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 （1 ページ）
- サポート対象製品 （2 ページ）
- アーキテクチャ （4 ページ）
- 概念 （9 ページ）
- サポートされるトポロジ （16 ページ）
- 他の機能との相互作用 （33 ページ）
- 従来のライセンスの変更点 （41 ページ）

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。

- ライセンスの購入または注文：既存の流通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。

  後払いライセンスを注文することもできます。CSSM で各ライセンスを確認することもできます。ライセンスはサブスクリプション ID とともにリストされます。

（注） 新しいハードウェアまたはソフトウェアの注文の場合、シスコは、次のアイテムを工場でインストールすることで、Smart Licensing Using Policy の実装を簡素化します（用語については、以下の「概念 （9 ページ）」の項で説明します）。

- カスタムポリシー（使用可能な場合）
- 承認コード（該当する場合のみ）この場合、注文時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入力する必要があります。
- CSSM に送信されるデータの信頼性を保証する信頼コード。これは、Cisco IOS XE cupertino 17.7.1a 以降でインストールされます。この信頼コードは、CSSMとの通信には使用できません。

- 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）を使用し、使用状況情報をCSSMに直接報告し、コントローラ（Cisco DNA CenterやCisco vManageなど）を使用し、Smart Software Manager オンプレミス（SSM オンプレミス）を展開して製品とライセンスをオンプレミスで管理できます。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）。これは、後払いライセンスを使用する場合に適用され、使用量に応じて請求されます。

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 *1*: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	サポートが導入されたときの導入リリース
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 IOS XE Amsterdam 17.3.2
	Cisco 4000 シリーズ サービス統合型ルータ	Cisco IOS XE Amsterdam 17.3.2
	Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	Cisco IOS XE Amsterdam 17.3.2
	Cisco クラウド サービス ルータ 1000v （CSRv.bin イメージから Catalyst 8000V ソフトウェアイメージにアップグレードする必要があります）。	Cisco IOS XE Bengaluru 17.4.1
	シスコサービス統合型仮想ルータ （ISRv.bin イメージから Catalyst 8000V ソフトウェアイメージにアップグレードする必要があります）。	Cisco IOS XE Bengaluru 17.4.1
Cisco Catalyst 8000 エッジ プラットフォーム ファミリ		
	Catalyst 8200 シリーズ エッジ プラットフォーム	Cisco IOS XE Bengaluru 17.4.1
	Catalyst 8300 シリーズ エッジ プラットフォーム	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8500 シリーズ エッジ プラットフォーム	Cisco IOS XE Amsterdam 17.3.2
	Catalyst 8000V エッジソフトウェア	Cisco IOS XE Bengaluru 17.4.1
Cisco ターミナル サービス ゲートウェイ		
	Cisco 1100 ターミナル サービス ゲートウェイ	Cisco IOS XE Bengaluru 17.4.1

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 （2 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 （16 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。
- 仮想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[1]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。
- Cisco DNA Center などのコントローラに（シスコが）組み込みます。
- Linux を実行しているマシン（ラップトップまたはデスクトップ）に CSLU を導入します。

CSLU は、Windows 10 および Linux オペレーティングシステムをサポートします。利用可能な最新バージョンの CSLU を常に使用することをお勧めします。リリースノートおよび最新バージョンをダウンロードするには、[Software Download] ページの [Smart Licensing Utility]https://software.cisco.com/download/home/286285506/type をクリックします。

（注） CSLU は Cisco SD-WAN（Cisco vManage）ではサポートされておらず、CSLU を使用して Cisco vManage によって管理されるルーティング製品インスタンスのライセンス使用状況を報告することはできません。

コントローラ

複数の製品インスタンスを管理する管理アプリケーションまたはサービス。

[1] 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。

サポートされているコントローラ、コントローラをサポートする製品インスタンス、およびコントローラと製品インスタンスで必要な最小ソフトウェアバージョンに関する情報を次の表に示します。

- コントローラのサポート情報：Cisco DNA Center
- コントローラのサポート情報：Cisco vManage

表 *2:* コントローラのサポート情報：*Cisco DNA Center*

Smart Licensing Using Policy へ移行するために必要な **Cisco DNA Center** の最小バージョン[2]	**Cisco IOS XE** に必要な最小バージョン[3]	サポート対象製品インスタンス
Cisco DNA Center リリース 2.2.2	Cisco IOS XE Amsterdam 17.3.2	Cisco アグリゲーションルータ、統合型ルータ、およびクラウドサービスルータ： • Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ • Cisco 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 Catalyst 8000 エッジ プラットフォーム ファミリ： • 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
	Cisco IOS XE Bengaluru 17.4.1	Cisco Catalyst 8000 エッジ プラットフォーム ファミリ： • Catalyst 8200 シリーズ エッジ プラットフォーム Cisco ターミナル サービス ゲートウェイ： • Cisco 1100 ターミナル サービス ゲートウェイ

[2] このコントローラに必要な最小バージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

[3] 製品インスタンスの Cisco IOS-XE に必要な最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

Cisco DNA Center の詳細については、https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/series.html でサポートページを参照してください。

表 3 : コントローラのサポート情報 : *Cisco vManage*

Smart Licensing Using Policy へ移行するために必要な Cisco vManage の最小バージョン[4]	Cisco IOS XE に必要な最小バージョン[5]	サポート対象製品インスタンス
Cisco vManage リリース 20.5.1	Cisco IOS XE Bengaluru 17.5.1a	サポート対象製品インスタンスの最新リストについては、Cisco SD-WAN スタートアップガイド →「License Management for Smart Licensing Using Policy」→「Supported Devices」を参照してください。

[4] このコントローラに必要な最小バージョン。これは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

[5] 製品インスタンスの Cisco IOS-XE に必要な最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

Cisco vManage の詳細については、https://www.cisco.com/c/en/us/support/routers/sd-wan/series.html でサポートページを参照してください。

サポートされているコントローラでトポロジを実装する方法については、コントローラを介して CSSM に接続 （21 ページ）を参照してください。

SSM オンプレミス

Smart Software Manager オンプレミス（SSM オンプレミス）は、CSSM と連動するアセットマネージャです。これにより、CSSMに直接接続する代わりに、オンプレミスで製品とライセンスを管理できます。

SSM オンプレミスで Smart Licensing Using Policy を実装するために必要なソフトウェアバージョンについては、次を参照してください。

Smart Licensing Using Policy に必要な SSM オンプレミスの最小バージョン[6]	Cisco IOS XE に必要な最小バージョン[7]	サポート対象製品インスタンス
バージョン 8、リリース 202102	Cisco IOS XE Amsterdam 17.3.3	すべての サポート対象製品（2 ページ）

[6] 必要なSSMオンプレミスの最小バージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。
[7] 製品インスタンスに必要な最小ソフトウェアのバージョンこれは、特に明記されていない限り、後続のすべてのリリースでサポートが継続されることを意味します。

MSLA による Smart Licensing Using Policy に必要な最小 SSM オンプレミスバージョン	MSLA による Smart Licensing Using Policy に必要な最小 Cisco IOS XE バージョン	サポート対象製品インスタンス
バージョン 8、リリース 202206	Cisco IOS XE Cupertino 17.9.1	Catalyst 8000V エッジソフトウェア 詳細については、MSLA （8 ページ）を参照してください。

SSM オンプレミスの詳細については、ソフトウェアダウンロードページの Smart Software Manager On-Prem [英語] を参照してください。ドキュメントリンクを表示するには、.isoイメージにカーソルを合わせます。

MSLA

マネージド サービス ライセンス契約（MSLA）は、ネットワーク内の製品インスタンスで使用するライセンスについてシスコと締結する契約です。この契約により、ライセンスの使用状況をシスコに報告し、使用するライセンスを前払いする代わりに、ライセンスの使用量に対して請求されることになります。契約条件の詳細については、https://www.cisco.com/c/en/us/about/legal/msla-direct-product-terms.htmlを参照してください。

MSLA を使用すると、Cisco commerce workspace（CCW）でサブスクリプション ID 付きのライセンスを注文できます。ライセンスは、対応するサブスクリプション ID とともに、CSSM の指定されたスマートアカウントおよびバーチャルアカウントに保管されます。

MSLA による Smart Licensing Using Policy に必要な最小 Cisco IOS XE バージョン	サポート対象製品インスタンス
Cisco IOS XE Cupertino 17.9.1	自律モードで実行されている Catalyst 8000V エッジソフトウェアのみ。

（注） この MSLA は、製品インスタンスが Cisco vManage によって管理される SD-WAN コントローラモードで実行されている製品インスタンスで利用可能な MSLA とは異なります。

サブスクリプション ID を持つライセンスを使用する製品インスタンスも、「ユーティリティモード」で有効にする必要があります。その後、製品インスタンスは、すべてのライセンスワークフローを完了するために、CSSM と直接、または CSLU や SSM オンプレミスを介して相互作用するように構成するか、切断モードで動作するように構成できます。

このような製品インスタンスでサポートされるトポロジの詳細については、「ユーティリティモード」を参照してください。

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 4 : SLAC を必要とするライセンス （10 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 *4: 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

