



ライセンス：製品認証キーライセンス

ライセンスでは、特定の Cisco ASA 上でイネーブルにするオプションを指定します。このマニュアルでは、すべての物理 ASA の製品認証キー（PAK）のライセンスについて説明します。ASA v については、[ライセンス：スマートソフトウェアライセンス（ASA v、ASA on Firepower）](#)を参照してください。

- [PAK ライセンスについて（1 ページ）](#)
- [PAK ライセンスのガイドライン（17 ページ）](#)
- [PAK ライセンスの設定（19 ページ）](#)
- [共有ライセンスの設定（AnyConnect 3 以前）（24 ページ）](#)
- [モデルごとにサポートされている機能のライセンス（31 ページ）](#)
- [PAK ライセンスのモニタリング（53 ページ）](#)
- [PAK ライセンスの履歴（64 ページ）](#)

PAK ライセンスについて

ライセンスでは、特定の ASA 上でイネーブルにするオプションを指定します。ライセンスは、160 ビット（32 ビットのワードが 5 個、または 20 バイト）値であるアクティベーションキーで表されます。この値は、シリアル番号（11 文字の文字列）とイネーブルになる機能とを符号化します。

事前インストール済みライセンス

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。

関連トピック

- [PAK ライセンスのモニタリング（53 ページ）](#)

永続ライセンス

永続アクティベーションキーを1つインストールできます。永続アクティベーションキーは、1つのキーにすべてのライセンス機能を格納しています。時間ベースライセンスもインストールすると、ASA は永続ライセンスと時間ベース ライセンスを1つの実行ライセンスに結合します。

関連トピック

[永続ライセンスと時間ベース ライセンスの結合](#) (3 ページ)

時間ベース ライセンス

永続ライセンスに加えて、時間ライセンスを購入したり、時間制限のある評価ライセンスを入手したりできます。たとえば、SSL VPN の同時ユーザの短期増加に対処するために時間ベースの AnyConnect Premium ライセンスを購入したり、1年間有効なボットネットトラフィックフィルタ時間ベース ライセンスを注文したりできます。



(注) ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

時間ベース ライセンス有効化ガイドライン

- 複数の時間ベースライセンスをインストールし、同じ機能に複数のライセンスを組み込むことができます。ただし、一度にアクティブ化できる時間ベースライセンスは、1機能につき1つだけです。非アクティブのライセンスはインストールされたままで、使用可能な状態です。たとえば、1000セッション AnyConnect Premium ライセンスと2500セッション AnyConnect Premium ライセンスをインストールした場合、これらのライセンスのうちいずれか1つだけをアクティブにできます。
- キーの中に複数の機能を持つ評価ライセンスをアクティブにした場合、そこに含まれている機能のいずれかに対応する時間ベースライセンスを同時にアクティブ化することはできません。たとえば、評価ライセンスにボットネットトラフィックフィルタと1000セッション AnyConnect Premium ライセンスが含まれる場合、スタンドアロンの時間ベース2500セッション AnyConnect Premium ライセンスをこの評価ライセンスと同時にアクティブ化することはできません。

時間ベース ライセンス タイマーの動作

- 時間ベース ライセンスのタイマーは、ASA 上でライセンスをアクティブにした時点でカウントダウンを開始します。
- タイムアウト前に時間ベースライセンスの使用を中止すると、タイマーが停止します。時間ベースライセンスを再度アクティブ化すると、タイマーが再開します。
- 時間ベースライセンスがアクティブになっているときに ASA をシャットダウンすると、タイマーはカウントダウンを停止します。時間ベースライセンスでは、ASA が動作して

いる場合にのみカウントダウンします。システムクロック設定はライセンスに影響しません。つまり、ASA稼働時間ではライセンス継続期間に対してのみカウントします。

永続ライセンスと時間ベースライセンスの結合

時間ベースライセンスをアクティブにすると、永続ライセンスと時間ベースライセンスに含まれる機能を組み合わせた実行ライセンスが作成されます。永続ライセンスと時間ベースライセンスの組み合わせ方は、ライセンスのタイプに依存します。次の表に、各機能ライセンスの組み合わせルールを示します。



- (注) 永続ライセンスが使用されていても、時間ベースライセンスがアクティブな場合はカウントダウンが続行されます。

表 1: 時間ベースライセンスの組み合わせルール

時間ベース機能	結合されたライセンスのルール
AnyConnect Premium セッション	時間ベースライセンスまたは永続ライセンスのうち、値の高い方が使用されます。たとえば、永続ライセンスが1000セッション、時間ベースライセンスが2500セッションの場合、2500セッションがイネーブルになります。通常は、永続ライセンスよりも機能の低い時間ベースライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。
Unified Communications Proxy セッション	時間ベースライセンスのセッションは、プラットフォームの制限数まで永続セッションに追加されます。たとえば、永続ライセンスが2500セッション、時間ベースライセンスが1000セッションの場合、時間ベースライセンスがアクティブである限り、3500セッションがイネーブルになります。
セキュリティ コンテキスト	時間ベースライセンスのコンテキストは、プラットフォームの制限数まで永続コンテキストに追加されます。たとえば、永続ライセンスが10コンテキスト、時間ベースライセンスが20コンテキストの場合、時間ベースライセンスがアクティブである限り、30コンテキストがイネーブルになります。

時間ベース機能	結合されたライセンスのルール
Botnet Traffic Filter	使用可能な永続ボットネットトラフィックフィルタライセンスはありません。時間ベースライセンスが使用されます。
その他	時間ベースライセンスまたは永続ライセンスのうち、値の高い方が使用されます。ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブルステータスのライセンスが使用されます。数値ティアを持つライセンスの場合、高い方の値が使用されます。通常は、永続ライセンスよりも機能の低い時間ベースライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。

関連トピック

[PAK ライセンスのモニタリング](#) (53 ページ)

時間ベース ライセンスのスタッキング

多くの場合、時間ベースライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベースライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベースライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。

すでにインストールされているのと同じ時間ベースライセンスをインストールすると、それらのライセンスは結合され、有効期間は両者を合わせた期間になります。

次に例を示します。

1. 52 週のボットネットトラフィックフィルタライセンスをインストールし、このライセンスを 25 週間使用します（残り 27 週）。
2. 次に、別の 52 週ボットネットトラフィックフィルタライセンスを購入します。2 つめのライセンスをインストールすると、ライセンスが結合され、有効期間は 79 週（52+27 週）になります。

同様の例を示します。

1. 8 週 1000 セッションの AnyConnect Premium ライセンスをインストールし、これを 2 週間使用します（残り 6 週）。

- 次に、別の 8 週 1000 セッションのライセンスをインストールすると、これらのライセンスは結合され、14 週（8 + 6 週）1000 セッションのライセンスになります。

これらのライセンスが同一でない場合（たとえば、1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンス）、これらのライセンスは結合されません。1 つの機能につき時間ベースライセンスを 1 つだけアクティブにできるので、ライセンスのうちいずれか 1 つだけをアクティブにすることができます。

同一でないライセンスは結合されませんが、現在のライセンスの有効期限が切れた場合、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。

関連トピック

[キーのアクティブ化または非アクティブ化](#)（22 ページ）

[時間ベース ライセンスの有効期限](#)（5 ページ）

時間ベース ライセンスの有効期限

機能に対応する現在のライセンスが期限切れになると、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。その機能に使用できる時間ベース ライセンスが他にない場合は、永続ライセンスが使用されます。

その機能に対して複数の時間ベース ライセンスを追加でインストールした場合、ASA は最初に検出されたライセンスを使用します。どのライセンスを使用するかは、ユーザが設定することはできず、内部動作に依存します。ASA がアクティブ化したライセンスとは別の時間ベースライセンスを使用するには、目的のライセンスを手動でアクティブにする必要があります。

たとえば、2500 セッションの時間ベース AnyConnect Premium ライセンス（アクティブ）、1000 セッションの時間ベース AnyConnect Premium ライセンス（非アクティブ）、500 セッションの永続 AnyConnect Premium ライセンスを所有しているとします。2500 セッション ライセンスの有効期限が切れた場合、ASA は 1000 セッション ライセンスを有効化します。1000 セッション ライセンスの有効期限が切れた後、ASA は 500 セッション永久ライセンスを使用します。

関連トピック

[キーのアクティブ化または非アクティブ化](#)（22 ページ）

ライセンスに関する注意事項

次の項で、ライセンスに関する追加情報について説明します。

AnyConnect Plus および Apex ライセンス

AnyConnect Plus および Apex ライセンスは、ライセンスが指定するユーザ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。<https://www.cisco.com/go/license> [英語] を参照し、各 ASA に個別に PAK を割り当てます。ASA に取得したアクティブセッションキーを適用すると、VPN 機能が最大許容数に切り替わりますが、ライセンスを共有するすべて

の ASA 上の実際の一意のユーザ数はライセンス限度を超えることはできません。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 \(FAQ\)](#)



(注) マルチ コンテキスト モードには AnyConnect Apex ライセンスが必要です。さらに、マルチ コンテキスト モードでは、フェールオーバー ペアの各ユニットにこのライセンスを適用する必要があります。ライセンスは集約されません。

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 セッションを開始した後、ポータルから AnyConnect クライアントセッションを開始した場合は、合計1つのセッションが使用されています。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）開始した後、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ています。

VPN ロード バランシング

VPN ロード バランシングには、強力な暗号化（3DES/AES）ライセンスが必要です。

レガシー VPN ライセンス

ライセンスに関するすべての関連情報については、「[AnyConnect の補足エンド ユーザ ライセンス契約書 \(Supplemental end User License Agreement for AnyConnect\)](#)」を参照してください。



(注) マルチ コンテキスト モードでは AnyConnect Apex ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

暗号化ライセンス

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
- GTP/GPRS
- SCTP

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があります。

- 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。

IPS モジュールのライセンス

IPS モジュールライセンスがあると、ASA で IPS ソフトウェア モジュールを実行することができます。また、IPS 側の IPS シグニチャ サブスクリプションが必要です。

次のガイドラインを参照してください。

- IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です（製品番号に、たとえば ASA5515-IPS-K9 のように「IPS」が含まれている必要があります）。IPS ではない製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。
- フェールオーバーについては、両方のユニットで IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスでないため、フェールオーバー時に共有されません。
- フェールオーバーについて、IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュールライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュールライセンスも技術的にはフェールオーバー クラスターライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、フェールオーバーの装置ごとに個別の IPS モジュールライセンスを購入する必要があります。

AnyConnect Premium 共有ライセンス（AnyConnect 3 以前）



- (注) ASAの共有ライセンス機能は、AnyConnect4以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバまたは参加ライセンスは不要になりました。

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。

フェールオーバーまたは ASA クラスター ライセンス

いくつかの例外を除き、フェールオーバーおよびクラスターユニットは、各ユニット上で同一のライセンスを必要としません。以前のバージョンについては、お使いのバージョンに該当するライセンスング マニュアルを参照してください。

