ポリシーを使用したスマートライセンシングに関する情報

概要

ポリシーを使用したスマートライセンシングは、ライセンスのさまざまな側面をシームレスに体験できるソフトウェアライセンス管理ソリューションです。

- ライセンスの購入：既存のチャネルからライセンスを購入し、Cisco Smart Software Manager（CSSM）ポータルを使用して製品インスタンスとライセンスを表示します。

（注） ポリシーを使用したスマートライセンシングの実装を簡素化するには、新しいハードウェアまたはソフトウェアを注文する際にスマートアカウントとバーチャルアカウントの情報を提供します。これにより、シスコは製造時に該当するポリシーおよび承認コード（用語は以下のセクション概念 （2 ページ）で説明）をインストールできます。

- 使用：ほとんどのライセンスは適用（エンフォース）されません。つまり、ソフトウェアとそれに関連付けられているライセンスの使用を開始する前に、キーの登録や生成などのライセンス固有の操作を完了する必要はありません。輸出規制および適用されたライセンスのみ、使用前にシスコの承認が必要です。ライセンスの使用状況はタイムスタンプとともにデバイスに記録され、必要なワークフローは後日完了できます。

- ライセンスの使用状況をCSSMにレポート：ライセンス使用状況レポートには複数のオプションを使用できます。Cisco Smart Licensing Utility（CSLU）を使用することも、CSSMに使用状況の情報を直接レポートすることもできます。使用状況情報をダウンロードしてCSSMにアップロードする、クローズドネットワークのオフラインレポートのプロビジョニングも使用できます。使用状況レポートはプレーンテキストのXML形式です。リソース使用率測定レポートの例を参照してください。
- 調整：差分請求が適用される状況用（購入と消費を比較して差分がある場合）。

概念

ここでは、ポリシーを使用したスマートライセンシングの主要な概念について説明します。

ライセンス執行（エンフォースメント）タイプ

所与のライセンスは、3つの適用タイプのいずれかに属します。適用タイプは、ライセンスを使用する前に承認が必要かどうかを示します。

- 不適用または非適用

  ライセンスの大半はこの適用タイプに属します。不適用ライセンスは、外部との接続がないネットワークで使用する前、または接続されたネットワークでの登録前に承認を必要としません。このようなライセンスの使用条件は、エンドユーザライセンス契約（EULA）に基づきます。

- 適用

  この適用タイプに属するライセンスは、使用前に承認が必要です。必要な承認は承認コードの形式で行われ、対応する製品インスタンスにインストールする必要があります。

  適用ライセンスの例としては、シスコの産業用イーサネットスイッチで利用可能なMedia Redundancy Protocol（MRP）クライアントライセンスがあります。

- 輸出規制

  この適用タイプに属するライセンスは米国の取引規制法によって輸出が制限されていて、これらのライセンスは使用前に承認が必要です。これらのライセンスの場合も、必要な承認コードは、対応する製品インスタンスにインストールする必要があります。シスコは、ハードウェア購入の際に発注がある場合、輸出規制ライセンスをプリインストールすることがあります。

  輸出規制ライセンスの例としては、特定のシスコルータで使用可能な高セキュリティ（HSECK9）ライセンスがあります。

適用および輸出規制ライセンスのリストは限定されています。シスコは、ハードウェア購入の際に発注がある場合、輸出規制および適用ライセンスに必要な承認をプリインストールすることがあります。完全で最新のリストについては、「承認コード」セクションの表 1 : SLAC を必要とするライセンス （3 ページ）を参照してください。

ライセンス継続期間

これは、購入したライセンスが有効な期間を指します。所与のライセンスは、上記のいずれかの適用タイプに属し、次の期間有効です。

- 永久：このライセンスには使用期限日はありません。
- サブスクリプション：ライセンスは特定の日付まで有効です。

承認コード

スマートライセンシング承認コード（SLAC）は、輸出規制または適用（エンフォース）ライセンスの有効化および継続使用を可能にします。承認コードは製品インスタンスにインストールされます。使用しているライセンスに承認コードが必要な場合は、CSSM から要求できます。

SLAC を削除して CSSM ライセンスプールに戻すことができます。ただし、これを行うには、まずライセンスを使用する機能を無効にする必要があります。使用中の SLAC は返却できません。

表 *1 : SLAC* を必要とするライセンス

適用タイプ	ライセンス
輸出規制	HSECK9
適用	MRP クライアント MRP マネージャ

（注） 以前のライセンスモデルからポリシーを使用したスマートライセンシングにアップグレードする場合は、これらのライセンスのうちいずれかを所有している可能性がありますが、それぞれのライセンスには固有の承認コードである特定ライセンス予約（SLR）または製品認証キー（PAK）があります。これらの既存のライセンスの承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後にサポートされます。

