Symantec™ Endpoint Protection 14.3 RU1 リリース ノート

更新日: **2020** 年 **12** 月

Table of Contents

著作権に関する声明

Symantec Endpoint Protection 14.3 RU1 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

- 新しい Symantec Mac エージェントと Symantec Linux エージェントが含まれており、オンプレミスの Symantec Endpoint Protection Manager または Integrated Cyber Defense Manager クラウドコンソールのいずれかからインストールして管理することができます。
  Mac 用 Symantec Endpoint Protection クライアントのインストール
  Symantec Agent for Linux 14.3 RU1 のインストール
- 約 1,400 のファイルの動作をリアルタイムで監視することで、macOS の新しい未知の脅威を防止します。 新しい Mac エージェントには、これらの動作保護機能が含まれています。 動作保護 (または SONAR) は、人工知能と高度な機械学習を使用してゼロデイ保護を行い、新たな脅威を効果的に阻止します。
  SONAR の管理
- 脅威としてまだ識別されていない PDF ファイルやスクリプトなどの信頼できない非ポータブル実行可能 (PE) ファイルをブロックします。 [例外ポリシー] で、 [Windows の例外] > [ファイルアクセス] をクリックします。
- Web ページの評価スコアに基づいて Web の脅威を防止します。 侵入防止ポリシーには、評価スコアが特定のしきい値を下回る Web ページをブロックする URL 評価フィルタが含まれます。 評価スコアの範囲は、-10 (不良) から +10 (良好) です。 [URL 評価を有効にする] オプションは、デフォルトで有効になっています。
- Symantec Endpoint Protection に、アプリケーションのハッシュ値に基づいてアプリケーションを学習させることができます。 [例外ポリシー] で、 [Windows の例外] > [アプリケーション] > [フィンガープリントによるアプリケーションの追加] をクリックします。
- ネットワーク トラフィック リダイレクト機能を使用して、Web ベースの悪質なサイトに対する攻撃からエンドポイントとユーザを保護します。 ネットワーク トラフィック リダイレクトは、すべてのネットワーク トラフィック (すべてのポート) または Web ベースのトラフィック (ポート 80 と 443) を Symantec Web Security Service にリダイレクトし、企業ポリシーに基づいてネットワーク トラフィックと SaaS アプリケーション アクセスを許可またはブロックします。 ネットワーク トラフィック リダイレクト ポリシーには、トンネル方式と呼ばれる新しいリダイレクト方法があります。 トンネル方式では、すべてのインターネット トラフィックを Symantec WSS に自動的にリダイレクトします。WSS では、Symantec Web Security Service ポリシーに基づいてトラフィックが許可または遮断されます。 トンネル方式はベータ機能です。 WSS ポリシーに対してアプリケーションの徹底的なテストを実行する必要があります。 Broadcom はテストガイドと、エクスペリエンスに関するフィードバックを残す場所を提供するベータ Web サイトを用意しています。 Broadcom 資格情報を使用して次の Web サイトにログオンします:
  Validate.broadcom.com
  ネットワークトラフィックリダイレクトの設定
- 統合ポリシーは、ネットワークトラフィックリダイレクトポリシーに名前が変更されました。
- Symantec EDR で MITRE エンリッチ イベントのサポートを提供します。 MITRE ATT&CK フレームワークを活用して、環境内で発生している状況を把握できます。
- 以下の Symantec EDR イベントをサポートすることで、エンドポイントの可視性が向上します。
  – AMSI イベントによって、従来のコマンドライン問い合わせ手法を回避できる脅威アクター手法を可視化できます。
  – ETW イベントによって、管理対象の Windows エンドポイントで発生しているイベントを可視化できます。
- 同じコンピュータで Windows Defender と Symantec Endpoint Protection の両方を実行する機能が含まれます。 Auto-Protect スキャンは Windows Defender の後で実行し、Windows Defender で見つからない脅威を検出できます。 [Windows **Defender** と共存] オプションを使用すると、Microsoft Defender が無効になっている場合に Auto-Protect が実行されます。 このオプションを無効にするには、 [ウイルスとスパイウェアの対策ポリシー] > [その他] > [その他] タブをクリックします。
- 攻撃チェーン緩和機能がハイブリッド管理クライアントでサポートされるようになりました。

