
Symantec Endpoint Security
SEP⇒SES移行ガイド

本資料について

SB C&S

・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 ・SEPMポリシー移行の項番を「2.3」⇒「2.2」に変更 ・クライアント移行の項番を「2.2」⇒「2.3」に変更 ・P18の内容を編集 ・P39、P40の内容を追加

アジェンダ

SB C&S

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）

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

SB C&S

攻撃前段階	侵入		感染			蔓延				情報流出		
事前攻撃	初期アクセス		実行	再攻撃	特権昇格	防衛回避	クレデンシャルアクセス	発見	横断的な攻撃	収集	外部流出	C&Cサーバ
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	振る舞い監視	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	

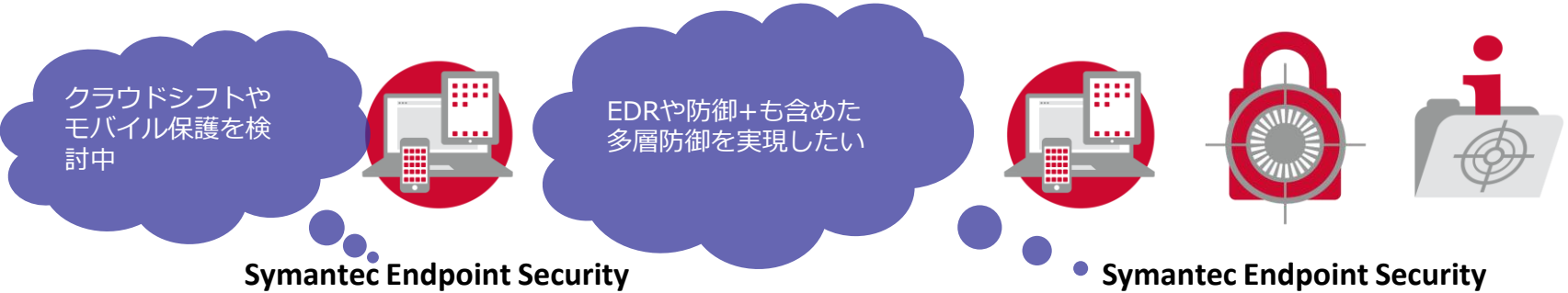
検出 & 対処 – フライトデーターレコーダー(Flight Data Recorder) | 振舞いフォレンジックス | 標的型攻撃クラウド分析 | Threat Hunter 分析

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リート

SB C&S



Symantec Endpoint Security
Enterprise

- 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
Complete

- 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

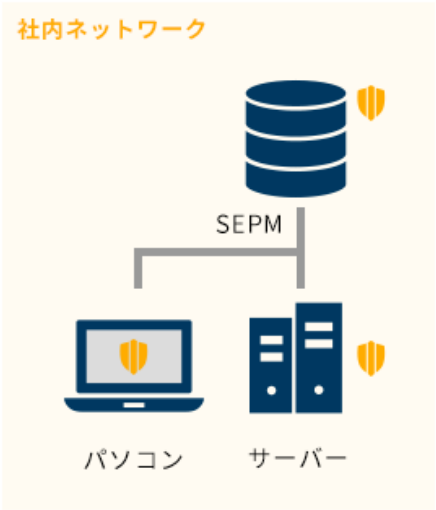
SESなら様々な運用パターンが可能

SB C&S

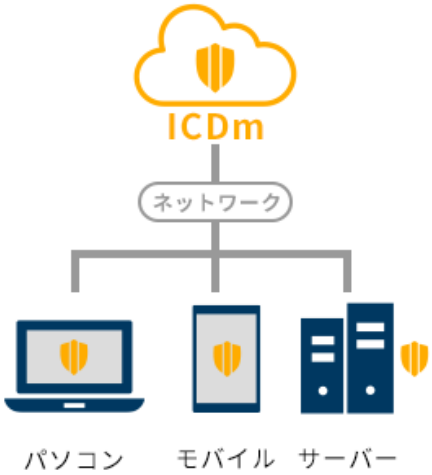
オンプレミス、クラウドまたはハイブリッドで管理可能

※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

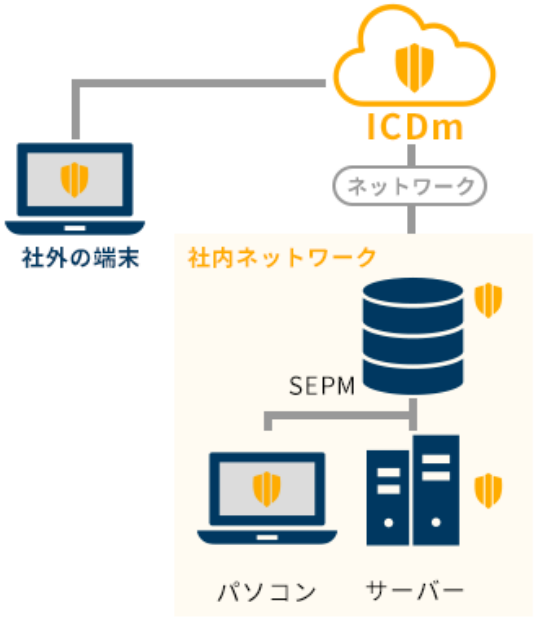


クラウドで管理



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

SB C&S

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。

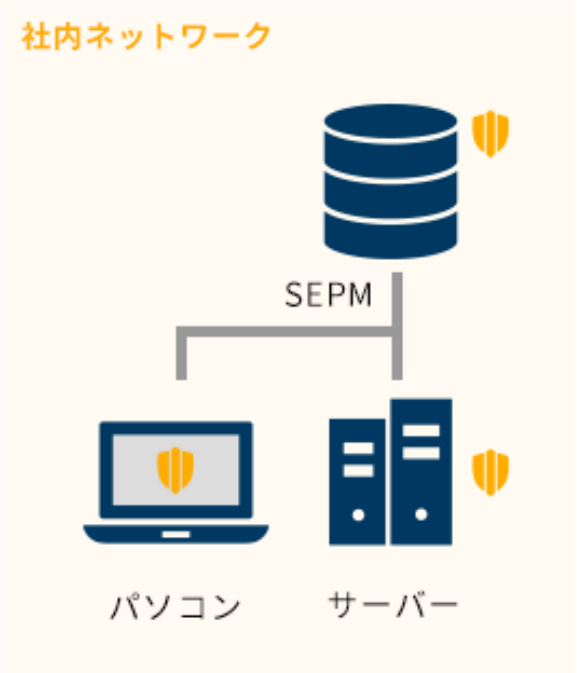
・**SES**
ICDmに直管理されているエージェントの呼称です。

2. フルクラウド移行手順

フルクラウドへ移行

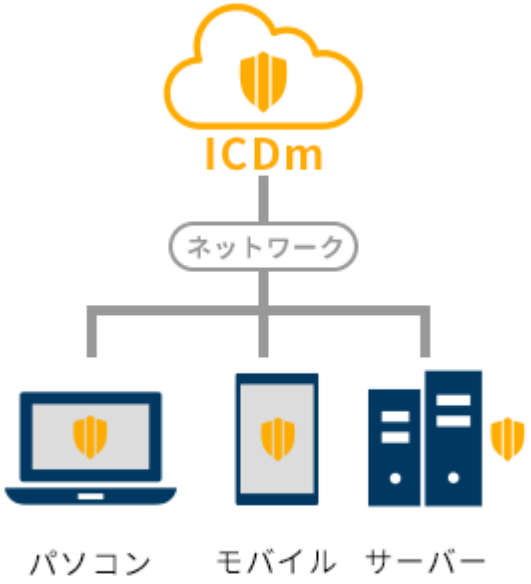
SB C&S

オンプレミスで管理



管理をSEPMからICDmへ

クラウドで管理

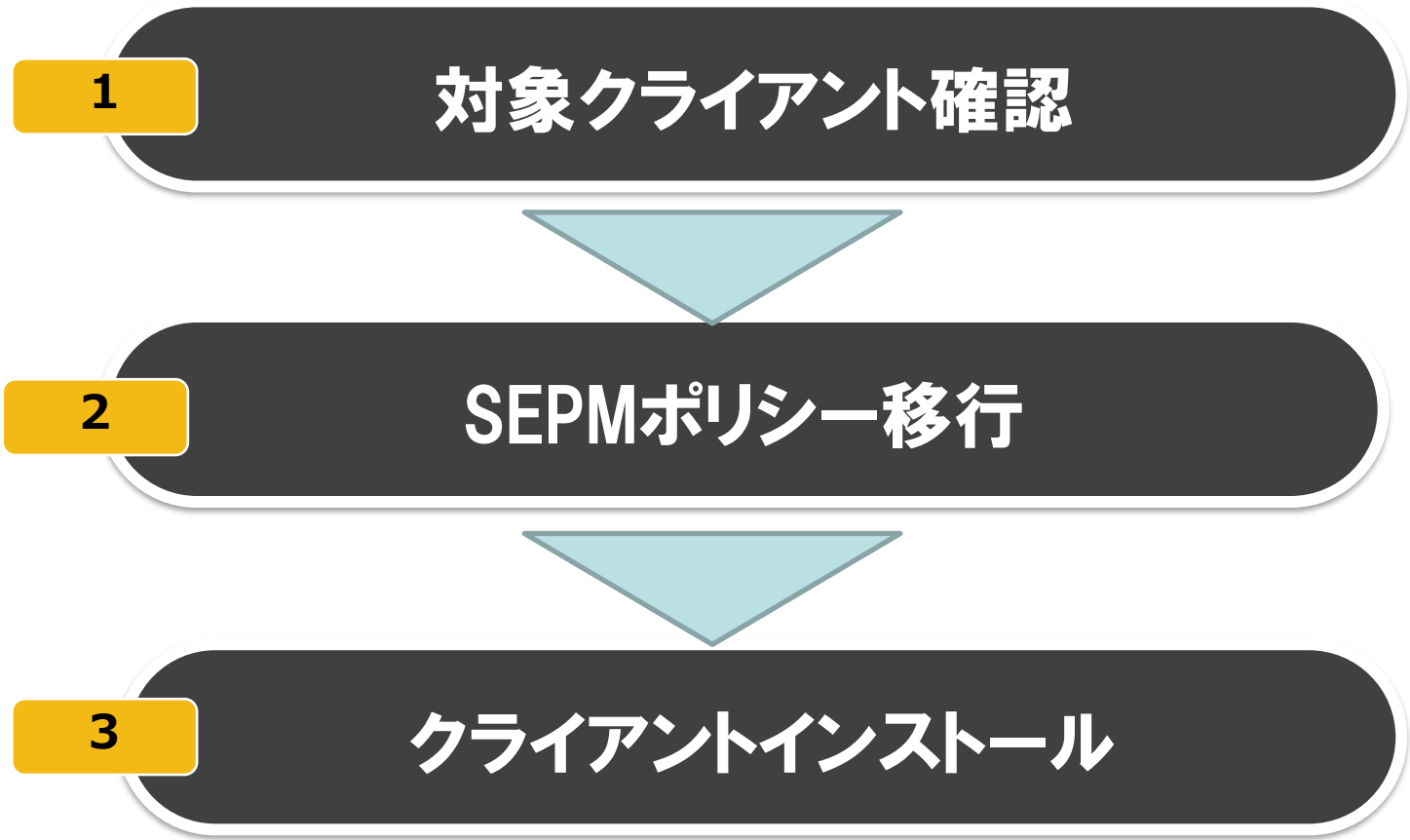


社内・社外のネットワークは
問わずクラウドで一斉管理

フルクラウドへ移行

SB C&S

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。



フルクラウドへ移行

SB C&S

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

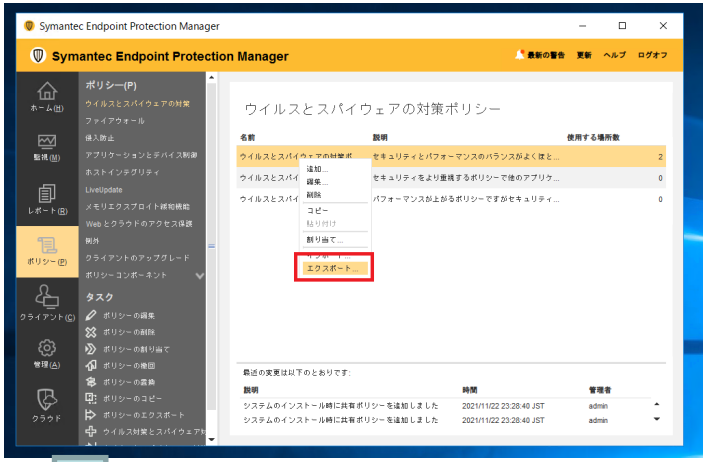
Symantec Endpoint Protectionを開き、「ヘルプ」＞「トラブルシューティング」＞「管理」
から確認可能です。

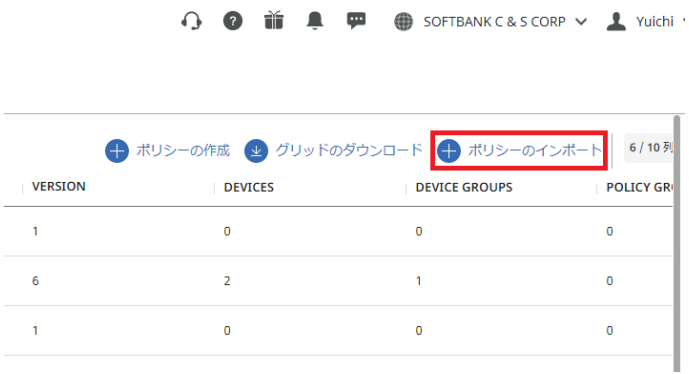
フルクラウドへ移行

SB C&S

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。

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。

2.2ポリシー移行

SB C&S

・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

2.2ポリシー移行

SB C&S

■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ございます。
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

