



Symantec Endpoint Security ソフトウェアアップグレード手順 オンプレミス版

SB C&S株式会社

全体目次

1. 本資料について
2. オンプレミスのSWアップグレード概要
3. SEPMアップグレード手順
4. クライアントアップグレード手順
5. アップグレードする際の考慮事項
6. Appendix

1. 本資料について

本資料について

本資料はBROADCOM社のプロダクトである、SES(Symantec Endpoint Security) の、ソフトウェアアップグレード実施手順について記載したものとなります。

オンプレミス環境での実施手順について記載しております。

2. オンプレミスのSWアップグレード概要

本項番ではオンプレミス構成におけるSWアップグレードの流れについて、説明いたします。大きく分けると下記2つの手順が発生します。

①SEPMアップグレード

オンプレミス構成の場合、まずは管理コンソールであるSEPMをアップグレード作業をする必要があります。

②エージェントアップグレード

SEPMのアップグレードを完了させたうえで、管理コンソールよりクライアント用のインストーラを作成し、

クライアントアップグレード方法について

クライアントアップグレードの方法は4通りあります。
それぞれの環境に合わせたアップグレード方法をご選択ください。

※Appendixとして手順の最後に詳細を載せております。

自動更新

中規模環境でシンプルなアップグレードスケジュールで実施する環境に向いています。

手動インストール

大規模環境でSEPMを経由せず、ユーザに手動で実施させる必要がある環境に向いています。

リモートプッシュ

小規模環境でSEPM経由で実施する環境に向いています。

メーカーサイトよりDL

スタンドアロン構成などでSEPMを構築しない場合にこの方法を利用します。

3. SEPMアップグレード手順

目次

3. SEPMインストール手順

- 3-1. SEPMバックアップ取得
- 3-2. SEPMサーバ証明書取得
- 3-3. SEPMの停止
- 3-4. SEPMインスーラダウンロード
- 3-5. SEPMアップグレード

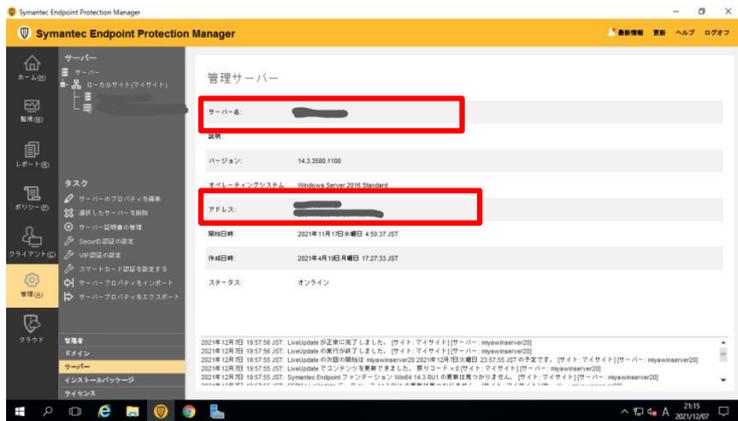
※

項番3-1と3-2はアップグレードを正常に行えなかった場合に、
切り戻しをするために必要な手順となります。

実施を強く推奨しますが、アップグレードに直接関与する手順ではございません。

3-1. SEPMバックアップ取得

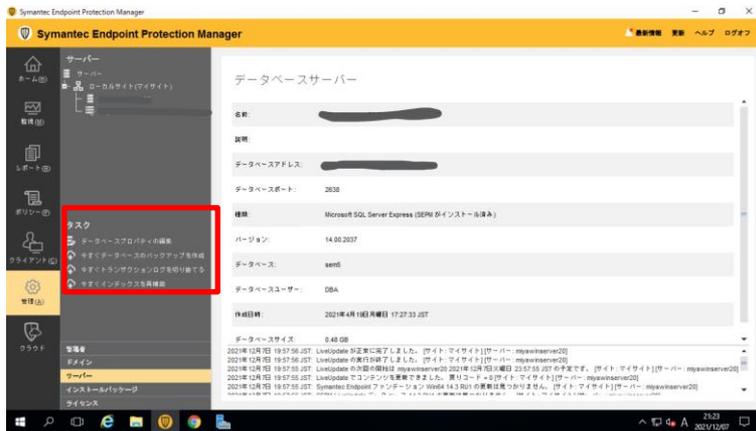
①



①

トップ画面⇒「管理」⇒「サーバ」の順に選択し、ローカルサイト(マイサイト)配下の管理サーバの欄にてIPアドレスとサーバ名をテキストなどに控えます。

②-1



②

同画面のマイサイト配下にて、データベースサーバーのホスト名を選択し、「タスク」⇒「今すぐデータベースのバックアップを作成」を選択します。

3-1. SEPMバックアップ取得

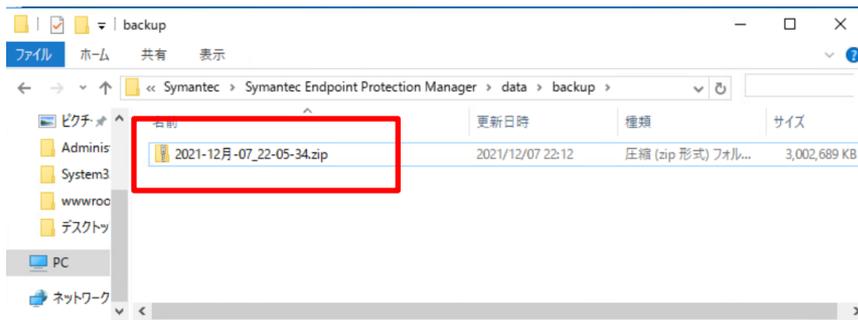
②-2



②-2

DBサーバのバックアップ取得は2とおり方法があり、端末のスタートメニューのアプリ一覧よりSEPMを選択し「データベースのバックアップと復元」を実行することでも取得が可能です。