Symantec Endpoint Protection Manager

- 埋め込みデータベースが Microsoft SQL Express データベースに更新されました。 SQL Server Express データベースはデフォルトの埋め込みデータベースよりも効率的にポリシーとセキュリティ イベントを格納し、Symantec Endpoint Protection Manager と共に自動的にインストールされます。
  埋め込みデータベースから Microsoft SQL Server Express データベースへのアップグレードに関するベストプラクティス
- Symantec Endpoint Protection Manager のインストール中またはアップグレード中に、管理サーバ設定ウィザードが以下を実行します。
  – LiveUpdate コンテンツを自動的にインストールします。
  – SQL Server と Symantec Endpoint Protection Manager 間の安全な通信に TLS 証明書を使うオプションを提供します。
- LiveUpdate は Symantec Endpoint Protection Manager の新しいエンジンを使用します。このエンジンは、クラウドコンソールでの実行に最適化されています。
  LiveUpdate Administrator のリリースノートおよび新しい修正
- 14.3 MP1 で使用できなかった [既存のサードパーティのセキュリティソフトウェアを自動的にアンインストール] オプションは、更新されたバージョンの 14.3 RU1 で再度使用できるようになりました。 このオプションは、サードパーティ製セキュリティソフトウェアをアンインストールするために使用されます。 このオプションにアクセスするには、 [管理] ページ > [パッケージ] > [クライアントインストールの設定] をクリックします。
  Endpoint Protection 14 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
  Endpoint Protection 14.3 RU1 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
- クライアント パッケージの配備に使うクライアント配備ウィザードは、資格情報を検証して Symantec Endpoint Protection Manager に接続できる必要があります。 検証プロセスが失敗した場合、クライアント配備プロセスは停止し、Active Directory ユーザーアカウントがロックされないようにします。
  リモート プッシュを使った Symantec Endpoint Protection クライアントのインストール
- コンピュータ状態ログおよびレポートで、 [クライアントのバージョン] および [IPS のバージョン] フィールドの範囲を選択できるようになりました。 [製品のバージョン] フィルタは、 [クライアントのバージョン] に名前が変更されました。
- [通知領域アイコンを無効にする] オプションは、端末サーバー上で実行されており、高い CPU 使用率とメモリ使用率の原因となっているクライアントで使用できます。 ユーザ セッション プロセス (SmcGui.exe や ccSvcHost.exe など) の複数インスタンスが実行されないようにするために、通知領域アイコン (システム トレー アイコンとも呼ばれます) を無効にすることができるようになりました。 このオプションは、 [クライアント] > [ポリシー] タブ > [セキュリティの設定] > [全般] タブで有効にします。
- 許可と遮断の機能を反映するようにホワイトリスト モードとブラックリスト モードを更新しました。 [クライアント] ページ > [ポリシー] タブ > [システムロックダウン] ダイアログボックスで、アプリケーションファイルのリストが [ホワイトリストモード] および [ブラックリストモード] から [許可モード] および [拒否モード] に変更されました。
- [管理] ページ > [サーバー] タブ > [外部ログ記録を設定] > [全般] タブで、 [マスターログ記録サーバー] オプションが [一次ログ記録サーバー] に変更されました。
- [システム ログの種類] > [管理ログと監査ログ] にコンピュータ名が表示されます。
- クライアントファイアウォールのログが収集され、クラウドコンソールでの通知が少なくなります。
- Oracle Java SE が OpenJDK に置き換えられました。
- サードパーティ コンポーネント JQuery を新しいバージョンに更新しました。

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 20H2 (Windows 10 バージョン 2009) をサポートしています
- Mac クライアントは macOS 10.15.7 をサポートします。
- 古い Mac クライアント インストール パッケージを [追加パッケージ] フォルダに移動しました。

削除済みの機能

- [リスクの重大度] および [重大度別のリスク分布 **(Risk Distribution by** Severity)] オプションは、通知およびレポートから削除されました。
- この機能は 14.3 で非推奨になったため、[CASMA] タブおよび **Analyze** コマンドは削除されました。
- Mac クライアントは macOS 10.13 をサポートしなくなりました。

マニュアル

Symantec Endpoint Protection Manager のヘルプはオンラインになり、「Symantec Endpoint Protection インストールガイドおよび管理者ガイド」からアクセスできます。

データベーススキーマ

データベーススキーマには以下の変更があります。

テーブル	列の変更
警告	ENRICHED_DATA 列が追加されました。
AGENT_BEHAVIOR_LOG1 AGENT_BEHAVIOR_LOG2 AGENT_PACKET_LOG_1 AGENT_PACKET_LOG_2 AGENT_SECURITY_LOG_1 AGENT_SECURITY_LOG_2 AGENT_SYSTEM_LOG_1 AGENT_SYSTEM_LOG_2 AGENT_TRAFFIC_LOG_1 AGENT_TRAFFIC_LOG_2 BASIC_METADATA COMMAND COMPUTER_APPLICATION ENFORCER_CLIENT_LOG_1 ENFORCER_CLIENT_LOG_2 ENFORCER_SYSTEM_LOG_1 ENFORCER_SYSTEM_LOG_2 ENFORCER_TRAFFIC_LOG_1 ENFORCER_TRAFFIC_LOG_2 IDENTITY_MAP LAN_DEVICE_DETECTED LAN_DEVICE_EXCLUDED LEGACY_AGENT LOCAL_METADATA LOG_CONFIG REPORTS SEM_APPLICATION SEM_CLIENT SEM_COMPUTER SEM_JOB SEM_SVA_CLIENT SEM_SVA_COMPUTER SERVER_ADMIN_LOG_1 SERVER_ADMIN_LOG_2 SERVER_CLIENT_LOG_1 SERVER_CLIENT_LOG_2 SERVER_ENFORCER_LOG_1 SERVER_ENFORCER_LOG_2 SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 SERVER_SYSTEM_LOG_1 SERVER_SYSTEM_LOG_2 SYSTEM_STATE V_AGENT_BEHAVIOR_LOG V_AGENT_PACKET_LOG V_AGENT_SECURITY_LOG V_AGENT_SYSTEM_LOG V_AGENT_TRAFFIC_LOG V_DOMAINS V_ENFORCER_CLIENT_LOG V_ENFORCER_SYSTEM_LOG V_ENFORCER_TRAFFIC_LOG V_GROUPS V_LAN_DEVICE_DETECTED V_LAN_DEVICE_EXCLUDED V_SEM_COMPUTER	各テーブルから以下の列が削除されました。 RESERVED_INT1 RESERVED_INT2 RESERVED_BIGINT1 RESERVED_BIGINT2 RESERVED_CHAR1 RESERVED_CHAR2 RESERVED_VARCHAR1 RESERVED_BINARY

