Cisco ASA 5500 バージョン 8.2 の機能ライセンスの管理

Managing Feature Licenses for Cisco ASA 5500 Version 8.2

OL-18431-02-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルでは、アクティベーション キーを取得してアクティブにする方法を説明します。また、各モデルで使用できるライセンスについても説明します。

このマニュアルは、次の内容で構成されています。

各モデルでサポートされる機能ライセンス

ここでは、各モデルで使用できるライセンスと、ライセンスに関する重要事項について説明します。この項は、次の内容で構成されています。

各モデルでのライセンス

ここでは、各モデルで使用できる機能ライセンスを示します。

イタリック体で示される項目は、基本ライセンスまたは Security Plus ライセンスの代わりに使用できるオプションのライセンスです。ライセンスは混在および一致させることができます。たとえば、10 セキュリティ コンテキスト ライセンスと Strong Encryption を組み合せたり、500 SSL VPN ライセンスと GTP/GPRS ライセンスを組み合せたり、あるいは 4 つのライセンスをすべて組み合せることができます。

表 1　ASA 5505 適応型セキュリティ アプライアンス ライセンス機能

ASA 5505	基本ライセンス		Security Plus	
ファイアウォール ライセンス				
Botnet Traffic Filter	無効	*オプションの一時ライセンス：使用可能*	無効	*オプションの一時ライセンス：使用可能*
同時ファイアウォール接続	10 K		25 K	
GTP/GPRS	サポートなし		サポートなし	
ユニファイド コミュニケーションの セッション数[1]	2	*オプションのライセンス：24*	2	*オプションのライセンス：24*
VPN ライセンス				
Adv. Endpoint Assessment	無効	*オプションのライセンス：使用可能*	無効	*オプションのライセンス：使用可能*
AnyConnect Essentials[1]	無効	*オプションのライセンス：使用可能*	無効	*オプションのライセンス：使用可能*
AnyConnect Mobile[1]	無効	*オプションのライセンス：使用可能*	無効	*オプションのライセンス：使用可能*
AnyConnect Premium SSL VPN（セッション数）[1]	2	*オプションの永続ライセンス：*	2	*オプションの永続ライセンス：*
		10 / *25*		*10* / *25*
IPSec VPN（セッション数）[1]	10（最大 25 の結合された IPSec と SSL VPN）		25（最大 25 の結合された IPSec と SSL VPN）	
VPN ロード バランシング	サポートなし		サポートなし	

表 1　　ASA 5505 適応型セキュリティ アプライアンス ライセンス機能 （続き）

ASA 5505	基本ライセンス		Security Plus	
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（ステートフル フェールオーバーなし）	
セキュリティ コンテキスト	サポートなし		サポートなし	
同時接続ユーザ数[2]	10[3]	*オプションのライセンス：*	10[3]	*オプションのライセンス：*
		50 *無制限*		*50* *無制限*
最大 VLAN/ ゾーン	3（2 つの標準ゾーンと 1 つの制限付きゾーン）		20	
最大 VLAN トランク	サポートなし		8 つのトランク	

1. 「ライセンスに関する注意事項」を参照してください。
2. ルーテッド モードでは、内側（ビジネス VLAN とホーム VLAN）のホストは、外側（インターネット VLAN）と通信するときに限り制限のカウントに算入されます。インターネット ホストは、制限のカウントに算入されません。ビジネスとホーム間のトラフィックを開始したホストも、制限のカウントに算入されません。デフォルト ルートに関連付けられたインターフェイスは、インターネット インターフェイスと見なされます。デフォルト ルートがない場合は、すべてのインターフェイスのホストが制限のカウントに算入されます。トランスペアレント モードでは、ホストの数が最も少ないインターフェイスが制限のカウントに算入されます。ホストの制限を表示する方法については、**show local-host** コマンドを参照してください。
3. 10 ユーザ ライセンスの場合、最大 DHCP クライアント数は 32 です。50 ユーザの場合、最大数は 128 です。無制限ユーザの場合、最大数は 250 です。これはその他のモデルの 最大数です。