③



③

所定のフォルダにバックアップが生成されたことを確認します。

3-2. SEPMサーバ証明書取得

①



①

トップ画面⇒「管理」⇒「サーバ」⇒「ローカルサイト」より管理サーバのホストを選択し、タスクより「サーバ証明書の管理」を選択します。

②



②

ウィザードが表示されるので、「次へ」を選択します。

3-2. SEPMサーバ証明書取得

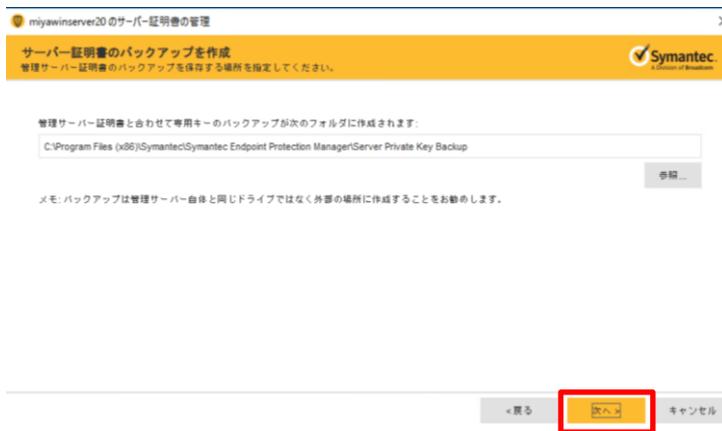
③



③

「サーバ証明書のバックアップを作成する」を選択し、「次へ」を選択します。

④



④

証明書の格納先を確認し、「次へ」を設定します。

3-2. SEPMサーバ証明書取得

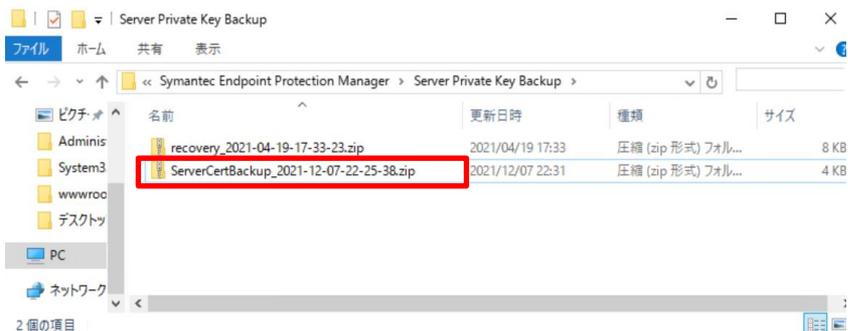
⑤



⑤

証明書が指定したフォルダに作成されます。
「完了」を選択します。

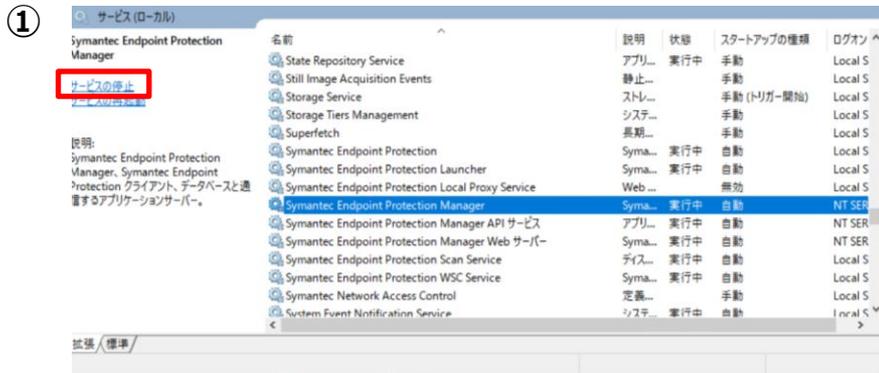
⑥



⑥

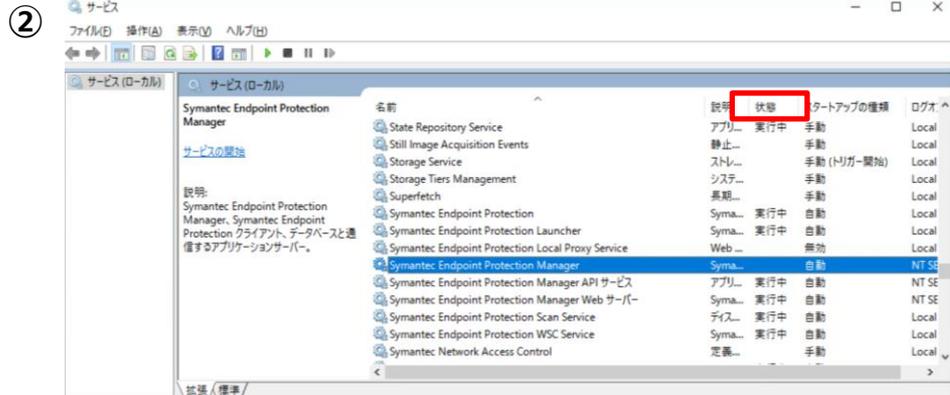
指定したフォルダにバックアップ証明書が生成されていることを確認します。

3-3. SEPMの停止



①

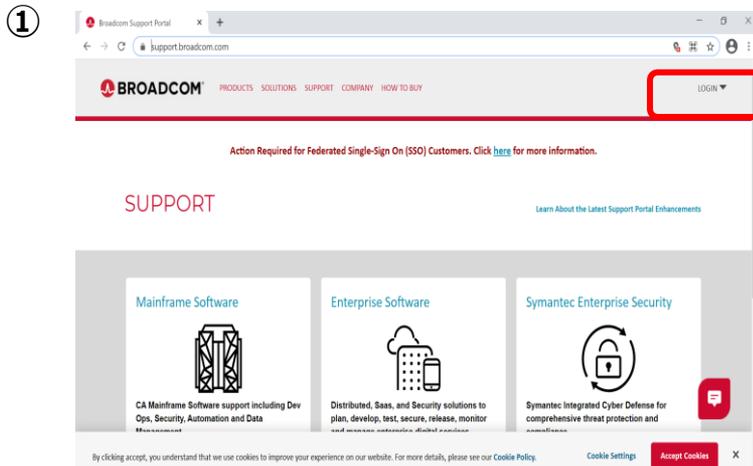
Windowsスタートメニューより、「管理ツール」⇒「サービス」の順に選択します。
サービス一覧より「Symantec Endpoint Protection Manager」を見つけサービスの停止を選択します。



②

「Symantec Endpoint Protection Manager」の状態のタブに実行中の表示がないことを確認します。

3-4. SEPMインストーラーダウンロード

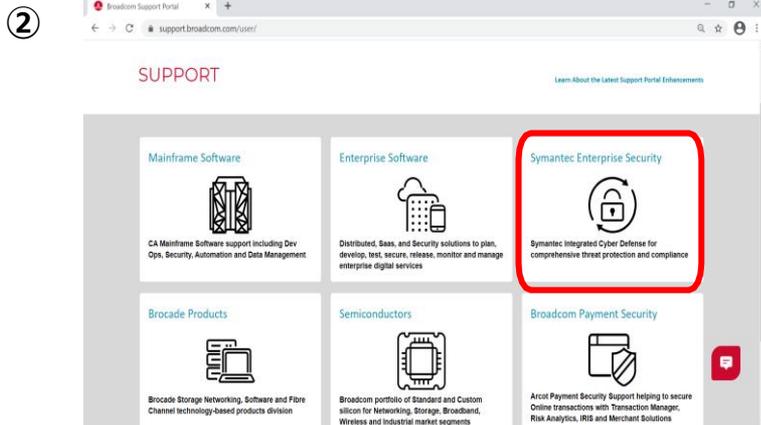


①

<https://support.broadcom.com/security/>
にアクセスし、
画面右上のLOGINよりサインインし
ます。

※

アカウント作成については完了しているもの
とします。
ブロードコムアカウントの作成が必要な場合
は、
別資料「ブロードコム登録手順.docx」をご
参照ください。

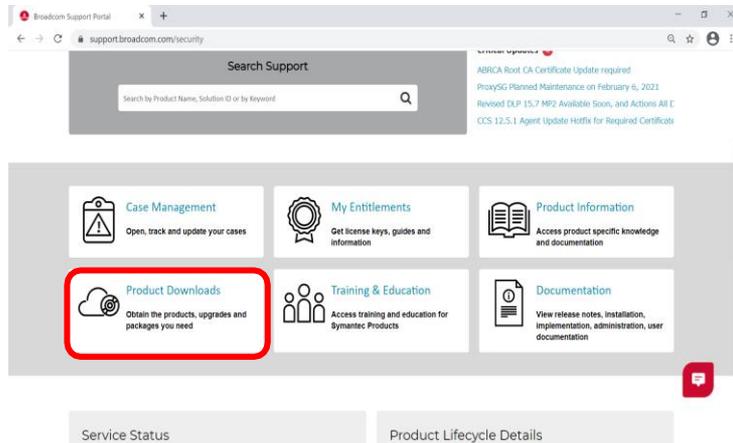


②

ダッシュボードよりSymantec
Enterprise Securityを選択します。

3-4. SEPMインストーラーダウンロード

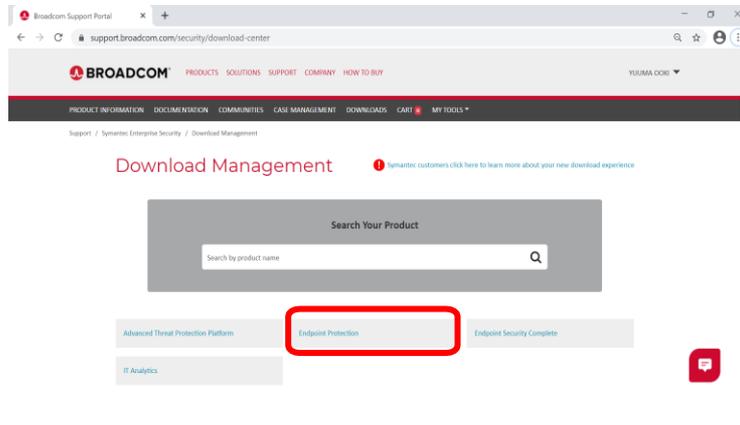
③



③

下記のダッシュボードが表示されるので、Product Downloadsを選択します。

④

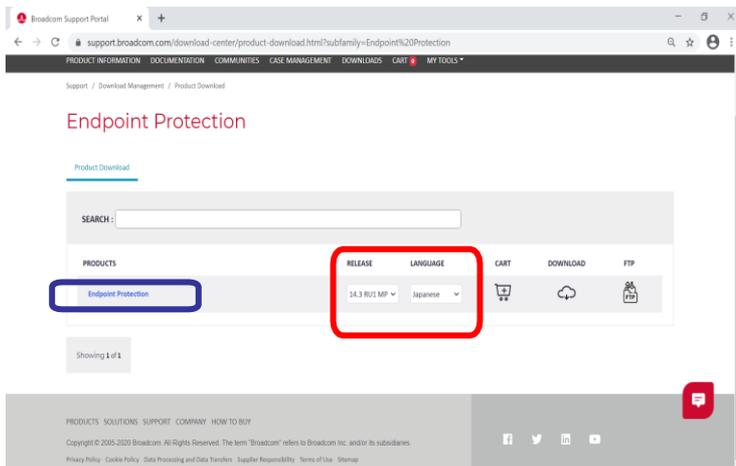


④

Download Managementのページが開かれます。選択肢よりEndpoint Protectionを選択します。

3-4. SEPMインストーラーダウンロード

⑤

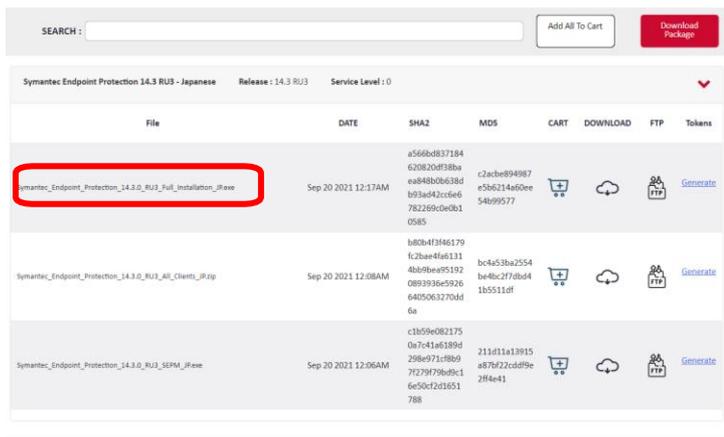


⑤

赤枠の部分でそれぞれ、
RELEASE→14.3 RU3
LANGUAGE→Japanese
を選択します。
その状態で青枠のEndpoint Protection
をクリックします。

※
本手順では14.3RU3へのアップグレードを
実施していますが、新バージョンがリリース
された場合は最新のバージョンの選択をお願い
いたします。

⑥



⑥

絞り込まれたインストーラーが表示され
ます。

Symantec_Endpoint_Protection_14.3.
0_RU3_Full_Installation_JP.exe
が該当するファイルとなります。(赤枠)
該当するファイルの欄にてDOWNLOAD
をクリックします。(右にある雲マーク)

