protection Manager の [クライアント] ページに、これらのクライアントのエージェント登録エントリが重複して作成されます。 機能上の影響はありません。また、14.3 RU1 クライアントの新しいエントリを使用し続けることもできます。Symantec Endpoint Protection Manager は古いエージェントエントリを削除します。
ハイブリッド管理オプション、プロキシ サーバ、境界ファイアウォールを使用する場合は、Symantec Endpoint Security URL を許可する [14.3]	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 が変更されました。[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 を許可し、プロキシサーバーまたは境界ファイアウォールを許可します。次のサイトを参照してください。 • SEP および SES がシマンテック社のサーバーへ接続するために許可する URL • クラウド管理の Symantec Agent をバージョン 14.2 RU2 MP1 以降にアップグレードする

問題	説明と解決策
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 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。
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。

Windows、Mac、Linux クライアントの問題

Table 3: Windows、Mac、Linux クライアントに関する既知の問題

問題	説明と解決策
システム時刻の変更後に Endpoint Protection Manager にログインすると予期しないサーバ エラーが発生し、クライアントが通信できなくなる [14.3 RU3]	システム時刻を以前の日時に戻した場合、以下のエラーが発生する可能性があります。 • Symantec Endpoint Protection Manager にログオンすると、予期しないサーバ エラーが表示されます。 • クライアントは SEPM と通信できずに 503 エラーを報告します。[SEP-74510] この問題を回避する方法。 • SEPM サービスを手動で再起動します。 • システムの日時がシステムの元の日時を過ぎるまで待ってから、日時を元に戻します。
Windows 11 上の Endpoint Protection 14.3 RU3 の Web とクラウドのアクセス保護の口グで Windows 10 オペレーティング システムが報告される [14.3 RU3]	クライアントが Windows 11 デバイスにインストールされている場合に、クライアント ユーザが SEP クライアントで Web とクラウドのアクセス保護の口グを表示すると、オペレーティング システムが Windows 10 と表示されます。クライアント コンソールで、[Web とクラウドのアクセス保護] > [オプション] > [ログの表示] をクリックします。
Validate image dependency integrity（イメージ依存関係の整合性の検証）緩和機能が Windows 10 または 11 オペレーティング システムに適用された後に Microsoft Edge ブラウザと Google Chrome ブラウザを起動できない。[14.3 RU3]	**Validate image dependency integrity**（イメージ依存関係の整合性の検証）機能は、Microsoft Edge で Windows オペレーティング システムを保護するために使用する緩和機能の 1 つです。Symantec Endpoint Protection クライアントのバージョン 14.2 RU2 MP1 以降が実行されている Windows 10 または 11 コンピュータでは、このオプションが有効になっている場合、Microsoft Edge および Google Chrome Web ブラウザの両方が起動しません。[SEP-75086] Microsoft Edge を起動できるようにするには、**Validate image dependency integrity**（イメージ依存関係の整合性の検証）機能を無効にします。Microsoft Edge の緩和機能の詳細については、「エクスプロイト保護をカスタマイズする」を参照してください。 関連項目：「Validate image dependence integrity（イメージ依存関係の整合性の検証）」緩和機能が適用され、SEP 14.2 RU2 MP1 以降がインストールされている場合に Microsoft Edge と Google Chrome が起動しない
最新の EDR イベントを取得するために再起動が不要の Windows クライアントを再起動する必要がある [14.3 RU3]	14.3 RU3 で追加の ETW イベントを利用できるようにするには、Symantec Endpoint Protection クライアントを再起動する必要があります。以下の場合に、クライアントを再起動する必要があります。[SEP-73327] • EDR が有効になっており、クライアントを RU3 に更新する場合。 • 14.3 RU3 がすでにインストールされており、EDR を有効または無効にする場合。新しく追加したイベントを有効または無効にするには、クライアントを再起動する必要があります。 参照：EDR および SEP 14.3 RU3 で一部の ETW イベントを表示するには再起動が必要になる場合がある
Linux クライアントのアップグレード後、スキャン エンジンの初期化に失敗する。[14.3 RU3]	Linux 用の Symantec Endpoint Protection クライアントをバージョン 14.3 RU3 にアップグレードした後、スキャン エンジンの初期化に失敗します。 回避策： 1. SEF 1.7.6 を含む最新のコンテンツで LiveUpdate サーバを更新します。 2. 「Scan Engine initialization failure（スキャン エンジンの初期化に失敗しました）」エラーが表示される Linux クライアント 14.3 RU3 をアンインストールします。 3. Linux クライアント 14.3 RU3 を再インストールします。
Linux クライアントのインストール後に `auditd` デーモンが有効になる。[14.3 RU3]	Linux 用 Symantec Endpoint Protection クライアントのインストーラは、インストール前に `auditd` デーモンが無効になっていた場合でも、エージェントのインストール後に `auditd` デーモンを有効にします。
ネットワーク フォレンジック情報を収集する場合（EDR）、Linux クライアントで `netstat` パッケージが必要になる。[14.3 RU3]	Linux クライアントで `netstat` パッケージが見つからない場合、ネットワーク イベントを除く他のすべての種類のイベントに関するフォレンジック情報が収集されます。