表 2　ASA 5510 適応型セキュリティ アプライアンス ライセンス機能

ASA 5510	基本ライセンス					Security Plus				
ファイアウォール ライセンス										
Botnet Traffic Filter	無効	*オプションの一時ライセンス：使用可能*				無効	*オプションの一時ライセンス：使用可能*			
同時ファイアウォール接続	50 K					130 K				
GTP/GPRS	サポートなし					サポートなし				
ユニファイド コミュニケーションの セッション数[1]	2	*オプションのライセンス：*				2	*オプションのライセンス：*			
		24	*50*	*100*			*24*	*50*	*100*	
VPN ライセンス										
Adv. Endpoint Assessment	無効	*オプションのライセンス：使用可能*				無効	*オプションのライセンス：使用可能*			
AnyConnect Essentials[1]	無効	*オプションのライセンス：使用可能*				無効	*オプションのライセンス：使用可能*			
AnyConnect Mobile[1]	無効	*オプションのライセンス：使用可能*				無効	*オプションのライセンス：使用可能*			
AnyConnect Premium SSL VPN（セッション数）[1]	2	*オプションの永続ライセンス：*					2	*オプションの永続ライセンス：*				
		10	*25*	*50*	*100*	*250*		*10*	*25*	*50*	*100*	*250*
	オプションの共有ライセンス：参加ユニットまたはサーバ。サーバの場合、これらのライセンスを使用できます。[1]						*オプションの共有ライセンス：参加ユニットまたはサーバ。サーバの場合、これらのライセンスを使用できます。[1]*					
	500 ～ 50,000（500 単位）		*50,000 ～ 545,000（1000 単位）*				*500 ～ 50,000（500 単位）*		*50,000 ～ 545,000（1000 単位）*			
	オプションの FLEX ライセンス：250						*オプションの FLEX ライセンス：250*					
IPSec VPN（セッション数）[1]	250（最大 250 の結合された IPSec と SSL VPN）						250（最大 250 の結合された IPSec と SSL VPN）					
VPN ロード バランシング	サポートなし						サポートあり					
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/スタンバイまたはアクティブ/アクティブ[1]					
セキュリティ コンテキスト	サポートなし						2	*オプションのライセンス：*				
								5				
最大 VLAN	50						100					

1. 「ライセンスに関する注意事項」を参照してください。

表 3　ASA 5520 適応型セキュリティ アプライアンス ライセンス機能

ASA 5520	基本ライセンス						
ファイアウォール ライセンス							
Botnet Traffic Filter	無効	*オプションの一時ライセンス：使用可能*					
同時ファイアウォール接続	280 K						
GTP/GPRS	無効	*オプションのライセンス：使用可能*					
ユニファイド コミュニケーション プロキシのセッション数[1]	2	*オプションのライセンス：*					
		24	*50*	*100*	*250*	*500*	*750*	*1000*
VPN ライセンス							
Adv. Endpoint Assessment	無効	*オプションのライセンス：使用可能*					
AnyConnect Essentials[1]	無効	*オプションのライセンス：使用可能*					
AnyConnect Mobile[1]	無効	*オプションのライセンス：使用可能*					
AnyConnect Premium SSL VPN（セッション数）[1]	2	*オプションの永続ライセンス：*					
		10	*25*	*50*	*100*	*250*	*500*	*750*
	オプションの共有ライセンス：参加ユニットまたはサーバ。サーバの場合、これらのライセンスを使用できます。[1]						
	500 ～ 50,000（500 単位）					*50,000 ～ 545,000（1000 単位）*	
	オプションの FLEX ライセンス：						
	250	*750*					
IPSec VPN（セッション数）[1]	750（最大 750 の結合された IPSec と SSL VPN）						
VPN ロード バランシング	サポートあり						
一般ライセンス							
暗号化	基本（DES）	*オプションのライセンス：強化（3DES/AES）*					
フェールオーバー	アクティブ / スタンバイまたはアクティブ / アクティブ[1]						
セキュリティ コンテキスト	2	*オプションのライセンス：*					
		5	*10*	*20*			
最大 VLAN	150						

1. 「ライセンスに関する注意事項」を参照してください。

表 4　ASA 5540 適応型セキュリティ アプライアンス ライセンス機能

ASA 5540	基本ライセンス								
ファイアウォール ライセンス									
Botnet Traffic Filter	無効	*オプションの一時ライセンス：使用可能*							
同時ファイアウォール接続	400 K								
GTP/GPRS	無効	*オプションのライセンス：使用可能*							
ユニファイド コミュニケーション プロキシのセッション数[1]	2	*オプションのライセンス：*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN ライセンス									
Adv. Endpoint Assessment	無効	*オプションのライセンス：使用可能*							
AnyConnect Essentials[1]	無効	*オプションのライセンス：使用可能*							
AnyConnect Mobile[1]	無効	*オプションのライセンス：使用可能*							
AnyConnect Premium SSL VPN（セッション数）[1]	2	*オプションの永続ライセンス：*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
	オプションの共有ライセンス：参加ユニットまたはサーバ。サーバの場合、これらのライセンスを使用できます。[1]								
	500 ～ 50,000（500 単位）						*50,000 ～ 545,000（1000 単位）*		
	オプションの FLEX ライセンス：								
	250	*750*	*1000*	*2500*					
IPSec VPN（セッション数）[1]	5000（最大 5000 の結合された IPSec と SSL VPN）								
VPN ロード バランシング	サポートあり								
一般ライセンス									
暗号化	基本（DES）	*オプションのライセンス：強化（3DES/AES）*							
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ[1]								
セキュリティ コンテキスト	2	*オプションのライセンス：*							
		5	*10*	*20*	*50*				
最大 VLAN	200								

