ライセンス：スマート ソフトウェア ライセンシング

スマート ソフトウェア ライセンシングによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンス キーを管理しなくても、簡単に ASA を導入したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

（注） スマート ソフトウェア ライセンシングは、ASA ハードウェアモデルおよび ISA 3000 ではサポートされていません。PAK ライセンスを使用します。PAK ライセンスについてを参照してください。

プラットフォーム別のスマートライセンスの機能と動作の詳細については、「Smart Enabled Product Families」を参照してください。

スマート ソフトウェア ライセンスについて

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、これは安全です。ユーザがアクセスできるものを制御できます。スマート ライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェア ライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンスを使用するには、まず Cisco Software Central でスマートアカウントを設定する必要があります（software.cisco.com）。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Firepower 4100/9300 シャーシの ASA のスマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ 上の ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 4100/9300 シャーシ スーパバイザと ASA に分割されています。

- Firepower 4100/9300 シャーシ：Smart Software Manager との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャをシャーシで設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。

（注） シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマート ライセンス方式を有効にする必要があります。

- ASA アプリケーション：ASA のすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、オプションで追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社ごとにアカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびデバイスの管理をより簡単に行うことができます。

オフライン管理

デバイスにインターネットアクセスがなく、Smart Software Manager に登録できない場合は、オフラインライセンスを設定できます。

永続ライセンス予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、Smart Software Manager への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様にライセンスを購入し、ASA のライセンス キーをインストールします。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用します。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。

ASAv 永続ライセンスの予約

権限付与に固有のライセンスを取得することで、標準層、権限付与に応じた最大スループット、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアントの機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- 100 Mbps の権限付与
- 1 Gbps の権限付与
- 2 Gbps の権限付与
- 10 Gbps の権限付与
- 20 Gbps の権限付与

ASAv の展開時に使用する権限付与レベルを選択する必要があります。その権限付与レベルによって、要求するライセンスが決まります。ユニットの権限付与レベルを後で変更したい場合

は、現在のライセンスを返却し、正しい権限付与レベルの新しいライセンスを要求する必要があります。展開済みの ASAv のモデルを変更するには、新しい権限付与の要件に合わせるために、ハイパーバイザから vCPU と DRAM の設定を変更します。各値については、ASAv のクイックスタートガイドを参照してください。

ライセンスの使用を停止した場合、ASAv で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

永続ライセンスの予約は Azure ハイパーバイザではサポートされません。

Firepower 1000 永続ライセンスの予約

ライセンスを取得することで、標準層、Security Plus（Firepower 1010）、最大のセキュリティコンテキスト（Firepower 1100）、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect クライアント の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 2100 永続ライセンスの予約

ライセンスを取得することで、標準層、最大のセキュリティコンテキスト、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect クライアント の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。また、ASA の設定で権限付与を要求することにより、ASA でそれらの機能を使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 4100/9300 シャーシ 永続ライセンスの予約

ライセンスを取得することで、標準層、最大のセキュリティコンテキスト、キャリアライセンス、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）のすべての機能が有効になります。AnyConnect クライアント の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。ライセンスは Firepower 4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、Firepower 4100/9300 シャーシで戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Smart Software Manager オンプレミス

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager オンプレミスサーバー（旧「Smart Software サテライトサーバー」）をインストールできます。Smart Software Manager オンプレミスは、Smart Software Manager の機能の一部を提供します。これにより、すべてのローカルデバイスに不可欠なライセンシングサービスを提供できます。ライセンスの使用状況を同期するためにメインの Smart Software Manager に定期的に接続する必要があるのは、Smart Software Manager オンプレミスだけです。スケジュールに沿って同期するか、または手動で同期できます。

Smart Software Manager オンプレミスでは、次の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-prem を参照してください。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのデバイスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシ 上で動作する ASA の場合：シャーシのみがデバイスとして登録される一方で、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3 つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

評価ライセンス

ASAv

ASAv は、評価モードをサポートしません。Smart Software Manager への登録の前に、ASAv は厳しいレート制限状態で動作します。

Firepower 1000

Firepower 1000 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 1000 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Firepower 2100

Firepower 2100 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 2100 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Firepower 4100/9300 シャーシ

Firepower 4100/9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシレベル評価モード：Firepower 4100/9300 シャーシ は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシ が Smart Software Manager に登録された後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録して永続ライセンスを取得する必要があります。

ライセンスについて（タイプ別）

ここでは、ライセンスに関する追加情報をタイプ別に説明します。

AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス

AnyConnect Plus または AnyConnect Apex ライセンスは、ライセンスで指定されたユーザープールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。AnyConnect VPN Only ライセンスは、特定の ASA に適用されます。スマート ライセンスを使用するデバイスでは、実際のプラットフォームに AnyConnect ライセンスを物理的に適用する必要はありません。ただし、同じライセンスを購入して、ソフトウェア センターへのアクセスやテクニカル サポートを使用するために契約番号を Cisco.com ID に関連付ける必要があります。詳細については、以下を参照してください。

- 『Cisco AnyConnect Ordering Guide』
- AnyConnect Licensing Frequently Asked Questions (FAQ)

その他の VPN ライセンス

その他の VPN セッションには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- VPN セッションの最大数の合計が、VPN AnyConnect とその他の VPN セッションの最大数よりも多くなっても、組み合わせたセッション数が VPN セッションの制限を超えることはできません。VPN の最大セッション数を超えた場合、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。
- クライアントレス SSL VPN セッションを開始後、ポータルから AnyConnect クライアント クライアントセッションを開始した場合は、合計で 1 つのセッションが使用されます。これに対して、最初に AnyConnect クライアント を（スタンドアロンクライアントなどから）開始後、クライアントレス SSL VPN ポータルにログインした場合は、2 つのセッションが使用されます。

暗号化ライセンス

高度暗号化：ASAv

Smart Software Manager または Smart Software Manager オンプレミスサーバーに接続する前に、管理接続に高度暗号化（3DES/AES）を使用できるため、ASDM を起動して Smart Software Manager に接続することが可能です。（VPN などの）高度暗号化を必要とする through-the-box トラフィックの場合、Smart Software Manager に接続して高度暗号化ライセンスを取得するまで、スループットは厳しく制限されます。

スマート ソフトウェア ライセンシング アカウントから ASAv の登録トークンを要求する場合、[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（お使いのアカウントでその使用が許可されている必要があります）。ASAv が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASAv はライセンスを保持し、レート制限状態に戻ることはありません。ASAv を再登録し、エクスポート コンプライアンスが無効になっている場合、または ASAv を工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度暗号化なしで ASAv を登録し、後で高度暗号化を追加する場合は、新しいライセンスを有効にするために ASAv をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：アプライアンスモードの Firepower 1000、Firepower 2100

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

スマート ソフトウェア ライセンシング アカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASA を工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：プラットフォームモードの Firepower 2100

Smart Software Manager または Smart Software Manager オンプレミスサーバーに接続する前に、管理接続に高度暗号化（3DES/AES）を使用できるため、ASDM を起動することが可能です。ASDM アクセスは、デフォルトの暗号化を適用する管理専用インターフェイスでのみ使用できることに注意してください。高度暗号化ライセンスに接続して取得するまで、（VPN などの）高度暗号化を必要とする through the box トラフィックは許可されません。

スマート ソフトウェア ライセンシング アカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASA を工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：Firepower 4100/9300 シャーシ

ASA を論理デバイスとして展開すると、すぐに ASDM を起動できます。高度暗号化ライセンスに接続して取得するまで、（VPN などの）高度暗号化を必要とする through the box トラフィックは許可されません。

スマート ソフトウェア ライセンシング アカウントからシャーシの登録トークンを要求する場合、[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、高度暗号化（3DES/AES）ライセンスが適用されるようにします（お使いのアカウントでその使用が許可されている必要があります）。

ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。シャーシを再登録し、エクスポートコンプライアンスが無効になっている場合、またはシャーシを工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度な暗号化なしでシャーシを登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA アプリケーションをリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

DES：すべてのモデル

DES ライセンスはディセーブルにできません。3DES ライセンスをインストールしている場合、DES は引き続き使用できます。強力な暗号化だけを使用したい場合に DES の使用を防止するには、強力な暗号化だけを使用するようにすべての関連コマンドを設定する必要があります。

キャリア ライセンス

キャリア ライセンスでは、以下のインスペクション機能が有効になります。

- Diameter：Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。
- GTP/GPRS：GPRS トンネリングプロトコルは、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS、および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザー データ パケットの伝送にもトンネリング メカニズムを使用します。
- M3UA：MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバープロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザーパート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。
- CTP：SCTP（Stream Control Transmission Protocol）は RFC 4960 で説明されています。プロトコルは IP 経由のテレフォニー シグナリング プロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャにおける複数のインターフェイス用の転送プロトコルでもあります。