問題	説明と解決策
Mac デバイスで接続の問題が発生する可能性がある。[14.3 RU2]	• 自動更新を使用して Mac エージェントをアップグレードし、デバイスを再起動すると、エージェントがネットワークに接続できない場合があります。 回避策： エージェント インストール パッケージを再実行します。 • スタンバイ モードの後で、Mac デバイスが次のエラーでネットワーク接続を失う場合があります：「Your connection was interrupted. A network change was detected.（接続が中断しました。ネットワークの変更が検出されました。）」 回避策： – ドッキング ステーションを使用する場合は、[システム環境設定] > [ネットワーク] で IP アドレスを手動で更新します。 – ドッキング ステーションを Mac デバイスから数秒間取り外して、再度接続します。
Rosetta は、Apple Silicon（M1）デバイスへの Mac エージェントのインストールを次のエラーで遮断する場合がある：「This version of Symantec Agent for Mac is not supported on Apple M1 chip.（このバージョンの Symantec Agent for Mac は Apple M1 チップでサポートされていません。）」[14.3 RU2]	詳細については、次を参照してください。 KB 222282
Symantec Endpoint Protection Manager で生成された Web リンクを使用した Mac エージェントのダウンロードとインストールが失敗する場合がある。[14.3 RU2]	管理者が Symantec Endpoint Protection Manager の [Web リンクと電子メール] オプションを使用して Mac エージェント 14.3 RU2 のインストールをユーザに招待し、ユーザが Safari ブラウザでこのリンクを使用してパッケージをダウンロードすると、Mac エージェントのインストールが以下のエラーで失敗する場合があります。 「The application Symantec Endpoint Protection Installer can't be opened（アプリケーション Symantec Endpoint Protection インストーラを開くことができません）」 回避策： • ファイルをダウンロードしたら、ダウンロード フォルダに移動して以下のコマンドを実行し、再度インストールを実行します。 `chmod +x ./Symantec\ Endpoint\ Protection/Symantec\ Endpoint\ Protection\ Installer.app/Contents/MacOS/Symantec\ Endpoint\ Protection\ Installer` • Safari ブラウザの [環境設定] を開き、[一般] タブで [ダウンロード後、“安全な” ファイルを開く] オプションをオフにします。次に、インストーラ パッケージをダウンロードしてインストールを実行します。
サポート対象外の言語のクライアントを英語に自動的にアップグレードした場合、クライアントは引き続き英語で定義の日付設定を表示する [14.3 RU1 以降]	この問題を回避するには、レガシ クライアントをアンインストールし、新しい英語のクライアント インストール パッケージを手動でインストールします。また、自動的にアップグレードされたクライアントに対する修正が予定されています。[SEP-72481]
スタンドアロン Symantec WSS Agent は、WSS エージェントと同じコンピュータに SEP をインストールする場合、Symantec Endpoint Protection クライアントのインストールをブロックする	Network Traffic Redirection（NTR）コンポーネントは、スタンドアロン Symantec WSS Agent（WSSA）と同じファイルを使用します。NTR は、デフォルトで Symantec Endpoint Protection と Symantec Endpoint Security クラウドコンソールの両方にインストールされます。NTR 機能がエンドポイントにインストールされている場合、WSSA はインストールできません。同様に、WSSA がインストールされている場合、NTR 機能はインストールできません。 以下のいずれかの方法を使って、クライアント全体をアンインストールすることなく、既存のエンドポイントから Network Traffic Redirection 機能を削除できます。 • Symantec Endpoint Protection Manager で、NTR を含まないクライアント インストール機能セットを作成してエンドポイントに適用します。次のサイトを参照してください。 既存の Endpoint Protection クライアントに機能を追加または削除する • 次のコマンド ライン オプションは、クライアントのインストール ファイルを使用して NTR を削除します： `setup.exe /s /v" REMOVE=NTR /qn"`