1. 「ライセンスに関する注意事項」を参照してください。

表 5　ASA 5550 適応型セキュリティ アプライアンス ライセンス機能

ASA 5550	基本ライセンス									
ファイアウォール ライセンス										
Botnet Traffic Filter	無効	*オプションの一時ライセンス：使用可能*								
同時ファイアウォール接続	650 K									
GTP/GPRS	無効	*オプションのライセンス：使用可能*								
ユニファイド コミュニケーション プロキシのセッション数[1]	2	*オプションのライセンス：*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN ライセンス										
Adv. Endpoint Assessment	無効	*オプションのライセンス：使用可能*								
AnyConnect Essentials[1]	無効	*オプションのライセンス：使用可能*								
AnyConnect Mobile[1]	無効	*オプションのライセンス：使用可能*								
AnyConnect Premium SSL VPN（セッション数）[1]	2	*オプションの永続ライセンス：*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
	オプションの共有ライセンス：参加ユニットまたはサーバ。サーバの場合、これらのライセンスを使用できます。[1]									
	500 ～ 50,000（500 単位）						*50,000 ～ 545,000（1000 単位）*			
	オプションの FLEX ライセンス：									
	250	*750*	*1000*	*2500*	*5000*					
IPSec VPN（セッション数）[1]	5000（最大 5000 の結合された IPSec と SSL VPN）									
VPN ロード バランシング	サポートあり									
一般ライセンス										
暗号化	基本（DES）	*オプションのライセンス：強化（3DES/AES）*								
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ[1]									
セキュリティ コンテキスト	2	*オプションのライセンス：*								
		5	*10*	*20*	*50*					
最大 VLAN	250									

1. 「ライセンスに関する注意事項」を参照してください。

表 6　ASA 5580 適応型セキュリティ アプライアンス ライセンス機能

ASA 5580	基本ライセンス										
ファイアウォール ライセンス											
Botnet Traffic Filter	無効	*オプションの一時ライセンス：使用可能*									
同時ファイアウォール接続	650 K										
GTP/GPRS	無効	*オプションのライセンス：使用可能*									
ユニファイド コミュニケーション プロキシのセッション数[1]	2	*オプションのライセンス：*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10000*[2]
VPN ライセンス											
Adv. Endpoint Assessment	無効	*オプションのライセンス：使用可能*									
AnyConnect Essentials[1]	無効	*オプションのライセンス：使用可能*									
AnyConnect Mobile[1]	無効	*オプションのライセンス：使用可能*									
AnyConnect Premium SSL VPN（セッション数）[1]	2	*オプションの永続ライセンス：*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
	オプションの共有ライセンス：参加ユニットまたはサーバ。サーバの場合、これらのライセンスを使用できます。[1]										
	500 ～ 50,000（500 単位）						*50,000 ～ 545,000（1000 単位）*				
	オプションの FLEX ライセンス：										
	250	*750*	*1000*	*2500*	*5000*						
IPSec VPN（セッション数）[1]	5000（最大 5000 の結合された IPSec と SSL VPN）										
VPN ロード バランシング	サポートあり										
一般ライセンス											
暗号化	基本（DES）	*オプションのライセンス：強化（3DES/AES）*									
フェールオーバー	アクティブ/スタンバイまたはアクティブ/アクティブ[1]										
セキュリティ コンテキスト	2	*オプションのライセンス：*									
		5	*10*	*20*	*50*						
最大 VLAN	250										

1. 「ライセンスに関する注意事項」を参照してください。
2. 10,000 セッション ライセンスでは、結合された合計セッション数を 10,000 にすることができますが、電話プロキシ セッションの最大数は 5000 です。