3-5. SEPMアップグレード

①



①

3-1でダウンロードしたインストーラーを実行し、「Symantec Endpoint Protection Manager のインストール」をクリックします。

※

押下した後、実行されるまでに時間がかかる場合がございますが、そのままお待ちください。

②



②

「次へ」をクリックします。

3-5. SEPMアップグレード

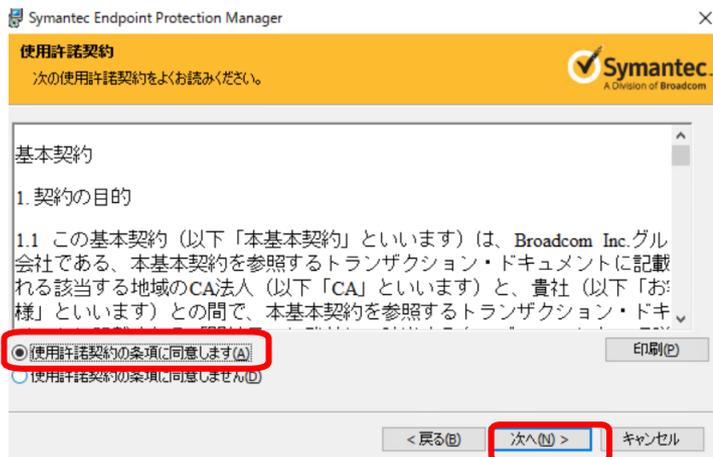
③



③

注意事項の内容を確認のうえ、「次へ」を選択します。

④

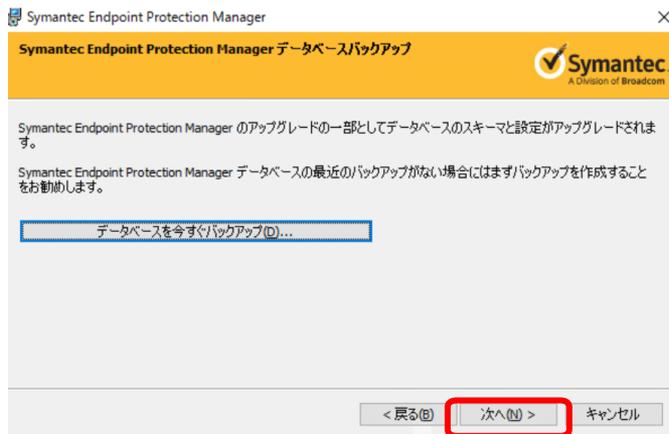


④

使用許諾を確認し、「同意します」を選択のうえ「次へ」を選択します。

3-5. SEPMアップグレード

⑤

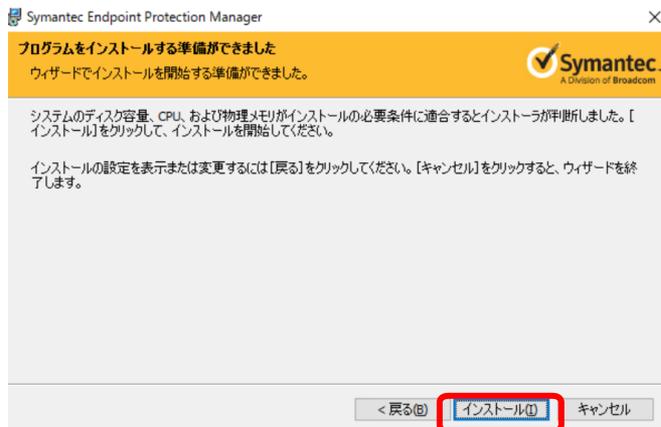


⑤

DBのバックアップを取得していない場合、ここで取得を推奨されます。完了している場合は「次へ」を選択します。

※ データベースのバックアップを実行する場合、セットアップは中段されるためバックアップ取得完了後に改めてセットアップウィザードを立ち上げる必要があります。

⑥



⑥

「インストール」を選択します。クリック後にインストール処理が走るので、完了するまで待ちます。

3-5. SEPMアップグレード

⑦



⑦

インストールが完了しアップグレードウィザードを開始します。「次へ」を選択します。

※
アップグレードウィザードの立ち上がりに時間がかかる場合がございます。

⑧



⑧

アップグレード対象バージョンを確認し、「次へ」を選択します。

3-5. SEPMアップグレード

⑨



⑨

アップグレードが開始されるので、完了するまで待ちます。

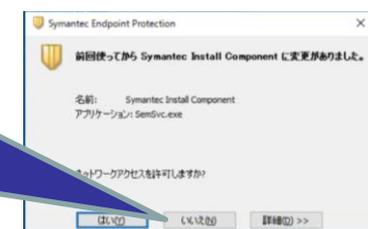
⑩



⑩

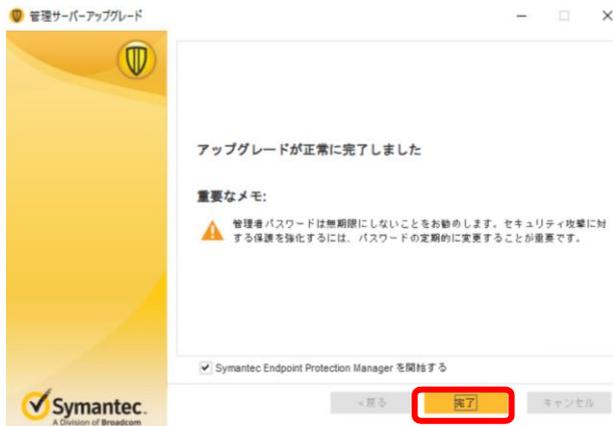
アップグレードが完了したら、「次へ」を選択します。

前回のインストールから変更のあるアプリケーションに対してアクセス許可を問われる場合がございますので判断のうえ「はい」「いいえ」をご選択ください。



3-5. SEPMアップグレード

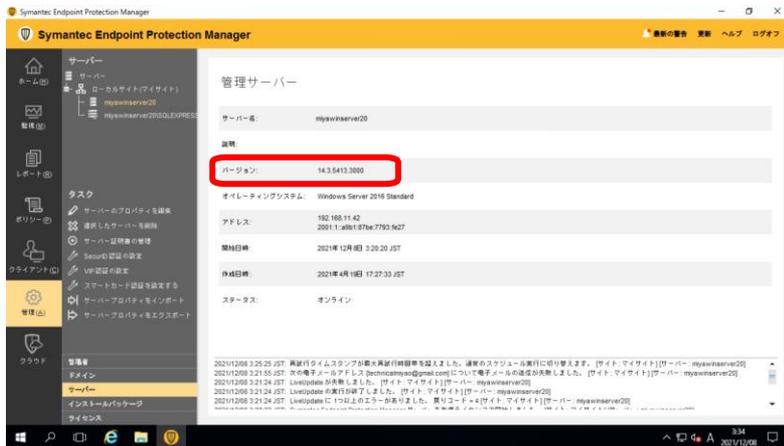
⑪



⑪

SEPMのアップグレードは完了です。
「完了」を選択し終了します。

⑫



⑫

管理コンソールログインし、
「管理」⇒「サーバー」を選択し、
マイサイトの管理サーバ側のホスト
名を選択することで実機上でも
バージョンを確認できます。

4. クライアントアップグレード手順

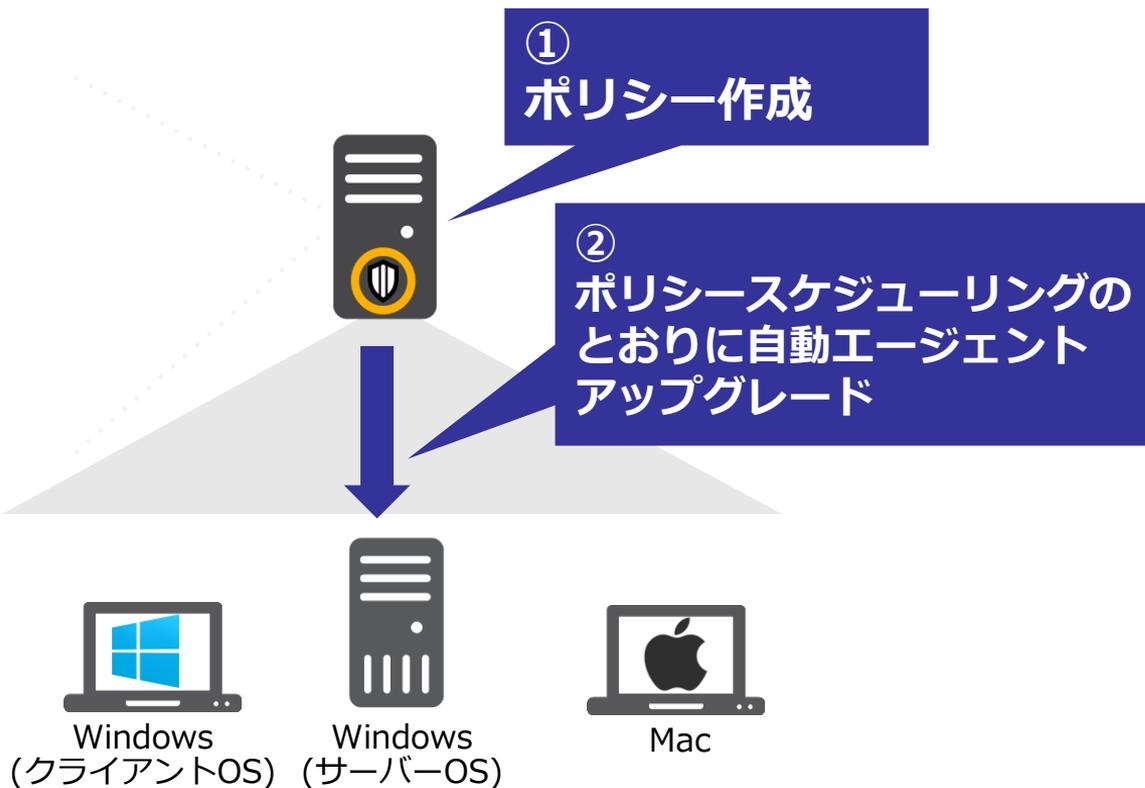
目次

4. SEPMインストール手順

- 4-1. 自動によるクライアントアップグレード
- 4-2. 手動によるクライアントアップグレード(パッケージエクスポート)
- 4-3. リモートプッシュによるアップグレード
- 4-4. メーカーサイトDLによるアップグレード

