Cisco Smart Licensing のセキュリティ

(2020 年 11 月更新)

目次

はじめに

お客様のソフトウェアライセンス管理を簡素化するために、シスコは柔軟なソフトウェア ライセンス モデルである Cisco® Smart Software Licensing を導入しました。このモデルは、お客様が組織全体のシスコ ソフトウェア ライセンスをアクティベートおよび管理する方法を合理化します。スマートライセンスでは、ソフトウェアライセンスの所有権と使用状況の詳細が可視化されるので、お客様は所有しているライセンスとその使用状況を把握できます。PAK の紛失や不明な PAK に悩まされる時代は終わりました。Cisco Smart Licensing は、組織全体で柔軟かつ自動的に使用できるライセンスまたはエンタイトルメントのプールを確立します。

さまざまなセキュリティ特性に合わせた各種導入オプション

Smart Licensing では、環境に必要なレベルのセキュリティを管理できます。シスコは、セキュリティに関しては「すべての組織に当てはまる」アプローチはないことを理解しているので、使用状況レポートには複数のオプションをご用意しています。お客様は、組織にとっての利便性や適合性の高さに基づいて、1 つの導入オプションを選択することも、複数のオプションを組み合わせることもできます。

（シスコでの）ダイレクトライセンス管理とレポーティング

最もシンプルな導入方法がダイレクトクラウドアクセスです。この方法では、インターネットまたは HTTP プロキシサーバーを介して、シスコ製品から使用状況に関する情報が直接送信されます。お使いのシスコ製品がインターネット経由で **Tools.cisco.com** に接続している場合は、このソリューションが最もシンプルです。追加の設定手順は不要で、「すぐに」利用を開始できます。

（オンプレミスでの）仲介型ライセンス管理とレポーティング

Cisco Smart Software Manager（SSM）オンプレミス ライセンス サーバーは、金融機関、公益事業、サービスプロバイダー、政府機関によって使用されている非常に人気の高いソリューションです。インフラストラクチャ デバイスに直接または HTTP プロキシサーバーを介したインターネット経由での接続を許可すると、セキュリティポリシーに違反する可能性がある場合は、オンプレミスのライセンス管理ソリューションが必要になります。

お客様またはパートナーは、無料のダウンロードを使用して Cisco SSM オンプレミス ライセンス サーバーを導入し、デバイスの通信をお客様のローカルネットワーク内に留めることができます。Cisco SMM オンプレミスサーバーは、「同期プロセス」を使用して Cisco Smart Software Manager（Cisco SSM）とライセンス情報を交換します。この情報は、ネットワークベースの自動転送またはオフラインの手動転送のいずれかによって交換できます。

非接続型（ライセンス予約方式）ライセンスの使用

非接続型の SSM オンプレミス ライセンス サーバーを利用しない（リモート導入やローハイサイド運用などの）完全なエアギャップ環境が必要な場合は、継続的な通信や追加のインフラストラクチャが不要のライセンス予約方式を使用すると効率性が高まります。約 30 台を超えるシスコデバイスを導入する場合は、ライセンスの変更と RMA プロセスを簡素化するために、この方式ではなく非接続型 SSM オンプレミス ライセンス サーバー導入モデルを推奨します。

最高レベルのセキュリティを確保するために、シスコはライセンス予約を通じた完全なオフラインアクセスを提供しています。この環境では、すべてのライセンスの変更が手動で処理されます。ライセンス予約では、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。この機能は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。

Smart Licensing Using Policy

Smart Licensing の新しい導入方法では、エンドカスタマーによるライセンスのアクティベートと管理が簡素化されます。Smart Licensing がよりシンプルかつ柔軟なオファー構造をサポートするようになったため、お客様はより簡単かつ迅速に、一貫した方法でライセンスを購入、更新、アップグレードできるようになりました。製品ポリシーに基づき、ソフトウェアの使用状況のレポートは必須ですが、デバイスごとの登録とシスコとの継続的な通信の条件は緩和されました。

オンラインの Cisco Smart Licensing

シスコは、個人データがどこから、どのように送信されてきたのかにかかわらず、個人データを尊重し保護することにより、お客様やパートナーの支援に努めています。また、義務付けられたプライバシーに関する法律を世界中で遵守しています。シスコは、セキュリティ、データ保護、プライバシーに関するプログラムを長年にわたって確立しています。これらのプログラムには、規制、お客様のニーズ、およびシスコ独自の企業行動規範を遵守するというコミットメントから派生した多くの要件がすでに含まれています。

シスコ オンライン プライバシー ステートメントの概要

シスコ オンライン プライバシー ステートメント（https://www.cisco.com/c/ja_jp/about/legal/privacy-full.html）と本概要は、このステートメントにリンクされているシスコと当社の関係会社の Web サイトに適用されます。シスコは、ユーザーの個人情報を尊重し、個人情報の保護に全力を尽くします。シスコのプライバシーステートメントは、個人情報の取り扱いに関して、データ使用の通知と選択、データアクセスと整合性、セキュリティ、転送と施行および監視について、現在のグローバル原則および基準を反映しています。

シスコのデータ保護プログラム

シスコはプライバシー保護の一環として、シスコのオファーの開発ライフサイクルの発案段階から設計と規定によるプライバシーの原則を取り入れることで、セキュリティ管理の強化を含めたプライバシー エンジニアリングに一層注力しています。

シスコのデータ保護プログラムは、データのライフサイクル全体を対象としています。まず、設計によるセキュリティとプライバシー、収集の管理、使用、処理、保管に取り組み、レポートと監視や、ライフサイクルの最後に行う安全な廃棄または破壊といった運用ニーズに対応します。

一般データ保護規制（GDPR）

EU の一般データ保護規制（GDPR）により、ヨーロッパでは以前より期待されていたデータ保護分野の一貫性がもたらされました。GDPR では、透明性、公平性、説明責任といったプライバシーの原則が明確に具体化されています。GDPR は、リスクベースのアプローチを採用することで、個人の権利を尊重しつつ、グローバルなデジタルエコノミーのイノベーションと発展を促します。

シスコは、EU-米国間およびスイス-米国間のプライバシーシールドに基づく承認を得ています。また、GDPR を完全に満たすポリシーにより、EU の拘束的企業準則の認定を取得しました。

世界中で合法的かつ安全にデータを転送

シスコはプライバシー保護の一環として、シスコのオファーの開発ライフサイクルの発案段階から設計と規定によるプライバシーの原則を取り入れることで、セキュリティ管理の強化を含めたプライバシー エンジニアリングに一層注力しています。

- **拘束的企業準則（BCR）：**シスコのデータ保護とプライバシーのポリシー、標準、および関連文書（「BCR-C」）は、欧州のデータ保護監督機関によって承認されています。
- **EU-米国間およびスイス-米国間のプライバシーシールド：**シスコは、EU-米国間およびスイス-米国間での個人データの収集、使用、処理、国境を越えた移転について米国商務省が定めた両方のフレームワークに基づく承認を得ています。（https://www.cisco.com/c/ja_jp/about/legal/privacy.html）
- **APEC 越境プライバシールールおよび PRP システム：**U.S. APEC Accountability Agent（米国の APEC 認証機関）は、シスコのグローバル プライバシー プログラムがアジア太平洋経済協力（APEC）の越境プライバシールール（CBPR）および個人データ処理者認定（PRP）システムに適合していることを認証しました。
- **EU モデル条項を使用するシスコのマスターデータ保護契約：**シスコとシスコのお客様それぞれが所有する個人データを必要に応じて世界中で転送できる自由を保護するために、シスコは、マスターデータ保護契約（MDPA）を利用できるようにしました。この契約をサプライヤに求め、お客様に提供します。

Smart Licensing のデータ共有

シスコは、IT 資産管理（ITAM）プラットフォームの ISO 19770 プロトコル仕様に緩やかに準拠しています。その一環として、シスコは次のデータを収集します。

- 使用されているライセンス
- 一意のデバイス ID（ハードウェアの場合、通常は製品 ID とシリアル番号。ソフトウェアの場合、たいていは汎用一意識別子（UUID））。
- ライセンスを使用しているデバイスのシリアル番号
- 使用されているライセンスの数量

お客様が生成するレポートを改善するために、製品のホスト名を含むオプションのデータをシスコと共有できます。共有するデータは、製品の設定によって制御できます。SSM オンプレミス ライセンス サーバーを使用している場合は、これらの情報をシスコに送信しないように個別に選択できます。共有できる項目は次のとおりです。

- ホスト名：登録済みシスコ製品インスタンスのホスト名
- IP アドレス：登録済みシスコ製品インスタンスの IP アドレス
- MAC アドレス：登録済みシスコ製品の Media Access Control（MAC）アドレス

Smart Licensing の暗号化

シスコでは、CA（認証局）を実装して Secure Sockets Layer（SSL）および Transport Layer Security（TLS）通信を使用するクライアントとサーバーに向けに公的に信頼できるアイデンティティのソースを提供しています。これらの認証局は、CA の秘密キーの保護と、認証局によって発行された X.509 証明書（SSL 証明書）の管理両方を行うシステム、製品、およびサービスで構成されます。

シスコ製品で使用される証明書

シスコ製品は、機能使用状況を Cisco Smart Software Manager（Cisco SSM）（または Cisco SSM オンプレミス）にレポートしてライセンスの使用状況を通知します。ライセンスデータの有効性を保証するために、シスコとシスコ製品は多くの重要な暗号化証明書を使用しています。

シスコライセンスルート証明書

- スマートエージェントを含むシスコ製品に組み込まれている、信頼チェーンのルートです。

シスコサブ CA

- シスコによって生成され、登録時にシスコ製品に送信されます。

ID 証明書（IDCERT）

- IDCERT は、登録プロセス中に製品の UDI を使用して Cisco SSM（または Cisco SSM オンプレミス）によって生成されます。IDCERT は（製品の UDI を通じた）製品の検証と、製品による Cisco SSM または SSM オンプレミス ライセンス サーバーの署名機関の検証に使用されます。IDCERT の有効期間は 1 年で、6 ヵ月ごとに自動更新されます。

署名証明書

- 登録時または更新時に SSM またはサテライトで生成され、シスコ製品に送信されます。署名証明書には CISCO SSM 公開キーが含まれています。このキーは、シスコ製品とシスコの間で交換される応答メッセージの署名の検証に使用されます。

スマートライセンスを使用するシスコ製品

Smart Licensing をサポートするシスコ製品は、次のメッセージを使用してライセンス使用状況レポートをシスコライセンスサーバーに送信します。

シスコ製品から送信される要求メッセージ

シスコ製品は、登録中に生成された秘密キーを使用して、すべての送信要求メッセージに署名します。シスコライセンスサーバーは、受信時に登録時の証明書署名要求（CSR）の公開キーを使用して、受信した要求メッセージの署名を検証します。証明書は SHA256 デジタル署名です。

シスコライセンスサーバー（Cisco SSM または Cisco SSM オンプレミス）から送信される応答メッセージ

シスコライセンスサーバー（Cisco SSM または Cisco SSM オンプレミス）は、登録中に生成された秘密キーを使用して、すべての送信応答メッセージに署名します。次にシスコ製品は、登録中に受信した署名証明書の公開キーを使用して、受信したメッセージの署名を検証します。証明書は SHA256 デジタル署名です。シスコライセンスサーバーは、受信時に登録時の証明書署名要求（CSR）のシスコ公開キーを使用して、受信した要求メッセージの署名を検証します。

データ交換でのデータ整合性の検証

データはシスコ製品間で交換され、このドキュメントに記載されている署名証明書のいずれかを使用して Cisco SSM に署名されます。署名プロセスを個別に監査する場合は、署名証明書から公開キーを抽出でき、暗号化ツール（OpenSSL など）を使用して、署名と照らして証明書を検証できます。

Smart License Using Policy およびマネージド サービス ライセンス契約（MSLA）をサポートするシスコ製品

Smart Licensing Using Policy およびマネージド サービス ライセンス契約（MSLA）をサポートするシスコ製品は、ISO 19770 で定義されたリソース使用状況測定（RUM）形式で使用状況レポートを蓄積します。このレポートは、シスコ ライセンス サーバーに転送する必要があります。

シスコ製品からの直接の使用状況データ収集

お客様は、各シスコ製品から使用状況レポートを送信したり、これらのレポートをシスコライセンスサーバーにアップロードしたりできます。これを行うには、使用状況データをシスコまたは認定シスコユーティリティに直接送信するように製品を設定するか（プッシュモード）、NETCONF/YANG を使用してデータを取得します（プルモード）。MSLA ではプルモードはサポートされません。

Cisco Smart Licensing Utility（CSLU）または SSM オンプレミスによる使用状況データの収集

シスコは、シスコ製品からのデータ収集を自動化する無料のソフトウェアオプションも提供しています。これらのソリューションを使用して、製品からプッシュ（レポートを送信）したり、製品からプル（レポートを取得）したりできます。収集したデータはローカルに保存され、シスコのライセンスサーバーにストアアンドフォワード方式でプロキシされます。

使用状況データ交換におけるデータ整合性の検証

シスコ製品から送信される使用状況データは、データの整合性を確保するために署名され、シスコライセンスサーバーによって検証されるため、レコードを処理する前にデータの整合性が確保されます。導入オプションに応じて、デバイスは異なるキーを使用して署名を生成できます。本書内で後述するように、整合性検証の目的は、製品とシスコの間の信頼を段階的に強化することです。

承認

Smart Licensing Using Policy により、シスコの貿易管理に従って、輸出管理機能の承認コードをダウンロードできます。

ポリシーのダウンロード

Smart Licensing Using Policy は、柔軟なレポート方法を提供します。このポリシーには、シスコへの使用状況レポート送信に義務付けられるレポート間隔と、永続ライセンスおよびサブスクリプション ライセンスのレポート期間が規定されています。Cisco スマートアカウントの対象となる特定のビジネス状況では、このポリシーが変更される場合があります。このポリシーは、ダイレクト接続方式または Cisco Smart Licensing Utility（CSLU）のいずれかによってダウンロードされます。

Cisco SSM オンプレミスによって使用される証明書

SSM オンプレミス ライセンス サーバーは、Cisco SSM への最初の登録時に、証明書署名要求（CSR）を含む登録ファイルを送信します。登録ファイルは、Cisco License Crypto Service（LCS）によって署名されます。

Smart Licensing で使用される Cisco SSM オンプレミス証明書

スマートライセンス情報の整合性を確保するために、シスコ製品は多数の証明書を利用してローカルにインストールされたオンプレミス ライセンス サーバーを検証します。これらの証明書はデータの暗号化のためではなく、サーバーが承認済みで信頼できることを立証するために使用されます。これらの証明書はシスコライセンスルート証明書から署名されており、変更することはできません。

Cisco SSM オンプレミス ライセンス サーバーの正常な動作中、最初に登録するときとその後に同期を取るときに、SSM オンプレミス ライセンス サーバーと Cisco SSM 間でテレメトリが交換されます。

