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



- 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)

ALING

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	前段階	侵入					感染			延	情報流出
事前	攻撃		初期アクセス			実行	実行 再攻撃 特権昇格 防衛回避 アレーディング			発見 横断的な 攻撃	収集 外部 六出
						۲				2	
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	テハコス制御 アプリ制御 分離ポリシー	ビキュアな技統	/侵入防止	ション分析	同臣な慨慨子首	スクリプト エミュレーター	ト緩和	振る舞い監代	7107937	セキュリティ	イットリークファイア ウォールと侵入防 止
適用 違反のシミュ レーションとレ ボート、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 の木ワイトリスト、 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	スクリプトペース 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	は& 対処 –	フライトデータ	ーレコーダー(Fli	ght Data Re	corder) 振舞	恥フォレンシ	ジックス 標的]型攻撃クラウド	分析丨Threa	t Hunter 分析	:
ا ت	ーバルインテリ	ジェンスネットワー	-ク - 世界最フ	大の民間脅威イ	ンテリジェンス 娄	枚十億のクエリ/	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

40



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。



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。



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。



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



社内・社外のネットワークは 問わずクラウドで一斉管理







2.1対象クライアント確認







2.2ポリシー移行



		·} ⑦ ₩	T 🌲 🟴 🌐 SOFTBANK C	& S CORP 🗸 💄 Yuichi 🕚
L	VERSION	ポリシーの作成 (型) オ DEVICES	ブリッドのダウンロード 🕕 ポリシ DEVICE GROUP	rーのインボート 6 / 10 列 S POLICY GR
	1	0	0	0
	6	2	1	O
	1	0	0	0

- ・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。



・SEPMで利用していたポリシーはICDmヘ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

■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。

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

■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	
6) ©	グループ階層	* 1 ポリシーの適用 ● ポリシーの削除 1 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	・子グルーフ
\cap	V Default	Default	
4	test		- すると、チ
Ľ.	test_tech		
		親グループ:Default	ポリシーガ
l		二 アグループ・	
!			
u		test,test_tech	
హి		クイック フィルタ v ク	
1		デパイス のリストを表示 (0 ~ 0 / 0 を表示)	
-0-		召前↑ ログオンユーザー OS OS のパージョン クライアントのパージョ IP	
6 3			
		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。





🔵 Symante	c Endpoint Protection Manager				-		×
🔘 Sym	antec Endpoint Protection	Manager		🥂 最新の警告	更新	ヘルプ	ログオフ
₩ *-2@	ポリシー(P) ウイルスとスパイウェアの対策 ファイアウオール 値入防止	ウイルスとスパ~	(ウェアの対策 , 戦明	ポリシー	使用する	場所数	
□ 監視(<u>M</u>)	アプリケーションとデバイス制御	ウイルスとスパイウェアの転篭者	セキュリティとパフォ	- マンスのパランスがよくほと…			2
	ホストインテグリティ LiveUodate	ウイルスとスパイ 編集	セキュリティをより重ね	見するポリシーで他のアプリケ			0
[<u>■</u>] レポート(<u>R</u>)	。 メモリエクスプロイト緩和機能 Webとクラウドのアクセス保護	ウイルスとスパイ ^{制隊} コピー 貼り付け	パフォーマンスが上が	5ポリシーですがセキュリティ			0
見 ポリシー(P)	開外 クライアントのアップグレード ポリシーコンボーネント	割り当て マンホー・ エクスポート					
Æ	927						
	 ✓ ポリシーの編集 ※ ポリシーの刷除 ※ ポリシーの創り当て 						
	 ▲ ポリシーの後回 ■ ポリシーの置換 	 最近の変更は以下のとおりです: 説明 		時間		理者	
259F	 第リシーのコピー ☆ ポリシーのエクスポート ☆ ウイルス対策とスパイウェアを 	システムのインストール時に共行 システムのインストール時に共行	Fボリシーを追加しました Fボリシーを追加しました	2021/11/22 23:28:40 JST 2021/11/22 23:28:40 JST	ad ad	min min	÷



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



🔘 エンドポイント

🕞 🚳 🗰 📮 ም 🛞 SOFTBANK C & S CORP 🗸 🛓 Yuichi '

â		5-57-5		フホーネント ホワシーの対象設定ルール					
6			ポリシーの!	リストを表示 (1 ~ 25 / 78 を表示)		#リシーの?	城 🕑 グリッドのダウンロー	- ド 🕕 ポリシーのインボート	6 / 10 Fl
D	解析	スタム フィルタか		AME	POLICY TYPE	VERSION	DEVICES	DEVICE GROUPS	POLICY GR
-` Ъ			Def	fault Adaptive Protection My Company Policy	建忘型保護	1	0	0	0
	検出語みアイテム		1 Def	fault Adaptive Protection Policy	進応型保護	6	2	1	•
	#US-		1 Def	rfault Adobe Acrobat Policy 🔥	PDF レンダラの隔離	1	0	0	0
1	インシデントと話	カスタム フィ.	1. Def	fault Adobe Acrobat Policy - [1]	PDF レンダラの隔離	1	0	0	0
			1. Def	fault Antimalware Policy	マルウェア対策	4	3	1	3
			1. Def	fault Antimalware Policy - [[1]]	マルウェア対策	2	0	0	0
7			1 Def	fault Antimalware Policy - [2]	マルウェア対策	1	0	0	0
\$	80E		1. Def	fault App Control Policy	App Control	2	0	0	2
			1 Def	efault App Control Policy - [1] 🔥	App Control	1	2	1	0

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。

Import Policy	\times
Import your Symantec Endpoint Protection Manager policies into the Integrated Cyber Defense Manager and apply them to Symantec Endpoint Security device groups. Before you begin:	
Export Symantec Endpoint Protection Manager policies in a .DAT format and save to the local drive. Learn more	
Only the .DAT file format is supported. Other file formats are not currently supported.	
→ You can import a maximum of 50 policies at a time.	
\bigcirc) The maximum supported file size is 1MB per file.	
Learn more about import policy.	