合計 TLS プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザー数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザー数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 次に例を示します。

```
interface gigabitethernet 0/0.100
vlan 100
```

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンス

ASAv のフェールオーバー ライセンス

スタンバイ ユニットにはプライマリ ユニットと同じモデル ライセンスが必要です。

Firepower 1010 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

両方の Firepower 1010 ユニットは、Smart Software Manager または Smart Software Manager オンプレミスサーバーに登録する必要があります。フェールオーバーを設定する前に、両方のユニットで標準ライセンスと Security Plus ライセンスを有効にする必要があります。

通常は、ユニットの登録時に両方のユニットが強力な暗号化トークンを取得する必要があるため、ASA で強力な暗号化（3DES/AES）機能ライセンスを有効にする必要もありません。登録トークンを使用する場合、両方のユニットに同じ暗号化レベルが設定されている必要があります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。この場合、フェールオーバーを有効にした後、アクティブユニットで有効にします。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブユニットのみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となり、高度暗号化トークンを使用する場合は、高度暗号化（3DES/AES）機能ライセンスを必要とする機能の設定変更を行えなくなりま

す。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 1100 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリ ユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

（注） フェールオーバーペアを形成する場合は、各 ASA に同じ暗号化ライセンスが必要です。スマート ライセンシング サーバに ASA を登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の 2 つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマートライセンシングサーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンシングサーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマート ライセンシング サーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクで AES/3DES を使用するには、両方のユニットをリロードする必要があります。1 つのユニットだけをリロードすると、そのユニットは AES/3DES を使用しようとしますが、元のユニットは DES を使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- Standard：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Stardard ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Standard ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - 標準ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1120 ユニットの場合、それらのライセンスで最大 4 つのコンテキストが追加されます。アクティブ/スタンバイペアのアクティブな装置に 3 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 7 つのコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が 5 なので、結合されたライセンスでは最大 5 つのコンテキストのみ許可されます。この場合、アクティブな Context ライセンスを 1 つのコンテキストとしてのみ設定することになる場合があります。
  - 標準ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1140 ユニットの場合、それらのライセンスで最大 4 つのコンテキストが追加されます。アクティブ/アクティブペアのプライマリユニットに 4 Context ライセンスを設定します。

この場合、集約されたフェールオーバーライセンスには8つのコンテキストが含まれています。たとえば、一方のユニットが5コンテキストを使用し、他方が3コンテキストを使用します（合計8の場合）。ユニットごとのプラットフォームの制限が10なので、結合されたライセンスでは最大10のコンテキストが許可されます。8コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを30日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 2100 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブフェールオーバーでは、フェールオーバーグループ1がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

（注） フェールオーバーペアを形成する場合は、各 ASA に同じ暗号化ライセンスが必要です。スマート ライセンシング サーバに ASA を登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の 2 つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマートライセンシングサーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンシングサーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマート ライセンシング サーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクで AES/3DES を使用するには、両方のユニットをリロードする必要があります。1 つのユニットだけをリロードすると、そのユニットは AES/3DES を使用しようとしますが、元のユニットは DES を使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- Standard：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Stardard ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Standard ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - Standard ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 2130 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 30 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 34 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 30 であるため、結合されたライセンスでは最大 30 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 25 のコンテキストのみを設定できます。
  - Standard ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 2130 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 14 のコンテキストが含まれ

ています。たとえば、一方のユニットが 9 コンテキストを使用し、他方が 5 コンテキストを使用します（合計 14 の場合）。ユニットごとのプラットフォームの制限が 30 であるため、結合されたライセンスでは最大 30 のコンテキストが許容されます。14 コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

フェールオーバーを設定する前に、両方の Firepower 4100/9300 は、Smart Software Manager または Smart Software Manager オンプレミスサーバーに登録する必要があります。セカンダリ ユニットに追加費用はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

アクティブ/スタンバイフェールオーバーの ASA ライセンス設定のフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブな装置のみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライ

センスはスタンバイ ユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Standard：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Stardard ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Standard ライセンスには 10 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Standard ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - Standard ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。アクティブ/スタンバイペアのアクティブな装置に 250 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 270 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 230 コンテキストを設定する必要があります。
  - Standard ライセンスには 10 のコンテキストがあり、2 つユニットがあるため、合計で 20 のコンテキストがあります。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 30 のコンテキストが含まれています。たとえば、一方のユニットが 17 コンテキストを使用し、他方が 13 コンテキストを使用します（合計 30 の場合）。ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。30 コンテキストは制限の範囲内です。
- キャリア：アクティブのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300 の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

クラスタリング機能自体にライセンスは必要ありません。強力な暗号化およびその他のオプションのライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシ がライセンス機関または Smart Software Manager の通常およびオンプレミスサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- 標準：制御ユニットのみがサーバから標準ライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトで標準ライセンスは 10 のコンテキストを含み、すべてのクラスタ メンバー上に存在します。各ユニットの標準ライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタに 6 台の Firepower9300 モジュールがある場合を考えます。標準ライセンスは 10 のコンテキストを含みます。6 つユニットの場合、合計で 60 のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 80 のコンテキストを含みます。モジュールごとのプラットフォーム制限は 250 であるため、統合されたライセンスに最大 250 のコンテキストが許容されます。80 のコンテキストは制限範囲内です。したがって、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して 80 コンテキストを持つことになります。
  - クラスタに Firepower 4112 が 3 台あるとします。標準ライセンスは 10 のコンテキストを含みます。3 つユニットの場合、合計で 30 のコンテキストが加算されます。制御ユニット上で追加の 250 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 280 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大 250 のコンテキス

トが許容されます。280コンテキストは制限を超えています。したがって、制御ユニット上で最大250のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して250のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして220のコンテキストのみを設定する必要があります。

- キャリア：分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- 高度暗号化（3DES）（2.3.0 より前の Cisco Smart Software Manager オンプレミス展開用、または管理目的用）のライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

スマート ソフトウェア ライセンスの前提条件

Smart Software Manager 定期およびオンプレミスの前提条件

Firepower 4100/9300

ASA ライセンス資格を設定する前に、Firepower 4100/9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

他のすべてのモデル

- デバイスからのインターネットアクセス、HTTP プロキシアクセス、Smart Software Manager オンプレミスサーバーへのアクセスを確保します。

- デバイスが Smart Software Manager の名前を解決できるように DNS サーバーを設定します。
- デバイスのクロックを設定します。プラットフォームモードの Firepower 2100 では、FXOS でクロックを設定します。
- Cisco Smart Software Manager でマスター アカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。

永続ライセンス予約の前提条件

- Cisco Smart Software Manager でマスター アカウントを作成します。

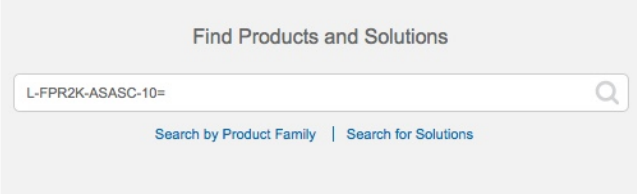
  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。永続ライセンス予約には ASA からスマートライセンスサーバーへのインターネット接続が必要ですが、永続ライセンスの管理には Smart Software Manager が使用されます。
- 永続ライセンス予約のサポートはライセンスチームから受けられます。永続ライセンス予約を使用する理由を示す必要があります。アカウントが承認されていない場合、永続ライセンスを購入して適用することはできません。
- 専用の永続ライセンスを購入します（ライセンス PID （21 ページ）を参照）。アカウントに正しいライセンスがない場合、ASA でライセンスを予約しようとすると、「The licenses cannot be reserved because the Virtual Account does not contain a sufficient surplus of the following perpetual licenses: 1 - Firepower 4100 ASA PERM UNIV(perpetual)」のようなエラーメッセージが表示されます。
- 永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアント の使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。
- ASAv：永続ライセンスの予約は Azure ハイパーバイザではサポートされません。

ライセンス PID

ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、主導でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [製品とソリューションの検索（Find Products and Solutions）] 検索フィールドを使用します。次のライセンス製品 ID（PID）を検索します。

図 *1:* ライセンス検索



ASAv PID

ASAv Smart Software Manager 定期およびオンプレミスPID：

- ASAv5：L-ASAV5S-K9 =
- ASAv10：L-ASAV10S-K9=
- ASAv30：L-ASAV30S-K9=
- ASAv50：L-ASAV50S-K9=
- ASAv100—L-ASAV100S-1Y=
- ASAv100—L-ASAV100S-3Y=
- ASAv100—L-ASAV100S-5Y=