- **登録要求ファイル：**SSM オンプレミス ライセンス サーバーが Cisco SSM に登録要求ファイルを送信します。
- **登録承認ファイル：**Cisco SSM は、登録要求を受信して処理した後、SSM オンプレミス ライセンス サーバーに承認ファイルを返し、SSM オンプレミス ライセンス サーバーが Cisco SSM に登録されたことと、完全な同期の詳細を通知します。
- **同期要求ファイル：**SSM オンプレミス ライセンス サーバーが同期要求ファイルを Cisco SSM に送信します。
- **同期応答ファイル：**Cisco SSM は、同期要求を受信して処理した後、SSM オンプレミス ライセンス サーバーに同期応答ファイルを返し、登録または同期が完了したことを通知します。

交換されるファイルの内容の整合性を維持するために、ファイルは作成時に署名証明書（このドキュメントに記載）で署名され、受信時に検証されます。内容と署名の照合には、署名証明書から抽出した公開キーが使用され、署名に照らして内容が検証されます。署名証明書と署名は Base64 でエンコードされているため、検証中にデコードする必要があります。

通信に使用される Cisco SSM オンプレミス証明書

シスコは、返されるシスコスマートライセンス証明書に加えて、TG_CERT と呼ばれる証明書も提供します。この証明書は、セキュアな接続を受け入れ、Cisco SSM オンプレミス ライセンス サーバーがセキュアな接続（HTTPS）を介してシスコ製品と通信できるようにするために使用されます。

シスコ製品のセキュリティ

シスコの製品開発プラクティスでは、デバイスやネットワークへの不正アクセス、機密情報の漏洩、セキュリティ機能や制限の回避を目的とする意図的な行動や製品機能の一切を禁じています。具体的には次のものがあります（これらに限定されません）。

- 未公開のデバイスアクセス方法（「バックドア」）
- ハードコード化されたアカウントログイン情報や隠しアカウントログイン情報
- 隠された通信チャネル
- 密かなトラフィックの宛先変更

シスコでは、このような製品の動作を重大な脆弱性と考えています。シスコはこの種の問題に最優先で対処します。また脆弱性が疑われる場合には Cisco Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）に報告し、即座の調査を依頼することをすべての関係者に推奨します。これらの脆弱性に関する内部および外部からの報告は、シスコのセキュリティ脆弱性ポリシーの条件に基づいて管理および開示されます。

Cisco Product Security Incident Response Team（PSIRT）

PSIRT は、シスコ製品のセキュリティインシデント対策を担当しています。Cisco PSIRT は、シスコの製品とネットワークに関係するセキュリティの脆弱性と問題に関する情報の受け取り、調査、およびレポートの公開を管理する専門のグローバルチームです。

https://www.cisco.com/c/dam/en_us/about/security/psirt/Cisco-PSIRT-Infographic.pdf‘

シスコのセキュリティ脆弱性ポリシー

シスコではセキュリティの脆弱性を、製品の完全性、可用性、または機密性を侵害する可能性がある、製品の意図しない脆弱性と定義しています。Cisco PSIRT は ISO/IEC 29147 に準拠しています。PSIRT は、24 時間年中無休で、シスコのお客様、独立したセキュリティ研究者、コンサルタント、業界団体、およびその他のベンダーと協力して、シスコ製品およびネットワークのセキュリティの潜在的な脆弱性と問題を特定しています。

https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

シスコ セキュリティ アドバイザリ

シスコ セキュリティポータルは、シスコの製品とサービス、およびサードパーティ製品のセキュリティの脅威と脆弱性に関する実用的なインテリジェンスを提供します。

https://tools.cisco.com/security/center/publicationListing

サードパーティ製ソフトウェアの脆弱性

シスコ製品で使用されているサードパーティ製ソフトウェアコンポーネントに脆弱性がある場合、通常シスコはコンポーネント開発元から提供される共通脆弱性評価システム（CVSS）のスコアを使用します。ただし、シスコ製品への影響を反映して CVSS スコアを調整する場合があります。

シスコは、次の基準を 1 つ以上満たす場合、サードパーティの脆弱性を「重大」とみなします。

- 脆弱性がサードパーティ製コンポーネント内に存在する。
- 複数のシスコ製品が影響を受けている。
- CVSS スコアが 5.0 以上。
- 脆弱性が世間で大きな注目を集めている。
- 脆弱性が活発にエクスプロイトされると予想されているか、すでに積極的にエクスプロイトされている。

シスコは、重大なサードパーティの脆弱性について、現在サポート期間中で影響を受けた可能性があるすべての製品の評価を開始し（ソフトウェアメンテナンスが終了していない製品を優先）、シスコが脆弱性を重大と分類してから 24 時間以内にセキュリティアドバイザリを公開します。影響を受けたことが判明したすべてのシスコ製品については、最初のセキュリティアドバイザリ（シスコの最初の情報開示から 7 日以内に公開）のアップデートで詳しい説明を提供します。脆弱な製品ごとにシスコのバグが作成されるので、登録済みのお客様は Cisco Bug Search Toolkit を介してシスコのバグを確認できます。重大に分類されていないサードパーティの脆弱性については、リリースノートのエンクロージャで開示します。

Cisco SSM オンプレミス アプリケーションのセキュリティ

Cisco SSM オンプレミス ライセンス サーバーは、シスコセキュア開発ライフサイクル（SDL）に準拠しています。SDL は、シスコ製品のレジリエンシと信頼性を高めるために設計された、反復可能かつ測定可能なプロセスです。

開発ライフサイクル中に導入されたツール、プロセス、営業活動やトレーニングの組み合わせにより、多層防御を促進し、製品のレジリエンシに対する包括的なアプローチが可能になり、セキュリティアウェアネスの文化を確立します。

シスコは四半期ごとに、SSM オンプレミス ライセンス サーバーのアップデートをリリースします。このアップデートには、機能とバグ修正に加え、サードパーティソフトウェアに対して報告された重大および深刻度の高い共通脆弱性識別子（CVE）が含まれています。最高レベルの製品セキュリティを確保するために、SSM オンプレミス ライセンス サーバーを常に最新のソフトウェアバージョンに更新しておくことを推奨します。

Cisco Smart Licensing 製品

製品の通信

スマート対応のシスコ製品は、ライセンスの使用状況に関する情報をシスコ内の Cisco Smart Software Manager（Cisco SSM）に定期的に送信するか、（設定されている場合）お客様の Cisco Smart Software Manager オンプレミス（Cisco SSM オンプレミス）ライセンスサーバーに送信します。送信される情報とその送信形式は、送信先に関係なく同じです。

デフォルトでは、製品はシスコ内の Cisco SSM と通信するように事前に設定されています。必要に応じて、製品を手動で設定して宛先 URL を変更し、トラフィックを Cisco SSM オンプレミス ライセンス サーバーに転送するか、プロキシを経由させることができます。この設定方法については、各製品のドキュメントを参照してください。

スマート ライセンス メッセージのトランスポート

通信は、通常は HTTPS（HTTP over TLS）を使用して暗号化されます。これがデフォルト設定です。1 つの例外として、直接 HTTP を使用して Cisco SSM オンプレミス ライセンス サーバーまたはプロキシと通信するようにシスコ製品を設定する場合もあります。この設定を行う理由として唯一考えられるのは、パケットをローカルでキャプチャし、デコードして検査する場合です。シスコのバックエンドとのすべての通信は、シスコ製品が Cisco SSM にダイレクト接続する場合でも、SSM オンプレミス ライセンス サーバーから Cisco SSM に接続する場合でも、HTTPS を使用して暗号化する必要があります。シスコ製品が暗号化されていない HTTP 通信を試みた場合、セッションは失敗します。Smart Licensing は製品に実装されている TLS に依存するため、TLS のバージョンは製品がサポートするバージョンによって異なります。

シスコ製品は、登録中に公開キーと秘密キーのペアと証明書署名要求（CSR）を作成します。公開キーは、CSR で Cisco SSM または SSM オンプレミス ライセンス サーバーに送信されます。シスコ製品は、秘密キーを使用して送信メッセージに署名します。Cisco SSM（または Cisco SSM オンプレミス）は、公開キーを使用して署名を検証します。

Smart Call Home

スマート ライセンス メッセージをシスコに送信する際、Cisco SSM は Smart Call Home API エンドポイントを使用してスマート ライセンス メッセージを Cisco SSM サーバーにリレーします。一部の製品は、Smart Call Home に製品改善やトラブルシューティングに関する情報も送信可能ですが、Smart Licensing は Smart Call Home サーバーの機能すべてを利用するわけでありません。シスコに送信する情報は Smart Call Home 設定で制限できます。

ライセンスの使用状況をシスコに報告するシスコ製品は、周知のシスコ API（tools.cisco.com）を使用します。サーバーは、地理的な場所に最適なサーバーへの多数のリージョンのロードバランサによってサポートされます。Cisco SSM オンプレミス ライセンス サーバーにライセンスの使用状況をレポートするシスコ製品は、ライセンスサーバーの URL（または IP アドレス）を使用します。Smart Call Home は、URL 形式に基づいて HTTP または HTTPS のいずれかを使用するように設定できます。HTTPS を使用することを強くお勧めします。Smart Call Home の詳細については、https://www.cisco.com/c/dam/en/us/td/docs/switches/lan/smart_call_home/SCH_Deployment_Guide.pdf を参照してください。

Smart Transport

Smart Transport は、サポート対象のシスコ製品で使用できるもう 1 つのトランスポートプロトコルです。スマートライセンスの「機能」という観点での違いはありません。Smart Transport は、一部のお客様（軍事機関）が Smart Call Home の使用を禁止する（その設定の存在を許可しない）ポリシーを採用しているために導入されました。つまり、Smart Call Home の設定またはトランスポートを使用せずに、スマート ライセンス メッセージをシスコに送信するための新しい手段が必要でした。

主な違いは、以下に示すように、使用されているトランスポート エンコーディングと API ゲートウェイです。

トランスポート	製品サポート	API ゲートウェイ	アクセス ポイント	プロトコル	VRF サポート	プロキシ サポート
Smart Call Home	すべて（デフォルトで有効）	tools.cisco.com	ローカル	HTTP/HTTPS（SOAP）	◯	◯
Smart Transport	一部	smartreceiver.cisco.com	米国	HTTPS（JSON）	×	◯

ほとんどのお客様は、幅広い製品サポート、管理 VRF のサポート、ファイアウォールの影響の簡素化、設定の標準化などの理由で Smart Call Home の使用を継続しています。

Smart Transport は、URL 形式に基づいて HTTP（非暗号化）モードと HTTPS（暗号化）モードの両方をサポートします。Cisco SSM オンプレミス ライセンス サーバーはどちらの形式も受け入れますが、Cisco SSM は HTTPS セッションのみを受け入れます。

スマートライセンスのプロトコルとポート

Smart Licensing に関連する通信はシスコ製品によって開始されます。シスコ内の Cisco SSM や Cisco SSM オンプレミス ライセンス サーバーから通信を開始することはできません。これらが実行できるのは、シスコ製品からの要求への応答のみです。この動作はファイアウォールルールに反映可能なので、ルールに反映させる必要があります。

シスコ製品は、適切なエンドポイント（Cisco SSM または SSM オンプレミス ライセンス サーバー）に到達できる必要があります。到達可能にするには、ファイアウォールルールや中間プロキシの設定が必要になる場合があります。使用されるチャネルとポートは、使用するトランスポートプロトコルによって異なります。以下を参照してください。

Smart Call Home

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

Smart Transport

- HTTPS（443）：smartreceiver.cisco.com

シスコ製品登録用の ID トークン

シスコ製品は、Cisco SSM オンプレミス ライセンス サーバーに登録するために、対象のローカル バーチャル アカウントから有効な ID トークンを取得する必要があります。シスコ製品が登録されると、製品からシスコライセンス サーバーに ID トークンが送信されます。サーバーはこの ID トークンを検索して、その有効性（有効期限内であることや取り消されていないこと）を確認します。

各 ID トークンは一意である必要があるため、ランダムな 32 バイト配列（KEY と呼ばれます）を使用して、ローカル バーチャル アカウント ID および現在のタイムスタンプ（TBS と呼ばれます）とともに生成されます。トークンが生成される際、結果は KEY によって署名されてから Base64 でエンコードされます。この文字列は TBS が付加されてからもう一度 Base64 でエンコードされます。その後、トークンはローカルデータベースに保存されます。

メッセージの内容

シスコ製品から Cisco SSM または Cisco SSM オンプレミス ライセンス サーバーに送信される情報には、次のものが含まれます。

- 製品が関連付けられているスマートアカウントとバーチャルアカウント。これは基本的に製品の所有者であり、製品登録時に決定されます。この情報は、最初は ID トークンを介して伝達され、その後は PIID と UDI によって伝達されます。
- 製品の固有のデバイス識別子（UDI）。ハードウェア製品の場合、通常は製品タイプ（PID）とシリアル番号です。ソフトウェアのみの製品は、汎用一意識別子（UUID）を使用します。ライセンス使用量の二重カウントを防ぐためにお客様向けレポートで使用されます。
- 使用されているライセンスと数量
- （オプション）ホスト名をシスコまたは Cisco SSM オンプレミス ライセンス サーバーに送信するようにシスコ製品を設定できます。ホスト名は、お客様向けの使用状況レポートで使用されます。レポートでのホスト名の使用は効率的だと多くのお客様から報告されています。ホスト名を使用しない場合は、UDI ごとに使用状況が表示されます。

スマート ライセンス メッセージのデータ要素の多くは、国際標準化機構（ISO）仕様 ISO/IEC-19770 で定義されている形式に準拠しています。ISO/IEC-19770 は、ソフトウェア資産と関連する IT 資産の管理に役立つ IT 資産管理（ITAM）の一連の標準規格です。Cisco Smart Software Licensing は、主にこの標準の 3 つの要素と関連性があります。

- ISO/IEC 19770-2 は、ソフトウェア識別タグ（「SWID」）向けのデータ標準です。
- ISO/IEC 19770-3 は、使用権、制限、メトリクス（「ENT」）を含む、ソフトウェア エンタイトルメント タグ向けのデータ標準です。
- ISO/IEC 19770-4 は、リソース使用率測定（「RUM」）に関するデータ標準です。

シスコはこれらの標準を使用して、ソフトウェア識別タグ、ソフトウェア エンタイトルメント タグ、RUM レポートなどのさまざまなデータフィールドの形式を定義しています。詳しい説明については、「ISO/IEC 19770-5：Overview and Vocabulary」（https://www.iso.org/obp/ui/#iso:std:iso-iec:19770:-5:ed-1:v1:en）を参照してください。