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。



◎ 開<		×
← → × ↑ 🕨 >	PC > デスクトップ	✓ ひ デスクトップの検索
整理 ▼ 新しいフォル	9-	i= • 💷 (
🏕 カイック アクセス	名前	種類 サイズ
🔓 デスクトップ	* 01/11/22	23:41 DAT ファイル 21 KB
🔈 ダウンロード	*	
📔 ドキュメント	*	
🔚 ピクチャ	*	
🧢 PC		
🥩 ネットワーク		
	<	>
77-	イル名(N): ウイルスとスパイウェアの対策ポリシー - パランス型.dat	 DAT ファイル
		開く(O) キャンセル

11:25:39 PM er page 25 🗸
er page 25 🗸

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。





	1 NEWLY CREATED	0 OVERRIDDEN	0 FAILED			×
port Summary						
OLICY NAME	POLICY TYPE	IMPORT STATUS	SERVER	DOMAIN	SITE	
マイルスとスパイウェアの対 球リシー - バランス型 - [1	Malware Protection	Success	WIN-2CCG8H1L04O	デフォルト	マイザイト	
				Page 1 of 1	<<>> Items per page	25 ∨

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。





🕢 🔕 🎬 🜲 🗭 🌐 SOFTBANK C & S CORP 🗸 🛓 Yuld

	ポリシー ポリシー	グループ	ポリシーコンボーネント ポ	リシーの対象	設定ルーノ	L			
ି ଜୁନ	フィルタ基準	11	Imported 例外ポリシー(DL) - [1]	ブラックリ スト	1	0	0	0	
å	以下のクイック フィルタまた はカスタム フィルタからクエ リを選択します。	11	Imported 例外ポリシー(DL) - [2]	ブラックリ スト	1	0	0	0	
Ъ	EH7	1	Imported 別外ポリシー(WL) 🛆	ホワイトリ スト (SEP 14)	1	0	0	0	
8	()] (BAD) (REM.)	11	mlyao_testpolicy	マルウェア 対策	1	0	0	1	
	クイックフィルタ	12	test	マルウェア 対策	1	0	0	0	
ū	> ポリシーの種類	11	test APP	App Control	1	0	0	0	
పి	> 状態のインボート	11	test_policy 🔥	マルウェア 対策	1	0	0	0	
ය ම		1	webトラフィックリダイレクト 🔥	トラフィッ クリダイレ クト	3	0	1	0	
			ウイルスとスパイウェアの対策ポリシー・バランス型	マルウェア 対策	1	0	0	0	
		11	ウイルスとスパイウェアの対策ポリシー・バランス型 ^	マルウェア 対策	1	0	0	0	1
		11	メモリエクスプロイト運作機能ポリシー	エクスプロ イト対策	1	0	0	0	



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。

Endpoint

·}Ø##.₽₽ €



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。





niyao_d	levice	egroup へのポリシーの適用					\times
		Imported 御時代リシー(DL)	1	ブラックリスト	0	0	
		Imported 御好代リシー(DL)-[1]	1	ブラックリスト	0	0	
		Imported 御外ポリシー(DL)-[2]	1	ブラックリスト	0	0	
		Imported 御外ポリシー(WL)	1	ホワイトリスト (SEP 14)	0	0	
		miyao_testpolicy	1	マルウェア対策	0	0	
		tesz	1	マルウェア対策	0	0	
		test APP	1	App Control	0	0	
		test_policy	1	マルウェア対策	0	0	
		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	
		ウイルスとスパイウェアの対策ポリシー - バランス型	1	マルウェア対策	0	0	
- 1		ウイルスとスパイウェアの対象ポリシー - バランス型 - [1]	1	マルウェア対策	0	0	
		メモリエクスプロイト通初機能ポリシー	1	エクスプロイト対策	0	0	
	51 to 7	75 / 79 items			n-9 3 /4 🗙) Items per page 25 V	
						arses 2	~
							_

ポリシ	一の対	「象設定ルールの選択				×
. se↓		s≡↓	パージョン	2011	有地	
		Quarantine	1	A target rule assigned to quarantined agents.	オン	
		Default	1	This is the default policy assignment rule	<i>オ</i> ン	
					#2 (X)	

(11)

インポートしたポリシーを選択し、「次へ」を選択 します。



「Default」を選択し、「次へ」を選択します。



選択の概略		
ポリシー	ポリシーの対象設定ルール	
ウイルスとスパイウェアの対策ポリシ	Default	





(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。

SB C&S

(13)

適用内容を確認し、「送信」を選択します。





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。







- ・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

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。



SB C&S





をのタブの「統合」を選択し、「登録」を選択します。

() エンドポイント



🗘 🗿 🎁 🚊 🗭 🌐 SOFTBANK C & S CORP 🗸 🛓 Yuichi 🔻

30





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。



Ø	Settings	×
	機能の表示	
	管理サーバでこのデータを取得して更新するかどうかを指定する機能を無効にできます。	
	Adaptive Protection 37	
	登録トークノ	
	Symantec Endpoint Protection ドメインを登録するには、登録トークンを以下に入力してください。トークンは Symantec Endpoint Security クラウド コンソールから取得します。詳しい説明を表示 E話トーケン ^a	
	V V R S S S S S S S S S S S S S S S S S	
	Symantec Endpoint Protection Manager の登録	
	Help	

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。



6

「状態:登録済み」でクラウドとの接続が完 了です。

SB C&S

0	Endpoint						🔔 警告デバイスとう	デバイスグループの同期が進行	中です。同期が完了する	までは、操作を実行しないでくださ	±υ.
		管理外デ	デバイス デバ	イスグループ							
6		デバイン	スの検索								
Q	调查	デバイス	リストを表示してい	ます (1 ~ 4 / 4 を表	示)				ユーザーの招待 🚇 イ	シストールパッケージ 9/13列	~
Ъ			名前 ↑	ログオンユーザー	OS	OS のパージョン	デバイスグループ	クライアントのバージョン	IPV4 アドレス	セキュリティ状態	
88	検出済みアイテム		DESKTOP-14K9HI3	Administrator	N						:
1		-	DESKTOP-SJL3KDM	Administrator	N						:
(!)	インシデントと警告	-	WIN-2CCG8H1L04O	Administrator	N						:
	レポートとテンプレート		ykym-windows-ze	ykym1234	v						:
<u>~</u>											

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。

SB C&S

🔘 Endpoint

	管理対象デバイス 管理タ	デバイス	デバイスグループ		
۵					
6	グループ階層	Ť	(す) ポリシーの適用	オリシーの削除 🏠	ポリシーグループの適用
Q	∽ 🖵 Default	0			-
n	口。ICDm 技術部門	1	¢,	テノオルトクルー	.)
<u>u</u>	iPhone	0			2024/42/07 4
88	□ MANUAL_TEST	1		∠ 管理対象デバイス	2021/12/07 1 作成日
1 =	imiyao_devicegroup	0		6	
B	🖵 test_miyao	0		適用されたポリシー	2249
(!)	□ テストグループ	0			
	~□□ 自社	0	管理対象デバイス	管理外デバイス	ポリシー 活動
ш	🏳 デフォルトグループ	2			
హి			フィルタを表示 💙	デバイスの検索	
ពា					
			デバイスリストを表示し	っています (1~2/2を表示	示)
\$			□ 名前↓	ログオンユーザー	OS
			WIN-2CCG8H1L0	40 Administrator	Windows Server 2
>			DESKTOP-SJL3KD	M 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。

0	Endpoint		001	î l
<u>ن</u>	管理対象デバイス 管理外デ	デバイス <u>デバイスグループ</u>		
6	グループ階層	① ポリシーの適用 ● ポリシーの米除 ③ ポリシーグループの適用 ● ポリシーグループの取用 ▼ その他の気度		
	 → Default ↓ ICDm 技術部内 ↓ Phone ↓ MANLAL, TEST ↓ miyao, devices youp ↓ test, miyao ↓ TS, HO/J, - J → Bitt 	6 7 7 7 7 7 7 7 7 7 7 7 7 7		
60 60 C2	□ text □ text □ 7フォルトグループ		BEORN	
				15:44