フェールオーバー ライセンスの要件および例外

フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスターライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5506-X および ASA 5506W-X	<ul style="list-style-type: none">• アクティブ/スタンバイ：Security Plus ライセンス。• アクティブ/アクティブ：サポートなし。 <p>(注) 各ユニットに同じ暗号化ライセンスが必要です。</p>

モデル	ライセンス要件
ASA 5512-X ~ ASA 5555-X	<ul style="list-style-type: none"> • ASA 5512 : Security Plus ライセンス。 • その他のモデル : 基本ライセンス。 <p>(注)</p> <ul style="list-style-type: none"> • 各ユニットに同じ暗号化ライセンスが必要です。 • マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。 • 各ユニットに同じ IPS モジュール ライセンスが必要です。両方の装置の IPS 側で IPS シグニチャ サブスクリプションも必要です。次のガイドラインを参照してください。 <ul style="list-style-type: none"> • IPS シグニチャ サブスクリプションを購入するには、IPS がプリインストールされた ASA が必要です (ASA5525-IPS-K9のように、製品番号に「IPS」が含まれている必要があります)。IPS 以外の製品番号の ASA に IPS シグニチャ サブスクリプションを購入することはできません。 • 両方の装置に IPS シグニチャ サブスクリプションが必要です。このサブスクリプションは ASA ライセンスではないため、フェールオーバー間で共有されません。 • IPS シグニチャ サブスクリプションには、装置ごとに個別の IPS モジュールライセンスが必要です。他の ASA のライセンスと同様に、IPS モジュールライセンスも技術的にはフェールオーバー クラスタ ライセンスで共有されます。しかし、IPS シグニチャ サブスクリプションの要件によって、装置ごとに個別の IPS モジュールライセンスを購入する必要があります。
ASAv	<p>ASAv のフェールオーバー ライセンスを参照してください。</p>

ASA クラスタ ライセンスの要件および例外

モデル	ライセンス要件
Firepower 4100/9300	Firepower 4100/9300 ジャーシの ASA のフェールオーバーライセンスを参照してください。
他のすべてのモデル	基本ライセンスまたは標準ライセンス。 (注) <ul style="list-style-type: none"> 各ユニットに同じ暗号化ライセンスが必要です。 マルチ コンテキスト モードでは、各ユニットに同じ AnyConnect Apex ライセンスが必要です。



- (注) 有効な永続キーが必要です。まれに、PAK 認証キーを削除できることもあります。キーがすべて0の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

ASA クラスタ ライセンスの要件および例外

クラスタ ユニットは、各ユニット上で同じライセンスを必要としません。一般的には、マスター ユニット用のライセンスのみを購入します。スレーブ ユニットはマスターのライセンスを継承します。複数のユニットにライセンスがある場合は、これらが統合されて単一の実行 ASA クラスタ ライセンスとなります。

このルールには、例外があります。クラスタリングの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 5585-X	クラスタ ライセンス、最大 16 ユニットのサポートします。 (注) 各ユニットに、同じ暗号化ライセンスが必要です。各ユニットに同じ 10 GE I/O/Security Plus ライセンスが必要です (ASA 5585-X と SSP-10 および SSP-20)。
ASA 5516-X	基本ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。
ASA 5512-X	Security Plus ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。

モデル	ライセンス要件
ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X	基本ライセンス、2 ユニットのサポートします。 (注) 各ユニットに同じ暗号化ライセンスが必要です。
Firepower 4100/9300 シャーシ	Firepower 4100/9300 シャーシ上の ASA の ASA クラスタライセンス を参照してください。
他のすべてのモデル	サポートしない

フェールオーバーまたは ASA クラスタ ライセンスの結合方法

フェールオーバー ペアまたは ASA クラスタでは、各ユニットのライセンスが結合されて 1 つの実行クラスタライセンスとなります。ユニットごとに別のライセンスを購入した場合は、結合されたライセンスには次のルールが使用されます。

- 数値ティアを持つライセンスの場合は（セッション数など）、各ユニットのライセンスの値が合計されます。ただし、プラットフォームの制限を上限とします。使用されているライセンスがすべて時間ベースの場合は、ライセンスのカウンタ ダウンは同時に行われません。

たとえば、フェールオーバーの場合は次のようになります。

- 2 つの ASA があり、それぞれに 10 個の TLS プロキシセッションが設定されている場合、ライセンスは結合され、合計で 20 個の TLS プロキシセッションになります。
- 1000 個の TLS プロキシセッションを設定した ASA 5545-X と、2000 個のセッションを設定した ASA 5545-X がある場合、プラットフォームの制限が 2000 であるため、結合されたライセンスでは 2000 個の TLS プロキシセッションを使用できます。
- 2 つの ASA 5545-X ASA があり、一方は 20 コンテキスト、もう一方は 10 コンテキストである場合、結合されたライセンスでは 30 コンテキストを使用できます。アクティブ/アクティブ フェールオーバーの場合は、コンテキストが 2 つのユニットに分配されます。たとえば、一方のユニットが 18 コンテキストを使用し、他方が 12 コンテキストを使用します（合計 30 の場合）。

たとえば、ASA クラスタリングの場合は次のようになります。

- デフォルトの 2 コンテキストの 2 つの ASA 5516-X ASA があります。プラットフォームの制限が 5 であるため、結合されたライセンスでは最大 4 のコンテキストが許容されます。したがって、プライマリ ユニット上で最大 4 のコンテキストを設定できます。各セカンダリユニットも、コンフィギュレーションの複製経由で 4 のコンテキストを持つこととなります。
- 4 つの ASA 5516-X ASA があります。これは、それぞれが 5 コンテキストの 3 つのユニットと、デフォルトの 2 コンテキストの 1 つのユニットです。プラットフォームの制限が 5 であるため、ライセンスは合計で 5 コンテキストに結合されます。したがって、プライマリ ユニット上で最大 5 のコンテキストを設定できます。各セカンダリ

ユニットも、コンフィギュレーションの複製経由で5のコンテキストを持つこととなります。

- ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブルステータスのライセンスが使用されます。
- イネーブルまたはディセーブル状態（かつ数値ティアを持たない）の時間ベースライセンスの場合、有効期間はすべてのライセンスの期間の合計となります。最初にプライマリ/マスターユニットのライセンスがカウントダウンされ、期限切れになると、セカンダリ/スレーブユニットのライセンスのカウントダウンが開始し、以下も同様です。このルールは、アクティブ/アクティブフェールオーバーとASAクラスタリングにも適用されます（すべてのユニットがアクティブに動作していても適用されます）。

たとえば、2つのユニットのポットネットトラフィックフィルタライセンスの有効期間が48週残っている場合は、結合された有効期間は96週です。

関連トピック

[PAK ライセンスのモニタリング](#)（53 ページ）

フェールオーバーまたは ASA クラスタ ユニット間の通信の途絶

ユニットの通信が途絶えてからの期間が30日を超えた場合は、各ユニットにはローカルにインストールされたライセンスが適用されます。30日の猶予期間中は、結合された実行ライセンスが引き続きすべてのユニットで使用されます。

30日間の猶予期間中に通信が復旧した場合は、時間ベースライセンスについては、経過した時間がプライマリ/マスターライセンスから差し引かれます。プライマリ/マスターライセンスが期限切れになるまでは、セカンダリ/スレーブライセンスのカウントダウンが開始することはありません。

30日間の期間が終了しても通信が復旧しなかった場合は、時間ベースライセンスについては、その時間がすべてのユニットのライセンスから差し引かれます（インストールされている場合）。これらはそれぞれ別のライセンスとして扱われ、ライセンスの結合によるメリットはありません。経過時間には30日の猶予期間も含まれます。

次に例を示します。

1. 52週のポットネットトラフィックフィルタライセンスが2つのユニットにインストールされています。結合された実行ライセンスでは、合計期間は104週になります。
2. これらのユニットが、1つのフェールオーバーユニット/ASAクラスタとして10週間動作すると、結合ライセンスの期間の残りは94週となります（プライマリ/マスターに42週、セカンダリ/スレーブに52週）。
3. ユニットの通信が途絶えた場合（たとえば、プライマリ/マスターユニットが停止した場合）は、セカンダリ/スレーブユニットは結合されたライセンスを引き続き使用し、94週からカウントダウンを続行します。
4. 時間ベースライセンスの動作は、通信がいつ復元されるかによって次のように異なります。

- 30 日以内：経過した時間がプライマリ/マスター ユニットのライセンスから差し引かれます。この場合、通信は 4 週間後に復元されます。したがって、4 週がプライマリ/マスター ライセンスから差し引かれて、残りは合計 90 週となります（プライマリに 38 週、セカンダリに 52 週）。
- 30 日経過以降：経過時間が両方の装置から差し引かれます。この場合、通信は 6 週間後に復元されます。したがって、6 週がプライマリ/マスターとセカンダリ/スレーブの両方のライセンスから差し引かれて、残りは合計 84 週となります（プライマリ/マスターに 36 週、セカンダリ/スレーブに 46 週）。

フェールオーバー ペアのアップグレード

フェールオーバーペアでは、両方の装置に同一のライセンスがインストールされている必要はないので、ダウンタイムなしに各装置に新しいライセンスを適用できます。リロードが必要な永続ライセンスを適用する場合、リロード中に他の装置へのフェールオーバーを実行できません。両方の装置でリロードが必要な場合は、各装置を個別にリロードするとダウンタイムは発生しません。

関連トピック

[キーのアクティブ化または非アクティブ化](#) (22 ページ)

ペイロード暗号化機能のないモデル

ペイロード暗号化機能のないモデルを購入することができます。輸出先の国によっては、Cisco ASA シリーズでペイロード暗号化をイネーブルにできません。ASA ソフトウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセーブルにします。

- ユニファイド コミュニケーション
- [VPN]

このモデルでも管理接続用に高度暗号化 (3DES/AES) ライセンスをインストールできます。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使用できます。ボットネットトラフィック フィルタ (SSL を使用) 用のダイナミック データベースをダウンロードすることもできます。

ライセンスを表示すると、VPN およびユニファイド コミュニケーションのライセンスはリストに示されません。

関連トピック

[PAK ライセンスのモニタリング](#) (53 ページ)

ライセンスの FAQ

AnyConnect Premium とボットネット トラフィック フィルタなど、複数の時間ベース ライセンスをアクティブにできますか。

はい。一度に使用できる時間ベース ライセンスは、1 機能につき 1 つです。

複数の時間ベース ライセンスを「スタック」し、時間制限が切れると自動的に次のライセンスが使用されるようにできますか。

はい。ライセンスが同一の場合は、複数の時間ベース ライセンスをインストールすると、時間制限が結合されます。ライセンスが同一でない場合（1000 セッション AnyConnect Premium ライセンスと 2500 セッション ライセンスなど）、ASA はその機能に対して検出された次の時間ベース ライセンスを自動的にアクティブにします。