テーブル	列の変更
BINARY_FILE SERVER_POLICY_LOG_1 SERVER_POLICY_LOG_2 V_SERVER_POLICY_LOG	• CONTENT 列のタイプが「image」から「varbinary」に変更されました • FILESTREAM_ID インデックスが付いた列が追加されました • FILESTREAM_ID インデックスが追加されました • 以下の列が削除されました。 – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
INVENTORYREPORT	以下の列が追加されました。 • PRODUCTVERSIONFROM • PRODUCTVERSIONTO • IDS_VERSIONFROM • IDS_VERSIONTO
SEM_AGENT	• NTR_MESSAGE 列が追加されました。 • 以下の列が削除されました。 – RESERVED_INT1 – RESERVED_INT2 – RESERVED_BIGINT1 – RESERVED_BIGINT2 – RESERVED_CHAR1 – RESERVED_CHAR2 – RESERVED_VARCHAR1 – RESERVED_BINARY
SEM_AGENT_VERSION	以下の列が追加されました。 • VERSION • FORMATTED_VERSION • REFRESH_USN • AGENT_VERSION_FORMAT_REFRESH • VERSION1 • VERSION2 • VERSION3 • VERSION4
SEM_SVA	以下の列が削除されました。 • RESERVED_INT1 • RESERVED_INT2 • RESERVED_BIGINT1 • RESERVED_BIGINT2 • RESERVED_CHAR1 • RESERVED_CHAR2 • RESERVED_VARCHAR1
V_ALERTS	ENRICHED_DATA 列が追加されました。

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

Symantec Endpoint Protection 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。

Table 1: アップグレードの問題

問題	説明と解決策
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。 .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。「ネットワーク接続が利用できない場合 SEPM のインストールに失敗する」を参照してください。
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ます。	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。
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

問題	説明と解決策
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
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]
ネットワークトラフィックリダイレクト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 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ーに許可します。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。 トンネル方式は現在ベータ機能です。
14.2.x から 14.3 MP1 以降へのアップグレード後のエージェ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 [デバイス] 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。

問題	説明と解決策
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。 「SEP および SES がシマンテックのサーバに接続するために許可する URL」を参照してください 「クラウド管理の Symantec Agents をバージョン 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 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。

Table 3: Windows、Mac、Linux クライアントの問題

問題	説明と解決策
Symantec Agent for Linux インストーラ ログに誤ったメッセージが記録されます。 [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します。 [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。 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、以下を参照してください

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

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、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 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 (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 RTM、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 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ほかのアプリケーションの RAM 必要条件によって 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 以降) • Windows 10 20H2 (Windows 10 バージョン 2009) (14.3 RU1 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、バージョン 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)
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。 **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	インストール時に 1 GB 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 10.14 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。 • macOS 10.15 ~ 10.15.7 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 • 500 MB の RAM • /var、/opt、および /tmp が同じファイルシステム/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.x、7.x、8.x • Oracle Enterprise Linux 6.x、7.x、8.x • Red Hat Enterprise Linux 6.x、7.x、8.x • SuSE Linux Enterprise Server 12.x、15.x • Ubuntu 14.04 LTS、16.04 LTS、18.04 LTS、20.04 LTS バージョン 14.3 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 以前のリリースでサポートされている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 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」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 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。

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。
	• OpenSSL 1.0.2k-fips 以降
	• 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`

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。

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 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 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 および 11 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。 例外は、12.1.4 より前の Mac クライアントです。これは、12.1.4 以降にアップグレードするか、アンインストールする必要があります。

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

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

NOTE
Symantec Agent for Linux 14.3 RU1 は、Linux 用の古い Symantec Endpoint Protection クライアントを検出してアンインストールし、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.t 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

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。

注:

- 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。

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 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)
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