上記のライセンススループットに加えて、250 Mbps（Tier 2 以上）を超えるライセンスには SLAC が必要です。

表 *5 : SLAC* を必要とするスループットレベル

製品インスタンス	**SLAC** を必要とするスループットレベル	その他の考慮事項
Cisco 4000 シリーズ サービス統合型ルータ Cisco 1100 ターミナル サービス ゲートウェイ	250 Mbps を超える暗号化されたスループット	製品インスタンスに次のいずれかがすでに含まれている場合は、SLACを再度インストールする必要はありません。 • HSECK9 ライセンス用の SLAC • HSECK9 PAK ライセンス • HSECK9 ライセンスを含む SLR 承認コード
Cisco 1000 シリーズ サービス統合型ルータ Catalyst 8200 シリーズ エッジ プラットフォーム 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 Catalyst 8000V エッジソフトウェア	250 Mbps を超える暗号化されたスループット	
Catalyst 8000V エッジソフトウェア （Cisco IOS XE Bengaluru 17.4.1 の Catalyst 8000V ソフトウェア イメージが必要とされる Cisco Cloud Services Router 1000v および Cisco Integrated Services Virtual Router にも適用されます）	250 Mbps を超える暗号化および非暗号化スループット（合計）	

（注） 以前のライセンスモデルから Smart Licensing Using Policy にアップグレードする場合、いずれかのライセンスを所有している可能性があり、各ライセンスには固有の承認コードである特定のライセンス予約（SLR）、製品アクティベーションキー（PAK）、パーマネントライセンス予約（PLR）があります。

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サポートされるようになります。

PAK 履行済みライセンスを所有している場合は、PAK ライセンスのスナップショット （47 ページ）を参照して必要なタスクを完了し、PAK 履行済みライセンスを引き続き使用してください。

パーマネントライセンス予約（PLR）承認コードを所有していて、引き続き使用する場合は、Smart Licensing Using Policy 環境のパーマネントライセンス予約 （50 ページ）を参照してください。

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。

  この値がゼロの場合、最初のレポートは必要ありません。
- Reporting frequency (days)：次の RUM 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。

  ここの値がゼロの場合、使用状況が変更されない限り、以降のレポートは必要ありません。
- 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。

  ここの値がゼロの場合、使用状況の変更時のレポートは必要ありません。

  ここの値がゼロでない場合は、変更を加えた後にレポートが必要です。次に示すすべてのシナリオは、製品インスタンスのライセンス使用状況における変更としてカウントされます。

  - 消費されたライセンスの変更（別のライセンスへの変更やライセンスの追加または削除を含む）。

- ライセンスの消費なしから 1 つ以上のライセンスの消費への移行。
- 1 つ以上のライセンスの消費からライセンスの消費なしへの移行。

（注） 製品インスタンスがライセンスを使用していない場合、ポリシーのレポート要件（最初のレポート要件、レポート頻度、変更に関するレポート）のいずれかにゼロ以外の値が設定されていても、レポートは必要ありません。

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 6 : ポリシー：Cisco default （13 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 *6 :* 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[8]	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

[8] 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のライセンス使用状況レポートです。RUM レポートは製品インスタンスによって生成され、CSSMによって使用されます。製品インスタンスは、ライセンス使用状況情報とすべてのライセンス使用状況の変更を、開いている RUM レポートに記録します。システムが決定した間隔で、開いている RUM レポートが閉じられ、新しい RUM レポートが開かれて、ライセンスの使用状況の記録が継続されます。閉じられた RUM レポートは、いつでも CSSM に送信できます。

RUM 確認応答（RUM ACK または 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。レポートの ACK が製品インスタンスで使用可能になると、対応する RUM レポートが不要になり、削除できることが示されます。

レポート方式、つまり CSSM への RUM レポートの送信方法は、実装するトポロジによって異なります。

CSSM は、最後に受信した RUM レポートに従ってライセンス使用状況情報を表示します。

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。

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

- 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 レポートの生成、保存、管理

Cisco IOS XE Cupertino 17.7.1 以降、RUM レポートの生成と関連プロセスが次のように最適化および強化されました。

- 製品インスタンスで使用可能なすべての RUM レポートのリストを表示できます（レポートの数、それぞれの処理状態、エラーがあるかどうかなど）。この情報は、show license rum、show license all、show license tech 特権 EXEC コマンドで入手できます。
- RUM レポートは、処理時間を短縮し、メモリ使用量を削減する新しい形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、次の状況では、トポロジに適用される方法で RUM レポートを送信することをお勧めします。

  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以前のリリースから、Cisco IOS XE Cupertino 17.7.1 以降のリリースにアップグレードする場合。

  Cisco IOS XE Cupertino 17.7.1 以降のリリースから、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以前のリリースにダウングレードする場合。
- 継続的なディスク領域とメモリの可用性を確保するために、製品インスタンスは、対象と見なされる RUM レポートの削除を検出してトリガーします。

信頼コード

製品インスタンスが使用する *UDI* に関連付けられた公開キー

- RUM レポートに署名します。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。
- CSSM でセキュア通信を有効化します。

信頼コードを取得する方法は複数あります。

- Cisco IOS XE cupertino 17.7.1a 以降は、すべての新規注文に対して工場出荷時に信頼コードがインストールされています。

（注） 出荷時にインストールされた信頼コードは、CSSM との通信には使用できません。

- 信頼コードは、IDM トークンを使用して CSSM から取得できます。

  ここでは SSM Web UI で *ID* トークンを生成して信頼コードを入手して製品インスタンスにインストールする必要があります。出荷時にインストールされた信頼コードがある場合は、上書きする必要があります。製品インスタンスが CSSM に直接接続されている場合は、この方法を使用して、製品インスタンスが CSSM と安全に通信できるようにします。信頼コードを取得するこの方法は、CSSM に直接接続するすべてのオプションに適用できます。詳細については、CSSM に直接接続 （18 ページ）を参照してください。

- Cisco IOS XE Cupertino 17.7.1 以降では、信頼コードは、製品インスタンスが CSLU へのデータ送信を開始するトポロジと、製品インスタンスがエアギャップネットワーク内にあるトポロジで自動的に取得されます。

  Cisco IOS XE Cupertino 17.9.1a 以降、CSLU が製品インスタンスのデータの取得を開始するトポロジでは、信頼コードが自動的に取得されます。

  出荷時にインストールされた信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM とのセキュアな通信に使用できます。

  対応するトポロジの説明と対応するワークフローを参照して、各シナリオにおける信頼コードの要求およびインストール方法を確認してください。サポートされるトポロジ（16 ページ）

信頼コードが製品インスタンスにインストールされている場合、**show license status** コマンドの出力の [Trust Code Installed] フィールドに更新されたタイムスタンプが表示されます。例：`Trust Code Installed: 2020 年 10 月 9 日 17 時 56 分 19 秒 (UTC)`

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。ワークフローにより、トポロジを実装する最も簡単で迅速な方法が提供されます。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。

（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：

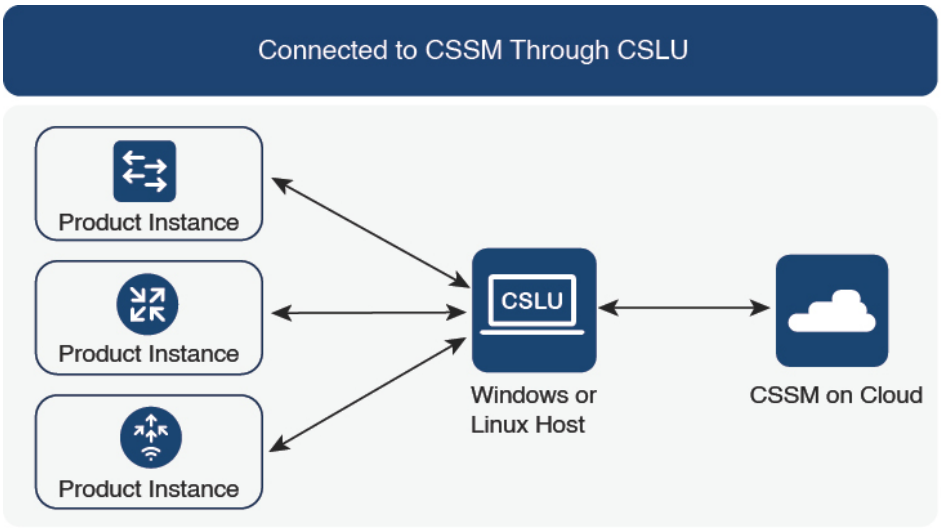
ここでは、ネットワーク内の製品インスタンスは CSLU に接続され、CSLU は CSSM との単一のインターフェイスポイントになります。製品インスタンスは、必要な情報を CSLU にプッ

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、UDI に関連付けられた信頼コード、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、UDI に関連付けられた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。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1a 以降：

- 信頼コードの要求とインストール

  信頼コードが製品インスタンスで使用できない場合、製品インスタンスは RUM レポートの一部として、信頼コードの要求を検出し、自動的に要求を含めます。CSSM からの対応する ACK には信頼コードが含まれています。出荷時にインストールされた既存の信頼コー

ドがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM との通信に使用できます。

これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。

このリリースでは、この拡張は、製品インスタンス開始モードにのみ適用されます。

Cisco IOS XE Cupertino 17.9.1a 以降：

- 信頼コードの要求とインストール

  このリリースから、信頼コードの要求とインストールはCSLU開始モードでもサポートされています。

- Virtual Routing and Forwarding（VRF）のサポート

  すべてのライセンスデータを送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。また、このトポロジを実装する場合は、製品インスタンス開始モードを実装する必要があります。

- RUM レポートスロットリング

  製品インスタンス開始モードでは、レポートの最小頻度は 1 日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

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ID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。

（注） 出荷時にインストールされた信頼コードは、CSSMとの通信には使用できません。つまり、このトポロジでは、CSSM Web UI で *ID* トークンを生成して、信頼コードを入手して製品インスタンスにインストールする必要があります。出荷時にインストールされた信頼コードがある場合は、上書きする必要があります。信頼コード （15 ページ）も参照してください。