Smart Licensing のメッセージのタイプと頻度

シスコ製品によって開始される 4 つの 主な Smart Licensing メッセージのタイプを以下に示します。

- 登録、更新、登録解除
- エンタイトルメント（ライセンス）要求
- 変換要求
- 特殊な要求（一部の製品のみでサポート）

登録：最初の登録では、Cisco SSM または SSM オンプレミス ライセンス サーバーのバーチャルアカウントに、このバーチャルアカウントから生成された ID トークンを使用してシスコ製品を登録します。ID トークンを作成できるのは、バーチャルアカウントの承認ユーザーのみです。このメカニズムは、製品の所有権と信頼の確立のために使用されます。ID トークンの説明については、ID トークンを参照してください。シスコ製品は、ID トークンとともに、自身の UDI、高可用性ピアの UDI、および製品タイプを識別する ISO 19770-2 ソフトウェア ID タグを送信します。登録の完了時に、X.509 ID 証明書、X.509 署名証明書、および一意のシスコ製品識別子（PIID）がシスコ製品に割り当てられます。ID 証明書は、アイデンティティと信頼のために使用されます。

登録更新の主な目的は、ID 証明書の更新です。ID 証明書の有効期間は 1 年です。デフォルトでは、シスコ製品は ID 証明書を 6 ヵ月ごとに更新します。ユーザーは、発行直後に登録の更新を強制するコマンドを発行できます。

登録解除すると、スマートアカウントとバーチャルアカウントから製品の登録が解除されます。

エンタイトルメント要求：エンタイトルメント要求（承認要求とも呼ばれます）は、ライセンスの使用状況情報を Cisco SSM または SSM オンプレミス ライセンス サーバーに送信するために使用されます。製品は、通常、使用状況とステータス情報の同期のために、ライセンスの使用量が変更されるたび（必要に応じて複数の変更を含めるために若干の遅延が生じます）、および 30 日ごとに、エンタイトルメント要求を送信します。ライセンスの使用量が頻繁に変更される一部の製品（ダイナミック セッション カウント ライセンスなど）は、要求の送信を調整します。通常、これらの製品は 1 日に発生した変更の数に関係なく、1 日に 1 回だけ要求を送信します。

エンタイトルメント要求には、シスコ製品の UDI、PIID、HA ピア情報、および使用中のライセンスが含まれています。ライセンスは、使用中の数量が含まれている ISO 19770-2 エンタイトルメントタグで識別されます。応答には、シスコ製品が関連付けられているバーチャルアカウントの準拠状況、次の要求までの間隔（常に 30 日、ただし製品による変更可能）、および承認有効期間（常に 90 日）が含まれています。

変換要求：通常、変換要求は、従来のライセンスモデルのみをサポートするソフトウェアレベルから、Smart Licensing をサポートするソフトウェアレベルに製品をアップグレードした後にライセンスを変換するために使用されます。シスコ製品のコマンド（CLI：**license smart Conversion Start** または GUI）によって開始されるこのメッセージを使用して、シスコ製品の従来のライセンスをスマートライセンスに自動的に変換します。通常変換要求は、障害が発生しない限り、製品によって 1 回だけ送信されます。この要求とともに送信される情報には、シスコ製品の UDI、シスコ製品 ID、ソフトウェア ID タグ、変換データが含まれます。変換データには、シスコ製品に保存されているライセンスファイル、エンタイトルメントタグ、製品に設定されている「信頼ベース」ライセンスの数が含まれます。応答では、要求されたライセンスの変換が成功したか失敗したかが返されます。

特殊な要求：特殊な状況で送信される他のタイプのメッセージもあります。これらのメッセージはすべての製品でサポートされているわけではありません。特殊な要求には次のようなものがあります。

- エンドポイントレポート：ライセンスを使用し、複数のコントローラ（アクセスポイントをレポートするワイヤレス LAN コントローラなど）のレポート対象のエンドポイントのレポートに使用されます。
- 輸出承認要求：米国の輸出規制対象機能を使用できるようにする輸出承認キーを要求します（詳細については、以下の「米国の輸出管理」を参照してください）。
- サードパーティキー要求：サードパーティデータ（通常はサードパーティからのライセンスキー）を要求します。
- ポーリング要求：応答を取得するために Cisco SSM または SSM オンプレミス ライセンス サーバーにポーリングします。通常は、最初の要求時に取得できなかった応答を取得するために行われます。

Smart License Using Policy のメッセージ転送

製品とシスコの間で交換されるすべての通信は、HTTPS（HTTP over TLS）を使用して暗号化されます。製品から送信される情報にはすべて、使用状況データとリターンコードの両方が含まれます。この情報は製品によって署名され、シスコによって検証されるため、レコード処理の前にデータの整合性が確保されます。詳細なフローについては、「付録」を参照してください。

米国の輸出管理

米国の輸出管理規制では、輸出ライセンスという特別な許可が付与されない限り、シスコから一部の組織（主に新興市場国の政府と軍部）への特定の機能（通常はユーザーデータの高速で強力な暗号化）の出荷を禁止しています。制限された機能の任意の組織への出荷には規制があり、禁輸対象の組織と制裁下の組織には特別な規則と制限があります。これらの規制の遵守は任意ではなく、シスコが完全に対応しています。ライセンスは、規制に確実に遵守するために使用されてきた主要なメカニズムの 1 つです。詳しい説明については、
https://www.cisco.com/c/en/us/about/legal/global-export-trade.html を参照してください。

実施される輸出検査には 2 つのタイプがあります。1 つはスマートアカウントの設定時に実施され、シスコはその時点でスマートアカウントの所有者になる企業に関連するすべての輸出関連制限の判定を試みます。もう 1 つは、取引の当事者が決定され、審査が行われる発注時に実施されます。製品によっては、これらの検査だけで、制限された機能の有効化を当該のお客様に許可できる場合があります。一方、特定のシスコ製品に関連付けられた特別な輸出承認キーを製品にインストールしなければ、制限された機能の有効化を許可できない場合もあります。輸出承認要求および応答は、必要なキーを要求してインストールする必要がある場合に使用されます。

サードパーティのライセンス

シスコ製品には、Smart Licensing を使用して Smart Licensing 以外からライセンス情報を要求する機能があります。この機能は、ライセンスを必要とするサードパーティソフトウェア機能用のライセンス（通常はライセンスファイル）を取得するために使用されます。たとえば、コラボレーションの「音声認識」機能は Nuance ライセンスを必要とします。

シスコ製品から送信されるサードパーティのライセンス要求には、製品の UDI、PIID、該当のサードパーティ、要求されるデータ（キー名や ID）、および要求を実行するために必要なその他のデータが含まれます。応答には、製品に関連付けられているバーチャルアカウント、シスコ製品の UDI および PIID の確認、および要求されたキーが含まれます。

ライセンス予約

ライセンス予約は、非接続型の Cisco SSM オンプレミス ライセンス サーバーを利用しない（リモート導入やローハイサイド運用など）完全なエアギャップ環境向けに一部の製品でサポートされている機能です。このオプションでは、継続的な通信も、インフラストラクチャを増強する必要もありません。ライセンス予約は、スマートライセンスのトラッキングを提供します。機能的にはノードロックとほぼ同等です。もともとライセンス予約では、オンライン通信を利用する自動プロセスを利用できないため、ライセンス予約を使用すると、特にシスコ製品間でのライセンスの移動やライセンス使用の変更などの操作では、運用のオーバーヘッドが増える可能性があります。ライセンス予約では、予約を更新するかシスコ製品から削除するまで、特定のシスコ製品用にライセンスを永続的に予約することになります。

ライセンス予約を行うには、シスコ製品から要求コードを生成して Cisco SSM に入力し、Cisco SSM 上で必要なライセンスを予約します。次に Cisco SSM が承認コードを生成するので、これをシスコ製品に入力する必要があります。ライセンス予約を削除し、他での使用のためにライセンスを解放する場合は、シスコ製品で予約を取り消し、結

果の確認コードをコピーして Cisco SSM に入力すると、Cisco SSM によって予約がキャンセルされます。予約に含まれるライセンスの増減のために予約を更新するには、Cisco SSM で該当のシスコ製品に移動し、予約を変更します。Cisco SSM によって新しい承認コードが生成されるので、これをシスコ製品に入力する必要があります。シスコ製品が確認コードを生成したら、次はこのコードを Cisco SSM に入力します。その時点で、Cisco SSM が予約から削除されたすべてのライセンスを解放します。予約からライセンスを削除せず、予約にライセンスを追加するだけの場合は、Cisco SSM への確認コードの入力は任意です。

ライセンス予約要求コードは ASCII 文字列で、UDI 以外は BASE58 でエンコードされているので、明確に入力できます。このコードには、バージョン、シーケンス番号、製品 UDI、SW ID タグ（9 文字のハッシュ値）、2 文字のハッシュが含まれています。

特定のライセンス予約承認コードは XML 形式のファイルで、改ざんを防止するために署名が含まれています。このコードには、製品が関連付けられているバーチャルアカウント、シスコ製品の確認用 UDI および PIID、および各予約済みライセンスのライセンスタイプ（永続、期限付き、またはサブスクリプション）、エンタイトルメントタグ、数、期間ライセンスまたは永続ライセンスの開始日と終了日、ライセンス名とその説明、サブスクリプション ID（該当する場合）、改ざん防止用の署名が含まれています。同じ承認コードは、最初の承認であるか変更であるかに関係なく、同じものです。

変更の確認に使用される確認コードは、UDI、シーケンス番号、PIID、SLR 承認コードからのタイムスタンプに基づいて計算されたハッシュです。このハッシュは BASE58 でエンコードされます。ライセンス予約の削除を確認するリターンコードでも、BASE58 でエンコードされた ASCII 文字列（バージョン、シスコ製品の PIID、および署名を含む）が使用されます。

スマートライセンスの状態

ライセンスの状態遷移は、ほとんどの場合ユーザーに対して透過的です。状態遷移について理解しておくと、主にトラブルシューティングの際に役立ちます。状態の変化の認識にも役立つでしょう。

スマート対応製品をインストールする場合、または従来のライセンスから Smart Licensing にアップグレードする場合の通常のイベントシーケンスを以下に示します。

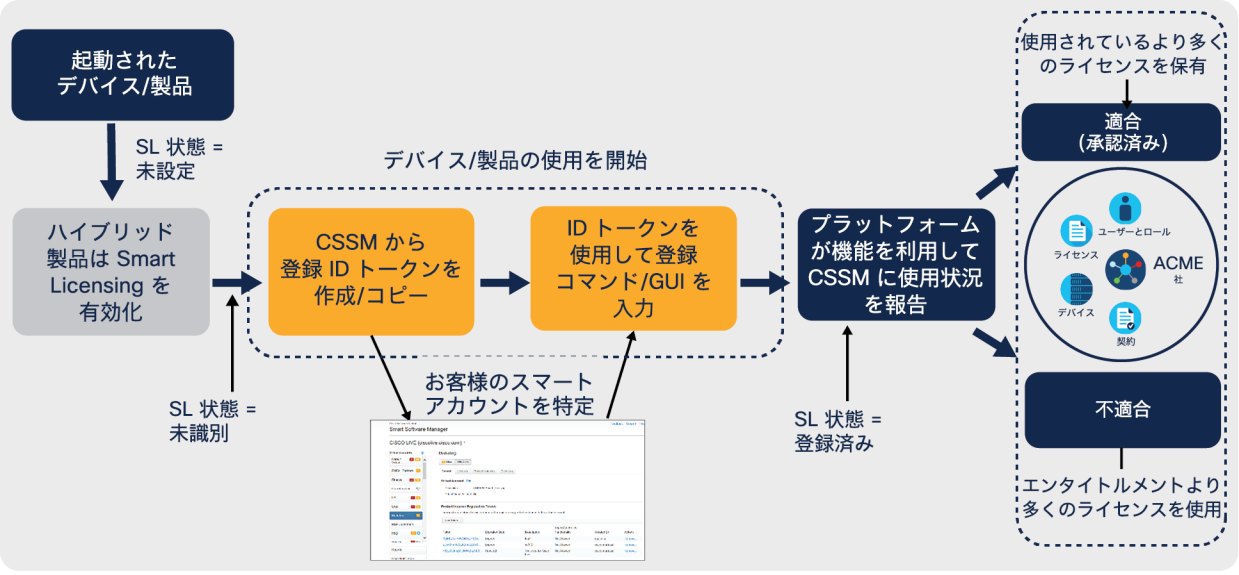


図 1.
Smart Licensing のワークフロー

このプロセスは、製品をスマート対応にし、従来のライセンスと Smart Licensing の両方をサポートできるようにすることから始まります。これらの製品では、アップグレード中の中断を最小限に抑えるために、デフォルトは従来のライセンスです。Smart Licensing のみをサポートする製品はもともとスマート対応なので、この手順は必要ありません。

次に行うのは、目的のスマートアカウントとバーチャルアカウントへのシスコ製品の登録です。この登録は、Cisco SSM または SSM オンプレミスライセンスのいずれか（シスコ製品との通信がどちらに設定されているかによって異なります）のスマートアカウント/バーチャルアカウント（SA/VA）から生成された ID トークンを使用して行われます。ID トークンは、シスコ製品を SA/VA に関連付ける手段だけのものです。ID トークンは製品固有のものではなく、1 つの ID トークンをあらゆる製品タイプで（作成時に制限が設定されていない限り）何度でも使用できます。ID トークンは最初の登録にのみ使用され、シスコ製品には保存されません。ID トークンの有効期限が切れても、登録済みのシスコ製品には影響しません。ID トークンの有効期限が切れた場合、そのトークンを使用して追加のシスコ製品を登録することはできません。

ほとんどの場合、他の操作は不要です。登録では、継続的なアイデンティティに使用される X.509 ID 証明書がシスコ製品に割り当てられ、Cisco SSM または SSM オンプレミス ライセンス サーバーとの信頼が確立されます。シスコ製品は、ライセンス使用情報を自動的に送信し、ステータスの更新を受信し、ID 証明書の有効期限を定期的に更新します。