ポリシー

ポリシーは、製品インスタンスに次のレポート手順を提供します。

- License usage report acknowledgement requirement (Reporting ACK required)：ライセンス使用状況レポートは RUM レポートと呼ばれ、確認応答は ACK と呼ばれます（「RUM レポートおよびレポート確認応答」を参照）。これは、この製品インスタンスのレポートにCSSM 確認応答が必要かどうかを指定する yes または no の値です。デフォルトポリシーは常に「yes」に設定されます。

- First report requirement (days)：最初のレポートは、ここで指定した期間内に送信される必要があります。
- Reporting frequency (days)：後続のレポートは、ここで指定した期間内に送信される必要があります。
- Report on change (days)：ライセンスの使用状況が変更された場合は、ここで指定した期間内にレポートが送信される必要があります。

ポリシー選択について

CSSMは、製品インスタンスに適用されるポリシーを決定します。特定の時点で使用されているポリシーは1つだけです。ポリシーとその値は、使用されているライセンスなど、さまざまな要因に基づいています。

`Cisco default`は、製品インスタンスで常に使用可能なデフォルトポリシーです。他のポリシーが適用されていない場合、製品インスタンスはこのデフォルトポリシーを適用します。次の表（表 2 : ポリシー：Cisco default （4 ページ））に、`Cisco default` ポリシー値を示します。

お客様はポリシーを設定することはできませんが、Cisco Global Licensing Operations チームに連絡して、カスタマイズされたポリシーを要求することができます。Support Case Manager に移動します。[OPEN NEW CASE] をクリックし、[Software Licensing] を選択します。ライセンスチームから、プロセスの開始や追加情報について連絡があります。カスタマイズされたポリシーは、CSSM のスマートアカウントを介して使用することもできます。

（注） 適用されているポリシー（使用中のポリシー）とそのレポート要件を確認するには、特権EXECモードで **show license all** コマンドを入力します。

表 *2 :* ポリシー：***Cisco default***

ポリシー：`Cisco default`	デフォルトポリシー値
Export (Perpetual/Subscription) （注） 適用タイプが「輸出規制」のライセンスにのみ適用されます。	Reporting ACK required：Yes First report requirement (days)：0 Reporting frequency (days)：0 Report on change (days)：0
Enforced (Perpetual/Subscription) （注） 適用タイプが「適用（エンフォース）」のライセンスにのみ適用されます。	Reporting ACK required：Yes First report requirement (days)：0 Reporting frequency (days)：0 Report on change (days)：0

ポリシー：`Cisco default`	デフォルトポリシー値
Unenforced/Non-Export Perpetual[1]	Reporting ACK required：Yes First report requirement (days)：365 Reporting frequency (days)：0 Report on change (days)：90
Unenforced/Non-Export Subscription	Reporting ACK required：Yes First report requirement (days)：90 Reporting frequency (days)：90 Report on change (days)：90

[1] Unenforced/Non-Export Perpetual の場合：デフォルトポリシーの最初のレポート要件（365日以内）は、ディストリビュータやパートナーからハードウェアやソフトウェアを購入した場合にのみ適用されます。

RUM レポートおよびレポート確認応答

リソース使用率測定レポート（RUM レポート）は、ポリシーで指定されたレポート要件を満たすために製品インスタンスが生成するライセンス使用状況レポートです。

確認応答（ACK）は CSSM からの応答であり、RUM レポートのステータスに関する情報を提供します。

製品インスタンスに適用されるポリシーによって、次のレポート要件が決まります。

- RUM レポートが CSSM に送信されるかどうか、およびこの要件を満たすために提供される最大日数。
- RUM レポートに CSSM からの確認応答（ACK）が必要かどうか。
- ライセンス消費の変化を報告するために提供される最大日数。

RUM レポートには、信頼コード要求や SLAC 要求などの他の要求が伴う場合があります。そのため、受信した RUM レポート ID に加えて、CSSM からの ACK には承認コード、信頼コード、およびポリシーファイルが含まれることがあります。

信頼コード

製品インスタンスがすべての RUM レポートに署名するために使用する、UDI に関連付けられた公開キー。これにより、改ざんが防止され、データの真正性が確保されます。

アーキテクチャ

ここでは、ポリシーを使用したスマートライセンシングの実装に含めることができるさまざまなコンポーネントについて説明します。

製品インスタンス

製品インスタンスとは、Unique Device Identifier（UDI）によって識別されるシスコ製品の単一インスタンスです。

製品インスタンスは、ライセンス使用状況（RUM レポート）を記録および報告し、期限切れのレポートや通信障害などに関するアラートとシステムメッセージを提供します。RUM レポートおよび使用状況データは、製品インスタンスに安全に保存されます。

