



# Symantec Endpoint Security SEP⇒SES移行ガイド

- ・本資料はSymantec Endpoint Protection(SEP)から後継製品であるSymantec Endpoint Security(SES)へ移行する際の手順となります。

## 改訂履歴

版数	改訂日	内容
第1版	2022/1/31	第1版として公開
第1.1版	2022/8/30	以下点を改定 <ul style="list-style-type: none"><li>・SEPMポリシー移行の項番を「2.3」⇒「2.2」に変更</li><li>・クライアント移行の項番を「2.2」⇒「2.3」に変更</li><li>・P18の内容を編集</li><li>・P39、P40の内容を追加</li></ul>

# アジェンダ

## 1. Symantec Endpoint Securityとは

## 2. SEP⇒SES移行手順

2.1対象クライアント確認

2.2SEPMポリシー移行

2.3クライアント移行

-2.3.1Switch機能で移行

-2.3.2インストーラーで手動インストール

-2.3.3smcコマンドで移行

-2.3.4ホストインテグリティポリシーで移行

## 3. ハイブリッド構成手順

3.1トークンの登録

3.2デバイス管理

3.3ポリシー管理

## 4. Appendix



# Symantec Endpoint Security (SES)

The background of the slide features a central image of a hand holding a large, glowing cyan padlock. This central image is overlaid on a series of concentric, dotted cyan circles. The words "CYBER SECURITY" are written in a light cyan font, curving along the inner edge of these circles. The entire scene is set against a dark blue background with a network of glowing cyan lines and nodes, creating a digital or cyber-themed atmosphere.

**Symantec Endpoint Protection (SEP) の後継製品  
管理コンソールがクラウドに集約**

# MITER ATT&CKチェーン全体をカバー



違反のシミュレーションとレポート、脆弱性評価とパッチ適用	デバイス制御アプリ制御分離ポリシー	セキュアな接続	エクスプロイト保護/侵入防止	クラウドレピュテーション分析	高度な機械学習	CP3 スクリプトエミュレーター	メモリエクスプロイト緩和	振り舞い監視	ディセプション	Active Directory セキュリティ	ネットワークファイアウォールと侵入防止
違反のシミュレーションとレポート、脆弱性評価とパッチ適用	ファイル、レジストリ、デバイスのアクセス制御。アプリケーションのホワイトリスト、実行制限	自動VPNとの通信を安全保護することによる、中間者攻撃を防止	既知の脆弱性の悪用をブロック	コミュニティの知恵を使用してファイルやウェブサイトの安全性を決定	新規および進化する脅威の実行前の検出	スクリプトベース脅威への実行前の動作分析 (VB, Java, Powershell)	未知の脆弱性に対するゼロデイエクスプロイトをブロック	不審な動作を示すファイルやNON PE ファイル、DLL サイドローディングの監視とブロック	攻撃者をだますことでセキュリティ侵害を特定	資格情報の誤用による横断攻撃拡大防止	アウトバンド C&Cトラフィックを情報流出防止のためにブロック

**検出 & 対処** - フライトデータレコーダー (Flight Data Recorder) | 振り舞いフォレンジックス | 標的型攻撃クラウド分析 | Threat Hunter 分析

**グローバルインテリジェンスネットワーク** - 世界最大の民間脅威インテリジェンス 数十億のクエリ/日で全ての保護と検出を強化

**サイバー防御の統合** - シマンテックとサードパーティのSIM / TIP / SOARとの統合

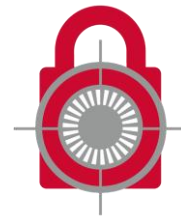
# エンドポイントセキュリティ エンタープライズとコンプライート

クラウドシフトや  
モバイル保護を検  
討中



EDRや防御+も含めた  
多層防御を実現したい

Symantec Endpoint Security  
Enterprise



Symantec Endpoint Security  
Complete

エンドポイントの保護

モバイル対応

クラウド対応

Symantec Endpoint Security Enterprise

+

Endpoint Detection and Response (EDR)

脅威ハンター

Active Directory の脅威対策 (TDAD)

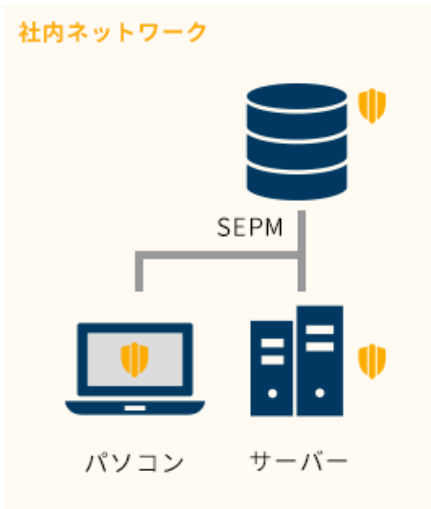
アプリケーション制御と隔離

# SESなら様々な運用パターンが可能

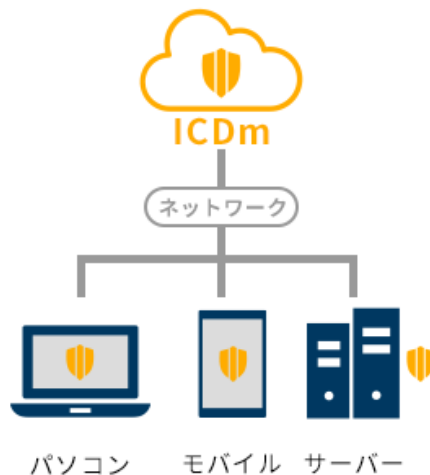
オンプレミス、クラウドまたはハイブリッドで管理可能

※現在のSEPの運用をそのままご利用いただく事も可能です。

## オンプレミスで管理

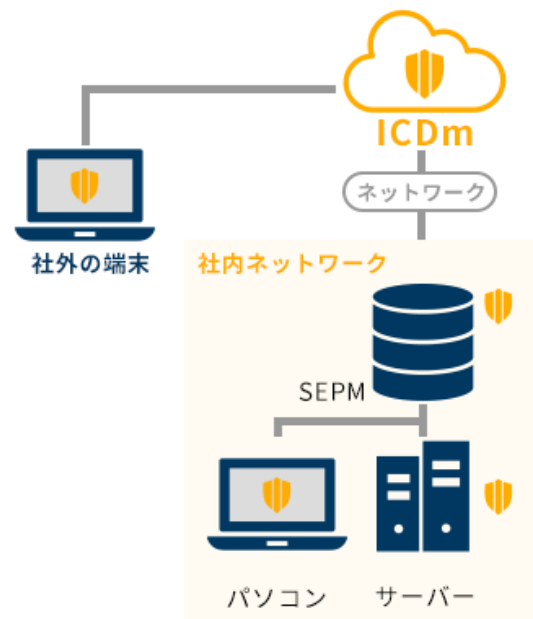


## クラウドで管理



社内・社外のネットワークは  
問わずクラウドで一斉管理

## ハイブリッドで管理



# パターン別管理方法

オンプレミス管理、ハイブリッド管理、クラウドのみ管理の3パターンにてそれぞれ管理方法を選択可能です。

## オンプレミス管理

### Symantec Endpoint Protection Manager (SEPM)

- Symantec Endpoint Protection
- Symantec Endpoint Security Enterprise
- Symantec Endpoint Security Complete

## クラウド管理

### Symantec Integrated Cyber Defense Manager (ICDm) (統合クラウドコンソール)

- Symantec Endpoint Security Enterprise
- Symantec Endpoint Security Complete

## ハイブリッド管理

### ICDm + SEPM ※SEPMへICDmドメインの追加が必要

- Symantec Endpoint Security Enterprise
- Symantec Endpoint Security Complete



# 用語について

本マニュアル内のマネージャーおよびエージェントの呼称について、以下にまとめさせていただきます。

## マネージャー名称

- **SEPM ( Symantec Endpoint Protection Manager )**  
オンプレミス構成でエージェントを管理するコンソールとなります
- **ICDm (Integrated Cyber Defense Manager)**  
クラウド直の構成でエージェントを管理するコンソールとなります

## エージェント名称

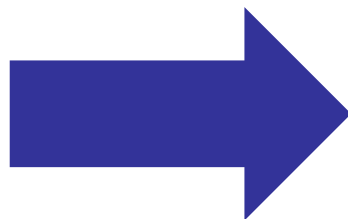
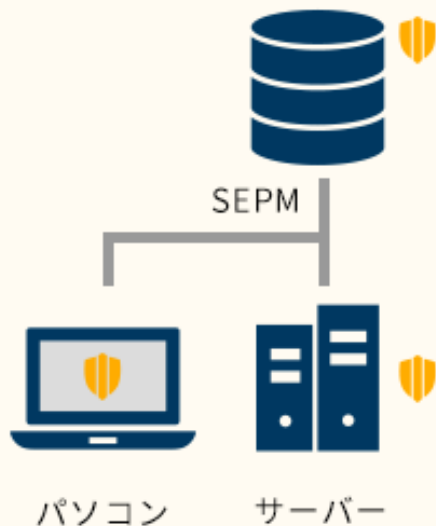
- **SEP**  
SEPM配下にて管理するエージェントの呼称です。  
名称はSEPとなっておりますが、SEPM配下で管理するSESエージェントとなります。
- **SES**  
ICDmに直管理されているエージェントの呼称です。

## 2. フルクラウド移行手順

# フルクラウドへ移行

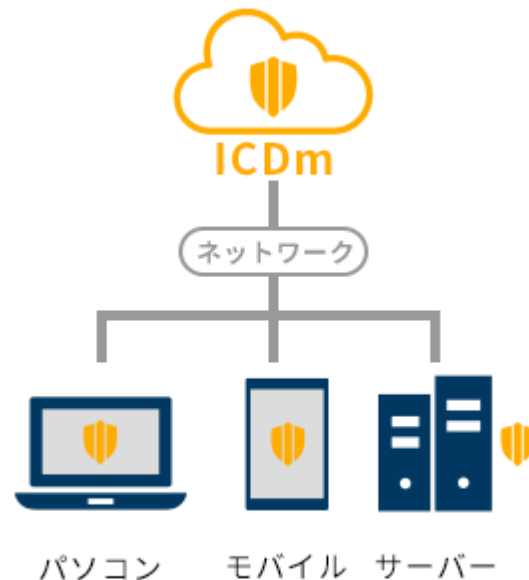
オンプレミスで管理

社内ネットワーク



管理をSEPM  
からICDmへ

クラウドで管理



社内・社外のネットワークは  
問わずクラウドで一斉管理

# フルクラウドへ移行

クラウドへ移行するには以下プロセスが必要となります。

1

対象クライアント確認

2

SEPMポリシー移行

3

クライアントインストール

# フルクラウドへ移行

クラウドへ移行するには以下プロセスが必要となります。

1

対象クライアント確認

2

SEPMポリシー移行

3

クライアントインストール

# 2.1対象クライアント確認

①



①

エージェントが現在、SEPM配下で管理されているか確認します。

クラウド (ICDm) へ移行すると管理先がクラウドへ変更されます。

## 確認方法

Symantec Endpoint Protectionを開き、「ヘルプ」>「トラブルシューティング」>「管理」から確認可能です。



# フルクラウドへ移行

クラウドへ移行するには以下プロセスが必要となります。

1

対象クライアント確認

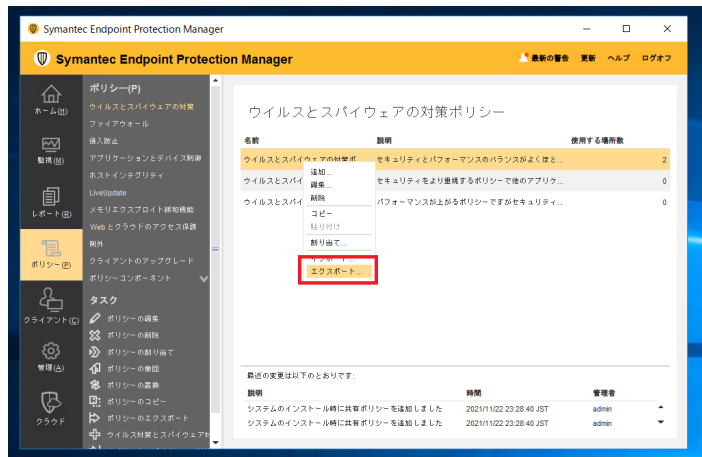
2

SEPMポリシー移行

3

クライアントインストール

## 2.2ポリシー移行



• SEPMで利用していたポリシーをICDmへ移行することが可能です。

• 本章では、クラウドシフトする際に既存のSEPMで設定したポリシーを継続して利用されたい方向けの手順となります。

SOFTBANK C & S CORP ユイチ

The screenshot shows the ICDm interface with a table of policies. The 'Import Policy' button is highlighted with a red box. The table has columns for 'VERSION', 'DEVICES', 'DEVICE GROUPS', and 'POLICY GR'. The table contains three rows of data.