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。

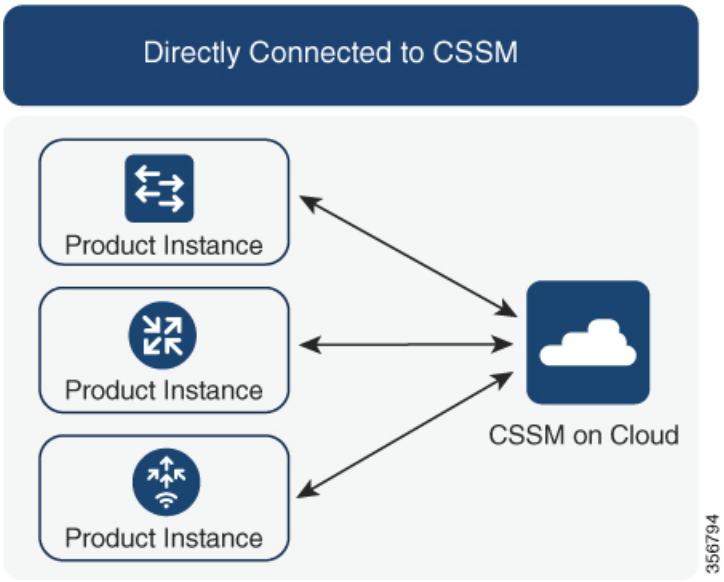
  - スマート転送：この方法では、製品インスタンスは特定のスマート転送ライセンスサーバ URL を使用します。これは、ワークフローのセクションに示すとおりに設定する必要があります。
  - HTTPS プロキシを介したスマート転送：この方法では、製品インスタンスはプロキシサーバを使用してライセンスサーバと通信し、最終的には CSSM と通信します。

- 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。

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。

（注） Call Home からスマート転送方式に変更する場合、Smart Licensing Using Policy を期待どおりに機能させるために「CiscoTAC-1」Call Home プロファイルを無効化する必要はありません。

  - 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。

- ユーティリティモード（17.9.1.a 以降で使用可能）で動作しているときにこのトポロジを実装する場合は、スマート転送のみを使用できます。つまり、スマート転送を直接使用す

るか、HTTP プロキシを介したスマート転送を使用します。Call Home はユーティリティモードではサポートされていません。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.9.1a 以降：

- Virtual Routing and Forwarding（VRF）のサポート

  すべてのライセンスデータを送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があり、このトポロジを実装する場合は、スマート転送オプションのみを使用できます。つまり、スマート転送を直接使用するか、HTTP プロキシを介したスマート転送を使用します。

- RUM レポートスロットリング

  このトポロジでは、レポートの最小頻度は 1 日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

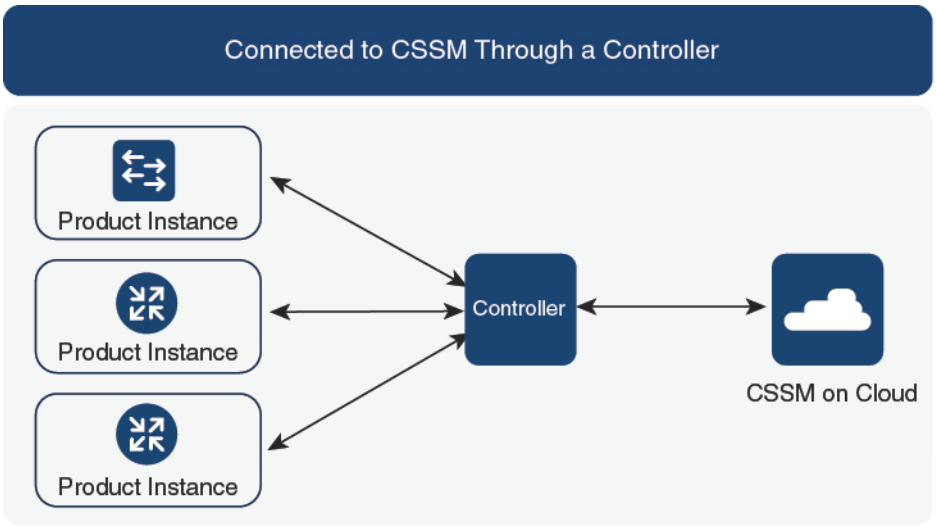
次の手順：

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に直接接続を参照してください。

コントローラを介して CSSM に接続

コントローラを使用して製品インスタンスを管理する場合、コントローラはCSSMに接続してCSSM とのすべての通信のインターフェイスとなります。

図 *3:* トポロジ：コントローラを介して *CSSM* に接続



Cisco アグリゲーションルータ、統合型ルータ、およびクラウドサービスルータ、Cisco Catalyst 8000 エッジプラットフォームファミリ、および Cisco ターミナル サービス ゲートウェイでは、Cisco DNA Center と Cisco vManage がコントローラとしてサポートされています。実装するコントローラに応じて、トポロジがどのように動作するように設計されているかについては、次の対応する項を参照してください。

コントローラとしての Cisco DNA Center

概要：

Cisco DNA Center がコントローラとして製品インスタンスを管理している場合、製品インスタンスはライセンスの使用状況を記録し、保存しますが、Cisco DNA Center が RUM レポートを取得し、CSSM に報告し、製品インスタンスにインストールするために ACK を返すために製品インスタンスとの通信を開始します。

Cisco DNA Center で管理する必要があるすべての製品インスタンスは、そのインベントリの一部である必要があり、サイトに割り当てる必要があります。Cisco DNA Center は NETCONF プロトコルを使用して設定をプロビジョニングし、製品インスタンスから必要な情報を取得します。したがって、これを容易にするために製品インスタンスで NETCONF を有効にする必要があります。

レポートの要件を満たすために、Cisco DNA Center は CSSM から該当するポリシーを取得し、次のレポートオプションを提供します。

- Ad hoc reporting：必要に応じてアドホックレポートをトリガーできます。
- Scheduled reporting：ポリシーで指定されたレポート頻度に対応し、Cisco DNA Center によって自動的に処理されます。

（注） 製品インスタンスが定期レポートの対象となる前に、アドホックレポートを少なくとも1回実行する必要があります。

最初のアドホックレポートにより、Cisco DNA Center は、後続の RUM レポートをアップロードする必要があるスマートアカウントとバーチャルアカウントを決定できます。製品インスタンスのアドホックレポートが一度も実行されていない場合は、通知されます。

Cisco DNA Center では、SLAC のインストールと削除ができます。SLAC のインストールと削除は、単一の製品インスタンスでも、複数の製品インスタンスでも実行できます。

（注） Cisco DNA Center の GUI には、輸出規制ライセンス（HSECK9）と特定の製品インスタンスに対してのみ、SLAC を生成するオプションがあります。表 1を参照してください。

信頼コードは必要ありません。

考慮事項または推奨事項：

これは、Cisco DNA Center を使用している場合に推奨されるトポロジです。

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：コントローラを介してCSSMに接続のコントローラとしての Cisco DNA Center の使用を参照してください。

コントローラとしての Cisco vManage

概要：

Cisco vManage をコントローラとして使用して製品インスタンスを管理する場合、Cisco vManage は CSSM に接続して CSSM とのすべての通信のインターフェイスとなります。

Cisco vManage はライセンスの使用状況を記録し、RUM レポートを生成し、24 時間ごとに RUM レポートを CSSM に送信します。 この時間はポリシーによって決定される固定のレポート間隔であり、変更できません。CSSM から返された RUM ACK も Cisco vManage に送信されます。

製品インスタンスが Cisco vManage によって管理されている場合、製品インスタンスではライセンス使用状況情報の保存や RUM レポートの生成は行われません。

Cisco vManage ポータルでは、エッジデバイスにライセンスを割り当て、使用されているライセンスおよび割り当てに使用可能なライセンスに関する情報を確認できます。

（注） Cisco vManage ポータルには、SLAC のインストールオプションはありません。輸出規制ライセンスまたは250 Mbpsを超えるスループットを使用するには、製品インスタンスで必要なCLIコマンドを使用してSLACを要求してインストールするか、CSSMからファイルをダウンロードして製品インスタンスに同様にインストールする必要があります。

以前のライセンス環境の HSECK9 ライセンスを使用している場合は、ポリシーを使用したスマートライセンシングへの移行後に同じライセンスがサポートされます。この場合、SLAC を再度インストールする必要はありません。

SLAC のインストールの詳細については、「コントローラとしての Cisco vManage の使用」を参照してください。

Cisco vManage でライセンス管理を処理する方法の詳細については、Cisco SD-WAN スタートアップガイドの「License Management for Smart Licensing Using Policy」セクションを参照してください。

考慮事項または推奨事項：

これは、Cisco vManage を使用している場合に推奨されるトポロジです。

Cisco IOS XE Bengaluru 17.5.1a 以降：Cisco SD-WAN は CSSM と連携して動作し、Cisco SD-WAN で動作するデバイスに対して Cisco vManage によるライセンス管理を提供します。

Cisco IOS XE Amsterdam 17.3.2 ー Cisco IOS XE Bengaluru 17.4.x：Cisco vManage はコントローラとしてサポートされていますが、ライセンス管理はサポートしていません。Cisco SD-WAN コントローラモードで実行されているエッジデバイスは、HSECK9 ライセンスの処理を除き、ポリシーを使用したスマートライセンシングの他の機能をサポートしていません。

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：コントローラを介して CSSM に接続の「コントローラとしての Cisco vManage の使用」を参照してください。

