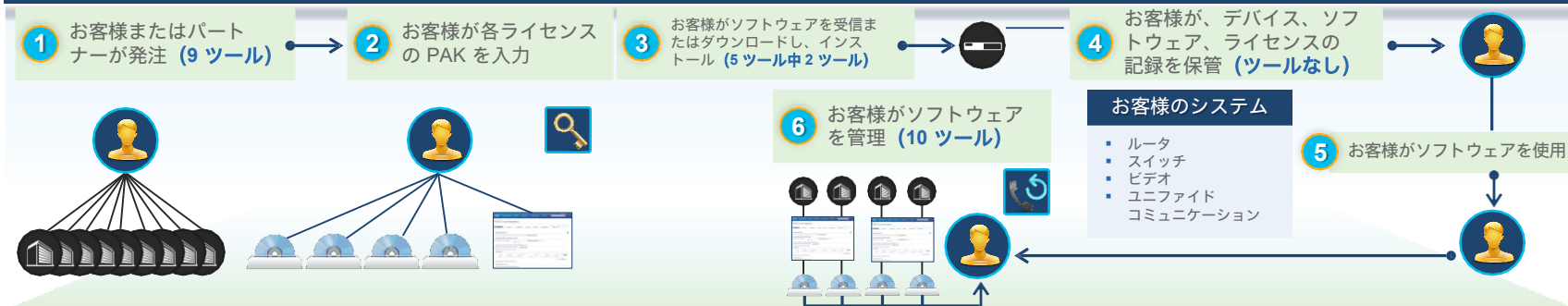


# Cisco Smart Software Manager オンプレミス ライセンス サーバ

# ソフトウェアのライセンス管理の再考

## 過去の運用



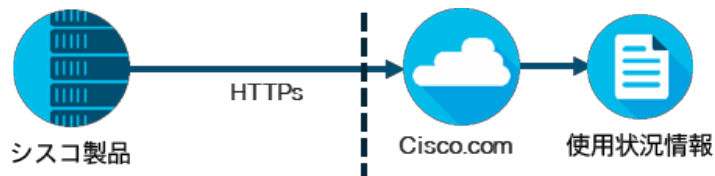
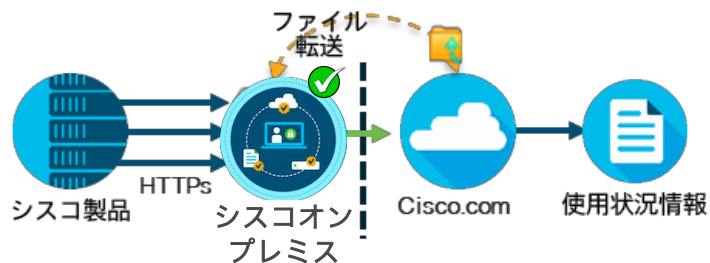
## 現在の運用



# スマートライセンス対応製品の導入

## シスコにアクセス

シスコ製品からインターネット、または HTTP プロキシサーバを介して使用状況情報が直接送信されます。追加のコンポーネントは不要です。

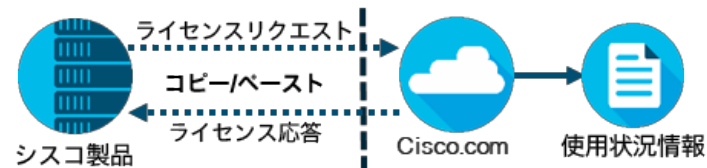


## オンプレミスのライセンス管理を通じてアクセス

シスコ製品は、ローカルにインストールされている **Smart Software Manager** に使用状況情報を送信します。接続されている環境では自動的に、接続されていない環境では手動で、定期的に情報を交換します。

## アクセス不要 - ライセンス予約

製品と Cisco.com 間で相互に情報をコピー/ペーストし、手動でライセンスのチェックイン/チェックアウトを行います。機能的には旧来のノードロックと同等ですが、スマートライセンスのトラッキング機能が利用できます。



使いやすい

# Smart Software Manager (SSM) オンプレミスとは何ですか。



## Smart Software Manager オンプレミスとは...

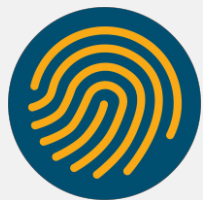
- Cisco Smart Licensing のコンポーネントの 1 つです。クラウドベースの Cisco Smart Software Manager (Cisco SSM) と連携して動作します。