VERSION	DEVICES	DEVICE GROUPS	POLICY GR
1	0	0	0
6	2	1	0
1	0	0	0

## 2.2ポリシー移行

- SEPMで利用していたポリシーはICDmへインポートが可能です
- SEPMのポリシーはSESでは以下ポリシーの種類に分類されます

SEP（オンプレ）移行前ポリシー	SES（クラウド）移行後ポリシー
ウイルスとスパイウェアの対策	マルウェア対策
ファイアウォール	ファイアウォール
侵入防止	Intrusion prevention
アプリケーションとデバイス制御	デバイス制御
LiveUpdate	システム
メモリエクスプロイト緩和機能	エクスプロイト対策
例外	・ブラックリスト ・ホワイトリスト

### ■ポリシー移行に関する注意点

#### エクスポートされるSEPMのポリシーについて

- ・ エクスポートされるSEPMのポリシーは.DATファイル形式でございます。  
他のファイル形式はサポートされておりません。
  - ・ 1度に最大50個のポリシーをインポートできます。
  - ・ サポートされているSEPMポリシーのバージョンは12.1.6以降となります。
- 
- ・ SEPMで使用していたポリシーをクラウドに取り込む際の詳細サポート情報について、一部移行できない設定がございます。（例：ユーザー定義設定されたポリシー）その場合、ICDm管理画面上で手動設定する必要があります。  
SEPMとICDmの詳細なポリシー差に関する情報は下記をご確認ください。

<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Upgrading/importing-policies-from-v132403022-d4155e11046.html>

## 2.2ポリシー移行

### ■ポリシー継承について

- SESのデバイスグループは親グループ⇒子グループでポリシーが継承されます。
- SESは「Default」が親グループの役割を果たし、デフォルトでポリシーが割り当てられています。

エンドポイント

管理対象デバイス 管理外デバイス デバイスグループ

グループ階層

- Default 0
- test 0
- test\_tech 0

Default  
デバイスグループ名

管理対象デバイス

クイックフィルタ

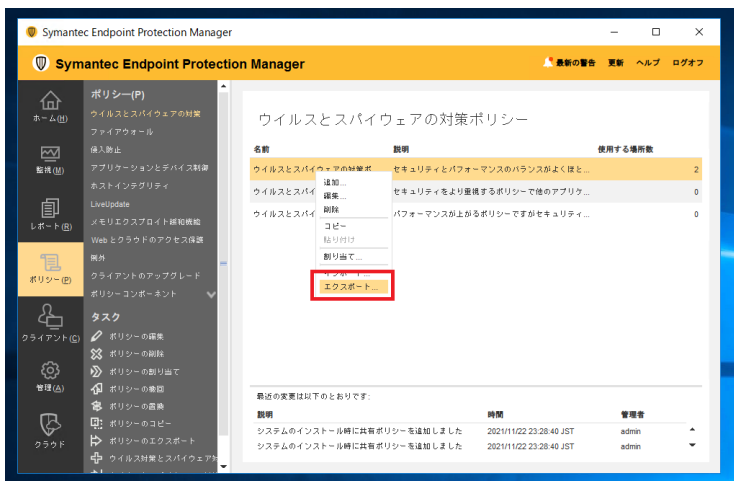
デバイスのリストを表示 (0 ~ 0 / 0 を表示)

<input checked="" type="checkbox"/> 名前 ↑	ログインユーザー	OS	OS のバージョン	クライアントのバージョン	IP
--	----------	----	-----------	--------------	----

利用可能なデータがありません。

- 子グループに直接ポリシーを適用すると、子グループで適用したポリシーが優先されます。

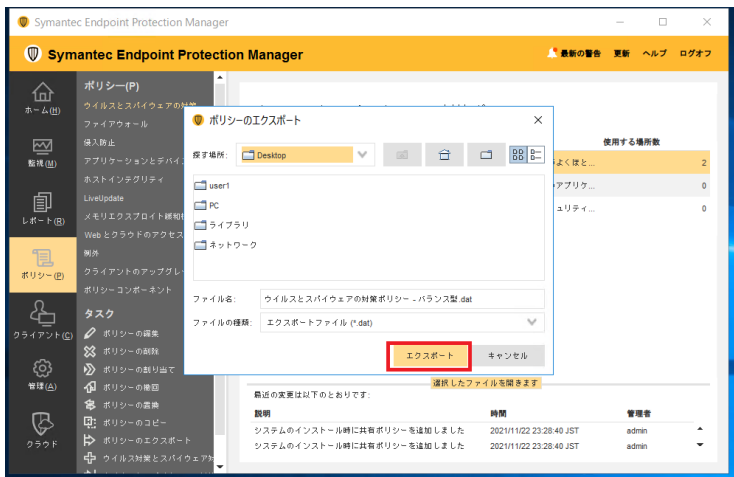
# 2.2ポリシー移行



①

エージェントが現在、SEPM配下で管理されているか確認します。

クラウド (ICDm) へ移行すると管理先がクラウドへ変更されます。



②

ポリシーの保存先を指定して、「エクスポート」を選択します。



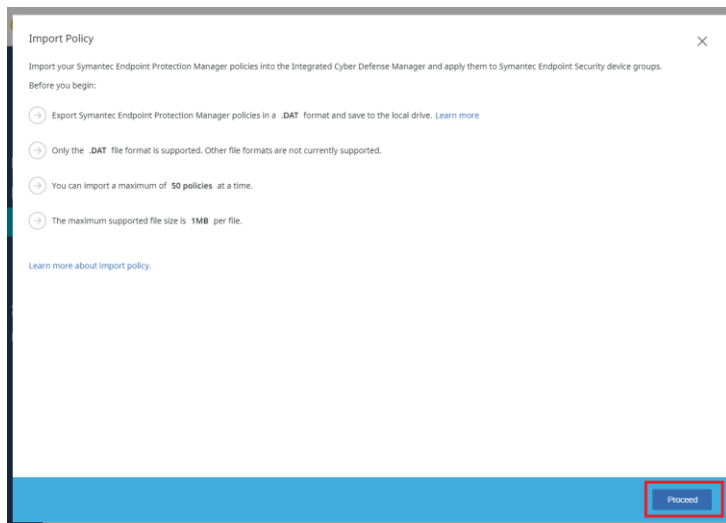
# 2.2ポリシー移行



③

ICDmの設定に移ります。

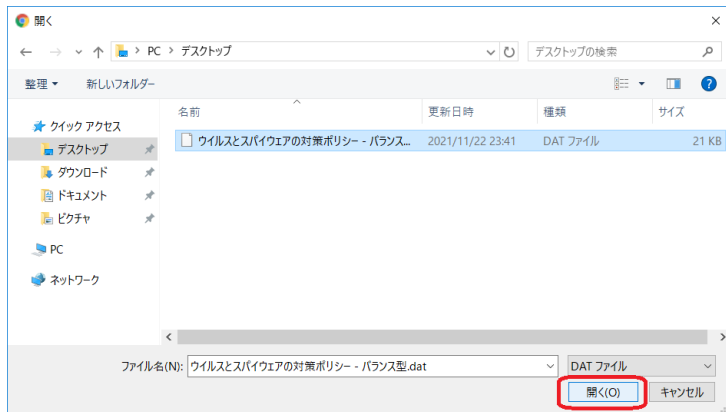
ICDmにログイン後、左側の「ポリシー」タブを選択し、「ポリシーのインポート」を選択します。



④

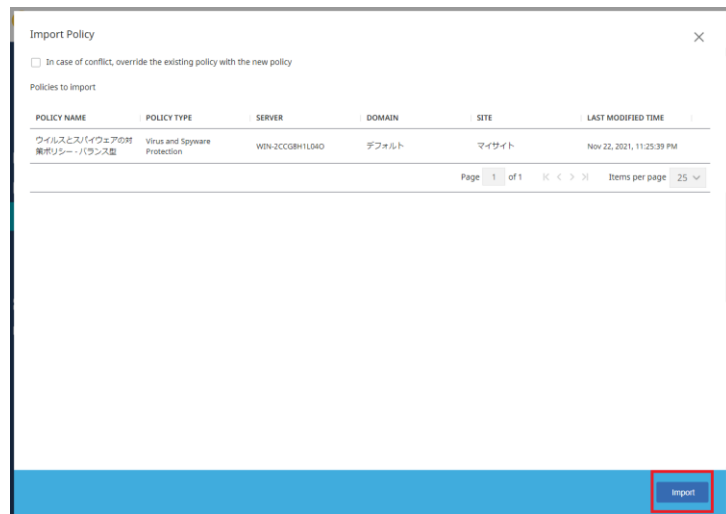
インポートに関する案内が表示されるので、「Proceed」を選択します。

## 2.2ポリシー移行



⑤

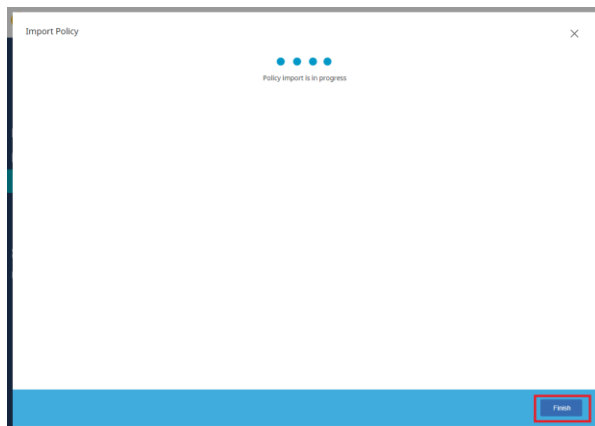
手順②でエクスポートしたポリシーを選択し、「開く」を選択します。



⑥

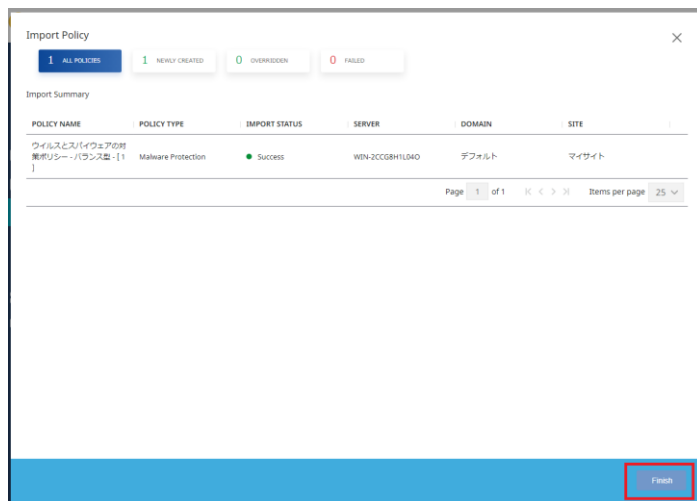
インポートしたポリシーの確認画面が表示されるので、「Import」を選択します。

## 2.2ポリシー移行



⑦

インポートのプロセスが実行されます。

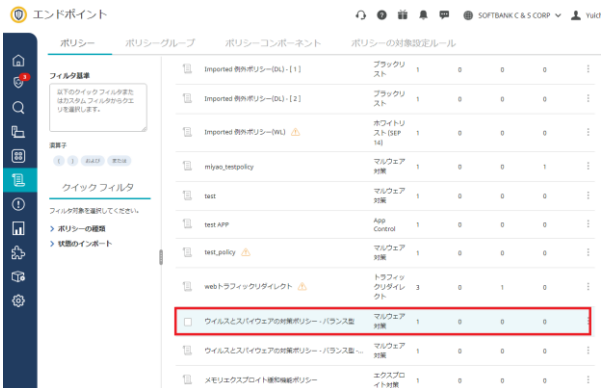


⑧

「IMPORT STATUS」が「Success」になると完了です。

「Finish」を選択します。

# 2.2ポリシー移行



9

インポートが完了すると、「ポリシー」画面よりインポートしたポリシーが表示されます。



10

インポートしたポリシーをデバイスグループに適用する際は、「デバイス」>「デバイスグループ」、対象のデバイスグループを選択し、「ポリシーの適用」を選択します。

## 2.2ポリシー移行

miyao\_devicegroup へのポリシーの適用

名前	バージョン	説明	ステータス	操作
<input type="checkbox"/> Imported 携帯ポリシー(DU)	1	ブラックリスト	0	0
<input type="checkbox"/> Imported 携帯ポリシー(DU-11)	1	ブラックリスト	0	0
<input type="checkbox"/> Imported 携帯ポリシー(DU-12)	1	ブラックリスト	0	0
<input type="checkbox"/> Imported 携帯ポリシー(WL)	1	ホワイトリスト (RFP 14)	0	0
<input type="checkbox"/> miyao_testpolicy	1	マルウェア対策	0	0
<input type="checkbox"/> test	1	マルウェア対策	0	0
<input type="checkbox"/> test APP	1	App Control	0	0
<input type="checkbox"/> test_policy	1	マルウェア対策	0	0
<input type="checkbox"/> webトラフィックリダイレクト	3	トラフィックリダイレクト	0	1
<input checked="" type="checkbox"/> クラウドとモバイルウェアの対策ポリシー - パラシタス	1	マルウェア対策	0	0
<input type="checkbox"/> クラウドとモバイルウェアの対策ポリシー - パラシタス (11)	1	マルウェア対策	0	0
<input type="checkbox"/> メモリエクスポイト緩和機能ポリシー	1	エクスポイト対策	0	0

51 to 75 / 79 items

ページ 3 / 4 < > items per page 25

次へ

⑪

インポートしたポリシーを選択し、「次へ」を選択します。

ポリシーの対象設定ルールを選択

名前	バージョン	説明	操作
<input type="checkbox"/> Quarantine	1	A target rule assigned to quarantined agents.	オン
<input checked="" type="checkbox"/> Default	1	This is the default policy assignment rule.	オン