SB C&S

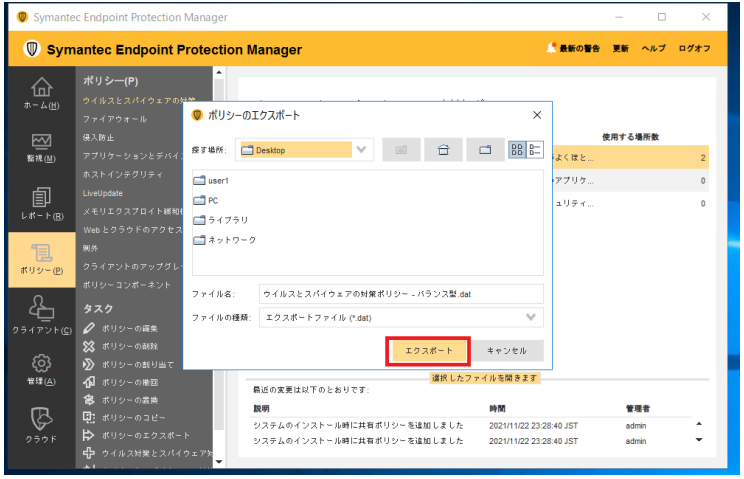
■ポリシー継承について

・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。

・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

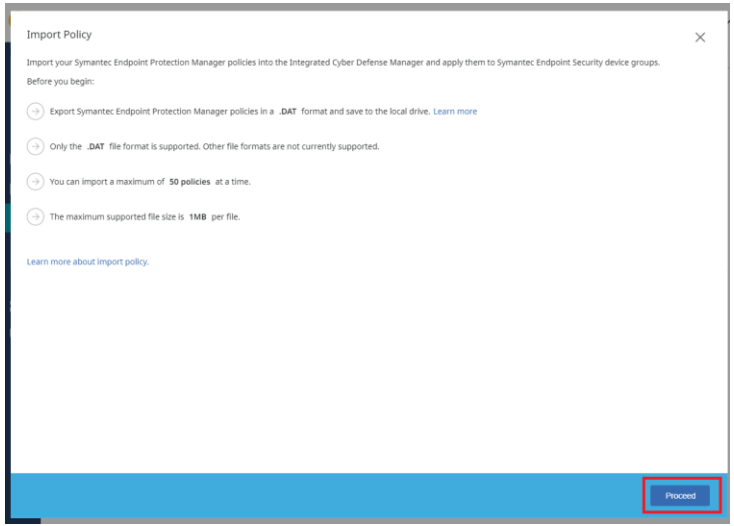
エージェントが現在、SEPM配下で管理されているか確認します。

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

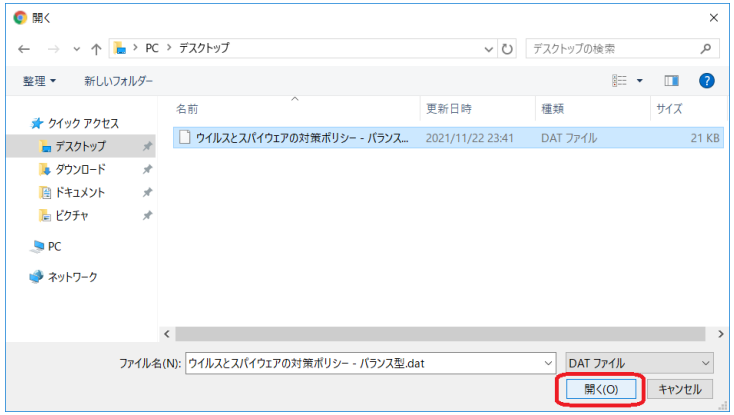
ICDmの設定に移ります。

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

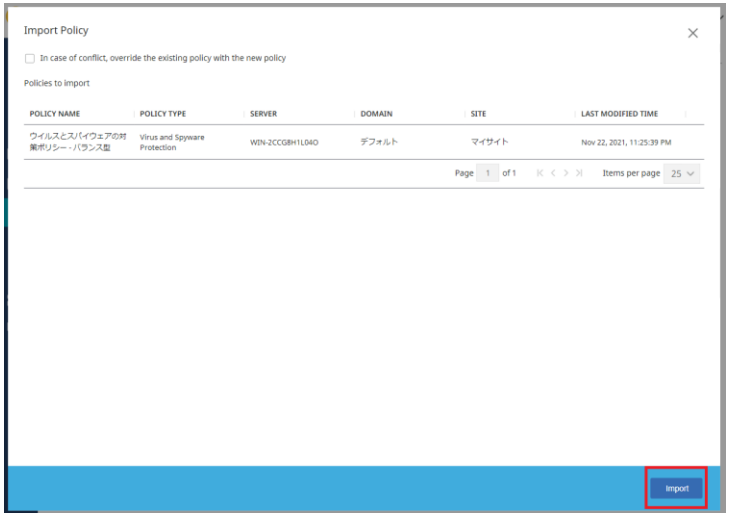
インポートに関する案内が表示されるので、「Proceed」を選択します。

2.2ポリシー移行



⑤

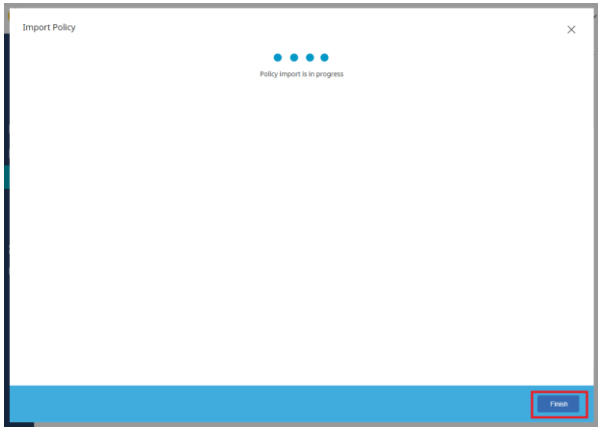
手順②でエクスポートしたポリシーを選択し、「開く」を選択します。



⑥

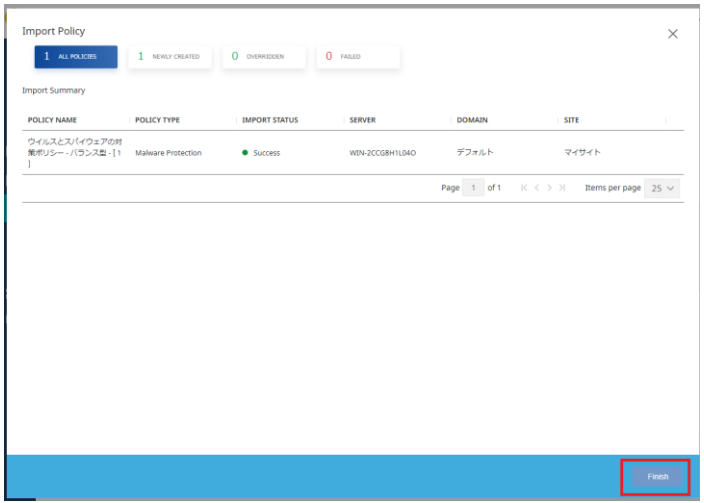
インポートしたポリシーの確認画面が表示されるので、「Import」を選択します。

2.2ポリシー移行



⑦

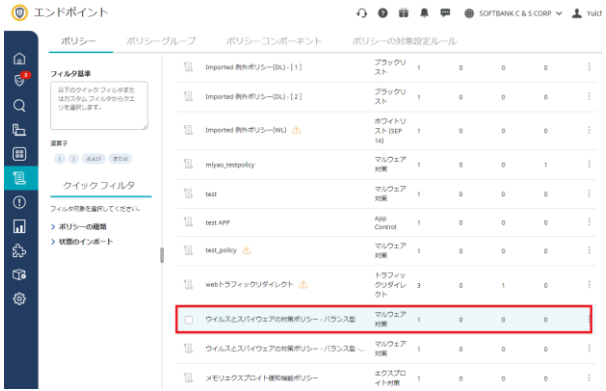
インポートのプロセスが実行されます。



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



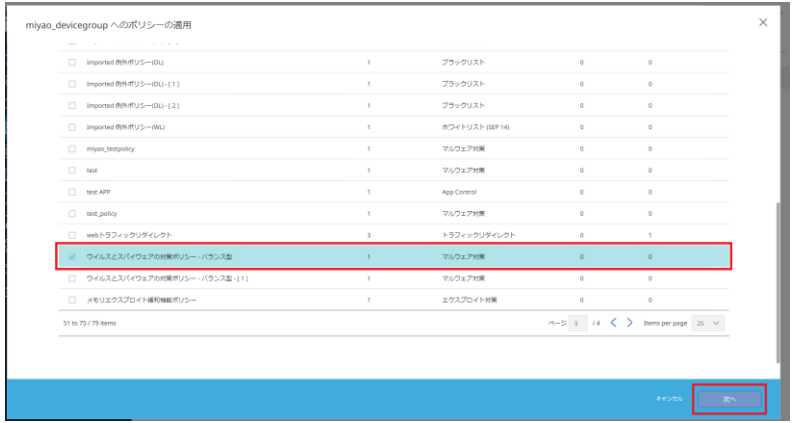
⑨

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

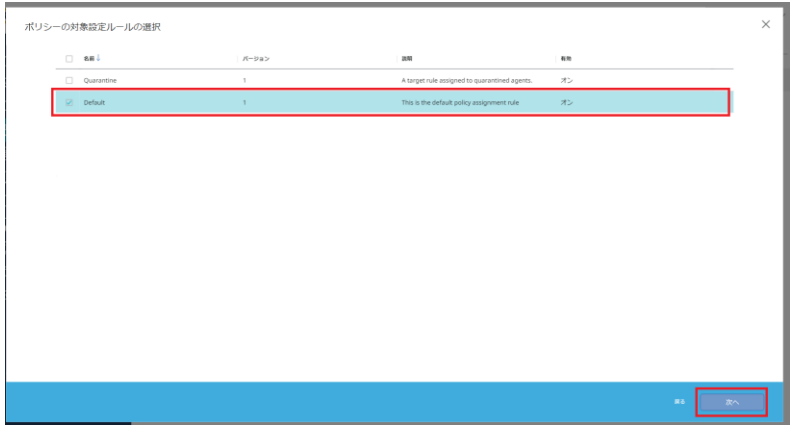
インポートしたポリシーをデバイスグループに適用する際は、「デバイス」＞「デバイスグループ」、対象のデバイスグループを選択し、「ポリシーの適用」を選択します。