アクティブな時間ベース ライセンスを維持しながら、新しい永続ライセンスをインストールできますか。

はい。永続ライセンスをアクティブ化しても、時間ベース ライセンスには影響しません。

フェールオーバーのプライマリ装置として共有ライセンスサーバを、セカンダリ装置として共有ライセンス バックアップ サーバを使用できますか。

いいえ。セカンダリ装置は、プライマリ装置と同じ実行ライセンスを使用します。共有ライセンス サーバには、サーバライセンスが必要です。バックアップ サーバには、参加ライセンスが必要です。バックアップサーバは、2つのバックアップサーバの別々のフェールオーバー ペアに配置できます。

フェールオーバー ペアのセカンダリ装置用に、同じライセンスを購入する必要がありますか。

いいえ。バージョン 8.3(1) から、両方の装置に同一のライセンスをインストールする必要はなくなりました。一般的に、ライセンスはプライマリ装置で使用するために購入されます。セカンダリ装置は、アクティブになるとプライマリライセンスを継承します。セカンダリ装置に別のライセンスを持っている場合は（たとえば、8.3 よりも前のソフトウェアに一致するライセンスを購入した場合）、ライセンスは実行フェールオーバー クラスタライセンスに結合されます。ただし、モデルの制限が最大数になります。

AnyConnect Premium（共有）ライセンスに加えて、時間ベースまたは永続の **AnyConnect Premium** ライセンスを使用できますか。

はい。ローカルにインストールされたライセンス（時間ベースライセンスまたは永続ライセンス）のセッション数を使い果たした後、共有ライセンスが使用されます。



(注) 共有ライセンス サーバでは、永続 AnyConnect Premium ライセンスは使用されません。ただし、共有ライセンス サーバライセンスと同時に時間ベース ライセンスを使用することはできます。この場合、時間ベース ライセンスのセッションは、ローカルの AnyConnect Premium セッションにだけ使用できます。共有ライセンスプールに追加して参加システムで使用することはできません。

PAK ライセンスのガイドライン

コンテキスト モードのガイドライン

マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用しません。

フェールオーバーのガイドライン

フェールオーバーまたは [ASA クラスタ ライセンス \(9 ページ\)](#) を参照してください。

モデルのガイドライン

- スマート ライセンスは、ASA v でのみサポートされます。
- 共有ライセンスは、ASA v、ASA 5506-X、ASA 5508-X および ASA 5516-X ではサポートされません。
- ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーションキーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、8.2 よりも前に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、8.2 以降で導入された機能ライセンスをアクティブ化した場合は、アクティベーションキーの下位互換性がなくなります。互換性のないライセンスキーがある場合は、次のガイドラインを参照してください。
 - 以前のバージョンでアクティベーション キーを入力した場合は、ASA はそのキーを使用します（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
 - 新しいシステムで、以前のアクティベーションキーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。
- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバスタな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
 - 複数の時間ベースのアクティベーションキーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくて

も、アクティブライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。

- フェールオーバーペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
- 1つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブのままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

その他のガイドライン

- アクティベーションキーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーションキーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要があり、このことが Cisco TAC によってカバーされている場合は、シスコのライセンスチームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンスチームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- ライセンシングで使うシリアル番号は、**show version** 出力。このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- 1つのユニット上で、同じ機能の2つの別個のライセンスを加算することはできません。たとえば、25セッション SSL VPN ライセンスを購入した後で50セッションライセンスを購入しても、75個のセッションを使用できるわけではなく、使用できるのは最大50個のセッションです。（アップグレード時に、数を増やしたライセンスを購入できることがあります。たとえば25セッションから75セッションへの増加です。このタイプのアップグレードは、2つのライセンスの加算とは別のものです）。
- すべてのライセンスタイプをアクティブ化できますが、機能によっては、機能どうしの組み合わせができないものがあります。AnyConnect Essentials ライセンスの場合、次のライセンスとは互換性がありません。AnyConnect Premium ライセンス、AnyConnect Premium（共有）ライセンス、およびAdvanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスをインストールした場合（使用中のモデルで利用できる場合）、このライセンスが前述のライセンスの代わりに使用されます。**webvpn**、次に **no anyconnect-essentials** コマンドを使用して、設定で AnyConnect Essentials ライセンスを無効にし、他のライセンスを使用できます。

PAK ライセンスの設定

この項では、アクティベーションキーを取得する方法とそれをアクティブ化する方法について説明します。また、キーを非アクティブ化することもできます。

ライセンスの PAK の注文とアクティベーションキーの取得

ASAにライセンスをインストールするには製品認証キーが必要です。その後、それをCisco.comに登録してアクティベーションキーを取得することができます。次に、ASAのアクティベーションキーを入力できます。機能ライセンスごとに個別の製品認証キーが必要になります。PAKが組み合わせられて、1つのアクティベーションキーになります。デバイス発送時に、すべてのライセンスPAKが提供されている場合もあります。ASAには基本ライセンスまたはSecurity Plusライセンスがプリインストールされ、ご使用資格を満たしている場合にはStrong Encryption (3DES/AES) ライセンスも提供されます。無料のStrong Encryptionライセンスを手動でリクエストする必要がある場合は、<http://www.cisco.com/go/license>を参照してください。

始める前に

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>

まだアカウントをお持ちでない場合は、このリンクをクリックして[新しいアカウントをセットアップ](#)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。

手順

ステップ1 追加ライセンスを購入するには、<http://www.cisco.com/go/ccw>を参照してください。次のAnyConnect発注ガイドおよびFAQを参照してください。

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

ライセンスを購入した後、製品認証キー (PAK) が記載された電子メールを受け取ります。AnyConnectライセンスの場合、ユーザセッションの同じプールを使用する複数のASAに適用できるマルチユース PAKを受け取ります。場合によっては、PAKが記載された電子メールを受け取るまで数日かかることがあります。

ASA FirePOWER モジュールは、ASAとは別のライセンスメカニズムを使用します。詳しくは、ご使用のモデルの[クイックスタートガイド](#)を参照してください。

ステップ2 次のコマンドを入力して、ASAのシリアル番号を取得します。

```
show version | grep Serial
```

ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

ステップ3 アクティベーション キーを取得するには、以下のライセンス Web サイトに移動します。

<http://www.cisco.com/go/license>

ステップ4 プロンプトが表示されたら、次の情報を入力します。

- Product Authorization Key（キーが複数ある場合は、まず1つを入力します。キーごとに個別のプロセスとして入力する必要があります）
- ASA のシリアル番号
- 電子メールアドレス

アクティベーションキーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。時間ベースライセンスの場合は、ライセンスごとに個別のアクティベーションキーがあります。

ステップ5 さらに追加の製品認証キーがある場合は、製品認証キーごとにこの手順を繰り返します。すべての Product Authorization Key を入力した後、最後に送信されるアクティベーションキーには、登録した永続機能がすべて含まれています。

ステップ6 キーのアクティブ化または非アクティブ化（22 ページ）に基づいて、アクティベーションキーをインストールします。

高度暗号化ライセンスの取得

ASDM（および他の多数の機能）を使用するには、高度暗号化（3DES/AES）ライセンスをインストールする必要があります。ASAに高度暗号化ライセンスがプリインストールされていない場合は、ライセンスを無料で入手できます。高度暗号化ライセンスに関するそれぞれ国の資格を満たす必要があります。

手順

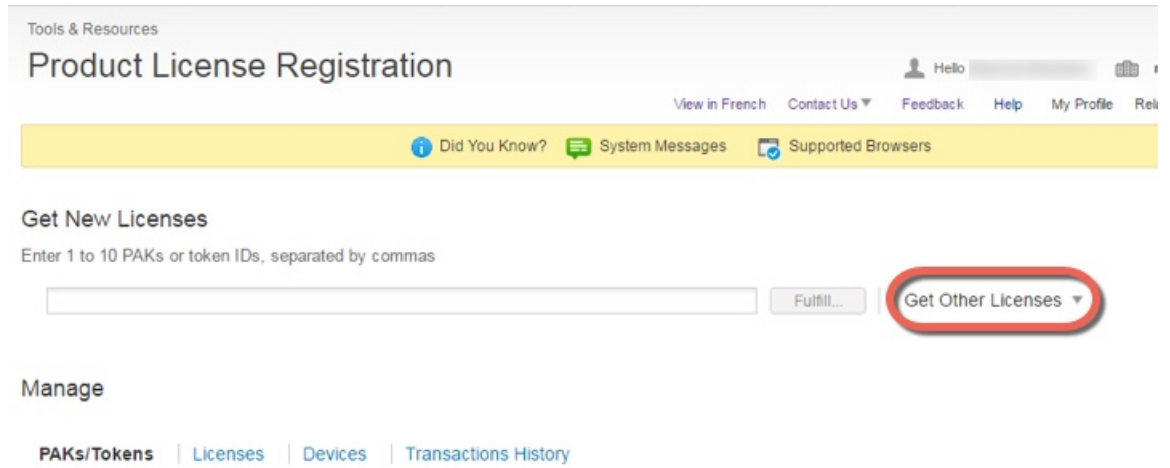
ステップ1 次のコマンドを入力して、ASA のシリアル番号を取得します。

```
show version | grep Serial
```

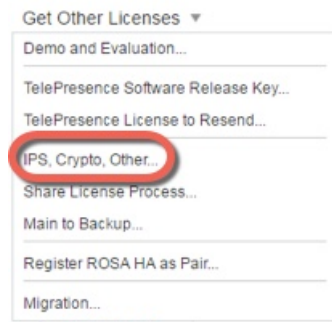
このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

ステップ2 <https://www.cisco.com/go/license> を参照し、[Get Other Licenses] をクリックしてください。

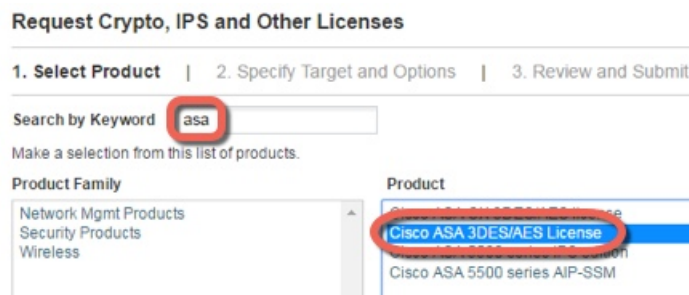
図 1:他のライセンスの取得



ステップ 3 [IPS, Crypto, Other] を選択します。

図 2: *IPS*、*Crypto*、その他

ステップ 4 [Search by Keyword] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 3: *Cisco ASA 3DES/AES* ライセンス

ステップ 5 [Smart Acfcount]、[Virtual Account] を選択し、ASA の [Serial Number] を入力して、[Next] をクリックします。

図 4: スマートアカウント、バーチャルアカウント、シリアル番号

Request Crypto, IPS and Other Licenses

1. Select Product | 2. Specify Target and Options

Smart Account
Select one ...