次へ

⑫

「Default」を選択し、「次へ」を選択します。

## 2.2ポリシー移行



⑬

適用内容を確認し、「送信」を選択します。



⑭

対象のデバイスグループの「ポリシー」から確認できると完了となります。



# フルクラウドへ移行

クラウドへ移行するには以下プロセスが必要となります。

1

対象クライアント確認

2

SEPMポリシー移行

3

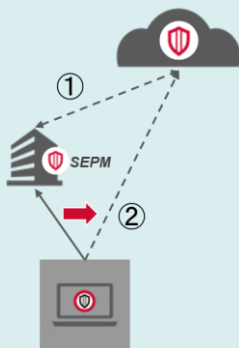
クライアントインストール

## 2.3クライアント移行

エージェントの移行方法は下記4つ方法がございます。  
各手順についてご案内いたします。

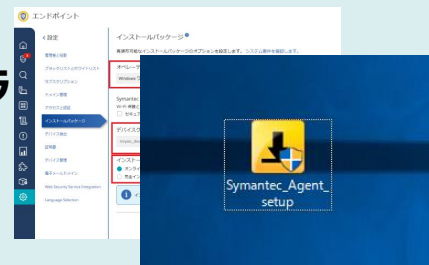
### 1. Switch機能で移行

- ・1度SEPMとICDmを連携して移行



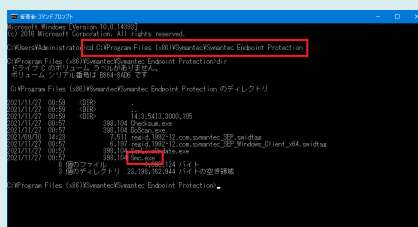
### 2. インストーラーで手動インストール

- ・クラウド版インストーラーでインストール



### 3. smcコマンドで移行

- ・クラウド版インストーラーをコマンドの引数に指定して移行

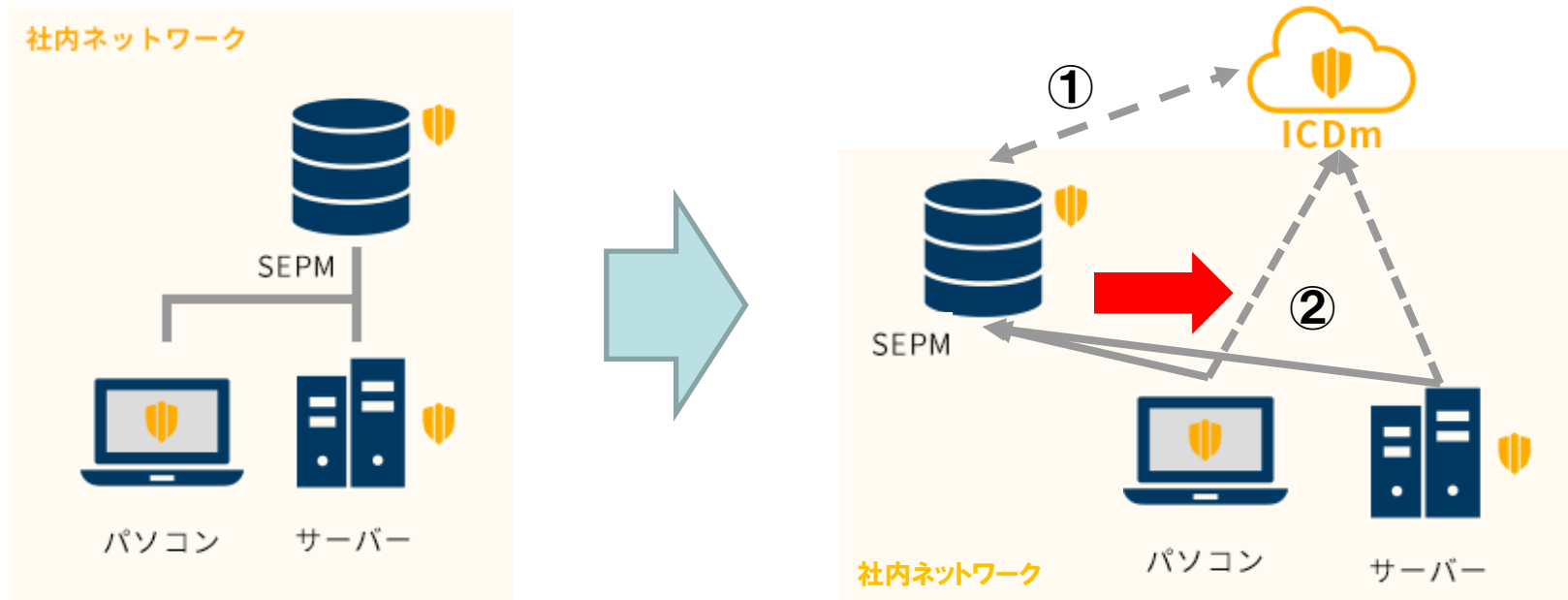


### 4. ホストインテグリティポリシーで移行

- ・SEPMのポリシーを利用して移行



## 2.3.1 Switch機能で移行



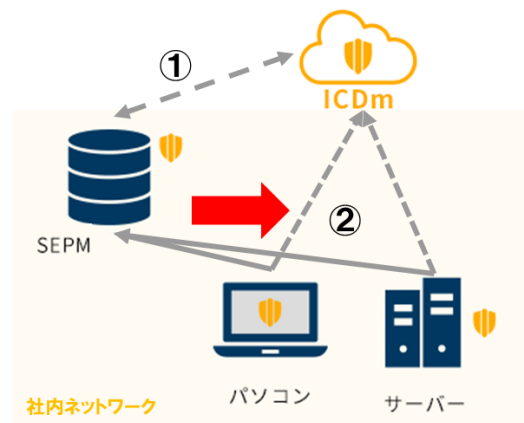
- ・ ICDmに搭載されているSwitch機能を使って移行いたします
- ・ 1度SEPMをクラウド連携して移行します
- ・ デバイスグループごとに移行し、子グループも自動的に移行されます

### Switch機能で移行

- 14.2RU1以降のバージョンで対応しております
- 1度クラウド管理が完了すると、SEPMへ戻すことは不可となります
- Windowsで実行可能です

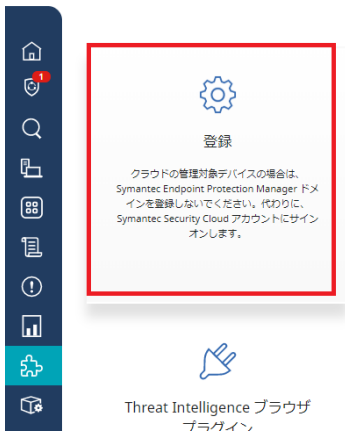


- デバイスグループ単位で**一括移行**することが可能です。
- デバイスグループ単位で移行いたしますが、デバイスグループのポリシー移行は**別途設定**が必要となります。ポリシーの設定については本手順が完了後にp42を実行ください。



# 2.3.1 Switch機能で移行

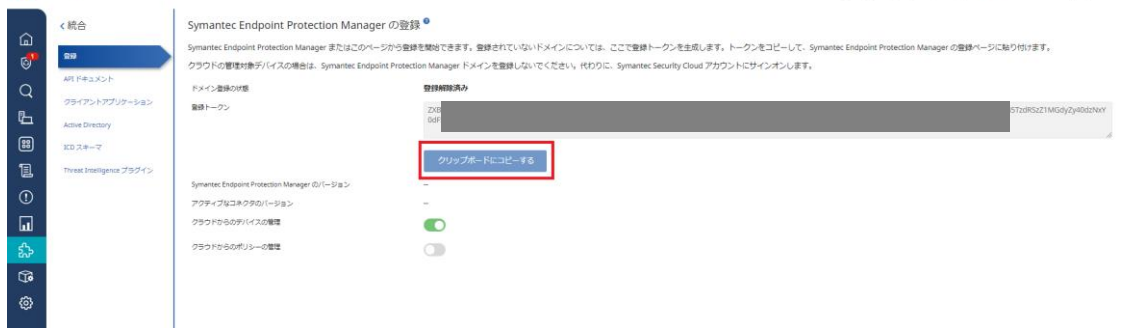
① エンドポイント



①

左のタブの「統合」を選択し、「登録」を選択します。

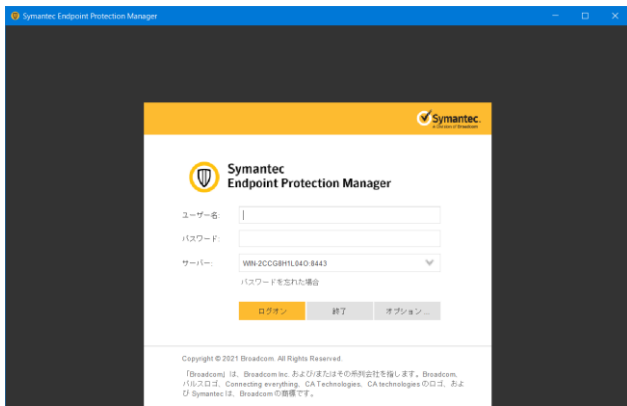
② エンドポイント



②

トークンをコピーします。「クリップボードにコピーする」を選択し、トークンをコピーします。

## 2.3.1 Switch機能で移行



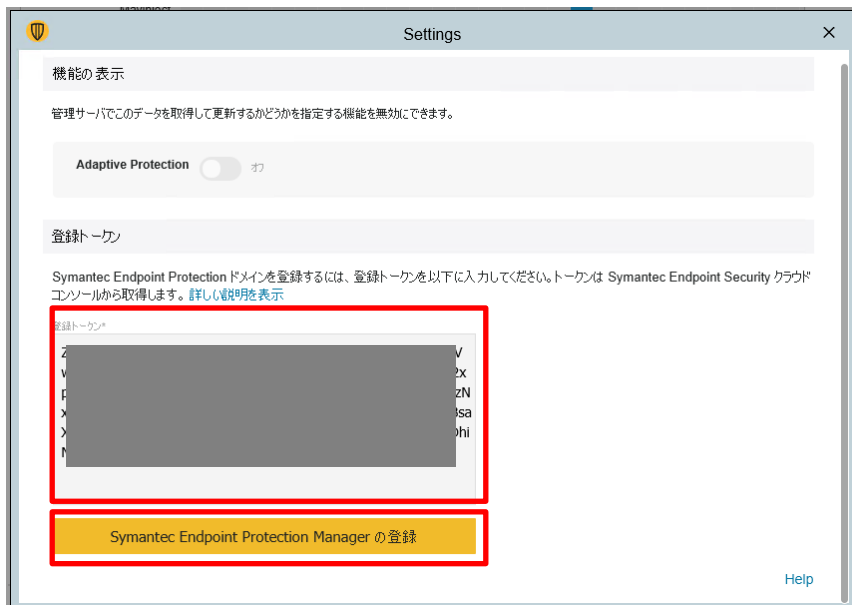
③

次は、SEPMでの操作となります。  
SEPMのユーザー名、パスワードを入力しログイン  
します。

④

左にある項目から「クラウド」を選択し、  
「Settings」を選択します。

## 2.3.1 Switch機能で移行



⑤

先ほどコピーしたトークンをペーストします。  
ペーストしたのち、「Symantec Endpoint Protection Managerの登録」を選択します。

# 2.3.1 Switch機能で移行



⑥

「状態：登録済み」でクラウドとの接続が完了です。



⑦

クラウド側の画面へ移ります。  
同期中は警告メッセージが表示されます。



## 2.3.1 Switch機能で移行

Endpoint

管理対象デバイス 管理外デバイス デバイスグループ

グループ階層

- Default (0)
- ICDm 技術部門 (1)
- iPhone (0)
- MANJAL\_TEST (1)
- miyao\_devicegroup (0)
- test\_miyao (0)
- テストグループ (0)
- 会社 (0)
- デフォルトグループ (2)**

デフォルトグループ  
デバイスグループ名

2	管理対象デバイス	2021/12/07 1	作成日
6	適用されたポリシー	--	説明

管理対象デバイス 管理外デバイス ポリシー 活動

フィルタを表示 ▼ デバイスの検索

デバイスリストを表示しています (1 ~ 2 / 2 を表示)

<input type="checkbox"/>	名前 ↓	ログオンユーザー	os
<input type="checkbox"/>	WIN-2CCG8H1L04D	Administrator	Windows Server 2...
<input type="checkbox"/>	DESKTOP-SJL3KDM	Administrator	Windows 10 Enter...

⑧

左側の「デバイス」タブを選択し、SEPMで管理されているデバイス、デバイスグループが表示されると、統合は完了です。

# 2.3.1 Switch機能で移行



⑨

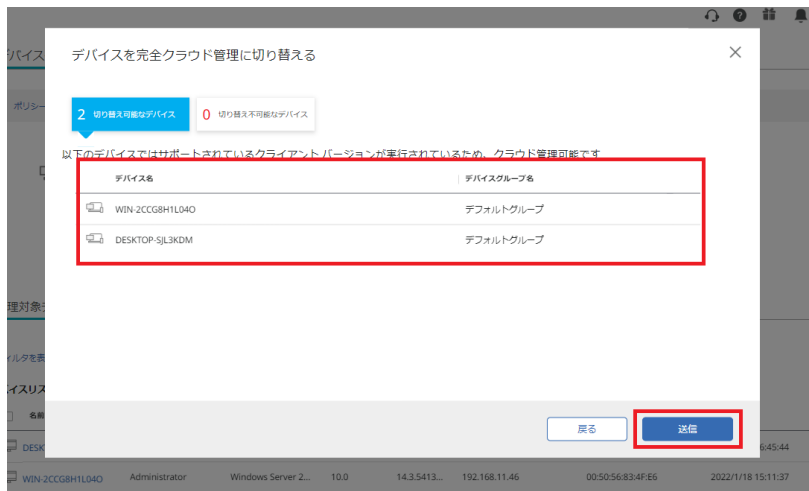
移行対象のデバイスグループを選択し、「その他の処理」から「クラウド管理に切り替え」を選択します。