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。

SB C&S

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。


バイス	デバイ	スを完全クラウ	ド管理に切り替える						×	
ポリシー	2 জগ	昔え可能なデバイス	0 切り替え不可能なデバイス							
L:	ノ下のデノ	(イスではサポート	されているクライアント	バージョンが	実行されてい	るため、クラウド(管理可能です			
Ę		デバイス名				デバイスグループ名				
	<u>n</u>	WIN-2CCG8H1L04O				デフォルトグループ	7			
	Ţ.	DESKTOP-SJL3KDM				デフォルトグルーフ	7			
理対象:										
ィルタを表										
7777										
3 8 10							展る	送信		
DESK										6:45:44
WIN-2CCG8	BH1L04O	Administrator	Windows Server 2	10.0	14.3.5413	192.168.11.46	00:50:56:83	3:4F:E6	2022/1/18	15:11:37

ポリシーの削除 デフオ) デバイスのト 2 電気は多アに c	i	これらのデバイスをクラウド管理に切り替えた後、再度 SEPM に切り替えることはできません。 デバイス グループ「デフォルトグループ」を切り替え ますか?	
で 調用されたポ 管理外デバイス	ポリシー	キャンセル 活動調歴	
デバイスの検索			

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。

<u>(12</u>)

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。

_												
0	Endpoint								✓ 正常に完了 デ	バイス グループ 「デフォルトグ」	レープ」の切り替えが	開始されました。
	管理対象デバイス 管理外ラ	デバイス	デバイスグループ									
۵												
62	グループ階層	£	🕤 #பல-ல்லோ 🧲	ポリシーの副語 🁩 🤊	ポリシーグループの適用	8 😑 ポリシーグループの潮除 (🚽 දගකිගකියි		_			
Q	~ □ Default	6							0 20	デバイス グループはクラウドへのい	り始え中です	^
R	口 ICDm 技術部門	0	.	テノオルト	911-J					TALS S FINIL CONA	0/2 充了	
4	🖾 iPhone	0		2		2022/01/18 14-21-06			273	轮表示		
8	ANUAL_TEST	0		2 管理対象デバイス		作曲日						
10	miyao_devicegroup	0		6								
-	Là test_miyao	0		適用されたポリシー		2010						
(!)	ニュ テストクループ	0										
	v ⊥o ⊟+I □ test	0	管理対象デバイス	管理外デバイス	ポリシー 活	動電歴						
<u>"</u>	- test2	0										
522	📥 ユ テフォルトグループ	2	フィルタを表示 🗸 ラ	バイスの検索								
œ	_		デバイスリストを表示して	います (1 ~ 2 / 2 を表示	Ð							10/11列 ¥
٢			6.M 1	ログオンユーザー	os	05のバー クライアン	IPV4 アドレス	MAC アドレス	前田の更新	セキュリティ状態	VM の開発元	
			DESKTOP-SJL3KDM	Administrator	Windows							
			WIN-2CCG8H1L04C	Administrator	Windows :							

· · · · ·

(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。

							• • • •		₩ ⊕ SQ
	トデバイス	状態が SEPM から ICD	m に切り替わったデ	バイス				×	:
	£	2 11/12	0 切り替え成功	2 切り替え中	 切り替え失敗 				Hu
68775	6	デバイス名	デバイスグルー	76	50.0E	任 可			フド管理に切り替え
	0	WIN-2CCG8H1L040	デフォルトグ	レープ	● 進行中	デバイスは切り替え中です。			
TEST vicegroup	0	DESKTOP-SJL3KDM	デフォルトグ	レープ	● 進行中	デバイスは切り替え中です。			
0	0								
~	0								
	0								
・グループ	2								
		切り替えることができないデバイ	スまたはデバイス グループにつ	かては、 クラウド コンソー/	しが 24 時間ごとに最大 30 日間	司武行します。			
								ස්රිය	セキュリティ状態
									安全
		WIN-2CCG8H1L040	Administrator Wini	dows Server 2 10.0	14.3.5413 192.1	168.11.46 00:50:56:83:4F:E6	2022/1/1	8 15:11:37	リスクあり





٢	Endpoint						0 🛛 🟥 📌 🗰 📾 sa	DFTBANK C & S CORP 🗸 🕹 Yuichi 🗸	
~	管理対象デバイス 管理外	デバイス	デバイスグループ						
ш 6 ⁸	グループ階層	£	ポリシーの適用	ポリシーの削除 🏾 👔 ポリシーグループの適応	日 😑 ポリシーグループの制除 🌚 その他の処理		● デバイス切り替えプロセスが正常に	-ಸೆ70ಕರ್ಗ X	(15)
		0 0 0 0 0 0 2	「二」	デフォルトグループ デバイスルーフ8 0 1 電料をデバイス 6 高利をさしたのシーー 管理外デバイス ポリシー 落	2022/01/18 14:31:06 nati 		マバイス& ウラウト理想に回り起来 レポートのグランロード	2/2 167	「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。
1 	- → = = 1 → test → test2 - → テフォルトグループ	0	フィルタを表示 V ラ デバイスリストを表示して V 8前	「ハイスの桃奈 (います (0 ~ 0 / 0 を表示) ログオンユーザー 05	05 0/(− 9947> IP47FbX	Q MAC 7F6 Z	新聞の更新 セキュリアイ状態	10 / 11 위 오 VM O開和以	
					利用可能なデー	タがありません。			

テハイス	テバイスクループ		
£	2 管理対象デバイス	2022/01/20 17:10:33 ^{作成日}	
2	9		
0	適用されたポリシー	22月1	
0			
0			
0	管理対象デバイス 管理外デバイン	ス ポリシー 活動履歴	
0			
	フィルタを表示 🗸 デバイスの検索	Q	
2	デバイスリストを表示しています (1 ~ 2 / 2	を表示)	10/1
	8前↓ ログオンユーザ	- OS OSのパー クライアン IPV4 アドレス	MAC アドレス
	wilk-20008H11 040 Administrato	(
	DESKTOP-SIL3KDM Administrato	t in the second s	
	2 0 0 0 0 2		

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。







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。







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。

ි ල







0:	エンドボイント				00 ii 4	🔁 🗭 🍵 SOFTBANK C & S CO	RP v 1 Yulon v
≙ €	< 統合 99	Symantec Endpoint Protection Manager の姿 Symantec Endpoint Protection Manager またはこのページがら登 クラウドの電琴は象デバイスの場合は、Symantec Endpoint Prote	録● 単を開始できます。登録されていないドメイン tion Manager ドメインを登録しないでくださ	については、ここで意味トータンを主成します。トータンをコピーして、Syma い、代わりに、Symantec Security Cloud アカウントにサインオンします。	ntec Endpoint Protection	n Manager の整線ページに陥り付けます	r.
Q L	AFL ドキュメント クライアントアプリケーション Active Directory	ドメイン意味の状態 発明トークン	ZXBb: odf59				hyZy4DdzNxV
	ICO スキーマ Threat Intelligence プラグイン	Symantee Endpoint Protection Manager のバージョン アクティブルコネクラのバージョン	クリップボードにつビーする 14.3.5413.3000 14.3.5033.3000				
		クラウドからのポリシーの管理 クラウドからのポリシーの管理		ドメインの登録解除	×		
0				BREALCRE DOTOTOTOTO Synamic languar function language Sanding Real Academic Configuration Sanding Real Ac	ラクドボータルとの 済みファイルが相称 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		
				Produ Po			