Virtual Account
Select one... Required with Smart Account

Cisco ASA 3DES/AES License
Serial Number: FCH1714J6HP

ステップ 6 送信先の電子メールアドレスとエンドユーザ名は自動的に入力されます。必要に応じて追加の電子メールアドレスを入力します。[I Agree] チェックボックスをオンにして、[Submit] をクリックします。

図 5: 送信

Request Crypto, IPS and Other Licenses

1. Select Product | 2. Specify Target and Options | 3. Review and Submit

Recipient and Owner Information
Enter multiple email addresses separated by commas. Your License Key will be emailed within the hour to the specified email addresses.

Send To: Add...

End User: Edit..

License Request

Serial Number
FCH1714J6HP

Smart Account	SKU Name	Qty
▶ Cisco Internal	ASA5500-ENCR-K9	1

ステップ 7 その後、アクティベーションキーの記載された電子メールが届きますが、[Manage]>[Licenses] エリアからキーをすぐにダウンロードすることもできます。

ステップ 8 キーのアクティブ化または非アクティブ化 (22 ページ) に基づいて、アクティベーションキーを適用します。

キーのアクティブ化または非アクティブ化

この項では、新しいアクティベーションキーの入力と、時間ベース キーのアクティブ化および非アクティブ化の方法について説明します。

始める前に

- すでにマルチ コンテキスト モードに入っている場合は、システム実行スペースにこのアクティベーション キーを入力します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。次の表に、リロードが必要なライセンスを示します。

表 2:永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード

手順

ステップ 1 アクティベーション キーを ASA に適用します。

activation-key *key* [**activate** | **deactivate**]

例：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

キーは、5つのエレメントからなる 16 進文字列です。各エレメントは1つのスペースで区切られます。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。

1つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。

activate および **deactivate** キーワードは、時間ベース キーだけに使用できます。値を入力しない場合は、**activate** がデフォルトです。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。アクティブな時間ベース キーを非アクティブにするには、**deactivate** キーワードを入力します。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブ ステートでインストールされます。

ステップ 2 (場合によって必須) ASA をリロードします。

reload

永続ライセンスによっては、新しいアクティベーション キーの入力後に ASA をリロードする必要があります。リロードが必要な場合は、次のメッセージが表示されます。

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

関連トピック

[時間ベースライセンス](#) (2 ページ)

共有ライセンスの設定 (AnyConnect 3 以前)



- (注) ASAの共有ライセンス機能は、AnyConnect 4以降のライセンスではサポートされていません。AnyConnect ライセンスが共有されているため、共有サーバまたは参加ライセンスは不要になりました。

この項では、共有ライセンス サーバと参加システムを設定する方法について説明します。

共有ライセンスについて

共有ライセンスを使用すると、多数の AnyConnect Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバとして、残りを共有ライセンス参加システムとして設定します。

共有ライセンスのサーバと参加システムについて

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバを含む共有ライセンス参加者とするかを決定し、各デバイスシリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. (オプション) 別の ASA を共有ライセンス バックアップ サーバとして指定します。バックアップ サーバには 1 台のみ指定できます。



- (注) 共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンスサーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバに登録します。



- (注) 参加者は IP ネットワークを経由してサーバと通信する必要がありますが、同じサブネット上にある必要はありません。

- 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。
- 参加者がローカルライセンスのセッションを使い果たした場合、参加者は共有ライセンスサーバに 50 セッション単位で追加セッションの要求を送信します。
- 共有ライセンス サーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。



(注) 共有ライセンス サーバは、共有ライセンス プールに参加することもできます。参加には参加ライセンスもサーバライセンスも必要ありません。

- 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。
 - 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバが要求に適切に対応できるまで続けます。
9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。



(注) ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバ間の通信問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔 3 倍の時間が経過した後で、サーバはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンスサーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンスサーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

共有ライセンス バックアップ サーバについて

共有ライセンス バックアップ サーバは、バックアップの役割を実行する前にメインの共有ライセンスサーバへの登録に成功している必要があります。登録時には、メインの共有ライセン

スサーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メインサーバとバックアップサーバは、10秒間隔でデータを同期します。初回同期の後で、バックアップサーバはリロード後でもバックアップの役割を実行できます。

メインサーバがダウンすると、バックアップサーバがサーバ動作を引き継ぎます。バックアップサーバは継続して最大30日間動作できます。30日を超えると、バックアップサーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メインサーバをこの30日間に確実に復旧するようにします。クリティカルレベルのsyslogメッセージが15日めに送信され、30日めに再送信されます。

メインサーバが復旧した場合、メインサーバはバックアップサーバと同期してから、サーバ動作を引き継ぎます。

バックアップサーバがアクティブでないときは、メインの共有ライセンスサーバの通常の参加者として動作します。



- (注) メインの共有ライセンスサーバの初回起動時には、バックアップサーバは独立して5日間のみ動作できます。動作制限は30日に到達するまで日ごとに増加します。また、メインサーバがその後短時間でもダウンした場合、バックアップサーバの動作制限は日ごとに減少します。メインサーバが復旧した場合、バックアップサーバは再び日ごとに増加を開始します。たとえば、メインサーバが20日間ダウンしていて、その期間中バックアップサーバがアクティブであった場合、バックアップサーバには、10日間の制限のみが残っています。バックアップサーバは、非アクティブなバックアップとしてさらに20日間が経過した後で、最大の30日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

フェールオーバーと共有ライセンス

ここでは、共有ライセンスとフェールオーバーの相互作用について説明します。

フェールオーバーと共有ライセンスサーバ

この項では、メインサーバおよびバックアップサーバと、フェールオーバーとの相互作用について説明します。共有ライセンスサーバでは、VPNゲートウェイやファイアウォールなど、ASAとしての通常機能も実行されます。このため、メインとバックアップの共有ライセンスサーバにフェールオーバーを設定して、信頼性を高めることをお勧めします。

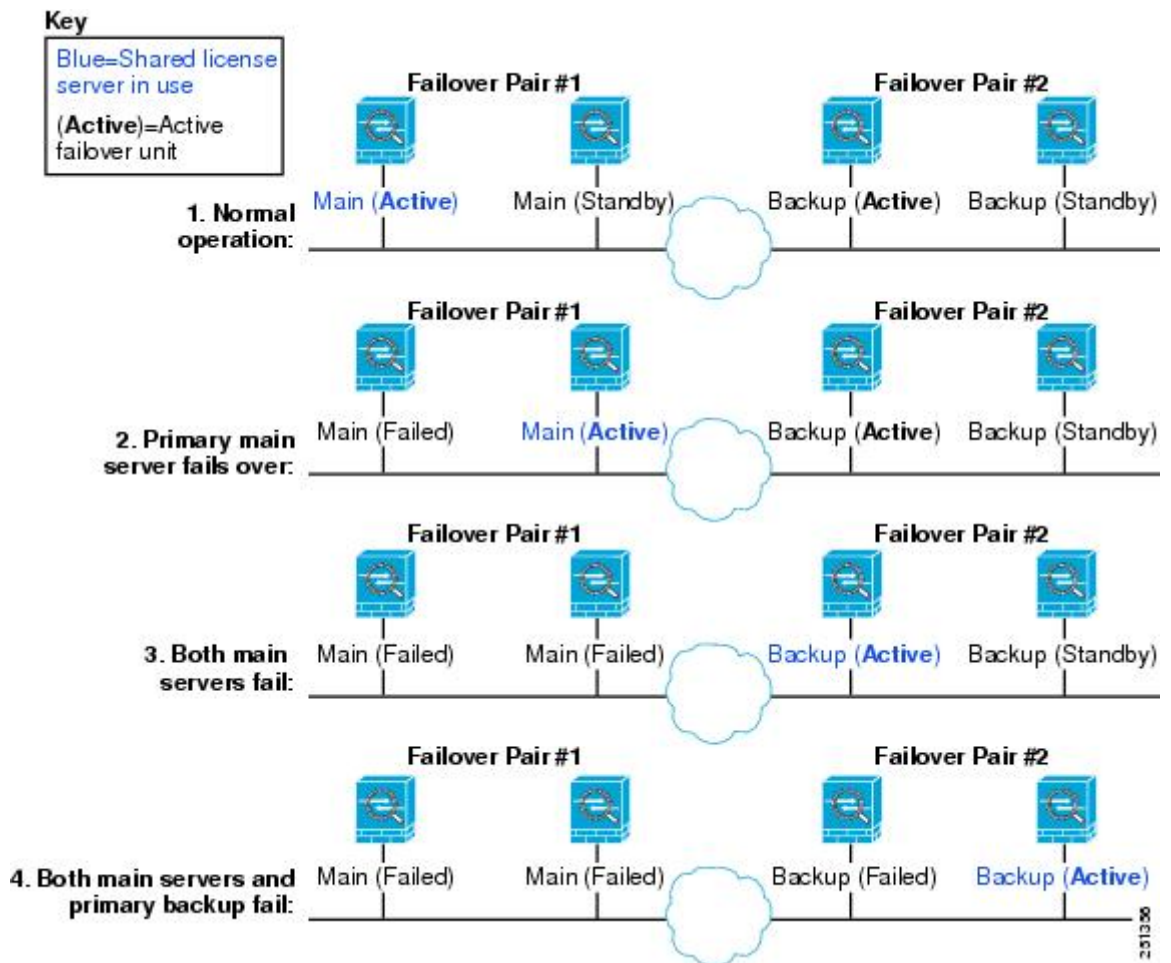


- (注) バックアップサーバメカニズムとフェールオーバーは異なりますが、両者には互換性があります。
- 共有ライセンスはシングルコンテキストモードでだけサポートされるため、アクティブ/アクティブフェールオーバーはサポートされません。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置が主要な共有ライセンスサーバとして機能し、スタンバイ装置はフェールオーバー後に主要な共有ライセンスサーバとして機能します。スタンバイ装置は、バックアップの共有ライセンスサーバとしては機能しません。必要に応じて、バックアップサーバとして機能する装置のペアを追加します。

たとえば、2組のフェールオーバー ペアがあるネットワークを使用するとします。ペア #1 にはメインのライセンスサーバが含まれます。ペア #2 にはバックアップサーバが含まれます。ペア #1 のプライマリ装置がダウンすると、ただちに、スタンバイ装置が新しくメインライセンスサーバになります。ペア #2 のバックアップサーバが使用されることはありません。ペア #1 の装置が両方ともダウンした場合だけ、ペア #2 のバックアップサーバが共有ライセンスサーバとして使用されるようになります。ペア #1 がダウンしたままで、ペア #2 のプライマリ装置もダウンした場合は、ペア #2 のスタンバイ装置が共有ライセンスサーバとして使用されるようになります (次の図を参照)。

図 6: フェールオーバーと共有ライセンスサーバ



スタンバイ バックアップサーバは、プライマリ バックアップサーバと同じ動作制限を共有します。スタンバイ装置がアクティブになると、その時点からプライマリ装置のカウントダウンを引き継ぎます。

関連トピック

[共有ライセンス バックアップ サーバについて](#) (25 ページ)