4-1. 自動クライアントアップグレード

自動SWアップグレードのイメージ



推奨環境

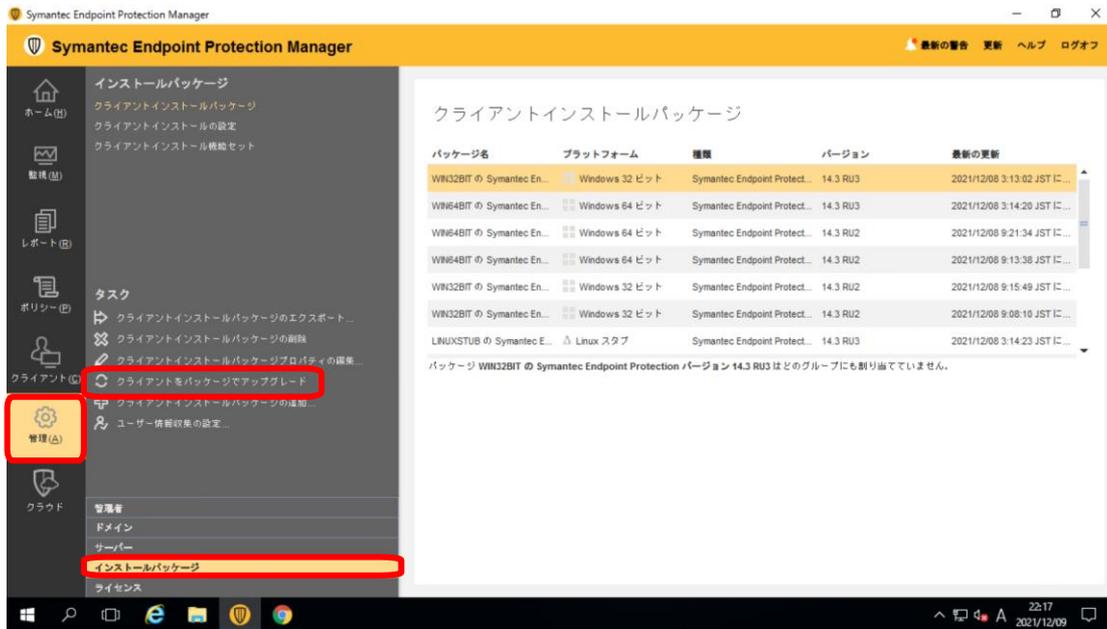
- ① 5000ユーザほどの中規模環境
- ② スケジュールや設定がシンプルなアップグレード計画

不向きな環境

- ① スピード感をもったアップグレードが必要な環境
- ② 詳細設定や複雑なスケジュールを利用する場合

4-1. 自動によるクライアントアップグレード

①



①

トップ画面より「管理」を選択します。

「インストールパッケージ」を選択します。

「クライアントをパッケージでアップグレード」を選択します。

4-1. 自動によるクライアントアップグレード

②



②

アップグレードウィザードが表示されるので、「次へ」を選択します。

4-1. 自動によるクライアントアップグレード

③



③

どのクライアントパッケージを使用するかを選択します。

「次へ」を選択します。

4-1. 自動によるクライアントアップグレード

④

グループのアップグレードウィザード

パッケージアップグレードの設定
ダウンロードの場所と拡張オプションを指定してください。

パッケージのダウンロード元を指定する:

管理サーバーからダウンロード

次の URL からダウンロード (http または https):

URL:

アップグレードの設定...

< 戻る 次へ > キャンセル

④

SEPMからダウンロードする場合、「管理サーバーからダウンロード」を選択します。

※
Webサーバーを利用する場合は、「次のURLからダウンロード」を選択し、URLを指定します。

「アップグレードの設定」を選択します。

4-1. 自動によるクライアントアップグレード

⑤

クライアントインストールパッケージの追加

全般 通知

バージョンの選択

このパッケージのバージョンを選択してください:

14.3.5413.3000

クライアントの設定

更新時に既存のクライアント機能を維持する

下で指定するクライアント機能と異なっている場合でも、更新時に既存のクライアント機能を保存します。以前のバージョンのクライアントで使用できない新しい機能は引き続きインストールされます。

使いたい機能を選択してください:

クライアントの完全保護

一部のプラットフォームではサポートされないセキュリティ機能があります。

インストールの設定:

Windows 向けのデフォルトの標準クライアントインストール設定

クライアントインストールパッケージに新しいコンテンツを含める

以前のバージョンでは提供されていなかった機能の新しいコンテンツを含めます。このオプションを選択すると、インストールパッケージのサイズが大きくなりますが、インストール直後からクライアントで最新のコンテンツを利用できます。クライアントインストールパッケージのサイズを小さくするには、このオプションの選択を解除してください。ただし、インストール後に新機能のコンテンツの取得が必要になります。

アップグレードスケジュール

開始: 00 : 00 終了: 23 : 59

アップグレードの配布期間: 0 日

OK キャンセル ヘルプ

「インストールの設定」

「インストールの設定」では3つからクライアントのモードを選択頂けます。詳細については下記URLをご参照ください。

<https://techdocs.broadcom.com/jp/ia/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Managing-a-custom-installation/preparing-for-client-installation-v16742985-d21e7/how-to-choose-a-client-installation-type-v116286636-d21e918.html>

※
クライアントモードを変更する場合は上書きができません。再インストールが必要です。

「アップグレードスケジュール」

開始時間と終了時間の指定が可能です。

配布期間を設定した場合、指定した期間内においてランダムにパッケージDLを行います。主に低帯域環境時の利用を想定した機能です。

スケジュール設定の詳細は下記URLをご参照ください。

※
日本語版のクライアントでは利用できない機能の記載もございます。

<https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/Client-Upgrade-Policy-Schedule.html>

4-1. 自動によるクライアントアップグレード

⑥

クライアントインストールパッケージの追加

全般 通知

ユーザーにアップグレードを通知するかどうかを指定します。

アップグレードの前にユーザーに通知する

通知メッセージ: デフォルトを使う

ユーザーによるアップグレード処理の遅延を許可する

ユーザーはアップグレード処理をある一定期間だけ遅延できます。ユーザーが選択できる時間範囲を指定してください。

最小時間: 30分

最大時間: 1日

OK キャンセル ヘルプ

「ユーザ通知」

アップグレード前にユーザにメッセージ通知が可能です。

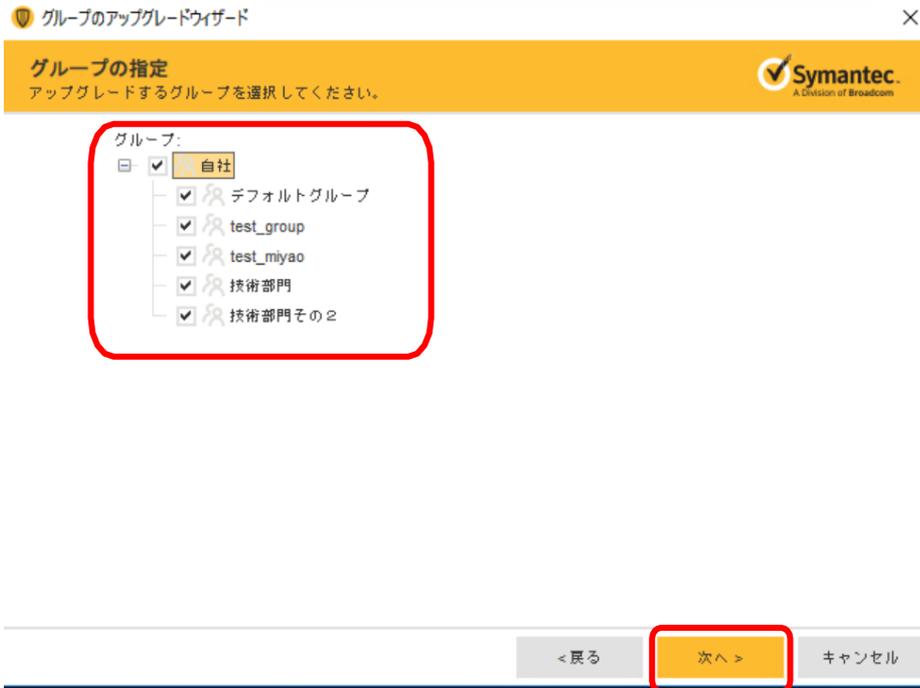
「アップグレード遅延許可」

ユーザ側にてのアップグレード処理遅延について最小と最大時間の指定が可能です。

設定項目について確認が完了したら、「OK」を選択します。

4-1. 自動によるクライアントアップグレード

⑦



⑦

自動アップグレードを有効化するグループにチェックを入れます。

「次へ」を選択します。

4-1. 自動によるクライアントアップグレード

⑧

⑧ グループのアップグレードウィザード

アップグレードパッケージを配備する準備ができています。
次の設定を選択しました:

Symantec
A Division of Broadcom

選択したグループ:
自社
デフォルトグループ
test_group
test_miyao
技術部門
技術部門その2

アップグレードの設定:
このパッケージのバージョン:
14.3.5413.3000
インストールの設定:
Windows 向けのデフォルトの標準クライアントインストール設定
アップグレード中、既存のクライアント機能を維持する。
管理サーバーからパッケージをダウンロードする。
アップグレードスケジュールが無効です。
アップグレード通知が無効です。
ユーザーによるアップグレード処理の延期を許可しません。
クライアントインストールパッケージに最新コンテンツを含めます。