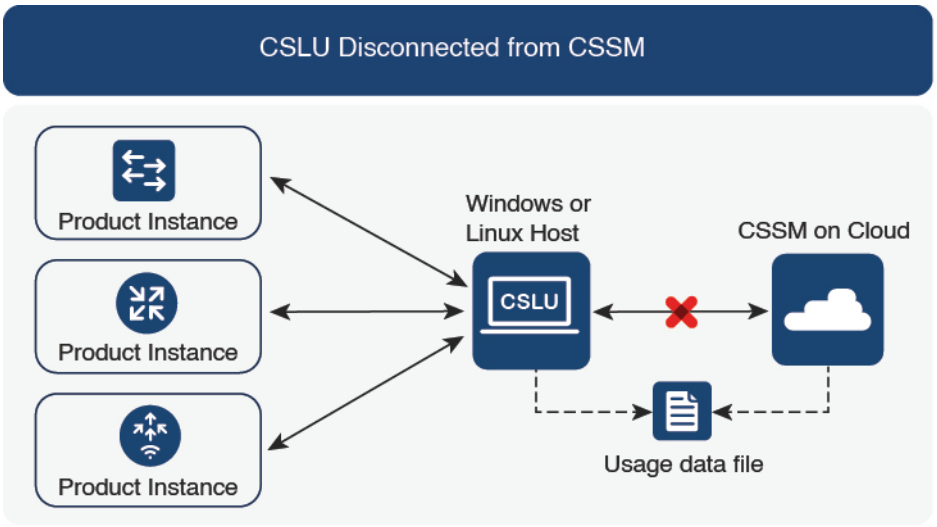
CSLU は CSSM から切断

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 *4 :* トポロジ：*CSLU* は *CSSM* から切断



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。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1a 以降：

- 信頼コードの要求とインストール

  信頼コードが製品インスタンスで使用できない場合、製品インスタンスは、CSLU に送信される RUM レポートの一部として要求を検出し、自動的にその要求を含めます。この要求は、CSSM にアップロードされます。CSSM からダウンロードする ACK には信頼コードが含まれています。出荷時にインストールされた既存の信頼コードがある場合は、自動的に上書きされます。この方法で取得した信頼コードは、CSSM との通信に使用できます。

  これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないメンバーやスタンバイの信頼コードを要求します。

  このリリースでは、この拡張は、製品インスタンス開始モードにのみ適用されます。

Cisco IOS XE Cupertino 17.9.1a 以降：

- 信頼コードの要求とインストール

  このリリースから、信頼コードの要求とインストールはCSLU開始モードでもサポートされています。

- Virtual Routing and Forwarding（VRF）のサポート

  すべてのライセンスデータを CSLU に送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。また、このトポロジを実装する場合は、製品インスタンス開始モードを実装する必要があります。

- RUM レポートスロットリング

  製品インスタンス開始モードでは、レポートの最小頻度は 1 日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

次の手順：

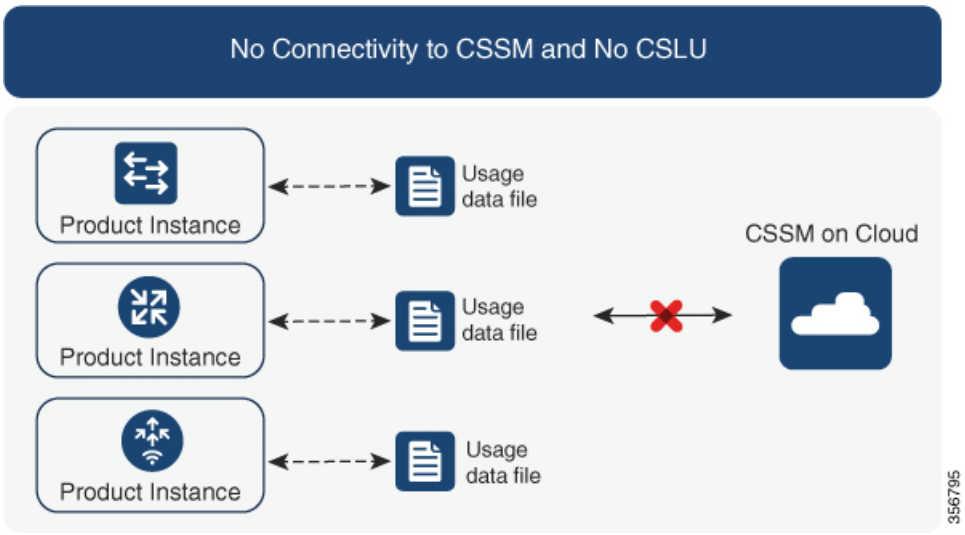
このトポロジを実装するには、トポロジのワークフロー：CSLU は CSSM から切断を参照してください。

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。これらのファイルは、RUM レポート、UDI に関連付けられた信頼コードの要求、および SLAC 要求ファイルです。

図 *5:* 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。

リリースごとの変更と拡張

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの変更と拡張について概説します。

Cisco IOS XE Cupertino 17.7.1a 以降：

- 信頼コードの要求とインストール

  製品インスタンスで信頼コードが使用できない場合、製品インスタンスは、ユーザーが保存し、CSSM にアップロードする RUM レポートに信頼コードの要求を自動的に含めます。CSSM からダウンロードする ACK には信頼コードが含まれています。

  出荷時にインストールされた信頼コードがある場合、ACK をインストールすると自動的に上書きされます。この方法で取得した信頼コードは、CSSM とのセキュアな通信に使用できます。

  これは、スタンドアロンおよび高可用性設定でサポートされます。高可用性設定では、アクティブな製品インスタンスは、信頼コードが使用できないすべての接続製品インスタンスの信頼コードを要求します。

- SLAC 要求とインストール

  SLAC 要求を生成し、製品インスタンスのファイルに保存できます。保存されたファイルには、必要なすべての詳細（UDI、ライセンス情報など）が含まれます。この方法では、SLAC を生成するために CSSM Web UI で必要な詳細情報を収集して入力する必要はありません。RUM レポートおよび ACK と同様に、SLAC 要求ファイルを CSSM にアップロー

ドし、SLAC コードを含むファイルをダウンロードして製品インスタンスにインストールする必要があります。

同様に、SLAC を返却する場合、正しいバーチャルアカウントの製品インスタンスを見つける必要はありません。RUM レポートと同様に、SLAC 返却ファイルをアップロードします。

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：CSSM への接続なし、CSLU なしを参照してください。

SSM オンプレミス展開

概要：

SSM オンプレミスは、オンプレミスに展開される CSSM の拡張として機能するように設計されています。

ここでは、製品インスタンスが SSM オンプレミスに接続され、SSM オンプレミスが CSSM との単一のインターフェイスポイントになります。SSM オンプレミスの各インスタンスは、SSM オンプレミスのローカルアカウントに必須の登録と同期を通じて、CSSM 内のバーチャルアカウントを使用して CSSM に通知する必要があります。

製品インスタンスを管理するために SSM オンプレミスを展開する場合、SSM オンプレミスに必要な情報をプッシュするように製品インスタンスを設定できます。または、設定可能な頻度で製品インスタンスから必要な情報をプルするように SSM オンプレミス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 SSM オンプレミスの REST エンドポイントを接続することで SSM オンプレミス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。

  このモードでの製品インスタンスと SSM オンプレミス間の通信のオプション：

  - 必要に応じて、CLI コマンドを使用して SSM オンプレミスに情報をプッシュします。
  - スケジュールされた頻度で RUM レポートを SSM オンプレミスに自動的に送信するには、CLI コマンドを使用し、レポート間隔を設定します。

- SSM オンプレミス開始型通信（プル）：製品インスタンスからの情報の取得を開始するには、SSM オンプレミスで NETCONF、RESTCONF、およびネイティブの REST API オプションを使用して製品インスタンスを接続します。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。

  このモードでの製品インスタンスと SSM オンプレミス間の通信のオプション：

- 必要に応じて（オンデマンドで）、1 つ以上の製品インスタンスから使用状況情報を収集します。
- スケジュールされた頻度で 1 つ以上の製品インスタンスから使用状況情報を収集します。

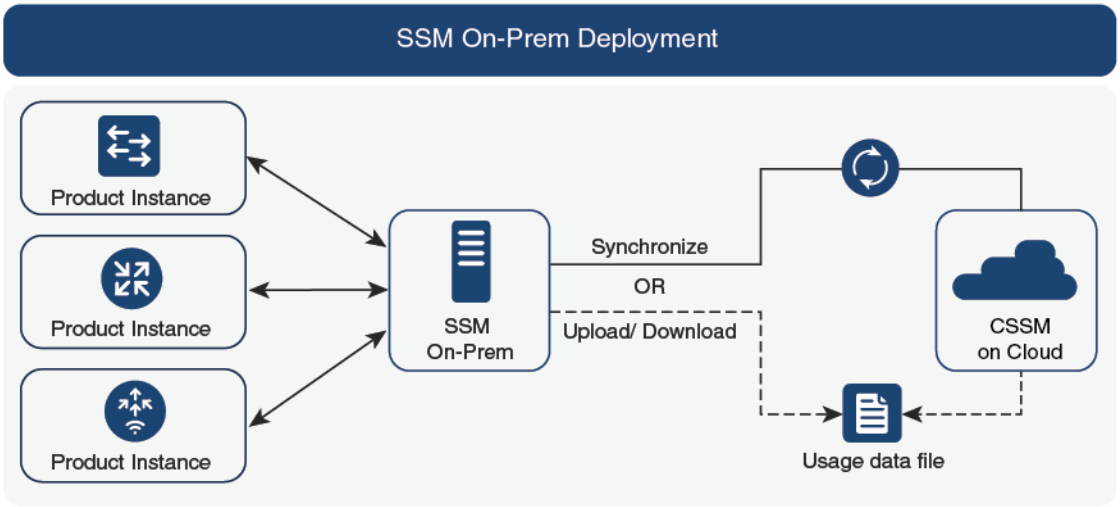
SSM オンプレミスでは、レポート間隔が製品インスタンスのデフォルトポリシーに設定されます。これは変更できますが、より頻繁に（より短い間隔で）レポートを作成するか、または使用可能な場合はカスタムポリシーをインストールできます。