フェールオーバーと共有ライセンス参加システム

参加システムのペアについては、両方の装置を共有ライセンスサーバに登録します。登録時には、個別の参加システム ID を使用します。アクティブ装置の参加システム ID は、スタンバイ装置と同期されます。スタンバイ装置は、アクティブに切り替わる時に、この ID を使用して転送要求を生成します。この転送要求によって、以前にアクティブだった装置から新しくアクティブになる装置に共有セッションが移動します。

参加者の最大数

ASA では、共有ライセンスの参加システム数に制限がありません。ただし、共有ネットワークの規模が非常に大きいと、ライセンスサーバのパフォーマンスに影響する場合があります。この場合は、参加システムのリフレッシュ間隔を長くするか、共有ネットワークを2つ作成することをお勧めします。

共有ライセンス サーバの設定

この項では、ASA を共有ライセンス サーバとして設定する方法について説明します。

始める前に

サーバが共有ライセンス サーバ キーを持っている必要があります。

手順

ステップ 1 共有秘密を設定します。

license-server secret *secret*

例：

```
ciscoasa(config)# license-server secret farscape
```

secret は、4 ～ 128 文字の ASCII 文字の文字列です。この秘密を持つ参加システムが、ライセンス サーバを使用できます。

ステップ 2 (オプション) 更新間隔を設定します。

license-server refresh-interval *seconds*

例：

```
ciscoasa(config)# license-server refresh-interval 100
```

間隔は 10 ～ 300 秒です。この値が、サーバと通信する頻度として参加システムに設定されます。デフォルトは 30 秒です。

ステップ 3 (オプション) サーバが参加ユニットからの SSL 接続をリッスンするポートを設定します。

license-server port *port*

例：

```
ciscoasa(config)# license-server port 40000
```

port は 1 ～ 65535 です。デフォルトは、TCP ポート 50554 です。

ステップ 4 (オプション) バックアップサーバの IP アドレスとシリアル番号を指定します。

license-server backup *address backup-id serial_number* [**ha-backup-id** *ha_serial_number*]

例：

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
```

バックアップサーバがフェールオーバーペアの一部である場合は、スタンバイ装置のシリアル番号も指定します。1つのバックアップサーバとそのオプションのスタンバイユニットのみを指定できます。

ステップ 5 このユニットを共有ライセンスサーバとしてイネーブルにします。

license-server enable *interface_name*

例：

```
ciscoasa(config)# license-server enable inside
```

参加システムがサーバと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップサーバを設定し、このユニットを *inside* インターフェイスおよび *dmz* インターフェイスで共有ライセンスサーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

共有ライセンスバックアップサーバの設定（オプション）

この項では、共有ライセンスのメインサーバがダウンした場合にバックアップサーバとして機能する参加システムをイネーブルにします。

始める前に

バックアップサーバには、共有ライセンス参加キーが必要です。

手順

ステップ1 共有ライセンスサーバのIPアドレスと共有秘密を指定します。

license-server address *address* **secret** *secret* [**port** *port*]

例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

デフォルトポートをサーバコンフィギュレーションで変更した場合は、同じポートをバックアップサーバにも設定します。

ステップ2 このユニットを共有ライセンスバックアップサーバとしてイネーブルにします。

license-server backup enable *interface_name*

例：

```
ciscoasa(config)# license-server backup enable inside
```

参加システムがサーバと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、ライセンスサーバと共有秘密を指定し、このユニットを内部インターフェイスとdmzインターフェイス上のバックアップ共有ライセンスサーバとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

共有ライセンス パーティシパントの設定

この項では、共有ライセンス サーバと通信する共有ライセンス参加システムを設定します。

始める前に

参加システムが共有ライセンス参加キーを持っている必要があります。

手順

ステップ 1 共有ライセンス サーバの IP アドレスと共有秘密を指定します。

```
license-server address address secret secret [port port]
```

例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

デフォルト ポートをサーバ コンフィギュレーションで変更した場合は、同じポートを参加システムにも設定します。

ステップ 2 (オプション) バックアップ サーバを設定した場合は、バックアップ サーバのアドレスを入力します。

```
license-server backup address address
```

例：

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

例

次に、ライセンス サーバの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape  
ciscoasa(config)# license-server backup address 10.1.1.2
```

モデルごとにサポートされている機能のライセンス

この項では、各モデルに使用できるライセンスと、ライセンスに関する特記事項について説明します。

モデルごとのライセンス

この項では、各モデルに使用できる機能のライセンスを示します。

イタリック体で示された項目は、基本ライセンス（または Security Plus など）ライセンスバージョンを置換できる個別のオプションライセンスです。オプションライセンスは、混在させることも統一することもできます。



(注) 一部の機能は互換性がありません。互換性情報については、個々の機能の章を参照してください。

ペイロード暗号化機能のないモデルの場合は、次に示す機能の一部がサポートされません。サポートされない機能のリストについては、[ペイロード暗号化機能のないモデル（15 ページ）](#)を参照してください。

ライセンスの詳細については、[ライセンスに関する注意事項（5 ページ）](#)を参照してください。

ASA 5506-X および ASA 5506W-X のライセンス機能

次の表に、ASA 5506-X および ASA 5506W-X のライセンス機能を示します。

ライセンス	基本ライセンス	Security Plus 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	サポートなし
ファイアウォールの接続、同時	20,000	50,000
キャリア	サポートなし	サポートなし
合計 TLS プロキシセッション	160	160

ライセンス	基本ライセンス		Security Plus ライセンス	
VPN ライセンス				
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 50	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 50
その他の VPN ピア	10		50	
合計 VPN ピア。全 タイプの 合計	50		50	
VPN ロード バラン シング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)	基本 (DES)	オプションライセンス：強化 (3DES/AES)
フェール オーバー	サポートなし		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		サポートなし	
クラス タ	サポートなし		サポートなし	
VLAN、 最大	5		30	

ASA 5506H-X ライセンスの各機能

次の表に、ASA 5506H-X のライセンス機能を示します。

ライセンス	基本ライセンス	
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	50,000	
キャリア	サポートなし	
合計 UC プロキシセッション	160	
VPN ライセンス		
AnyConnect Plus または Apex ライセンス（個別に購入）、最大プレミアムピア	50	
合計 VPN ピア。全タイプの合計	50	
その他の VPN ピア	50	
VPN ロードバランシング	イネーブル	
一般ライセンス		
暗号化	基本（DES）	オプションライセンス：強化（3DES/AES）
フェールオーバー	Active/Standby または Active/Active	
セキュリティコンテキスト	サポートなし	
クラスター	サポートなし	
VLAN、最大	30	

ASA 5508-X ライセンスの各機能

次の表に、ASA 5508-X のライセンス機能を示します。

ライセンス	基本ライセンス		
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		
キャリア	サポートなし		
合計 TLS プロキシセッション	320		
VPN ライセンス			
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 100	
合計 VPN ピア。全タイプの合計	100		
その他の VPN ピア	100		
VPN ロードバランシング	イネーブル		
一般ライセンス			
暗号化	基本 (DES)	オプション ライセンス：強化 (3DES/AES)	
フェールオーバー	Active/Standby または Active/Active		
セキュリティコンテキスト	2	オプション ライセンス：	5
クラスタ	サポートなし		
VLAN、最大	50		

ASA 5512-X ライセンスの機能

次の表に、ASA 5512-X のライセンス機能を示します。

ライセンス	基本ライセンス					Security Plus ライセンス						
ファイアウォール ライセンス												
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能				ディセーブル	オプションの時間ベース ライセンス：使用可能					
ファイアウォールの接続、同時	100,000					250,000						
キャリア	サポートなし					サポートなし						
合計 TLS プロキシセッション	2	オプション ライセンス：					2	オプション ライセンス：				
		24	50	100	250	500		24	50	100	250	500
VPN ライセンス												
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 250				ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 250					
その他の VPN ピア	250					250						
合計 VPN ピア。全タイプの合計	250					250						
VPN ロードバランシング	サポートなし					イネーブル						

ライセンス	基本ライセンス		Security Plus ライセンス	
一般ライセンス				
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)	基本 (DES)	オプションライセンス：強化 (3DES/AES)
フェールオーバー	サポートなし		Active/Standby または Active/Active	
セキュリティコンテキスト	サポートなし		2	オプションライセンス：5
クラスタ	サポートなし		2	
IPS モジュール	ディセーブル	オプションライセンス：使用可能	ディセーブル	オプションライセンス：使用可能
VLAN、最大	50		100	

ASA 5515-X ライセンスの機能

次の表に、ASA 5515-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能
ファイアウォールの接続、同時	250,000	

ライセンス	基本ライセンス						
キャリア	サポートなし						
合計 TLS プ ロキシ セッ ション	2	オプションライセンス：	24	50	100	250	500
VPN ライセンス							
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 250					
その他 の VPN ピア	250						
合計 VPN ピ ア。全 タイプ の合計	250						
VPN ロード バラン シング	イネーブル						
一般ライセンス							
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)					
フェー ルオー バー	Active/Standby または Active/Active						
セキュ リティ コンテ キスト	2	オプションライセンス：	5				
クラス タ	2						

ライセンス	基本ライセンス	
IPS モジュール	ディセーブル	オプションライセンス：使用可能
VLAN、最大	100	

ASA 5516-X ライセンスの機能

次の表に、ASA 5516-X のライセンス機能を示します。

ライセンス	基本ライセンス	
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	250,000	
キャリア	サポートなし	
合計 TLS プロキシセッション	1000	
VPN ライセンス		
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 300
その他の VPN ピア	300	
合計 VPN ピア。全タイプの合計	300	
VPN ロードバランシング	イネーブル	
一般ライセンス		
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)

ASA 5525-X ライセンスの各機能

ライセンス	基本ライセンス		
フェールオーバー	Active/Standby または Active/Active		
セキュリティコンテキスト	2	オプションライセンス：	5
クラスタ	2		
VLAN、最大	150		

ASA 5525-X ライセンスの各機能

次の表に、ASA 5525-X のライセンス機能を示します。

ライセンス	基本ライセンス								
ファイアウォール ライセンス									
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能							
ファイアウォールの接続、同時	500,000								
キャリア	ディセーブル	オプション ライセンス：使用可能							
合計 TLS プロキシセッション	2	オプション ライセンス：	24	50	100	250	500	750	1000
VPN ライセンス									
AnyConnect ピア	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス：最大 750							
その他の VPN ピア	750								

ライセンス	基本ライセンス				
合計 VPN ピア。全 タイプの の合計	750				
VPN ロード バラン シング	イネーブル				
一般ライセンス					
暗号化	基本 (DES)	オプション ライセンス：強化 (3DES/AES)			
フェール オーバー	Active/Standby または Active/Active				
セキュ リティ コンテ キスト	2	オプション ライセンス：	5	10	20
クラス タ	2				
IPS モ ジュール	ディセーブル	オプション ライセンス：使用可能			
VLAN、 最大	200				