（注） ASAv100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。

ASAv 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアントの機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- ASAv5—L-ASAV5SR-K9=
- ASAv10—L-ASAV10SR-K9=
- ASAv30—L-ASAV30SR-K9=
- ASAv50—L-ASAV50SR-K9=
- ASAv100—L-ASAV100SR-K9=

Firepower 1010 PID

Firepower 1010 Smart Software Manager 定期およびオンプレミス PID：

- 標準ライセンス：L-FPR1000-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- Security Plus ライセンス：L-FPR1010-SEC-PL=。Security Plus ライセンスによってフェールオーバーが有効になります。
- Strong Encryption（3DES/AES）license—L-FPR1K-ENC-K9=. アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1010 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアントの機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- L-FPR1K-ASA-BPU=

Firepower 1100 PID

Firepower 1100 Smart Software Manager 定期およびオンプレミス PID：

- 標準ライセンス：L-FPR1000-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 5 コンテキストライセンス：L-FPR1K-ASASC-5=。コンテキストライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 10 コンテキストライセンス：L-FPR1K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- Strong Encryption（3DES/AES）license—L-FPR1K-ENC-K9=. アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアントの機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- L-FPR1K-ASA-BPU=

Firepower 2100 PID

Firepower 2100 Smart Software Manager 定期およびオンプレミス PID：

- 標準ライセンス：L-FPR2100-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。

- 5 コンテキスト ライセンス：L-FPR2K-ASASC-5=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 10 コンテキスト ライセンス：L-FPR2K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 強力な暗号化 (3DES/AES) のライセンス：L-FPR2K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 2100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- L-FPR2K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 Smart Software Manager 定期およびオンプレミス PID：

- 標準ライセンス：L-FPR4100-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 10 コンテキスト ライセンス：L-FPR4K-ASASC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 230 コンテキスト ライセンス：L-FPR4K-ASASC-230=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- 250 コンテキスト ライセンス：L-FPR4K-ASASC-250=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR4K-ASA-CAR=
- 高度暗号化（3DES/AES）ライセンス：L-FPR4K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 4100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- L-FPR4K-ASA-BPU=

Firepower 9300 PID

Firepower 9300 Smart Software Manager 定期およびオンプレミス PID：

- 標準ライセンス：L-F9K-ASA=。標準ライセンスは無料ですが、スマート ソフトウェア ライセンシング アカウントに追加する必要があります。
- 10 コンテキスト ライセンス：L-F9K-ASA-SC-10=。コンテキスト ライセンスは追加的であり、ニーズに合わせて複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-F9K-ASA-CAR=
- 高度暗号化（3DES/AES）ライセンス：L-F9K-ASA-ENCR-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 9300 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。AnyConnect クライアントの使用権を有効にする AnyConnect ライセンスを購入すれば、AnyConnect クライアント の機能もプラットフォームの上限まで有効になります（「AnyConnect Plus、AnyConnect Apex、AnyConnect VPN Only ライセンス （7 ページ）」を参照）。

- L-FPR9K-ASA-BPU=

スマート ソフトウェア ライセンスのガイドライン

- スマート ソフトウェア ライセンスのみがサポートされます。ASAv の古いソフトウェアについては、PAK ライセンスが供与された既存の ASAv をアップグレードする場合、前にインストールしたアクティベーションキーは無視されますが、デバイスに保持されます。ASAv をダウングレードする場合は、アクティベーション キーが復活します。
- 永続ライセンスの予約については、デバイスを廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しいデバイスに再使用できません。
- Cisco Transport Gateway は非準拠の国番号の証明書を使用するため、ASA をその製品と組み合わせて使用する場合は HTTPS を使用できません。Cisco Transport Gateway で HTTP を使用する必要があります。

スマート ソフトウェア ライセンスのデフォルト

ASAv

- ASAv のデフォルト設定には、Licensing Authority の URL を指定する、「License」という Smart Call Home プロファイルが含まれます。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

- ASAv を展開するときに、機能層とスループットレベルを設定します。現時点では、標準レベルのみを使用できます。永続ライセンス予約の場合、これらのパラメータを設定する必要はありません。永続ライセンス予約を有効にすると、これらのコマンドはコンフィギュレーションから削除されます。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

- また、導入時に任意で HTTP プロキシを設定できます。

```
call-home
  http-proxy ip_address port port
```

Firepower 1000 および 2100

Firepower 1000 および 2100 のデフォルト設定には、Licensing Authority の URL を指定する「License」という Smart Call Home プロファイルが含まれています。

```
call-home
  profile License
   destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Firepower 4100/9300 シャーシ 上の ASA

デフォルト設定はありません。標準ライセンス階層、およびその他のオプション ライセンスは手動で有効化する必要があります。

ASAv：スマート ソフトウェア ライセンシングの設定

このセクションでは、ASAv にスマート ソフトウェア ライセンスを設定する方法を説明します。次の方法の中から 1 つを選択してください。

手順

ステップ 1 ASAv：定期スマート ソフトウェア ライセンシングの設定 （27 ページ）。

ステップ 2 ASAv：Smart Software Manager オンプレミスライセンシングの設定 （31 ページ）。

ステップ 3 ASAv：ユーティリティモードおよびMSLA スマート ソフトウェア ライセンシングの設定（33 ページ）

ステップ 4 ASAv：永続ライセンス予約の設定 （37 ページ）。

ASAv：定期スマート ソフトウェア ライセンシングの設定

ASAv を展開する場合は、デバイスを事前に設定し、Smart Software Manager に登録するために登録トークンを適用して、スマート ソフトウェア ライセンシングを有効にできます。HTTP プロキシサーバー、ライセンス権限付与を変更する必要がある場合、または ASAv を登録する必要がある場合（Day0 設定に ID トークンを含めなかった場合など）は、このタスクを実行します。

（注） ASAv を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASAv を展開したときに Day0 設定で登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。

手順

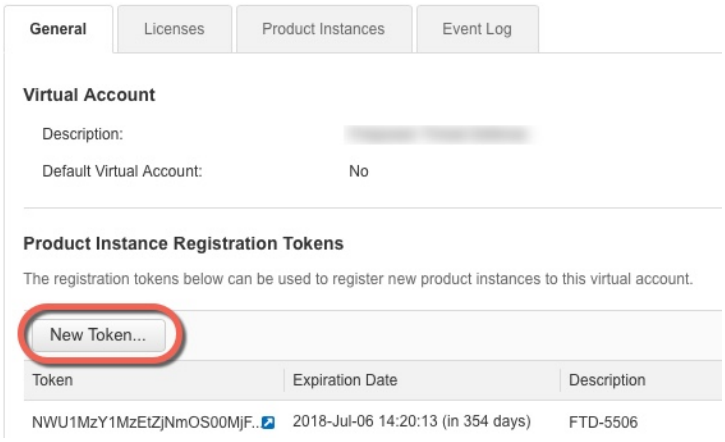
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 2:インベントリ

b) [General] タブで、[New Token] をクリックします。

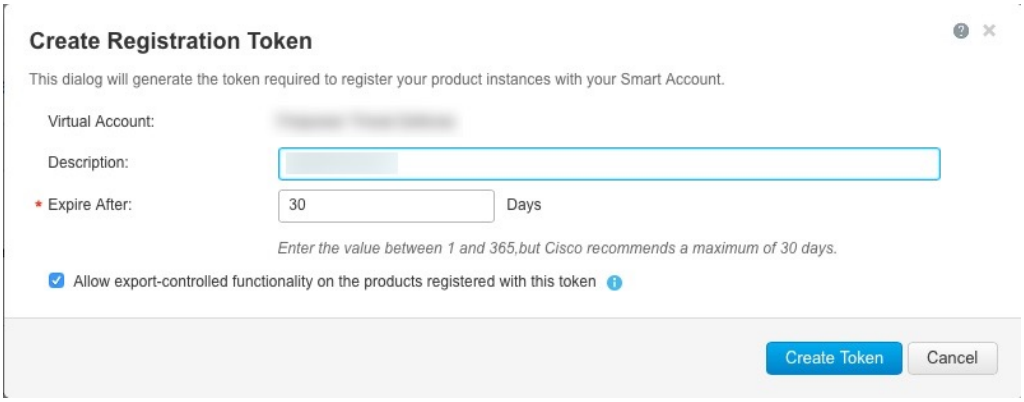
図 *3*：新しいトークン



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

図 *4*：登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *5：* トークンの表示

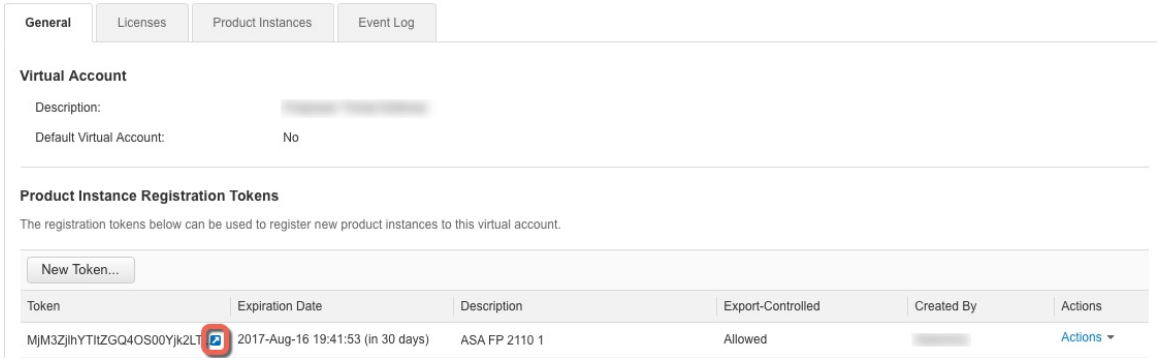
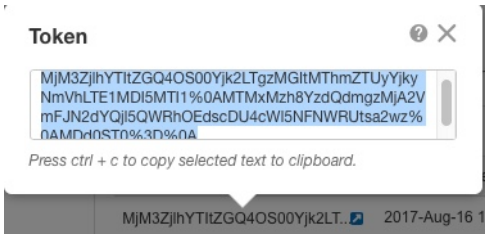


図 *6：* トークンのコピー



ステップ 2 （任意） ASAv で、HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 3 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。

c) スループット レベルを設定します。

throughput level {**100M** | **1G** | **2G** | **10G** | **20G**}

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

a) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する（**exit** または **end**）か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 4 Smart Software Manager で ASAv を登録します。

ASAv を登録すると、Smart Software Manager は ASAv と Smart Software Manager 間の通信用の ID 証明書を発行します。また、ASAv が該当する仮想アカウントに割り当てられます。通常、この手順は 1 回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、ASAv の再登録が必要になります。

a) ASAv の登録トークンを入力します。

license smart register idtoken *id_token* [**force**]

例：

force キーワードを使用して、Smart Software Manager と同期されていない可能性がある登録済みの ASAv を登録します。たとえば、Smart Software Manager から誤って ASAv を削除した場合に **force** を使用します。

ASAv が、Smart Software Manager への登録と設定されたライセンス権限付与の承認要求を試行します。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASAv：Smart Software Manager オンプレミスライセンシングの設定

この手順は、Smart Software Manager オンプレミスを使用する ASAv に適用されます。

始める前に

Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-premを参照してください。

手順

ステップ 1 Smart Software Manager オンプレミスで登録トークンを要求します。

ステップ 2 （任意） ASA で、HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 3 ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

call-home

profile License

destination address http https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

ステップ 4 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。

c) スループット レベルを設定します。

throughput level {**100M** | **1G** | **2G** | **10G** | **20G**}

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

a) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する（**exit** または **end**）か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 5 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager オンプレミスに登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager オンプレミスは、お使いのアカウントで許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                     1 AUTHORIZED
```