管理対象デバイス 管理外デバイス デバイスグループ

9	グループ階層	£	2	里対象デバイス	2022/01/20 17: ^{作成日}	10:33			
2	∽ 🗔 Default	2	9						
	二 ICDm 技術部門	0	181.0	用されたポリシー	252409				
1	iPhone	0							
::)	MANUAL_TEST	0							
_	imiyao_devicegroup	0	管理対象デバイス	管理外デバイス	ポリシー 涼	舌動履歴			
1	🖾 test_miyao	0							
0	ニュ テストグループ	0	フィルタを表示 🗸	デバイスの検索			Q		
_	🗔 デフォルトグループ	2			an				
al I			テハイスリストを表示し	こいます (1~2/2を	衣示)				10/11列 >
3			< 名前↓	ログオンユーザー	OS	os のバー	クライアン	IPV4 アドレス	MAC アドレス
а			WIN-2CCG8H1L04	O Administrator					
Lo				Administrator					
<u>ĝ</u>			a according to a provide the second sec						

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。



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。



Endpoint (1) 管理対象デバイス 管理外デバイス デバイスグループ ඛ 🕋 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 グループ階層 0 ✓ □ Default デフォルトグループ - ICDm 技術部門 デバイスグループ名 Ъ Phone iPhone 2021/12/07 1 - MANUAL TEST 管理対象デバイス 在成日 imiyao_devicegroup 1 test miyao 適用されたポリシー 波明 □ テストグループ () 自社 . 管理対象デバイス 管理外デバイス ポリシー 活動 🗔 デフォルトグループ హి フィルタを表示 🗸 デバイスの検索 (j) デバイスリストを表示しています (1~2/2を表示) ѱ 名前 ログオンユーザー OS WIN-2CCG8H1L04O Windows Server 2 Administrato DESKTOP-SJL3KDM Administrator Windows 10 Enter. 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。

0	Endpoint	🖓 😰 🏥 📮 🐖 🌐 SOFTBANK C & S CORP 🗸 💄 YUKN 🐃
۵ 8	管理対象デバイス 管理外デバ グループ階層	 デバイスクループ 創 ポリシーの編号 ● ポリシーの株形 ● ポリシークループの編号 ● ポリシークループの紙件 ● その他の発展
Q 1 1 1 1 1	 □ Default □ COm IRREPT □ Phone □ MANUAL,TET □ miyao, devicegroup □ etc.miyao □ FXトグループ □ 73 / μ. h7/b - プ 	2 デブイルトクループ デバイス20-フタ 2 1 1 1 1 1 1 1 1 1 1 1 1 1
 4 4	 □ Bt □ デフォルトクループ 	

SB C&S

	Default Adaptive Protection My Company Policy - [33	1	潮信用編集	0	0
	Padault Adaptive Protection Mr. Company Company - (2)		VALUE AND A	0	0
	Default Adaptive Protection My Company Policy - [4]	1	油の高速の構成	0	2
	Default Adaptive Protection Policy	9	適応型保護	0	1
	Default Adobe Acrobat Policy	1	PDF レンダラの隔離	0	0
	Dafault áriaba árrabat Balicu- f 1.1	1	DDELLA/KG小陽線	0	0
	Default Antimalware Policy	4	マルウェア対策	4	7
	Default Antimalware Policy - [1]	2	マルウェア対策	0	0
	Default Antimalware Policy - [2]	1	マルウェア対策	0	0
	Default App Control Policy	2	App Control	0	0
	Default App Control Policy - [1]	1	App Control	0	1

sa ↓	パージョン	3200	កំណ	
Ouarantine Default	1	A target rule assigned to guarantined an This is the default policy assignment rule	16 オン 17 オン	
- Decadin		this is the density pointy assignment run		

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。





5
「送信」を選択します。

SB C&S



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

6

管理対象デバイス 管理外デバイス デバイスグループ



\bigcirc

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



SB C&S



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。

🗘 🞯 🎬 💄 ም 🌐 SOFTBANK C & S CORP 🗸 💄 Yuichi



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。	5







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。





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。







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。



0	Endpoint			0 0 i	
â	ж —Д	管理外デバイス	デバイスグループ		9
6	マイタスク	Ť	🇊 ポリシーの進用 😑 ポリシーの削除 🇊 ポリシーグループの進用 😑 ポリシーグループの削除 🕑 その他の処理		ICDmでも 「デバイス」>「デバイスグル―プ」
Q	词直	0			
Ŀ		2	miyao_devicegroup デバイスグループを		から対象のテハイスクルーノを選択します。
	検出済みアイテム	0	1 2021/06/30 17:49:50 電影論をアバイス の項目		「管理対象テバイス」でも確認できます。
1	ポリシー	up 1 0	9		本作業はこちらで完了です。
(!)	インシデントと書告	0	周川で(たかりンー お田		
ш	レポートとテンプレート		管理対象デバイス 管理外デバイス ポリシー 活動履歴		
హి	統合				
(je	クイックセットアップ		フィルタを表示 🗸 デバイスの検索	Q	
{	設定		デバイスリストを表示しています (1~1/1を表示)		
			□ 名前	MAC アド	
			WIN-2CCG8H1L04O Administrator Windows Server 2 10.0.14393 14.3.5413 192.168.11.46	00:50:56	

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。









ライセンスの有効期間など、製品のサブスクリプ ションの詳細を表示します。

Q

証明書

管理します。

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。



インストールパッケージ

再頒布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	\sim	拡張オプション
ymantec Agent の機能 Wi-Fi 保護と Network Integrity 機能を有効にしますか? したキュア接続 ● デバイスグループ		
miyao_devicegroup		変更
インストールの種類 ^Q ● オンラインィンストールパッケージ ○ 売全インストールパッケージクリエータ		