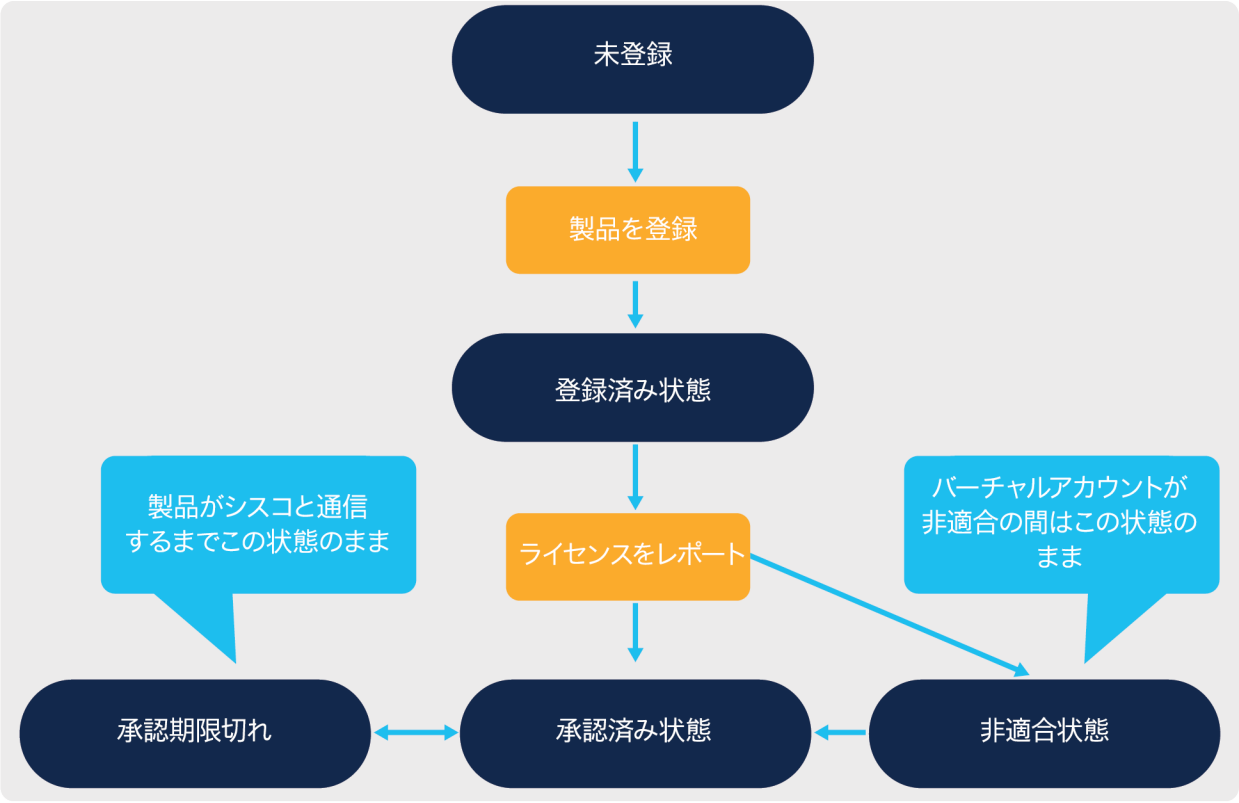


図 2.
スマートライセンス製品の状態

Smart Licensing はさまざまな状態になる可能性があります。この図は、これらの状態を示しています。

未登録状態：Smart Licensing の初期状態は「未登録」です。これは、Smart Licensing を有効にした（スマートのみに対応する製品の場合は起動した）だけで、Cisco SSM または Cisco SSM オンプレミス ライセンス サーバーに登録する前の製品の状態です。

評価モード：多くの場合、シスコ製品の初期モードは「評価モード」です。評価期間とは、未登録の製品がライセンスを使用している期間です。製品には、1 回限り有効の 90 日間（製品の寿命期間）の評価タイマーがあります。このタイマーは、製品が稼働中で、ライセンスを使用中で、未登録の間に動作します。有効な期間が残っている場合、これらの 3 つの基準を満たしていれば、いつでも再度評価モードに戻ることができます。評価期間は、シスコ製品を登録するか、すべてのライセンス使用設定を解除することで、無期限に一時停止できます。

登録済み状態：シスコ製品は、正常に登録されると、自身が使用しているライセンス情報を含む承認要求を自動的に送信します。承認要求は、情報の同期を維持するために、ライセンス使用量が変更される（増減する）たび、および に 30 日ごとに送信されます。

承認済み状態：次にシスコ製品は、バーチャルアカウントのライセンス使用ステータスが含まれる応答を受信します。ここでの問題は、このバーチャルアカウントが、自身に関連付けられている全シスコ製品からの承認要求を満たすのに十分なライセンスを保有しているかということです。バーチャルアカウントに十分なライセンスがある場合、ライセンスは「承認済み」と判断されます。

不適合状態：バーチャルアカウントに十分なライセンスがない場合、ライセンスは「不適合」と判断されます。不適合のライセンスを使用している製品はすべて、不適合状態になります。これはシスコ製品ではなくバーチャルアカウントのステータスですが、シスコ製品に影響する可能性があることに注意してください。ライセンスはバーチャルアカウント内でプールされるため、個々のライセンスが特定のシスコ製品に割り当てられることはありません（ライセンス予約を使用する場合を除く）。また、別のシスコ製品が承認済みのときに特定のシスコ製品が不適合になるという概念はありません。これは、シスコ製品が、承認要求を送信して応答を受信したときにしかライセンスのステータスの変更を認識しないことを示唆しています。ユーザーには、承認要求を手動で強制的に送信し（手順については製品ドキュメントを参照）、簡単にステータスを更新できるオプションがあります。

上記の通常のプロセスを妨げる可能性のあるシナリオの 1 つは通信障害です。通信障害があると、登録済みシスコ製品は承認要求/応答シーケンスを正常に完了できません。障害が発生する理由は、リンクのダウンから、シスコ製品を分離する新しいファイアウォールルールまでさまざまです。通信障害が発生すると、シスコ製品は（コンソールおよび syslog）エラーを送信し、要求を再試行します。再試行の間隔は、承認の状態によって異なります。

- 製品が承認済み状態の場合は、23 時間ごとに再試行されます（毎日まったく同じ時刻には再試行しないようにします）。
- 製品が不適合状態の場合は、最初の 2 時間は 15 分ごとに再試行され、その後は 4 時間ごとに再試行されます。
- 製品が承認期限切れ状態にある場合は、1 時間ごとに再試行されます。

承認期限切れ状態：通信障害が長期間続くと、分離されているシスコ製品のライセンス承認期限が切れる場合があります。ライセンス承認は 90 日間有効です。期限切れになると、シスコ製品は承認期限切れ状態になり、毎週 syslog エラーメッセージを送信します。

ID 証明書は、シスコ製品のアイデンティティの要であり、信頼の基盤ですが、有効期間は 1 年です。ID 証明書は、通常 6 ヵ月ごとに自動更新されます。通信障害が発生すると ID 証明書の更新は失敗するため、シスコ製品は ID 証明書の有効期限が切れるまで 1 時間ごとに更新を再試行します。さらにシスコ製品は、以下の間隔で、通信障害による再試行のたびに ID 証明書の有効期限の警告に関する syslog メッセージを送信します。

- 期限切れの 60 日前

- 期限切れの 30 日前
- 週 1 回（最後の 30 日間）
- 1 日 1 回（最後の 1 週間）
- 1 時間に 1 回（最終日）

ID 証明書の有効期限：通信障害が長時間続くと、ID 証明書の有効期限が切れ、重大なエラーが発生し、製品の再登録と修正が必要になる場合があります。ID 証明書の有効期限が切れた時点で、評価期間が残っている場合、シスコ製品は未識別状態に戻り、再度評価モードになります。製品の登録が解除されると、製品インスタンスも未識別状態になります。

未承認状態での製品の動作

シスコは、お客様が未承認の状態を修復し、製品を適合状態に戻す（使用されているライセンスと同じ数以上のライセンスをバーチャルアカウントに提供する）ことを想定しています。これは、次の 4 つのいずれかの方法で行うことができます。

1. 通信障害を解消し、製品がライセンス使用状況をレポートできるようにする。
2. 追加のライセンスを購入し、バーチャルアカウントに提供する。
3. 余剰ライセンスを保有するバーチャルアカウントから、ライセンスが不足しているバーチャルアカウントにライセンスを移行する。
4. バーチャルアカウントに関連付けられた十分な数のシスコ® 製品で、ライセンスを必要とする機能の設定を解除し、使用中のライセンス数を使用可能なライセンス数以下に減らす。

シスコ製品は、未承認の状態であっても、その大半はアクションを起こしません。しかしながら、ユーザーがシスコ製品や Cisco スマートアカウントを準拠状態に戻す責任から解放されるわけではありません。一部の製品は、承認済み状態に戻らない場合、何らかの措置を講じます（たいていは機能の追加を制限します）。

各種状態や各種シナリオにおける製品固有の動作については、製品のドキュメントまたは https://www.cisco.com/jp/go/smartlicensing を参照してください。

評価

前述のように、シスコ製品が未登録/未識別のままでライセンスを使用しているときの評価期間は、シスコ製品のライフサイクル全体で最大 90 日間です。Out of compliance 米国の輸出規制により、シスコ製品に別の輸出承認キーがインストールされているか、別の輸出関連規制に準拠している場合以外は、最初の評価期間に輸出規制対象機能をシスコ製品で動作させることはできません（シスコがシスコ製品を運用している当事者を確認できないため）。ほとんどのハードウェアベースの製品では、評価期間中に輸出制限のない機能を無制限で使用できます。すべてではありませんが、多くのソフトウェアベースの製品には機能制限があり、通常はスループットが制限されます。

不適合

バーチャルアカウントが不適合の場合、ユーザーがその状況を認識できるように、複数のアラームと通知が送信されます。シスコ内の Cisco SSM は、不適合通知に登録しているユーザーに電子メール通知を送信します。Cisco SSM と Cisco SSM オンプレミス ライセンス サーバーはともに、不適合状態になったときに該当ユーザーにエラー通知を送信します。不適合ライセンスを使用している製品インスタンスは、1 週間に 1 回 syslog エラーメッセージを送信します。

承認期限切れ

ほとんどのハードウェアベースの製品は、syslog エラーを通知する以外のアクションは実行しません。ただし、一部のソフトウェアのみの製品ではアクションが実行されます。一般的なアクションは、追加機能の設定の制限です。

ID 証明書期限切れ

シスコ製品の ID 証明書の有効期限が切れて未識別モードになると、不適合や承認期限切れの場合よりも多くの製品がアクションを実行しますが、大半の製品はアクションを実行しません。通常は機能の追加が制限されます。

Cisco SSM オンプレミス ライセンス サーバー

Cisco SSM オンプレミス ライセンス サーバーは、シスコ製品全体のソフトウェアライセンスを管理するライセンス管理システムです。お客様に、シスコ ソフトウェア ライセンスをローカルで管理、追跡、更新する機能を提供します。また、単一のユーザーインターフェイスを介して、ライセンスの所有権と使用状況に関する情報を提供します。

Cisco SSM オンプレミスのデータ共有とプライバシー

Cisco SSM オンプレミス ライセンス サーバーを Cisco SSM に初めて登録すると、Cisco SSM オンプレミス ライセンス サーバーと Cisco SSM の間で次の 2 つのファイルが交換されます。

- **登録要求ファイル：**Cisco SSM オンプレミス ライセンス サーバーが Cisco SSM に登録要求ファイルを送信します。
- **承認応答ファイル：**Cisco SSM は、登録要求を受信して処理した後、Cisco SSM オンプレミス ライセンス サーバーに承認ファイルを返し、Cisco SSM オンプレミス ライセンス サーバーが Cisco SSM に登録されたことと、完全同期の詳細を通知します。

定期的な同期中に、Cisco SSM オンプレミス ライセンス サーバーと Cisco SSM は、次の 2 つの追加ファイルを交換します。

- **同期要求ファイル：**Cisco SSM オンプレミス ライセンス サーバーが同期要求ファイルを Cisco SSM に送信します。
- **同期応答ファイル：**Cisco SSM は、同期要求を受信して処理した後、Cisco SSM オンプレミス ライセンス サーバーに同期応答ファイルを返し、登録または同期が完了したことを通知します。

Cisco SSM オンプレミスホスト OS のセキュリティ

Linux カーネル

Cisco SSM オンプレミス ライセンス サーバーの基盤は CentOS 1804 システムです。CentOS 1804 システムは、SCAP Security Guide（SSG）を利用して、政府レベルの規制を満たすように構成および強化されています。ホスト OS は、未使用の通信ポートを閉じ、「root」アクセス権を削除し、単一の「admin」ユーザーを使用することで、セキュリティをさらに強化しています。

導入プロファイル

Cisco SSM オンプレミス ライセンス サーバーは、ソフトウェアの導入時に使用できる、次の 2 つの異なるプロファイルを提供します。

- **標準プロファイル：**ログインすると、標準の CentOS bash シェルが開き、オプションで Cisco SSM オンプレミス ライセンス サーバー コンソールを使用できます。このプロファイルは、通常国防関連以外の組織と金融機関に求められる標準セキュリティ機能を提供します。
- **DISA STIG プロファイル：**ログインすると、Cisco SSM オンプレミス ライセンス サーバー オンプレミス コンソールが開きます。このコンソールは、「ホワイトリストに登録された」コマンドのメニューを提供し、「**sudo**」や「**root**」レベルのアクセスを防止します。STIG への準拠が必要な場合は、インストール時にこのセキュリティプロファイルを選択します。このプロファイルを選択することで、米国国防総省のセキュリティシステムに必要なセキュリティ機能が有効になります。また、このプロファイルの選択によって有効になる機能は、セキュリティ技術導入ガイド（STIG）の標準にも準拠しています。

ホスト OS アクセス

Cisco SSM オンプレミス ライセンス サーバー コンソールは、組み込みのコマンドライン インタープリタ（CLI）の使用を通じて Cisco SSM オンプレミス ライセンス サーバーを管理する安全なアプローチを提供します。多くの場合、これらのプロファイル間の主な相違によって、お客様の実稼働環境のホスト OS へのアクセスレベルが決まります。**標準プロファイル**は Bash アクセスを提供しますが、**DISA STIG プロファイル**は強化されたシェルのみを提供するため、セキュリティのレベルが高くなります。

Cisco SSM オンプレミス アプリケーションのセキュリティ

通信ポートおよびプロトコル

Cisco SSM オンプレミス ライセンス サーバーは、お客様のネットワークとシスコ間の安全な通信のために Hypertext Transfer Protocol Secure（HTTPS）を使用します。オプションで、製品は設定された宛先 URL に基づいて、HTTP または HTTPS を使用できます。一方 Cisco SSM オンプレミス ライセンス サーバーは、デフォルトの HTTPS TCP ポート 443 および 8443 を使用します。製品でのみ使用可能な HTTP は、ポート 80 を使用します。次の表に、Cisco SSM オンプレミス ライセンス サーバーで現在使用されているポートの概要を示します。

	製品	ブラウザ	高可用性
暗号化	443	8443	5432（バージョン 7） 22（バージョン 8）
暗号化されていない	80	該当なし	該当なし

製品と Cisco SSM オンプレミスとの通信

Cisco SSM オンプレミス ライセンス サーバーは、Smart Licensing を提供する Smart Call Home API のサブセットのみを複製します。Cisco SSM ライセンスサーバーと同様に、Cisco SSM オンプレミス ライセンス サーバーは、ネットワークのニーズに基づいて、HTTPS（443）と HTTP（80）の両方を提供します。

Cisco SSM オンプレミスと Cisco SSM の通信

Cisco SSM オンプレミス ライセンス サーバーは、公開されているシスコ ソフトウェア API である swapi.cisco.com を使用してシスコとデータを交換します。この API はエニーキャストアドレスを介して利用できます。

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

Cisco ソフトウェア API に加えて、シングルサインオンサーバーである cloudsso.cisco.com も、ローカルアカウント登録時の CCOID の認証に使用されます。

Cisco SSM オンプレミスへのシスコ製品の登録

Cisco SSM オンプレミス ライセンス サーバーがシスコ製品からの登録要求を受け入れるには、Cisco SSM オンプレミス ライセンス サーバーを Cisco Smart Software Manager ポータルに登録する必要があります。登録プロセス中に、Cisco SSM オンプレミス ライセンス サーバーは 3 層証明書と 4 層証明書を含む一連の証明書を受け取ります。