## Smart Software Manager オンプレミスが想定するお客様

- セキュリティ要件が厳格で、インターネットに直接接続してシスコクラウドの Smart Software Manager ライセンスデータベースと通信することを回避したいお客様です。

# Cisco SSM オンプレミスの利点

信頼できる  
セキュリティ



セキュリティを備えた、ライセンス使用に関する単一のオンプレミス情報源

リアルタイムの  
エンタイトルメント



バックエンド インストール ベースとの定期的同期に基づいた、ほぼリアルタイムのライセンスのエンタイトルメント

使用状況  
の可視化



ソフトウェア、サービス、デバイスを使いやすいポータルで包括的に把握

管理性の  
向上



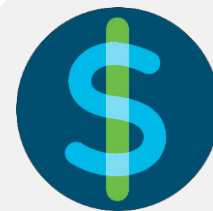
組織全体の範囲でライセンスをデバイス間で共用できる柔軟なライセンスプール方式

ロック  
解除



デバイスへのノードロックライセンスを排し、RMAプロセスをシンプル化

コストの  
削減



ライセンスを効率よく共用することにより、時間とコストを削減可能

# SSM オンプレミス - 導入モデルの概要



Smart Software  
Manager  
オンプレミス



サービスプロバイダー



シスコパートナー



大企業

複数のローカル  
アカウントを  
サポート



100,000 以上の製品と  
500 のローカルアカウント  
まで拡張可能



オンラインまたは  
オフラインで接続可能



Cisco SSM と同様の  
ユーザインターフェイス



組み込みのセキュリ  
ティ機能でレジリエ  
ンスと信頼性を向上



Smart Software Manager オンプレミスソリューションの詳細は、ユーザガイドでご確認ください。

<https://www.cisco.com/jp/go/smartlicensing>

# Cisco SSM オンプレミスをインストールする 5 つの手順



Cisco SSM オンプレミスライセンスサーバを物理環境または仮想環境に展開する手順をサポート。



ISO のインストール

IP アドレスの入力

ログイン情報の変更

インストールの完了

アカウントの登録

200 GB のハードディスク  
8GB のメモリ  
製品\*：  
4 vCPU / 50,000 台  
6 vCPU / 100,000 台

IP とサブネット/  
プレフィックス、  
および DNS を  
入力

シェル/GUI PWD、  
言語、ホストの  
共通名

インストールを完了  
し、オンプレミス  
サーバを起動

NTP を入力し、  
ローカルアカウント  
をシスコに登録



\*ローカルアカウントあたりの 最大 25,000 台です。

# データセキュリティ：Smart License Manager オンプレミス

## ライセンスポータルと管理ポータル

### ライセンスポータル



software.cisco.com と同様の機能



ローカルアカウント、ユーザ、製品インスタンス、デバイス、ライセンスを管理可能



ユーザによる新規ローカルアカウントの作成、ローカルアカウントへのアクセス要求、ローカルアカウントとローカルバーチャルアカウントの管理が可能



### 管理ポータル



ユーザ制御、アカウント管理、登録、同期などの内部管理機能



外部認証、syslog、プロキシのサポートなどを含む、その他の機能をサポート



承認されたユーザのみ使用可能



# データセキュリティ：Smart License Manager オンプレミス

## ライセンスポータルと管理ポータルのロール



### 管理ポータルのロール

#### システム管理者

システムオペレータのすべての権限に加えて、ローカルアカウントの承認/削除およびすべてのシステム設定を実施可能。



#### システムオペレータ

管理者としてすべてのローカルアカウントへのフルアクセス権限を持ち、ローカルアカウントの登録/同期が可能。システム設定の変更は不可。



#### システムユーザ

管理ポータルの権限はない。ライセンスポータルのロールに基づくローカルアカウントへのアクセス。



### ライセンスポータルのロール

CSSM のスマートアカウントおよびバーチャルアカウントのロールと同様。ただし、SSM オンプレミス内のローカルレベルに限定。

ローカルアカウント管理者

ローカルアカウントユーザ

ローカルバーチャルアカウント管理者

ローカルバーチャルアカウントユーザ

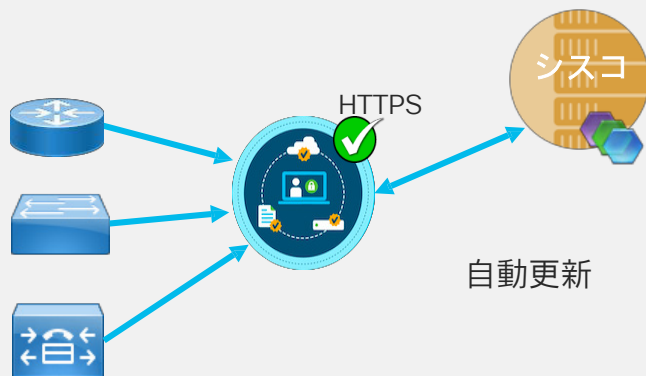
# データセキュリティ：Smart License Manager オンプレミス