(1)	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。
```









~ 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。

対象端末から「コマンドプロンプト」を実行します。

SB C&S



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

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

::¥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。





トラブルシューティング			×
クラウド管理 クラウド接続の状態 クライアントのアップグレード バージョン ボルタログ	クラウド 管理 全般情報 クラウト usea1.r3	.securitycloud.symantec.com	
デバラクロク Windows アカウント コンピュータ インストールの設定 サブスクリプションの状態	グループ: Default/i 場所の認識: 有効 場所: Default/ ポリソー	miyao_devicegroup	
	名前	パージョン	^
	Default Detection and Response Policy ウイルスとスパイウェアの対策ポリシー - パランス型 Default Blacklist Policy	5	
	Default System Policy	5	
	Default Intrusion Prevention Policy	1	
	Default Device Control Policy	3	
	Default Firewall Policy	3	
< >>	Detault MEM Policy ポリシープロファイル トラブルシューティングデータ 更新(U) エクスポート(X)	,	•
		閉じる(C)	ヘルブ

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。



0	Endpoint				0 0 i	
		ちゅん ゴバノフ	デバノフグル 一プ			(9)
6		345777777	57/12010-2			č
6	マイタスク	土	🕥 ポリシーの連用 😑 ポリシーの削除	🇊 ポリシーグループの連用 😑 ポリシーグループの削除 💿 その他の処理		ICDmでも 「デバイフー>「デバイフグル―プ」
Q	調査	o				
۲ <u>د</u>		2	miyao_de	evicegroup		から対象のテハイスクルーノを選択します。
88	検出済みアイテム	0	1	2021/06/30 17:49:50		「管理対象デバイス」でも確認できます。
12	ポリシー	up 1 0	9			本作業はこちらで完了です。
(!	インシデントと警告	0	適用されたポリミ	認期		
ш	レポートとテンプレート		管理対象デバイス 管理外デバイ	スーポリシー 活動階層		
హి	統合			IN SUIDUL		
G	クイックセットアップ		フィルタを表示 🗸 デバイスの検索		Q	
63	設定		デバイスリストを表示しています (1 ~ 1 / 1	を表示)		
			A前↑ ログオンユー!	f- OS OSのパー クライアン IPV4アドレス	MAC アド	
			WIN-2CCG8H1L04O Administrat	or Windows Server 2 10.0.14393 14.3.5413 192.168.11.46	00:50:56	

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

🕏 カスタム必要条件		
名前: Migrate SEP Client t	to ICDm	
クライアントの種類: Windows		
クライアントの聴聴 Windows カスクムの要素料スクリプト //mart altamenta behav: File Counting of the Under Run a program 近の)		機能を選択してください・ ユーティリティブログラムを発行 プフリゲージョンを発行するコマントをジラインントだの形分い人を言かく指定します。Sandars 4200時現法前を見えます。 marateSonmarte Cological Protection func. am ² + Q Elect02211(Ouxdamaged C If empSynamte, Aget, package, 04 see コログラム(安美行) コーザーのアブリアーションを発行するスペアのラインアトにのインダンを提びあるかどうかを指定します。 モンフタームコンテキスト ロークリインコージーのコンテキスト内 ープログラム(安美行) するまでの意大的ち相信を指定します。 実行が完了するまでの意大的ち相信を指定します。 実行が完了するまでの意大的ち相信を指定します。 メリカが完了するまでの意大的ち相信を指定します。 ジード 新しいプロセスフィンドクを表示する
i@hn	ሉምጽ	
746/378	Prints	
○ 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	



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。

SB C&S

🔘 エンドポイント



🗛 🚳 🗰 🐥 🏴 🛞 SOFTBANK C & S CORP 🗸 🛓 Yuichi

ユーザーの招待

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。









SB C&S

SB C&S

Ø Symantec E	indpoint Protection Manager			-	o x
🔘 Sym	antec Endpoint Protection Manag	jer		- 最新の警告 更新 ヘルブ	ログオフ
	ポリシー(P) ウイルスとスパイウェアの対象 ファイアウォール	ホストインテグリティオ	ポリシー		
23400 237000 1-2 ⁴⁷ - + (2) 7972- (2)	(4) 所立 オブリク・シングバイス映画 たいしたクラリティ しゃしたのか メモリエアスプロイト通信映画 やみとクラウマドロプリセス原語 世界 クライブイルのプップリレード グリバーマングルタン、 ▶	名前 ホストインアグリティボリレー	観想 製品のインストール中に自動的な作成しました。	使用する場所数	0
یندیندر هیچه ا	タスク ● ホストインテクリティポリシーを金加手を ● ホストインテクリティポリシーを金加手を ○ ホストインテクリティポリシーを全つポート				
<i>0</i> 7 7₽	▲ アフリフーションの使用	最近の変更は以下のとおりです: 説明 システムのインストール時に共有ポリシーを	時間 1歳2月11月1日22328-4938T	登場者 admin	

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。

 ♥ ポリシーのインポート × 						
探す場所:	デスクトップ V 図 コ こ 88 日					
IN32BIT	Migrate SEP Client to ICDm - full installation					
IN64 BIT	🗋 メモリエクスプロイト緩和機能ポリシー.dat					
フォルトグル	プ_WIN32BIT					
フォルトグル	プ_WIN64BIT					
•						
ファイル名:	Migrate SEP Client to ICDm - full installation.dat					
ファイルの種	: エクスポートファイル (*.dat)					
	インボート キャンセル					

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

SB C&S

Symantec Er	dpoint Protection Manager				
🔘 Syma	antec Endpoint Protection Mana	ger		🙏 最新の警告 更新 ヘルブ	ログオフ
 *−4(±)	ポリシー(P) ウイルスとスパイウェアの対策 ファイアウォール	ホストインテグリティボ	リシー		
₩ 1 1 1 1 1 1 1 1 1 1 1 1 1	借入防止 アブリケーションとデバイス新聞 ホストインデグリティ	名前 ホストインテグリティボリシー Migrate SEP Client to ICDm - full installation	説明 製品のインストール中に自動的に作成しました。 Created by Joost Nienhuis (Joost Nienhuis@Broadcom	使用する場所数 .comPrereq	0
₽ ₽#− ► (B)	LiveUpdate メモリエクスプロイト緩和酰能 Web とクラウドのアクセス保護				-
1000 ポリシー(P)	例外 クライアントのアップグレード ポリシーコンボーネント ♥				
25 2⇒472+(タスク <i>•</i> ポリシーの編集				
	 ボリシーの角峰 ボリシーの用り当て ボリシーの期回 				
259F	 ネリシーの最終 ボリシーのコピー ホリシーのエクスポート 	最近の変更は以下のとおりです: 説明	時間	管理者	
	 ホストインテクリティボリシーを追加する ホストインテグリティボリシーをインボート アブリケーションの検索 	共有 ホストインテグリティボリシー を追加 システムのインストール時に共有ポリシーを)	しました: Migrate SEP Client 2021/12/21 2:42:56 JST 創加しました 2021/11/22 23:28:40 JST	admin 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。

SB C&S

Migrate SEP Client to ICDm - full installation X					
ホストインテグリティ ポ	リシー				
祖要 必要条件 拡張設定	必要条件 クライアントホストインテグリテ	(検査を実行するタイミング			
	 常にホストインテグリティ 管理サーバーに接続してい ホストインテグリティ検査 	検査を実行する るときにのみホストインテグリ・ を実行しない	ティ検査を実行する		
	ホストインテグリティの必要条件				
	+/- 名前			有効にする	
	Migrate SEP Client to ICI) m		✓ 有効にする	5
		_			
		追为0	編集	t 上口移	下に移
			ок	キャンセ	ヘルブ

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。

SB C&S

🔘 カスタム必要条件			
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 File: Download Onary Norro pr 一成功	クリプト ow. grow		機能を選択してください: フィイル・フィイルをダウンロード 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。 アイル URL: http://192.168.11.42/Symantec_Agent_setup.exe 対象フォルタ
			 □ 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ダリティを中止できる
3	章为o	南北东	
この必要条件がう	₹敗してもホストインテグリテ	ィ検査の合格を許可する	ок キャンセ ヘルブ

(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」