2.2ポリシー移行



⑪

インポートしたポリシーを選択し、「次へ」を選択します。



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。

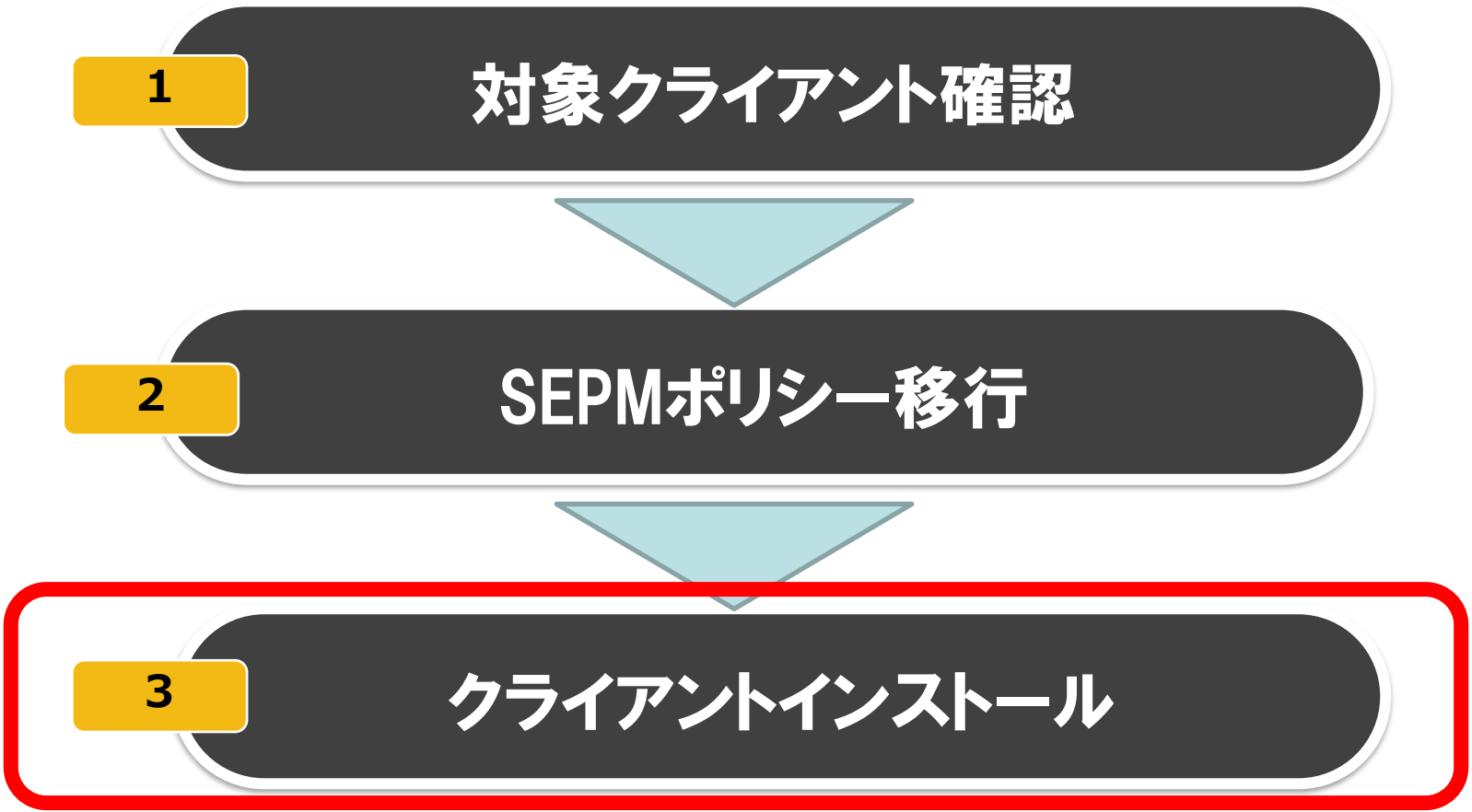
⑭

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

SB C&S

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。

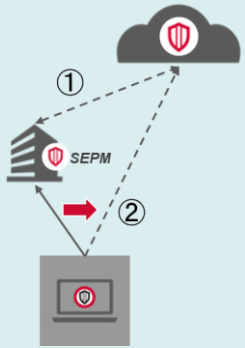


2.3クライアント移行

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

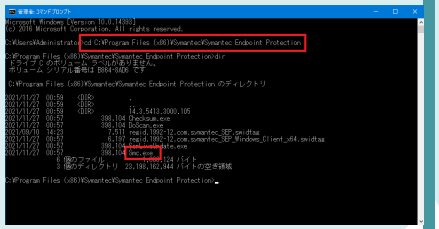


2. インストーラーで手動インストール

・クラウド版インストーラでインストール

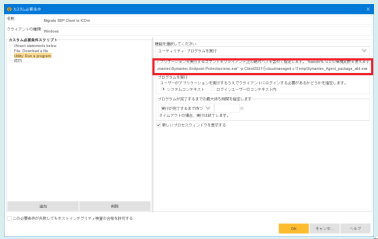
3. smcコマンドで移行

・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

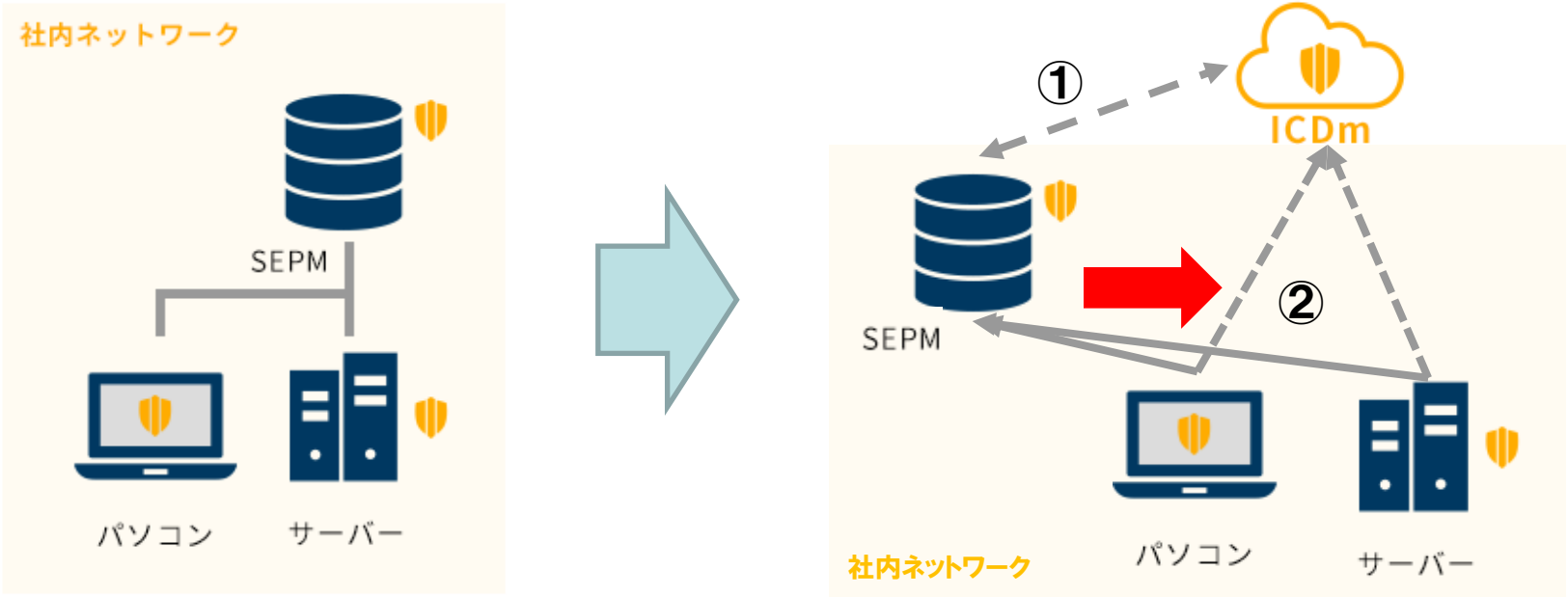


4. ホストインテグリティポリシーで移行

・SEPMのポリシーを利用して移行



2.3.1Switch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

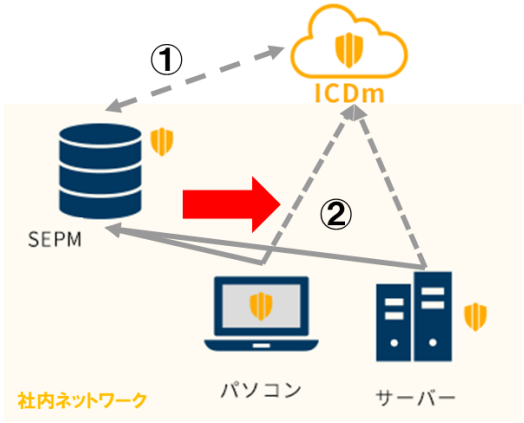
・デバイスグループごとに移行し、子グループも自動的に移行されます

2.3.1 Switch機能で移行

SB C&S

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

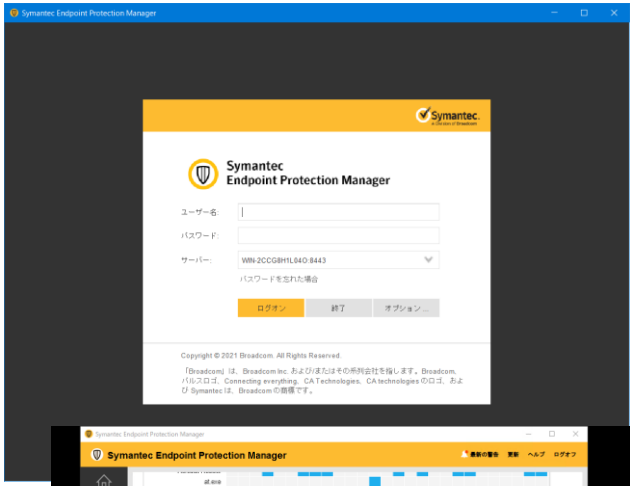
①

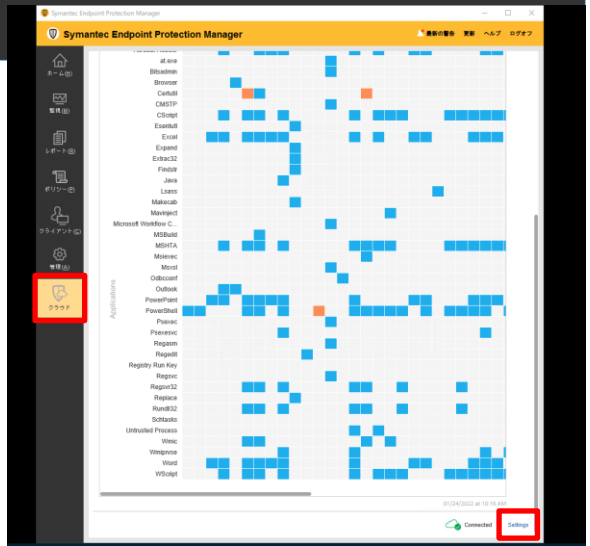
左のタブの「統合」を選択し、「登録」を選択します。

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





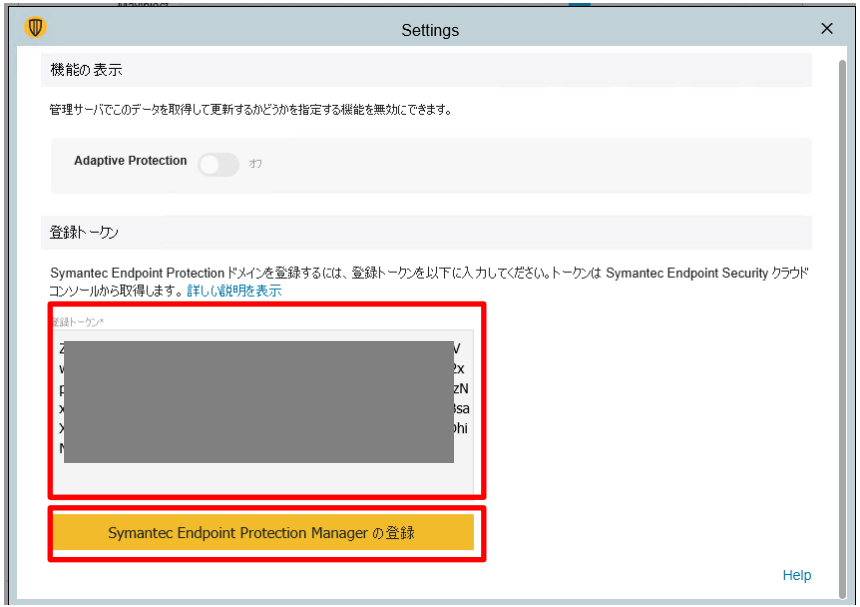
③

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

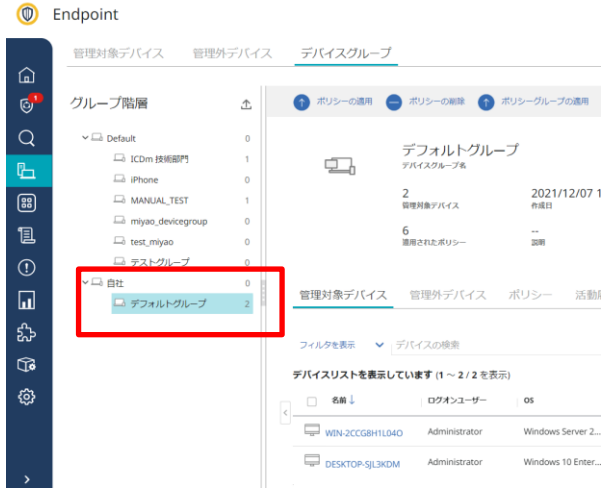
⑥

「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



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

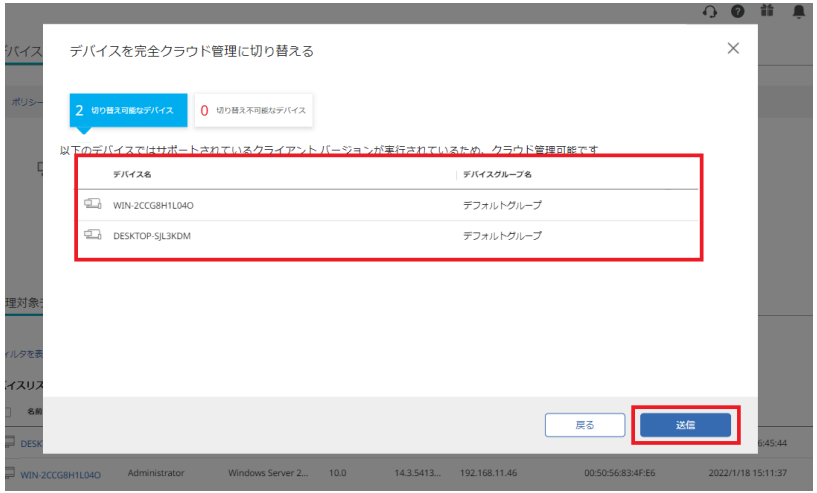
⑨

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

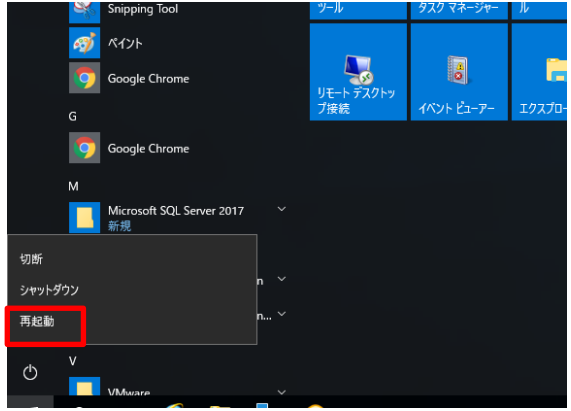
⑮

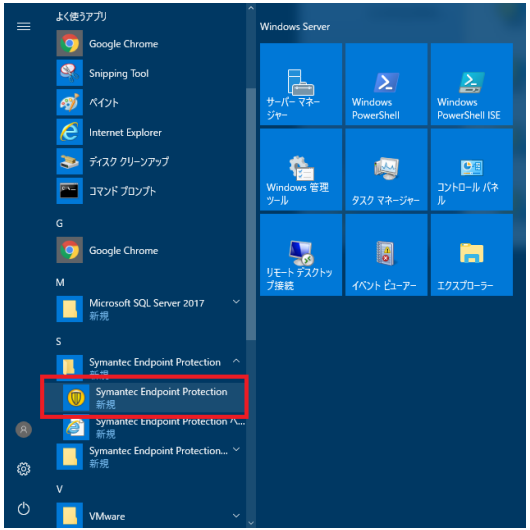
「デバイス切り替えプロセスが正常に完了しました」と表示されるとデバイスの移行が完了となります。

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。

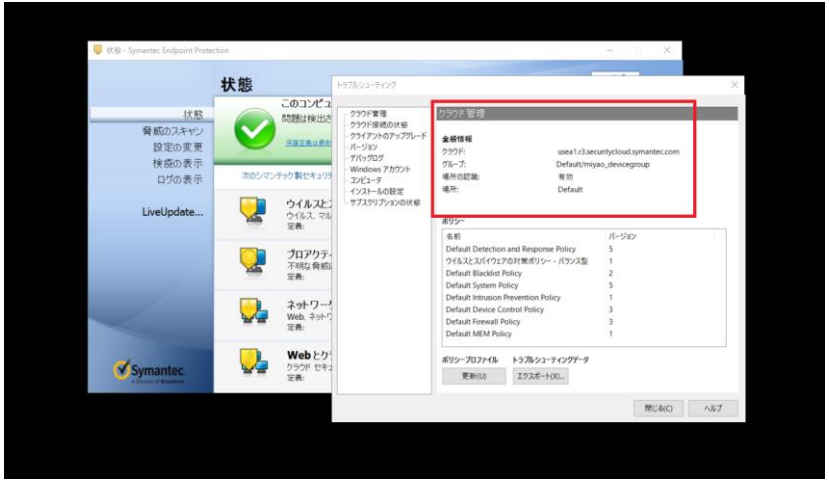
スタートから「Symantec Endpoint Proteciton」を選択します。