このドキュメントでは、「製品インスタンス」という用語は、特に明記しない限り、サポートされているすべての物理および仮想製品インスタンスを指します。このドキュメントの範囲内にある製品インスタンスについては、サポート対象製品 （12 ページ）を参照してください。

CSSM

Cisco Smart Software Manager（CSSM）は、一元化された場所からすべてのシスコ ソフトウェア ライセンスを管理できるポータルです。CSSM は、現在の要件を管理し、将来のライセンス要件を計画するための使用傾向を確認するのに役立ちます。

CSSM Web UI には https://software.cisco.com からアクセスできます。[License] タブで、[Smart Software Licensing] のリンクをクリックします。

CSSM に接続できるさまざまな方法については、サポートされるトポロジ （7 ページ） のセクションを参照してください

CSSM では、次のことができます。

- バーチャルアカウントを作成、管理、または表示する。
- 製品インスタンスの登録トークンを作成および管理する。
- バーチャルアカウント間または表示ライセンス間でライセンスを転送する。
- 製品インスタンスを転送、削除、または表示する。
- バーチャルアカウントに関するレポートを実行する。
- 電子メール通知の設定を変更する。
- バーチャルアカウント情報を表示する。

CSLU

Cisco Smart License Utility（CSLU）は Windows ベースのレポートユーティリティで、CSSM に接続されている間、または切断モードの際の、ライセンス集約ワークフローを提供します。このユーティリティが実行する主な機能は次のとおりです。

- ワークフローのトリガー方法に関するオプションを提供します。ワークフローは、CSLU や製品インスタンスによってトリガーできます。
- 製品インスタンスから使用状況レポートを収集し、その使用状況レポートを対応するスマートアカウントやバーチャルアカウントにアップロードします。オンラインでもオフライン（ファイルを使用）でも可能です。同様に、RUM レポート ACK をオンラインまたはオフラインで収集し、製品インスタンスに返送します。
- 承認コード要求を CSSM に送信し、承認コード[2]を CSSM から受信します。

CSLU は、次の方法で実装に含めることができます。

- CSSM に接続されているスタンドアロンツールとして CSLU を使用するための Windows アプリケーションをインストールします。
- CSSM から切断されているスタンドアロンツールとして CSLU を使用するための Windows アプリケーションをインストールします。このオプションを使用すると、必要な使用状況情報がファイルにダウンロードされ、CSSM にアップロードされます。これは、外部と接続していないネットワークに適しています。

サポートされるトポロジ

このセクションでは、ポリシーを使用したスマートライセンシングを実装するさまざまな方法について説明します。各トポロジについて、付属の概要を参照してセットアップの動作設計を確認し、考慮事項と推奨事項（ある場合）を参照してください。

トポロジを選択した後

トポロジを選択したら、「ポリシーを使用したスマートライセンシングの設定方法：トポロジ別のワークフロー」の対応するワークフローを参照して、その実装方法を確認してください。これらのワークフローは、トポロジを実装する最も簡単で迅速な方法を提供します。これらのワークフローは、新しい展開用であり、既存のライセンスソリューションからのアップグレード用や移行用ではありません。

初期実装後、追加の設定タスクを実行する必要がある場合（たとえば、一括で承認コードを手動で要求する場合、または RUM レポートの同期などのメンテナンスタスクを実行する場合）は、「ポリシーを使用したスマートライセンシングのタスクライブラリ」を参照してください。