## 導入モード - 接続モードと非接続モード



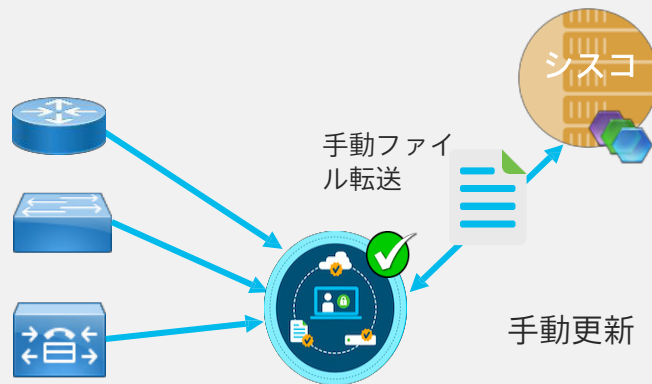
### 接続モード

- このモードは SSM オンプレミスから cisco.com への **直接接続**がある場合に使用
- ライセンスの使用状況とエンタイトルメントを、オンデマンドまたはスケジューリングにより自動で Cisco SSM と同期可能
- 導入が最も容易な標準モデル



### 非接続モード

- このモードは SSM オンプレミスから cisco.com への **接続がない**場合に使用
- SSM オンプレミスは、ファイルのアップロードとダウンロードを介して Cisco SSM との同期が可能



# SSM オンプレミスの主な機能



## マルチテナント：単一の管理ポータルで複数のローカルアカウントを管理

- 複数のローカルアカウントをサポート
- 複数レベルの RBAC（管理者、オペレータ、ユーザ）



## データプライバシー

- 製品情報（ホスト名、IP など）のシスコへの送信を制限
- SSM オンプレミスとシスコ間で監査可能なデータを交換
- ローカルユーザ認証制御：LDAP、Active Directory
- ユーザが Cisco CCOID または Cisco スマートアカウントにアクセスする必要性を、ローカルユーザアカウントによって制限



## ネットワークサポート

- IPv4 および IPv6 のサポート
- 複数の NIC：複数のインターフェイスにより、ネットワーク管理用のトラフィックと製品インスタンスの登録用のトラフィックを分離可能
- プロキシのサポート：SSM オンプレミスとシスコの間にプロキシを構成することが可能
- ファイアウォールゾーン：内部（アクセスあり）または外部（アクセスなし）のインターフェイスを構成する機能



## システムアラートと通知

- E メールと syslog サポート：アカウントイベントが syslog サーバに送信されるように設定可能

# SSM オンプレミスの主な機能



## ライセンスに関する新機能

- ライセンス AppHA：スタンバイアプリケーションおよびアクティブアプリケーションで、単一のライセンスの使用状況をレポート
- ライセンス階層：下位階層のライセンスが利用できない場合に上位階層のライセンスの借用が可能



## API サポート

- リソースとオーナーのログイン情報付与をサポート
- 5 つの主要な API グループで、15 を超える固有の API に対応



## より長い同期間隔

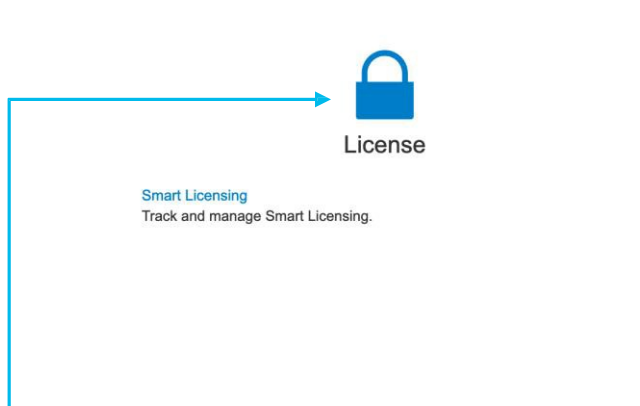
- 365 日の同期スケジュールをネイティブにサポート
- 年に 1 度のシスコとの同期で、SSM オンプレミスが正常に機能