選択したすべてのグループに現在の設定でパッケージを配備するには、[完了] をクリックします。
現在の設定の一部を変更するには、[戻る] を選択します。

< 戻る **完了** キャンセル

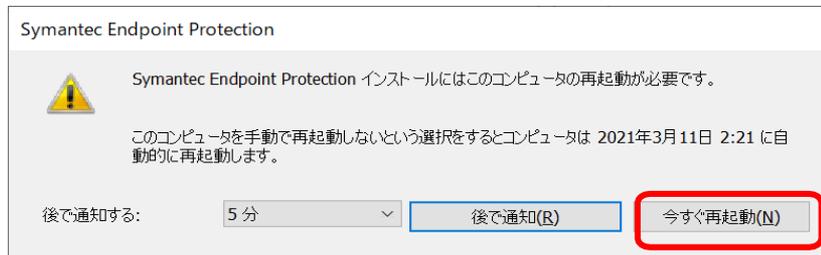
⑧

設定した内容の最終確認を行います。

「完了」を選択します。

4-1. 自動によるクライアントアップグレード

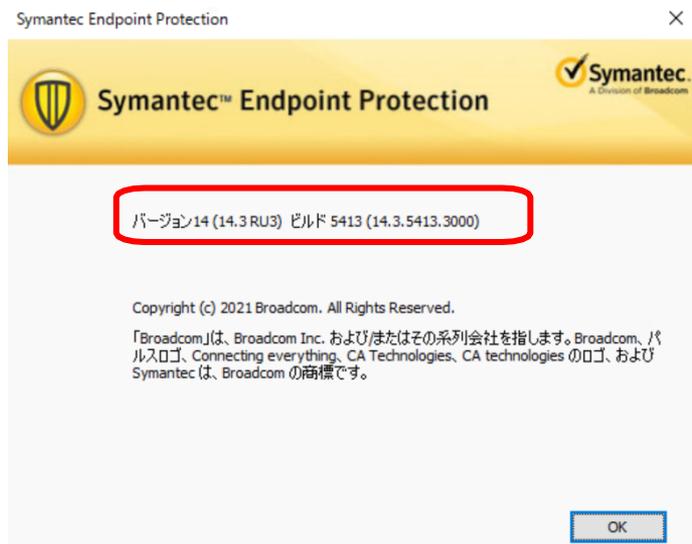
⑨



⑨

端末側で指定したスケジュールに基づき、再起動を促されます。本手順では「今すぐ再起動」を選択します。

⑩

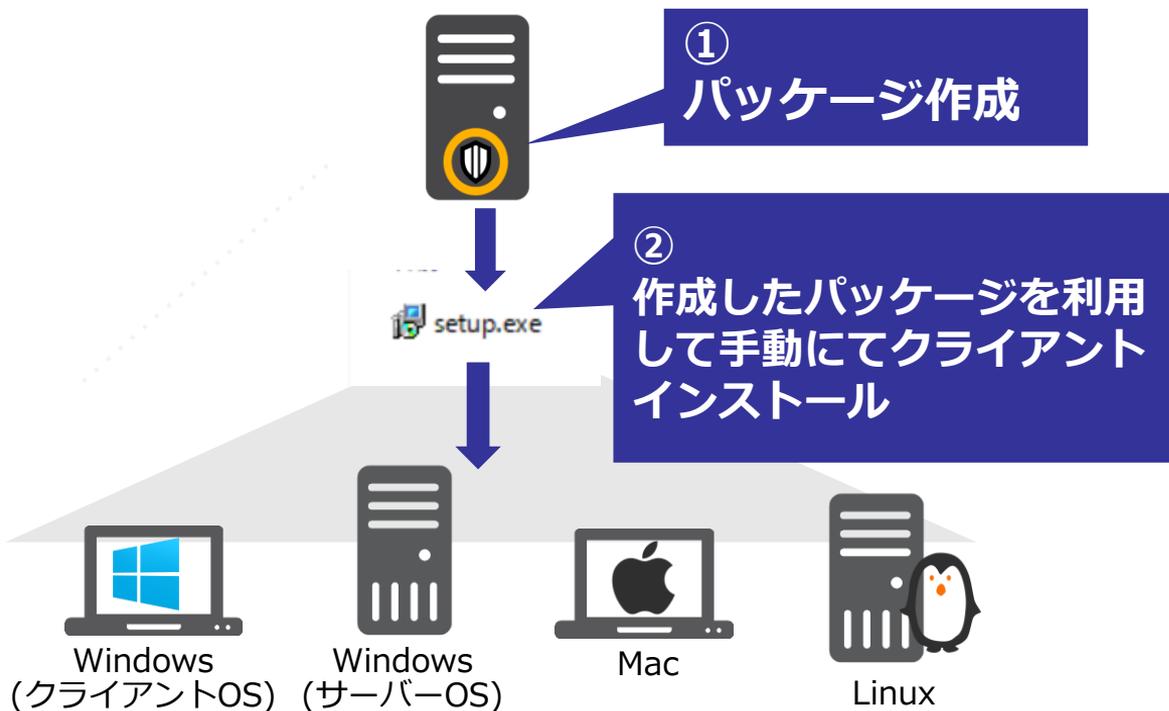


⑩

端末側でシマンテックを開き、「ヘルプ」⇒「バージョン情報」にて、端末のバージョン情報が確認できます。

4-2. 手動アップグレード(パッケージエクスポート)

手動SWアップグレードのイメージ



推奨環境

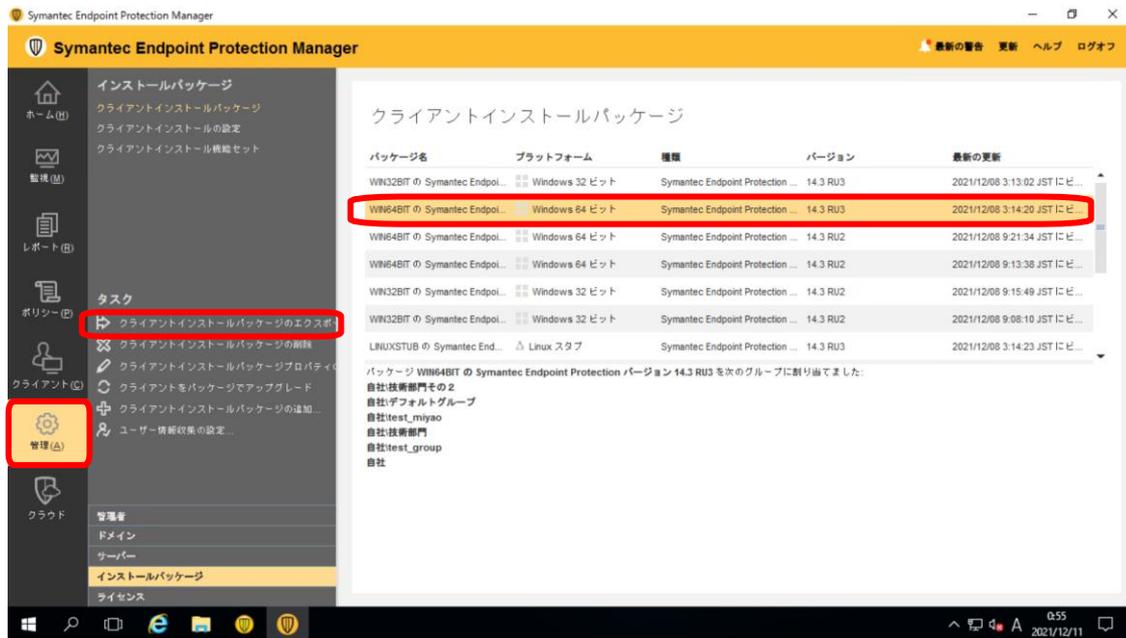
- ① 5000ユーザ以上の大規模環境
- ② サードパーティ製品連携によるアップグレードをする場合

不向きな環境

- ① クライアント側での作業が不可な環境
- ② SEPMでのみ運用している環境

4-2. パッケージエクスポートによるアップグレード

①



①

「管理」⇒「インストールパッケージ」を選択します。

エクスポートしたいパッケージ種別を選択します。

「クライアントインストールパッケージのエクスポート」を選択します。

②

パッケージのエクスポート: WIN64BIT の Symantec Endpoint Protection バージョン 14.3 RU3

エクスポートフォルダ: | 参照...

バージョンの選択
このパッケージのバージョンを選択してください:
14.3.5413.3000

インストール機能と設定
 更新時に既存のクライアント機能を維持する
このパッケージのセキュリティ機能を選択してください:
クライアントの完全保護
一部のプラットフォームではサポートされないセキュリティ機能があります。
このパッケージのインストール設定を選択してください:
Windows向けのデフォルトの標準クライアントインストール設定
 クライアントのインストールパッケージにウイルス定義を含める。
このオプションのチェックマークをはずして、ウイルス定義を含まないで他のすべてのコンテンツを含む、サイズの小さいクライアントインストールパッケージを作成します。クライアントがインストールされたらすぐにクライアントで LiveUpdate を実行して、ウイルス定義をダウンロードします。

エクスポートの設定
 管理下クライアントをエクスポート
 管理外クライアントをエクスポート
 パッケージを次のグループのポリシーと組み合わせてエクスポートする:
[+] 会社
- デフォルトグループ
- test_group
- test_miyao
- 技術部門
- 技術部門その2

ポリシーモード
コンピュータモードは保護コンピュータのすべてのユーザーにポリシーを適用します。ユーザーモードは保護コンピュータのログオンユーザーにポリシーを適用します。

OK キャンセル ヘルプ

②

「エクスポートフォルダ」でパッケージを出力する場所を指定します。

「インストールと機能の設定」では、端末種別に合わせた保護機能とクライアントモードの選択が可能です。定義ファイルをエクスポートパッケージに含めるかどうかの選択も可能です。

「ポリシーモード」ではポリシー適用をどのように行うか指定が可能です。

「エクスポートの設定」では、管理下クライアント/管理外クライアントの選択やどのデバイスグループのポリシーを踏襲するかの指定が可能です。

詳細については下記URLをご参照ください。

<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/Dialog-Overview/cs-admin-page-install-packages-v14650803-d21e4696/export-package-settings-v8429280-d21e5419.html>

4-2. パッケージエクスポートによるアップグレード

パッケージのエクスポート中...