ご使用のシスコ製品に最新のスマートエージェントコードが実装されておらず、Cisco SSM が 3 層証明書のみを要求している場合は、Cisco SSM オンプレミス ライセンス サーバーを Cisco SSM に登録後、48 時間待機する必要があります。この証明書は手動で署名されます。48 時間後、3 層証明書が local_sub_ca_cert: 応答フィールドに埋め込まれます。この時点で、3 層デバイスを Cisco SSM オンプレミス ライセンス サーバーに登録できます。

信頼チェーンの自動検証を促進にするために、証明書のパス長が 4 レベル（4 層）に拡張されました。4 層証明書を使用する場合、スマートエージェントは証明書全体のパスの長さを検証します。Cisco SSM オンプレミス ライセンス サーバーで、シスコライセンスルート証明書によって署名されていることを確認します。

最初の登録時に、Cisco SSM オンプレミス ライセンス サーバーから Cisco SSM に送信される CSR にはただちに署名されます。ただし、信頼チェーンが自動的に機能するように、製品のスマートエージェント、Cisco SSM オンプレミス ライセンス サーバー、および Cisco SSM 製品に変更を加える必要があります。

付録

用語

Cisco SSM または CSSM – Cisco Smart Software Manager	**PID** – 製品 ID
CSR – 証明書署名要求	**PLR** – 永続ライセンス予約
DLC – Device Led Conversion	**SA** – スマートアカウント
DNS – ドメインネームサーバー	**SBP** – サブスクリプション課金プラットフォーム
FQDN – 完全修飾ドメイン名	**SCH** – Smart Call-Home
LCS – ライセンス暗号モジュールのサポート	**SKU** – 最小在庫管理単位
LVA – ローカル バーチャル アカウント	**SLR** – 特定のライセンス予約
MSLA – マネージド サービス ライセンス契約	**TPL** – サードパーティのライセンス
OOC – 不適合	**UUID** – 汎用一意識別子
PI – 製品インスタンス	**VA** – バーチャルアカウント

データの定義

顧客データ：顧客データとは、シスコの製品またはサービスの使用に関連してシスコに提供されるすべてのデータ（テキスト、音声、ビデオ、または画像ファイルを含む）を指します。顧客データには、以下に定義されている管理データ、支払データ、サポートデータ、テレメトリデータは含まれません。

管理データ：管理データとは、製品またはサービスのサインアップ、購入、契約、または管理の際に提供される、お客様の担当者に関する情報です。管理データには、最初の契約時に収集されたものか、その後の製品またはサービスの管理中に収集されたものであるかを問わず、氏名、住所、電話番号、IP アドレス、電子メールアドレスが含まれる場合があります。

支払データ：支払データは、製品またはサービスの購入時またはライセンス契約の締結時にお客様から提供される情報です。支払データには、氏名、請求先住所、支払手段番号、支払手段に関連付けられたセキュリティコード、およびその他の財務データが含まれることがあります。

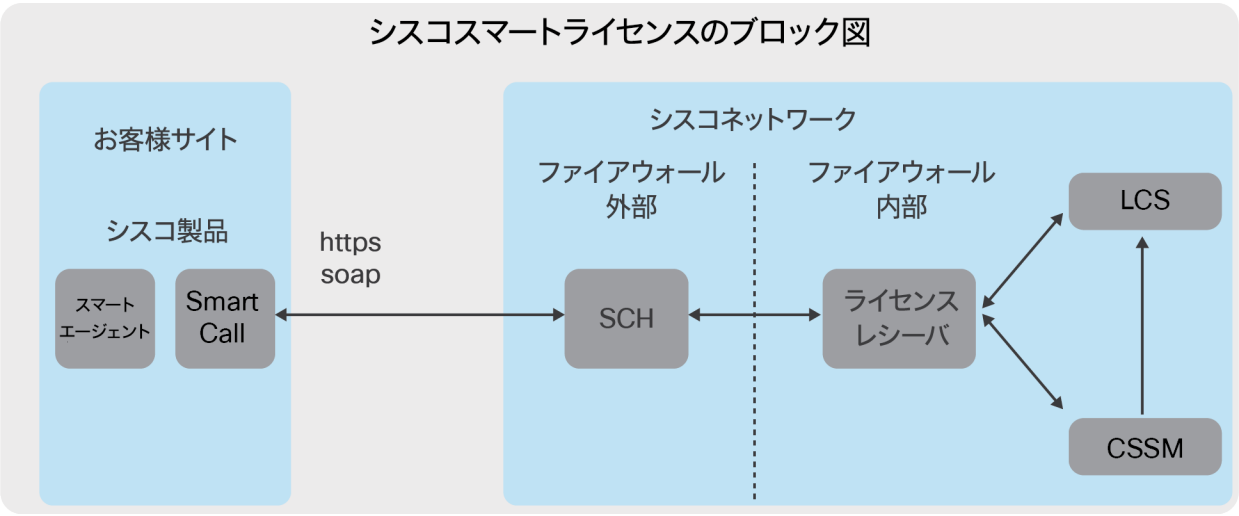
サポートデータ：サポートデータとは、お客様がサポートサービスまたはその他のトラブルシューティングのリクエストを送信する際にシスコが収集するデータです。ハードウェア、ソフトウェア、サポートインシデントに関連するその他の詳細情報が含まれることがあります。この詳細情報の例として、認証情報、製品の状態に関する情報、ソフトウェアのインストールやハードウェアの構成に関するシステムデータやレジストリデータ、エラー追跡ファイルなどがあります。サポートデータには、サポートリクエストの誘因となった問題のトラブルシューティングに役立つようにシスコに提供された、製品から取得したログ、構成ファイルやファームウェアファイル、コアダンプは含まれません。

テレメトリデータ：テレメトリデータは、電子メール、Web、およびネットワークトラフィックのサンプルです。例として、email-message 属性や Web-request 属性に関するデータ、シスコ製品によるさまざまなタイプの電子メールメッセージや Web リクエストの処理およびルーティング方法に関する情報などが挙げられます。テレメトリデータに含まれる電子メールメッセージメタデータと Web 要求は、無関係の第三者への開示の前に、個人を特定できる情報を削除するために匿名化または難読化されます。

使用状況レポート：Smart Licensing Using Policy および MSLA の使用状況レポートに使用される、ISO 19770 で定義されているリソース使用状況測定（RUM）形式。

シスコ製品プロトコルの概要

このドキュメントでは、スマートエージェントを Cisco SSM に登録する方法、証明書の使用方法、メッセージの署名方法について説明します。



シスコ製品の登録

シスコ製品からの登録要求

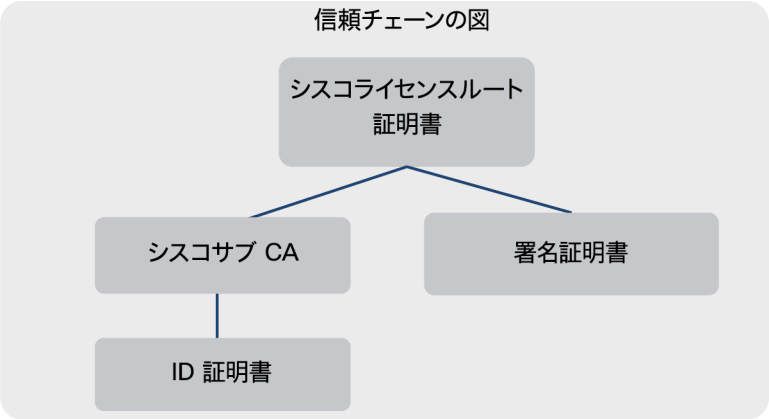
- お客様が Cisco SSM ポータルを使用してシスコスマートアカウントから ID トークンを取得します。
  - ID トークンは、お客様を安全に識別する手段です。
- お客様がシスコ製品で登録コマンドと ID トークンを使用して、シスコスマートエージェントで登録プロセスを開始します。
  - 注：登録が完了すると、ID トークンは不要になります。
- スマートエージェントが CSR（証明書署名要求）を生成します。
  - 署名は SHA256 です。
  - シスコ製品の UDI が CN（共通名）フィールドに入力されます。
- スマートエージェントが秘密キーと公開キーのペアを生成します。長さは 2048 です
  - シスコスマートエージェントが秘密キーを使用して要求メッセージに署名し、Cisco SSM に送信します。
  - 公開キーは CSR で送信され、スマートエージェントは秘密キーを信頼できるストアに保存します。
  - Cisco SSM が公開キーを使用して、受信したメッセージの署名を検証します。
- スマートエージェントが Cisco SSM への登録要求で以下を送信します。
  - CSR
  - ID トークン
  - ソフトウェア ID タグ
  - UDI
- 登録メッセージが、HTTPS と SOAP を使用する Smart Call Home コンポーネントを介して送信されます。
  - Smart Call Home は、HTTPS メッセージを保護するために、必要な証明書を PKI 信頼プールに送信する責任を負います。
- スマートエージェントは登録応答を受信すると、Cisco SSM に ACK を送信します。これにより Cisco SSM は、スマートエージェントが証明書を受信したことを認識します。

Cisco SSM ライセンスサーバーからの登録応答

- Cisco SSM が LCS を利用して 3 つの証明書と 1 つの公開キー/秘密キーのペアを作成します。
  - Cisco SSM が秘密キーを保存し、シスコ製品に送信する応答メッセージにこの秘密キーで署名します。
  - サブ CA
  - 署名証明書
    - シスコスマートエージェントが応答メッセージの署名を検証するために使用する公開キーが含まれています。
  - ID 証明書
- Cisco SSM が、この登録インスタンスを一意に識別するためにシスコ製品 ID（PIID）を作成します。
  - Cisco SSM が、自身のデータベース内の証明書、UDI、および PIID を関連付けます。
- Cisco SSM が証明書と PIID をシスコ製品に送り返します。
- スマートエージェントが、再起動後も使用できるように、自身の信頼されるストアにこの証明書と PIID を保存します。

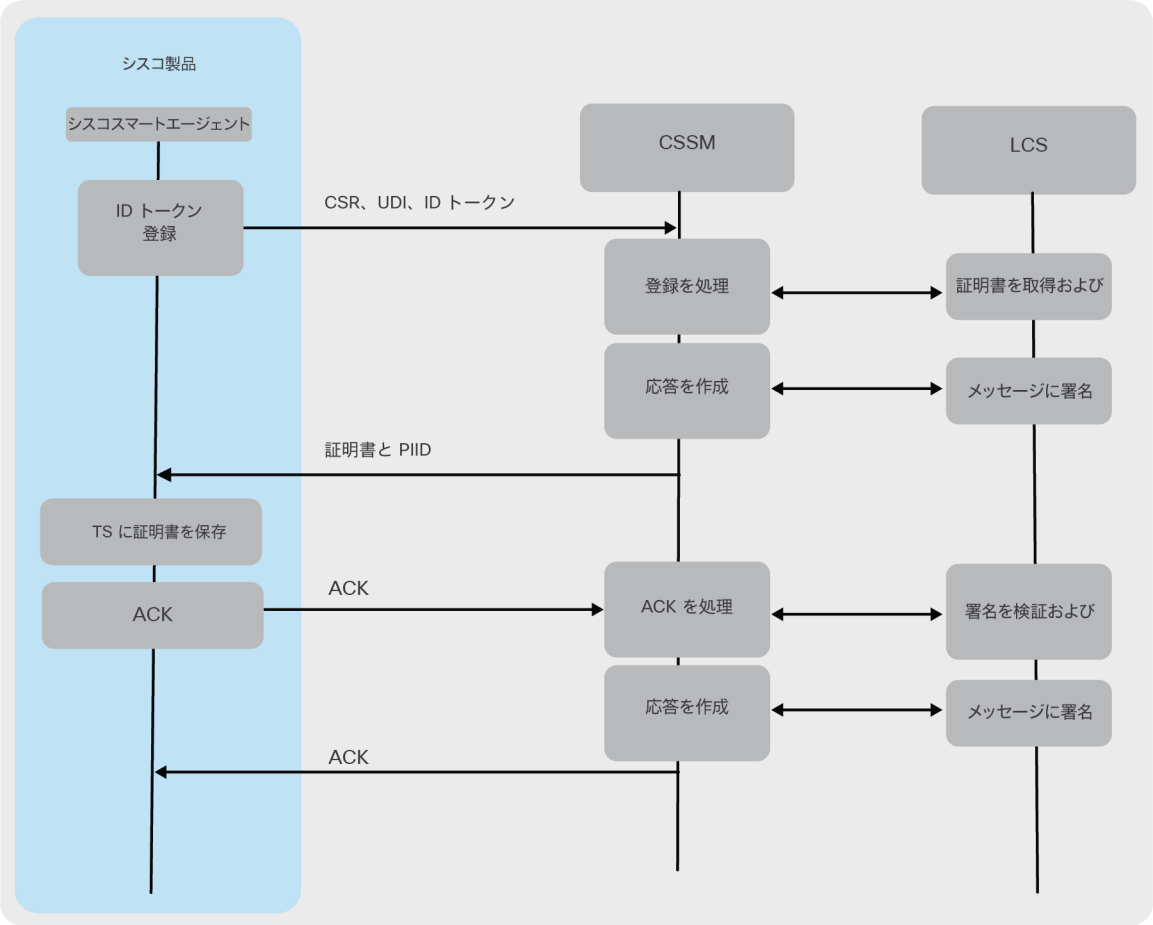
登録応答の検証

1. シスコスマートエージェントが、スマートエージェントコードに埋め込まれて難読化されているルート証明書も含めて、受け取った証明書の信頼チェーンを検証します。
2. ID 証明書の UDI とシスコ製品の UDI が一致することを検証します。