ライセンスに関する注意事項

表 7 に 「各モデルでのライセンス」（P.2）の各表の脚注を示します。

表 7　　ライセンスに関する注意事項

ライセンス	注意事項
アクティブ/アクティブ フェールオーバー	アクティブ/アクティブ フェールオーバーと VPN は併用できません。VPN を使用する場合は、アクティブ/スタンバイ フェールオーバーを使用してください。
AnyConnect Essentials	このライセンスでは、適応型セキュリティ アプライアンスに AnyConnect VPN クライアントからアクセスできます。このライセンスは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop の展開をサポートしません。これらの機能を使用するには、AnyConnect Essentials ライセンスではなく、AnyConnect Premium SSL VPN ライセンスを有効にしてください。 **（注）** AnyConnect Essentials ライセンスを使用すると、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）できます。 AnyConnect クライアント ソフトウェアは、このライセンスで有効になっているか AnyConnect Premium SSL VPN ライセンスで有効になっているかに関係なく、同じクライアント機能セットを提供します。 AnyConnect Essentials ライセンスは、特定の適用型セキュリティ アプライアンスで AnyConnect Premium SSL VPN ライセンス（すべてのタイプ）または Advanced Endpoint Assessment ライセンスと同時にアクティブにできません。ただし、同じネットワーク内にある別の適応型セキュリティ アプライアンスで AnyConnect Essentials ライセンスと AnyConnect Premium SSL VPN ライセンスの両方を実行できます。 デフォルトでは、セキュリティ アプライアンスは AnyConnect Essentials ライセンスを使用しますが、このライセンスを無効にし、**no anyconnect-essentials** コマンドを使用して他のライセンスを使用できます。
AnyConnect Mobile	このライセンスでは、Windows Mobile 5.0、6.0、および 6.1 が実行されているタッチスクリーン モバイル デバイスの AnyConnect クライアントにアクセスできます。AnyConnect 2.3 以降のバージョンへのモバイル アクセスをサポートする場合は、このライセンスを使用することを推奨します。このライセンスを使用するには、AnyConnect Essentials または AnyConnect Premium SSL VPN のいずれかのライセンスをアクティブにして、許可される SSL VPN セッションの合計数を指定する必要があります。
AnyConnect Premium SSL VPN 共有	共有ライセンスでは、セキュリティ アプライアンスは複数のクライアント セキュリティ アプライアンスの共有ライセンス サーバとして機能します。共有ライセンス プールは大容量ですが、各セキュリティ アプライアンスで使用されるセッションの最大数は、永続ライセンスにリストされている最大数を超えることはできません。

表 7　ライセンスに関する注意事項 （続き）

ライセンス	注意事項
結合された IPSec および SSL VPN セッション	• IPSec および SSL VPN セッションの最大数が VPN セッションの最大数を超える値になっても、結合されたセッション数は、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は、セキュリティ アプライアンスをオーバーロードして、ネットワークのサイズを適切なサイズに設定できます。 • クライアントレス SSL VPN セッションを開始した後に、ポータルから AnyConnect クライアント セッションを開始すると、1 つのセッションが合計に使用されます。ただし、最初に AnyConnect クライアントをスタンドアロンのクライアントなどから開始し、クライアントレス SSL VPN ポータルにログインすると、2 つのセッションが使用されます。
ユニファイド コミュニケーション プロキシのセッション数	電話プロキシ、モビリティ プロキシ、プレゼンス フェデレーション プロキシ、および TLS プロキシはすべて UC プロキシ とともにライセンスを受け、混在および一致させることができます。たとえば、プライマリおよびバックアップ Cisco Unified Communications Manager を使用する電話機を設定すると、2 つの TLS/SRTP 接続が確立されるので、2 つの UC プロキシ セッションが使用されます。

機能ライセンスに関する情報

ライセンスは、特定のセキュリティ アプライアンスで有効にするオプションを指定します。これは、160 ビット（5 つの 32 ビットの語または 20 バイト）値で表されます。この値はシリアル番号（11 文字のストリング）と有効な機能を符号化します。

この項は、次の内容で構成されています。

事前インストール済みライセンス

デフォルトでは、セキュリティ アプライアンスにすでにインストールされたライセンスが付属しています。このライセンスは、ユーザが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である場合と、すでにすべてのライセンスがインストールされている場合があります。インストールしたライセンスを確認する方法については、「現在のライセンスの表示」（P.19）を参照してください。

一時ライセンス、VPN Flex ライセンス、および評価ライセンス

永続ライセンスに加えて、一時ライセンスの購入、または有効期限の付いた評価ライセンスを受け取ることができます。たとえば、VPN Flex ライセンスを購入して、同時接続 SSL VPN ユーザの数の短期間の急増に対処したり、1 年間有効の Botnet Traffic Filter 一時ライセンスを注文したりできます。