メッセージ:

準備中...
グループ 自社\デフォルトグループ で作業中...
フォルダ C:\Users\Administrator\Desktop\自社_デフォルトグル
ープ管理サーバーリストを取り込んでいます...
管理サーバーからパッケージデータを取り込んでいます...

キャンセル

パッケージのエクスポート中...



正常に完了しました

メッセージ:

グループポリシーを保存しました...
グループの侵入防止ファイルを保存しました...

閉じる

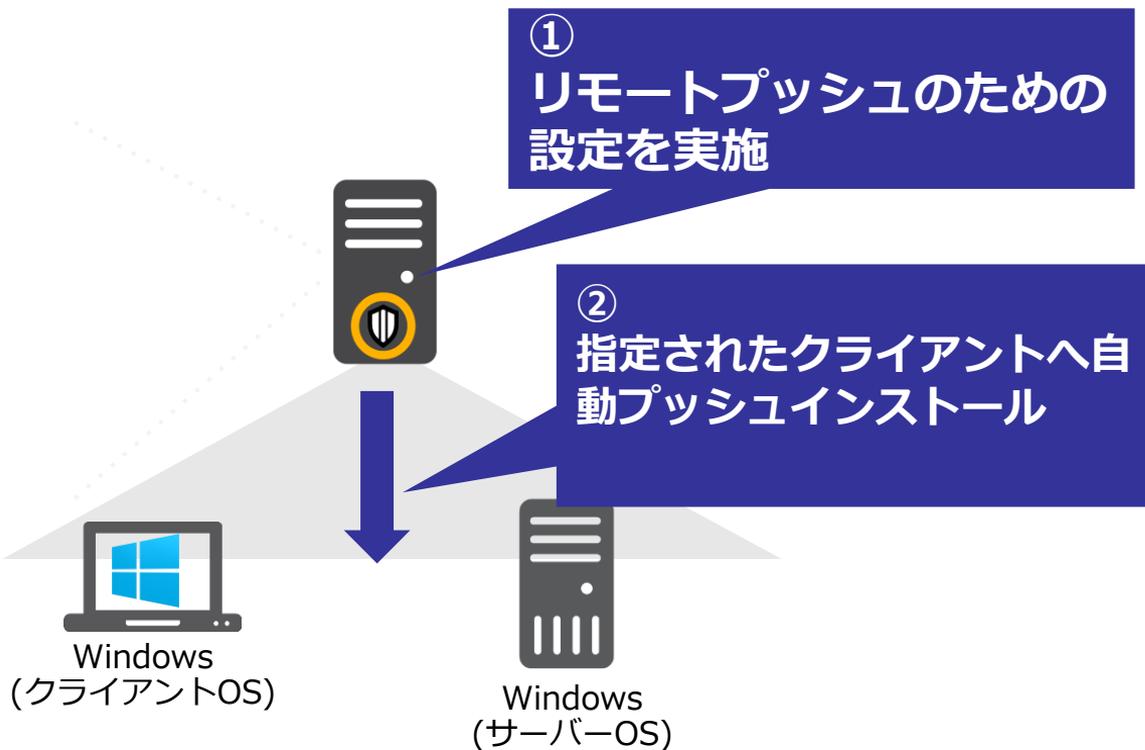


エクスポートの流れ

図の順にエクスポート処理が実行され、
処理が完了すると指定したフォルダにexeファイルが生成されます。

Exeファイルを実行して、アップグレードを実施します。

4-3. リモートプッシュによるアップグレード



推奨環境

- ① 250ユーザ未満の小規模環境
- ② Windowsクライアントのアップグレードを実施する場合

不向きな環境

- ① 大規模環境
- ② Windowsクライアント以外をアップグレードする場合

4-3. リモートプッシュ(クライアント配備ウィザード)によるアップグレード

①

The screenshot displays the Symantec Endpoint Protection Manager interface. The top navigation bar is orange and contains the Symantec logo and the text "Symantec Endpoint Protection Manager". On the left, there is a dark sidebar with icons for Home, Dashboard, Reports, Policies, Clients, Management, and Cloud. The main content area is divided into several sections:

- セキュリティの状態 (Security Status):** Shows a large green checkmark and the text "良好" (Good). Below it, a notification icon indicates "通知: 1".
- エンドポイントの状態 (Endpoint Status):** A donut chart shows the status of endpoints. A legend indicates: Symantec Endpoint Protection (2 total), 最新です (1), 最新ではありません (0), オフライン (1), 無効 (0), and ホストインテグリティの失敗 (0).
- ライセンス状態 (License Status):** Shows "ライセンス" (License) and "シマンテックセキュリティレスポンス" (Symantec Security Response).
- 活動の概略 (Activity Overview):** A table with columns for "ウイルス検出" (Virus Detection) and "エクスプロイト" (Exploit). The table shows various activities like "クリーニング/更新" (Cleaning/Update), "削除" (Delete), "検疫" (Quarantine), "疑いあり" (Suspicious), "新規感染" (New Infection), and "手解決感染" (Manually Resolved Infection).
- お気に入りレポート (Favorite Reports):** Lists reports such as "保護技術別のリスク分布" (Risk Distribution by Protection Technology) and "上位を占める攻撃の種別" (Attack Types that Dominate the Top).

In the top right corner, a "ヘルプ" (Help) menu is open, showing options like "トピックの検索" (Search Topics), "サポートへのお問い合わせ" (Contact Support), "Symantec Diagnostic Tool のダウンロード" (Download Symantec Diagnostic Tool), "コンソールログ" (Console Log), "ピアツーピア討論フォーラム" (Peer-to-Peer Discussion Forum), "「始めましょう」ページ" (Get Started Page), "新機能のページ" (New Features Page), and "バージョン情報" (Version Information).

①

トップ画面右上の「ヘルプ」⇒
「始めましょう」ページを開きま
す。

②

Symantec Endpoint Protection
を始めましょう

必須タスク
コンピュータを完全に保護するために次のタスクをただちに完了してください。

- 今すぐ LiveUpdate を実行します
前回のコンテンツダウンロード: 2021/12/11 1:12:34 JST
- ライセンスを追加
製品がアクティブになりました。
- コンピュータにクライアントソフトウェアをインストールします

共通のタスク
これらの共通のタスクによって、クライアントコンピュータの管理と保護を改善することができます。

- クラウドを起動する

このページを再び表示しない 閉じる

②

「コンピュータにクライアントソフトウェアをインストールします」を選択します。

4-3. リモートプッシュ(クライアント配備ウィザード)によるアップグレード

③

クライアント配備ウィザード

配備の種類を選択

① クリックしてクライアントのインストールツールを表示する

新しいパッケージ配備

サーバーからのパッケージを選択し、クライアントグループと機能を指定します。

既存のパッケージ配備

ハードディスクドライブ上にある以前にエクスポートしたパッケージから選択します。

参照...

通信の更新パッケージの配備

既存の Symantec Endpoint Protection クライアントのインストールで、通信設定を変更するパッケージを作成します。このオプションを使って、クライアントと Symantec Endpoint Protection Manager 間の通信を復元し、クライアントを新しい Symantec Endpoint Protection Manager に接続するか、または非管理対象クライアントを管理対象クライアントに変換します。

< 戻る 次へ > キャンセル

③

新しいパッケージを作成するか、既存のパッケージを流用するか選択します。

4-3. リモートプッシュ(クライアント配備ウィザード)によるアップグレード

④

クライアント配備ウィザード

グループとインストール機能セットの選択

インストールパッケージ: Windows - Symantec Endpoint Protection バージョン 14.3 RU3 - 日本語

バージョン: 14.3.5413.3000

この選択項目に含まれるもの:
WIN32BIT: Windows - Symantec Endpoint Protection バージョン 14.3 RU3 - 日本語 (21/12/08)
WIN64BIT: Windows - Symantec Endpoint Protection バージョン 14.3 RU3 - 日本語 (21/12/08)

グループ: 自社デフォルトグループ 参照...

インストール機能セット: クライアントの完全保護
ノートパソコンやデスクトップの場合に推奨 - すべての保護技術がインストールされます
一部のプラットフォームではサポートされないセキュリティ機能があります。詳しくは製品マニュアルを参照してください。

インストールの設定: Windows 向けのデフォルトの標準クライアントインストール設定 オプション...