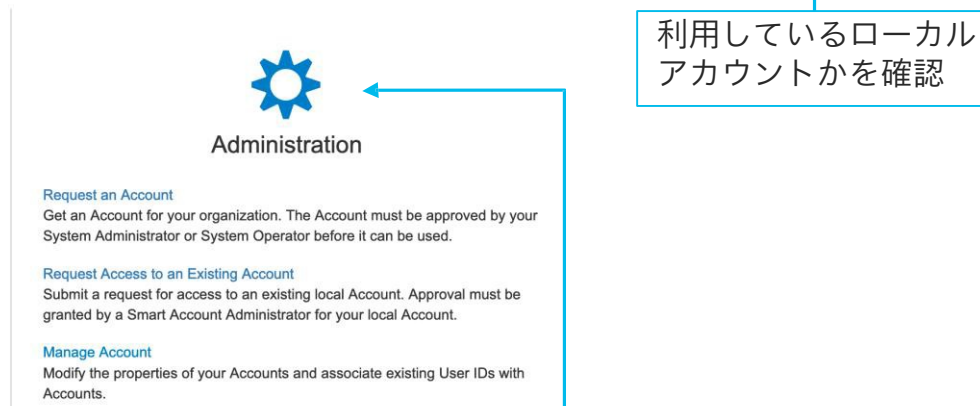
## 拡張性の向上

- 500 以上のアカウント
- 100,000 台の製品インスタンス（ローカルアカウントあたり 25,000）
- 規模の拡大に向けた開発をアクティブに継続中

# ライセンスワークスペース



- ✓ ローカルライセンスの可用性と使用状況を表示
- ✓ オンプレミスに登録された製品を管理
- ✓ 製品とライセンスの使用状況に関するレポートを作成
- ✓ ローカルアカウントのアクティビティを表示



利用しているローカルアカウントかを確認

- ✓ ローカル バーチャル アカウントの作成と管理
- ✓ ローカルユーザのアカウントアクセスを管理
- ✓ タグとローカルユーザグループをカスタマイズ
- ✓ イベントログを表示する

# 管理ワークスペース - 登録



アカウント

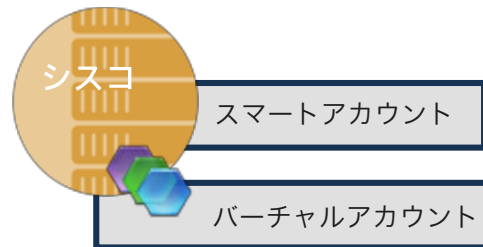
- すべてのローカルアカウントはスマートアカウント/バーチャルアカウントにマッピングされます。
- 柔軟なアカウント設定モデル
  - 単一のスマートアカウントを複数のオンプレミスアカウントにマッピング
  - 複数のスマートアカウントを複数のオンプレミスアカウントにマッピング



SSM オンプレミス ローカル アカウント

ローカル バーチャル アカウント (デフォルト)

- データセンターアセット
- 本社スタッフアセット



# 管理ワークスペース - アカウント登録

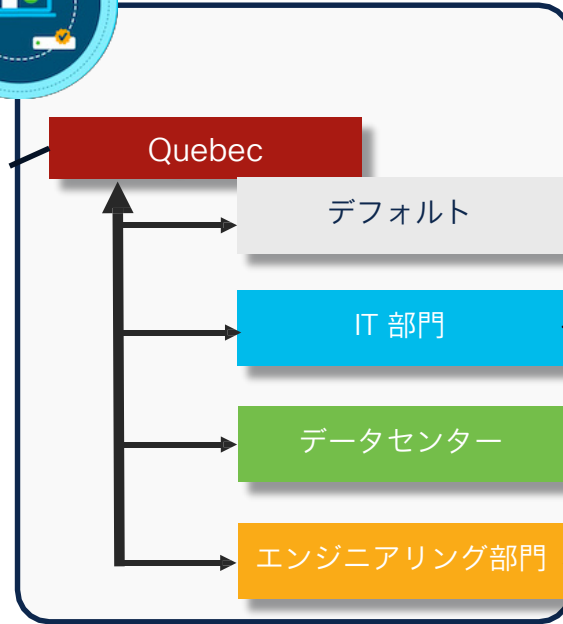
例：オンプレミスのアカウントを単一のスマートアカウントに登録



アカウント



(software.cisco.com)