2.3.2インストーラーで手動インストール

SB C&S

⑲

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

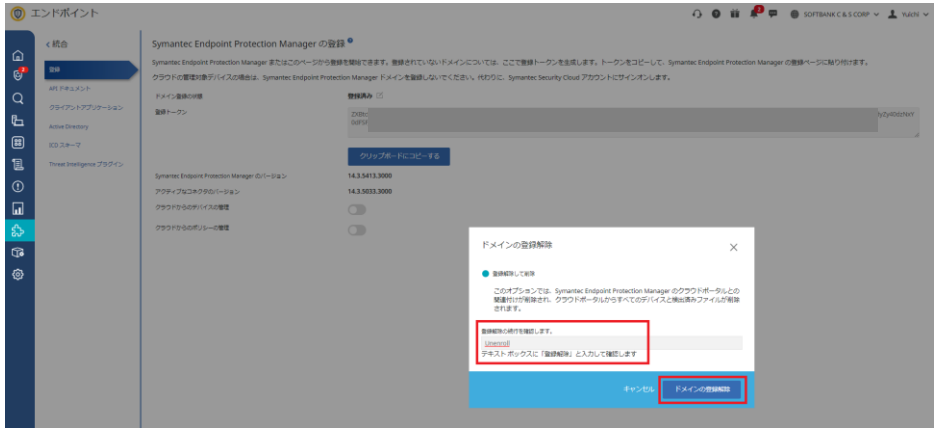
㉑

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。

㉒

「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



⑬

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。

⑭

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。

2.3.1 Switch機能で移行（ポリシー設定）

SB C&S

■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おります。

・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おります。

・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おります。

・Default System Policy

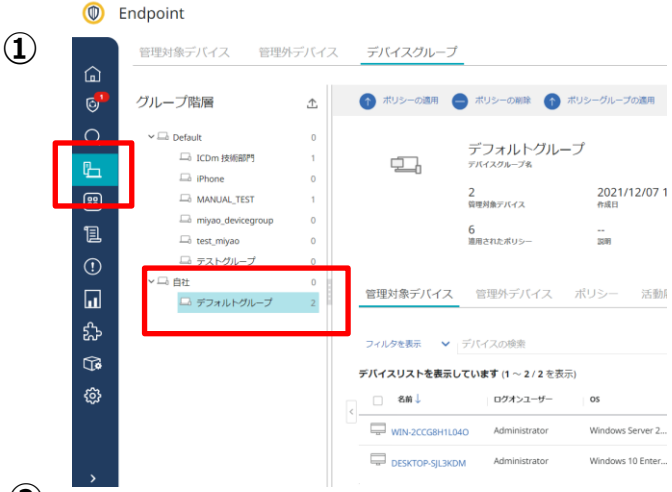
Liveupdate先のサーバやスケジュールやクライアントのアップグレード間隔などの設定についてまとめられております。

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

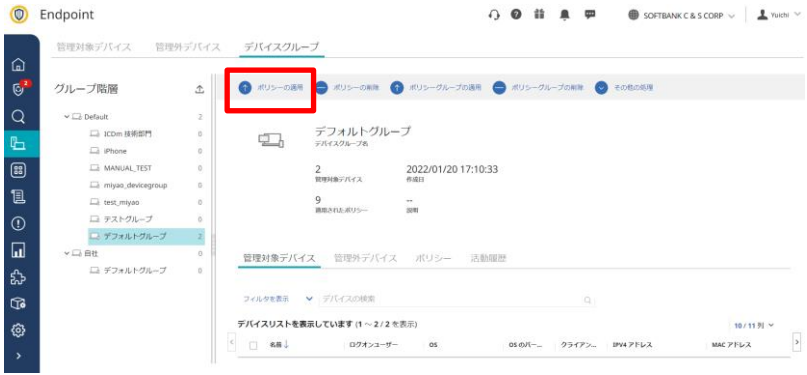
2.3.1 Switch機能で移行（ポリシー設定）

SB C&S

①



②



①

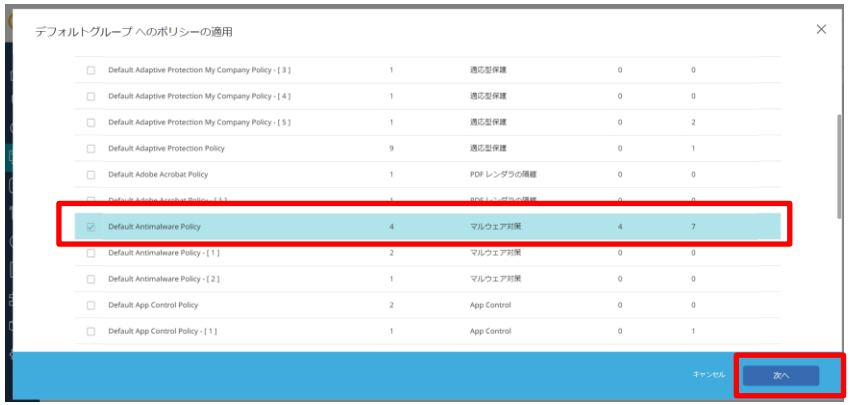
左タブより「デバイス」を選択し、「デバイスグループ」を選択します。
移行したデバイスグループを選択します。

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）

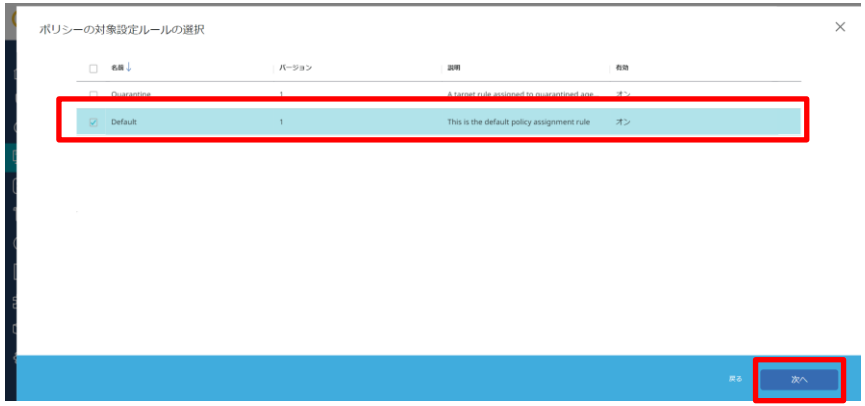
③



③

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

④

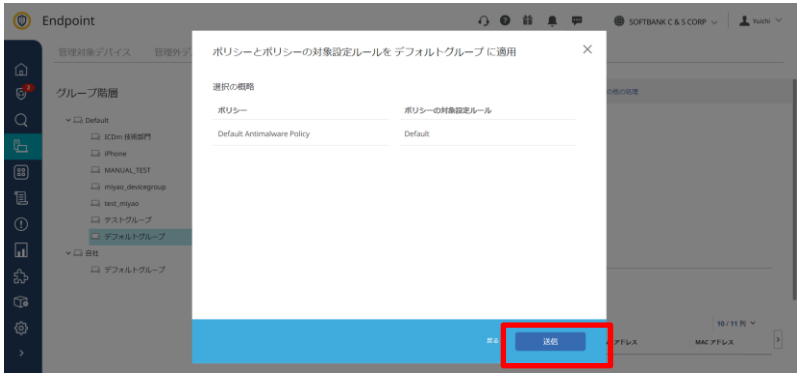


④

「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

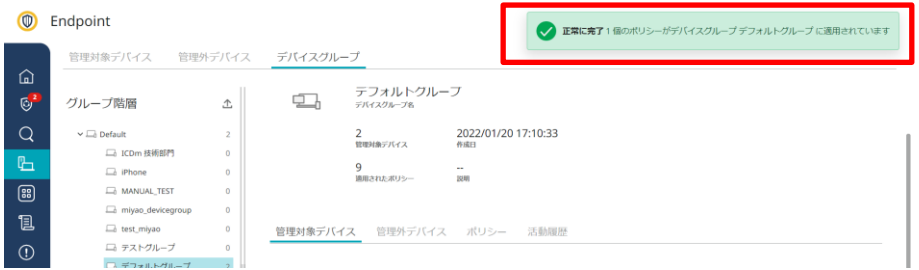


⑤

「送信」を選択します。

2.3.1 Switch機能で移行（ポリシー設定）

⑥



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

⑦

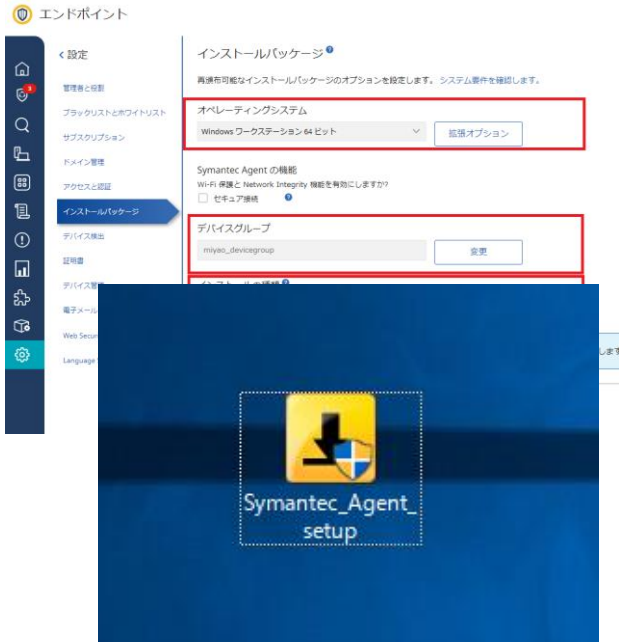
対象のデバイスグループの「ポリシー」を選択し、適用されたポリシーが確認できます。
以上で設定は完了です。

2.3.2インストーラーで手動インストール

SB C&S

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

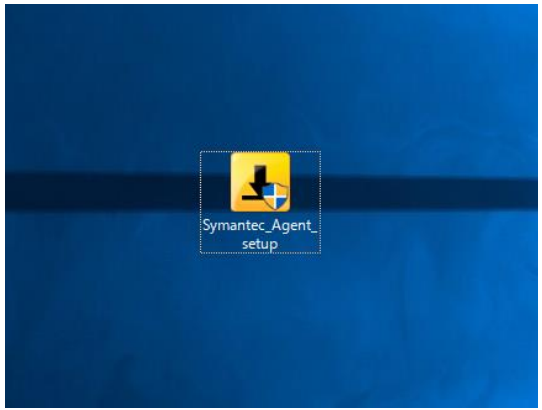
①

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



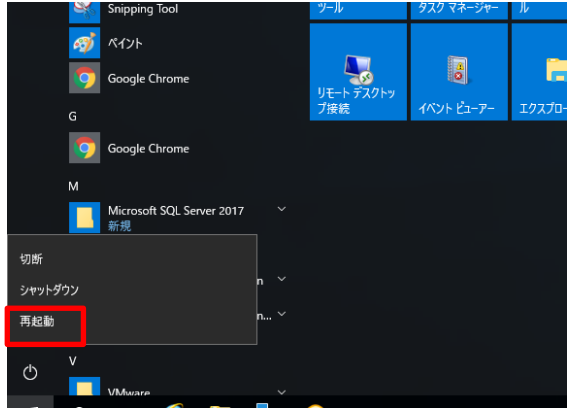
③

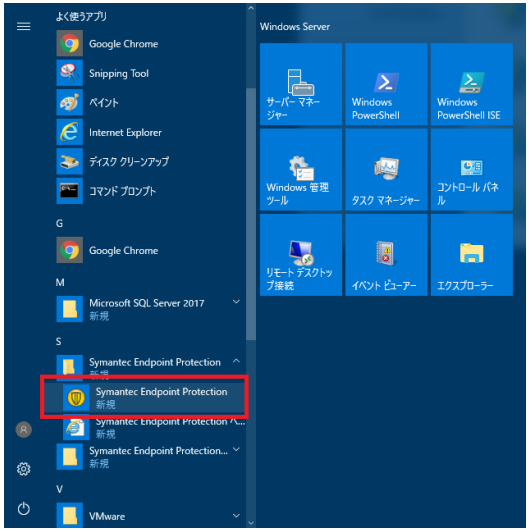
インストーラーを実行します。

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。

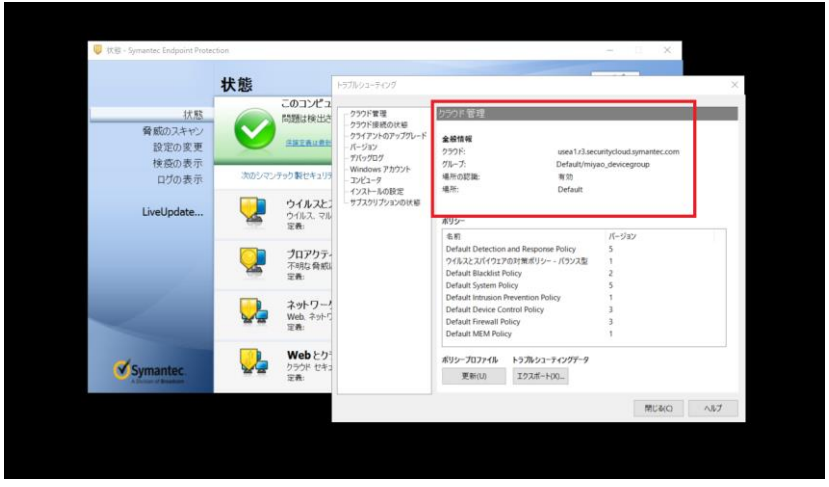
スタートから「Symantec Endpoint Proteciton」を選択します。

2.3.2インストーラーで手動インストール

SB C&S

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

⑨

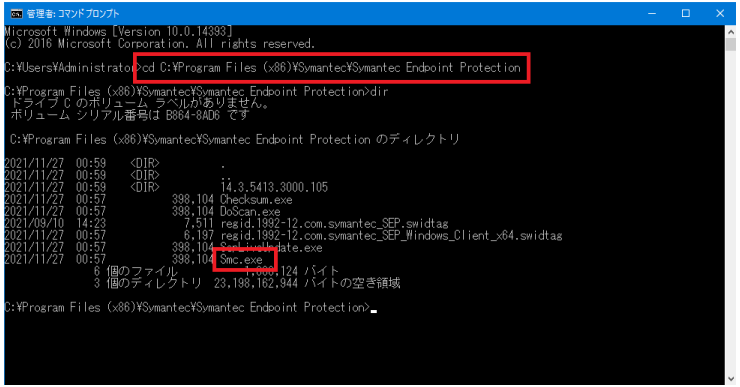
ICDmでも、「デバイス」＞「デバイスグループ」から対象のデバイスグループを選択します。
「管理対象デバイス」でも確認できます。
本作業はこちらで完了です。