⑩

クラウド管理に切り替える画面が表示されます。「次へ」を選択します。

## 2.3.1 Switch機能で移行



⑪

クラウド管理に切り替えるデバイスが表示されます。  
確認して「送信」を選択します。



⑫

確認画面が表示されます。  
この操作を完了後、再度SEPMに切り替える事は出来ません。  
確認後、「送信」を選択します。

# 2.3.1 Switch機能で移行



⑬

デバイス管理へ切り替えが開始します。「詳細を表示」を選択すると、⑬のデバイス移行の状況が表示されます。



⑭

移行状況の画面となります。

# 2.3.1 Switch機能で移行

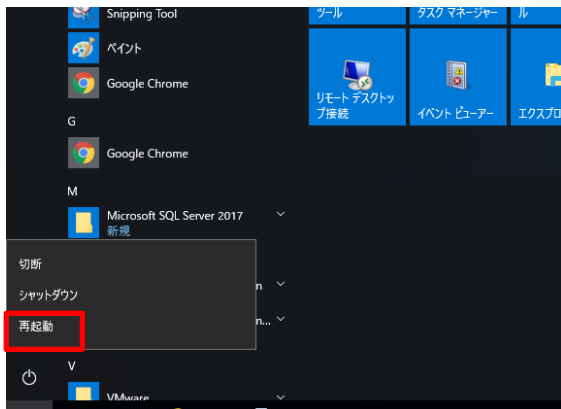


15 「デバイス切り替えプロセスが正常に完了しました」と表示されるとデバイスの移行が完了となります。



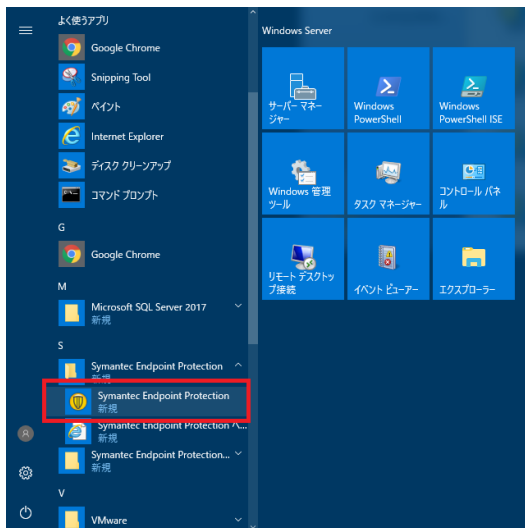
16 クラウド配下のデバイスグループにデバイスが移行されています。

## 2.3.2 インストーラーで手動インストール



⑰

デバイスの切り替えが完了すると、再起動が必要となります。  
再起動を実行してください。

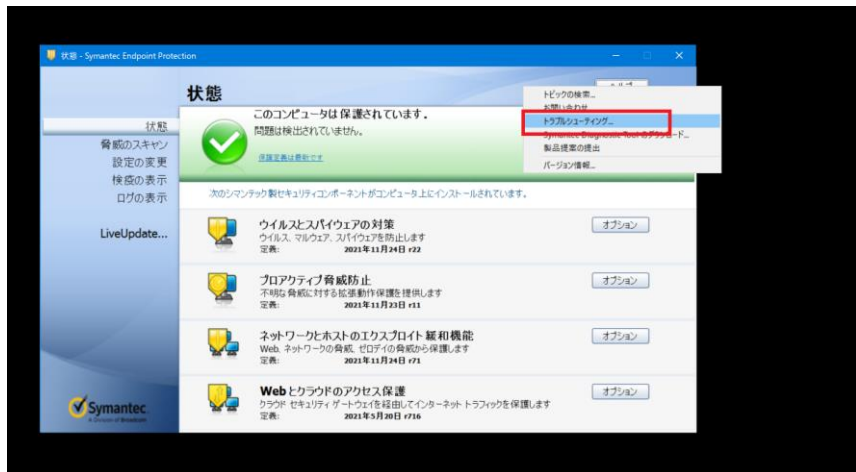


⑱

再起動後、エージェントがクラウド管理に移行されているか確認します。

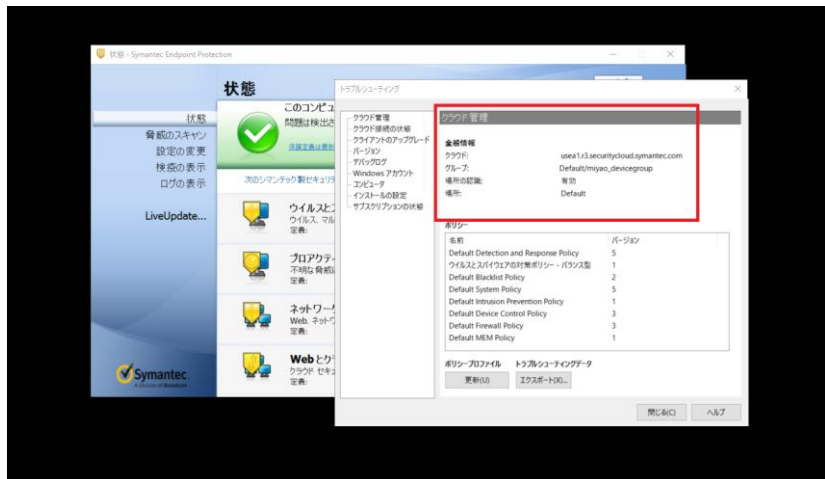
スタートから「Symantec Endpoint Protection」を選択します。

## 2.3.2 インストーラーで手動インストール



⑱

再起動完了後、エージェントを起動し、「ヘルプ」>「トラブルシューティング」を選択します。



⑳

クラウド管理である事が確認できれば移行は完了です。

# 2.3.1 Switch機能で移行



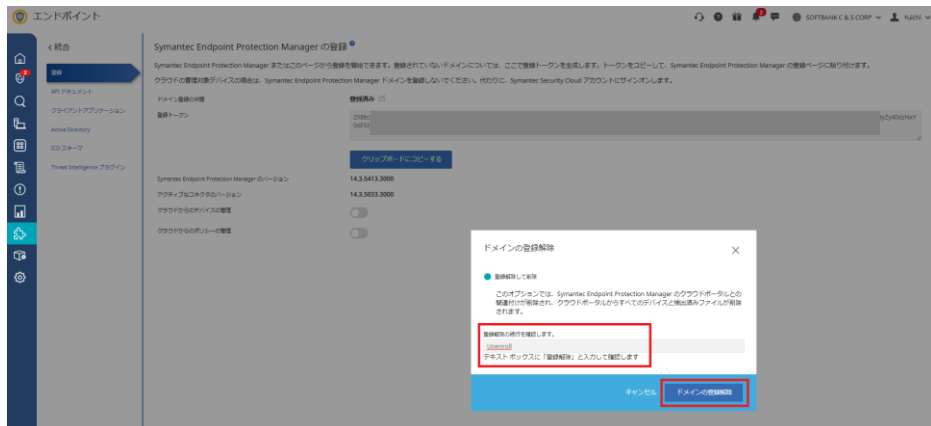
①  
移行が完了すると、SEPMとICDmの連携を解除します。  
左側にあるタブの「統合」を選択し、「登録」を選択します。



②  
「ドメイン登録の状態」が現在「登録済み」となっております。  
選択し、「Unenroll」を選択します。



# 2.3.1 Switch機能で移行



23

確認画面が表示されます。  
入力欄に「Unenroll」と入力し、「ドメインの登録解除」を選択すると、解除処理が開始されます。



24

ドメインの解除が完了すると、デバイスグループからSEPMのデバイスグループが消去されております。

本作業はこちらで完了です。

### ■ メーカー推奨最小構成ポリシーについて

ICDmで利用できる17個のデフォルトポリシーのうち適用が推奨されるポリシーは下記の4つとなります。

#### ・ Default Antimalware Policy

ウイルススキャンに関わる設定や疑わしいファイルに対する処置方法の設定についてまとめられています。

#### ・ Default Intrusion Prevention Policy

侵入防止の設定の有効/無効化やデフォルトの監査シグネチャ外のアクションに対する設定についてまとめられています。

#### ・ Default MEM Policy

MEM(Memory Exploit Mitigation)はシグネチャレスでOSを強化し未知のウイルスからの攻撃を阻止する機能です。

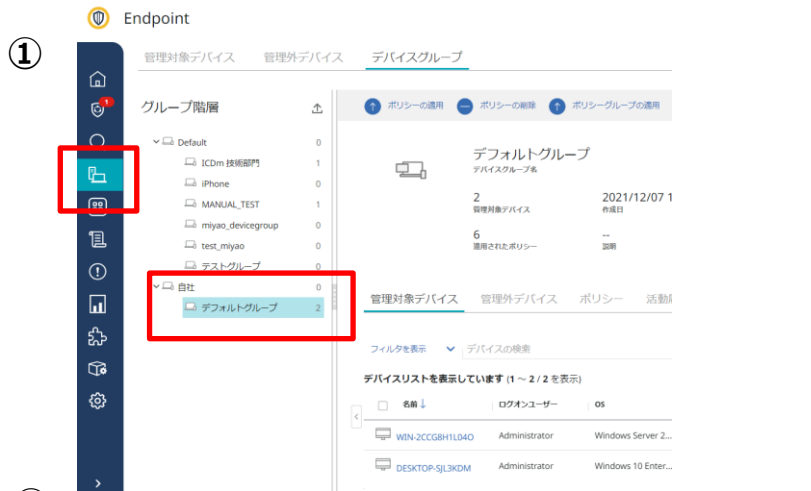
各機能の有効/無効化や推奨外のアプリケーションの保護に関する設定についてまとめられています。

#### ・ Default System Policy

Liveupdate先のサーバやスケジュールやクライアントのアップグレード間隔などの設定についてまとめられています。

本手順ではDefault Antimalware Policyを例に適用手順をご案内いたします。

# 2.3.1 Switch機能で移行（ポリシー設定）



①

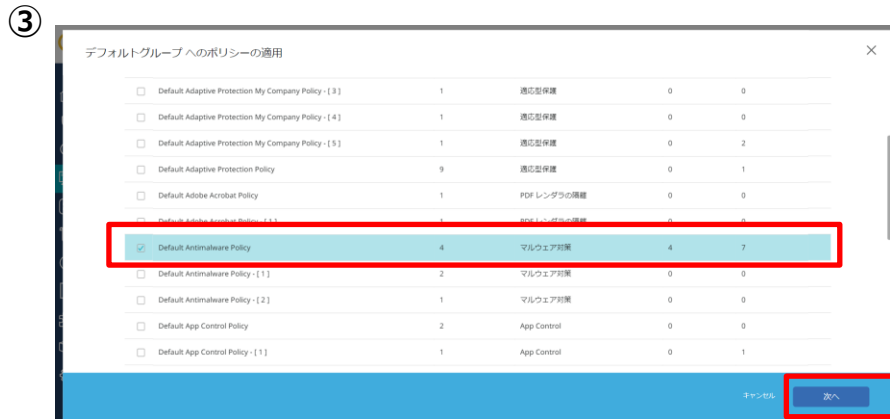
左タブより「デバイス」を選択し、「デバイスグループ」を選択します。  
移行したデバイスグループを選択します。



②

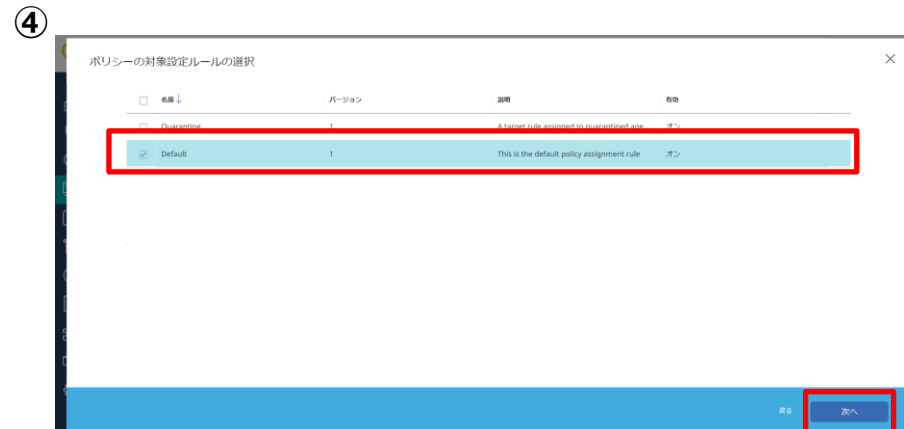
「ポリシーに適用」を選択します。

## 2.3.1 Switch機能で移行（ポリシー設定）



③

「Default Antimalware Policy」を選択し、「次へ」を選択します。

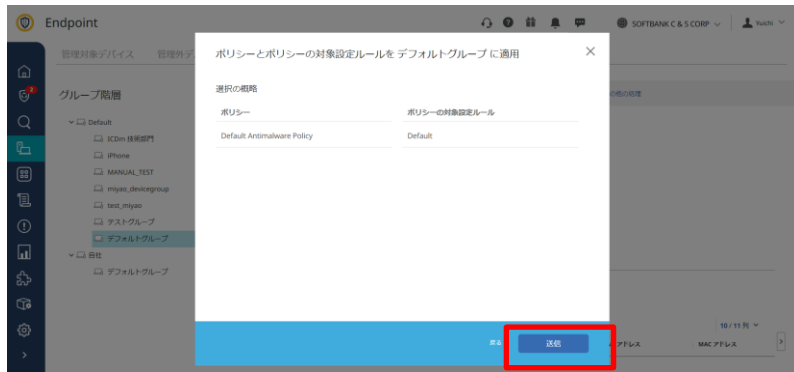


④

「Default」を選択し、「次へ」を選択します。

## 2.3.1 Switch機能で移行（ポリシー設定）

⑤



⑤

「送信」を選択します。

## 2.3.1 Switch機能で移行（ポリシー設定）

⑥

The screenshot shows the 'Endpoint' management interface. A red box highlights a green checkmark and the text: 「正常に完了」1個のポリシーがデバイスグループ「デフォルトグループ」に適用されています. The interface includes a sidebar with navigation icons and a main content area with tabs for '管理対象デバイス', '管理外デバイス', and 'デバイスグループ'. The 'デバイスグループ' tab is active, showing a list of groups on the left and details for the 'デフォルトグループ' on the right.

⑥

ポリシーの適用が完了すると、「正常に完了」と表示されます。

⑦

The screenshot shows the 'Endpoint' management interface with the 'ポリシー' tab selected. A red box highlights the 'ポリシー' tab. The interface includes a sidebar with navigation icons and a main content area with tabs for '管理対象デバイス', '管理外デバイス', and 'ポリシー'. The 'ポリシー' tab is active, showing a list of policies on the left and details for the 'Default Antimalware Policy' on the right.