SB C&S

🔘 カスタム必要条件			×			
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 - //insert stateme - File: Download - Hildly, Kum a pri - 成功	y J J ► Its below: If lie gram		柔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 アブ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。 Swindir% などの環境変数を使えます 1 Files (p66)(Symantec Endpoint ProtectionIsmc exe* - cloudmanaged c.'Temp(Symantec_Agent_package_64 exe プログラムを実行 ユーザーがアブリケーションを実行するうえでクライアントにロヴインする必要があるかどうかを指定します。 シンステムコンテキスト ○ ログノ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の最大待ち時間を指定します また。 ジストロックトの場合、実行は称了します。 ジ 新しいプロセスウィンドウを表示する			
ì	皇力口	削除				
□ この必要条件がら	₹敗してもホストイン∃	- グリティ検査の合格を許可する	ок キャンセ ヘルブ			

<u>1</u>2

「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。

SB C&S



	;追加		,
追加したいポリシーの精	重類を選択して [次へ]	をクリックします	•
ーポリシーの種類			
ホストインテグリティ	*ポリシー		
x + y + y X 7 1 1 1	・統和職能不リシー		
ホストインテグリティ	ポリシーは、クライアン	ントコンビュータ」 	EIC必要なセキュ
ホストインテグリティ リティコンプライアン	ポリシーは、クライア スまたはアブリケーシ	ントコンビュータ」 ョンを指定します。	LIC必要なセキュ

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

」たの「クライアント」を選択し、「ホリンー」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。

SB C&S



(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。
SB C&S

🕲 Sym	antec Endpoint Protectio	n Manager			「長期の冒合	更新 ヘルプ	ログオフ
 ∗-4⊎	クライアント 前社 - デフォルトグループ	自社			ポリシーシリアル番号: B21	IF-12/15/2021 10.25	50 535
	_ test?	クライアント ポリシー(P) 詳細	インストールパッケージ				
an telligi		システムロックダウン	オフ	クライアントログ	外部通信		•
		ネットワークアプリケーション監視	オフ	パスワード	LiveUpdate コンテンツボリシー		
υ#−+(<u>B</u>)		場所面有のポリシーと設定					
_		∧ 場所の設定: デフォルト				18.91	
围		∧ 堪所国有のポリシー:				ポリシーの違加。	
		ウイルスとスパイウェアの対策	ウイルスとスパイウェアの	対策ポリシー・バランス型 [共有]		タスク	, =
0		ファイアウォール	ファイアウォールポリシー	[共有]		920	£
4	47h	侵入防止	侵入防止ボリシー [共有]			920	1
クライアントレー	0 1878/01/01/0	アプリケーションとデバイス制御	アブリケーションとデバイ	ス創御ボリシー [共有]		タスク	<u>.</u>
1	✓ 38/7003£70	ホストインテグリティ	Migrate SEP Client to ICDn	- full installation [共有]		920	
<u>ي</u>		LiveUpdate	LiveUpdate 設定ポリシー	[共有]		タスク	
2012(A)	▶ 通信記定のエクスホート_	クライアントのアップグレード	クライアント アップグレー	ドボリシー [共有]		タスク	<u> </u>
	東 クルーフボリシーのコピー	メモリエクスプロイト緩和機能	Default MEM Policy v1 [sh	ared, cloud]		C	5
B		Web とクラウドのアクセス保護	Web とクラウドのアクセス	保護ボリシー [共有]		タスク	(
2425		例外	例外ポリシー [共有]			\$2,5	•
		最近の変更は以下のとおりです。					
		10:09		10.00	管理者		
		共有 [ホストインテグリティボリシー]・	Migrate SEP Client to ICDm	- full install 2021/12/21 3:40:41 JS	T admin		
		共有 ホストインテグリティボリシー	を編集しました Migrate SEF	NM Table 15EP Clast to CDm-Md Incal 2021/12/13/40.41.051 admn * .8L/L: Migrate SEP Cleart to: 2021/12/13/20.31.051 admn *			

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。



シマンテック社のダウンロードマネージャ - ★ Symantec Agent インストール中..



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。





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。





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

/	Enapoint					
		管理外デバイス	デバイスグループ			
)	ホーム			-		
P		£	↑ ポリシーの適用 🧲	ポリシーの削除 🕜 ポリシーグルーフ	プの遅用 😑 ポリシーグループの削除 💿 その他の処理	
ł	清査	o				
		2 0	무규	miyao_devicegroup デバイスグループ名		
	検出済みアイテム	0		1 管理対象デバイス	2021/06/30 17:49:50 作成日	
ļ		0		9 速用されたポリシー		
	インシデントと書告	0		18/19 C1 (6,759 5	5547	
]	レポートとテンプレート		管理対象デバイス	管理外デバイス ポリシー	活動履歴	
	統合					
3	クイックセットアップ		フィルタを表示 💙 📑	デバイスの検索		Q
}	設定		デバイスリストを表示して	ています (1 ~ 1 / 1 を表示)		
			(名前丁	ログオンユーザー OS	OS のバー… クライアン… IPV4 アドレス	MAC
			WIN-2CCG8H1L040	Administrator Windows	s Server 2 10.0.14393 14.3.5413 192.168.11.46	00:50

23

0 0 1

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





※任意の手順となります

ハイブリッド構成





※任意の手順となります

SB C&S





「なっ」を選切

2

(1)

🗘 🗿 🎁 🚊 🗭 🌐 SOFTBANK C & S CORP 🗸 🛓 Yuichi 🔻

左のタブの「統合」を選択し、「登録」を選択しま す。

6

Ъ

88 111.

Symantec Endpoint Protection Manager の登録 [●]

Symantee Endpoint Protection Manager またはこのページから登録を説めてきます。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主成します。トークンをコピーして、Symantee Endpoint Protection Manager の登録ページに知り付けます。 クラウドの客様が伸子バイスの通信は、Symantee Endpoint Protection Manager ドメインを登録しないでください、代わりに、Symantee 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	至19月前消入2
クライアントアプリケーション	意録トークン	ZiBid7jlaX
Active Directory		OdFSPyaLic
80 2+-7		Annual Arconductor
Threat Intelligence プラグイン		20092#-Pk-4E-30
	Symantec Endpoint Protection Manager (0)/(— S/ $_{\rm B}$ $>$	
	アクティブなコネクタのバージョン	-
	クラウドからのデバイスの種種	
	クラウドからのポリシーの管理	0



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



ger		
	<i>d</i> 1 1 1 1	
	Symantec.	
6	Symantec	
U	Endpoint Protection Manager	
ユーザーキ	š:	
パスワー	6	
7-1	WN-2CCG8H1L040:8443	
	バスワードを忘れた場合	
	ログオン 終了 オブション	
Copyright	© 2021 Broadcom. All Rights Reserved.	
Broader	- om] は、Broadcomine、および/またはその所列会社を指します。Broadcom、	
パルスロ: び Syman	ゴ、Connecting everything、CATechnologies、CAtechnologiesのロゴ、およ tec は、Broadcomの商標です。	



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。

SB C&S

V	Settings	×
	機能の表示	
	管理サーバでこのデータを取得して更新するかどうかを指定する機能を無効にできます。	
	Adaptive Protection 17	
	登録トークノ	
	Symantec Endpoint Protection ドメインを登録するには、登録トークンを以下に入力してください。トークンは Symantec Endpoint Security クラウド コンソールから取得します。詳しい説明を表示	
	221トーウン*	
	ex wt	
	pz N XY ša XZ hi	
	Nr	
	Symanter Endouint Protection Manager の登録	
	Synance Engoint Hotedon Hanaga (<u>) Hak</u>	
	Help	

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。





6

「状態:登録済み」でクラウドとの接続が完 了です。

٢	Endpoint		B書デバイスとデバイスグルーブの同期が進行中です。同期が完了するまでは、操作を実行しないでください
		管理外デバイス デバイスグループ	
6		デバイスの検索	9
Q	调查	デバイスリストを表示しています (1 ~ 4 / 4 を表示)	(b) ユーザーの招待 🥶 インストールパッケージ 9/13月 M