ASAv：ユーティリティモードおよび MSLA スマート ソフトウェア ライセンシングの設定

この手順は、マネージド サービス ライセンス契約（MSLA）プログラムに登録されているスマート ライセンシング ユーティリティ モードの ASAv に適用されます。ユーティリティモードでは、Smart Agent はライセンスの権限付与の使用状況を時間単位で追跡します。スマート

エージェントは、Smart Software Manager 定期またはオンプレミスサーバーに 4 時間ごとにライセンス使用状況レポートを送信します。使用状況レポートは課金サーバーに転送され、お客様にライセンスの使用に関する月次請求書が送信されます。

始める前に

Smart Software Manager オンプレミスを使用している場合は、Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-premを参照してください。

手順

ステップ 1 Smart Software Manager 定期またはオンプレミスで登録トークンを要求します（「デバイス登録とトークン （71 ページ）」を参照）。

ステップ 2 ASAv で、MSLA Smart Licensing 向けにデバイスを設定します。

a) MSLA ライセンスメッセージングに使用するスマートトランスポート（HTTP）を指定します。

transport type *callhome smart*

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport type smart
```

重要 Smart Licensing は、デフォルトで Smart Call Home インフラストラクチャを使用して Smart Software Manager と通信します。ただし、Smart Call Home は MSLA をサポートしていません。MSLA 標準ユーティリティモードで ASAv を実行する予定の場合は、Smart Transport を設定する必要があります。

b) Smart Transport を使用する場合、Smart Software Manager 定期（デフォルト）またはオンプレミスの URL を指定できます。必要に応じて、ライセンスを提供するスマートエージェントによって生成されるライセンス使用状況レポートの 2 番目の宛先を指定できます。

transport url *transport-url* **default utility** *utility-url*

例：

```
ciscoasa(config-smart-lic)# transport url
http://server99.cisco.com/Transportgateway/services/DeviceRequestHandler
ciscoasa(config-smart-lic)# transport url utility
http://server-utility.cisco.com/Transportgateway/services/DeviceRequestHandler
```

（注） エントリが指定されていない場合、**transport url** の設定はデフォルトの **https://smartreceiver.cisco.com/licservice/license** になります。

c) （任意） ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。

transport proxy *proxy-url* **port** *proxy-port-number*

（注） 認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 443
```

ステップ 3 ライセンスメッセージでは、ライセンスデバイスのホスト名または Smart Agent バージョン番号を抑制することを選択できます。

privacy all hostname version

例：

```
ciscoasa(config-smart-lic)# privacy all
```

ステップ 4 ユーティリティライセンス情報を設定します。これには、課金のために必要な顧客情報が含まれます。

a) ユーティリティ コンフィギュレーション モードを開始します。

utility

例：

```
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)#
```

b) 一意の顧客 ID を作成できます。この ID は、Utility Licensing 使用状況レポートメッセージに含まれます。

custom-id *custom-identifier*

例：

```
ciscoasa(config-smart-lic-util)# custom-id MyCustomID
```

c) 一意の顧客プロファイルを作成できます。この情報は、Utility Licensing 使用状況レポートに含まれます。

customer-info city country id name postalcode state street

例：

```
ciscoasa(config-smart-lic-util)# customer-info city MyCity
ciscoasa(config-smart-lic-util)# customer-info country MyCountry
```

```
ciscoasa(config-smart-lic-util)# customer-info id MyID
ciscoasa(config-smart-lic-util)# customer-info name MyName
ciscoasa(config-smart-lic-util)# customer-info postalcode MyPostalCode
ciscoasa(config-smart-lic-util)# customer-info state MyState
ciscoasa(config-smart-lic-util)# customer-info street MyStreet
```

ステップ 5 （任意） このコマンドは、ASAv を標準 MSLA モードで動作させる必要がある場合に使用します。標準 MSLA モードでは、Smart Transport を使用するように Smart Licensing を設定する必要があります。このコマンドの **no** バージョンを使用すると、標準 MSLA モードがクリアされ、ASAv がデフォルトのユーティリティモードになります。このモードでは、Smart Transport または Smart Call Home を使用できます。

mode standard

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)# mode standard
```

ステップ 6 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ライセンスのステータスと使用状況をチェックするには、**show run license** コマンドを使用します。

例：