ASA 5545-X ライセンスの機能

次の表に、ASA 5545-X のライセンス機能を示します。

ライセ ンス	基本ライセンス
ファイアウォール ライセンス	

ライセンス	基本ライセンス									
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能								
ファイアウォールの接続、同時	750,000									
キャリア	ディセーブル	オプション ライセンス：使用可能								
合計 TLS プロキシセッション	2	オプション ライセンス：	24	50	100	250	500	750	1000	2000
VPN ライセンス										
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 2500								
その他の VPN ピア	2500									
合計 VPN ピア。全タイプの合計	2500									
VPN ロード バランシング	イネーブル									
一般ライセンス										
暗号化	基本 (DES)	オプション ライセンス：強化 (3DES/AES)								

ライセンス	基本ライセンス					
フェールオーバー	Active/Standby または Active/Active					
セキュリティコンテキスト	2	オプションライセンス：	5	10	20	50
クラスタ	2					
IPS モジュール	ディセーブル	オプションライセンス：使用可能				
VLAN、最大	300					

ASA 5555-X ライセンスの機能

次の表に、ASA 5555-X のライセンス機能を示します。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能
ファイアウォールの接続、同時	1,000,000	
キャリア	ディセーブル	オプションライセンス：使用可能

ライセンス	基本ライセンス									
合計 TLS プ ロキシ セッ ション	2	オプション ライセンス：								
		24	50	100	250	500	750	1000	2000	3000
VPN ライセンス										
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 5000								
その他 の VPN ピア	5000									
合計 VPN ピ ア。全 タイプ の合計	5000									
VPN ロード バラン シング	イネーブル									
一般ライセンス										
暗号化	基本 (DES)	オプション ライセンス：強化 (3DES/AES)								
フェー ルオー バー	Active/Standby または Active/Active									
セキュ リティ コンテ キスト	2	オプション ライセンス：	5	10	20	50	100			
クラス タ	2									
IPS モ ジュール	ディセーブル	オプション ライセンス：使用可能								

ライセンス	基本ライセンス
VLAN、最大	500

ASA 5585-X (SSP-10) ライセンスの各機能

次の表に、ASA 5585-X (SSP-10) のライセンス機能を示します。

同一のシャーシで同じレベルの2つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-10 と SSP-20 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて2つの SSP をフェールオーバーペアとして使用できます。

ライセンス	基本ライセンスと Security Plus ライセンス									
ファイアウォール ライセンス										
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能								
ファイアウォールの接続、同時	1,000,000									
キャリア	ディセーブル	オプション ライセンス：使用可能								
合計 TLS プロキシセッション	2	オプション ライセンス：								
		24	50	100	250	500	750	1000	2000	3000
VPN ライセンス										
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 5000								
その他の VPN ピア	5000									

ライセンス	基本ライセンスと Security Plus ライセンス							
合計 VPN ピア。全 タイプの 合計	5000							
VPN ロード バラン シング	イネーブル							
一般ライセンス								
10 GE I/O	基本ライセンス：ディセーブル。ファイバ ifcs は 1 GE で動作します			Security Plus ライセンス：イネーブル。ファイバ ifcs は 10 GE で動作します				
暗号化	基本 (DES)		オプション ライセンス：強化 (3DES/AES)					
フェール オーバー	Active/Standby または Active/Active							
セキュ リティ コンテ キスト	2	オプション ライセンス：		5	10	20	50	100
クラス タ	ディセーブル		オプション ライセンス: 16 単位で利用可能					
VLAN、 最大	1024							

ASA 5585-X (SSP-20) ライセンスの機能

次の表に、ASA 5585-X (SSP-20) のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません (たとえば、SSP-20 と SSP-40 の組み合わせはサポートされていません)。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。



(注) 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシセッションの最大数は 5000 です。

ライセンス	基本ライセンスと Security Plus ライセンス										
ファイアウォール ライセンス											
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能									
ファイアウォールの接続、同時	2,000,000										
キャリア	ディセーブル	オプション ライセンス：使用可能									
合計 TLS プロキシセッション	2	オプション ライセンス：									
		24	50	100	250	500	750	1000	2000	3000	5000
VPN ライセンス											
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 10,000									
その他の VPN ピア	10,000										
合計 VPN ピア。全タイプの合計	10,000										

ASA 5585-X (SSP-40 および -60) ライセンスの機能

ライセンス	基本ライセンスと Security Plus ライセンス								
VPN ロード バラン シング	イネーブル								
一般ライセンス									
10 GE I/O	基本ライセンス：ディセーブル。ファイバ ifcs は 1 GE で動作します				Security Plus ライセンス：イネーブル。ファイバ ifcs は 10 GE で動作します				
暗号化	基本 (DES)		オプションライセンス：強化 (3DES/AES)						
フェー ルオー バー	Active/Standby または Active/Active								
セキュ リティ コンテ キスト	2	オプションライセンス：		5	10	20	50	100	250
クラス タ	ディセーブル		オプションライセンス: 16 単位で利用可能						
VLAN、 最大	1024								

ASA 5585-X (SSP-40 および -60) ライセンスの機能

次の表に、ASA 5585-X (SSP-40 および -60) のライセンス機能を示します。

同一のシャーシで同じレベルの 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません (たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません)。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。



(注) 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシセッションの最大数は 5000 です。

ライセ ンス	基本ライセンス
ファイアウォール ライセンス	

ライセンス	基本ライセンス											
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能										
ファイアウォールの接続、同時	5585-X (SSP-40) : 4,000,000						5585-X (SSP-60) : 10,000,000					
キャリア	ディセーブル	オプションライセンス：使用可能										
合計 TLS プロキシセッション	2	オプションライセンス：										
		24	50	100	250	500	750	1000	2000	3000	5000	10,000
VPN ライセンス												
AnyConnectピア	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス：最大 10,000										
その他の VPN ピア	10,000											
合計 VPN ピア。全タイプの合計	10,000											
VPN ロードバランシング	イネーブル											
一般ライセンス												
10 GE I/O	イネーブル。ファイバインターフェイスは 10 GE で動作											
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)										

ライセンス	基本ライセンス							
フェールオーバー	Active/Standby または Active/Active							
セキュリティコンテキスト	2	オプションライセンス：	5	10	20	50	100	250
クラスタ	ディセーブル	オプションライセンス: 16 単位で利用可能						
VLAN、最大	1024							

ASASM ライセンスの機能

次の表に、ASA サービス モジュールのライセンス機能を示します。



(注) 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシセッションの最大数は 5000 です。

ライセンス	基本ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	ディセーブル	オプションの時間ベース ライセンス：使用可能
ファイアウォールの接続、同時	10,000,000	
キャリア	ディセーブル	オプション ライセンス：使用可能

ライセンス	基本ライセンス										
合計 TLS プ ロキシ セッ ション	2	オプション ライセンス：									
		24	50	100	250	500	750	1000	2000	3000	5000
VPN ライセンス											
AnyConnect ピア	ディセーブル	オプションの AnyConnect Plus または Apex ライセンス：最大 10,000									
その他 の VPN ピア	10,000										
合計 VPN ピ ア。全 タイプ の合計	10,000										
VPN ロード バラ ン シ ン グ	イネーブル										
一般ライセンス											
暗号化	基本 (DES)	オプション ライセンス：強化 (3DES/AES)									
フェー ルオー バー	Active/Standby または Active/Active										
セキュ リテイ コンテ キスト	2	オプション ライセンス：									
		5	10	20	50	100	250				
クラス タ	サポートなし										
VLAN、 最大	1000										

ISA 3000 ライセンスの各機能

次の表に、ISA 3000 のライセンス機能を示します。

ライセンス	基本ライセンス		Security Plus 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		サポートなし	
ファイアウォールの接続、同時	20,000		50,000	
キャリア	サポートなし		サポートなし	
合計 TLS プロキシセッション	160		160	
VPN ライセンス				
AnyConnect ピア	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 25	ディセーブル	オプションの <i>AnyConnect Plus</i> または <i>Apex</i> ライセンス：最大 25
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	25		50	
VPN ロードバランシング	サポートなし		サポートなし	

ライセンス	基本ライセンス		Security Plus ライセンス	
一般ライセンス				
暗号化	基本 (DES)	オプションライセンス：強化 (3DES/AES)	基本 (DES)	オプションライセンス：強化 (3DES/AES)
フェールオーバー	サポートなし		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		サポートなし	
クラスタ	サポートなし		サポートなし	
VLAN、最大	5		25	

PAK ライセンスのモニタリング

この項では、ライセンス情報の表示方法について説明します。

現在のライセンスの表示

この項では、現在のライセンスと、時間ベース アクティベーション キーの残り時間を表示する方法について説明します。

始める前に

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN および Unified Communications ライセンスは一覧に示されません。詳細については、「[ペイロード暗号化機能のないモデル \(15 ページ\)](#)」を参照してください。

手順

永続ライセンス、アクティブな時間ベースライセンス、および実行ライセンスを表示します。実行ライセンスとは、永続ライセンスとアクティブな時間ベース ライセンスの組み合わせです。

show activation-key [detail]

detail キーワードを使用すると、非アクティブな時間ベース ライセンスも表示されます。

フェールオーバーまたはクラスタ ユニットでは、このコマンドは、すべてのユニットの結合キーである「クラスタ」ライセンスも示します。

例

例 1：show activation-key コマンドのスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、およびアクティブな各時間ベース ライセンスを示す、スタンドアロン ユニットの **show activation-key** コマンドの出力例を示します。

```
ciscoasa# show activation-key

Serial Number: JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xale21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                   : 150            perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
VPN-DES                          : Enabled        perpetual
VPN-3DES-AES                     : Enabled        perpetual
Security Contexts                : 10             perpetual
GTP/GPRS                        : Enabled        perpetual
AnyConnect Premium Peers        : 2              perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                  : 750            perpetual
Total VPN Peers                  : 750            perpetual
Shared License                   : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
Advanced Endpoint Assessment     : Disabled       perpetual
UC Phone Proxy Sessions         : 12             62 days
Total UC Proxy Sessions         : 12             62 days
Botnet Traffic Filter            : Enabled        646 days
Intercompany Media Engine       : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter            : Enabled        646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions         : 10             62 days
```

例 2：show activation-key detail のスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベースライセンスの組み合わせ）、および永続ライセンスとインストールされている各時間ベースライセンス（アクティブおよび非アクティブ）を示す、スタンドアロンユニットの **show activation-key detail** コマンドの出力例を示します。

```
ciscoasa# show activation-key detail
```

```
Serial Number: 88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : 8 perpetual
VLANs : 20 DMZ Unrestricted
Dual ISPs : Enabled perpetual
VLAN Trunk Ports : 8 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Standby perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 25 perpetual
Total VPN Peers : 25 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 39 days
Intercompany Media Engine : Disabled perpetual
```

```
This platform has an ASA 5512-X Security Plus license.
```

```
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : 8 perpetual
VLANs : 20 DMZ Unrestricted
Dual ISPs : Enabled perpetual
VLAN Trunk Ports : 8 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Standby perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 25 perpetual
Total VPN Peers : 25 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 39 days
Intercompany Media Engine : Disabled perpetual
```

```
The flash permanent activation key is the SAME as the running permanent key.
```

```
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter : Enabled 39 days
```

```
Inactive Timebased Activation Key:
Oxyadayada3 Oxyadayada3 Oxyadayada3 Oxyadayada3 Oxyadayada3
AnyConnect Premium Peers          : 25      7 days
```