SSM オンプレミスで使用状況が使用できるようになったら、同じ間隔で CSSM と同期して、製品インスタンス数、ライセンス数、およびライセンス使用状況情報が CSSM と SSM オンプレミスの両方と同じであることを確認します。SSM オンプレミスと CSSM 間の使用状況の同期オプション：プッシュとプルモードの場合：

- CSSM でアドホック同期を実行します（Cisco と同期されました）。
- 指定した時刻で CSSM との同期をスケジュールします。
- オフラインで保存されている指名済みファイルを通じて CSSM と通信し、場合によって SSM オンプレミスまたは CSSM からアップロードするか、またはダウンロードします。

（注） このトポロジでは、SSM オンプレミスと CSSM 間で 2 つの異なる同期が行われます。1 つは、ローカルアカウントと CSSM との同期です。この同期は、SSM オンプレミスインスタンスに CSSM を認識させるためであり、SSM オンプレミスの [Synchronization] ウィジェットを使用して実行します。2 番目は、CSSM に接続するか、またはファイルをダウンロードおよびアップロードすることのいずれかによるライセンスの使用状況の CSSM との同期です。ライセンスの使用状況を同期する前に、ローカルアカウントを同期する必要があります。

図 *6 :* トポロジ：*SSM* オンプレミス展開



考慮事項または推奨事項：

- このトポロジは、次の状況に適しています。
  - CSSM と直接通信せずにオンプレミスで製品インスタンスを管理する場合。
  - 会社のポリシーにより、製品インスタンスでライセンスの使用状況をシスコ（CSSM）に直接報告できない場合。
  - 製品インスタンスがエアギャップネットワーク内にあり、ネットワーク外にあるものとオンラインで通信できない場合。
- Smart Licensing Using Policy のサポートとは別に、SSM オンプレミスのバージョン 8 の主な利点は次のとおりです。
  - マルチテナント：1 つのテナントが 1 つのスマートアカウントとバーチャルアカウントのペアを構成します。SSM オンプレミスでは複数のペアを管理できます。ここでは、SSM オンプレミスに存在するローカルアカウントを作成します。CSSM のスマートアカウントとバーチャルアカウントのペアへの複数のローカルアカウントのロールアップ。詳細については、『Cisco Smart Software Manager On-Prem User Guide』[英語]の「About Accounts and Local Virtual Accounts」を参照してください。

（注） CSSM と SSM オンプレミスのインスタンス間の関係は、まだ 1 対 1 です。

  - スケール：合計 300,000 の製品インスタンスをサポートします。
  - 高可用性：2 台の SSM オンプレミスサーバをアクティブ/スタンバイクラスタの形式で実行できます。詳細については、『Cisco Smart Software On-Prem Installation Guide』[英語] の「Appendix 4 Managing a High Availability (HA) Cluster in Your System」を参照してください。

    高可用性展開は SSM オンプレミスのコンソールでサポートされており、必要なコマンドの詳細については『Cisco Smart Software On-Prem Console Guide』で確認できます。
  - CSSM へのオンライン接続とオフライン接続のオプション。
- SSM オンプレミスの制限：
  - ライセンス使用の同期を目的とした CSSM との通信のプロキシサポートが利用できるのは、バージョン 8 202108 以降のみです。ローカルアカウントの同期を目的とするプロキシの使用はサポートされています。これは [Synchronization] ウィジェットを使用して実行され、Smart Licensing Using Policy がサポートされている SSM オンプレミス導入リリースから利用可能です。
  - SSM オンプレミス開始型通信は、ネットワークアドレス変換（NAT）設定の製品インスタンスではサポートされていません。製品インスタンス開始型通信を使用する必要があります。さらに、NAT 設定の製品インスタンスをサポートするために SSM オ

ンプレミスを有効にする必要があります。詳細は、このトポロジのワークフローで提供されます。

リリースごとの変更と拡張：

このセクションでは、このトポロジに影響するリリースごとのソフトウェアの重要な変更と拡張について概説します。

Cisco IOS XE Cupertino 17.9.1a 以降：

- Virtual Routing and Forwarding（VRF）のサポート

  すべてのライセンスデータを CSLU に送信するように VRF を設定できます。そのため、製品インスタンスは VRF をサポートするインスタンスである必要があります。また、このトポロジを実装する場合は、製品インスタンス開始モードを実装する必要があります。

- RUM レポートスロットリング

  製品インスタンス開始モードでは、レポートの最小頻度は1日に制限されます。これは、製品インスタンスが 1 日に複数の RUM レポートを送信しないことを意味します。これにより、特定のライセンスに対して生成および送信される RUM レポートが多すぎるという問題が解決されます。また、RUM レポートの過剰な生成によって引き起こされたメモリ関連の問題とシステムのスローダウンも解決します。

  特権 EXEC モードで **license smart sync** コマンドを入力すると、スロットリングの制限をオーバーライドできます。

  RUM レポートスロットリングは、17.3.x トレインの Cisco IOS XE Amsterdam 17.3.6 以降のリリース、および 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.4 以降のリリースにも適用されます。17.9.1 以降、RUM レポートスロットリングは後続のすべてのリリースに適用されます。

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：SSM オンプレミス展開を参照してください。

SSM オンプレミスの既存のバージョンから移行する場合は、アップグレード関連のさまざまなアクティビティを実行する順序が重要です。Smart Licensing Using Policy をサポートする SSM オンプレミスのバージョンへの移行を参照してください。

ユーティリティモード

概要：

これは、必要なライセンスの前払いではなく、ライセンスの実際の使用量に対して支払う後払いモデルであり、MSLA によって管理されます。

製品インスタンスはサブスクリプションIDを持つライセンスを使用し、「ユーティリティモード」で有効になっています。製品インスタンスは、すべてのライセンスワークフローを完了するために、CSSM と直接、または CSLU や SSM オンプレミスを介して相互作用するように構成するか、切断モードで動作するように構成できます。製品インスタンスとの通信には、ユーティリティモードで動作していることを示すフラグが設定されます。MSLA の使用量が CSSM に達すると、使用量に応じて課金されます。

ユーティリティモードの製品インスタンスでは、30 日ごとに ACK をインストールする必要があります。レポートをタイムリーに作成するために、レポートの間隔は7日以内にすることを推奨します。

ユーティリティモードで実装できるトポロジは次のとおりです。

- CSSM に直接接続 （18 ページ）

  ユーティリティモードでこのトポロジを実装する場合は、スマート転送のみを使用できます。つまり、スマート転送を直接使用するか、HTTP プロキシを介したスマート転送を使用します。

- CSLU を介して CSSM に接続 （16 ページ）、CSLU は CSSM から切断 （24 ページ）
- SSM オンプレミス展開 （28 ページ）
- CSSM への接続なし、CSLU なし （26 ページ）

考慮事項または推奨事項：

- CCW でプリペイドライセンスを注文する場合、後払いの HSECK9 ライセンスは注文できません。このライセンスはプリペイドライセンスのみです。
- サードパーティの課金プラットフォームに使用状況レポートを送信することはできません。使用できるサポートされている代替手段は、CSLU または SSM オンプレミスを実装することです。実装すると CSSM に送信されます。
- CSLU または SSM オンプレミスを実装する予定の場合は、Smart Licensing Using Policy 環境に、MSLA 対応の必要な最小バージョンをインストールしてください。
  - CSLU の場合：バージョン 2.0.0
  - SSM オンプレミスの場合：バージョン 8、リリース 202206

次の手順：

サポートされるトポロジの 1 つを実装します。

（注） ワークフローのステップはすべて、特に明記されていない限り、ユーティリティモードに適用されます。

トポロジのワークフロー：CSSM に直接接続

トポロジのワークフロー：CSLU を介して CSSM に接続
トポロジのワークフロー：CSLU は CSSM から切断
トポロジのワークフロー：CSSM への接続なし、CSLU なし
トポロジのワークフロー：SSM オンプレミス展開

他の機能との相互作用

ハイ アベイラビリティ

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

デュアルシャーシ セットアップ[9]（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[10]。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。

（注） Cisco vManage を使用して製品インスタンスを管理する場合、すべてのデバイスにライセンスが必要です。 高可用性はサポートされていません。

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。
- 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。
- デバイススタックの場合は、アクティブな場合のみ承認コードが必要です。

[9] 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。
[10] 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。

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。

上記のいずれかのイベントが発生すると、**show license status** 特権EXECコマンドの [Next report push] の日付が更新されます。ただし、レポートが製品インスタンスによって送信されるかどうかは、実装されたトポロジと関連するレポート方法で決まります。たとえば、製品インスタンスが切断されているトポロジ（[Transport Type] が [Off]）を実装した場合は、[Next report push] の日付が更新されても、製品インスタンスは RUM レポートを送信しません。

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

このセクションでは、次の点について説明します。

- 以前のライセンスモデルから Smart Licensing Using Policy への移行

  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。このポリシーを使用したスマートライセンシングへの移行 セクションでは、移行シナリオの例を示します。

- Smart Licensing Using Policy 環境でのアップグレード：アップグレード元のソフトウェアバージョンとアップグレード先のソフトウェアバージョンの両方で、Smart Licensing Using Policy がサポートされます。

アップグレード前に現在のライセンシングモデルを識別する

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前に、製品インスタンスで有効な現在のライセンスモデルを確認するには、特権 EXEC モードで show license all コマンドを入力します。このコマンドにより、RTU ライセンスモデルを除くすべてのライセンスモデルに関する情報が表示されます。show license right-to-use 特権 EXEC コマンドでは、ライセンスモデルが RTU の場合にのみライセンス情報が表示されます。