⑦

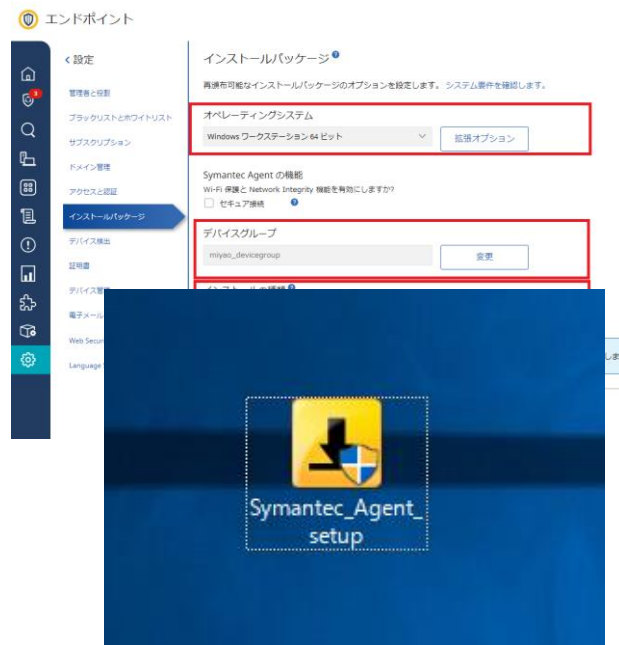
対象のデバイスグループの「ポリシー」を選択し、適用されたポリシーが確認できます。以上で設定は完了です。

### インストーラーで手動インストール

- ICDmでパッケージを作成し、対象デバイスにインストールします
- バージョン12.1.6MP5以降で対応しております
- 端末上で実行します
- Windows、Mac、Linuxで実行可能



- 一番シンプルな手順となります
- 普段のインストール手順の方法で移行可能です
- **Windows、Mac、Linux**で実行可能です



## 2.3.2 インストーラーで手動インストール



①

左側のタブより「設定」を選択し、「インストールパッケージ」を選択します。

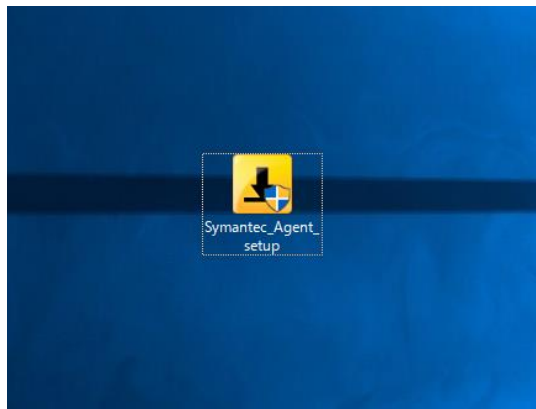


②

「オペレーティングシステム」  
「デバイスグループ」  
「インストールの種類」  
で各設定し、「パッケージのダウンロード」を選択  
します。  
インストーラーが端末にダウンロードされます。



## 2.3.2 インストーラーで手動インストール



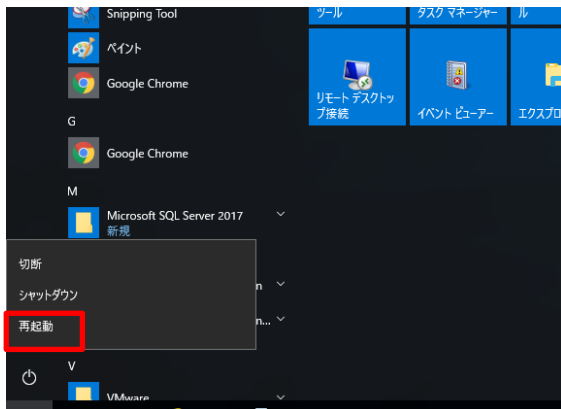
③

インストーラーを実行します。

④

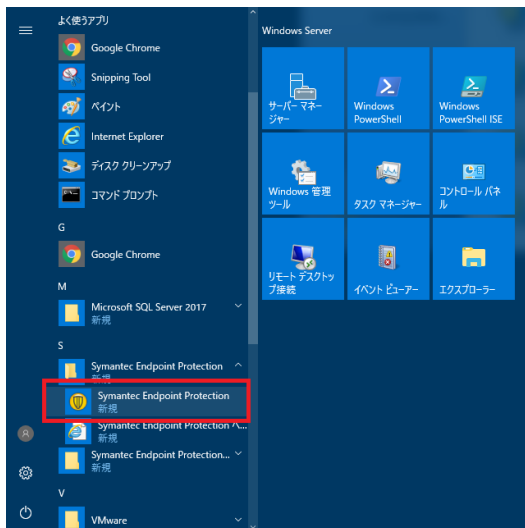
実行画面が表示されます。

## 2.3.2 インストーラーで手動インストール



⑤

インストールが完了すると、再起動が必要となります。  
再起動を実行してください。

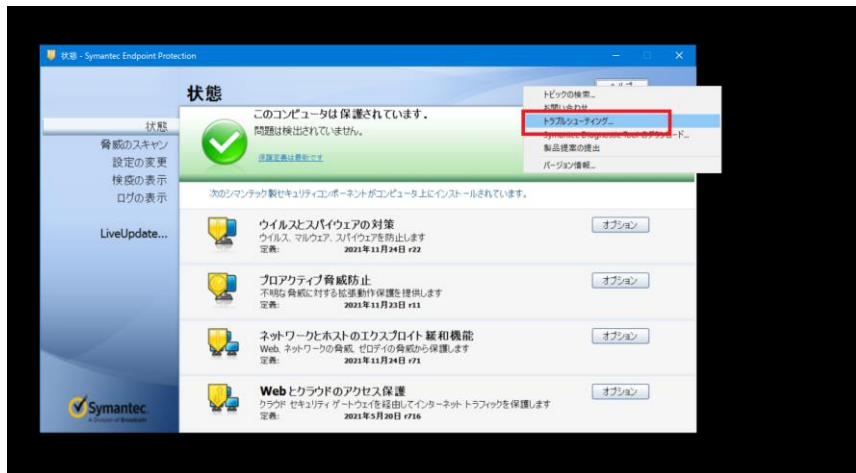


⑥

再起動後、エージェントがクラウド管理に移行されているか確認します。

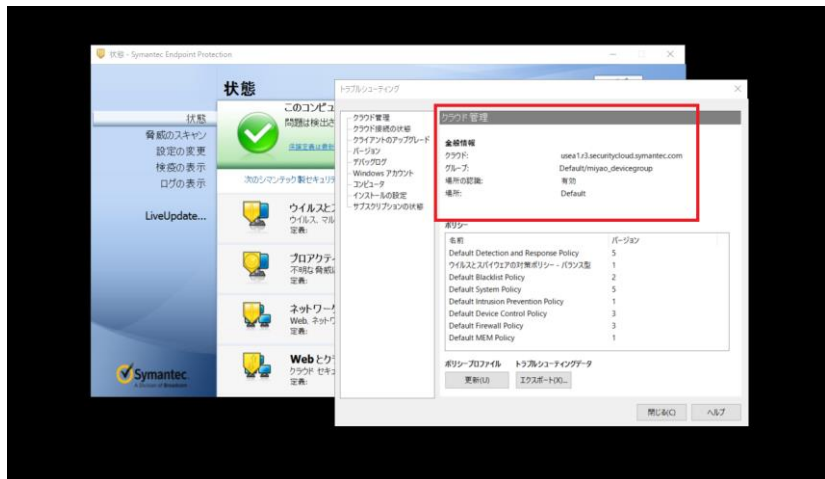
スタートから「Symantec Endpoint Protection」を選択します。

## 2.3.2 インストーラーで手動インストール



⑦

「ヘルプ」>「トラブルシューティング」を選択します。



⑧

クラウド管理である事が確認できれば移行は完了です。

## 2.3.2 インストーラーで手動インストール

Endpoint

管理外デバイス **デバイスグループ**

ポリシーの適用 ポリシーの削除 ポリシーグループの適用 ポリシーグループの削除 その他の処理

miyao\_devicegroup  
デバイスグループ名

1	管理対象デバイス	2021/06/30 17:49:50
9	適用されたポリシー	--

管理対象デバイス 管理外デバイス ポリシー 活動履歴

フィルタを表示 デバイスの検索

デバイスリストを表示しています (1 ~ 1 / 1 を表示)

名前 ↑	ログインユーザー	OS	OS のバー...	クラウン...	IPV4 アドレス	MAC アド...
WIN-2CCG8H1D40	Administrator	Windows Server 2...	10.0.14393	14.3.5413...	192.168.11.46	00:50:56

⑨

ICDmでも、「デバイス」>「デバイスグループ」から対象のデバイスグループを選択します。「管理対象デバイス」でも確認できます。本作業はこちらで完了です。

### Symantec Management Client(smc)※コマンドで移行

- Symantec Management Client(smc)サービスを使用して、クラウド管理へ切り替えます
- 14.3MP1以降のバージョンで利用可能でございます。
- クラウド⇒オンプレの切り替えも可能

**Point!**



- コマンドプロンプトを使用いたします
- Windowsのみ実行可能となります
- **再起動不要**となります

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files (x86)\Symantec\Symantec Endpoint Protection
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>dir
ドライブのボリューム ラベルがありません。
ボリューム シリアル番号は B864-8A06 です。

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection のディレクトリ
2021/11/27 00:59 <DIR> .
2021/11/27 00:59 <DIR> ..
2021/11/27 00:59 <DIR> 14,3,5419,3000,105
2021/11/27 00:57 398,104 Checksum.exe
2021/11/27 00:57 398,104 DoScan.exe
2021/09/10 14:23 7,511 regid.1992-12.com.symantec_SEP.swidtag
2021/11/27 00:57 8,197 regid.1992-12.com.symantec_SEP_Client_x64.swidtag
2021/11/27 00:57 398,104 SymantecUpdate.exe
2021/11/27 00:57 398,104 Svc.exe
6 個のファイル 1,999,124 バイト
3 個のディレクトリ 23,188,162,944 バイトの空き領域

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>
```

※smc : Symantecが提供しているコマンドラインインターフェース。Windowsクライアントサービスを実行できます。

## 2.3.3 smcコマンドで移行

④ エンドポイント



### 管理者と役割

管理者を作成し、製品を管理するために管理者に与える権限を設定します。



### ブラックリストとホワイトリスト

ブラックリストとホワイトリストのポリシーに含まれるすべてのアーティファクト (ファイルハッシュ、シユ、URL、ドメイン、証明書) の観念リストを表示します。



### サブスクリプション

ライセンスの有効期限など、製品のサブスクリプションの詳細を表示します。



### インストールパッケージ

クライアントソフトウェアの配備に使用する再頒布可能なパッケージを作成して、Windows デバイスを登録します。



### デバイス検出

1 つ以上のデバイスを検出エージェントとして設定します。これは、クラウドポータルで登録されていないネットワーク上のデバイスを検出するために使用できます。



### 証明書

SSL トラフィックインスペクション用の証明書を管理します。

①

左側のタブより「設定」を選択し、「インストールパッケージ」を選択します。

## 2.3.3 smcコマンドで移行

### インストールパッケージ

再選択可能なインストールパッケージのオプションを設定します。システム要件を確認します。

オペレーティングシステム  
Windows ワークステーション 64 ビット 拡張オプション

Symantec Agent の機能  
Wi-Fi 保護と Network Integrity 機能を有効にしますか?  
 セキュア接続

デバイスグループ  
miyao\_devicegroup 変更

インストールの種類  
 オンラインインストールパッケージ  
 完全インストールパッケージクリエータ

インストールパッケージをダウンロードして、登録する Windows デバイスで実行可能ファイルを実行します。

②

「オペレーティングシステム」  
「デバイスグループ」  
「インストールの種類」  
で各設定し、「パッケージのダウンロード」を選択  
します。  
インストーラーが端末にダウンロードされます。

ユーザーの招待

パッケージのダウンロード

## 2.3.3 smcコマンドで移行



③

インストーラーをダウンロードし、対象端末にインストーラーをおきます。

④

対象端末から「コマンドプロンプト」を実行します。



## 2.3.3 smcコマンドで移行

```
管理者: コマンドプロンプト
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files (x86)\Symantec\Symantec Endpoint Protection

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>dir
ドライブ C のボリューム ラベルがありません。
ボリューム シリアル番号は B864-8AD6 です

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection のディレクトリ

2021/11/27  00:59    <DIR>          .
2021/11/27  00:59    <DIR>          ..
                14,354,113,3000,105
2021/11/27  00:59    <DIR>          .
                398,104  Checksum.exe
                398,104  DoScan.exe
2021/09/10  14:23             7,511  regid.1992-12.com.symantec_SEP.swidtag
2021/11/27  00:57             6,197  regid.1992-12.com.symantec_SEP_Windows_Client_x64.swidtag
2021/11/27  00:57             398,104  SetupUpdate.exe
2021/11/27  00:57             398,104  Smc.exe
                6 個のファイル  1,666,124 バイト
                3 個のディレクトリ  23,198,162,944 バイトの空き領域

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>
```

⑤

Symantec Endpoint Protectionのフォルダに移動します。

「Smc.exe」がある事を確認します。  
デフォルトでは、以下に配置されています。

```
管理者: コマンドプロンプト

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>
C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>smc -cloudmanaged C:\Users\Administrator\Downloads\Symantec_Agent_setup.exe
クラウド専用機能をインストールしています...