< 戻る 次へ > キャンセル

④

インストールするパッケージ種別/
バージョン/所属させるデバイスグ
ループ/インストール機能/クライア
ントモードについて設定します。

設定事項を確認し、「次へ」を選
択します。

⑤

クライアント配備ウィザード

リモートコンピュータに Symantec Endpoint Protection をインストール
希望のインストール方法を選択してください。

パッケージの保存
実行可能なインストールパッケージを作成しますが、保護ソフトウェアをリモートコンピュータに配布しません。

リモートプッシュ
クライアントインストールパッケージを作成してパッケージをクライアントコンピュータにプッシュ型で転送します。パッケージはコンピュータ上に自動的にインストールされます。
? リモートプッシュインストールを準備するには

Web リンクと電子メール
ダウンロードの手順を電子メール通知でユーザーに送信できるようにクライアントインストールパッケージと電子メールテンプレートを作成します。
! Web リンクにより、指定した最新のインストールパッケージがインストールされます。ウィザードを再実行し、別のインストールパッケージを選択しても、Web リンクは最新のパッケージのみをリダイレクトします。同じグループに複数のインストールパッケージを割り当てることはできません。

< 戻る **次へ >** キャンセル

⑤

配備方法にて「リモートプッシュ」を選択します。

「次へ」を選択します。

4-3. リモートプッシュ(クライアント配備ウィザード)によるアップグレード

⑥

クライアント配備ウィザード

コンピュータの選択

クライアントインストールパッケージまたは通信設定を受信するコンピュータを選択します。



保護クライアントをインストールするコンピュータのネットワークを参照または検索します。

利用可能なコンピュータ:

ネットワークタイムアウトの設定...

保護クライアントのインストール先:

コンピュータ 種類 現在の保護

ネットワークの参照 ネットワークの検索

ホスト名	IP アドレス
192.168.11.7	192.168.11.7
192.168.11.9	192.168.11.9
192.168.11.5	192.168.11.5
192.168.11.16	192.168.11.16
192.168.11.17	192.168.11.17

検索された端末からリモートプッシュする対象を指定し矢印をクリック

コンピュータの検索

結果の消去

ヒント:Ctrl キーまたは Shift キーを押しながら

検索条件:

IPアドレス範囲

検索条件: 192.168.0.10
開始: 192 . 168 . 11 . 1
終了: 192 . 168 . 11 . 255

<戻る

次へ >

キャンセル

コンピュータ名または IP アドレス

テキストファイルからコンピュータリストをインポート (行ごとに1つのホストまたは IP アドレス)

検索するNWレンジの指定

OK

キャンセル

⑥

リモートプッシュする端末の検索には、「ネットワークの参照」と「ネットワークの検索」から選択できます。

本マニュアルとしては「ネットワークの検索」の検索イメージとなります。

4-3. リモートプッシュ(クライアント配備ウィザード)によるアップグレード

⑦

⑦ ログイン資格情報

Symantec Endpoint Protection をインストールするには
192.168.11.15 (192.168.11.15) クライアントコンピュータ上のデ
フォルト管理者アカウントを使う必要があります。

ログイン資格情報

ユーザー名:

パスワード:

ドメインまたはワーク
グループ:

OK キャンセル

⑦

端末指定する際にログイン情報を
求められるため入力します。

⑧

⑧ クライアント配備ウィザード

コンピュータの選択
クライアントインストールパッケージまたは通信設定を受信するコンピュータを選択します。

保護クライアントをインストールするコンピュータのネットワークを参照または検索します。

利用可能なコンピュータ:
ネットワークタイムアウトの設定...

保護クライアントのインストール先:

コンピュータ	種類	現在の保護
DESKTOP-0NDEVH	64 ビット	Symantec Endpoint Protecti...

ネットワークの参照 ネットワークの検索

ホスト名	IP アドレス
192.168.11.15	192.168.11.15
192.168.11.20	192.168.11.20
192.168.11.18	192.168.11.18
192.168.11.23	192.168.11.23
192.168.11.22	192.168.11.22

コンピュータの検索 結果の消去

ヒント: Ctrl キーまたは Shift キーを押しながら複数のコンピュータを選択できます。

<戻る 次へ > キャンセル

⑧

端末がセットできたら「次へ」を
選択します。

4-3. リモートプッシュ(クライアント配備ウィザード)によるアップグレード



⑨

内容を確認し「送信」をクリックします。



⑩

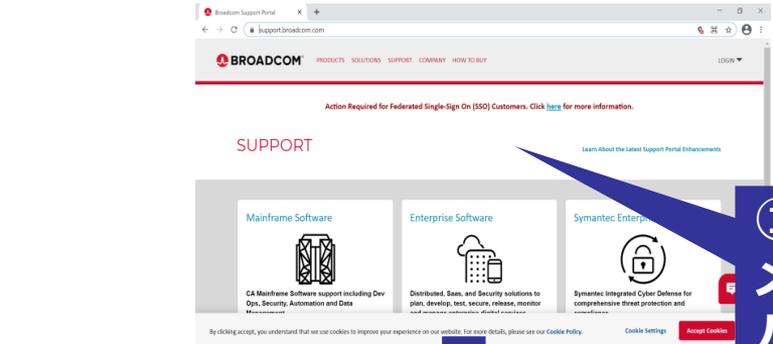
しばらく待つと送信ステータスが
表示されるので正常に完了したこ
とを確認します。

リモートプッシュの詳細について
は下記URLをご参照ください。

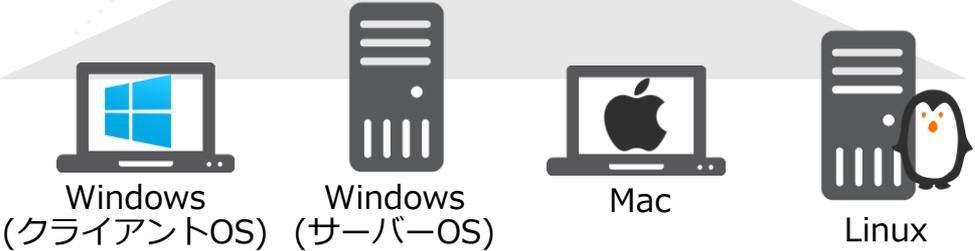
<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/getting-up-and-running-on-for-the-first-time-v45150512-d43e1033/installing-clients-with-remote-push-v16194683-d21e1695.html>

4-4. メーカーサイトDLによるアップグレード

メーカーサイトDLによるアップグレードのイメージ



①
メーカーサイトから
パッケージDL



②
作成したパッケージを利用して
手動にてクライアント
インストール

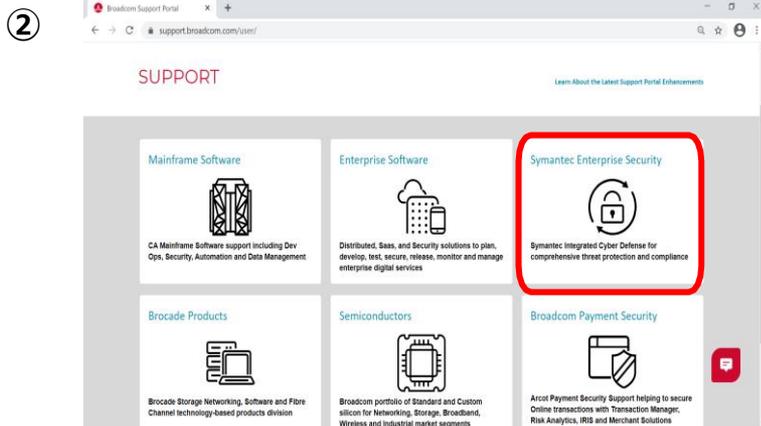
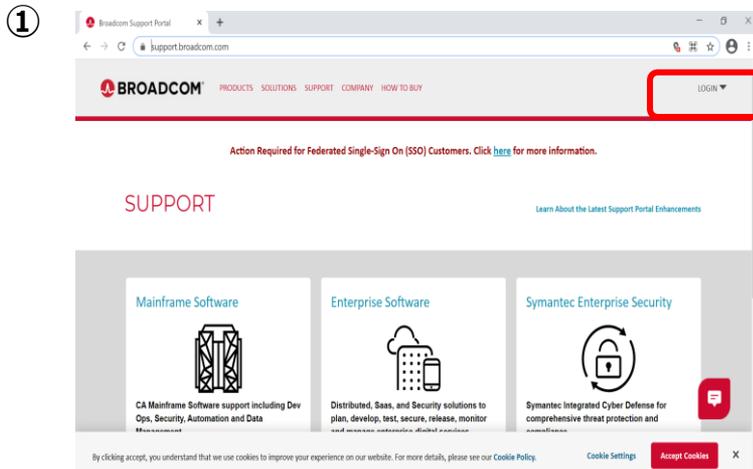
推奨環境

①
SEPMを利用しない環境
(スタンドアロン構成)

不向きな環境

①
SEPMを利用しない環境

4-4. メーカーサイトよりDL(スタンドアロン)



①

<https://support.broadcom.com/security/>
にアクセスし、
画面右上のLOGINよりサインインし
ます。

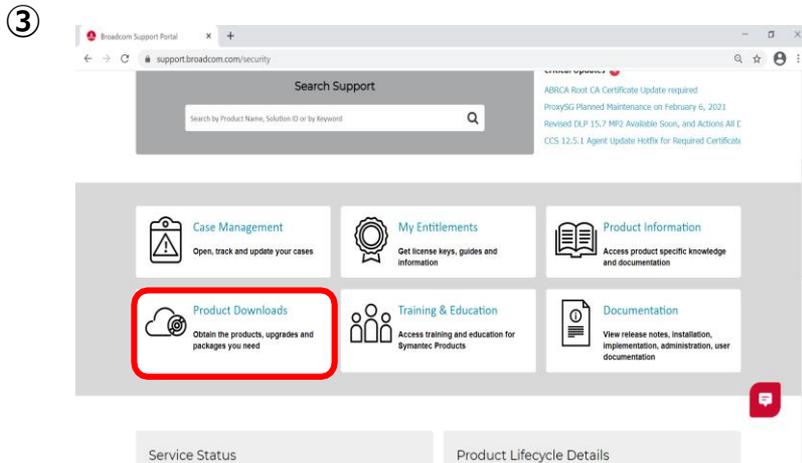
※

アカウント作成については完了している
ものとします。
ブロードコムアカウントの作成が必要な
場合は、
別資料「ブロードコム登録手順.docx」を
ご参照ください。