2.3.3 smcコマンドで移行

SB C&S

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



- 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

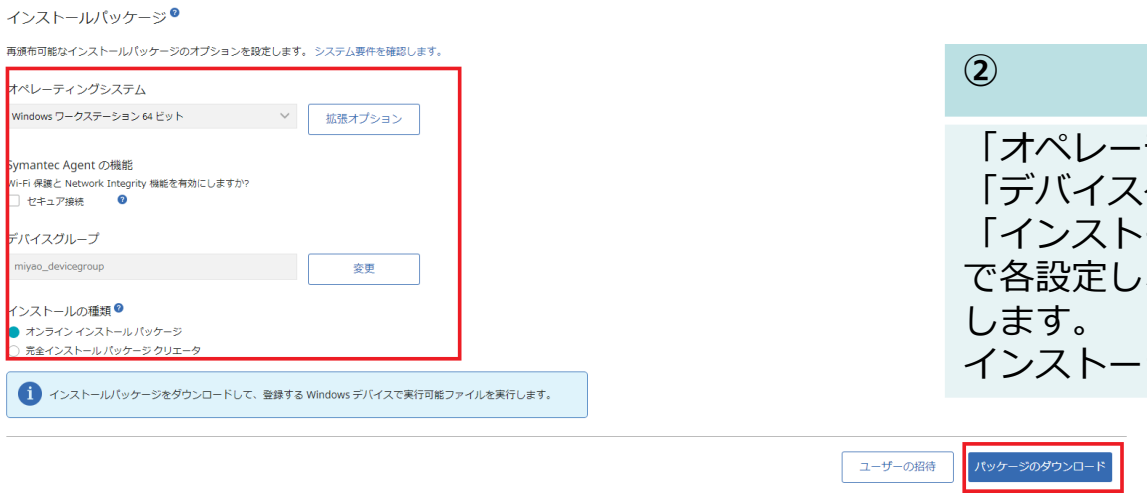
※smc：Symantecが提供しているコマンドラインインターフェース。 Windowsクライアントサービスを実行できます。

2.3.3 smcコマンドで移行

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。

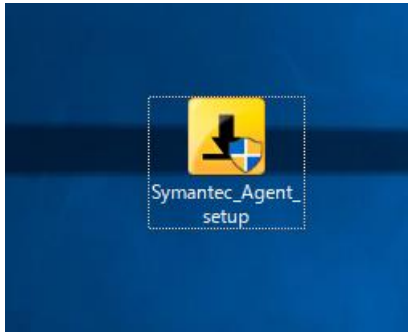
2.3.3 smcコマンドで移行



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。

2.3.3 smcコマンドで移行



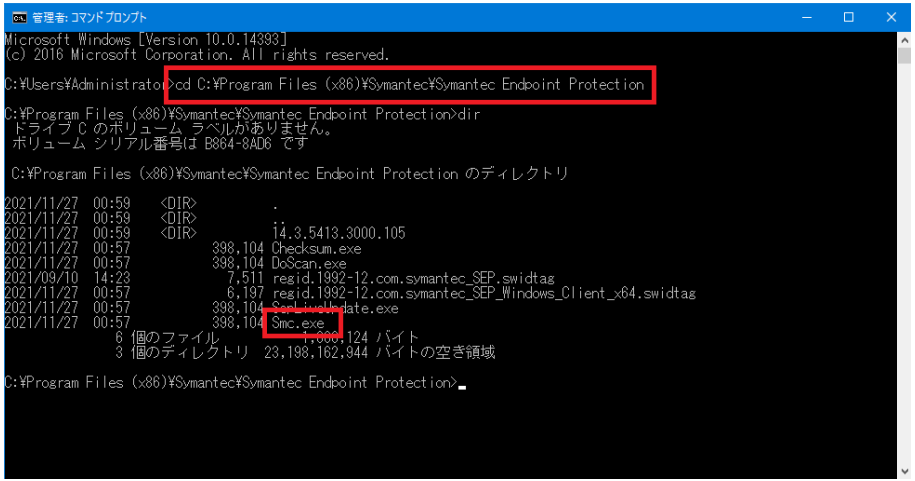
③

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

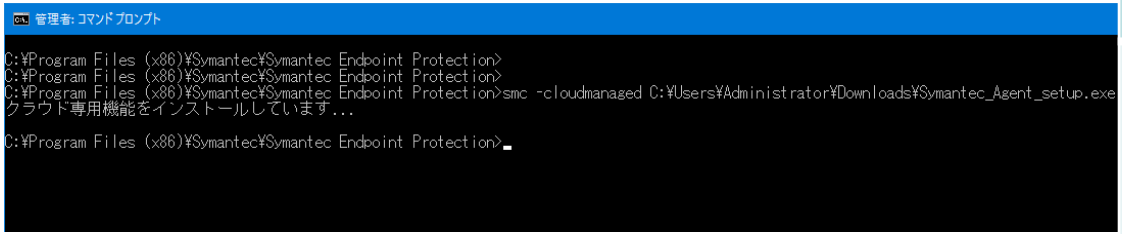
対象端末から「コマンドプロンプト」を実行します。

2.3.3 smcコマンドで移行



⑤

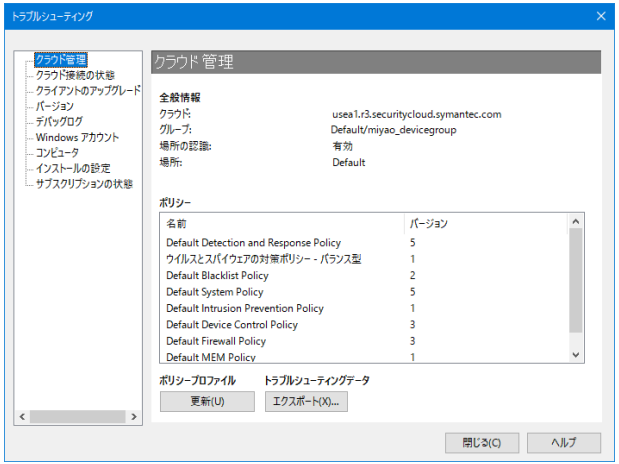
Symantec Endpoint Protectionのフォルダに移動します。
「Smc.exe」がある事を確認します。
デフォルトでは、以下に配置されています。



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

⑨

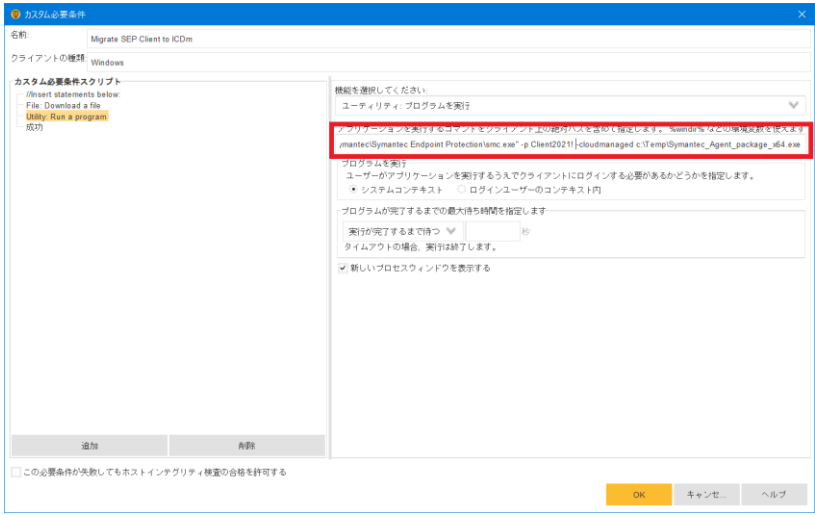
ICDmでも、「デバイス」＞「デバイスグループ」から対象のデバイスグループを選択します。
「管理対象デバイス」でも確認できます。
本作業はこちらで完了です。

2.3.4ホストインテグリティポリシーで移行

SB C&S

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

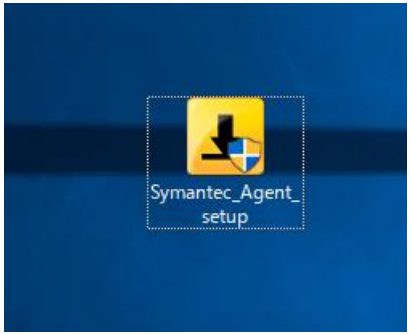
①

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

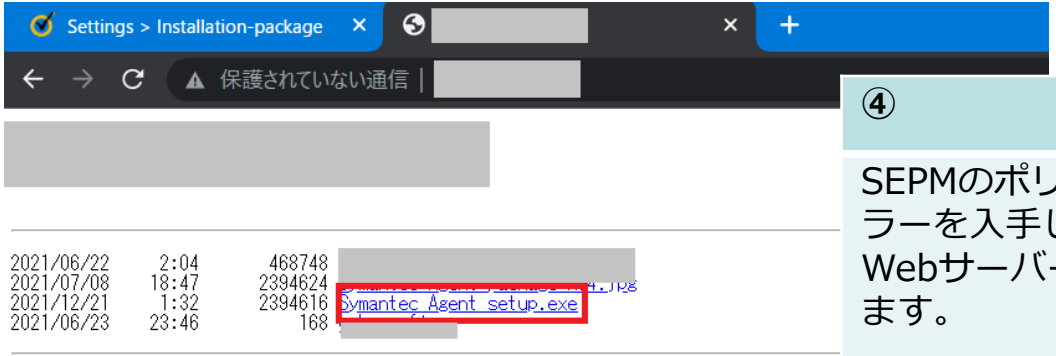
「オペレーティングシステム」
「デバイスグループ」
「インストールの種類」
で各設定し、「パッケージのダウンロード」を選択します。
インストーラーが端末にダウンロードされます。

2.3.4ホストインテグリティポリシーで移行



③

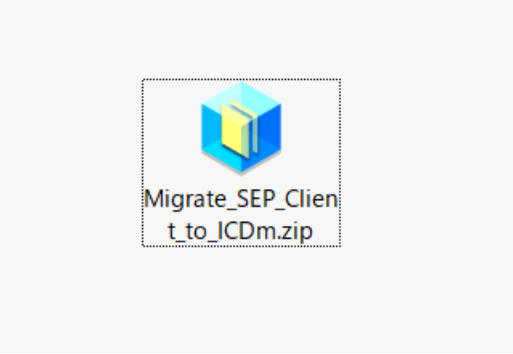
左側のタブより「設定」を選択し、「インストールパッケージ」を選択します。



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。

2.3.4ホストインテグリティポリシーで移行

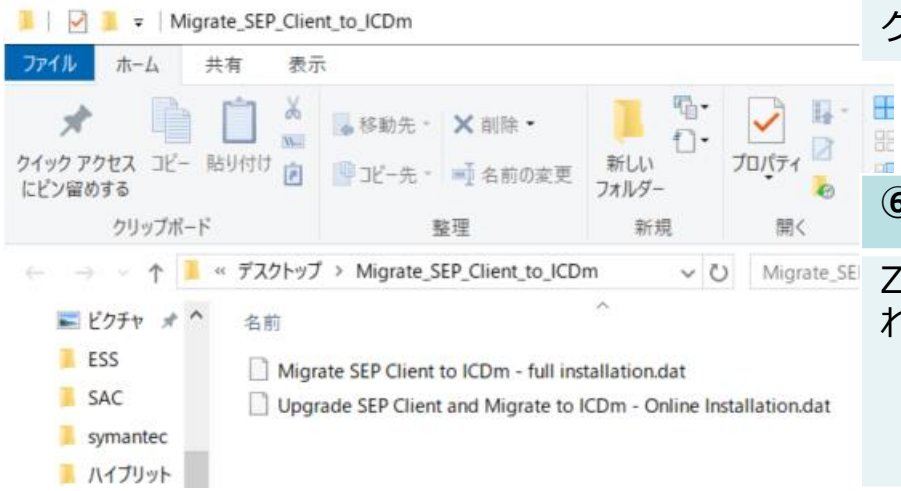


⑤

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

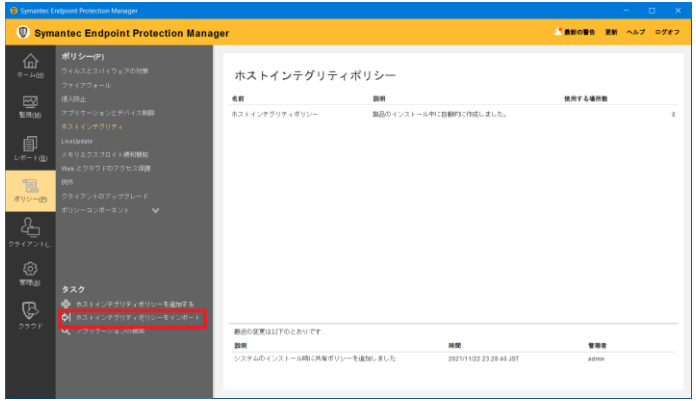
メーカーサイトのリンクになっている「Migrate_SEP_Client_to_ICDm.zip」をクリックします。



⑥

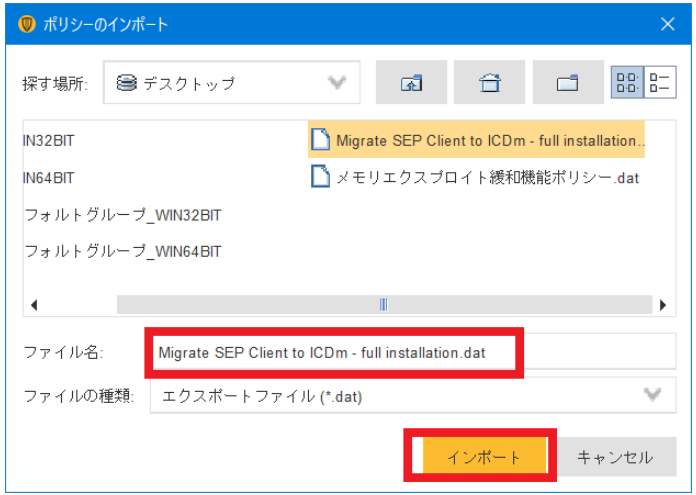
Zipファイルを展開すると2つのファイルが格納されております。

2.3.4ホストインテグリティポリシーで移行



⑦

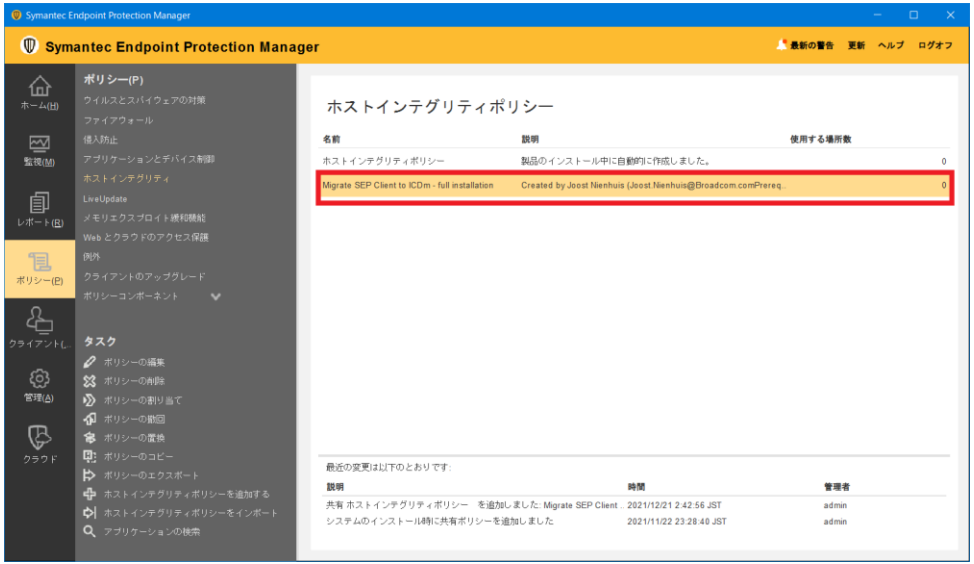
SEPMの操作になります。
SEPMにログイン後、「ポリシー」を選択し、「ホストインテグリティ」＞「ホストインテグリティポリシーをインポート」
を選択します。