例3：show activation-key detail に対するフェールオーバー ペアのプライマリユニット 出力

次に、プライマリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスター」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットの永続ライセンス。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key detail
```

```
Serial Number: P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xale21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs               : 150          perpetual
Inside Hosts                : Unlimited perpetual
Failover                    : Active/Active perpetual
VPN-DES                     : Enabled   perpetual
VPN-3DES-AES                : Enabled   perpetual
Security Contexts           : 12       perpetual
GTP/GPRS                    : Enabled   perpetual
AnyConnect Premium Peers    : 2        perpetual
AnyConnect Essentials       : Disabled perpetual
Other VPN Peers             : 750     perpetual
Total VPN Peers             : 750     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   33 days
Intercompany Media Engine   : Disabled perpetual
```

```
This platform has an ASA 5520 VPN Plus license.
```

```
Failover cluster licensed features for this platform:
```

```
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs               : 150          perpetual
Inside Hosts                : Unlimited perpetual
```



```

Failover                : Active/Active  perpetual
VPN-DES                 : Enabled      perpetual
VPN-3DES-AES           : Enabled      perpetual
Security Contexts      : 12          perpetual
GTP/GPRS                : Enabled      perpetual
AnyConnect Premium Peers : 4          perpetual
AnyConnect Essentials  : Disabled    perpetual
Other VPN Peers        : 750        perpetual
Total VPN Peers        : 750        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 : 4          perpetual
Total UC Proxy Sessions : 4          perpetual
Botnet Traffic Filter  : Enabled      33 days
Intercompany Media Engine : Disabled     perpetual

```

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:

```

Maximum Physical Interfaces : Unlimited    perpetual
Maximum VLANs              : 150         perpetual
Inside Hosts                : Unlimited    perpetual
Failover                    : Active/Active perpetual
VPN-DES                     : Enabled      perpetual
VPN-3DES-AES                : Disabled    perpetual
Security Contexts           : 2           perpetual
GTP/GPRS                    : Disabled    perpetual
AnyConnect Premium Peers    : 2           perpetual
AnyConnect Essentials       : Disabled    perpetual
Other VPN Peers             : 750        perpetual
Total VPN Peers             : 750        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       : Disabled    perpetual
Intercompany Media Engine   : Disabled    perpetual

```

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:

```

0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter : Enabled      33 days

```

Inactive Timebased Activation Key:

```

Oxyadayad3 Oxyadayad3 Oxyadayad3 Oxyadayad3 Oxyadayad3
Security Contexts : 2           7 days
AnyConnect Premium Peers : 100        7 days

```

```

Oxyadayad4 Oxyadayad4 Oxyadayad4 Oxyadayad4 Oxyadayad4
Total UC Proxy Sessions : 100        14 days

```

例 4 : show activation-key detail に対するフェールオーバー ペアのセカンダリ ユニット 出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスター」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリ ユニットの永続ライセンス。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number: P3000000011
Running Activation Key: Oxyadayad1 Oxyadayad1 Oxyadayad1 Oxyadayad1 Oxyadayad1

Licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                   : 150           perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts               : 2             perpetual
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers        : 2             perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 750           perpetual
Total VPN Peers                 : 750           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           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces      : Unlimited      perpetual
Maximum VLANs                   : 150           perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts               : 10            perpetual
GTP/GPRS                        : Enabled        perpetual
AnyConnect Premium Peers        : 4             perpetual
AnyConnect Essentials           : Disabled       perpetual
Other VPN Peers                 : 750           perpetual
Total VPN Peers                 : 750           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      : 4          perpetual
Total UC Proxy Sessions      : 4          perpetual
Botnet Traffic Filter         : Enabled    33 days
Intercompany Media Engine     : Disabled      perpetual

```

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: Oxyadayad1 Oxyadayad1 Oxyadayad1 Oxyadayad1 Oxyadayad1

Licensed features for this platform:

```

Maximum Physical Interfaces   : Unlimited    perpetual
Maximum VLANs                 : 150          perpetual
Inside Hosts                  : Unlimited    perpetual
Failover                       : Active/Active perpetual
VPN-DES                       : Enabled      perpetual
VPN-3DES-AES                   : Disabled     perpetual
Security Contexts             : 2            perpetual
GTP/GPRS                      : Disabled     perpetual
AnyConnect Premium Peers      : 2            perpetual
AnyConnect Essentials         : Disabled     perpetual
Other VPN Peers               : 750          perpetual
Total VPN Peers               : 750          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         : Disabled     perpetual
Intercompany Media Engine     : Disabled     perpetual

```

The flash permanent activation key is the SAME as the running permanent key.

例5：show activation-key に対する、フェールオーバー ペアでの ASA サービス モジュールのプライマリ ユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key
```

```
erial Number: SAL144705BF
```

```
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
```

```
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
```

```
Licensed features for this platform:
```

```
Maximum Interfaces      : 1024          perpetual
Inside Hosts           : Unlimited      perpetual
Failover               : Active/Active  perpetual
DES                    : Enabled        perpetual
3DES-AES               : Enabled        perpetual
Security Contexts      : 25            perpetual
GTP/GPRS               : Enabled        perpetual
Botnet Traffic Filter  : Enabled        330 days
```

```
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
```

```
Failover cluster licensed features for this platform:
```

```
Maximum Interfaces      : 1024          perpetual
Inside Hosts           : Unlimited      perpetual
Failover               : Active/Active  perpetual
DES                    : Enabled        perpetual
3DES-AES               : Enabled        perpetual
Security Contexts      : 50 perpetual
GTP/GPRS               : Enabled        perpetual
Botnet Traffic Filter  : Enabled        330 days
```

```
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
```

```
The flash permanent activation key is the SAME as the running permanent key.
```

```
Active Timebased Activation Key:
```

```
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter      : Enabled      330 days
```

例6：show activation-keyに対する、フェールオーバーペアでのASAサービスモジュールのセカンダリユニット出力

次に、セカンダリフェールオーバーユニットの **show activation-key** コマンドの出力例を示します。

- セカンダリユニットライセンス（永続ライセンスと時間ベースライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバークラスタ」ライセンス。これは、ASAで実際に実行されているライセンスです。プライマリおよびセカンダリライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリのインストール済みの時間ベースライセンス（アクティブおよび非アクティブ）。このユニットには時間ベースライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail
```

```
Serial Number: SAD143502E3
```

```
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683
```

```
Licensed features for this platform:
```

```
Maximum Interfaces      : 1024          perpetual
Inside Hosts           : Unlimited      perpetual
```

```

Failover                : Active/Active  perpetual
DES                    : Enabled        perpetual
3DES-AES               : Enabled        perpetual
Security Contexts     : 25          perpetual
GTP/GPRS               : Disabled      perpetual
Botnet Traffic Filter  : Disabled      perpetual

```

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

```

Failover cluster licensed features for this platform:
Maximum Interfaces     : 1024          perpetual
Inside Hosts          : Unlimited     perpetual
Failover              : Active/Active perpetual
DES                   : Enabled        perpetual
3DES-AES             : Enabled        perpetual
Security Contexts    : 50 perpetual
GTP/GPRS             : Enabled perpetual
Botnet Traffic Filter : Enabled 330 days

```

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

例 7：クラスタでの show activation-key の出力

```

ciscoasa# show activation-key
Serial Number: JMX1504L2TD
Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9

```

```

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 2 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 : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

```

This platform has an ASA 5585-X base license.

```

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual

```

```

Encryption-3DES-AES : Enabled perpetual
Security Contexts : 4 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 4 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 : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

```

This platform has an ASA 5585-X base license.

The flash permanent activation key is the SAME as the running permanent key.

共有ライセンスのモニタリング

共有ライセンスをモニタするには、次のいずれかのコマンドを入力します。

- **show shared license [detail | client [hostname] | backup]**

共有ライセンス統計情報を表示します。オプションキーワードはライセンスサーバだけに使用できます。**detail** キーワードを使用すると、参加システムごとの統計情報が表示されます。表示内容を1台の参加システムに限定するには、**client** キーワードを使用します。**backup** キーワードを使用すると、バックアップサーバに関する情報が表示されます。

共有ライセンスの統計情報をクリアするには、**clear shared license** コマンドを入力します。

次に、ライセンス参加ユニットでの **show shared license** コマンドの出力例を示します。

```

ciscoasa> show shared license
Primary License Server : 10.3.32.20
  Version                : 1
  Status                  : Inactive

Shared license utilization:
  SSLVPN:
    Total for network    :      5000
    Available             :      5000
    Utilized              :           0
  This device:
    Platform limit       :         250
    Current usage        :           0
    High usage           :           0
  Messages Tx/Rx/Error:
    Registration         : 0 / 0 / 0
    Get                   : 0 / 0 / 0
    Release               : 0 / 0 / 0
    Transfer              : 0 / 0 / 0

```

次に、ライセンスサーバ上での **show shared license detail** コマンドの出力例を示します。

```

ciscoasa> show shared license detail

```

```
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID         : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
SSLVPN:
  Total for network :      500
  Available         :      500
  Utilized          :         0
This device:
  Platform limit   :      250
  Current usage    :         0
  High usage       :         0
  Messages Tx/Rx/Error:
    Registration   : 0 / 0 / 0
    Get            : 0 / 0 / 0
    Release        : 0 / 0 / 0
    Transfer       : 0 / 0 / 0

Client Info:

Hostname           : 5540-A
Device ID          : XXXXXXXXXXXX
SSLVPN:
  Current usage    : 0
  High             : 0
  Messages Tx/Rx/Error:
    Registration   : 1 / 1 / 0
    Get            : 0 / 0 / 0
    Release        : 0 / 0 / 0
    Transfer       : 0 / 0 / 0
...