3. 信頼できるストアに証明書を保存します。
4. Cisco SSM に ACK を送信します。

登録フローを示す図



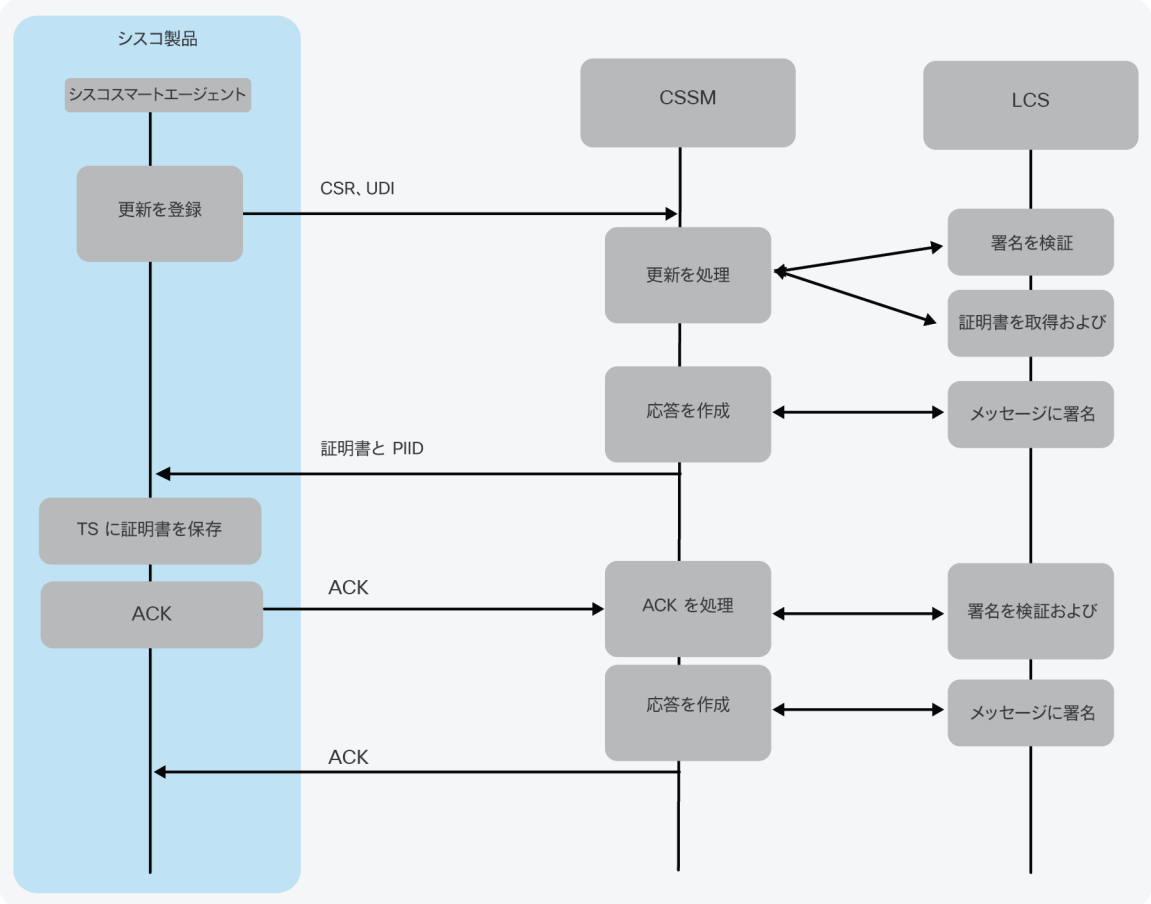
シスコ製品登録の更新

ID 証明書の有効期間は発行日から 1 年です。Cisco Smart Agent は、6 ヵ月後に証明書の更新を自動的に試みます。シスコスマートエージェントで更新がトリガーされた場合のフローは、登録フローとほぼ同じです。

- スマートエージェントが新しい CSR を生成します。
- スマートエージェントが新しい秘密キーと公開キーのペアを生成します。長さは 2048 です
- スマートエージェントが Smart Call Home サーバーを介して、更新要求で次の情報を Cisco SSM に送信します。
  - CSR
  - ソフトウェア ID タグ
  - UDI
  - 注：ID トークンはありません。ID トークンは、最初の登録が終了すると、使用も保存もされません。

- Cisco SSM が 3 つの新しい証明書と 1 つの公開キー/秘密キーのペアを作成します。
  - サブ CA
  - 署名証明書
  - ID 証明書
- Cisco SSM が証明書をシスコ製品に送り返します
- シスコスマートエージェントは登録応答を受信すると、Cisco SSM に ACK を送信します。これにより Cisco SSM は、スマートエージェントが証明書を受信したことを認識します。
- Cisco SSM がスマートエージェントに最終 ACK を返します。
- この時点で、スマートエージェントは古い証明書を削除し、新しい証明書の使用を開始します。
- スマートエージェントが新しい証明書を自身の信頼できるストアに保存します。
- このプロセスのどこかで通信障害が発生した場合、スマートエージェントは更新プロセスを最初からやり直し、最終 ACK を受信するまで古い証明書を使用し続けます。

更新フローを示す図



シスコ製品の証明書

- シスコライセンスルート証明書
  - シスコスマートエージェントを含むイメージに埋め込まれ、難読化されます。変更されることはありません。これが信頼チェーンのルートです。
- シスコサブ CA
  - シスコによって生成され、スマートエージェントに送信されます。
- ID（ノード）証明書
  - 登録時または更新時に Cisco SSM または SSM オンプレミス ライセンス サーバーで生成され、スマートエージェントに送信されます。
  - 有効期間は 1 年です。
  - ID 証明書にはシスコ製品の UDI も埋め込まれているため、正しいシスコ製品であることを確認できます。受信時および起動時に検証されます。
  - スマートエージェントは、この証明書を 6 ヵ月ごとに自動更新します。
- 署名証明書
  - 登録時または更新時に Cisco SSM または SSM オンプレミス ライセンス サーバーで生成され、スマートエージェントに送信されます。
  - Cisco Smart Agent が受信する応答メッセージの署名の検証に使用される Cisco SSM 公開キーが含まれています。

シスコ製品のメッセージへの署名

- シスコスマートエージェントの署名
  - シスコスマートエージェントは、登録中に生成した秘密キーを使用して、すべての送信要求メッセージに署名します。
  - Cisco SSM または SSM オンプレミス ライセンス サーバーは、登録中に CSR で送信された公開キーを使用して、受信したメッセージの署名を検証します。
  - SHA256 デジタル署名
- Cisco SSM による検証
  - 登録時の CSR の公開キーを使用して、受信した要求メッセージの署名を検証します。

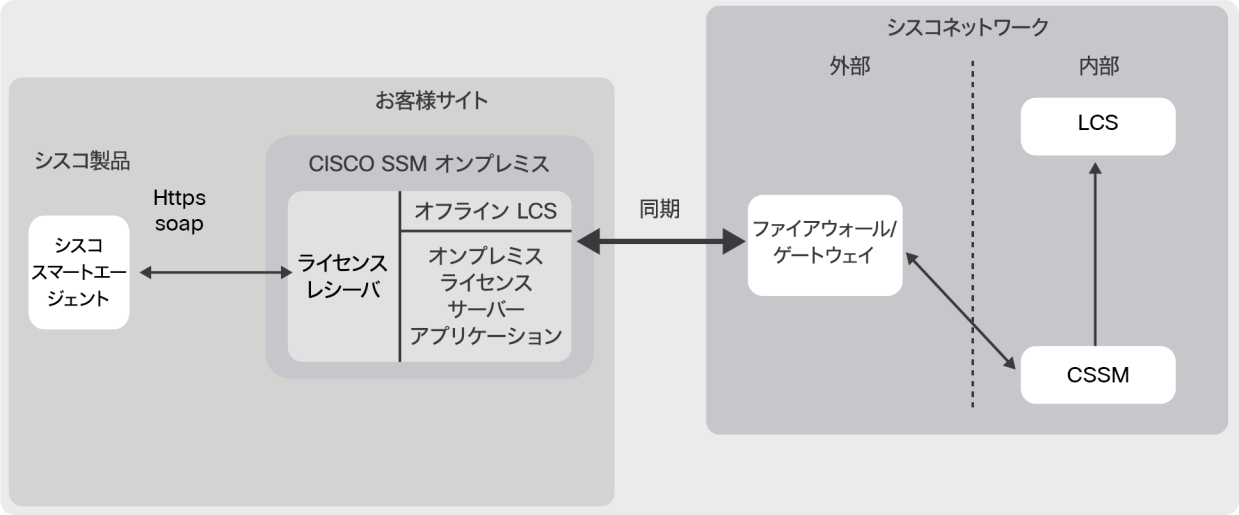
Cisco SSM ライセンスサーバーによるメッセージへの署名

- Cisco SSM によるメッセージへの署名
  - Cisco SSM は、登録中に生成した秘密キーを使用して、すべての送信応答メッセージに署名します。
  - シスコスマートエージェントは、登録中に受信した署名証明書に含まれている公開キーを使用して、受信したメッセージの署名を検証します。
  - SHA256 デジタル署名
- スマートエージェントによる検証
  - 登録時の CSR の公開キーを使用して、受信した要求メッセージの署名を検証します。

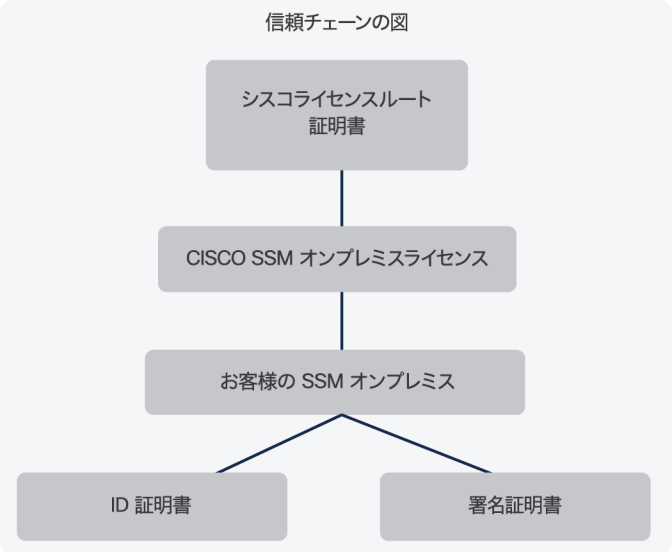
Cisco SSM オンプレミスプロトコルの概要

シスコスマートエージェントが Cisco SSM オンプレミス ライセンス サーバーに接続されている場合の証明書の使用方法は、上記の説明とほぼ同じです。このセクションでは、違いについて説明します。

Cisco SSM オンプレミス ライセンス サーバーのブロック図



エージェントが Cisco SSM オンプレミス ライセンス サーバーに接続されている場合は、作成される証明書が若干異なります。3 層の信頼チェーンではなく、4 層の信頼チェーンが使用されます。



Cisco SSM オンプレミス ライセンス サーバー証明書

- Cisco SSM オンプレミス ライセンス サーバー サブ CA
  - サテライト登録時に Cisco SSM で生成されます。Cisco SSM オンプレミス ライセンス サーバーに送信され、その後シスコスマートエージェントが Cisco SSM オンプレミス ライセンス サーバーに登録する際にエージェントに送信されます。
- お客様の SSM オンプレミス ライセンス サーバー サブ CA
  - Cisco SSM オンプレミス ライセンス サーバーの登録時に Cisco SSM で生成されます。Cisco SSM オンプレミス ライセンス サーバーに送信され、その後シスコスマートエージェントが Cisco SSM オンプレミス ライセンス サーバーに登録する際にエージェントに送信されます。

登録要求ファイル

SSM オンプレミス ライセンス サーバーを Cisco SSM に最初に登録するときに、Cisco SSM オンプレミス ライセンス サーバーは、スマートアカウント内の特定のバーチャルアカウントへのリンクを確立するために Cisco SSM に登録ファイルを送信します。登録ファイルには、表 1 に示す主要な情報と 3 つの証明書署名要求（CSR）が含まれています。CSR はシスコによって署名され、Cisco SSM オンプレミス ライセンス サーバーで使用するために返されます。

表 1. 登録要求ファイルのコンポーネント

コンポーネント	説明
instance_id:	Cisco SSM オンプレミス ライセンス サーバーの 128 ビットの汎用一意識別子。Open Software Foundation によって標準化されています。詳細については、IEEE RFC122 を参照してください。
exported_timestamp:	登録要求ファイル作成時のタイムスタンプ。
lcs_csr:	LCS（ライセンス暗号化サービス）への証明書署名要求。シスコ製品が Cisco SSM オンプレミス ライセンス サーバーとの信頼を確立するために使用する IDCERT への署名に使用されます。
tg_csr:	Cisco SSM オンプレミス ライセンス サーバーとシスコ製品間の HTTPS 通信を保護するために使用される証明書署名要求。
ssms_csr:	Cisco SSM オンプレミス ライセンス サーバーのユーザーインターフェイスとブラウザ間の HTTPS 通信を保護するために使用される証明書署名要求。

承認応答ファイル

登録要求ファイルの受信時に、Cisco SSM は、Cisco SSM オンプレミス ライセンス サーバーの UUID をターゲットのバーチャルアカウントに関連付け、承認応答ファイルを作成します。このファイルには、Cisco SSM オンプレミス ライセンス サーバーを完全に動作可能な状態にするために必要なキー情報が含まれています。承認応答ファイルには、シスコ製品（PI）の登録に必要な、シスコによって署名された 8 種類の証明書が含まれていることに注目してください。

表 2. 承認応答ファイルの証明書

証明書	説明
id_cert:	Cisco SSM オンプレミス ライセンス サーバーは、この証明書を使用してすべてのシスコ製品を識別します。CSSM は、この証明書を使用して Cisco SSM オンプレミス ライセンス サーバーを識別します。この証明書は、Cisco SSM オンプレミス ライセンス サーバーと CSSM が同期するたびに更新されます。
sub_ca_cert:	すべてのシスコ製品にインストールされているライセンスエージェントは、この証明書を使用してサブ CA を識別します。
signing_cert:	Cisco SSM オンプレミス ライセンス サーバーは、この証明書を使用して、**id_cert** が **license_root_ca** によって署名されていることを検証します。
local_sub_ca_cert_1_1:	ローカル SSM オンプレミス ライセンス サーバー LCS と Cisco SSM オンプレミス ライセンス サーバーは、この証明書を使用して 4 層のシスコ製品の登録を処理します。 3 層および 4 層証明書の詳細については、「**3 層証明書と 4 層証明書**」セクション（9 ページ）を参照してください。 LCS は、この証明書を使用して、製品へのデータ送信時に **id_cert** に署名します。登録応答ファイルは **sub_ca_cert** を返します。
tg_ssl_cert:	トランスポートゲートウェイ（TG）はこの証明書を使用して、セキュアな接続を受け入れ、セキュアな接続（HTTPS）経由で通信します。
tg_issuer_cert:	TG はこの証明書を使用して CA 発行者の階層を確立します。たとえば、（TG ソースコードに埋め込まれている）ライセンスルート証明書が **tg_issuer_cert** を発行し、この証明書が **tg_ssl_cert** を発行します。

証明書	説明
satellite_cert:	オンライン LCS はこの証明書を使用してローカルオフライン LCS 用の **local_sub_ca_cert_1_1** に署名します。
ssms_ssl_cert:	SSM オンプレミス ライセンス サーバーは、この証明書を使用してセキュアな接続を受け入れ、Web ブラウザがセキュアな接続（HTTPS）を介して SSM オンプレミス ライセンス サーバーと通信できるようにします。

CSSM は、割り当てられたシスコスマートアカウントと SSM オンプレミス ライセンス サーバーの情報も返します。

キー	説明
status:	登録の成功または失敗のステータス
uuid:	この SSM オンプレミス ライセンス サーバーに割り当てられた ID
smart_account:	登録先のシスコスマートアカウントの名前
account_domain:	スマートアカウントに関連付けられたドメイン
satellite_name:	登録されたローカルアカウントの名前