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。

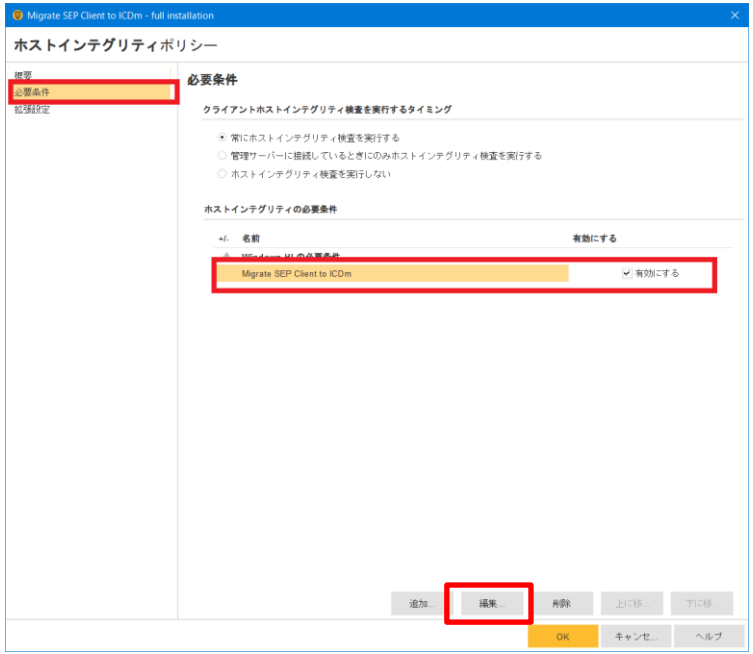
2.3.4ホストインテグリティポリシーで移行



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。

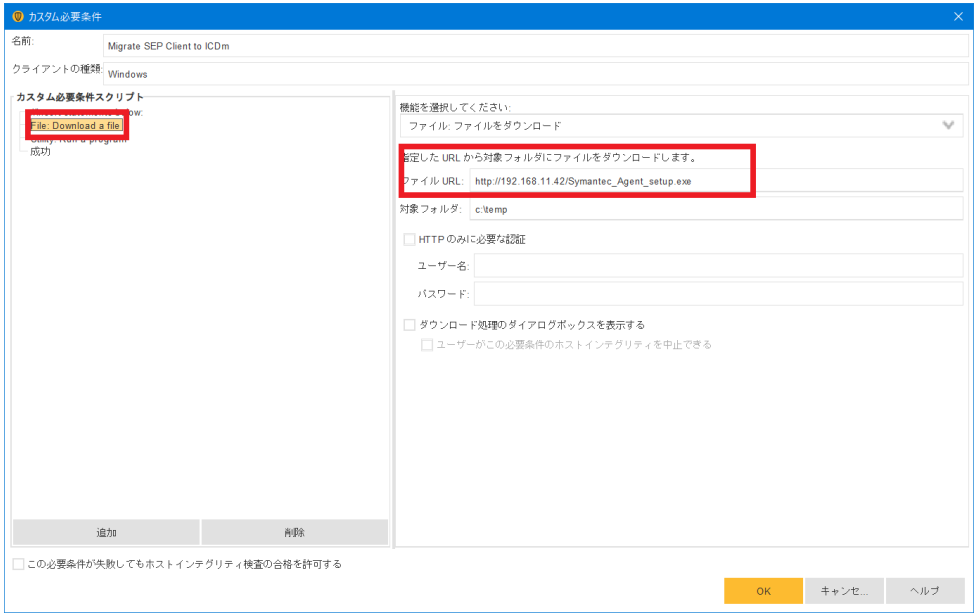
2.3.4ホストインテグリティポリシーで移行



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。

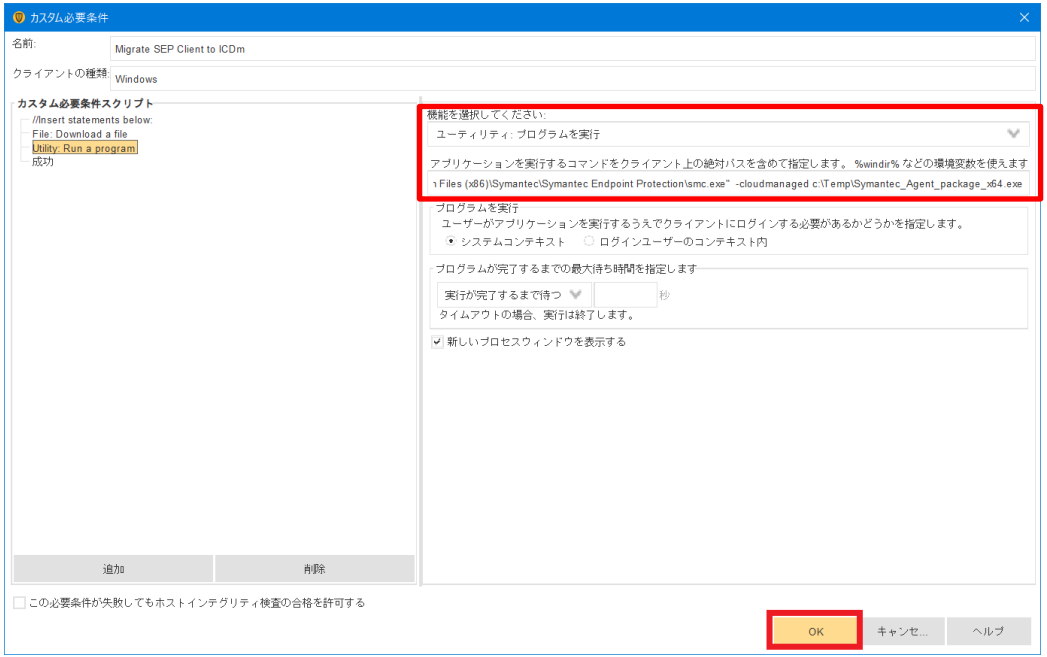
2.3.4ホストインテグリティポリシーで移行



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



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：

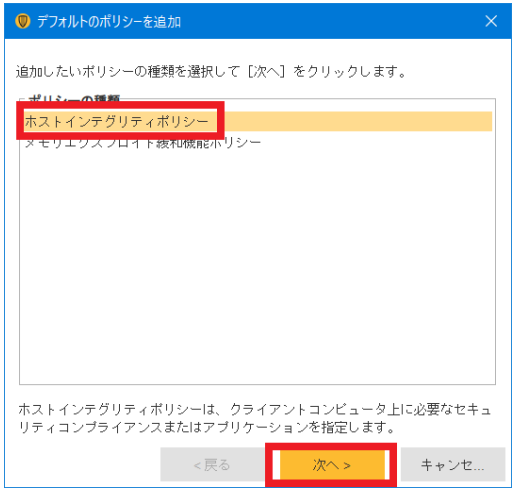
「"c:¥Program Files (x86)¥Symantec¥Symantec Endpoint Protection¥smc.exe" -cloudmanaged c:¥Temp¥Symantec_Agent_package_x64.exe」

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

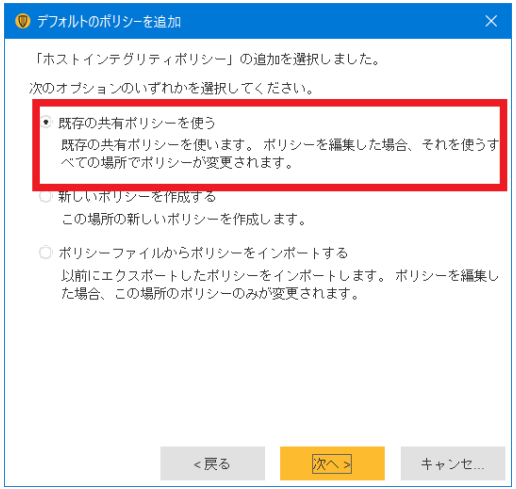
適用するデバイスグループに設定したポリシーを有効にします。
左の「クライアント」を選択し、「ポリシー」を選択します。
「場所固有のポリシー」から「ポリシーの追加」を選択します。



⑭

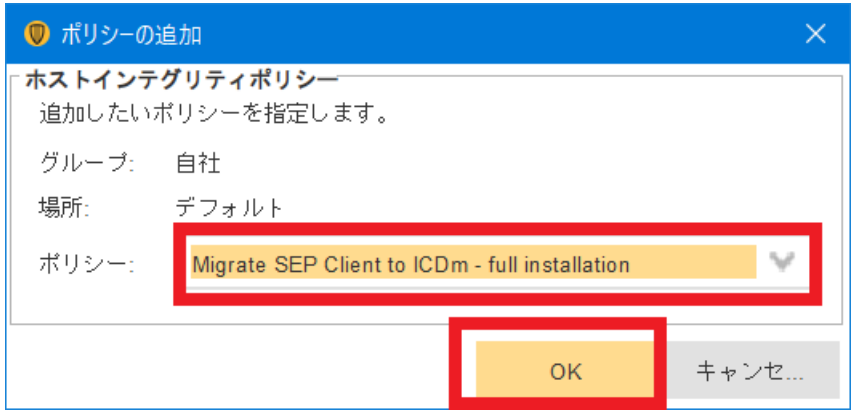
「ホストインテグリティポリシー」を選択して「次へ」を選択します。

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

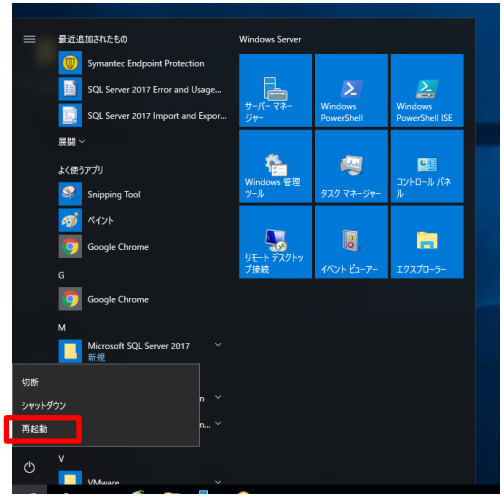
⑰

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

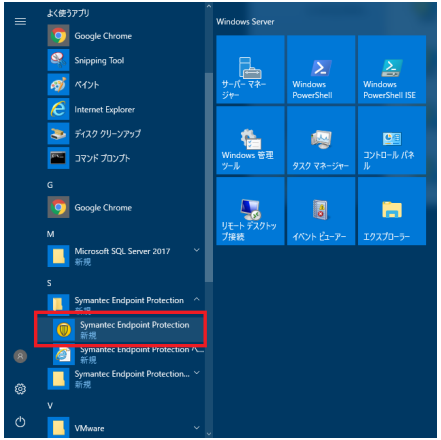
ポリシーの設定が完了すると、クライアント側でエージェントのアップグレードが実行されます。



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



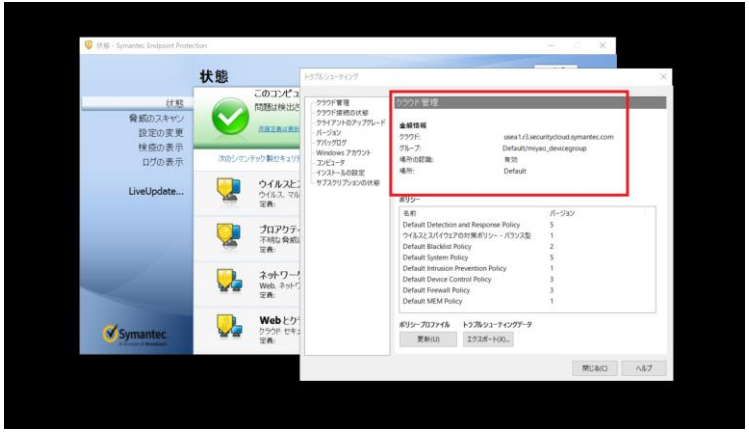
⑳

「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



⑫

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。

⑬

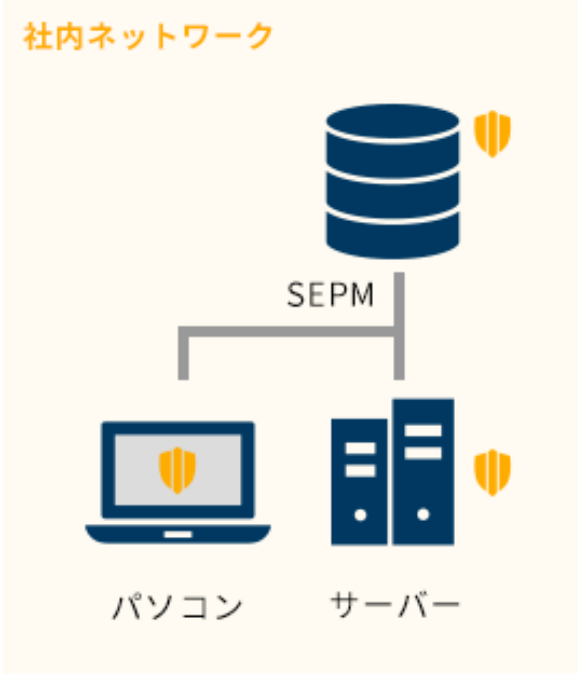
ICDmでも、「デバイス」＞「デバイスグループ」から対象のデバイスグループを選択します。
「管理対象デバイス」でも確認できます。
本作業はコチラで完了です。