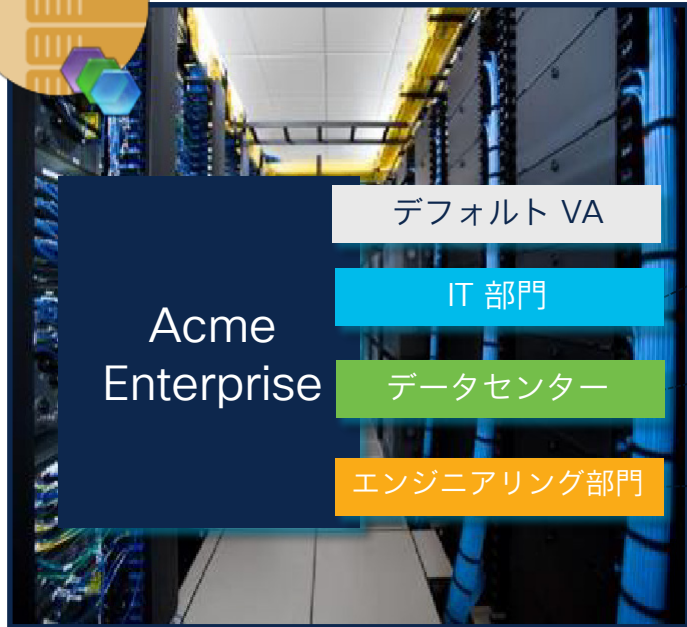
SSM オンプレミス

# 管理ワークスペース - アカウント登録

例：オンプレミスのアカウントを単一のスマートアカウントに登録



アカウント



(software.cisco.com)



SSM オンプレミス



# 管理ワークスペース - アカウント登録

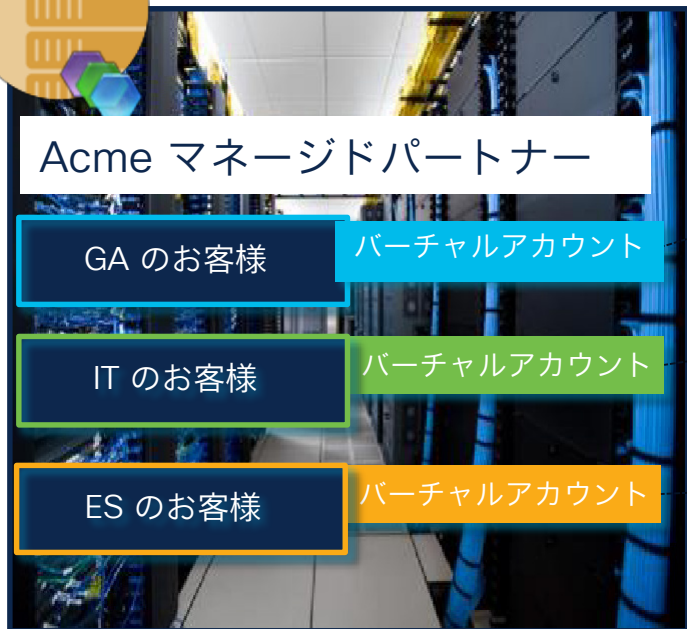
例：オンプレミスのアカウントを複数のスマートアカウントに登録



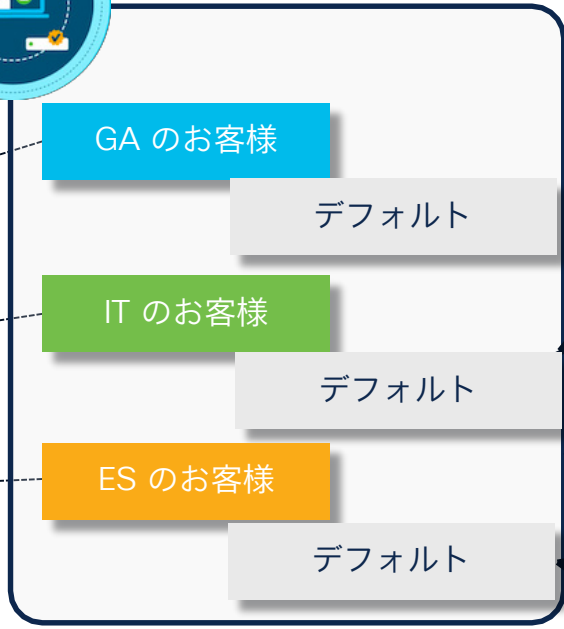
アカウント



シスコ



(software.cisco.com)