[2] CSLU を使用して、コントローラモード（Cisco SD-WAN 機能用）で動作するシスコルータの承認コード要求を転送できます。

（注） 続行する前に、必ず「サポートされるトポロジ」を確認してください。

CSLU を介して CSSM に接続

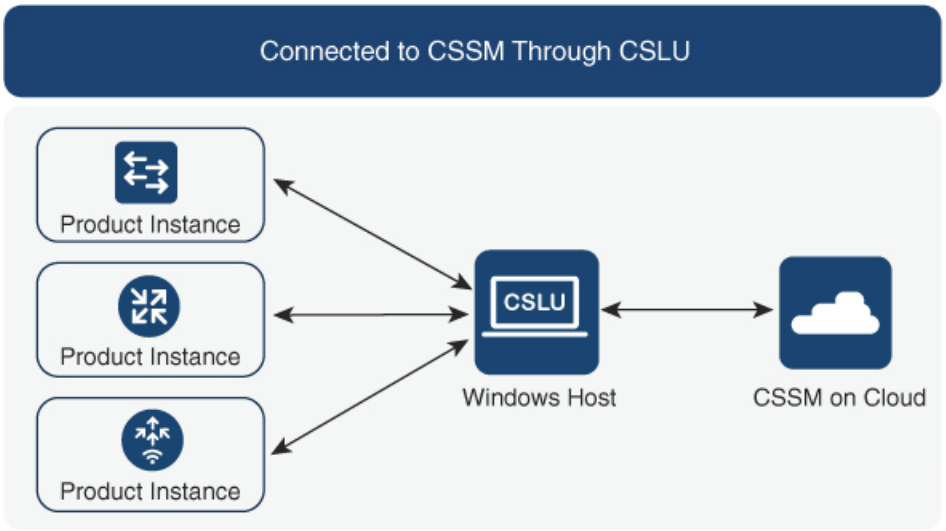
概要：

ここでは、ネットワーク内の製品インスタンスは CSLU に接続され、CSLU は CSSM との単一のインターフェイスポイントになります。製品インスタンスは、必要な情報を CSLU にプッシュするように設定できます。または、構成可能な頻度で製品インスタンスから必要な情報を取得するように CSLU を設定することもできます。

製品インスタンス開始型通信（プッシュ）：製品インスタンスは、CSLU の REST エンドポイントに接続することで、CSLU との通信を開始します。送信されるデータには、RUM レポート、および承認コード、信頼コード、ポリシーの要求が含まれます。必要な間隔で自動的に RUM レポートを CSLU に送信するように製品インスタンスを設定できます。これは、製品インスタンスのデフォルトの方法です。

CSLU 開始型通信（pull 型）：製品インスタンスからの情報の取得を開始するために、CSLU は YANG を使用した NETCONF、RESTCONF、gRPC のモデル、またはネイティブ REST API を使用して製品インスタンスに接続します。サポートされるワークフローには、RUM レポートの製品インスタンスからの受信と CSSM への送信、承認コードのインストール、信頼コードのインストール、およびポリシーの適用が含まれます。

図 *1:* トポロジ：***CSLU*** を介して ***CSSM*** に接続



考慮事項または推奨事項：

ネットワークのセキュリティポリシーに応じて通信方法を選択します。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSLU を介して CSSM に接続を参照してください。

CSSM に直接接続

概要：

このトポロジは、スマートライセンシングの以前のバージョンで使用でき、ポリシーを使用したスマートライセンシングで引き続きサポートされます。

ここでは、製品インスタンスから CSSM への直接かつ信頼できる接続を確立します。直接接続には、CSSM へのネットワーク到達可能性が要求されます。その後、製品インスタンスがメッセージを交換し、CSSM と通信するには、このトポロジで使用可能な転送オプションのいずれかを設定します（以下を参照）。最後に、信頼を確立するには、CSSM の対応するスマートアカウントとバーチャルアカウントからトークンを生成し、製品インスタンスにインストールする必要があります。

次の方法で CSSM と通信するように製品インスタンスを設定できます。

- スマート転送を使用して CSSM と通信する。

  スマート転送は、スマートライセンシング（JSON）メッセージが HTTPS メッセージ内に含まれ、製品インスタンスと CSSM の間で交換されることにより通信する転送方法です。次のスマート転送設定オプションを使用できます。

  - スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりに設定する必要があります。
  - HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。

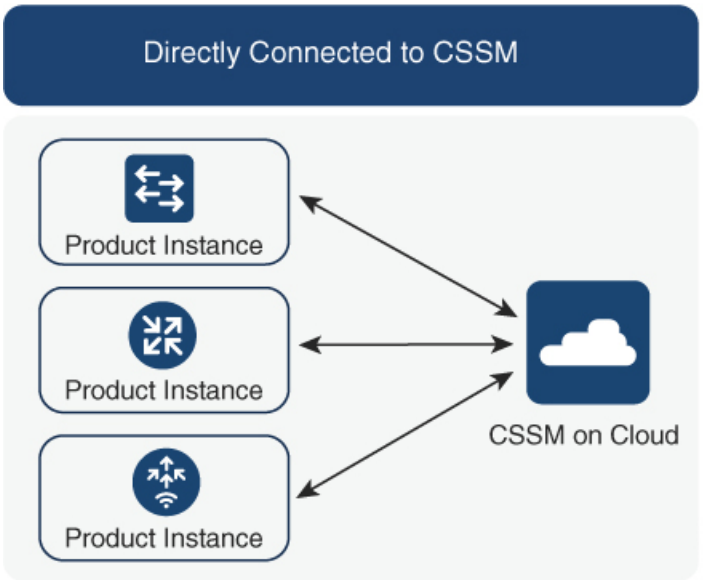
- Call Home を使用して CSSM と通信する。

  Call Home を使用すると、E メールベースおよび Web ベースで重大なシステム イベントの通知を行えます。CSSM へのこの接続方法は、以前のスマートライセンシング環境で使用でき、ポリシーを使用したスマートライセンシングで引き続き使用できます。次の Call Home 設定オプションを使用できます。