３．ハイブリッド構成手順

ハイブリッド構成

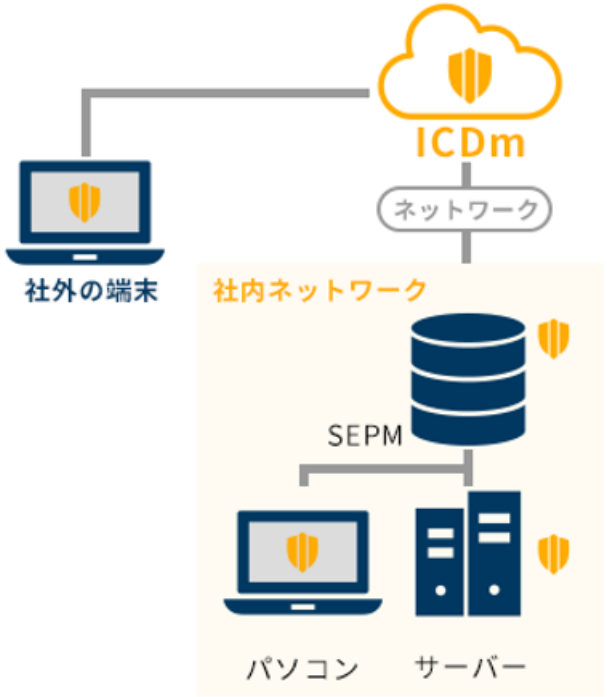
SB C&S

オンプレミスで管理



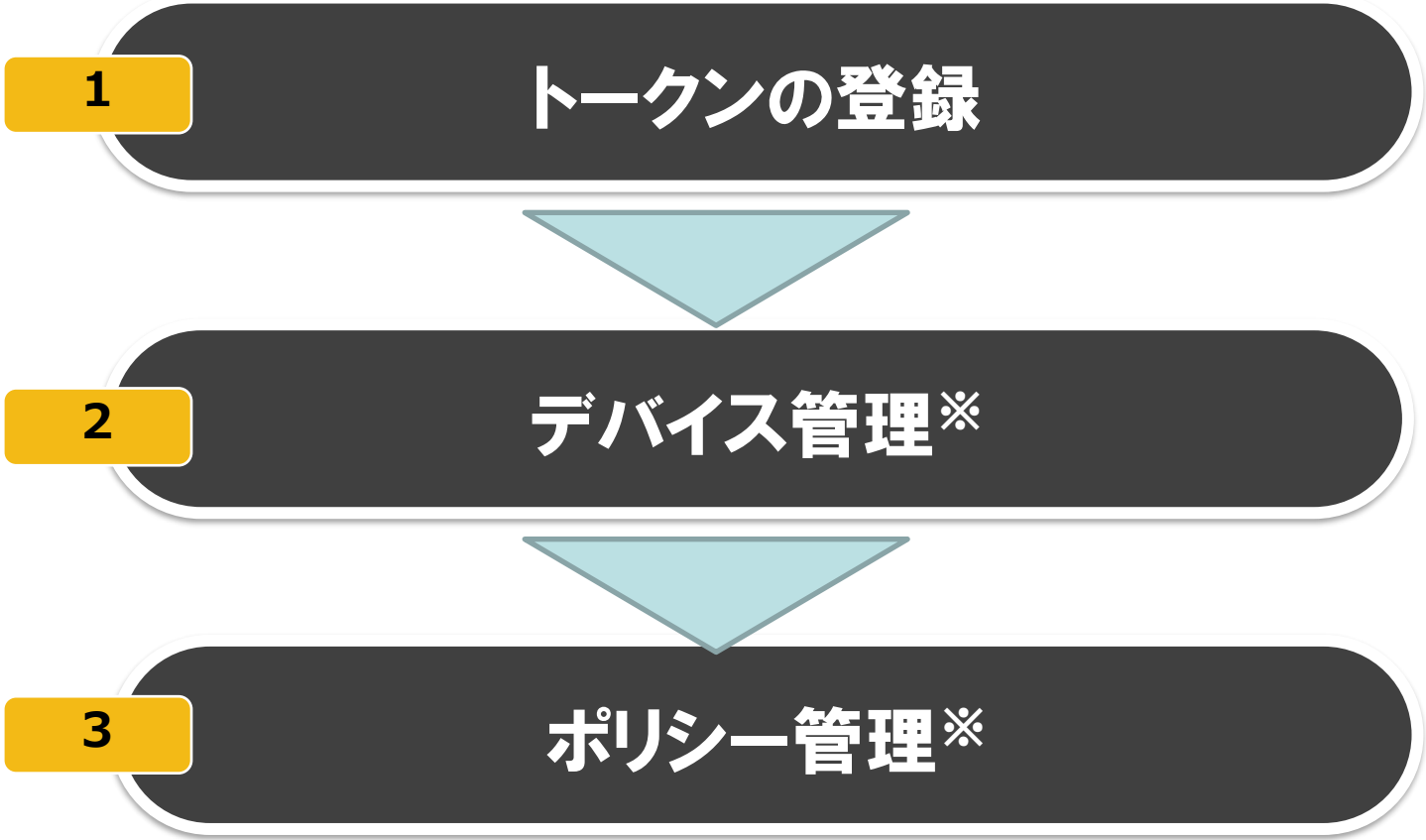
SEPMとICDmで管理

ハイブリッドで管理



ハイブリッド構成

SB C&S



※任意の手順となります

ハイブリッド構成

SB C&S

※任意の手順となります

3.1トークンの登録

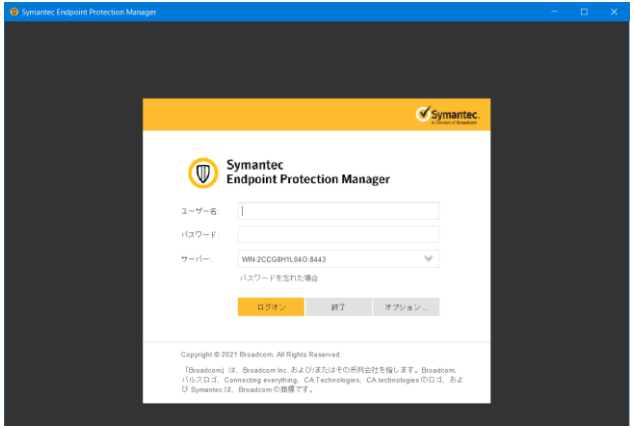
①

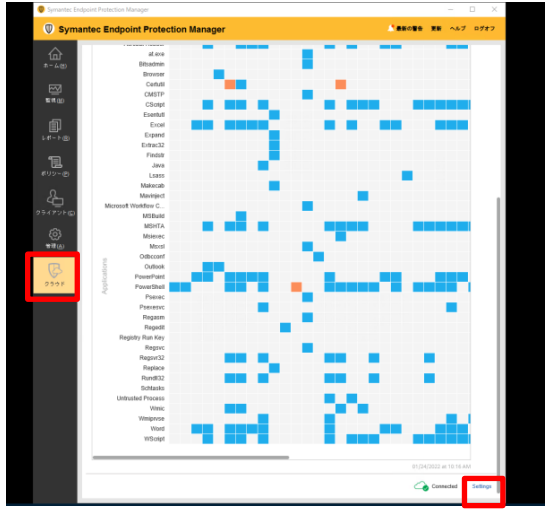
左のタブの「統合」を選択し、「登録」を選択します。

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





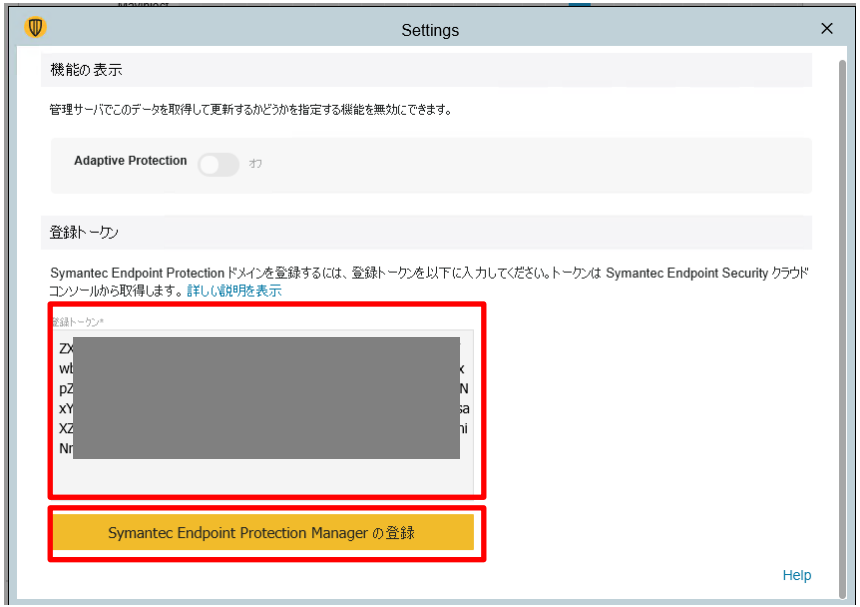
③

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

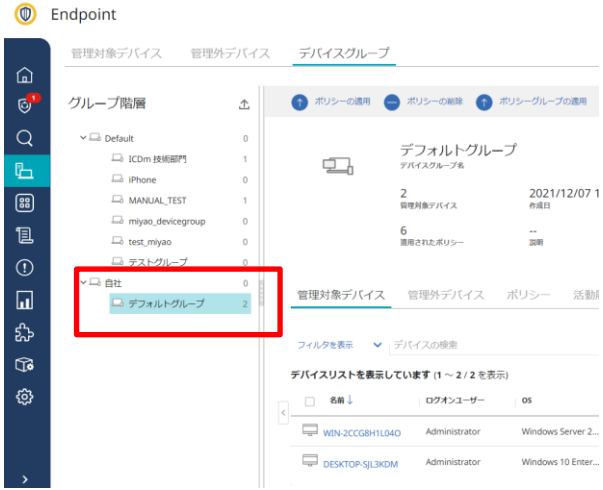
⑥

「状態：登録済み」でクラウドとの接続が完了です。

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。

ハイブリッド構成

※任意の手順となります

3.2デバイス管理

SB C&S

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。

・**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
介いたします。

3.2デバイス管理

クラウドからのデバイスの管理

①

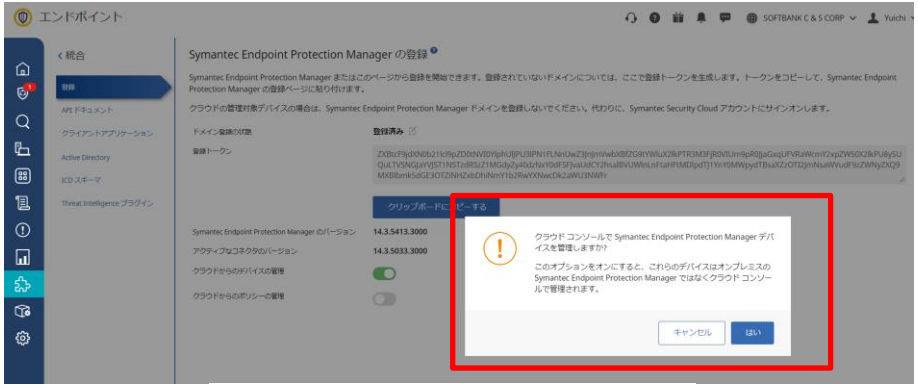
クラウド経由でSEPM配下のデバイス管理が可能となります。
左側のタブの「統合」を選択し、「登録」を選択します。