```
ciscoasa# show run license

license smart
 feature tier standard
 throughput level 2G
 transport type smart
 transport url http://10.196.155.133:80/Transportgateway/services/DeviceRequestHandler
 transport url utility
http://10.196.155.133:80/Transportgateway/services/DeviceRequestHandler
 utility
 mode standard
 custom-id CUSTOM-ID-AUTOMATION1234
 customer-info id ID-AUTOMATION1234
 customer-info name NAME-AUTOMATION
 customer-info street KitCreekRoad
 customer-info city RTP
 customer-info state NC
 customer-info country USA
 customer-info postalcode 12345
```

ASAv：永続ライセンス予約の設定

ASAv に永続ライセンスを割り当てることができます。このセクションでは、ASAv の廃止やモデル層の変更などによって新しいライセンスが必要となった場合に、ライセンスを返却する方法についても説明します。

手順

ステップ 1 ASAv 永続ライセンスのインストール （37 ページ）

ステップ 2 （任意） （オプション）ASAv の永続ライセンスの返却 （39 ページ）

ASAv 永続ライセンスのインストール

インターネットアクセスを持たない ASAv の場合は、Smart Software Manager から永続ライセンスを要求できます。

（注） 永続ライセンスの予約については、ASAv を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASAv に再使用できません。（オプション）ASAv の永続ライセンスの返却 （39 ページ）を参照してください。

（注） 永久ライセンスをインストールした後に設定をクリアした場合（**write erase** を使用するなど）、ステップ 1 に示すように、引数を指定せずに **license smart reservation** コマンドを使用して永久ライセンスの予約を再度有効にする必要があります。この手順の残りの部分を完了する必要はありません。

始める前に

- 永続ライセンスを購入すると、Smart Software Manager でそれらのライセンスを使用できます。すべてのアカウントが永続ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。
- ASAv の起動後に永続ライセンスを要求する必要があります。Day 0 設定の一部として永続ライセンスをインストールすることはできません。

手順

ステップ 1 ASAv CLI で、永続ライセンスの予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

次のコマンドが削除されます。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

通常のスマート ライセンスを使用するには、このコマンドの **no** 形式を使用し、上記のコマンドを再入力します。その他の Smart Call Home 設定はそのまま維持されますが、使用されないため、それらのコマンドを再入力する必要はありません。

ステップ 2 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

ASAv 展開時に使用するモデルレベル（ASAv5/ASAv10/ASAv30/ASAv50）を選択する必要があります。そのモデル レベルによって、要求するライセンスが決まります。後でモデル レベルを変更したい場合は、現在のライセンスを返却し、変更後のモデル レベルに対応する新規ライセンスを要求する必要があります。展開済みの ASAv のモデルを変更するには、新しいモデルの要件に合わせるために、ハイパーバイザから vCPU と DRAM の設定を変更します。各値については、ASAv のクイックスタートガイドを参照してください。現在のモデルを表示するには、**show vm** コマンドを使用します。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネント ライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASAv にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。（オプション）ASAv の永続ライセンスの返却 （39 ページ）を参照してください。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 [ライセンスの予約（License Reservation）] をクリックし、ASAv のコードをボックスに入力します。[Reserve License] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネント ライセンスの予約について承認されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 5 ASAv で、承認コードを次のように入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

これで、ASAv ライセンスが完全に適用されました。

（オプション）ASAv の永続ライセンスの返却

（ASAv を廃棄する場合やモデルレベルの変更によって新しいライセンスが必要になった場合など）永続ライセンスが不要になった場合、以下の手順に従ってライセンスを正式に Smart Software Manager に戻す必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために容易に解除できなくなります。

手順

ステップ 1 ASAv で返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちに ASAv のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンスを要求する（**license smart reservation request universal**）か、ASAv のモデルレベルを変更する（電源を切って

vCPU/RAM を変更する）と、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

ステップ 2 ASAv ユニバーサルデバイス識別子（UDI）が表示されるため、Smart Software Manager で ASAv インスタンスを見つることができます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASAv を確認し、[アクション（Actions）] > [削除（Remove）] の順に選択して、ASAv の返却コードをボックスに入力します。[Remove Product Instance] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

（オプション）ASAv の登録解除（定期およびオンプレミス）

ASAv の登録を解除すると、アカウントから ASAv が削除され、ASAv のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい ASAv に利用することもできます。あるいは、Smart Software Manager から ASAv を削除できます。

（注） ASAv を登録解除した場合、ASAv をリロードすると重大なレート制限状態に戻ります。

手順

ASAv の登録を解除します。

license smart deregister

その後、ASAv がリロードされます。

（オプション）ASAv ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス）

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

Firepower 1000、2100：スマート ソフトウェア ライセンシングの設定

この項では、Firepower 1000、 2100 にスマート ソフトウェア ライセンシングを設定する方法を説明します。次の方法の中から 1 つを選択してください。

手順

ステップ 1 Firepower 1000、2100：定期スマート ソフトウェア ライセンシングの設定 （42 ページ）。

（オプション）Firepower 1000、2100 の登録解除（定期およびオンプレミス） （53 ページ）または （オプション）Firepower 1000、2100 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス） （54 ページ） も可能です。

ステップ 2 Firepower 1000、2100：Smart Software Manager オンプレミスライセンシングの設定 （46 ページ）。

（オプション）Firepower 1000、2100 の登録解除（定期およびオンプレミス） （53 ページ）または （オプション）Firepower 1000、2100 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス） （54 ページ） も可能です。

ステップ 3 Firepower 1000、2100：永続ライセンス予約の設定 （49 ページ）。

Firepower1000、2100：定期スマートソフトウェアライセンシングの設定

この手順は、Smart Software Manager を使用する ASA に適用されます。

手順

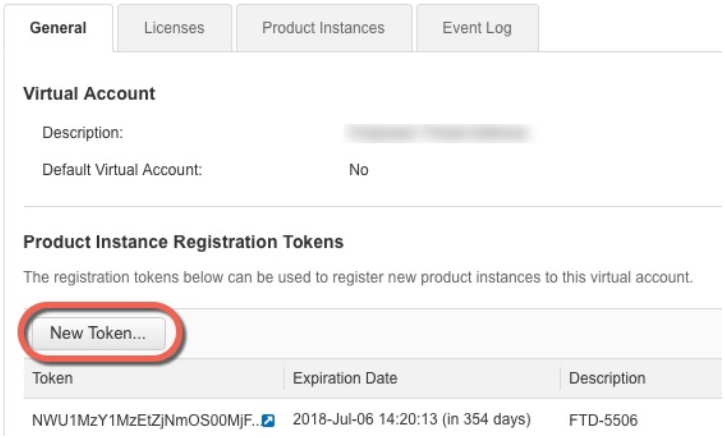
ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

a) [Inventory] をクリックします。

図 *7*：インベントリ

b) [General] タブで、[New Token] をクリックします。

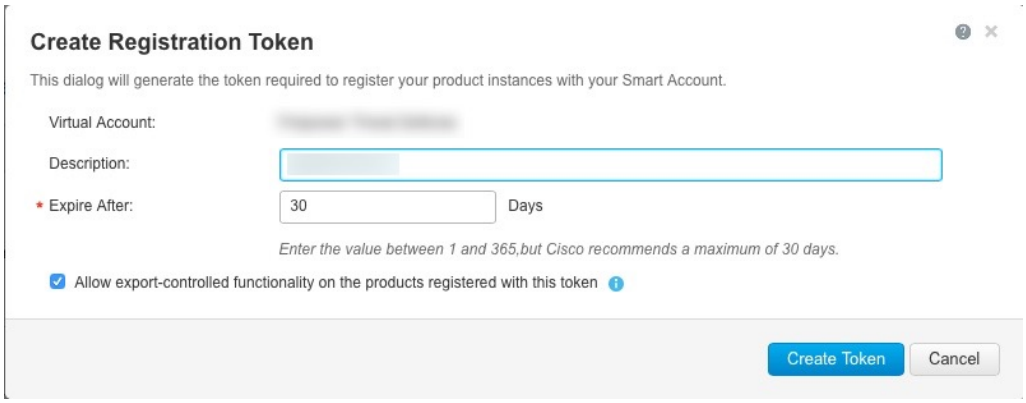
図 *8*：新しいトークン



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

- **[説明（Description）]**
- [有効期限（Expire After）]：推奨値は 30 日です。
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

図 *9*：登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *10*：トークンの表示

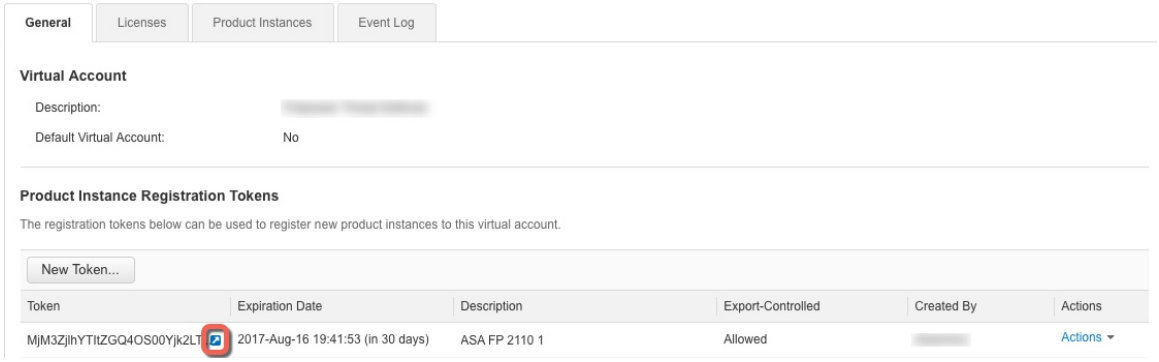
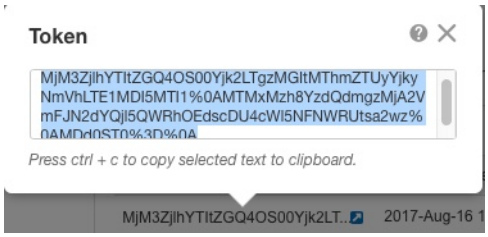


図 *11*：トークンのコピー



ステップ 2 （任意） ASA で、HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 3 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能階層を設定します。

feature tier standard

利用できるのは標準ライセンスのみです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

c) セキュリティコンテキストのライセンスを要求します。

feature context *number*

（注） このライセンスは、Firepower 1010 ではサポートされていません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：25 コンテキスト
- Firepower 2110：25 コンテキスト
- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （任意） (Firepower 1010）Request the Security Plus license to enable Active/Standby Failover.

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

ステップ 4 手順 1 でコピーしたトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager に登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager は、ご使用のアカウントが許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
```

```
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                     1 AUTHORIZED
```

Firepower 1000、2100：Smart Software Manager オンプレミスライセンシングの設定

この手順は、Smart Software Manager オンプレミスを使用する ASA に適用されます。

始める前に

Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager.html#~on-premを参照してください。

手順

ステップ 1 Smart Software Manager オンプレミスサーバーで登録トークンを要求します。

ステップ 2 （任意） ASA で、HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンスのプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 3 ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスサーバーに移動します。

call-home

profile License

destination address http https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

ステップ 4 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能階層を設定します。

feature tier standard

利用できるのは標準ライセンスのみです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

c) （任意） セキュリティコンテキストのライセンスを要求します。

feature context *number*

（注） このライセンスは、Firepower 1010 ではサポートされていません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：25 コンテキスト
- Firepower 2110：25 コンテキスト
- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （任意）(Firepower 1010）Request the Security Plus license to enable Active/Standby Failover.