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。

PAK ライセンスを使用している場合は、システムによる PAK ライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、PAK ライセンスのスナップショット （47 ページ）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、一般的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。アップグレード前に、製品インスタンスがスマートアカウントに登録されており、CSSM には 250 Mbps を超えるスループットが許可されるように輸出規制フラグのみが有効になっていて、輸出規制ライセンス（HSECK9）が有効になっていない場合は、Smart Licensing Using Policy への移行の一部として、さらにいくつかの手順を実行する必要があります。これは、米国の輸出規制により、250 Mbps を超えるスループットを許可する方法として輸出規制フラグのみの使用が許可されなくなったためです。

  - 仮想製品インスタンス（Cisco Cloud Services Router 1000v（CSR 1000v）または Cisco Integrated Services Virtual Router（ISRv））でスループットが 250 Mbps を超え、CSSM で輸出規制フラグのみが有効になっている場合は、設定の要件に従って手順を進めます。

    - SLR 設定のスループットが 250 Mbps を超える CSR 1000v または ISRv：最初に SLR 承認コードを更新して、該当する HSECK9 ライセンスを含めてから、製品インスタンスのみをアップグレードします。これにより、アップグレード後もスループットが中断されなくなります。

（注） このシナリオでは、最初に SLR 承認コードを更新せずにソフトウェアイメージをアップグレードして HSEK9 ライセンスを含めると、Smart Licensing Using Policy へのアップグレード後は、SLAC がインストールされるまで、スループットが 250 Mbps に設定されます。SLAC のインストール後すぐに、最後に設定した値が復元されます。

      製品固有の HSECK9 ライセンスの名前については、ルーティング製品インスタンスの HSECK9 ライセンス マッピング テーブルを参照してください。移行シナリオ例については、例：スマートライセンス（スループットが 250 Mbps を超える SLR、輸出規制ライセンスなし）から Smart Licensing Using Policy へを参照してください。

    - CSSM に接続され、自律モードのスループットが 250 Mbps を超える CSR 1000v またはISRv：250 Mbpsを超えるスループットがスタートアップ コンフィギュレーションの一部であることを確認します。また、CSSM 内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で該当する HSECK9 ライセンスのバランスがプラスであることも確認します。アップグレード前のアクションは必要ありません。

製品インスタンスがCSSMに接続されている限り、アップグレード時に製品インスタンスは自動的にHSECK9要求をトリガーし、SLACをインストールします。

- スループットが250 Mbpsを超え、CSSMに輸出規制フラグのみが設定されており、CSSMに接続されている自立モードの物理製品インスタンス（Cisco 1000シリーズサービス統合型ルータ（ISR 1000）、Cisco 4000シリーズサービス統合型ルータ（ISR 4000）、またはCisco 1000シリーズアグリゲーションサービスルータ（ASR 1000））の場合：**license feature hseck9** コマンドがスタートアップコンフィギュレーションに設定されており、CSSM内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で該当するHSECK9ライセンスのバランスがプラスであることを確認します。アップグレード前のアクションは必要ありません。アップグレード時に製品インスタンスがCSSMに接続されている限り、製品インスタンスは自動的にHSECK9要求をトリガーし、SLACをインストールします。
- 物理製品インスタンスまたは仮想製品インスタンスの場合、CSSMで輸出規制フラグのみを使用して250 Mbpsを超えるスループットがあり、SD-WANコントローラモードで動作している場合：アップグレード後にSLACを要求してインストールする必要があります。アップグレードが完了したら、CSSMからのSLACの生成とファイルへのダウンロードを実行し、次に製品インスタンスへのファイルのインストールを実行します。

対照的に、輸出規制ライセンスが以前のライセンス環境にある次のシナリオでは、アップグレード後にSLACを再度インストールする必要がないことに注意してください。

- 製品インスタンス（Cisco 1000シリーズサービス統合型ルータやCisco 4000シリーズサービス統合型ルータなど）に、スマートアカウントに登録されたHSECK9ライセンスがあり、CSSMで輸出規制フラグが有効になっている場合、ポリシーを使用したスマートライセンシングにアップグレード後に、承認コードが適用されます。ライセンス使用状況情報は、アップグレード後にのみCSSMと同期する必要があります。SLACを再度インストールする必要はありません。例：スマートライセンス（登録済みおよび承認済みのライセンス）から Smart Licensing Using Policy へを参照してください。
- アップグレード前に製品インスタンスにHSECK9 PAKライセンスが存在した場合、アップグレード後にSLACを再度インストールする必要はありません。例：Cisco ソフトウェアライセンシング（PAK ライセンス）から Smart Licensing Using Policy へを参照してください。

  PAKライセンスを使用している場合は、システムによるPAKライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、PAKライセンスのスナップショット （47ページ）を参照してください。
- 製品インスタンスにHSECK9ライセンスを含むSLR承認コードが含まれていた場合、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後にライセンスが適用されるため、SLACを再度インストールする必要はありません。例：スマートライセンス（輸入規制ライセンスを使用した SLR）から Smart Licensing Using Policy へ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レポートに与える影響

既存ライセンス	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のレポート要件
使用権（RTU）	使用されているライセンスによって異なります。 サポートされるトポロジの移行および展開後、**show license usage** コマンドの出力で `Next ACK deadline` フィールドを参照して、レポートが必要かどうか、およびいつ必要かを確認します。
スマートライセンシング（登録および承認済みライセンス）	ポリシーによって異なります。
特定のライセンス予約（SLR）	ライセンス消費に変更がある場合にのみ必要です。 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。
製品認証キー（PAK）	ライセンス消費に変更がある場合にのみ必要です。 PAK ライセンスには永続的な有効期間がありますが、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。 また、システムによる PAK ライセンスの処理方法の変更と、使用可能なオプションをよく理解してください。詳細については、PAK ライセンスのスナップショット （47 ページ）を参照してください。
パーマネントライセンス予約（PLR）	不要。 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）	不要。 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。
評価ライセンスまたは期限切れライセンス	シスコのデフォルトポリシーのレポート要件に基づいています。

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	off
	SLR PLR	off
	登録	smart
N/A たとえば、既存のライセンスモデルが RTU または PAK の場合。	N/A たとえば、既存のライセンスモデルが RTU または PAK の場合。	cslu

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、Smart Licensing Using Policy では不要です。トークン生成機能は、CSSM で引き続き使用でき、Smart Licensing Using Policy 環境の特定のトポロジで信頼を確立するために使用されます。

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。

Smart Licensing Using Policy 環境内のアップグレード

この項では、Smart Licensing Using Policy がサポートされているリリースから Smart Licensing Using Policy がサポートされているリリースに製品インスタンスをアップグレードする場合に適用される、リリース固有の考慮事項またはアクションについて説明します。

Cisco IOS XE Cupertino 17.7.1a 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、Smart Licensing Using Policy をサポートする以前のリリースから Cisco IOS XE Cupertino 17.7.1a 以降のリリースにアップグレードする場合は、標準的な方法として1回の使用状況レポートを完了することをお勧めします。

ダウングレード

ここでは、以前のライセンスモデルへのダウングレードについて説明します。また、Smart Licensing Using Policy 環境内のダウングレードに関連する情報についても説明します。

新規展開のダウングレード

このセクションでは、Smart Licensing Using Policy がデフォルトで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、Smart Licensing Using Policy 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された場合に適用される考慮事項とアクションについて説明します。

ダウングレードの結果は、Smart Licensing Using Policy 環境での操作中に信頼コード（信頼コード （15 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。ダウングレード先のリリースによっては、さらにアクションが必要になる場合があります。

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。そのため、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生じます。次の表を参照してください。

- 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。

Smart Licensing Using Policy 環境内のダウングレード

この項では、Smart Licensing Using Policy がサポートされているリリースから Smart Licensing Using Policy がサポートされている別のリリースに製品インスタンスをダウングレードする場合に適用される、リリース固有の考慮事項またはアクションについて説明します。

Cisco IOS XE Cupertino 17.7.1a 以降、RUM レポートは処理時間を短縮する形式で保存されます。古い形式と新しい形式の違いによって生じる使用状況レポートの不整合を避けるために、Cisco IOS XE Cupertino 17.7.1a 以降のリリースから Smart Licensing Using Policy をサポートする

以前のリリースにダウングレードする際に、1 回の使用状況報告を完了することをお勧めします。

従来のライセンスの変更点

ここでは、Smart Licensing Using Policy 環境で引き続きサポートされるために、特定の従来のライセンスで実施されている変更について説明します。変更には、自動的に実行されるアクション、ユーザーが実行する必要があるアクション、または両方のアクションが含まれる場合があり、適宜呼び出されます。

デバイスに固有の HSECK9 ライセンスの段階的廃止

HSECK9 ライセンスは、さまざまな Cisco アグリゲーション、サービス統合型、およびクラウドサービスルータでサポートされています。Cisco 1000 シリーズ サービス統合型ルータと Cisco 4000 シリーズ サービス統合型ルータでは、ライセンス名はルータモデルに従ってタグ付けされます（たとえば、HSECK9 ライセンスを使用している Cisco 4461 サービス統合型ルータでは「ISR_4400_Hsec」を使用します）。

このセクションでは、このようなデバイスに固有の HSECK9 ライセンスの変更点、その変更がユーザーに与える影響、取らなければならない可能性があるアクション（ある場合）、デバイスに固有の HSECK9 ライセンスの所有者が使用できるオプションについて説明します。

デバイスに固有の HSECK9 ライセンスのリストについては、「ルーティング製品インスタンスの HSECK9 ライセンス マッピング テーブル」を参照してください。