  - ダイレクトクラウドアクセス：この方法では、製品インスタンスはインターネット経由で CSSM に使用状況情報を直接送信します。接続に追加のコンポーネントは必要ありません。
  - HTTPS プロキシを介したダイレクトクラウドアクセス：この方法では、製品インスタンスはインターネット経由でプロキシサーバ（Call Home Transport Gateway または市販のプロキシ（Apache など）のいずれか）を介して CSSM に使用状況情報を送信します。

（注） ポリシーを使用したスマートライセンシングは、Cisco Smart Software Manager On-Prem（旧称 Cisco Smart Software Manager サテライト）をサポートしていません。

図 *2:* トポロジ：*CSSM* に直接接続



考慮事項または推奨事項：

CSSMに直接接続する場合は、スマート転送が推奨される転送方法です。この推奨事項は以下に適用されます。

- 新規展開
- 以前のライセンスモデル。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。
- 現在 Call Home 転送方法を使用している登録済みライセンス。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。
- 以前のライセンスモデルの評価ライセンスや期限切れのライセンス。ポリシーを使用したスマートライセンシングへの移行後に設定を変更します。

移行後に設定を変更するには、トポロジのワークフロー：CSSMに直接接続の「製品インスタンスの設定」にある「接続方法と転送タイプの設定」のオプション 1 を参照してください。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSSMに直接接続を参照してください。

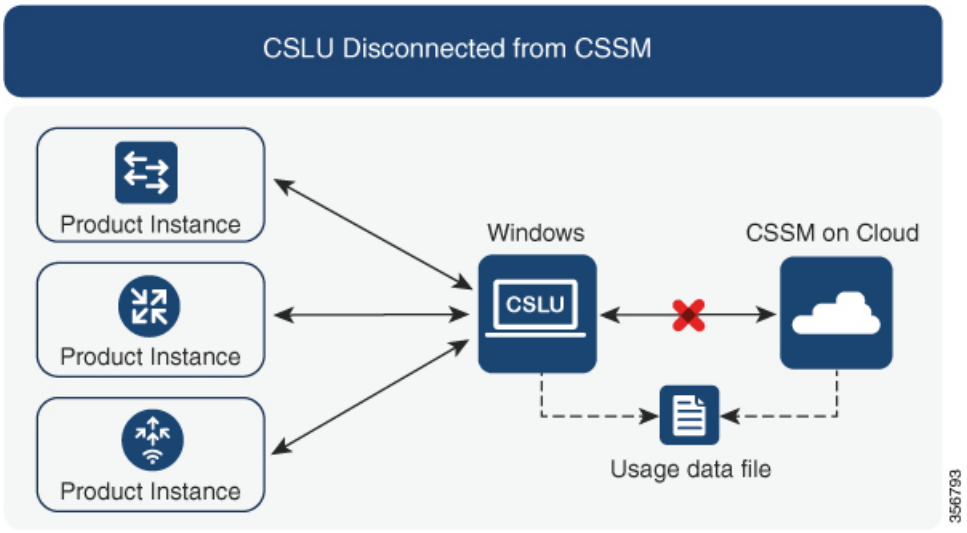
CSLU は CSSM から切断

概要：

ここでは、製品インスタンスが CSLU と通信し、製品インスタンス開始の通信または CSLU 開始の通信を実装するオプションがあります（CSLU を介して CSSM に接続のトポロジと同様）。CSLU と CSSM 間の通信のもう一方はオフラインです。CSLU には、CSSM から切断されたモードで動作するオプションがあります。

CSLU と CSSM 間の通信は、署名済みファイルの形式で送受信され、オフラインで保存された後、場合によっては CSLU または CSSM にアップロードまたはダウンロードされます。