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

ステップ 5 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager オンプレミスサーバーに登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager オンプレミスサーバーは、お使いのアカウントで許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
```

```
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                     1 AUTHORIZED
```

Firepower 1000、2100：永続ライセンス予約の設定

Firepower 1000、2100 に永続ライセンスを割り当てることができます。この項では、ASA を廃止する場合にライセンスを返す方法についても説明します。

手順

ステップ 1 Firepower 1000、2100 永続ライセンスのインストール （49 ページ）。

ステップ 2 （任意） （オプション）Firepower 1000、2100永続ライセンスの返却 （52 ページ）。

Firepower 1000、2100 永続ライセンスのインストール

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。永続ライセンスでは、すべての機能が有効になります（セキュリティコンテキストが最大の標準ライセンス）。

（注） 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。（オプション）Firepower 1000、2100永続ライセンスの返却 （52 ページ）を参照してください。

始める前に

パーマネント ライセンスを購入すると、Smart Software Manager でそれらを使用できます。すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

手順

ステップ 1 ASA CLI で、永続ライセンスの予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

ステップ 2 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネント ライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。（オプション）Firepower 1000、2100永続ライセンスの返却 （52 ページ）を参照してください。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 [License Reservation] をクリックして、ASA のコードをボックスに入力します。[Reserve License] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネント ライセンスの予約について承認されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 5 ASA で、承認コードを次のように入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

ステップ 6 ASA でライセンス権限付与を要求します。

ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能階層を設定します。

feature tier standard

利用できるのは標準ライセンスのみです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。

c) （任意） セキュリティコンテキストのライセンスを要求します。

feature context *number*

（注） このライセンスは、Firepower 1010 ではサポートされていません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：25 コンテキスト
- Firepower 2110：25 コンテキスト
- Firepower 2120：25 コンテキスト
- Firepower 2130：30 コンテキスト
- Firepower 2140：40 コンテキスト

たとえば、Firepower 2110 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （任意） (Firepower 1010）Request the Security Plus license to enable Active/Standby Failover.

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

（オプション）Firepower 1000、2100永続ライセンスの返却

永続ライセンスが不要になった場合（ASAを廃止する場合など）は、この手順を使用して正式にSmart Software Managerにライセンスを返却する必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために容易に解除できなくなります。

手順

ステップ1 ASAで返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちにASAのライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンス（**license smart reservation request universal**）を要求すると、このコードを再表示できなくなることに注意し

てください。必ず、コードをキャプチャして、戻す作業を完了してください。評価期間が終了すると、ASA は期限切れ状態に移行します。コンプライアンス違反状態の詳細については、コンプライアンス逸脱状態 （72 ページ）を参照してください。

ステップ 2 ASA ユニバーサル デバイス識別子（UDI）が表示されるので、Smart Software Manager で ASA インスタンスを見つることができます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASA を確認し、**[Actions]** > **[Remove]** を選択して、ASA の返却コードをボックスに入力します。[Remove Product Instance] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

（オプション）Firepower1000、2100の登録解除（定期およびオンプレミス）

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。あるいは、Smart Software Manager（SSM）から ASA を削除できます。

手順

ASA の登録解除：

license smart deregister

（オプション）Firepower1000、2100ID証明書またはライセンス権限付与の更新（定期およびオンプレミス）

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

Firepower 4100/9300：スマート ソフトウェア ライセンスの設定

この手順は、Smart Software Manager、Smart Software Manager オンプレミスを使用するシャーシ、または永続ライセンスの予約に適用されます。方法を前提条件として設定するには、FXOS 設定ガイドを参照してください。

永続ライセンス予約の場合、ライセンスはすべての機能、すなわちセキュリティ コンテキストが最大の標準ティアおよびキャリア ライセンスを有効にします。ただし、ASA がこれらの機能を使用することを「認識する」ためには、ASA でそれらを有効にする必要があります。

始める前に

ASA クラスタの場合は、設定作業のために制御ユニットにアクセスする必要があります。Firepower Chassis Manager でどのユニットが制御ノードなのかを確認してください。この手順に示すように、ASA CLI からも確認できます。

手順

ステップ 1 Firepower 4100/9300 シャーシ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* **console connect asa**

例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

次回 ASA コンソールに接続するときは、ASA に直接移動します。**connect asa** を再入力する必要はありません。

ASA クラスタの場合、ライセンス設定などの設定を行う場合にのみ、制御ユニットにアクセスする必要があります。通常、制御ユニットがスロット 1 にあるため、このモジュールにまず接続する必要があります。

ステップ 2 ASA CLI で、グローバル コンフィギュレーション モードを入力します。論理デバイスの展開時に設定しない限り、デフォルトではイネーブルパスワードは空白ですが、**enable** コマンドを最初に入力したときに変更するように求められます。

enable configure terminal

例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa# configure terminal
asa(config)#
```

ステップ 3 ASA クラスタの場合は、必要に応じて、このユニットが制御ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
```