C:\Program Files (x86)\Symantec\Symantec Endpoint Protection>
```

⑥

以下コマンドを実行します。

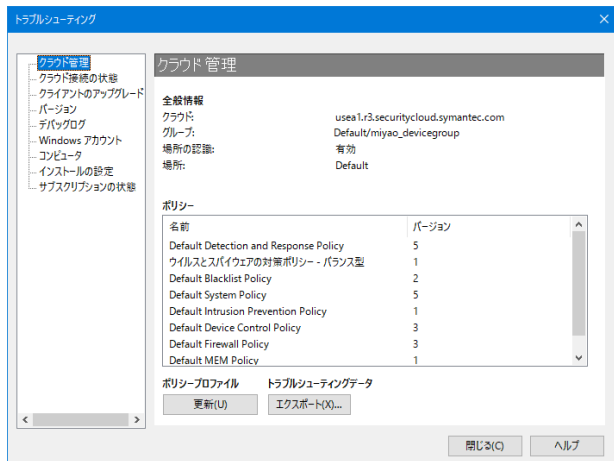
「smc -cloudmanaged path¥Symantec\_Agent\_Setup.exe」  
Pathでは先ほどDLしたエージェントの格納先を指定します。

## 2.3.3 smcコマンドで移行



⑦

管理がクラウドへ変更されたか確認します。Symantec Endpoint Protectionを開き、「ヘルプ」を選択し、「トラブルシューティング」を選択します。



⑧

クラウド管理と表示されれば移行は完了となります。

## 2.3.3 smcコマンドで移行

Endpoint

管理外デバイス **デバイスグループ**

ポリシーの適用 | ポリシーの削除 | ポリシーグループの適用 | ポリシーグループの削除 | その他の処理

miyao\_devicegroup  
デバイスグループ名

1	管理対象デバイス	2021/06/30 17:49:50
9	適用されたポリシー	--

管理対象デバイス | 管理外デバイス | ポリシー | 活動履歴

フィルタを表示 | デバイスの検索

デバイスリストを表示しています (1 ~ 1 / 1 を表示)

<input type="checkbox"/>	名前 ↑	ログインユーザー	OS	OS のバー...	クラウン...	IPV4 アドレス	MAC アド...
<input checked="" type="checkbox"/>	WIN-2CCG8H1D40	Administrator	Windows Server 2...	10.0.14393	14.3.5413...	192.168.11.46	00:50:56

⑨

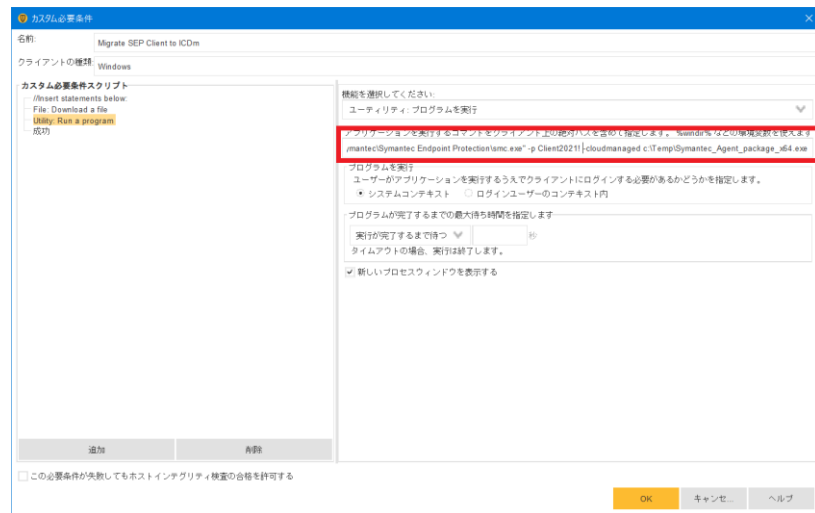
ICDmでも、「デバイス」>「デバイスグループ」から対象のデバイスグループを選択します。「管理対象デバイス」でも確認できます。本作業はこちらで完了です。

### ホストインテグリティポリシーで移行

- SEPMで配信しているポリシーを利用して移行いたします
- 移行したい端末がアクセスできるWebサーバー上にパッケージを保存します
- Broadcomのサイトから移行用のひな型ポリシーをダウンロードして、SEPMにインポートします



- **SEPMのポリシー**を利用します
- SEPMにひな形ポリシーをインポートする必要があります
- Windowsのみ実行可能となります



# 2.3.4ホストインテグリティポリシーで移行



①

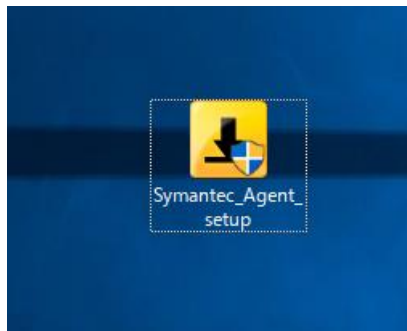
左側のタブより「設定」を選択し、「インストールパッケージ」を選択します。



②

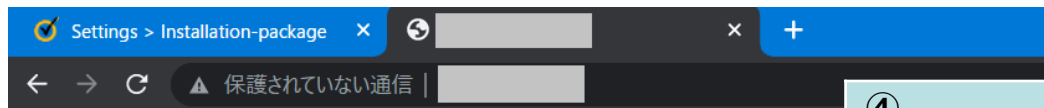
「オペレーティングシステム」  
「デバイスグループ」  
「インストールの種類」  
で各設定し、「パッケージのダウンロード」を選択  
します。  
インストーラーが端末にダウンロードされます。

## 2.3.4ホストインテグリティポリシーで移行



③

左側のタブより「設定」を選択し、「インストールパッケージ」を選択します。

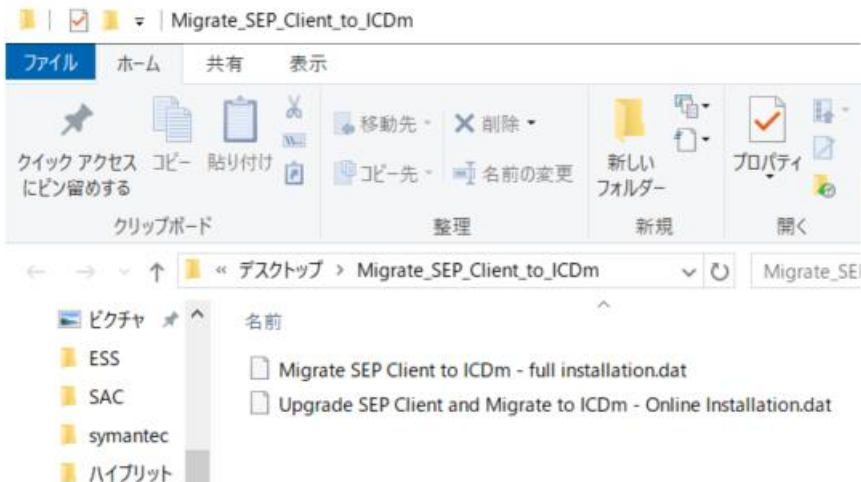
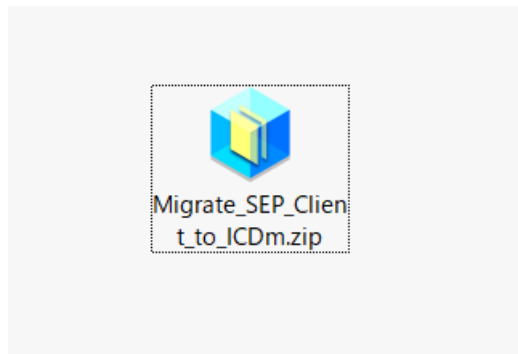


④

SEPMのポリシーでは、https経由でインストーラーを入手し、上書きインストールを実行します。Webサーバーにインストーラーをアップロードします。

2021/06/22	2:04	468748	[REDACTED]
2021/07/08	18:47	2394624	[REDACTED]
2021/12/21	1:32	2394616	<a href="#">Symantec_Agent_setup.exe</a>
2021/06/23	23:46	168	[REDACTED]

## 2.3.4ホストインテグリティポリシーで移行



⑤

SEPMのポリシーで利用するひな形をメーカーサイトからダウンロードいたします。  
以下メーカーサイトへアクセスし、ひな形をダウンロードします。

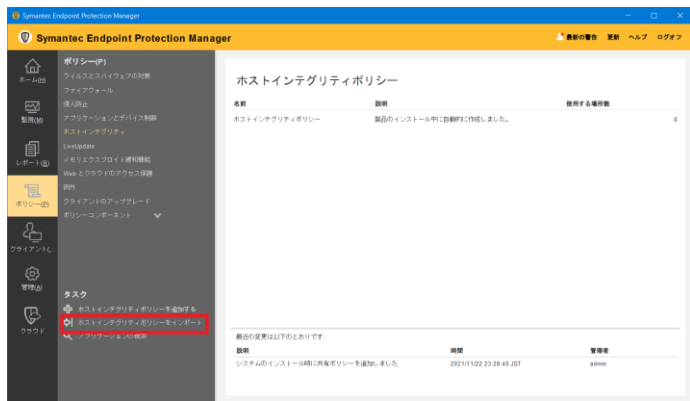
<https://techdocs.broadcom.com/us/en/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Upgrading/Converting-a-Symantec-Endpoint-Protection-managed-client-to-a-cloud-managed-Symantec-Agent.html>

メーカーサイトのリンクになっている  
「Migrate\_SEP\_Client\_to\_ICDm.zip」をクリックします。

⑥

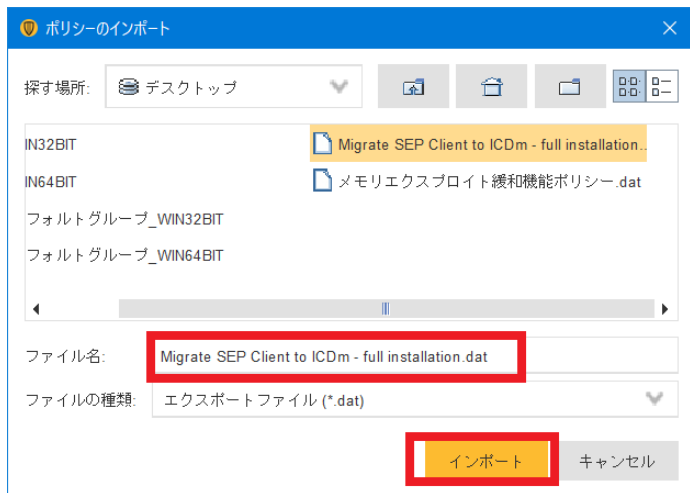
Zipファイルを展開すると2つのファイルが格納されております。

## 2.3.4ホストインテグリティポリシーで移行



⑦

SEPMの操作になります。  
SEPMにログイン後、「ポリシー」を選択し、「ホストインテグリティ」>「ホストインテグリティポリシーをインポート」を選択します。



⑧

先ほど展開したファイルの1つをインポートします。  
「Migrate SEP Client to ICDm - full installation.dat」をインポートいたします。



## 2.3.4ホストインテグリティポリシーで移行

The screenshot shows the Symantec Endpoint Protection Manager interface. The left sidebar contains navigation options like 'ポリシー(P)', 'タスク', and 'クラウド'. The main content area is titled 'ホストインテグリティポリシー' and displays a table of policies. One policy, 'Migrate SEP Client to ICDm - full installation', is highlighted with a red border. Below the table, there is a section for recent updates.

名前	説明	使用する場所数
ホストインテグリティポリシー	製品のインストール中に自動的に作成しました。	0
Migrate SEP Client to ICDm - full installation	Created by Joost Nienhuis (Joost.Nienhuis@Broadcom.com)Prereq.	0

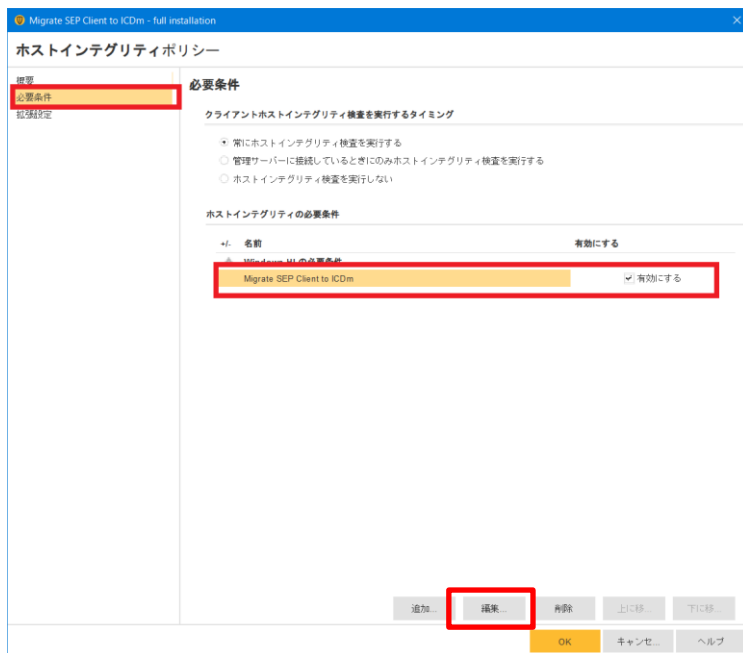
最近の変更は以下のとおりです:

説明	時間	管理者
共有 ホストインテグリティポリシー を追加しました: Migrate SEP Client .	2021/12/21 12:42:56 JST	admin
システムのインストール時に共有ポリシーを追加しました	2021/11/22 23:28:40 JST	admin

⑨

インポートしたポリシーを選択してください。  
ポリシーを編集いたします。

## 2.3.4ホストインテグリティポリシーで移行



⑩

「必要条件」を選択し、「Migrate SEP Client to ICDm」を選択します。  
「編集」を選択し、ポリシー内容を編集します。

## 2.3.4ホストインテグリティポリシーで移行

名前: Migrate SEP Client to ICDm

クライアントの種類: Windows

カスタム必要条件スクリプト

File: Download a file

機能を選択してください:

ファイル: ファイルをダウンロード

指定した URL から対象フォルダにファイルをダウンロードします。

ファイル URL: http://192.168.11.42/Symantec\_Agent\_setup.exe

対象フォルダ: c:\temp

HTTP のみに必要な認証

ユーザー名:

パスワード:

ダウンロード処理のダイアログボックスを表示する

ユーザーがこの必要条件のホストインテグリティを中止できる

追加 削除

この必要条件が失敗してもホストインテグリティ検査の合格を許可する

OK キャンセル... ヘルプ

⑪

「File:Download a file」を選択します。  
ファイルURLに以下URLを指定します。  
**ファイルURL:**  
「http://<WebサーバーのIPアドレス>/Symantec\_Agent\_setup.exe」

## 2.3.4ホストインテグリティポリシーで移行

名前: Migrate SEP Client to ICDm

クライアントの種類: Windows

カスタム必要条件スクリプト

Insert statements below:

- File: Download a file
- Utility: Run a program (成功)

機能を選択してください

ユーティリティ: プログラムを実行

アプリケーションを実行するコマンドをクライアント上の絶対パスを含めて指定します。 %windir% などの環境変数を使えます

Files (x86)\Symantec\Symantec Endpoint Protection\smc.exe" -cloudmanaged c:\Temp\Symantec\_Agent\_package\_x64.exe

プログラムを実行

ユーザーがアプリケーションを実行するうえでクライアントにログインの必要があるかどうかを指定します。

- システムコンテキスト
- ログインユーザーのコンテキスト内

プログラムが完了するまでの最大待ち時間を指定します

実行が完了するまで待つ  秒

タイムアウトの場合、実行は終了します。

新しいプロセスウィンドウを表示する

追加 削除