```

- **show activation-key**

ASA にインストールされているライセンスを表示します。 **show version** コマンドでもライセンス情報が表示されます。

- **show vpn-sessiondb**

VPN セッションのライセンス情報を表示します。

PAK 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
接続数と VLAN 数の増加	7.0(5)	次の制限値が増加されました。 <ul style="list-style-type: none"> • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
SSL VPN ライセンス	7.1(1)	SSL VPN ライセンスが導入されました。
SSL VPN ライセンスの追加	7.2(1)	5000 ユーザの SSL VPN ライセンスが ASA 5550 以降に対して導入されました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。

機能名	プラットフォーム リリース	説明
VLAN 数の増加	7.2(2)	<p>ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5 (3つのフル機能インターフェイス、1つのフェールオーバーインターフェイス、1つのバックアップインターフェイスに制限されるインターフェイス) から20のフル機能インターフェイスに増加されました。また、トランクポート数も1から8に増加されました。フル機能のインターフェイスの数が20になり、バックアップ ISP インターフェイスを停止するために <code>backup interface</code> コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。<code>backup interface</code> コマンドは、これまでどおり Easy VPN 設定用に使用できます。</p> <p>VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは10から50に、Security Plus ライセンスでは25から100に、ASA 5520 では100から150に、ASA 5550 では200から250に増えています。</p>

機能名	プラットフォーム リリース	説明
ASA 5510 Security Plus ライセンスに対するギガビットイーサネットサポート	7.2(3)	<p>ASA 5510 は、Security Plus ライセンスを使用する Ethernet 0/0 および 0/1 ポート用にギガビットイーサネット（1000 Mbps）をサポートしています。基本ライセンスでは、これらのポートは引き続きファストイーサネット（100 Mbps）ポートとして使用されます。いずれのライセンスに対しても、Ethernet 0/2、0/3、および 0/4 はファストイーサネットポートのままです。</p> <p>（注） インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。</p> <p>speed コマンドを使用してインターフェイスの速度を変更します。また、show interface コマンドを使用して各インターフェイスの現在の設定速度を確認します。</p>

機能名	プラットフォーム リリース	説明
Advanced Endpoint Assessment ライセンス	8.0(2)	<p>Advanced Endpoint Assessment ライセンスが導入されました。Cisco AnyConnect またはクライアントレス SSL VPN 接続の条件としてリモートコンピュータでスキャン対象となる、アンチウイルス アプリケーションやアンチスパイウェア アプリケーション、ファイアウォール、オペレーティング システム、および関連アップデートの種類が、大幅に拡張されました。また、任意のレジストリ エントリ、ファイル名、およびプロセス名を指定してスキャン対象にすることもできます。スキャン結果を ASA に送信します。ASA は、ユーザ ログイン クレデンシャルとコンピュータ スキャン結果の両方を使用して、ダイナミック アクセス ポリシー (DAP) を割り当てます。</p> <p>Advanced Endpoint Assessment ライセンスを使用すると、バージョン要件を満たすように非標準コンピュータのアップデートを試行する機能を設定して、Host Scan を拡張できます。</p> <p>シスコは、Host Scan でサポートされるアプリケーションとバージョンの一覧に、Cisco Secure Desktop とは異なるパッケージで、タイムリーなアップデートを提供できます。</p>
ASA 5510 の VPN ロード バランシング	8.0(2)	VPN ロード バランシングが ASA 5510 Security Plus ライセンスでサポートされるようになりました。
AnyConnect for Mobile ライセンス	8.0(3)	AnyConnect for Mobile ライセンスが導入されました。これにより、Windows モバイル デバイスは AnyConnect クライアントを使用して、ASA に接続できます。
時間ベース ライセンス	8.0(4)/8.1(2)	時間ベース ライセンスがサポートされるようになりました。

機能名	プラットフォーム リリース	説明
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。
Unified Communications Proxy セッション ライセンス	8.0(4)	<p>UC Proxy セッション ライセンスが導入されました。電話プロキシ、Presence Federation Proxy、および Encrypted Voice Inspection アプリケーションでは、それらの接続に TLS プロキシセッションが使用されます。各 TLS プロキシセッションは、UC ライセンスの制限に対してカウントされます。これらのアプリケーションは、すべて UC Proxy として包括的にライセンスされるので、混在させたり、組み合わせたりできます。</p> <p>この機能は、バージョン 8.1 では使用できません。</p>
ボットネット トラフィック フィルタ ライセンス	8.2(1)	ボットネット トラフィック フィルタ ライセンスが導入されました。ボットネット トラフィック フィルタでは、既知の不正なドメインや IP アドレスに対する接続を追跡して、マルウェア ネットワーク アクティビティから保護します。

機能名	プラットフォーム リリース	説明
AnyConnect Essentials ライセンス	8.2(1)	<p>AnyConnect Essentials ライセンスが導入されました。このライセンスにより、AnyConnect VPN クライアントは ASA にアクセスできるようになります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。</p> <p>(注) AnyConnect Essentials ライセンスを所有する VPN ユーザは、Web ブラウザを使用してログインし、AnyConnect クライアントをダウンロードおよび起動 (WebLaunch) することができます。</p> <p>このライセンスと AnyConnect Premium ライセンスのいずれでイネーブル化されたかには関係なく、AnyConnect クライアントソフトウェアには同じクライアント機能のセットが装備されています。</p> <p>特定の ASA では、AnyConnect Premium ライセンス (全タイプ) または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。</p> <p>デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、webvpn を使用し、次に no anyconnect-essentials コマンドを使用すると、AnyConnect Essentials ライセンスを無効にして他のライセンスを使用できます。</p>

機能名	プラットフォーム リリース	説明
SSL VPN ライセンスの AnyConnect Premium SSL VPN Edition ライセンスへの変更	8.2(1)	SSL VPN ライセンスの名前が AnyConnect Premium SSL VPN Edition ライセンスに変更されました。
SSL VPN の共有ライセンス	8.2(1)	SSL VPN の共有ライセンスが導入されました。複数の ASA で、SSL VPN セッションのプールを必要に応じて共有できます。
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。
ASA 5585-X (SSP-20) 用 10 GE I/O ライセンス	8.2(3)	ASA 5585-X (SSP-20) の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビットイーサネットの速度をイネーブルにしました。SSP-60 は、デフォルトで 10 ギガビットイーサネットの速度をサポートします。 (注) ASA 5585-X は 8.3(x) ではサポートされていません。
ASA 5585-X (SSP-10) 用 10 GE I/O ライセンス	8.2(4)	ASA 5585-X (SSP-10) の 10 GE I/O ライセンスを導入し、ファイバポートでの 10 ギガビットイーサネットの速度をイネーブルにしました。SSP-40 は、デフォルトで 10 ギガビットイーサネットの速度をサポートします。 (注) ASA 5585-X は 8.3(x) ではサポートされていません。
同一でないフェールオーバーライセンス	8.3(1)	フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリユニットおよびセカンダリユニットからの結合されたライセンスです。 show activation-key および show version の各コマンドが変更されました。

機能名	プラットフォーム リリース	説明
スタック可能な時間ベースライセンス	8.3(1)	時間ベースライセンスがスタック可能になりました。多くの場合、時間ベースライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベースライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベースライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。
Intercompany Media Engine ライセンス	8.3(1)	IME ライセンスが導入されました。
複数の時間ベースライセンスの同時アクティブ化	8.3(1)	時間ベースライセンスを複数インストールできるようになり、同時に機能ごとに1つのアクティブなライセンスを保持できるようになりました。 show activation-key および show version の各コマンドが変更されました。
時間ベースライセンスのアクティブ化と非アクティブ化の個別化	8.3(1)	コマンドを使用して、時間ベースライセンスをアクティブ化または非アクティブ化できるようになりました。 activation-key [activate deactivate] コマンドが変更されました。
AnyConnect Premium SSL VPN Edition ライセンスの AnyConnect Premium SSL VPN ライセンスへの変更	8.3(1)	AnyConnect Premium SSL VPN Edition ライセンスの名前が AnyConnect Premium SSL VPN ライセンスに変更されました。

機能名	プラットフォーム リリース	説明
輸出用のペイロード暗号化なしイメージ	8.3(2)	<p>ASA 5505 ～ 5550 にペイロード暗号化機能のないソフトウェアをインストールした場合、Unified Communications、強力な暗号化VPN、強力な暗号化管理プロトコルをディセーブルにします。</p> <p>(注) この特殊なイメージは 8.3(x) でのみサポートされます。 8.4(1) 以降で暗号化機能のないソフトウェアをサポートするには、ASA の特別なハードウェア バージョンを購入する必要があります。</p>
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	<p>ASA 5550 および ASA 5585-X (SSP-10) では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X (SSP-20) 以降では、コンテキストの最大数が 50 から 250 に引き上げられました。</p>
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	<p>ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。</p>
ASA 5580 および 5585-X での接続数の増加	8.4(1)	<p>ファイアウォール接続の最大数が次のように引き上げられました。</p> <ul style="list-style-type: none"> • ASA 5580-20 : 1,000,000 から 2,000,000 へ。 • ASA 5580-40 : 2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10 : 750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20 : 1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40 : 2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60 : 2,000,000 から 10,000,000 へ。

機能名	プラットフォーム リリース	説明
AnyConnect Premium SSL VPN ライセンスの AnyConnect Premium ライセンスへの変更	8.4(1)	AnyConnect Premium SSL VPN ライセンスの名前が AnyConnect Premium ライセンスに変更されました。ライセンス情報の表示が「SSL VPN ピア」から「AnyConnect Premium ピア」に変更されました。
ASA 5580 での AnyConnect VPN セッション数の増加	8.4(1)	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	8.4(1)	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
IKEv2 を使用した IPsec リモートアクセス	8.4(1)	<p>AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモートアクセス VPN が追加されました。</p> <p>(注) ASA での IKEv2 のサポートに関して、重複するセキュリティアソシエーションがサポートされていないという制約が現在あります。</p> <p>Other VPN ライセンス（以前の IPsec VPN）には IKEv2 サイトツーサイトセッションが追加されました。Other VPN ライセンスは基本ライセンスに含まれています。</p>
輸出用のペイロード暗号化なしハードウェア	8.4(1)	ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、特定の国に ASA を輸出できるよう、ASA ソフトウェアのユニファイドコミュニケーションと VPN 機能を無効にしています。

機能名	プラットフォーム リリース	説明
デュアル SSP (SSP-20 および SSP-40)	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません (たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません)。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバーペアとして使用できます。2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。
ASA 5512-X ~ ASA 5555-X での IPS モジュール ライセンス	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X での IPS SSP ソフトウェア モジュールには IPS モジュールライセンスが必要です。
ASA 5580 および ASA 5585-X のクラスタリング ライセンス。	9.0(1)	クラスタリングライセンスが ASA 5580 および ASA 5585-X に対して追加されました。
ASASM での VPN のサポート	9.0(1)	ASASM は、すべての VPN 機能をサポートするようになりました。
ASASM でのユニファイド コミュニケーションのサポート	9.0(1)	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート (SSP-40 および SSP-60 に加えて)、デュアル SSP に対する VPN サポート	9.0(1)	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました (同一シャーシ内で同じレベルの SSP を 2 つ使用できます)。デュアル SSP を使用するとき VPN がサポートされるようになりました。

機能名	プラットフォーム リリース	説明
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタ をサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになりません。ASA 5512-X では Security Plus ライセンスが必要です。
ASA 5585-X の 16 の クラスタ メンバ の サポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタ をサポートするようになりました。
ASAv4 および ASAv30 の 標準 および プレミアム モデル ライセンス の 導入	9.2(1)	シンプルなライセンス方式で ASAv が導入されました（標準またはプレミアムレベルの ASAv4 および ASAv30 永続ライセンス）。アドオンライセンスは使用できません。