SSM オンプレミス

# 管理ワークスペース - 同期

## 同期の要件

SSM オンプレミスサーバは、シスコと定期的に同期する必要があります。

- 接続モードの場合、自動的に同期を行うようにスケジュール
- 非接続モードの場合、手動でファイルを転送することで同期
- 同期はスケジュールまたは手動での実行可能
  - デフォルトの場合、SSM オンプレミスは **30 日間隔** でシスコと同期
  - 手動で同期を実行する場合、お客様の多くは **90 日間隔** でシスコと同期
  - シスコでは同期間隔が **180 日 (6 か月)** を超えないことを推奨
- **364 日以内にシスコとの同期が必要**  
364 日間同期が実行されない場合
  - シスコに新しいアカウントの登録が必要
  - アカウント内のすべての ID トークンの期限切れ
  - 製品の再登録が必要



同期

# 管理ワークスペース - 同期

## アカウントの同期



同期

ローカルアカウント : Quebec

デフォ

License	Billing	Purchased
+	Cisco ASAv30	Prepaid 5
+	CSR 1KV AX 100M	Prepaid 15



ASAv30

5
0
+ 0
= 5

CSR 1KV

15
0
+ 0
= 15

スマートアカウント :  
Acme Enterprise



Quebec VA

License	Billing	Purchased
+	Cisco ASAv30	Prepaid 5
+	CSR 1KV AX 100M	Prepaid 15

# 管理ワークスペース - 同期

## アカウントの同期

ローカルアカウント : Quebec

### デフォルト

<input type="checkbox"/>	License	Billing	Purchased
<input type="checkbox"/>			
<input checked="" type="checkbox"/>	Cisco ASAv30	Prepaid	1
<input checked="" type="checkbox"/>	CSR 1KV AX 100M	Prepaid	6

### IT 部門 LVA :

<input type="checkbox"/>	License	Billing	Purchased
<input type="checkbox"/>			
<input checked="" type="checkbox"/>	Cisco ASAv30	Prepaid	4
<input checked="" type="checkbox"/>	CSR 1KV AX 100M	Prepaid	7

### データセンター LVA :

<input type="checkbox"/>	License	Purchased
<input type="checkbox"/>		
<input checked="" type="checkbox"/>	CSR 1KV AX 100M	2



同期

スマートアカウント :  
Acme Enterprise

シスコ

### Quebec VA

<input type="checkbox"/>	License	Billing	Purchased
<input type="checkbox"/>			
<input checked="" type="checkbox"/>	Cisco ASAv30	Prepaid	5
<input checked="" type="checkbox"/>	CSR 1KV AX 100M	Prepaid	15

# 管理ワークスペース - 同期

## アカウントの同期



同期

ローカルアカウント : Quebec

### デフォルト

License	Billing	Purchased
<input type="checkbox"/>		
+ Cisco ASAv30	Prepaid	1
+ CSR 1KV AX 100M	Prepaid	6

### IT 部門 LVA :

License	Billing	Purchased
<input type="checkbox"/>		
+ Cisco ASAv30	Prepaid	4
+ CSR 1KV AX 100M	Prepaid	7

### データセンター

License	Purchased
<input type="checkbox"/>	
+ CSR 1KV AX 100M	2



### ASAv30

1
4
+ 0
= 5

### CSR 1KV

6
7
+ 2
= 15

スマートアカウント :  
Acme Enterprise



### Quebec VA

License	Billing	Purchased
<input type="checkbox"/>		
+ Cisco ASAv30	Prepaid	5
+ CSR 1KV AX 100M	Prepaid	15



# SSM オンプレミス - 製品の登録

## 厳格な証明書チェックによる製品登録

- ・ 厳格な SSL 証明書チェックをサポートする製品では、**ホスト共通名**が、製品に設定されている「宛先 http」の URL アドレスと一致する必要があります。
- ・ ホスト名に有効な DNS エントリがない場合は、SSM オンプレミスサーバの IP アドレスを代用してください。