同期要求ファイル

Cisco SSM オンプレミス ライセンス サーバーは、CSSM と同期する際に、同期要求ファイルを CSSM に送信します。このファイルには、登録された製品とライセンスの使用状況に関する情報が含まれおり、CSR と 2 つの証明書が CSSM に送信されます。

表 3. 同期要求ファイルのコンポーネント

コンポーネント	説明
sync_version:	CSSM との同期コードのバージョン
ssms_version:	Cisco SSM オンプレミス ライセンス サーバーのバージョン
id_cert, signing_cert:	CSSM はこれらの証明書を使用して、SSM オンプレミス ライセンス サーバーが有効であることを確認します。
collector_id	この SSM オンプレミス ライセンス サーバーを一意に識別するために使用される UUID
csr (lcs csr):	この CSR は使用されなくなりました。
tg_csr:	SSM オンプレミス ライセンス サーバーは、自身の IP アドレスが変更されるたびに、この CSR を CSSM に送信します。この CSR は、製品と SSM オンプレミス ライセンス サーバー間にセキュアな通信を確立するために使用されます。
ssms_csr:	SSM オンプレミス ライセンス サーバーは、管理者の IP アドレスが変更された場合、または SSM オンプレミス ライセンス サーバーが別のホスト（別の IP アドレス）に復元された場合にのみ、この CSR を CSSM に送信します。ブラウザから SSM オンプレミス ライセンス サーバーにアクセスします。
last-sync:	SSM オンプレミス ライセンス サーバーと CSSM が最後に同期されたときのタイムスタンプ。その同期以降の新しいデータの識別に使用されます。

コンポーネント	説明
last_generated:	同期要求ファイルが最後に生成されたときのタイムスタンプ。変更されたデータの識別に使用されます。
virtual_accounts:	SSM オンプレミス ライセンス サーバーに登録されているバーチャルアカウント、製品、およびライセンス。

同期要求ファイルには、基本的な同期制御情報に加えて、シスコバーチャルアカウントの更新に使用される製品とライセンスの使用状況の情報も含まれています。表 4 に、同期要求ファイルのバーチャル アカウント セクションのコンポーネントを示します。

表 4. 同期要求ファイルのバーチャルアカウントのセクション

コンポーネント	説明
:id:	Cisco SSM オンプレミス ライセンス サーバーの登録先のバーチャルアカウントを識別するために使用される一意の番号。
:name:	登録時またはそれ以降（CSSM ポータルで変更された場合）に、SSM オンプレミス ライセンス サーバーに付けられた名前。
:product_instances:	SSM オンプレミス ライセンス サーバーに登録されている製品を識別する YAML セクションの開始部。
:id:	あるシスコ製品を識別するために SSM オンプレミス ライセンス サーバーによって割り当てられた一意の番号。各シスコ製品には、製品の登録時に番号が割り当てられます。
:is_active:	製品が現在登録されている場合は true、シスコバーチャルアカウントから削除される場合は false。
:software_tag_identifier:	ISO 19770 で定義されている、製品のエンタイトルメントを識別するためのソフトウェアタグ。
:udi_pid:	製品識別子（PID）。
:hostname:	製品に設定されているホスト名。*1
:ip_address:	ライセンスを使用しているデバイスの IP アドレス。*1
:mac_address:	ライセンスを使用するデバイスの MAC アドレス。*1
:host_identifier:	未使用。
:license:	製品によって使用されているライセンスをリストする YAML セクションの開始部。
:id:	使用されているライセンスを識別するために登録製品によって使用される一意の番号。この番号は、SSM オンプレミス ライセンス サーバーによって割り当てられます。
:tag:	ISO 19770 で定義されている、製品によって使用されているライセンスを識別するためのソフトウェアタグ。
:consumed_quantity:	使用中のライセンスの数。

*1. デフォルトでは、ホスト名、IP アドレス、MAC アドレスが要求とともに送信されます。同期要求ファイルにこの情報を含めたくない場合は、データプライバシー設定を使用して無効にできます（『SSM オンプレミス ライセンス サーバー ユーザー ガイド』を参照してください）。

同期応答ファイル

Cisco SSM オンプレミス ライセンス サーバーから同期要求ファイルを受信した後、CSSM は承認のために同期応答を送信し、SSM オンプレミス ライセンス サーバーと同期します。

完全な同期は、SSM オンプレミス ライセンス サーバーが最初に CSSM に登録されたときに行われ、同期応答ファイルに反映されます。同期応答ファイルの同期セクションの内容は、承認ファイルの同期部分と同期応答ファイルの両方で同じです。

SSM オンプレミス ライセンス サーバーが CSSM に定期的な同期を要求すると、CSSM は同期応答ファイルで、証明書情報とバーチャルアカウントとライセンスに関する情報を SSM オンプレミス ライセンス サーバーに返します。

表 5 に、同期応答ファイル内の証明書を示します。

表 5. 同期要求ファイルの証明書

証明書	説明
id_cert	CSSM はこれらの証明書を使用して、Cisco SSM オンプレミス ライセンス サーバーが有効であることを確認します。
sub_ca_cert:	すべてのシスコ製品にインストールされているライセンスエージェントは、この証明書を使用してサブ CA を識別します。
signing_cert:	Cisco SSM オンプレミス ライセンス サーバーは、この証明書を使用して、id_cert が **license_root_ca** によって署名されていることを確認します。
local_sub_ca_cert:	SSM オンプレミス ライセンス サーバーと LCS は、この証明書を使用して 3 層シスコ製品の登録を処理します。この証明書が同期応答ファイルに含まれるのは、SSM オンプレミス ライセンス サーバーが登録されてから 48 時間以上経過した場合のみです。 3 層および 4 層証明書の詳細については、「**3 層証明書と 4 層証明書**」セクション（9 ページ）を参照してください。
local_sub_ca_cert_1_1:	ローカル SSM オンプレミス ライセンス サーバー LCS と SSM オンプレミス ライセンス サーバーは、この証明書を使用して 4 層のシスコ製品の登録を処理します。 LCS は、この証明書を使用して、製品へのデータ送信時に **id_cert** に署名します。登録応答ファイルは **sub_ca_cert** を返します。
tg_ssl_cert:	トランスポートゲートウェイ（TG）はこの証明書を使用して、セキュアな接続を受け入れ、セキュアな接続（HTTPS）経由で通信します。
tg_issuer_cert:	TG はこの証明書を使用して CA 発行者の階層を確立します。たとえば、TG ソースコードに埋め込まれているライセンスルート証明書が **tg_issuer_cert** を発行し、この証明書が **tg_ssl_cert** を発行します。
satellite_cert:	オンライン LCS はこの証明書を使用してローカルオフライン LCS 用の **local_sub_ca_cert_1_1** に署名します。
ssms_ssl_cert:	SSM オンプレミス ライセンス サーバーはこの証明書を使用して、ユーザーの Web ブラウザと Cisco SSM オンプレミス ライセンス サーバー（HTTPS）の間にセキュアな接続を確立します。現在は使用されていません。

表 6. 同期応答ファイルの補足コンポーネント

コンポーネント	定義
collector_instance_id:	SSM オンプレミス ライセンス サーバーを一意に識別するために、この SSM オンプレミス ライセンス サーバーに割り当てられた ID。
satellite_name:	[**管理（Administration）**] ワークスペースで設定した SSM オンプレミス ライセンス サーバー名。
last_generated:	同期要求ファイルが最後に生成されたときのタイムスタンプ。変更されたデータの識別に使用されます。
last-sync:	SSM オンプレミス ライセンス サーバーと CSSM が最後に同期されたときのタイムスタンプ。その同期以降の新しいデータの識別に使用されます。
Synchronization:	SSM オンプレミス ライセンス サーバーに登録され、CSSM に同期されているシスコ製品、タイプ、およびライセンスを識別する行。
virtual_accounts:	SSM オンプレミス ライセンス サーバーに登録され、CSSM に同期されているシスコバーチャルアカウントを識別する行。

サードパーティプロバイダーの情報

Cisco SSM は、Cisco SSM オンプレミス ライセンス サーバーとの完全な同期中に、同期応答ファイルでプロバイダー情報を送信できます。プロバイダー情報には、SpeechView、Apple Push Notifications、PnP それぞれのサードパーティサポート状況を含めることができます。

Device-Led Conversion（DLC）

Device-Led Conversion（DLC）サポートを使用する場合、Cisco SSM は、同期応答ファイルの device_conversion_response: セクションで Cisco SSM オンプレミス ライセンス サーバーの変換情報を提供します。device_conversion_response: セクションには、DLC を開始した Cisco SSM オンプレミス ライセンス サーバーに登録済みの各シスコ製品のステータス情報がリストされます。

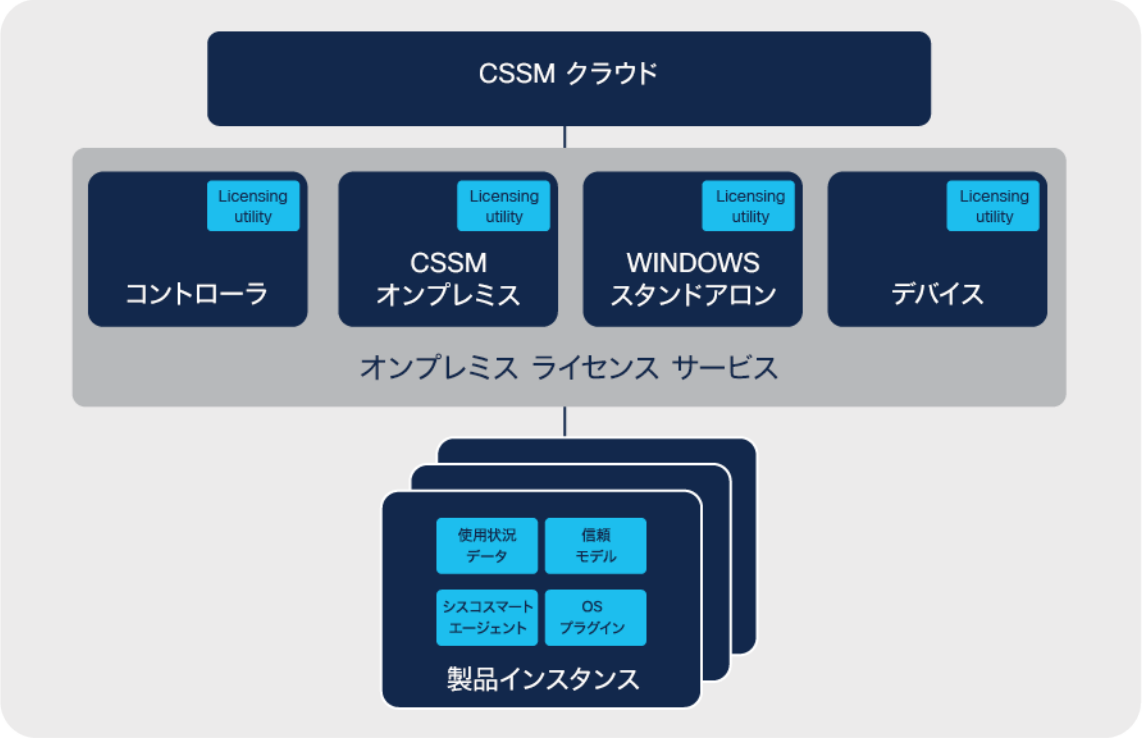
表 7. 同期応答ファイルの DLC セクションのコンポーネント

コンポーネント	説明
:udi_pid:	製品の識別子。
:udi_serial_number:	PI のシリアル番号。
:conversion_status:	変換が完了したか失敗したかを示します。
:status_message:	変換が失敗した場合、このフィールドには変換失敗の理由に関する情報が表示されます。変換が完了した場合、このフィールドは空白になります。
:status_message_localized:	変換が失敗した場合、このフィールドには変換失敗の理由に関する情報がローカライズされた言語で表示されます。変換が完了した場合、このフィールドは空白になります。
:software_tag_identifier:	**udi_pid** にロードされたソフトウェアの識別タグ。

Cisco Smart License Using Policy

Smart Licensing の新しい導入方法では、エンドカスタマーによるライセンスのアクティベートと管理が簡素化されます。Smart Licensing がよりシンプルかつ柔軟なオファー構造をサポートするようになったため、お客様はより簡単かつ迅速に、一貫した方法でライセンスを購入、更新、アップグレードできるようになりました。

- 製品の起動時に評価モードなし、cisco.com への登録は不要
- デバイスごとのシスコクラウドとの継続的な通信はなし
- ソフトウェア使用状況の報告は必要
- ネットワーク導入の運用コストなし



製品からシスコに送信される情報

製品から送信される情報には、使用状況データとリターンコードの両方が含まれます。この情報は製品によって署名され、シスコによって検証されるため、レコード処理の前にデータの整合性が確保されます。

- **デフォルトの署名キー：**各シスコ製品には製品固有のキーがあります。
- **製品署名キー：**シスコ製品がシスコと通信するときは、通信を保護するために非対称キーが使用されます。各製品には一意の秘密キー（RSA-2048）があり、このキーを使用してシスコに送り返すデータに署名できます。このキーは認証され、シスコルートに関連付けられます。

シスコから製品に返される情報

すべての特権承認は、シスコによって署名が行われ、承認されたエンティティに関連付けられる必要があります。承認の範囲には、適用されるライセンスの使用権や、適用されるライセンスの無制限の使用を許可するポリシーが含まれることがあります。いずれの場合も、このドキュメントでは、シスコがこれらの承認を生成する唯一の機関であることを前提としています。署名の安全性を確保するために、シスコはレコードへの署名に使用される秘密キー

（ECDSA）を所有します。これらの署名済みレコードを受信するクライアントは、シスコルート、およびこれらの署名の検証に使用できる公開証明書を保有します。

オンプレミス ライセンス サービスの使用

シスコは、Cisco Smart Licensing Utility（CSLU）、スタンドアロンの Windows アプリケーション、および SSM オンプレミス ライセンス サーバーを通じて、ライセンスの使用状況を収集およびレポートする機能を提供します。これらの各ソフトウェアオプションは、使用状況データをレポートするためのオンラインまたはオフラインの接続モデルをサポートできます。