Ë.	デバイス	□ 名前 ↑ □ ログオンユーザー OS OSの/C	(ージョン デバイスグループ クライアントのバージョン IPV4アドレス セキュリティ状態
:::	検出済みアイテム	DESKTOP-14K9HI3 Administrator V	
1		DESKTOP-SJL3KDM Administrator V	
()	インシデントと警告	WIN-2CCG8H1L04O Administrator W	
ū	レポートとテンプレート	ykym-windows-ze ykym1234 W	
£5	統合		

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。

Endpoint

	管理対象デバイス 管理外	トデバイス	デバイスグループ		
۵					
6	グループ階層	Ť	(1) 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
Q	∽ 🖵 Default	0			
P	🖵 ICDm 技術部門	1		テノオルトクルー デバイスグループ名	-)
ЧЦ	iPhone	0		2	2021/12/07 1
88	□ MANUAL_TEST	1		∠ 管理対象デバイス	2021/12/07 1 作成日
¶⊒)	miyao_devicegroup	0		6	
	Là test_miyao	0		適用されたポリシー	說明
(!)	シーテストグループ	0			
u	◆ □= 日仁	2	管理対象デバイス	管理外デバイス	ポリシー 活動!
హి			フィルタを表示 🗸	デバイスの検索	
(j)					_
~			デバイスリストを表示し	ています (1 ~ 2 / 2 を表:	示)
63			< 名前↓	ログオンユーザー	os
			WIN-2CCG8H1L0	40 Administrator	Windows Server 2
>				M 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。

SB C&S

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



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。







クラウドからのデバイスの管理

🔘 エンドポイント



プラグイン

 $(\mathbf{1})$

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。

(1) エンドポイント



🗘 🙆 🎁 💄 🗭 🌐 SOFTBANK C & S CORP

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 クラウドの管理対象デバイスの場合は、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。 ● 日本 ● 14.3.5413.3000 14.3.5033.3000

$(\mathbf{2})$

[クラウドからのデバイスの管理]をオンに します。



クラウドからのデバイスの管理

0	エンドポイント			Q	0 II #	SOFTBANK C & S CORP V	L Yuichi
ⓐ <mark>॑</mark> Q ∐ 8 1	く 統合 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	Symantee Endpoint Protection Mar Symantee Endpoint Protection Marager 進行などの Protection Marager の語語ケーンに見かけでます。 クランドック部分(第一次の場合は、Symance C ドメイン部分が開 編計ーークン	hager の登録 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	GUVEX4>COVEL CCE GUEXEX, HEDOC, Syn PREENUUSEEJIJIIVUUSEEDE PRIMEISIJIIUUCZEUSEE	· 雪緑トークンを生成 unitec Security Clou rvWluX28keTR3M28/ nunFtaHPCM20pdTj	います。トークンをコピーして、Symane はアカウントでサインオンします。 PRATURE PRATURE TRANSFORMATION THIN PRATURE TRANSFORMATION	c Endpoint xalicPU8ySU z2VMyZXQ9
0 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7 7		Symante Endpoint Protection Manager のパーション アウティブロンスネクタウル(ーンコン ウランドットションボントーの単体 クランドやらいボントーの単体	HI35413300 (1) (1) (1) (1) (1) (1) (1) (1)	クラウドコンゾールで symant イスを管理しますか? ごのオプションをオンにすると、 Symante Endpoint Protection ルで管理されます。	et Endpoint Protect これらのデバイス Manager ではなく・ キャンセル	ion Manager デバ はオンプレモスの) クラウドニンソー / はい	l

Endpoint

	管理対象デバイス 管理外	トデバイス	デバイスグループ
٦			
© ²	グループ階層	£	🕥 ポリシーの適用 😑 ポリシーの削除
Q	∽ 🗔 Default	2	
P	□ ICDm 技術部門	0	
411	🗔 iPhone	0	
**	□ MANUAL_TEST	0	0
¶≣	miyao_devicegroup	0	
a	🗔 test_miyao	0	b 適用されたポリシー
(!)	ローテストグループ	0	
u	Lia テフォルトグループ ~ Lia 自社	2	管理対象デバイス 管理外デバィ
ፚ	ニュ デフォルトグループ	0	
(ji			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 (0 ~ 0 /
			✓ OSのバー… クライアン… IPV-

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。

SB C&S

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。







lpoint						-} Ø # ⊥	
管理対象デバイス 管理外	デバイス	デバイスグループ	_				
ブループ階層	⊥	● ボリシーの適用	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	副験 🔪 その他の処理	
→ 🗔 Default	1					デバイスの追加	_
🖵 ICDm 技術部門	1	<u> </u>	自社			子グループの作成	
- iPhone	0		テハイスクループも			デバイスグループの漫	除
□ MANUAL_TEST	1		0 管理対象デバイス	2021/12/10	13:21:31		
iniyao_devicegroup	0		6				
□o test_miyao	0		6 適用されたポリシー	23.00			
🖵 テストグループ	0						
~ □ 自社	0						
🖵 test	0	管理対象デバイス	管理外デバイン	ス ポリシー 活動	躍歴		

		و ه	0	
ィス			\times	
	デバイスグループの作成			
ペリシー	デバイスグループ名*			oneo
	test			
▱	說明			
5.+ 90 =				
A J PAR .				
夕を表				0
292				
2.81				

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。





クラウドからのデバイスの管理

Endpoint



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





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。





クラウドからのポリシーの管理

Active Directory

デバイス グループを問題するには Symanter

Directory を設定します。



ジョン

アクティブなコネクタのパージョン

クラウドからのデパイスの管理

クラウドからのポリシーの管理

Symantec Endpoint Protection Manager の登録 ⁰

Symantec Endpoint Protection Manager のパー 14.3.5413.3000

ZXRt

xpZW

14.3.5033.3000

🕣 🗿 🎬 🐥 💬 🌐 SOFTBANK C.B. S. CORP 🗸 主 Yulchi 🗸

 \odot

ICD スキーマ

grated Cyber Defense スキーマはイ トの種類を力学ゴリ形に整理します。



$(\mathbf{1})$

左のタブから「統合」を選択し、 「登録」を 選択いたします。

🔘 エンドポイント

Intelligence プラグインをインストールしま

< 統合 ۵ 数编 0 API ドキュメント Q Ъ Active Directory 88 ICD スキーマ 1 Threat Intelligence プラグイン ū Û <u>ون</u>

🗛 🙆 🎬 📮 🗭 🌐 SOFTBANK C & S CORP 🗸 💄 Yuichi 🗸

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、Symantec Endpoint 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は、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



[クラウドからのポリシーの管理]をオンに します。

SB C&S



クラウドからのポリシーの管理

	登録演み 🗹		
	ZXBtcf xpZW TBsaX		kcmY2 Wpyd
lanager (D/('	<u>クリップボード</u> 14.3.5413.3000 14.3.5033.3000	ポリシー管理を Symartec Endpoint Protection Manager からクラウ ドコンソールに変更しますか? ごのオプションを有効にすると、Symantec Endpoint Protection Manager ドメインを有登録するまで、懸効にすることはできません。	
	•	キャンセル はい	

🔘 エンドポイント

	く統合	Symantec Endpoint Protection	n Manager の登録 🎱
ы 6 ⁹	211	Symantec Endpoint Protection Manager ま て、Symantec Endpoint Protection Manage	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 erの登録ページに貼り付けます。
q	API ドキュメント	クラウドの管理対象デバイスの場合は、Sym ます。	antec 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
п	クライアントアプリケーション	ドメイン登録の状態	豊得済み 区
	Active Directory	登録トークン	728
	ICD スキーマ		xpZ TBs
11	Threat Intelligence プラヴイン		ALL THE DETUINE
1			2332M PICAL 48