デバイスに固有の HSECK9 ライセンスの変更点

Cisco 1000 シリーズ サービス統合型ルータと Cisco 4000 シリーズ サービス統合型ルータで使用可能なデバイスに固有の HSECK9 ライセンスは、HSECK9 ライセンスの管理を簡素化するために段階的に廃止されます。

Cisco IOS XE Bengaluru 17.6.1a 以降、HSECK9 ライセンスは、（ISR_4331_Hsec などの）ルータモデルに応じてタグ付けされるのではなく、Router US Export Lic for DNA（DNA_HSEC）としてタグ付けされます。これらの製品の新しい HSECK9 ライセンスを購入する場合は、DNA_HSEC を購入する必要があります。

製品インスタンスで実行されているソフトウェアバージョンが Cisco IOS XE Bengaluru 17.6.1a 以降の場合は、次のような影響があります。

- すでに使用中のデバイスに固有の HSECK9 ライセンスは引き続きサポートされるため、これ以上のアクションは必要ありません。
- CSSM のスマートアカウントとバーチャルアカウントで未使用のデバイスに固有の HSECK9 ライセンスは、引き続き製品インスタンスで使用できます。複数のオプションが用意されており、適切なオプションで続行できます。詳細については、以下の「HSECK9 ライセンスで使用可能なオプション」セクションを参照してください。

HSECK9 ライセンスの注文の詳細については、「HSECK9 ライセンスの注文情報」を参照してください。

この変更の影響を受ける製品インスタンス

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

HSECK9 ライセンスで使用可能なオプション

次の表に、未使用のデバイスに固有の HSECK9 ライセンスの所有者として使用可能なオプションに関する情報を示します。また、アクションは必要ないものの、説明や確認のために提供されている追加のシナリオについても説明します。

以下の表で使用されている重要な用語と略語の説明と定義：

- デバイスに固有の HSECK9 ライセンス：デバイスモデルにタグ付けされた HSECK9 ライセンス名を指します。
- DNA_HSEC：Router US Export Lic for DNA
- オナー（HSECK9 ライセンス）：HSECK9 形式が製品インスタンスに存在する場合、HSECK9 または輸出規制対象の機能を使用できることを意味します。ただし、その形式で新しい HSECK9 ライセンスをインストールすることはできません。
- SLP：ポリシーを使用したスマートライセンシング
- SL：スマートライセンス
- PAK：製品アクティベーションキー

表 *7 : HSECK9* ライセンスで使用可能なオプション

現在の状態	CSSM の HSECK9 権限タイプ	製品インスタンスの現在のソフトウェアバージョン	結果と必要なアクション（該当する場合）
製品インスタンスが HSECK9 ライセンスを使用していない。	デバイスに固有の HSECK9 ライセンス	Cisco IOS XE Bengaluru 17.6.1a 以降	HSECK9 ライセンスを使用する場合は、次のいずれかのオプションを選択します。 • **オプション 1** : デバイスに固有の HSECK9 ライセンスの SLAC をオフラインモードでインストールします。 「CSSM からの SLAC の生成とファイルへのダウンロード」と「製品インスタンスへのファイルのインストール」の手順を実行します。 • **オプション 2** : CCW から DNA-HSEC-UPGD= を無料で入手し、デバイスに固有の HSECK9 ライセンスを DNA_HSEC に変換して DNA_HSEC を使用するための SLAC をインストールします。 「デバイスに固有の HSECK9 ライセンスの変換」の手順を実行し、導入したトポロジに従って DNA_HSEC の SLAC をインストールします。 • **オプション 3** : 1. 17.3.x ～ 17.5.x の任意のリリースにダウングレードします。 2. 導入したトポロジに従ってデバイスに固有の HSECK9 ライセンスの SLAC をインストールします。 3. Cisco IOS XE Bengaluru 17.6.1a 以降のリリースに戻します。

現在の状態	CSSM の HSECK9 権限タイプ	製品インスタンスの現在のソフトウェアバージョン	結果と必要なアクション（該当する場合）
製品インスタンスが HSECK9 ライセンスを使用していない。	DNA_HSEC	Cisco IOS XE Bengaluru 17.6.1a 以降	HSECK9 ライセンスを使用する場合は、導入したトポロジに従って DNA_HSEC の SLAC をインストールします。
製品インスタンスが HSECK9 ライセンスを使用していない。	デバイスに固有の HSECK9 ライセンス	Cisco IOS XE Amsterdam 17.3.2 ～ Cisco IOS XE Bengaluru 17.5.x の任意のリリース	HSECK9 ライセンスを使用する場合は、導入したトポロジに従ってデバイスに固有の HSECK9 ライセンスの SLAC をインストールします。
製品インスタンスが HSECK9 PAK ライセンスか HSECK9 ライセンスを含む SLR 承認コードを使用している。	デバイスに固有の HSECK9 ライセンス または DNA_HSEC	Cisco IOS XE Amsterdam 17.3.1 以前のリリース	Cisco IOS XE Amsterdam 17.3.2 以降のリリースにアップグレードする場合、これ以上のアクションは必要ありません。 Device-Led Conversion（DLC）がアップグレード時に自動的にトリガーされ、HSECK9 PAK ライセンスか HSECK9 ライセンスを含む SLR 承認コードが適用されます。
製品インスタンスが HSECK9 ライセンスを使用している。	デバイスに固有の HSECK9 ライセンス または DNA_HSEC	17.3.x トレインの Cisco IOS XE Amsterdam 17.3.4 以降のリリース（17.3.4 以上）。 または 17.4.x トレインの Cisco IOS XE Bengaluru 17.4.2 以降のリリース（17.4.2 以上）。 または Cisco IOS XE Bengaluru 17.5.x（17.5.x）	これ以上のアクションは必要ありません。 使用されている HSECK9 ライセンスが適用されます。

現在の状態	CSSM の HSECK9 権限タイプ	製品インスタンスの現在のソフトウェアバージョン	結果と必要なアクション（該当する場合）
製品インスタンスが HSECK9 ライセンスを使用していない。	DNA_HSEC	17.3.4 以上、17.4.2 以上、または 17.5.x	DNA_HSEC が CSSM の権限タイプである場合、それは CCW でソフトウェアバージョン 17.6.1a 以降のデバイスが注文されたことを意味します。 さらに、DNA_HSEC とハードウェアが同時に購入された場合、SLAC は出荷時にインストールされます。インストールされていない場合は、次のいずれかの方法で SLAC をインストールしてください（いずれかのオプションを選択します）。 • **オプション 1**：DNA_HSEC ライセンスの SLAC をオフラインモードでインストールします。 「CSSM からの SLAC の生成とファイルへのダウンロード」と「製品インスタンスへのファイルのインストール」の手順を実行します。 • **オプション 2**： 1. Cisco IOS XE Bengaluru 17.6.1a 以降のリリースにアップグレードします。 2. 導入したトポロジに従って DNA_HSEC の SLAC をインストールします。 3. 必要なリリースに戻します（ダウングレードします）。

現在の状態	CSSM の HSECK9 権限タイプ	製品インスタンスの現在のソフトウェアバージョン	結果と必要なアクション（該当する場合）
SLAC がインストールされているかどうかわからない。	DNA_HSEC	Cisco IOS XE Everest 16.10.1a ～ Cisco IOS XE Amsterdam 17.3.1	（注） オプションとして使用できますが、関連するリリースのソフトウェアメンテナンスが終了しているため、この変換は推奨されません。 DNA_HSEC ライセンスをデバイスに固有の HSECK9 ライセンスに変換する場合は、次のプロセスを実行します。 **1.** 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。 ダウングレードの理由を記載し、既存の HSEC ライセンスの購入証明書を提示します。 **2.** サポートチームから連絡があり、デバイスに固有の HSECK9 スペア（ISR4330 の場合は FL-4330-HSEC-K9= など）の発注書を 100% 割引で作成するよう求められます。 **3.** サポートチームが発注書と同じ数の DNA_HSEC ライセンスを取り消します。また、割引の内部承認を求めるといった要求の処理も行います。承認されると注文が処理されます。 **4.** CSSM のスマートアカウントとバーチャルアカウントに該当する数のデバイスに固有の HSECK9 ライセンスが保管されます。

現在の状態	CSSM の HSECK9 権限タイプ	製品インスタンスの現在のソフトウェアバージョン	結果と必要なアクション（該当する場合）
SLAC がインストールされているかどうかわからない。	デバイスに固有の HSECK9 ライセンス	Cisco IOS XE Fuji 16.9.x	（注） オプションとして使用できますが、関連するリリースのソフトウェアメンテナンスが終了しているため、この変換は推奨されません。 デバイスに固有の HSECK9 ライセンスを PAK HSECK9 ライセンスに変換する場合は、ケースをオープンします。 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。 サポート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。

表 *8 : HSECK9* ライセンスが使用されるライセンスモデルとリリースマトリックス

リリース	リリースで使用可能なライセンスモデル	PAK HSECK9 のサポート	HSECK ト
16.9 以下	PAK	対応	N/A
16.10.1a ～ 17.3.1	SL	オナー	対応
17.3.2 ～ 17.3.3、17.4.1	SLP	オナー	オナー
17.3.4 以上、17.4.2 以上、17.5.x	SLP	オナー	オナー
17.6.1a 以上	SLP	オナー	オナー

PAK ライセンスのスナップショット

システムの製品アクティベーションキー（PAK）ライセンスの処理方法は大幅に変更されています。ここでは、変更内容、変更がユーザーに与える影響、実行する必要があるアクション（ある場合）、および PAK ライセンス所有者が利用できるオプションについて説明します。