②

「クラウドからのデバイスの管理」をオンにします。

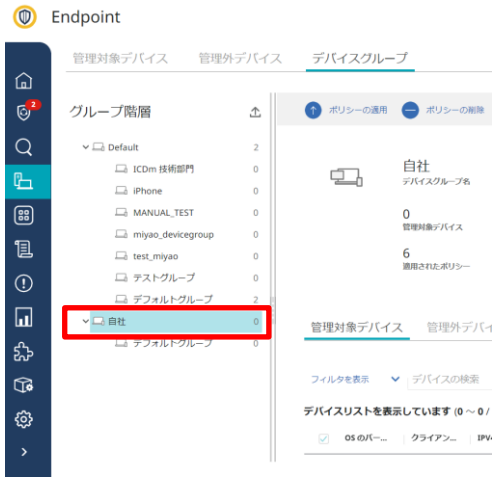
3.2デバイス管理

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。

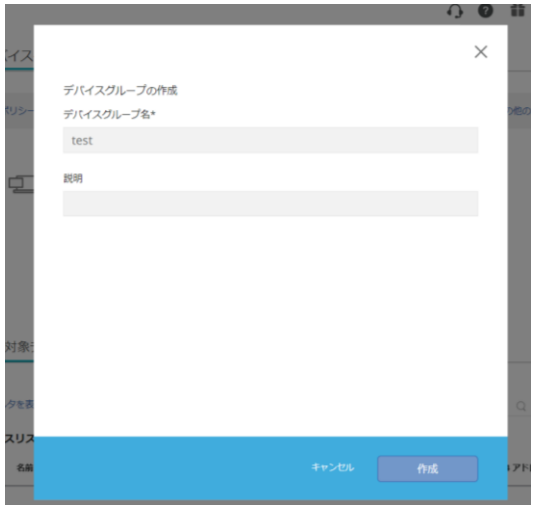


④

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。

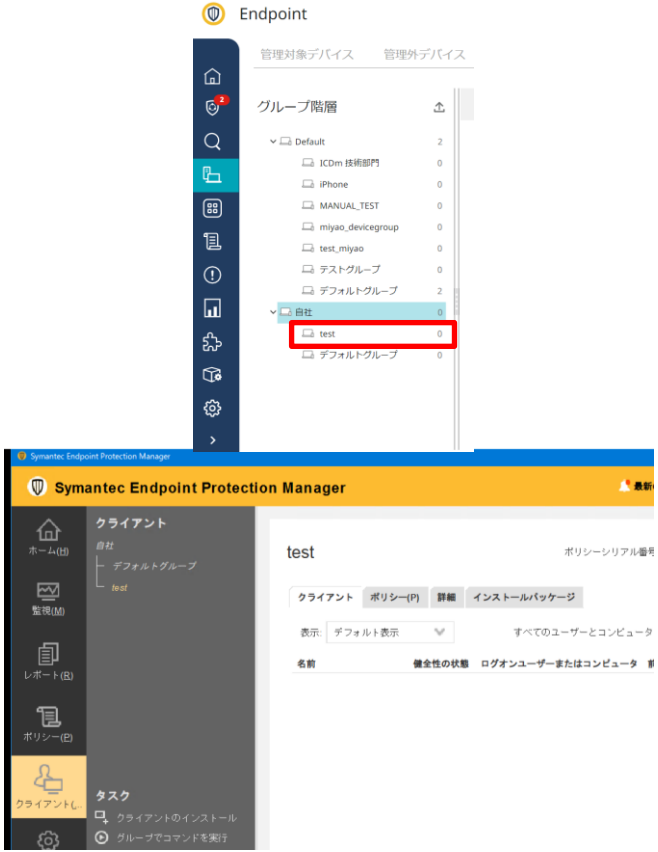
⑥

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

SB C&S

クラウドからのデバイスの管理



⑦

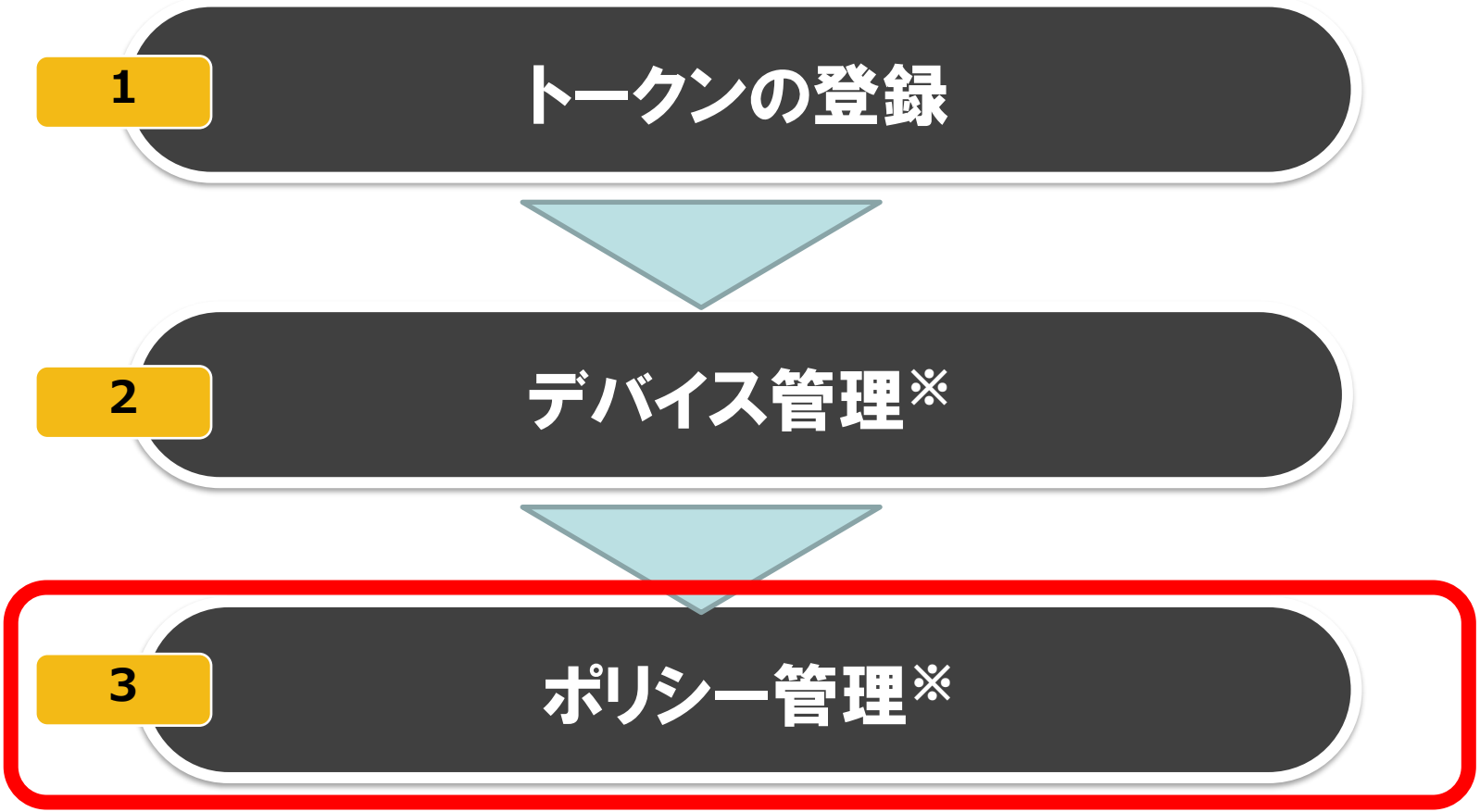
デバイスグループが作成された事が確認でききます。

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。

ハイブリッド構成

SB C&S



※任意の手順となります

3.3ポリシー管理

SB C&S

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

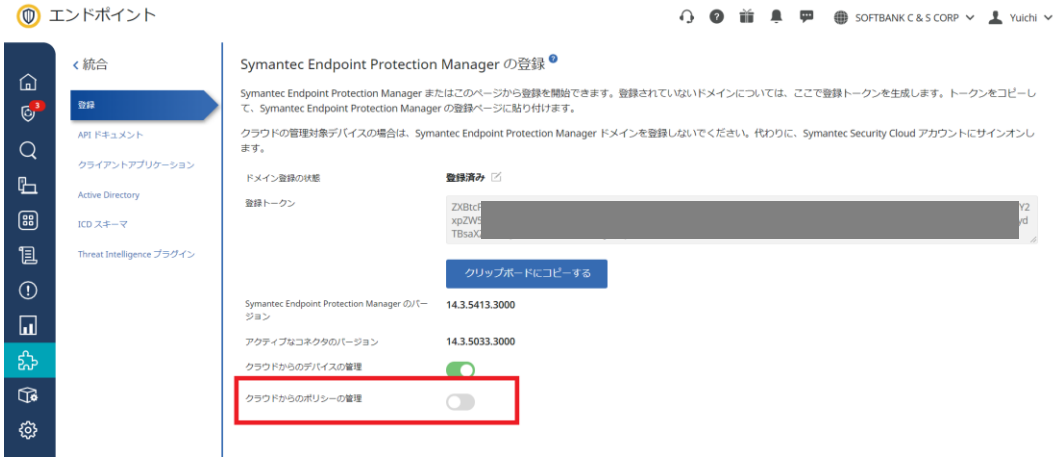
・SEPMとICDm双方のポリシーが適用されます
・最終的にはフルクラウドに移行する際はポリシーを継続して利用が可能です。

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。



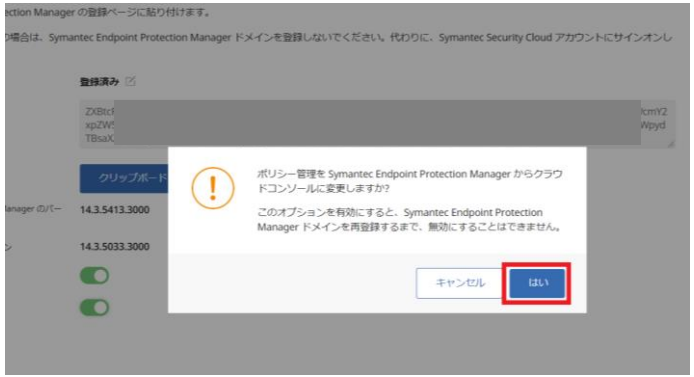
②

「クラウドからのポリシーの管理」をオンにします。

3.3ポリシー管理

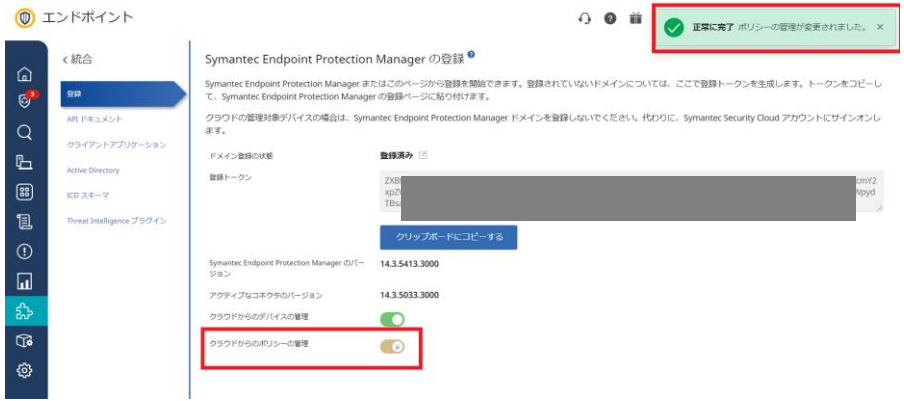
SB C&S

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。

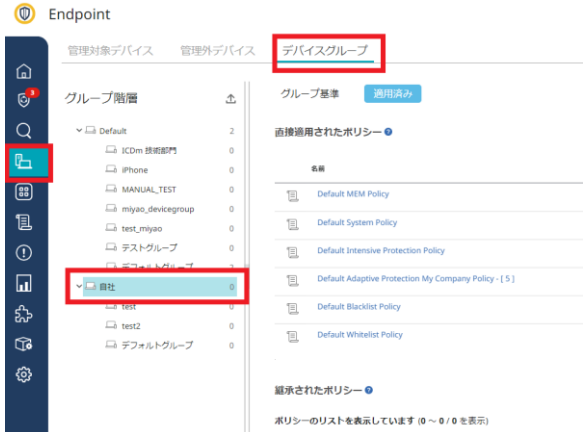


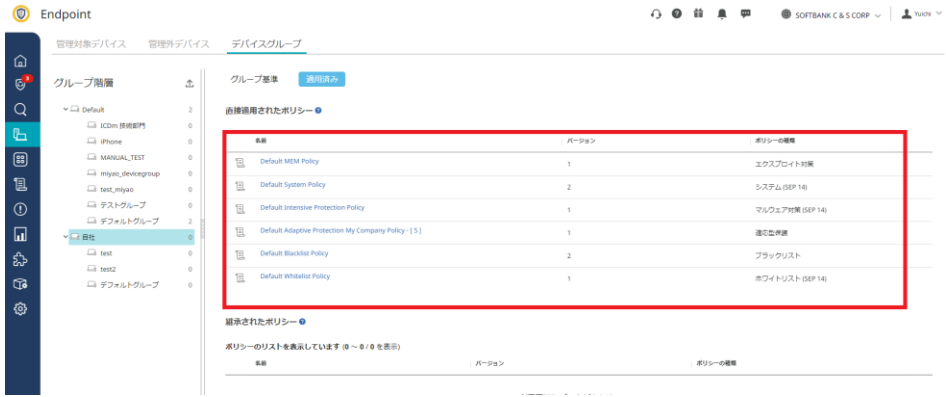
④

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。

3.3ポリシー管理

SB C&S

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おります。

・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おります。

・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おります。

・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

Appendix

SB C&S

■通信先URL

エージェントおよびSEPMとICDMとの連携に必要となるポートとURLが記載されております。

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おります。

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

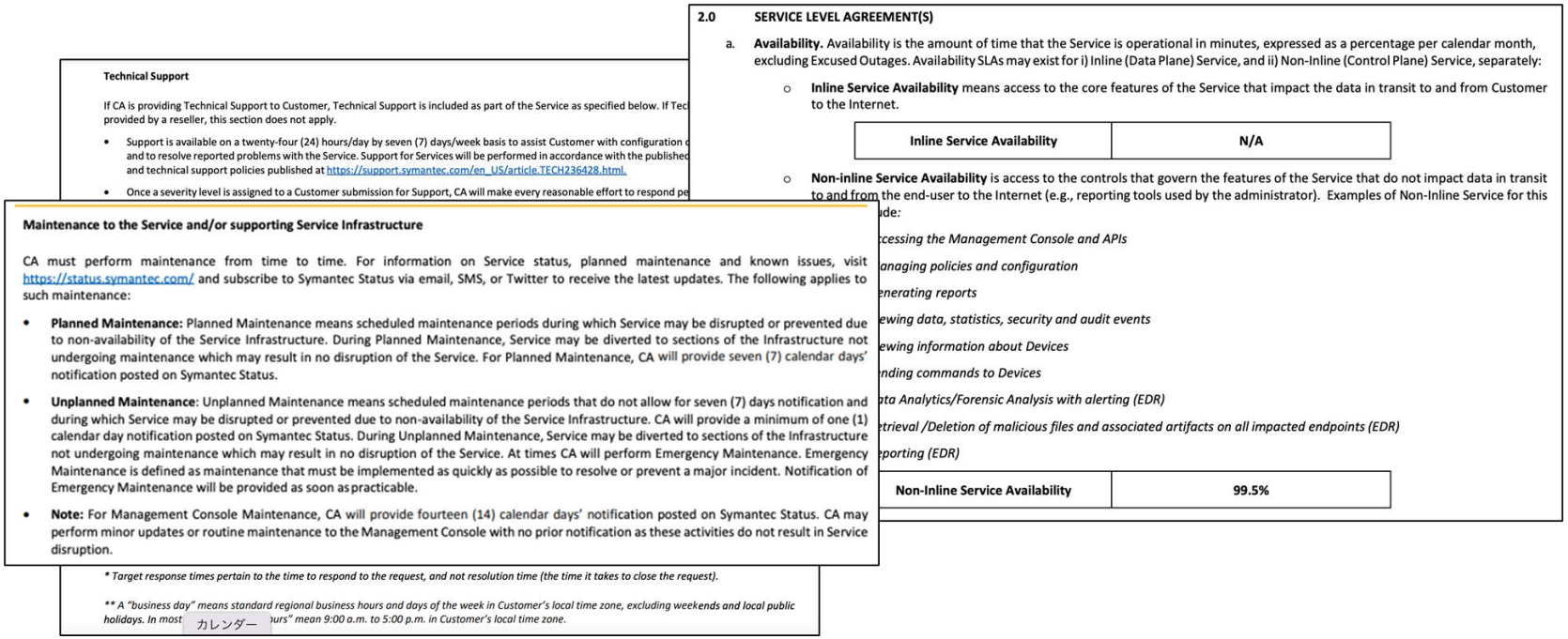
低帯域モードでも利用可能です

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 Tec
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.
- Once a severity level is assigned to a Customer submission for Support, CA will make every reasonable effort to respond pe

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* カレンダー *urs" 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 ude:

ccessing the Management Console and APIs
anaging policies and configuration
enerating reports
ewing data, statistics, security and audit events
ewing information about Devices
nding commands to Devices
ta Analytics/Forensic Analysis with alerting (EDR)
trieval /Deletion of malicious files and associated artifacts on all impacted endpoints (EDR)
porting (EDR)

Non-Inline Service Availability	99.5%


SB C&S