問題	説明と解決策
クリーン インストールに使用されるアップグレード インストール パッケージでデフォルト機能セットがインストールされる。[14.3 RU1 MP1 以前]	[更新時に既存のクライアント機能を維持する] オプションをオンにしてアップグレード インストール パッケージを作成し、このパッケージを使ってクリーン インストールを行うと、デフォルト機能セットがクライアント デバイスにインストールされます。 カスタム機能セットをインストールする場合は、クリーン インストール用に個別のインストール パッケージを作成する必要があります。
サポート対象外のアップグレード パスを指定すると、クラウド コンソールに重複したデバイスが作成される。[14.3 RU1]	Symantec Agent for Mac を 14.2/14.3 から 14.3 RU1 にアップグレードする前に、macOS を 10.15 から 11.0 にアップグレードすると、クラウド コンソールに重複したデバイスが作成されます。 重複を回避するには、オペレーティング システムをアップグレードする前にクライアントをアップグレードする必要があります (例： Symantec Agent for Mac を 14.2/14.3 から 14.3 RU1 にアップグレードしてから macOS を 10.15 から 11.0 にアップグレードする) 。
Linux 用 Symantec Agent のインストーラ ログに誤ったメッセージが記録される。[14.3 RU1]	エージェントインストーラによって、一致しないドライババージョンに関連する不正なメッセージや、再起動が必要であることを示すメッセージがログに記録される場合があります。 これらのメッセージは、エージェントの機能には影響しません。
SuSe Linux デバイス上で、zypper が「at」パッケージの削除時に SEP Linux クライアント パッケージを削除する。[14.3 RU1]	SuSe Linux デバイス上では、「at」パッケージが必須依存パッケージとして追加され、zypper コマンドが未使用の依存関係を持つパッケージとして SEP クライアントパッケージ「sdcss-kmod」および「sdcss-sepagent」を自動的に削除しようとするため、「zypper remove at」コマンドを実行すると SEP Linux クライアントパッケージが削除されます。 回避策: 「at」パッケージを削除する場合は、コマンド「rpm -e --nodeps at」を実行します。
macOS 10.15 以降でのアップグレードの問題 [14.3 MP1]	macOS 10.15 以降では、クライアント配備ウィザードの [リモートコンピュータに **Symantec Endpoint Protection** をインストール] 機能で、古いバージョンからバージョン 14.3 MP1 への Symantec Endpoint Protection クライアントのアップグレードが失敗します。 回避策: macOS 10.15 以降では、**Symantec Endpoint Protection Manager** の自動更新を使用して Symantec Endpoint Protection クライアントの更新を実行します。
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。次のサイトを参照してください。 UWF が有効な Windows 10 1803 にインストールすると Endpoint Protection が誤動作する

問題	説明と解決策
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。
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。

解決済みの問題は、以下を参照してください

- Symantec Endpoint Protection 14.3 RU3 の新しい修正とコンポーネント
- Symantec Endpoint Protection 14.3 RU1 MP1 の新しい修正とコンポーネント
- Symantec Endpoint Protection 14.3 RU1 の新しい修正とコンポーネント
- Symantec Endpoint Protection 14.3 MP1 の新しい修正とコンポーネント
- Symantec Endpoint Protection 14.3 の新しい修正とコンポーネント