この必要条件が失敗してもホストインテグリティ検査の合格を許可する

OK キャンセル ヘルプ

⑫

「Utility:Run a program」を選択し、各設定値に以下記入いたします。

**機能：**「ユーティリティ：プログラムを実行」  
**実行するコマンド：**

「"c:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protection¥smc.exe" -cloudmanaged c:¥Temp¥Symantec\_Agent\_package\_x64.exe」

完了後は「OK」を選択します。

## 2.3.4ホストインテグリティポリシーで移行

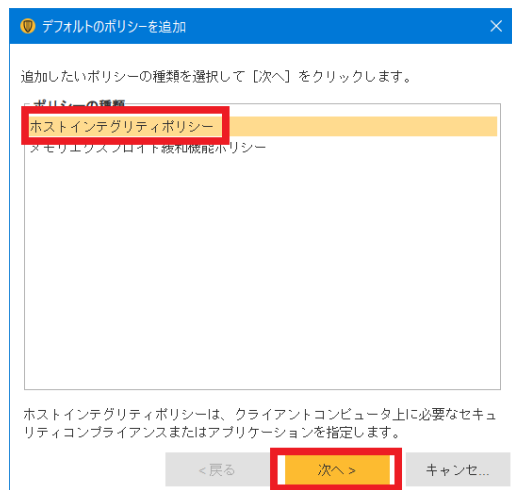


⑬

適用するデバイスグループに設定したポリシーを有効にします。

左の「クライアント」を選択し、「ポリシー」を選択します。

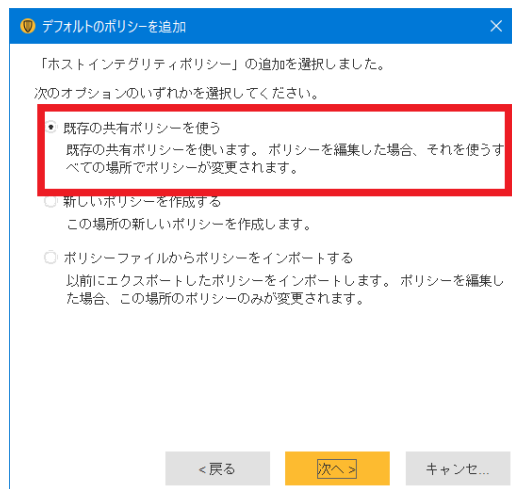
「場所固有のポリシー」から「ポリシーの追加」を選択します。



⑭

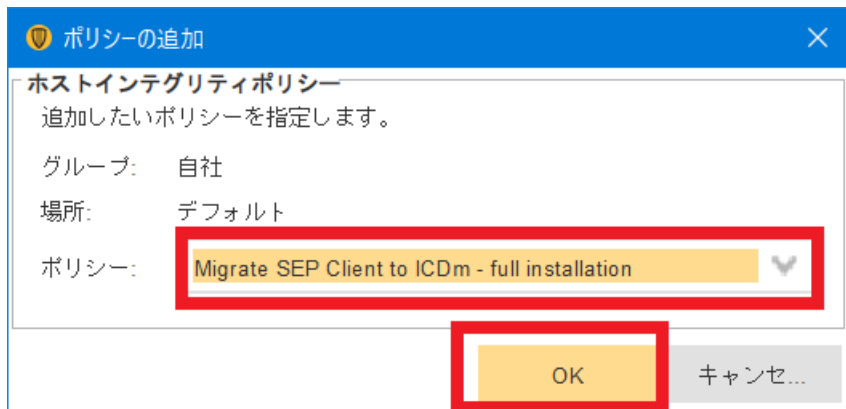
「ホストインテグリティポリシー」を選択して「次へ」を選択します。

## 2.3.4ホストインテグリティポリシーで移行



⑮

「既存の共有ポリシーを使う」を選択します。



⑯

「Migrate SEP Client to ICDm-full installation」を選択し、「OK」を押下するとデバイスグループにポリシーが設定されます。

# 2.3.4ホストインテグリティポリシーで移行



17

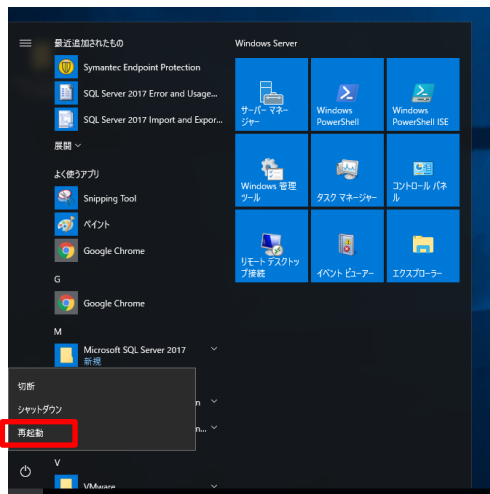
ポリシーが適用されていることが確認するとポリシーの設定が完了です。

## 2.3.4ホストインテグリティポリシーで移行



⑱

ポリシーの設定が完了すると、クライアント側でエージェントのアップグレードが実行されます。

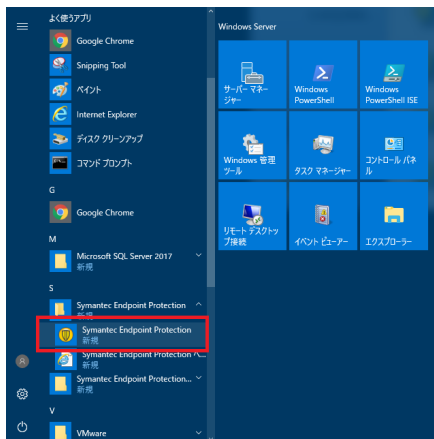


⑲

実行完了後は再起動が必要となります。  
「スタート」>「再起動」を選択して再起動を実行してください。



## 2.3.4ホストインテグリティポリシーで移行



②0

「Symantec Endpoint Protection」を選択し、起動します。



②1

起動後、「ヘルプ」>「トラブルシューティング」を選択してください。

## 2.3.4ホストインテグリティポリシーで移行

22

クラウド管理情報がオンプレのSEPMからクラウドに変更されております。



Endpoint



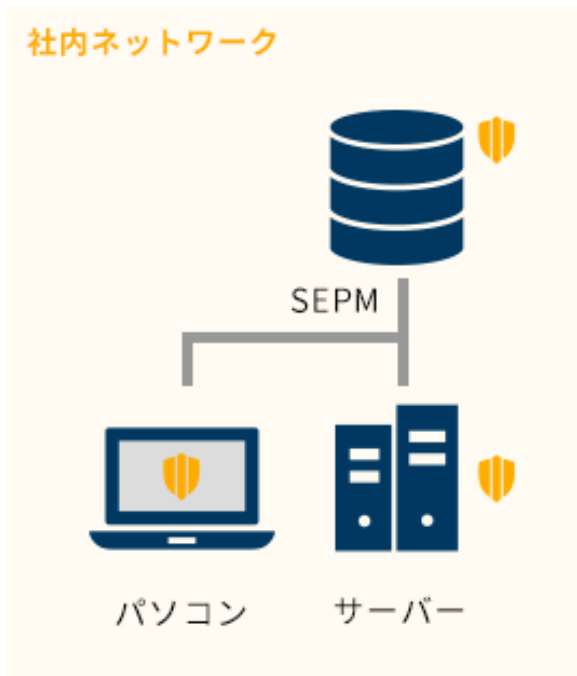
23

ICDmでも、「デバイス」>「デバイスグループ」から対象のデバイスグループを選択します。「管理対象デバイス」でも確認できます。本作業はコチラで完了です。

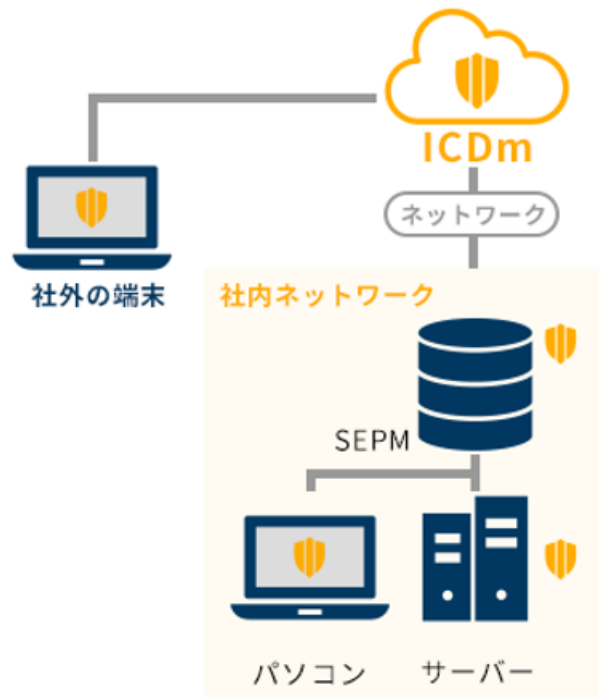
## 3. ハイブリッド構成手順

# ハイブリッド構成

オンプレミスで管理



ハイブリッドで管理



SEPMとICDm  
で管理

1

トークンの登録

2

デバイス管理※

3

ポリシー管理※

※任意の手順となります

1

トークンの登録

2

デバイス管理※

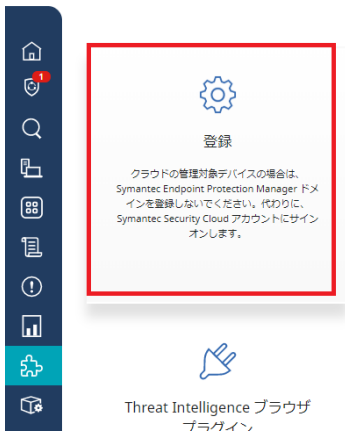
3

ポリシー管理※

※任意の手順となります

# 3.1 トークンの登録

🏠 エンドポイント



①

左のタブの「統合」を選択し、「登録」を選択します。

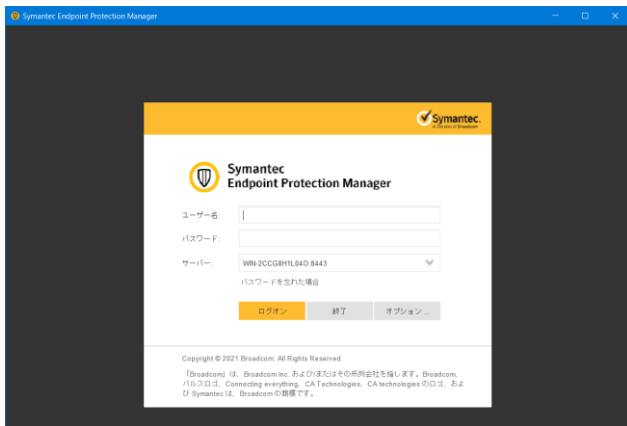
🏠 エンドポイント



②

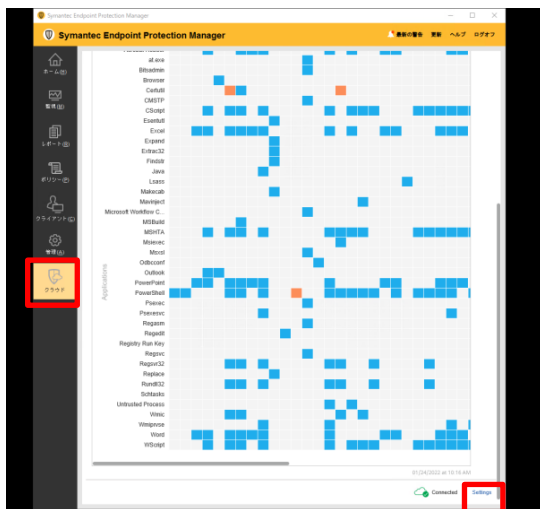
トークンをコピーします。「クリップボードにコピーする」を選択し、トークンをコピーします。

# 3.1 トークンの登録



③

次は、SEPMでの操作となります。  
SEPMのユーザー名、パスワードを入力しログイン  
します。

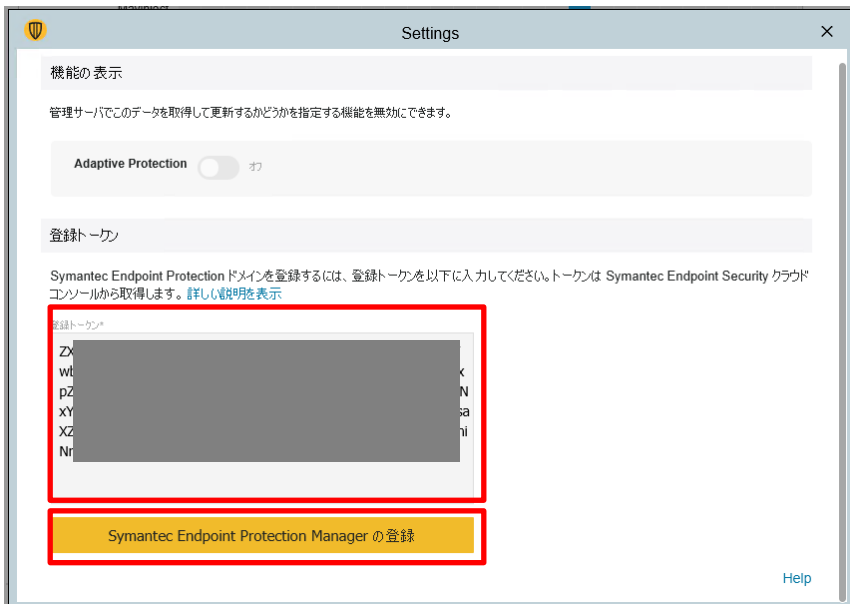


④

左にある項目から「クラウド」を選択し、  
「Settings」を選択します。



# 3.1 トークンの登録



⑤

先ほどコピーしたトークンをペーストします。  
ペーストしたのち、「Symantec Endpoint Protection Managerの登録」を選択します。

# 3.1 トークンの登録



⑥

「状態：登録済み」でクラウドとの接続が完了です。

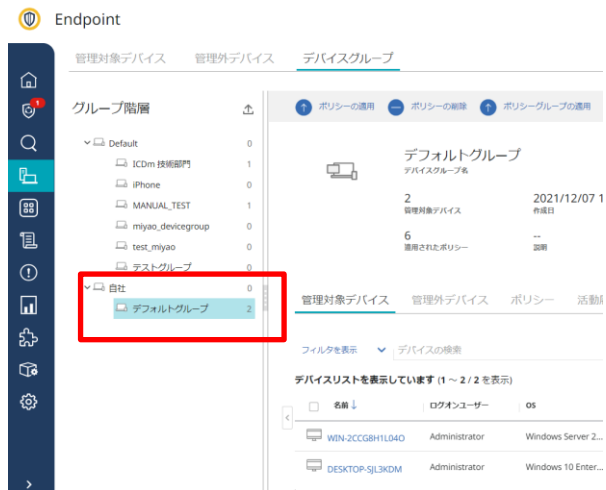
Endpoint



⑦

クラウド側の画面へ移ります。  
同期中は警告メッセージが表示されます。

# 3.1 トークンの登録



⑧

左側の「デバイス」タブを選択し、SEPMで管理されているデバイス、デバイスグループが表示されると、統合は完了です。

1

トークンの登録

2

デバイス管理※

3

ポリシー管理※

※任意の手順となります

### デバイス管理

- ICDm内で、SEPM配下のデバイス管理が可能となります
- デバイス管理ではICDmでデバイスの編成（グループ、デバイスの移動など）を制御できます。
- 本オプションを無効にするとSEPMでデバイスの編成が必要となります。

**Point!**

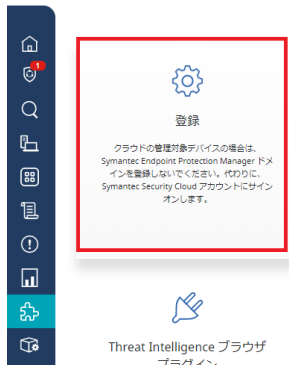


- **シングルコンソール**でデバイス管理が可能となります。
- **本手順書ではデバイス管理の例としてICDmからSEPM配下のデバイスグループの作成手順をご紹介します。**



## クラウドからのデバイスの管理

エンドポイント



API ドキュメント

API ドキュメントには、例、json でのサンプルレスポンス、レスポンスコードなどが含まれます。

Threat Intelligence ブラウザ  
プラグイン

①

クラウド経由でSEPM配下のデバイス管理が可能となります。  
左側のタブの「統合」を選択し、「登録」を選択します。

エンドポイント



### Symantec Endpoint Protection Manager の登録

Symantec Endpoint Protection Manager またはこのページから登録を開始できます。登録されていないドメインについては、ここで登録トークンを生成します。トークンをコピーして、Sym Protection Manager の登録ページに貼り付けます。

クラウドの管理対象デバイスの場合、Symantec Endpoint Protection Manager ドメインを登録しないでください。代わりに、Symantec Security Cloud アカウントにサインオンします。

ドメイン登録の状態

登録済み

登録トークン

クリップボードにコピーする

Symantec Endpoint Protection Manager のバージョン 14.3.5413.3000

アカウント/コネクタのバージョン 14.3.5033.3000

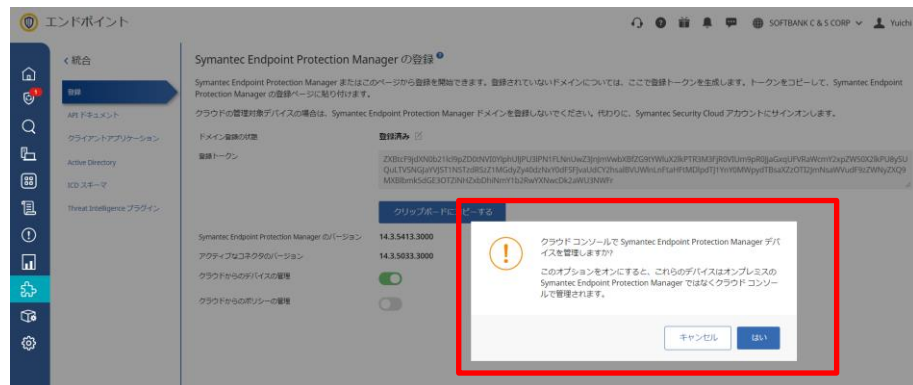
クラウドからのデバイスの管理

②

「クラウドからのデバイスの管理」をオンにします。

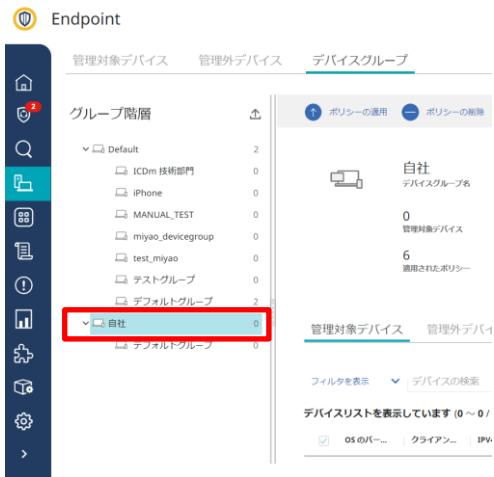
# 3.2デバイス管理

## クラウドからのデバイスの管理



③

確認画面が表示されます。  
「はい」を選択すると、ICDmでSEPM配下のデバイスが管理可能です。



④

SEPMのデバイスグループを作成してみます。  
左タブの「デバイス」を選択し、「デバイスグループ」を選択します。  
SEPM配下のデバイスグループを選択します。

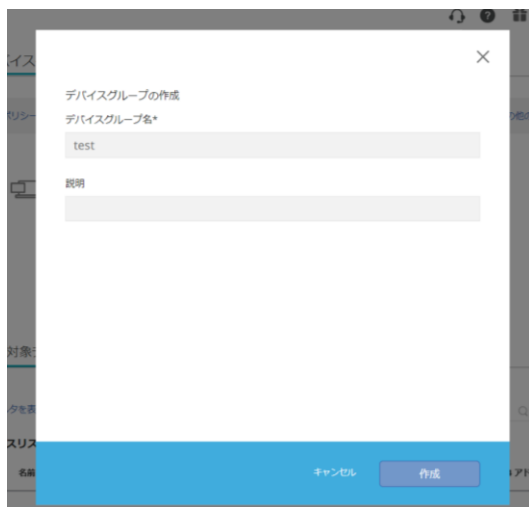
# 3.2デバイス管理

## クラウドからのデバイスの管理



⑤

クラウド経由でSEPM配下のデバイス管理が可能となります。  
左側のタブの「統合」を選択し、「登録」を選択します。



⑥

任意でデバイスグループ名を入力し、「作成」を選択すると、デバイスグループが作成されます。



# 3.2デバイス管理

## クラウドからのデバイスの管理



⑦

デバイスグループが作成された事が確認できます。



⑧

SEPMもデバイスグループが作成された事が確認できます。  
本作業はコチラで完了です。

1

トークンの登録

2

デバイス管理※

3

ポリシー管理※

※任意の手順となります

## ポリシー管理

- SEPM配下のデバイスに対してICDm配下でポリシー管理することが可能です
- SEPM配下のセキュリティイベントをICDmで表示します
- SEPMで利用しているSEPMのポリシーと合わせてICDmのポリシーを利用可能となります

**Point!**



- SEPMとICDm双方のポリシーが適用されます
- 最終的にはフルクラウドに移行する際はポリシーを継続して利用が可能です。



# 3.3ポリシー管理

## クラウドからのポリシーの管理



①

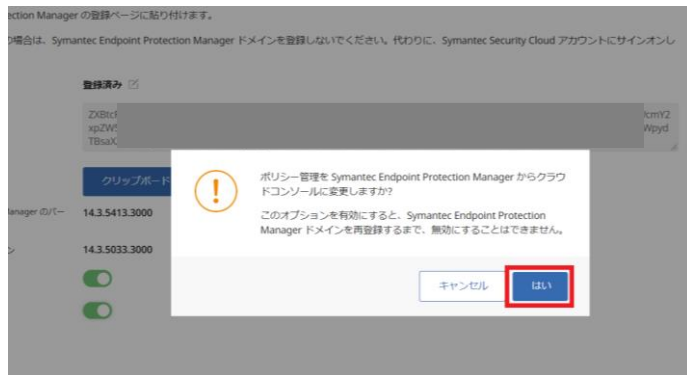
左のタブから「統合」を選択し、「登録」を選択いたします。



②

「クラウドからのポリシーの管理」をオンにします。

## クラウドからのポリシーの管理



③

注意画面が表示されるので、「はい」を選択します。  
本操作を完了すると、ポリシー管理を解除することは不可となります。  
ポリシー管理を解除する際はハイブリッド構成を解除する必要があります。

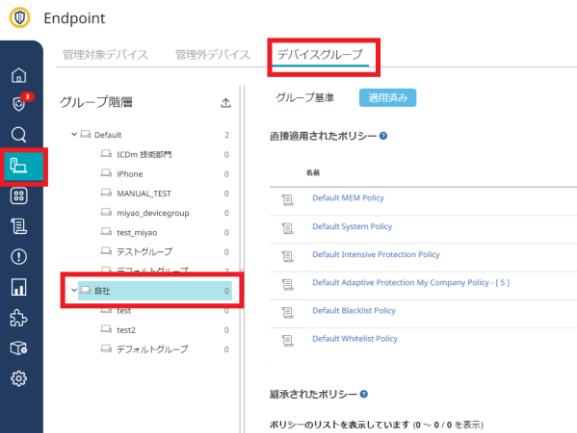


④

設定が完了すると、「正常に完了」の画面が左記画面の様に表示されます。

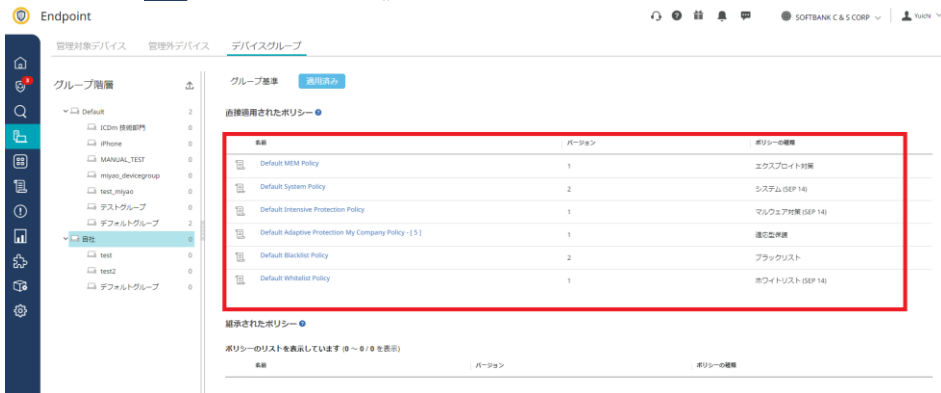
# 3.3ポリシー管理

## クラウドからのポリシーの管理



⑤

ポリシーの確認を行います。  
左のタブから「デバイス」を選択し、「デバイスグループ」を選択します。  
SEPMのデバイスグループを選択します。