		Symantec Endpoint Protection Manager のパー ジョン	14.3.5413.3000
ш		アクティブなコネクタのパージョン	14.3.5033.3000
హి		クラウドからのデバイスの管理	
€D		クラウドからのポリシーの管理	
63			

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。

SB C&S



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。





クラウドからのポリシーの管理

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	£	グループ基準 通用済み
∽ 🗁 Default	2	直接適用されたポリシー ●
🕞 ICDm 技術部門	0	
🕞 iPhone	0	為前
ANUAL_TEST	0	Default MEM Policy
imiyao_devicegroup	0	TEI Default System Policy
Lo test_miyao	0	
ニュ テストグループ	0	Default Intensive Protection Policy
~ □ 自社	0	Default Adaptive Protection My Company Policy - [5]
⊥a test	0	Default Blacklist Policy
La test2	0	Tel Default Whitelist Policy
🖵 デフォルトグループ	0	
		縋承されたポリシー ♥
		ポリシーのリストを表示しています (0 ~ 0 / 0 を表示)

Endpoint

管理対象デバイス 管理外デバイス デバイスグループ グループ基準 適用済み グループ階層 直接適用されたポリシー 9 COm Hitister ポリシーの補精 - iPhone 名前 A MANUAL_TEST 18 Default MEM Policy エクスプロイト対策 miyan devicenceu 1 Default System Policy システム (SEP 14) test_miyao 山 テストグループ Default Intensive Protection Policy マルウェア対策 (SEP 14 □ デフォルトグループ Default Adaptive Protection My Company Policy - [5] 建忘型保護 i test 1 Default Blacklist Policy 2 - test2 1 Default Whitelist Policy ホワイトリスト (SEP 14) □ デフォルトグループ 継承されたポリシー 😡 ポリシーのリストを表示しています(0~0/0を表示) 2.0 バーウォン ポリシーの凝血

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

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

■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-andmanagement/endpoint-security/sescloud/Troubleshooting/urls-to-whitelist-for-v129099891d4155e9710.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

			SERVICE LE	EVEL AGREEMENT(S)			
	Technical Support	a.	Availability excluding Excluding Excluding Excluding	v. Availabili xcused Ou nline Servi	ity is the amount of time that the Service tages. Availability SLAs may exist for i) Inlir ce Availability means access to the core t	e that the Service is operational in minutes, expressed as a percentage per calendar month, nay exist for i) Inline (Data Plane) Service, and ii) Non-Inline (Control Plane) Service, separately: ccess to the core features of the Service that impact the data in transit to and from Customer	
	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.		to	o the Inter	net.		
	 Support is available on a twenty-four (24) hours/day by seven (7) days/week basis to assist Customer with configuration of and to resolve reported problems with the Service. Support for Services will be performed in accordance with the published at https://support.ymaintee.com/an_US/rticleTECH236428.html. Once a severity level is assigned to a Customer submission for Support, CA will make every reasonable effort to respond performed in accord. 		o N	lon-inline	Inline Service Availability Service Availability is access to the contri-	N/A ols that govern the features of the Service that d ing tools used by the administrator). Examples o	o not impact data in transit f Non-Inline Service for this
Mair	tenance to the Service and/or supporting Service Infrastructure				ıde:		
	maintenance to the service and/or supporting service intrastructure				cessing the Management Console and APIs		
CA	CA must perform maintenance from time to time. For information on Service status, planned maintena			es, visit	anaging policies and configuration		
such	such maintenance:			enerating reports			
•	Planned Maintenance: Planned Maintenance means scheduled maintenance periods during which Service may to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sec undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, CA will pr notification posted on Symantec Status.	nted due ture not dar days'	ewing data, statistics, security and audit events ewing information about Devices nding commands to Devices				
•	Unplanned Maintenance: Unplanned Maintenance means scheduled maintenance periods that do not allow for	seven (7) days notification and I provide a minimum of one (1) to sections of the Infrastructure tency Maintenance. Emergency			ta Analytics/Forensic Analysis with alerting (EDR)		
	during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. CA wil calendar day notification posted on Symantec Status. During Unplanned Maintenance. Service may be diverted t				trieval /Deletion of malicious files and associated artifacts on all impacted endpoints (EDR)		
	not undergoing maintenance which may result in no disruption of the Service. At times CA will perform Emerg				porting (EDR)		
	Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a Emergency Maintenance will be provided as soon as practicable.			cation of	Non-Inline Service Availability	99.5%	
•	Note: For Management Console Maintenance, CA will provide fourteen (14) calendar days' notification postee perform minor updates or routine maintenance to the Management Console with no prior notification as these a disruption.	antec Status. o not result ir	. CA may n Service				
	* Target response times pertain to the time to respond to the request, and not resolution time (the time it takes to close the req	quest).					
	** A "business day" means standard regional business hours and days of the week in Customer's local time zone, excluding week holidays. In most カレンダー ``Purs'' mean 9:00 a.m. to 5:00 p.m. in Customer's local time zone.	ekends and lo	ocal public				

SBC&S