②

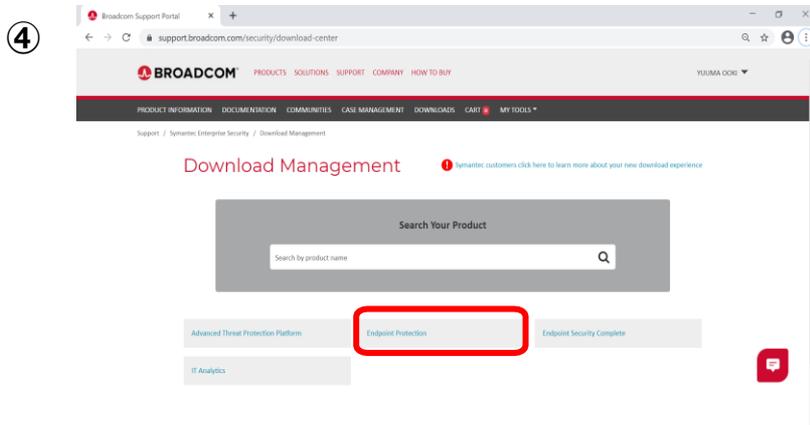
ダッシュボードよりSymantec
Enterprise Securityを選択します。

4-4. メーカーサイトよりDL(スタンドアロン)



③

下記のダッシュボードが表示されるので、Product Downloadsを選択します。

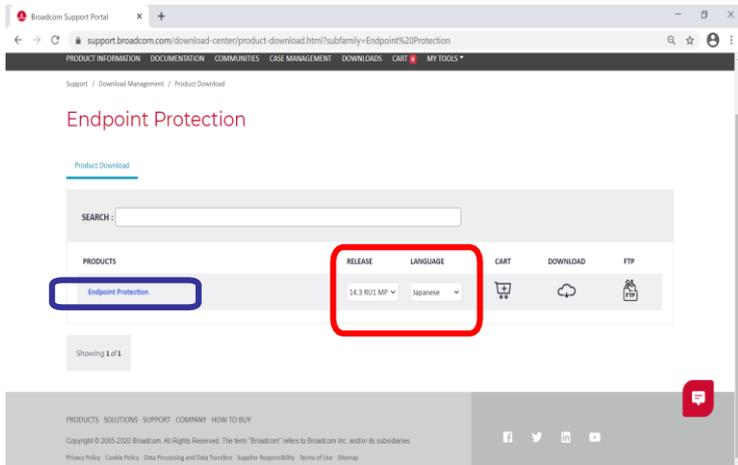


④

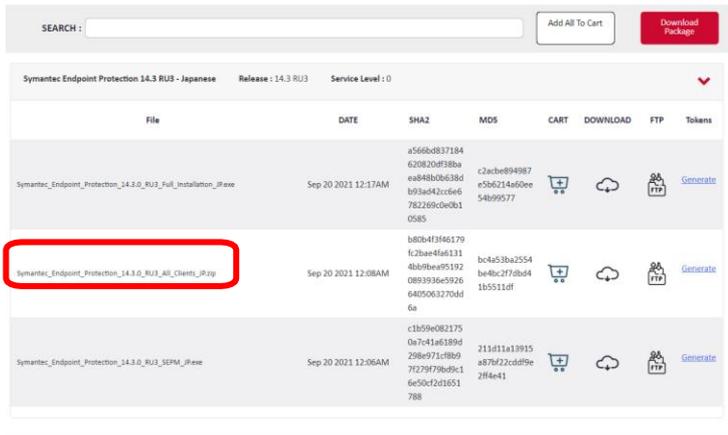
Download Managementのページが開かれます。選択肢よりEndpoint Protectionを選択します

4-4. メーカーサイトよりDL(スタンドアロン)

⑤



⑥



⑤

赤枠の部分でそれぞれ、
RELEASE→14.3 RU3
LANGUAGE→Japanese
を選択します。
その状態で青枠のEndpoint Protectionを
クリックします。

※
本手順では14.3RU3へのアップグレードを
実施していますが、新バージョンがリリース
された場合は最新のバージョンの選択をお願い
いたします。

⑥

絞り込まれたインストーラーが表示され
ます。

Symantec_Endpoint_Protection_14.3.
0_RU3_All_Clients_JP.zip
が該当するファイルとなります。(赤枠)
該当するファイルの欄にてDOWNLOAD
をクリックします。(右にある雲マーク)

5.アップグレードする際の考慮事項

目次

5.既存の製品からアップグレードする際の考慮事項

5-1. SEP14へのアップグレードについて

5-1-1.既存のSEPからのアップグレードパス(共通事項)

5-1-2.既存のSEPからのアップグレードパス(各OSごと)

5-2. その他の考慮事項

5-1. SEP14へのアップグレードについて

既存でsymantecをご利用頂いておりアップグレードする場合のシチュエーションについて次ページより各クライアントOSごとにまとめております。

下記は参照元のメーカーページとなりますので、合わせてご参考ください。

<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-protection/all/upgrading-to-a-new-release-v14510472-d27e6/supported-upgrade-paths-to-the-latest-version-of-1-v59311492-d27e869.html>

5-1-1.既存のSEPからSEP14へのアップグレードパス

共通事項(SEP14.xへの移行について)

SEPMに関して

- ① 埋め込みデータベースを使用するSEPMバージョン12.1.6MP10以降は、Microsoft SQL Server Expressデータベース、バージョン14.3RU1MP1にシームレスにアップグレードされます。12.1.6 MP9以前のバージョンから14.3RU1MP1への直接アップグレードはできません。
- ② 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OS、および 32 ビット版OS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。

SEPクライアントに関して

- ① SEP14.xクライアントは、サポート対象のOS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のクライアントバージョンを直接アップグレードできます。例外は12.1.4以前のMac版クライアントです。こちらは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。※最新ver.への移行については次のページからの各OSごとのリストをご参照ください。

5-1-2.既存のSEPからSEP14へのアップグレードパス

新バージョンへ直接アップグレードが可能なバージョン

OS	バージョン
Windows	<ul style="list-style-type: none">・ 11.x、Small Business Edition 12.0(Symantec Endpoint Protectionクライアントのみ、サポート対象OSの場合)・ 12.1.6MP10までの12.1.xバージョン・ 14、14MP1、14MP2・ 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
Mac	<ul style="list-style-type: none">・ 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、14.3 RU1
Linux	<ul style="list-style-type: none">・ 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、14.3 RU1

5-2. その他の考慮事項

SEP14.xにてサポートが終了となった機能や考慮が必要な項目について、概要を記載しておりますためご参考ください。

SEPMに関して

- ①SEPMは、Windows Server 2003、32ビットOS、またWindowsXPを含むデスクトップOSのサポートを終了。
- ②SEPMデータベースはMicrosoftSQL Server2005のサポートを終了。
- ③SEPMは、バージョン11.xまたはSmall Business Edition (SBE) 12.0からの移行をブロックします。
- ④SEPMは、11.xクライアントパッケージをインポートまたは作成しません。
- ⑤SEPMは11.xコンテンツをダウンロードしません。
- ⑥SEPMの移行により、管理サーバーデータベースから11.xコンテンツが削除されます。
- ⑦SEPMは、vShield対応のShared Insight Cache (VSIC) およびSecurity Virtual Appliance (SVA) のサポートを終了。

※11.xのサポート終了に伴うアナウンス機能追加

- ・11.xクライアントを管理するSEPMは、サポートされていないクライアントについて通知する通知をSEPManager管理者に送信するようになりました。

SEPクライアントに関して

- ①Windows用のSEPクライアントは、Windows XP、Windows Server 2003および、Windows Embedded Standard2009などのWindowsXPに基づくバージョンのWindowsEmbeddedのサポートを終了。

詳細につきましては下記参照元URLをご参照願います。

<https://knowledge.broadcom.com/external/article/150312>

6. Appendix

アップグレード方法	推奨される環境	不向きな環境
<p>自動更新 「グループのアップグレードウィザード」を使用 比較的小規模な環境に推奨</p>	<ul style="list-style-type: none"> ○ クライアントの数が 5,000 以下のように、比較的少ない場合。 ○ ユーザーの作業を中断しないように実行する必要がある場合。 ○ SEPM を使用してアップグレードする場合。 ○ よりシンプルなアップグレードを行いたい場合。 	<ul style="list-style-type: none"> ○ グループ単位でアップグレードの設定を行うため、グループの数が多いため、工数と時間がかかる場合があります。 ○ アップグレードのスケジュールを複雑で詳細に設定する必要がある場合。
<p>手動インストール 大規模な環境に推奨</p>	<ul style="list-style-type: none"> ○ SEPMを使用せずに手動でクライアントパッケージをアップグレードしたい場合。 ○ 既存のサードパーティ製品を使用してクライアントパッケージをアップグレードしたい場合。 	<ul style="list-style-type: none"> ○ SEPMを使用してのみ運用を行う環境。
<p>リモートプッシュ 小規模な環境に推奨</p>	<ul style="list-style-type: none"> ○ クライアントの数が、250 未満など、比較的少ない場合。 ○ SEPM を使用してアップグレードしたい場合 ○ よりシンプルにアップグレードをする必要がある場合。 	<ul style="list-style-type: none"> ○ 大規模なネットワーク環境の場合。
<p>メーカーサイトDL スタンドアロン</p>	<ul style="list-style-type: none"> ○ SEPMを利用しない環境 	<ul style="list-style-type: none"> ○ SEPMを利用する環境。

 SB C&S