```
Serial No.: JAB0815R0JY
CCL IP : 127.2.1.3
CCL MAC : 000f.f775.541e
Last join : 19:13:20 UTC Sep 23 2015
Last leave: N/A
```

別のユニットが制御ユニットの場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

ステップ 4 ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

ステップ 5 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。アカウントに十分なティアライセンスが必要です。そうでないと、他の機能ライセンスまたはライセンスを必要とする機能を設定できません。

ステップ 6 次の機能の 1 つ以上をリクエストします。

- キャリア（GTP/GPRS、Diameter、および SCTP インスペクション）

  feature carrier

- セキュリティ コンテキスト

  feature context *<1-248>*

  永続ライセンスの予約では、最大コンテキスト（248）を指定できます。

- 強力な暗号化（3DES/AES）

  feature strong-encryption

  Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

ステップ 7 ASA コンソールを終了して Telnet アプリケーションに戻るには、プロンプトで「~」と入力します。スーパバイザ CLI に戻るには、「**quit**」と入力します。

モデルごとのライセンス

このセクションでは、ASAv および Firepower 4100/9300 シャーシASA セキュリティ モジュールに使用可能なライセンス資格を示します。

ASAv

すべての ASAv ライセンスを、サポートされているすべての ASAv vCPU/メモリ構成で使用できます。これにより、ASAv を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。また、サポート対象の AWS および Azure インスタンスタイプの数も増えます。ASAv を設定する場合、サポートされる最大 vCPU 数は 8 個です（VMware と KVM 上の ASAv100 では 16 個）。また、サポートされる最大メモリ容量は 64GB RAM です。

重要 ASAv の最小メモリ要件は 2GB です。現在の ASAv が 2GB 未満のメモリで動作している場合、ASAv VM のメモリを増やすことなく、以前のバージョンから 9.13(1) 以降にアップグレードすることはできません。また、最新バージョンを使用して新しい ASAv VM を再展開することもできます。

1 つ以上の vCPU を使用して ASAv を展開する場合、ASAv の最小メモリ要件は 4GB です。

柔軟なライセンスのガイドライン

- ライセンスされた機能およびライセンスされていないプラットフォーム機能のセッション制限は、VM メモリの量に基づいて設定されます。
- AnyConnect クライアントおよびTLS プロキシのセッション制限は、ASAv プラットフォームの権限付与によって決定されます。セッション制限は、ASAv モデルタイプ（ASAv5/10/30/50/100）に関連付けられなくなりました。

  セッション制限には最小メモリ要件があります。VM メモリが最小要件を下回っている場合、セッション制限はそのメモリ量でサポートされる最大数に設定されます。
- ファイアウォール接続、同時接続、およびVLANは、ASAv メモリに基づくプラットフォームの制限です。
- 権限付与の制限はありません。すべての権限付与は、vCPU（最大 8 個、VMware と KVM 上の ASAv100 では最大 16 個）とメモリ（最大 64 GB）の任意の組み合わせで実行できます。

- 既存の権限付与に変更はありません。権限付与 SKU と表示名には、引き続きモデル番号（ASAv5/10/30/50/100）が含まれます。
- 権限付与は、レート制限を介して最大スループットを設定します。
- お客様の発注プロセスに変更はありません。

ライセンス	柔軟なライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	イネーブル
通信事業者	イネーブル
Total TLS Proxy Sessions	100 Mbps の権限付与：500 1 Gbps の権限付与：500 2 Gbps の権限付与：1000 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
VPN ライセンス	
AnyConnect ピア	100 Mbps の権限付与：50 1 Gbps の権限付与：250 2 Gbps の権限付与：750 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
その他の VPN ピア	100 Mbps の権限付与：50 1 Gbps の権限付与：250 2 Gbps の権限付与：1000 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
合計VPNピア。全タイプの合計	100 Mbps の権限付与：50 1 Gbps の権限付与：250 2 Gbps の権限付与：1000 10 Gbps の権限付与：10,000 20 Gbps の権限付与：20,000
一般ライセンス	

ライセンス	柔軟なライセンス
スループット レベル	ASAv STD 100M：100 Mbps ASAv STD 1G：1 Gbps ASAv STD 2G：2 Gbps ASAv STD 10G：10 Gbps ASAv STD 20G：20 Gbps
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）
フェールオーバー	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし
クラスタ	サポートなし
vCPUs、RAM	サポートされる最大 vCPU 数は 8 個です（VMware と KVM 上の ASAv100 では 16 個）。また、サポートされる最大メモリ容量は 64 GB RAM です。vCPU とメモリの任意の組み合わせを使用して、任意の ASAv 権限付与レベルを展開できます。 • ASAv の最小メモリ要件は 2GB です。 • 1 つ以上の vCPU を使用して ASAv を展開する場合、ASAv の最小メモリ要件は 4GB です。 • プラットフォームの制限は、必要なメモリの量によって適用されます。 • セッション制限は、展開されている権限付与のタイプによって異なり、最小メモリ要件によって適用されます。 • 100 Mbps の権限付与：2 ～ 7.9 GB • 1 Gbps の権限付与：2 ～ 7.9 GB • 2 Gbps の権限付与：8 ～ 15.9 GB • 10 Gbps の権限付与：16 ～ 31.9 GB • 20 Gbps の権限付与：32 ～ 64 GB

プラットフォームの制限

ファイアウォール接続、同時接続、および VLAN は、ASAv メモリに基づくプラットフォームの制限です。

（注） ASAv がライセンスされていない状態にある場合、ファイアウォール接続は 100 に制限されます。権限付与によってライセンスが付与されると、接続はプラットフォームの制限に移行します。ASAv の最小メモリ要件は 2GB です。

表 *1:* プラットフォームの制限

ASAv のメモリ	**ファイアウォールの接続、同時**	**VLANs**
2 GB ～ 7.9 GB	100,000	50
8 GB ～ 15.9 GB	500,000	200
16 ～ 31.9 GB	2,000,000	1024
32 GB ～ 64 GB	4,000,000	1024

Firepower 1010

次の表に、Firepower 1010 のライセンス機能を示します。

ライセンス	**Standard ライセンス**	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	100,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシ セッション	4,000	
VPN ライセンス		
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus*、*AnyConnect Apex*、または *VPN Only* ライセンス、最大：*75*
その他の VPN ピア	75	
合計 VPN ピア。全タイプの合計	75	

ライセンス	Standard ライセンス	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
Security Plus（フェールオーバー)	ディセーブル	オプション
セキュリティ コンテキスト	サポートしない	
クラスタ	サポートしない	
VLAN、最大	60	

Firepower 1100 シリーズ

次の表に、Firepower 1100 シリーズのライセンス機能を示します。

ライセンス	Standard ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。
ファイアウォールの接続、同時	Firepower 1120：200,000 Firepower 1140：400,000 Firepower 1150：600,000
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。
合計 TLS プロキシセッション	Firepower 1120：4,000 Firepower 1140：8,000 Firepower 1150：8,000
VPN ライセンス	

ライセンス	**Standard** ライセンス	
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus*、*AnyConnect Apex*、または *VPN Only* ライセンス、最大： *Firepower 1120：150* *Firepower 1140：400* *Firepower 1150：800*
その他の VPN ピア	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
合計 VPN ピア。全タイプの合計	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大： *Firepower 1120：5* *Firepower 1140：5* *Firepower 1150：25*
クラスタ	サポートしない	
VLAN、最大	1024	

Firepower 2100 シリーズ

次の表に、Firepower 2100 シリーズのライセンス機能を示します。

ライセンス	**Standard** ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。

ライセンス	Standard ライセンス	
ファイアウォールの接続、同時	Firepower 2110：1,000,000 Firepower 2120：1,500,000 Firepower 2130：2,000,000 Firepower 2140：3,000,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシ セッション	Firepower 2110：4,000 Firepower 2120：8,000 Firepower 2130：8,000 Firepower 2140：10,000	
VPN ライセンス		
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus*、*AnyConnect Apex*、または *VPN Only* ライセンス、最大： *Firepower 2110：1,500* *Firepower 2120：3,500* *Firepower 2130：7,500* *Firepower 2140：10,000*
その他の VPN ピア	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
合計 VPN ピア。全タイプの合計	Firepower 2110：1,500 Firepower 2120：3,500 Firepower 2130：7,500 Firepower 2140：10,000	
一般ライセンス		

ライセンス	Standard ライセンス	
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大： *Firepower 2110：25* *Firepower 2120：25* *Firepower 2130：30* *Firepower 2140：40*
クラスタ	サポートしない	
VLAN、最大	1024	

Firepower 4100

次の表に、Firepower 4100 のライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 4110：10,000,000 Firepower 4112：10,000,000 Firepower 4115：15,000,000 Firepower 4120：15,000,000 Firepower 4125：25,000,000 Firepower 4140：25,000,000 Firepower 4145：40,000,000 Firepower 4150：35,000,000	
通信事業者	ディセーブル	オプション ライセンス：通信事業者
合計 TLS プロキシ セッション	Firepower 4110：10,000 その他すべて：15,000	
VPN ライセンス		

ライセンス	**Standard** ライセンス	
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus*、*AnyConnect Apex*、または *VPN Only* ライセンス： *Firepower 4110*：*10,000* *Firepower 4112*：*10,000* *Firepower 4115*：*15,000* *Firepower 4120*：*15,000* *Firepower 4125*：*20,000* *Firepower 4140*：*20,000* *Firepower 4145*：*20,000* *Firepower 4150*：*20,000*
その他の VPN ピア	Firepower 4110：10,000 Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4120：15,000 Firepower 4125：20,000 Firepower 4140：20,000 Firepower 4145：20,000 Firepower 4150：20,000	
合計 VPN ピア。全タイプの合計	Firepower 4110：10,000 Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4120：15,000 Firepower 4125：20,000 Firepower 4140：20,000 Firepower 4145：20,000 Firepower 4150：20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	

ライセンス	Standard ライセンス	
セキュリティ コンテキスト	10	オプションライセンス：最大 *250*
クラスタ	イネーブル	
VLAN、最大	1024	

Firepower 9300

次の表に、Firepower 9300 のライセンス機能を示します。

ライセンス	Standard ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 9300 SM-56：60,000,000 Firepower 9300 SM-48：60,000,000 Firepower 9300 SM-44：60,000,000 Firepower 9300 SM-40：55,000,000 Firepower 9300 SM-36：60,000,000 Firepower 9300 SM-24：55,000,000	
キャリア	無効	オプション ライセンス：通信事業者
合計 TLS プロキシ セッション	15,000	
VPN ライセンス		
AnyConnect ピア	Unlicensed	オプションの *AnyConnect Plus*、*AnyConnect Apex*、または *VPN Only* ライセンス：最大 *2* 万
その他の VPN ピア	20,000	
合計 VPN ピア。全タイプの合計	20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	

ライセンス	**Standard** ライセンス	
セキュリティ コンテキスト	10	オプションライセンス：最大 *250*
クラスタ	イネーブル	
VLAN、最大	1024	

スマート ソフトウェア ライセンシングのモニタリング

デバッグ メッセージをイネーブルにするだけでなく、ライセンスの機能、ステータス、および証明書をモニターすることもできます。

現在のライセンスの表示

ライセンスを表示するには、次の コマンドを参照してください。

- **show license features**

  次に、基本ライセンスのみ（現在のライセンス権限なし）の ASAv の例を示します。

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- **すべてのライセンスの表示**

  スマート ソフトウェア ライセンシング、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、資格ステータス、使用許可証明書情報および予定のスマート エージェント タスクを表示します。

  次の例は、ASAv ライセンスを示しています。