図 *3 :* トポロジ：*CSLU* は *CSSM* から切断



考慮事項または推奨事項：

なし。

次の手順：

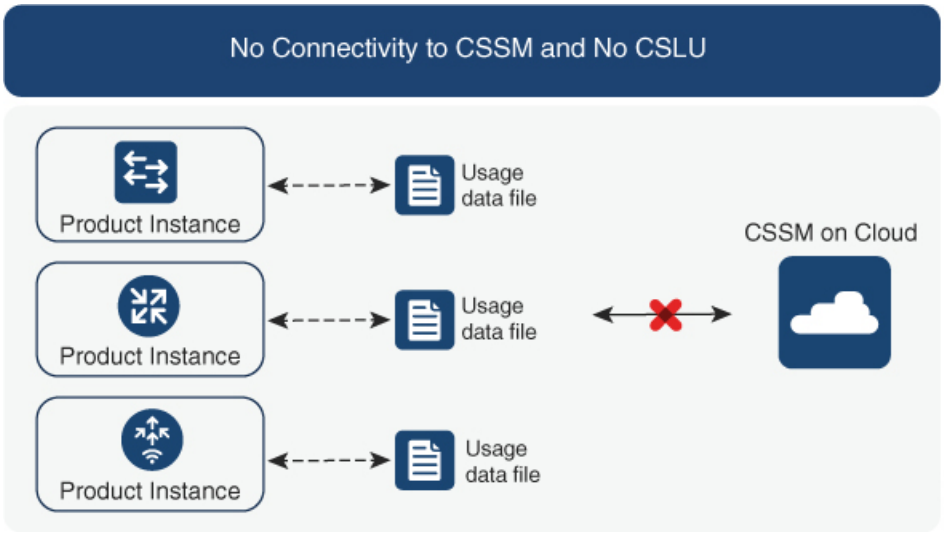
このトポロジを実装するには、トポロジのワークフロー：CSLU は CSSM から切断を参照してください。

CSSM への接続なし、CSLU なし

概要：

ここでは、製品インスタンスと CSSM は相互に切断され、他の中間ユーティリティまたはコンポーネントはありません。すべての通信は、ファイルのアップロードとダウンロードという形式です。

図 *4:* トポロジ：***CSSM*** への接続なし、***CSLU*** なし



考慮事項または推奨事項：

このトポロジは、製品インスタンスがネットワークの外部とオンラインで通信できない高セキュリティ展開に適しています。

次の手順：

このトポロジを実装するには、トポロジのワークフロー：CSSM への接続なし、CSLU なしを参照してください。

サポート対象製品

このセクションでは、ポリシーを使用したスマートライセンシングをサポートする Cisco IOS-XE 製品インスタンスについて説明します。特に指定のない限り、製品シリーズのすべてのモデル（製品 ID または PID）がサポートされます。

表 *3:* ポリシーを使用したスマートライセンシング：サポート対象製品

製品カテゴリ	製品シリーズ
Cisco アグリゲーション、統合、およびクラウドサービスルータ	
	Cisco 1000 シリーズ サービス統合型ルータ
	Cisco 4000 シリーズ サービス統合型ルータ
	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ
Cisco Catalyst 8000 エッジ プラットフォーム ファミリ	

製品カテゴリ	製品シリーズ
	Catalyst 8300 シリーズ エッジ プラットフォーム
	Catalyst 8500 シリーズ エッジ プラットフォーム

他の機能との相互作用

高可用性

このセクションでは、ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンを実行するときに、高可用性設定に適用される考慮事項について説明します。次の高可用性セットアップは、このドキュメントの範囲内です。

1つのアクティブ、1つのスタンバイ、および1つ以上のメンバーで構成されるデバイススタック

デュアル RP（ルートプロセッサ）セットアップ。1 つのシャーシに 2 つの RP がインストールされ、1 つはアクティブ、もう 1 つはスタンバイです。

デュアルシャーシ セットアップ[3]（固定またはモジュラ）。一方のシャーシにアクティブ、もう一方のシャーシにスタンバイがあります。

モジュラシャーシでの、デュアルシャーシとデュアル RP のセットアップ[4]。ここでも 2 つのシャーシが関係し、1 つのシャーシにアクティブ RP、もう 1 つのシャーシにスタンバイ RP があります。デュアル RP とは、最小要件である 1 つのシャーシだけに追加のシャーシ内スタンバイ RP、または各シャーシにシャーシ内スタンバイ RP があることを指します。

高可用性セットアップでの承認コード要件

使用前に承認が必要なライセンスを使用していて（SLAC または SLR、PLR など）、上記の高可用性セットアップのいずれかを使用している場合、必要な承認コードの数は、UDI の数に対応します。

- アクティブとスタンバイの UDI が同じ場合は、1 つの承認コードのみが必要です。これは、UDI が（個々の RP にではなく）シャーシにある場合です。
- 同じシャーシ内のデュアル RP に 2 つの異なる UDI がある場合（つまり UDI が RP にある場合）、各 RP に専用の承認コードが必要です。
- 高可用性セットアップで 2 つのシャーシが関係している場合は、各シャーシに専用の UDI があるため、専用の承認コードが必要です。