Cisco SSM オンプレミス ライセンス サーバー

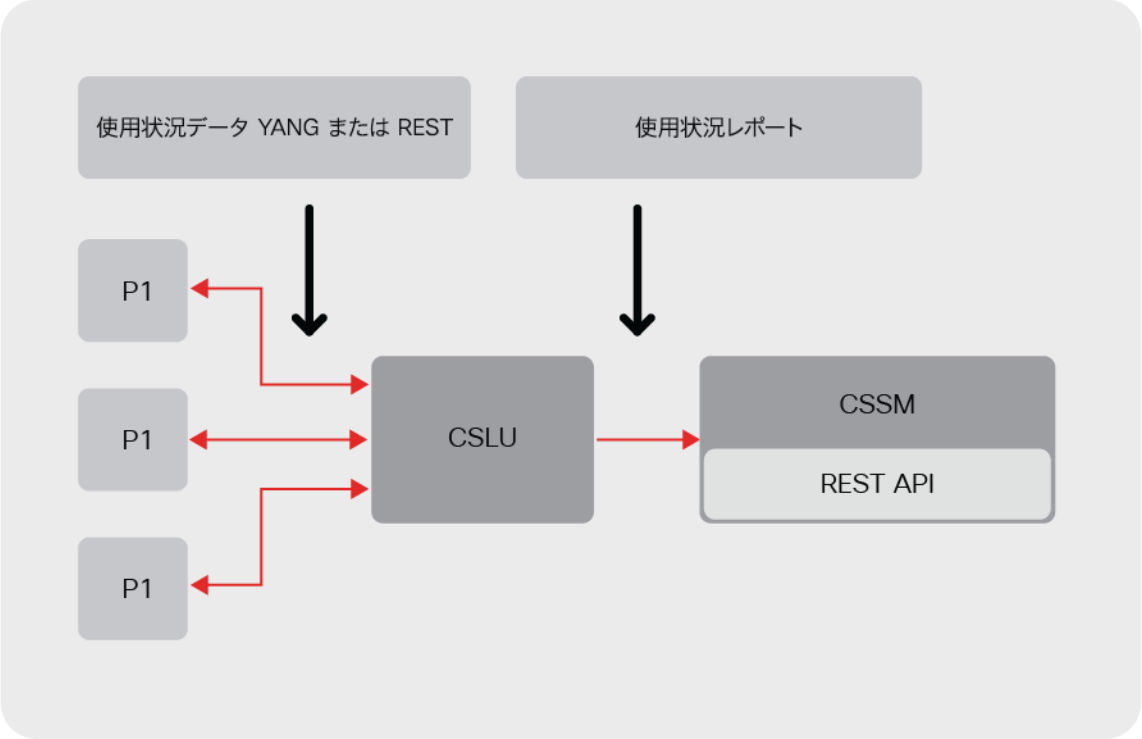
Cisco SSM オンプレミスを使用している場合、Cisco SSM オンプレミスは現在スマートライセンスをサポートしているため、Smart License Using Policy 機能をサポートして使用状況データの収集とレポートを自動化します。

Cisco DNA Center（DNAC）ライセンスサービスの使用

シスコは、Cisco DNA Center（DNAC）を使用してライセンス使用状況データを収集する機能と、CSLU にレポートする機能を提供します（動作は以下の図を参照）。この機能とセキュリティの詳細については、DNAC の製品資料を参照してください。

Cisco Smart License Utility（CSLU）

Cisco Smart Licensing Utility は、「ストアアンドフォワード」型の Windows アプリケーションです。このアプリケーションを使用すると、シスコ製品からライセンス使用状況データを収集し、シスコ ライセンス サーバーに送信して準拠状況を可視化できます。



CSLU の使用状況レポート形式は、ISO 19770-4 標準 RUM レポート形式に基づいています。JSON 形式で提供され、信頼モデルごとに署名されます。使用状況レポートは、最初に SHA-256 を使用してハッシュ化されます。次にこのハッシュは、デフォルトの署名キーまたは製品署名キーから提供されたキーを使用して署名されます。

ID トークンの登録と Smart License Using Policy

このモデルでは、登録や ID トークンは必要ありません。ただし、後方互換性を確保するために、お客様は現在の ID トークンをオプションとして使用し、オンラインで CSSM との信頼を確立して、署名付きメッセージを交換できます。このモードでは、登録の有効期限切れ、承認の更新、登録の更新、登録済み状態という概念はありません。

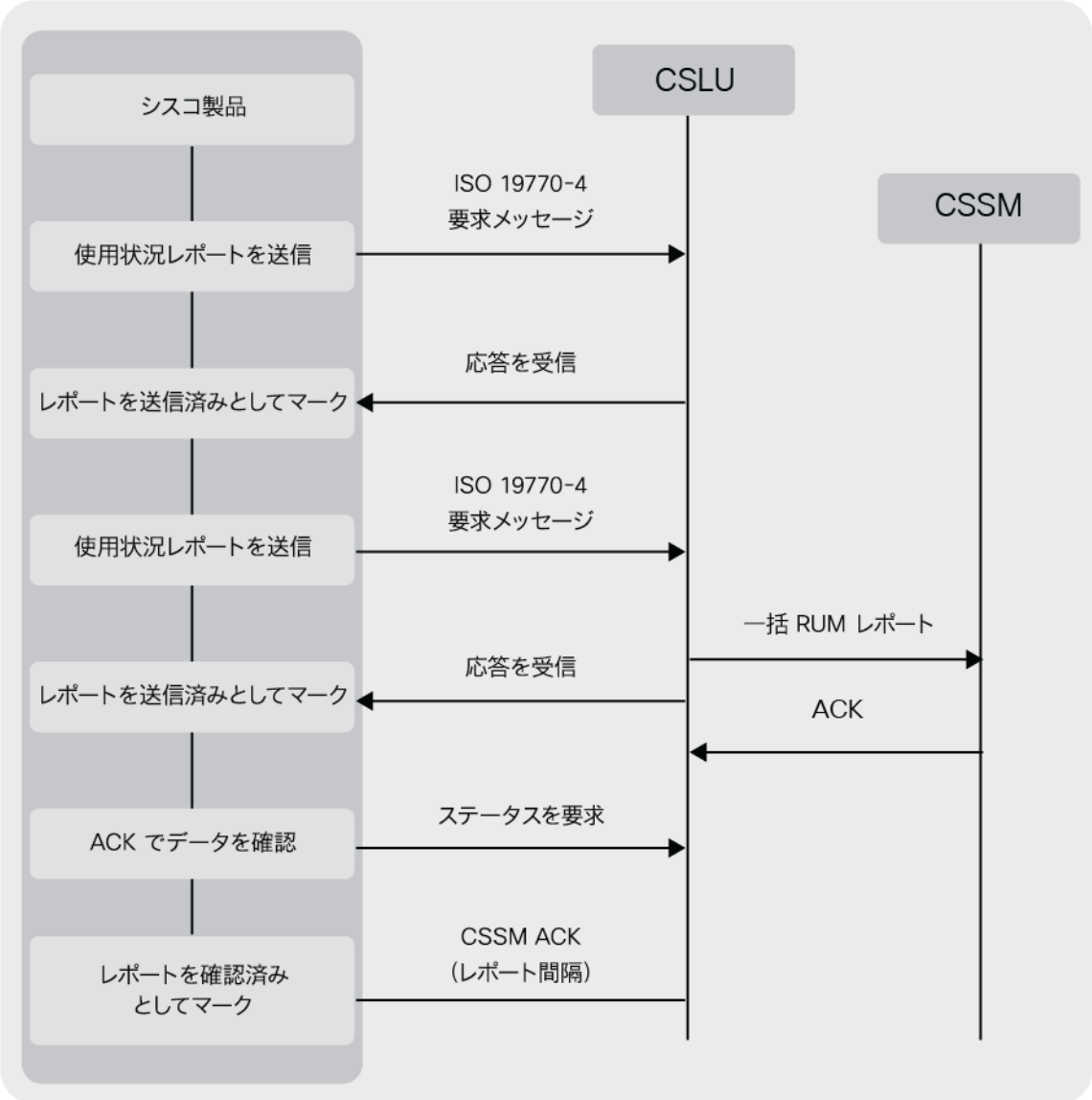
製品からの使用状況データの送信

製品が使用状況レポートを CSLU REST エンドポイントに直接送信する際、製品には次のオプションを設定する必要があります。

CSLU エンドポイント

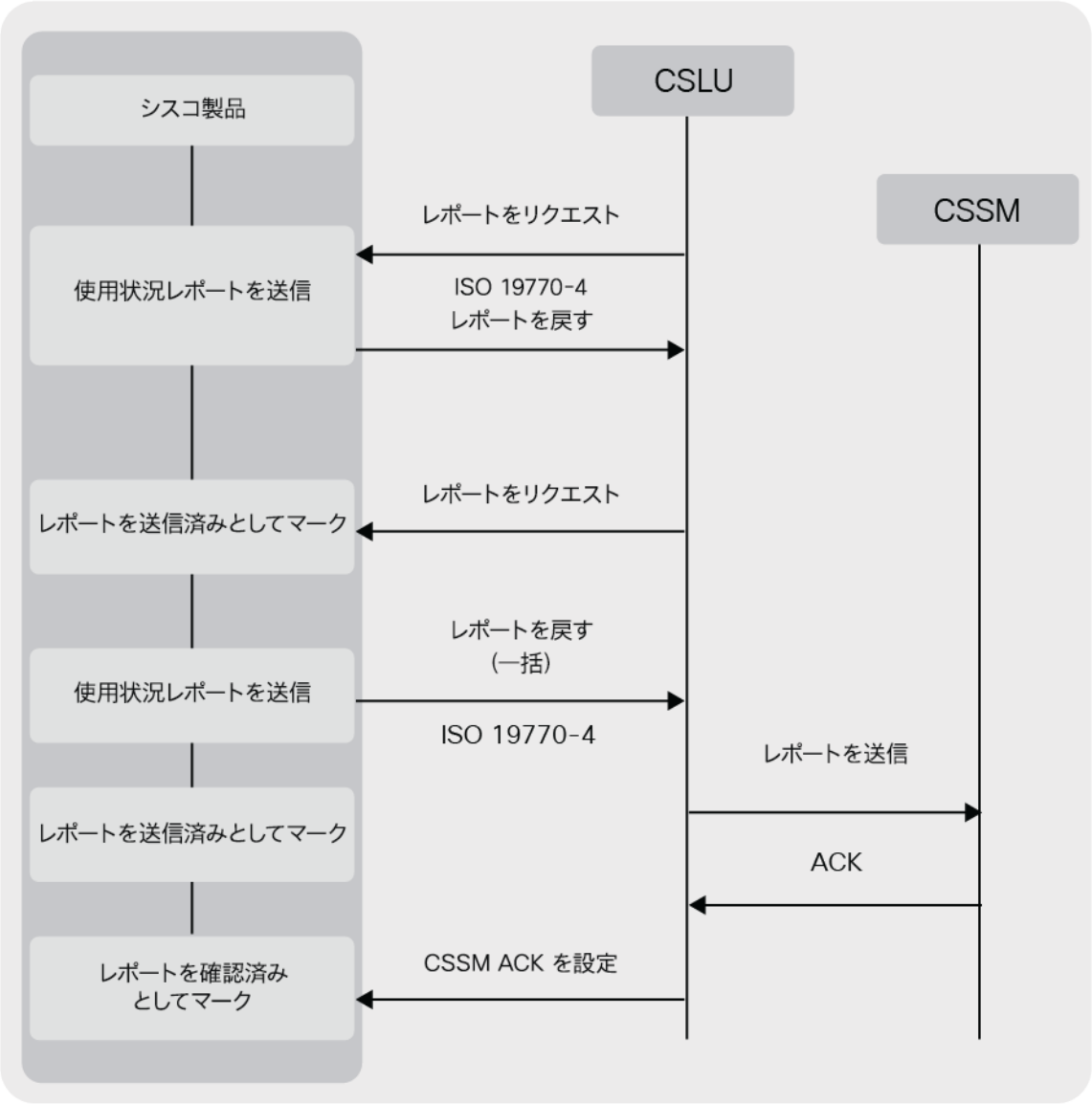
レポート期間の間隔の設定

製品は、多くの使用状況レポートで構成される単一の使用状況レポートを作成し、CSLU に送信します。また、定期的なスケジュールで CSLU にポーリングして ACK 応答を受け取ります。



CSLU による使用状況レポートの取得

CSSM との通信は、オンラインの場合もオフラインの場合もあることに注意してください。CSLU は、（存在する場合）すべての ACK 応答を製品に送信します。



ライセンスポリシー

ライセンスポリシーには、ライセンス エンタイトルメント パラメータ（初回レポート、レポート頻度、レポート適用、更新時の機能適用、輸出分類、過剰使用など）も含まれています。パラメータにはデフォルトセットがありますが、お客様の EA（シスコ エンタープライズ アグリーメント）や、シスコとのその他のライセンス契約に固有のパラメータもあります。

信頼モデル

通信は、製品と Cisco Smart Licensing Utility（CSLU）間、および CSLU から Cisco SSM（クラウド）の間に確立されます。製品から CSLU への通信の信頼手法は、お客様のネットワークの一部としてお客様の責任とみなされます。CSLU から Cisco OAUTH への通信の信頼手法は、現行の Cisco SSM-Cloud API で使用されている手法です。ライセンス使用状況データは、次のいずれかの方法で署名されます。

1. 信頼コードのインストール。
   a. 工場出荷時の登録（オフラインでの信頼の確立）により、公開キーと秘密キーのペアが設定され、信頼コードがインストールされます。秘密キーは、使用状況レポートの署名に使用されます。
   b. 製品の秘密キーがローカルの信頼されるストアに保存されるため、この方法はかなり安全です。
   c. この方法では、製造時に製品にインストールされる信頼コードを使用します。
2. 製品の信頼ストアに保存されるキー。
   a. 製品は HMAC-SHA246 署名アルゴリズムを使用します。
   b. 製品のライセンスタイプごとに異なるキーがあります。
   c. シスコによって生成、暗号化、base64 エンコードが行われます。

Smart License Using Policy の基本的なレポートのルール

製造工程を経る製品には、購入されたライセンスを説明する情報が製品にインストールされます。製造プロセス中に、これらの購入済みライセンスは使用中として自動的にレポートされます。インストール済みポリシーによって、継続的なレポートの必要性が定義されます。

通常は次のようになります。

1. 製品が「購入されたライセンスの情報」に記載されている数より多い数のライセンスを使用していなければ、上記の「購入されたライセンスの情報」に含まれている永続ライセンス/エンタイトルメントについては、レポートは不要です。
2. 製品が「購入されたライセンスの情報」に記載されている数より多くのライセンスを使用している場合、またはライセンスが「購入されたライセンスの情報」に含まれていない場合は、サブスクリプション ライセンスと永続ライセンスについてのレポートが必要です。

参考資料

1. Cisco Security [英語]
   (https://tools.cisco.com/security/center/home.x)
2. Cisco Root CA 2048 Certification Practice Statement [英語]
   (https://www.cisco.com/security/pki/policies/CiscoRootCA2048-CPS.pdf)
3. Cisco Security Vulnerability Policy [英語]
   (https://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html)
4. Vendor Vulnerability Reporting and Disclosure Policy [英語]
   (https://www.cisco.com/c/en/us/about/security-center/vendor-vulnerability-policy.html)
5. Third-Party Code Attestation Policy [英語]
   (https://www.cisco.com/c/en/us/about/security-center/third-party-attestation-policy.html)
6. Trust Center
   (https://www.cisco.com/c/ja_jp/about/trust-center.html)
7. Cisco Secure Development Lifecycle
   (https://www.cisco.com/c/ja_jp/about/trust-center/technology-built-in-security.html)

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C11-743812-01 12/20