Security

Account Password Certificates Event Log

Product Certificate

Host Common Name  
10.83.111.69

Save

NOTE: The Host Common Name is typically composed of Host + Domain Name and will look like "www.yoursite.com" or "yoursite.com". The SSL Server Certificate used for product communications is specific to the Common Name that has been issued at the Host. Therefore, the Common Name must match the Web address you will use to configure the Cisco Product when connecting to SSM On-Prem. If you change the Common Name, you must resynchronize your Local Account in order for Cisco to issue a new CSR

Browser Certificate

Add Generate CSR

localhost  
(Default Certificate) EXPIRATION DATE: - ▾

宛先 http のアドレス <https://10.83.111.69/Transportgateway/services/DeviceRequestHandler>

# SSM オンプレミス - 製品の登録

## 厳格な証明書チェックによる製品登録

オンプレミス証明書に **CN=Cisco-On-Prem** が割り当てられ、IP アドレスが 10.83.111.69 の場合

- デバイスの URL を次のように変更できる場合：  
<https://Cisco-On-Prem/Transportgateway>
- デバイスが「Cisco-On-Prem」を有効な IP アドレスとして解決できることを意味します。
- 通常の IOS では、ホスト名を IP にスタティックマップできます。  
例：「ip host Cisco-On-Prem 10.83.111.69」

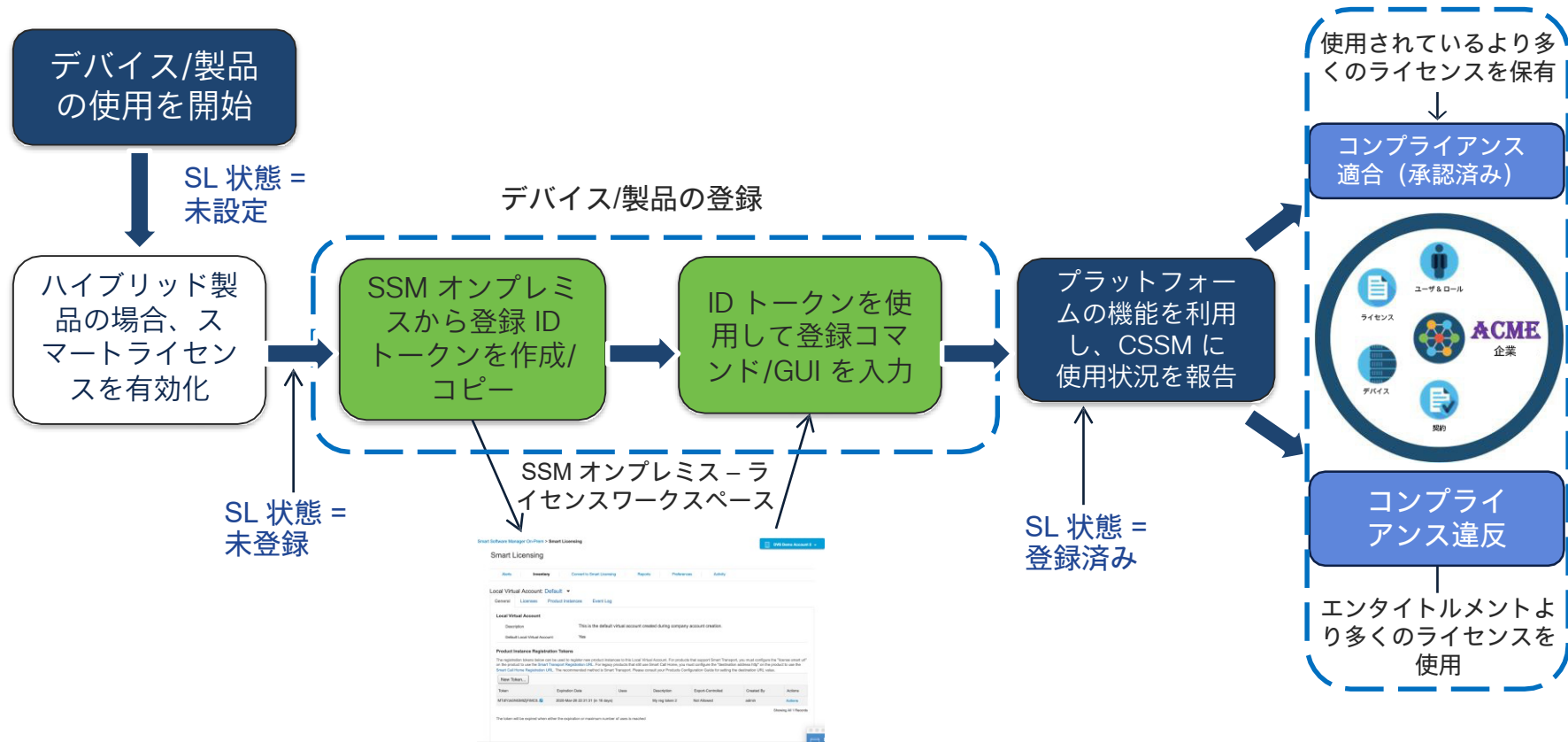
- デバイスの URL を次のように変更できる場合：  
<https://10.83.111.69/Transportgateway>
- オンプレミス名を 10.83.111.69 に構成する必要があります。
- この構成により、証明書が CN = 10.83.111.69 に割り当てられます。