[3] Cisco Catalyst スイッチで使用可能な Cisco StackWise Virtual 機能が、このようなセットアップの例です。
[4] Cisco Catalyst スイッチで使用可能なルートプロセッサ冗長性を備えたクアッドスーパーバイザが、このようなセットアップの例です。

- デバイススタックの場合は、アクティブのみに承認コードが必要です。

UDI 情報を表示するには、特権 EXEC モードで **show license udi** コマンドを使用します。高可用性セットアップの場合は、すべての UDI が表示されます。

高可用性セットアップでの信頼コード要件

必要な信頼コードの数は、UDIの数によって異なります。アクティブな製品インスタンスは、高可用性セットアップのすべてのデバイスに対する要求を送信し、ACK で返されるすべての信頼コードをインストールできます。

高可用性セットアップでのポリシー要件

高可用性セットアップにのみ適用されるポリシー要件はありません。スタンドアロン製品インスタンスの場合と同様に、高可用性セットアップにも1つのポリシーのみが存在し、これがアクティブになります。アクティブのポリシーは、設定のすべてのスタンバイまたはメンバーに適用されます。

高可用性セットアップでの製品インスタンス機能

このセクションでは、高可用性セットアップでの一般的な製品インスタンス機能と、新しいスタンバイまたはメンバーが既存の高可用性セットアップに追加された場合の製品インスタンスの動作について説明します。

承認コードと信頼コードの場合：アクティブな製品インスタンスは、スタンバイおよびメンバーの承認コードと信頼コードを（必要な場合に）要求し、インストールできます。

ポリシーの場合：アクティブな製品インスタンスがスタンバイと同期します。

レポートの場合：アクティブな製品インスタンスのみが使用状況を報告します。アクティブは、高可用性セットアップのすべてのデバイス（スタンバイまたはメンバーを適宜）の使用状況情報を報告します。スケジュールされたレポートに加えて、次のイベントがレポートをトリガーします。

- スタンバイの追加または削除。RUM レポートには、新しく追加または削除されたスタンバイまたはメンバーに関する情報が含まれます。
- スイッチオーバー。
- リロード。

新規メンバーまたはスタンバイ追加の場合：

- CSLU に接続されている製品インスタンスは、それ以上のアクションを実行しません。
- CSSMに直接接続されている製品インスタンスは、信頼の同期を実行します。信頼の同期には、次のものが含まれます。

  スタンバイまたはメンバーに信頼コードがまだインストールされていない場合は、信頼コードのインストール。

信頼コードがすでにインストールされている場合は、信頼の同期プロセスにより、新しいスタンバイまたはメンバーがアクティブと同じスマートアカウントおよびバーチャルアカウントにあることが保証されます。そうでない場合、新しいスタンバイまたはメンバーは、アクティブと同じスマートアカウントとバーチャルアカウントに移動されます。

承認コード、ポリシー、および購入情報のインストール（該当する場合）

現在の使用状況情報を含む RUM レポートの送信。

アップグレードとダウングレード

以前のライセンスモデルから、ポリシーを使用したスマートライセンシングをサポートするソフトウェアイメージにアップグレードした後は、ポリシーを使用したスマートライセンシングが唯一のサポートされるライセンスモデルであり、製品インスタンスはライセンスの変更なしで動作し続けます。ただし、ライセンスワークフローのすべての側面が期待どおりに機能し続けるように、他の設定が必要な場合があります。このセクションでは、そのような変更の概要について説明します。

（注） ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードまたは移行するには、『Early Field Trial Guide』を参照してください。

アップグレードが既存ライセンスの適用タイプに与える影響

ポリシーを使用したスマートライセンシングをサポートするソフトウェアバージョンにアップグレードする場合、既存の PLR、SLR、CSL、PAK、および RTU ライセンスの処理方法は、適用タイプによって異なります。

- アップグレード前に使用されていた不適用ライセンスは、アップグレード後も引き続き使用できます。
- アップグレード前に使用されていた適用ライセンスは、必要な承認が存在する場合、アップグレード後も引き続き使用できます。これは、アップグレード時にシステムによって認証されます。必要な承認が存在しない場合は、使用する前に SLAC をインストールする必要があります。SLAC の手動要求と自動インストールを参照してください。
- アップグレード前に使用されていた輸出規制ライセンスは、必要な承認が存在する場合、一般にはアップグレード後も引き続き使用できます。

  ただし、例外があります。製品インスタンスが輸出規制フラグを持つスマートアカウントに登録されているために HSECK9 ライセンスを持っている場合、ポリシーを使用してスマートライセンシングにアップグレードした後に、SLAC をインストールする必要があります。