PAK ライセンスとは

PAK フルフィルメントを使用して発行されるライセンスは、PAK ライセンスと呼ばれます。たとえば、Cisco ASR 1000 で使用可能な「adventerprise」ライセンスは PAK 履行済みにすることができ、Cisco 4000 シリーズ ISR で使用できる「securityk9」ライセンスも PAK 履行済みにできます。同様に、さまざまなシスコルータで利用可能な HSECK9 ライセンスは、PAK 履行済みにできます。

PAK ライセンスの変更点：PAK ライセンスのスナップショット

Cisco IOS XE Dublin 17.11.1a 以降、PAK ライセンスを管理するライブラリはソフトウェアイメージから削除されています。既存の PAK ライセンスを引き続きサポートおよび受け入れるために、次のアクションが自動的に実行されます。

- PAK ライセンスのスナップショットが作成されます。このスナップショットは、スナップショットの時点における PAK ライセンスの永続的な記録として機能します。
- Device-Led Conversion（DLC）プロセスがトリガーされます。DLC 後、PAK 履行済みライセンスをスマートアカウントで使用できます。

製品インスタンスで実行されているソフトウェアバージョンが次のいずれかである場合にのみ、PAK ライセンスのスナップショットが作成されます。

- 17.3.x トレインの Cisco IOS XE Amsterdam 17.3.5 以降のリリース。
- 17.6.x トレインの Cisco IOS XE Bengaluru 17.6.2 以降のリリース。
- 17.7.x トレインの Cisco IOS XE Cupertino 17.7.1 以降のリリース、および後続のトレインのすべてのリリース、つまり Cisco IOS XE Cupertino 17.8.x、Cisco IOS XE Cupertino 17.9.x、および Cisco IOS XE Dublin 17.10.x まで。

⚠

注意 前述のリリースおよびトレイン以前の場合のみ、PAK ライセンスのスナップショットが作成されます。Cisco IOS XE Dublin 17.11.1a 以降、PAK 管理ライブラリは廃止され、スナップショットを作成するためのプロビジョニングは利用できなくなりました。Cisco IOS XE Dublin 17.11.1a 以降のソフトウェアイメージは、PAK ライセンスに関するスナップショット情報のみに依存しています。

スナップショットのない PAK ライセンスがあり、Cisco IOS XE Dublin 17.11.1a 以降のリリースにアップグレードする場合は、2 回アップグレードする必要があります。まず、PAK ライセンスのスナップショットと完全な DLC が作成される前述のリリースのいずれかにアップグレードしてから、必要な後続のリリースに再度アップグレードします。

PAK のパーマネントライセンスのみが受け入れられ、PAK の評価ライセンスは受け入れられません。

スナップショットが作成されると、PAK ライセンスへの変更はサポートされなくなります。スナップショットの作成後に、ソフトウェアバージョンを以前のリリースにダウングレードし、

PAK ライセンスに変更を加え（返却を含む）、後続のリリースに戻した場合でも、PAK ライセンスの変更はサポートされません。

製品インスタンスの PAK ライセンスのスナップショットが作成されているか確認するには、特権 EXEC モードで **show platform software sl-infra pak-info** コマンドを入力します。 スナップショットが作成されている場合、コマンドの出力に次の情報が表示されます。

```
Device# show platform software sl-infra pak-info
<output truncated>

Pak License Snapshot Information
================================
Platform Supports PAK License snapshot
PAK License Snapshot integrity check pass
PAK License Snapshot available

<output truncated>
```

PAK ライセンスをサポートする製品インスタンス

以下の製品インスタンスは PAK ライセンスをサポートしています。以下の製品インスタンスのいずれかを使用しており、製品インスタンスで PAK ライセンスが使用されている場合は、「PAK ライセンスで利用可能なオプション」を参照して、実行可能な内容の詳細を確認してください。

- 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 クラウド サービス ルータ 1000v
- Catalyst 8000V エッジソフトウェア（シスコ クラウド サービス ルータ 1000v であり、Cisco IOS XE Bengaluru 17.4.1 以降のリリースへの .bin アップグレードが実行されている場合のみ）

PAK ライセンスで利用可能なオプション

PAK ライセンスを所有している場合は、次の方法で続行できます。

（注） 製品インスタンスに複数の PAK ライセンスがある場合は、すべてのライセンスの使用を継続するか、すべてのライセンスを削除して返却します。所有している PAK ライセンスを変更する必要があると思う場合は、すべての PAK ライセンスを削除し、製品インスタンスでスマートライセンスを設定して、最初からやり直してください。

- PAK ライセンスがあり、変更を加えずに製品インスタンスで引き続き使用する場合は、PAK ライセンスの使用を継続するを参照してください。
- 製品インスタンスに PAK ライセンスがあり、そのライセンスを削除する場合は、PAK ライセンスの削除を参照してください。

- 障害が発生した製品インスタンスに PAK ライセンスがあり、ライセンスを返却または削除する場合は、障害が発生した製品インスタンスの PAK ライセンスの削除を参照してください。

Smart Licensing Using Policy 環境のパーマネントライセンス予約

パーマネントライセンス予約とは

パーマネントライセンス予約（PLR）を使用すると、製品インスタンスの任意のライセンスを無制限に使用できます。PLR コードは、CSSM によって生成される承認コードであり、ライセンス要求を認証するために製品インスタンスにインストールする必要があります。

PLR 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または完全なエアギャップネットワークに適しています。

Smart Licensing Using Policy 環境における PLR の要件

Smart Licensing Using Policy 環境で PLR を使用するためには、次のものが必要です。

- ソフトウェアバージョン：Cisco IOS XE Dublin 17.10.1a 以降。
- PLR コードのバージョン 3。

Smart Licensing Using Policy 環境で PLR をサポートする製品インスタンス

- Catalyst 8000V エッジソフトウェア
- シスコ クラウド サービス ルータ 1000v（CSRv イメージから Catalyst 8000V ソフトウェアイメージに .bin アップグレード済み）

既存の PLR の処理方法：アップグレードとダウングレード

現在のセットアップ	条件 （このアクションが実行された場合）	結果と影響
製品インスタンス：シスコ クラウド サービス ルータ 1000v PLR ステータス：PLR がアクティブ化されています。古いバージョン（バージョン 1 またはバージョン 2）の PLR コードがインストールされています。 ソフトウェアバージョン：Cisco IOS XE Everest 16.5.x から Cisco IOS XE Amsterdam 17.3.x。	ソフトウェアバージョン Cisco IOS XE Dublin 17.10.1a 以降のリリースへの .bin アップグレードを実行します。	250 Mbps を超えるスループットと、HSECK9 ライセンスが必要な輸出規制機能を除き、有効になっている既存の機能はすべて受け入れられ、引き続き機能します。 古いバージョンの PLR コードは製品インスタンスから削除されませんが、サポートされません。 スループットを復元し、HSECK9 ライセンスを使用するには、PLR コードをバージョン 3 にアップグレードします。PLR のアップグレードを参照してください。
製品インスタンス：シスコ クラウド サービス ルータ 1000v PLR ステータス：PLR がアクティブ化されています。古いバージョン（バージョン 1 またはバージョン 2）の PLR コードがインストールされています。 ソフトウェアバージョン：Cisco IOS XE Everest 16.5.x から Cisco IOS XE Amsterdam 17.3.x。	Cisco IOS XE Bengaluru 17.4.x と Cisco IOS XE Cupertino 17.9.x の間のリリースへの .bin アップグレードを実行します。	250 Mbps を超えるスループットと、HSECK9 ライセンスが必要な輸出規制機能を除き、有効になっている既存の機能はすべて受け入れられ、引き続き機能します。 古いバージョンの PLR コードは製品インスタンスから削除されませんが、サポートされません。 PLR を使用するには、ソフトウェアバージョンを Cisco IOS XE Dublin 17.10.1a にアップグレードしてから、PLR コードをバージョン 3 にアップグレードする必要があります。 PLR のアップグレードを参照してください。

現在のセットアップ	条件 （このアクションが実行された場合）	結果と影響
製品インスタンス：シスコ クラウド サービス ルータ 1000v ルータ（Catalyst 8000V ソフトウェアイメージに .bin アップグレード済み） PLR ステータス：PLR がアクティブ化されています。PLR コードのバージョン 3 がインストールされています。 ソフトウェアバージョン：Cisco IOS XE Dublin 17.10.1a 以降。	Cisco IOS XE Amsterdam 17.3.x 以前のリリースにダウングレードします。	ダウングレード後、古いバージョンのソフトウェアイメージで PLR コードバージョン 3 を検証できず、受け入れもサポートもできません。 製品インスタンスは、ライセンスがインストールされていないかのように動作します。 PLR コードは製品インスタンスから削除されません。
製品インスタンス：シスコ クラウド サービス ルータ 1000v ルータ（Catalyst 8000V ソフトウェアイメージに .bin アップグレード済み） PLR ステータス：PLR アップグレードは完了していません。古いバージョン（バージョン 1 またはバージョン 2）の PLR コードがインストールされています。 ソフトウェアバージョン：Cisco IOS XE Dublin 17.10.1a 以降。	Cisco IOS XE Amsterdam 17.3.x 以前のリリースにダウングレードします。	ダウングレード後、古いバージョンのソフトウェアイメージで PLR コードを検証し、コードを使用してライセンス要求を満たすことができます。

Smart Licensing Using Policy 環境での PLR のアクティブ化、アップグレード、非アクティブ化

- Catalyst 8000V エッジソフトウェアに PLR を実装する場合は、PLR のアクティブ化を参照してください。
- シスコ クラウド サービス ルータ 1000v ルータで .bin アップグレードを実行していて、PLR の使用を継続する場合は、PLR のアップグレードを参照してください。
- PLR を無効にする場合は、PLR の非アクティブ化を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。