デフォルトでは、HTTPS は SSL ハンドシェイク中にサーバ ID チェックを実行し、宛先 URL が証明書に入力された共通名（ホスト名または IP）と同じであることを確認します。

注：製品がサポートしている場合は、「*no http secure server-identity-check*」を使用してチェックを無効化し、引き続き URL で IP アドレスを使用できます。

# SSM オンプレミス - 製品の登録

## スマートライセンスのワークフロー





# SSM オンプレミス - 製品の登録

## 設定

- オンプレミスへの製品登録は、シスコと完全に同じ方法で行います。
- 「承認済みのバックエンドアドレス」を変更します（製品マニュアルを参照してください）。

## Smart Transport の構成

```
Device(config)# license smart transport smart
Device(config)# license smart privacy [all | hostname | version]
Device(config)# license smart url https://10.83.111.69/SmartTransport
```

または

## Smart Call Home の設定

```
call-home
 data-privacy level hostname
 profile "CiscoTAC-1"
  no destination transport-method email
  destination address http https://10.83.111.69/Transportgateway/services/DeviceRequestHandler
  no destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

# SSM オンプレミス - 製品の登録

## グローバル データ プライバシー設定

```
:sync: 2.0.0,
:version: 2.0.0
:id_cert: |- XXXXXXXXXXXXXXXXXXXX

:collector_id: 4cdd0470-e5e4-0132-a310-005056841670
:csr: |-
:last_sync: 2017-Jun-22 08:50:35 UTC
  :last_generated: 2017-Jul-20 11:22:16 UTC
:virtual_accounts:
- :id: 101342
  :name: Virtual-Account-1
  :product_instances:
- :id: 2373d312-2cd8-4029-9517-8c60037cca8c
  :registration_date: 2017-Jun-12 07:25:40 UTC
  :last_contact_date: 2017-Jul-02 06:13:47 UTC
  :is_active: true
  :software_tag_identifier: regid.2013-08.com.cisco.CSR1000V,1.0_1562da96-9176-4f99-a6cb-14b4dd0fa135
  :udi_pid: CSR1000V
  :hostname: Router-1
  :ip_address:
  :mac_address:
  :udi_serial_number: 97YZFA9VYJK
  :host_identifier:
  :licenses:
- :tag_id: 1146
  :tag: regid.2014-05.com.cisco.ax_2500M,1.0_3e0288f3-4838-47c2-93a8-3d8743850f0c
  :consumed_quantity: 1
```

### Global Synchronization Data Privacy Settings

Exclude the following from the product instance data sent to Cisco. This change applies to all accounts unless overridden individually on each account.

- Hostname
- IP Address
- MAC Address

注：シスコ製品がオンプレミスにこれらを送信する場合も、オンプレミス管理ワークスペースのデータプライバシー設定により、シスコとのデータ交換で除外できます。

# SSM オンプレミス - 通信チャネルおよびポート



シスコ製品はデフォルトで通信を開始（Smart Software Manager とは追加設定なしで通信可能）

## 製品：

HTTPS (443) : tools.cisco.com  
HTTP (80) : www.cisco.com

## オンプレミス

HTTPS (443) : swapi.cisco.com  
IPv4 : 146.112.59.25  
IPv6 : 2a04:e4c7:ffe::4

シスコ製品は Smart Software Manager オンプレミスとの通信に、同じプロトコルを使用

## プロトコル：

ユーザインターフェイス : HTTPS (8443) のみ

製品 : HTTP (80) / HTTPS (443)

CSSM : HTTPS (443)

## 同期：

api.cisco.com (旧)

swapi.cisco.com (新)

アカウント登録：

cloudsso.cisco.com

ありがとうございました