マニュアル

マニュアルは、Broadcom Symantec Security Tech Docs Portal にあります。

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。

PDF ファイル、リリース ノート、Symantec Endpoint Protection Manager のデータベース スキーマを見つけるには、「Related Documents」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。

Symantec Endpoint Protection（SEP）14.3 RU3 のシステム要件

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 4: 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 • Windows Server 2022（14.3 RU3 以降） **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、14.2x 以前ではサポートされていません。
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 Chromium ベースのブラウザ (14.3 以降) • Microsoft Edge **Note:** 32 ビット版の Windows 10 では、Edge ブラウザ上での Web コンソール アクセスをサポートしていません。 • Microsoft Internet Explorer 11 (14.2.x 以前) • Mozilla Firefox 5.x ~ 83 • Google Chrome 87

コンポーネント	必要条件
データベース	Symantec Endpoint Protection Manager には、デフォルトデータベースが含まれています。 • Microsoft SQL Server Express 2014 (Windows Server 2008 R2 用) • Microsoft SQL Server Express 2017 • Sybase 埋め込みデータベース (14.3 MP.x 以前のみ) 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 SP1、SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 以降) **Note:** 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 以降）。 **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。次のサイトを参照してください。 **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。;" • Microsoft Visual C++ 2017 再頒布可能パッケージ（x64/x86） **Note:** 必要なバージョンの Visual C++ は、Symantec Endpoint Protection Manager のインストール中に自動的にインストールされます。

Table 5: 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
プロセッサ	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	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

コンポーネント	必要条件
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	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
その他	有効なネットワーク インターフェース カード

SQL Server データベースを使う場合は、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 で使うドライブ、データベース保守の必要条件、その他のデータベースの設定によって異なります。

Table 6: 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 以降) • Windows 10 20H2（Windows 10 バージョン 2009）（14.3 以降） • Windows 10 21H1（14.3 RU1 時点） • バージョン 14.3 RU3 は、すべての Windows 11 プレリリース バージョンでテスト済みであり、これらのバージョンと互換性があります（14.3 RU3 以降）。
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) • Windows Server、バージョン 2004 • Windows Server、バージョン 20H2 (14.3 RU1) • Windows Server 2022（14.3 RU3 以降） 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、次を参照してください。 • Windows と Endpoint Protection クライアントの互換性 • Windows 10 アップデートと Windows Server 2016/Server 2019 に対する Endpoint Protection のサポート

コンポーネント	必要条件
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。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」を参照してください。

Table 7: 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: 最低限 2 GHz Pentium 4 with x86-64 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
ディスプレイ	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。 **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 8: 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 9: 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 10: 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
プロセッサ	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） • Windows Embedded 10（14.3 RU3 以降） • バージョン 14.3 RU3 は、すべての Windows 11 Embedded プレリリース バージョンでテスト済みであり、これらのバージョンと互換性があります（14.3 RU3 以降）。
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	• アプリケーション互換性（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 • シンクライアント 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 11: 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
プロセッサ/チップ	64 ビットの Intel Core 2 Duo 以降 Apple M1 chip（14.3 RU2 以降）
物理 RAM	2 GB の RAM
ハードディスクドライブ	: インストール時に 1 GB のハードディスク空き領域
ディスプレイ	800 x 600
オペレーティングシステム	• macOS 10.15 ~ 10.15.7 • macOS 11（Big Sur） 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、次を参照してください。 Mac とエンドポイント保護クライアントの互換性

Table 12: 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または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	バージョン 14.3 RU1 の時点でサポートされているオペレーティングシステム: • Amazon Linux 2 • CentOS 6、7、8 • Debian 9、10（14.3 RU2 以降） • 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 詳細情報と、サポート対象の Linux OS のマイナー バージョンのリストについては、以下を参照してください。 Symantec Linux エージェントでサポートされているカーネル バージョン 14.3 MP1 以前でサポートされているオペレーティング 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 ビットおよび 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 以前のリリースでサポート対象となっているオペレーティング システムのカーネルのリストについては、以下を参照してください。 Symantec Endpoint Protection for Linux 14.x 用にプリコンパイルされた Auto-Protect ドライバ/モジュールを含む Linux ディストリビューションおよびカーネルのリスト
その他の環境要件（14.3 RU1 以降）	• OpenSSL 1.0.2k-fips 以降