  対照的に、後述する例のように、以前のスマートライセンシング環境の輸出規制ライセンスでは、アップグレード後に SLAC を再インストールする必要はありません。アップグレード前に製品インスタンスに HSECK9 PAK ライセンスがあった場合、または製品イン

スタンスに HSECK9 ライセンスを含む SLR 承認コードがあった場合は、ポリシーを使用したスマートライセンシングへのアップグレード後にライセンスが適用されます。SLAC を再度インストールする必要はありません。

アップグレードが既存ライセンスのレポートに与える影響

使用権（RTU）レポート：レポートの要件はライセンスによって異なります。詳細については、適用されるポリシーを参照してください。また、**show license usage** コマンドの `Next ACK deadline` フィールドを参照して、レポートが必要かどうかを確認することもできます。

特定ライセンス予約（SLR）レポート：既存の SLR 承認コードは、ポリシーを使用したスマートライセンシングへのアップグレード後に既存のライセンス消費を承認します。したがって、ライセンス消費に変更がある場合は、レポートが必要です。

製品承認キー（PAK）レポート：PAK ライセンスには永続的な有効期間（ライセンス期間）がありますが、ライセンス消費に変更がある場合はレポートが必要です。

永続ライセンス予約（PLR）レポート：PLR ライセンスには永続的な有効期間があり、ライセンス消費に変更がある場合でもレポートは必要ありません。

Cisco ソフトウェアライセンシング（CSL）レポート：CSL ライセンスには永続的な有効期間があり、ライセンス消費に変更がある場合でもレポートは必要ありません。

アップグレードが既存ライセンスの転送タイプに与える影響

既存の設定で転送タイプが設定されている場合、ポリシーを使用したスマートライセンシングへのアップグレード後も転送タイプが保持されます。

スマートライセンシングの以前のバージョンと比較した場合、ポリシーを使用したスマートライセンシングでは追加の転送タイプを使用できます。デフォルトの転送モードにも変更があります。次の表に、これがアップグレードに与える影響を示します。

アップグレード前の転送タイプ	アップグレード前のライセンスまたはライセンスの状態	アップグレード後の転送タイプ
デフォルト（callhome）	評価	cslu（ポリシーを使用したスマートライセンシングのデフォルト）
	SLR PLR	off
	登録	callhome
smart	評価	smart
	SLR PLR	smart
	登録	smart

アップグレードがトークン登録プロセスに与える影響

以前のバージョンのスマートライセンシングでは、CSSMへの登録と接続にトークンが使用されていました。ID トークンの登録は、ポリシーを使用したスマートライセンシングでは必要ありません。トークン生成機能はCSSMでも引き続き使用でき、該当するトポロジの信頼の確立に使用されます。

インサービス ソフトウェア アップグレード

あるリリースから別のリリースにアップグレードする場合、ISSU 方式を使用することで、適用（エンフォースメント）、レポート、および転送の面では通常のアップグレードと同じルールに従います（上記を参照）。

ポリシーを使用したスマートライセンシングに関する追加の考慮事項は適用されません。

ダウングレード

ダウングレードするには、製品インスタンスのソフトウェアバージョンをダウングレードする必要があります。このセクションでは、新規展開のダウングレードについてのみ説明します。

新規展開のダウングレード

ポリシーを使用したスマートライセンシングがデフォルトですでに有効になっているソフトウェアバージョンで新しく購入した製品インスタンスがあり、ポリシーを使用したスマートライセンシングがサポートされていないソフトウェアバージョンにダウングレードする場合、ダウングレードの結果は、ポリシーを使用したスマートライセンシング環境での操作中に 信頼コード （5 ページ） がインストールされたかどうかによって異なります。

ポリシーを使用したスマートライセンシング環境で実装したトポロジが「CSSMに直接接続」である場合、トポロジ実装の一部として信頼コードが必要であるため、信頼コードのインストールが想定または仮定されます。他のトポロジでは、信頼の確立は必須ではありません。したがって、これらの他のトポロジのいずれかを使用する製品インスタンスをダウングレードすると、スマートライセンシング環境で適用される手順に従って、ライセンスを登録済みおよび承認済みの状態に復元する必要があります。

- ポリシーを使用したスマートライセンシング環境で信頼が確立された場合、製品インスタンスはダウングレード後に CSSM との信頼を更新しようとします。

  更新が正常に完了すると、ライセンスは登録済みの状態になり、以前のバージョンのスマートライセンシングが製品インスタンスで有効になります。

- ポリシーを使用したスマートライセンシング環境で信頼が確立されなかった場合、製品インスタンスのライセンスはダウングレード後に評価モードになり、スマートライセンシングの以前のバージョンが製品インスタンスで有効になります。