⑥

デフォルトでポリシーが適用されています。  
ポリシーの管理設定はこちらで完了です。  
デフォルトで適用されるポリシーはP.94をご確認ください。

### ハイブリッド環境下のSEPMで適用可能なセキュリティポリシー

ポリシー管理をオンにすると、ICDmでは下記ポリシーが適用可能となります。

- ・ **Default Intensive Protection Policy**

ウイルススキャンに関わる設定や疑わしいファイルに対する処置方法の設定についてまとめられています。

- ・ **Default MEM Policy**

MEM(Memory Exploit Mitigation)はシグネチャレスでOSを強化し未知のウイルスからの攻撃を阻止する機能です。

各機能の有効/無効化や推奨外のアプリケーションの保護に関する設定についてまとめられています。

- ・ **Default System Policy**

Liveupdate先のサーバやスケジュールやクライアントのアップグレード間隔などの設定についてまとめられています。

- ・ **Default Blacklist Policy**

遮断するファイルをSHA-256やMD5のハッシュ値によって設定するポリシーです。

- ・ **Default Whitelist Policy**

スキャンを除外するファイル、URL、その他の項目を設定するポリシーです。

- ・ **Default Adaptive Protection Policy**※ (SES-C) 限定

MITRE ATT&CKに基づき、不審な挙動を隔離するポリシーです。

標的型攻撃を保護するために、通常利用するアプリケーションから実行される疑わしい動作を検知することにより攻撃対象領域を減らすことが可能です。

# 4. Appendix



## ■ 通信先URL

エージェントおよびSEPMとICDMとの連携に必要なポートとURLが記載されています。

<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Troubleshooting/urls-to-whitelist-for-v129099891-d4155e9710.html>

## ■ 通信量

エージェントの各機能で使用する帯域幅の量が記載されています。

<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Troubleshooting/network-usage-data-v131977301-d4155e10338.html>

低帯域モードでも利用可能です

<https://techdocs.broadcom.com/jp/ja/symantec-security-software/endpoint-security-and-management/endpoint-security/sescloud/Dialog-Help/Policies-Help/general-settings-v129409706-d4155e21722.html>

# SES ICDmのSLA等

SESのクラウド利用などにあたりSLAがメーカーから公開されております。

<https://docs.broadcom.com/doc/endpoint-security-ses-sesc-sess-saas-listing>

### Technical Support

If CA is providing Technical Support to Customer, Technical Support is included as part of the Service as specified below. If Technical Support is provided by a reseller, this section does not apply.

- Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published and technical support policies published at [https://support.symantec.com/en\\_US/article.TECH236428.html](https://support.symantec.com/en_US/article.TECH236428.html).
- Once a severity level is assigned to a Customer submission for Support, CA will make every reasonable effort to respond per the published policies.

### Maintenance to the Service and/or supporting Service Infrastructure

CA must perform maintenance from time to time. For information on Service status, planned maintenance and known issues, visit <https://status.symantec.com/> and subscribe to Symantec Status via email, SMS, or Twitter to receive the latest updates. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, CA will provide seven (7) calendar days' notification posted on Symantec Status.
- **Unplanned Maintenance:** Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. CA will provide a minimum of one (1) calendar day notification posted on Symantec Status. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times CA will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.
- **Note:** For Management Console Maintenance, CA will provide fourteen (14) calendar days' notification posted on Symantec Status. CA may perform minor updates or routine maintenance to the Management Console with no prior notification as these activities do not result in Service disruption.

\* Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the request).

\*\* A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding weekends and local public holidays. In most cases, "business days" mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone.

### 2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. Availability SLAs may exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately:

- **Inline Service Availability** means access to the core features of the Service that impact the data in transit to and from Customer to the Internet.

Inline Service Availability	N/A
-----------------------------	-----

- **Non-inline Service Availability** is access to the controls that govern the features of the Service that do not impact data in transit to and from the end-user to the Internet (e.g., reporting tools used by the administrator). Examples of Non-Inline Service for this Service include:

- Accessing the Management Console and APIs
- Managing policies and configuration
- Generating reports
- Downloading data, statistics, security and audit events
- Downloading information about Devices
- Downloading commands to Devices
- Downloading Data Analytics/Forensic Analysis with alerting (EDR)
- Downloading/Deletion of malicious files and associated artifacts on all impacted endpoints (EDR)
- Downloading reports (EDR)

Non-Inline Service Availability	99.5%
---------------------------------	-------

**SB C&S**