コンポーネント	必要条件

その他の環境要件 (14.3 MP1 以前)	• 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。
	• 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
	• 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ってインストールできます。このインストールでは、`sudo` を使った次のコマンドが示すように、スーパーユーザ権限が必要です。
	– 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`

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 Symantec Agent for Linux 14.3 RU1 には、グラフィカルユーザーインターフェースがありません。

詳しい情報

Endpoint Security およびすべてのバージョンの Endpoint Protection のリリースバージョン、リリースノート、新しい修正、およびシステム要件

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

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。次のサイトを参照してください。

Endpoint Security およびすべてのバージョンの Endpoint Protection のリリースバージョン、リリースノート、新しい修正、およびシステム要件

サポートされているアップグレードパス

- 埋め込みデータベースを使用する Symantec Endpoint Protection Manager バージョン 12.1.6 MP10 以降は、Microsoft SQL Server Express データベース、バージョン 14.3 RU1 MP1 にシームレスにアップグレードされます。12.1.6 MP9 以前から 14.3 RU1 MP1 へのアップグレードは遮断されます。
- Symantec Endpoint Protection Manager 14.x は、12.1.x をシームレスにアップグレードします。ただし、Windows Server 2003、デスクトップオペレーティングシステム、および 32 ビット版オペレーティングシステムのほか、一部のバージョンの SQL Server など、サポートが終了されたものは除きます。
- Symantec Endpoint Protection 14.x クライアントは、サポート対象のオペレーティング システムにインストールされている以前のすべての 12.1 クライアント バージョンをシームレスにアップグレードします。次のサイトを参照してください。

Symantec Endpoint Protection 14 の移行に関する考慮事項

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 RU1 MP2
- 14.2、14.2 MP1
- 14.2 RU1、14.2 RU1 MP1
- 14.2 RU2、14.2 RU2 MP1
- 14.3、14.3 MP1
- 14.3 RU1、14.3 RU1 MP1、14.3 RU2

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 RU1 MP2

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。
- 14.2、14.2 MP1
- 14.2 RU1、14.2 RU1 MP1
- 14.2 RU2、14.2 RU2 MP1
- 14.3、14.3 MP1
- 14.3 RU1、14.3 RU1 MP1 （2021 年 6 月に利用可能）、14.3 RU2

Linux クライアント

> **NOTE**
> 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、新しいクライアントの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。

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 RU1 MP2
- 14.2、14.2 MP1
- 14.2 RU1、14.2 RU1 MP1
- 14.2 RU2、14.2 RU2 MP1
- 14.3、14.3 MP1
- 14.3 RU1、14.3 RU1 MP1、14.3 RU2

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、以下の製品をアンインストールする必要があります。

- Symantec AntiVirus および Symantec Client Security (サポートされていません)。
- シマンテック社のすべての Norton 製品
- Symantec Endpoint Protection for Windows XP Embedded 5.1
- 12.1.4 より前の Mac 用 Symantec Endpoint Protection クライアント。または、12.1.4 以降にアップグレードすることもできます。

追加情報

- 12.1.x より前のバージョンの Symantec Endpoint Protection クライアントの移行はサポートされていません。
- Symantec Endpoint Protection Manager 11.0.x または Symantec Endpoint Protection Manager Small Business Edition 12.0.x を Symantec Endpoint Protection Manager 14 の任意のバージョンに直接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 の最新バージョン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。
- 14.0.x では、Windows XP、Server 2003、および Windows XP に基づく Windows Embedded オペレーティングシステムのサポートを終了しました。Symantec Endpoint Protection Manager 14.2 RU1 では、これらのコンピュータをレガシー 12.1.x クライアントとして管理できます。ただし、12.1.x クライアントは EOL です。これらのクライアントについては、Data Center Security (DCS) など、これらのレガシーオペレーティングシステムを引き続きサポートする Symantec 製品を使用することができます。
- 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 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。
  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

以下の表に、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 13: 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	関連ドキュメント ページ その他の言語については、 [English] ドロップダウン メニューをクリックします。
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