```
ciscoasa# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=============
Smart Agent for Licensing: 1.6_reservation/36
```

- **show license status**

  スマート ライセンスのステータスを表示します。

  次に、通常のスマート ソフトウェア ライセンシングを使用する ASAv のステータスの例を示します。

```
ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

次に、永続ライセンス予約を使用する ASAv のステータスの例を示します。

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC

Licensing HA configuration error:
    No Reservation Ha config error
```

- **show license summary**

  スマート ライセンスのステータスと使用量のサマリーを表示します。

  次に、通常のスマート ソフトウェア ライセンシングを使用する ASAv のサマリーの例を示します。

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
```

```
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (ASAv-STD-1G)                     1 AUTHORIZED
```

次に、永続ライセンス予約を使用する ASAv のサマリーの例を示します。

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  スマート ライセンスの使用量を表示します。

  次に、ASAv の使用状況の例を示します。

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

UDI の表示

ユニバーサル製品識別子（UDI）を表示するには、次のコマンドを参照してください。

show license udi

次に、ASAv の UDI の例を示します。

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

スマート ソフトウェア ライセンスのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  スマート エージェントからのデバッグをオンにします。

- **debug license** *level*

  Smart Software Licensing Manager のデバッグの各種レベルをオンにします。

Smart Software Manager 通信

このセクションでは、デバイスが Smart Software Manager と通信する方法について説明します。

デバイス登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各デバイスを導入するとき、または既存のデバイスを登録するときにこのトークン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

（注） Firepower 4100/9300 シャーシ：デバイス登録は、ASA 論理デバイス上ではなく、シャーシで設定されます。

展開後の起動時、または既存のデバイスでこれらのパラメータを手動で設定した後、デバイスは Smart Software Manager に登録されます。トークンを使用してデバイスを登録すると、Smart Software Manager はデバイスと Smart Software Manager 間の通信用の ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

Smart Software Manager との定期的な通信

デバイスは、30 日ごとに Smart Software Manager と通信します。Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、すぐに変更されるようにすることができます。または、スケジュールどおりにデバイスが通信するのを待ちます。

必要に応じて、HTTP プロキシを設定できます。

ASAv

ASAvでは、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネットアクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間遵守が維持されます。猶予期間終了後は、Smart

Software Manager に連絡する必要があり、そうしないと ASAv がコンプライアンス違反の状態になります。

Firepower 1000

Firepower 1000 では、直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネットアクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Smart Software Manager に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行えませんが、動作には影響ありません。

Firepower 2100

Firepower 2100 では、直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネットアクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Smart Software Manager に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行えませんが、動作には影響ありません。

Firepower 4100/9300

Firepower 4100/9300では、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネットアクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Smart Software Manager に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行えませんが、動作には影響ありません。

コンプライアンス逸脱状態

次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 使用超過：デバイスが利用できないライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、デバイスで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反状態では、モデルによってはデバイスが制限されている可能性があります。

- ASAv：ASAv は影響を受けません。
- Firepower 1000：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加する

ことはできません。最初の登録時に十分な標準ライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。

- Firepower 2100：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分な標準ライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。
- Firepower 4100/9300：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分な標準ライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。

Smart Call Home インフラストラクチャ

デフォルトでは、Smart Call Home のプロファイルは、Smart Software Manager の URL を指定する設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの設定可能なオプションは、Smart Software Manager の宛先アドレス URL のみであることに注意してください。Cisco TAC に指示されない限り、Smart Software Manager の URL は変更しないでください。

（注） Firepower 4100/9300 シャーシ の場合、ライセンスの Smart Call Home は ASA ではなく Firepower 4100/9300 シャーシ スーパバイザで設定されます。

スマート ソフトウェア ライセンスの Smart Call Home をディセーブルにすることはできません。たとえば、**no service call-home** コマンドを使用して Smart Call Home を無効化しても、スマート ソフトウェア ライセンシングは無効化されません。

他の Smart Call Home の機能は、特に設定しない限り、有効になりません。

スマート ライセンス証明書の管理

ASA は Smart Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。サーバー証明書を発行する階層が変更される場合、サービスの中断を防ぐため、定期的な trustpool バンドルの自動更新が有効になるように、 **auto-update** コマンドを設定します。

スマート ライセンス サーバーから受信したサーバー証明書は、[Extended Key Usage] フィールドに「ServAuth」が含まれていなければなりません。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

スマート ソフトウェア ライセンスの履歴

機能名	プラットフォームリリース	説明
ASAv100 永続ライセンス予約	9.14(1.30)	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。**注**：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。
ASAv MSLA サポート	9.13(1)	ASAvは、シスコのマネージドサービス ライセンス契約（MSLA）プログラムをサポートしています。このプログラムは、マネージド ソフトウェア サービスをサードパーティに提供するシスコのお客様およびパートナー向けに設計された、ソフトウェアのライセンスおよび消費のフレームワークです。 MSLAはスマートライセンスの新しい形式で、ライセンス スマート エージェントは時間単位でライセンス権限付与の使用状況を追跡します。 新規/変更されたコマンド：**license smart**、**mode**、**utility**、**custom-id**、**custom-info**、**privacy**、**transport type**、**transport url**、**transport proxy**
ASAv 柔軟なライセンス	9.13(1)	すべてのASAvライセンスは、サポートされているすべてのASAv vCPU/メモリ構成で使用できるようになりました。AnyConnect クライアント および TLS プロキシのセッション制限は、モデルタイプに関連付けられたプラットフォーム制限ではなく、インストールされたASAvプラットフォームの権限付与によって決まります。 新規/変更されたコマンド： **show version**、**show vm**、**show cpu**、**show license features**
Firepower 4100/9300 シャーシのフェールオーバー ペアのライセンスの変更	9.7(1)	アクティブなユニットのみがライセンス権限を要求します。以前は、両方のユニットがライセンスの権限付与を要求していました。FXOS 2.1.1 でサポートされます。
ASAv の短かい文字列の拡張機能向けの永続ライセンス予約	9.6(2)	スマート エージェント（1.6.4 への）の更新により、要求と認証コードには短い文字列が使用されます。 変更されたコマンドはありません。

機能名	プラットフォームリリース	説明
ASAv のサテライトサーバーのサポート	9.6(2)	デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト サーバーをインストールできます。 変更されたコマンドはありません。
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。
ASAv の永続ライセンス予約	9.5(2.200) 9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASAv 用に永続ライセンスを要求できます。 9.6(2) では、Amazon Web Services の ASAv 向けに、この機能のサポートが追加されました。この機能は Microsoft Azure ではサポートされません。 次のコマンドが導入されました。**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return**

機能名	プラットフォームリリース	説明
スマート エージェントの v1.6 へのアップグレード	9.5(2.200) 9.6(2)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5（2.200）からダウングレードした場合、ASAv はライセンス登録状態を保持しません。**license smart register idtoken** *id_token* **force** コマンドを使用し、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 次のコマンドが導入されました。**show license status**、**show license summary**、**show license udi**、**show license usage** 次のコマンドが変更されました。**show license all**、**show tech-support license** 次のコマンドが非推奨になりました。 **show license cert**、**show license entitlement**、**show license pool**、**show license registration**
FirePOWER 9300 の ASA に高度暗号化（3DES）ライセンスを自動的に適用	9.5(2.1)	通常の Cisco Smart Software Manager（SSM）ユーザーの場合、FirePOWER 9300 で登録トークンを適用すると、対象となるお客様には強力な暗号化ライセンスが自動的に有効になります。 （注） スマート ソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、ASA の展開後に ASA CLI を使用して、高度暗号化ライセンスを有効にする必要があります。 この機能には、FXOS 1.1.3 が必要です。 サテライト以外の構成では、次のコマンドが除去されました。**feature strong-encryption**
サーバー証明書の発行階層が変更された場合の Smart Call Home/スマート ライセンス証明書の検証	9.5(2)	スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを最初に設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA はサーバー証明書の発行階層が変更された場合の証明書の検証をサポートします。トラストプール バンドルの定期的な自動更新を有効にできます。 次のコマンドが導入されました。**auto-import**

機能名	プラットフォームリリース	説明
新しいキャリア ライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 上の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次のコマンドが導入または変更されました。**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version**
FirePOWER 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	9.4(1.150)	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。**feature strong-encryption**、**feature mobile-sp**、**feature context**
ASAv のシスコ スマート ソフトウェア ライセンス	9.3(2)	Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAK ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単に ASAv を展開したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。 **clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level** 各コマンドが導入されました。

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。