この項は、次の内容で構成されています。

一時ライセンスのタイマーの機能

- 一時ライセンスのタイマーは、一時ライセンスをセキュリティ アプライアンスでアクティブにしたときにカウント ダウンが開始されます。
- 永続ライセンスまたは別の一時ライセンスをアクティブにした場合など、一時ライセンスがタイムアウトする前にその使用を停止すると、タイマーは停止します。タイマーは、一時ライセンスを再アクティブ化した場合に限りもう一度開始されます。
- 一時ライセンスがアクティブなときに、セキュリティ アプライアンスをシャットダウンすると、タイマーはカウント ダウンし続けます。期間の延長に備えてセキュリティ アプライアンスをシャットダウン状態にしておく場合は、永続ライセンスをアクティブにしてからシャットダウンして、一時ライセンスを保持する必要があります。
- 一時ライセンスの期限が切れた場合、セキュリティ アプライアンスを次にリロードすると、永続ライセンスが使用されます。ライセンスの期限が切れた後すぐにリロードを実行する必要はありません。

（注） 一時ライセンスをインストールした後にシステム クロックを変更しないことを推奨します。クロックを今よりも後の日付に設定してからリロードすると、セキュリティ アプライアンスは元のインストール時に対してシステム クロックをチェックし、実際に使用されているよりも多くの時間が経過したものと見なします。クロックを元に戻し、実際の実行時間が元のインストール時からシステム クロックまでの時間を超えると、リロード後すぐにライセンスの期限が切れます。

複数のライセンスの連携

- 一時ライセンスをアクティブにすると、永続ライセンスと一時ライセンスの両方の機能が結合されて実行ライセンスを構成します。セキュリティ アプライアンスは、各機能の各ライセンスにおける最も高い値を使用し、一時アクティベーション キーを入力するときに解決済みのライセンス間の競合を表示します。まれに一時ライセンスが永続ライセンスよりも下位の機能を使用している場合があります。この場合、永続ライセンスの値が使用されます。
- 永続ライセンスをアクティブにすると、現在実行されている永続ライセンスと一時ライセンスが上書きされて、実行ライセンスになります。

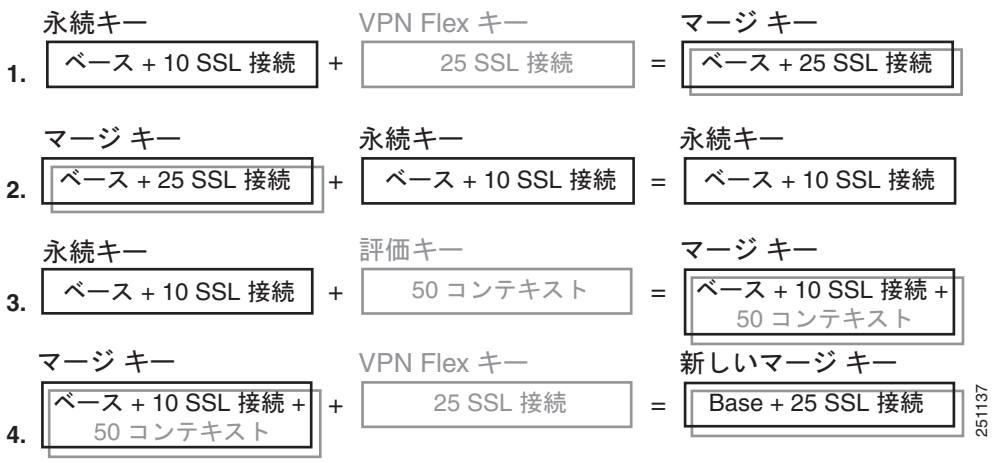
（注） 新しい永続ライセンスをインストールし、それが一時ライセンスからのダウングレードである場合は、セキュリティ アプライアンスをリロードして一時ライセンスを無効にし、永続ライセンスを復元する必要があります。リロードするまで一時ライセンスはカウント ダウンを続けます。

*すでにインストールされている*永続ライセンスを再アクティブ化する場合は、セキュリティ アプライアンスをリロードする必要はありません。一時ライセンスはカウントダウンを続行せず、トラフィックは切断されません。

- 後から永続ライセンスをアクティブ化する場合に一時ライセンスの機能を再有効化するには、単純に一時アクティベーション キーを再入力します。ライセンスをアップグレードする場合、リロードの必要はありません。
- 別の一時ライセンスに切り替えるには、新しいアクティベーション キーを入力します。新しいライセンスは古い一時ライセンスの代わりに使用され、永続ライセンスと組み合わされて新しい実行ライセンスを作成します。セキュリティ アプライアンスには複数の一時ライセンスをインストールできますが、一度にアクティブにできるのは 1 つのライセンスだけです。

永続アクティベーション キーと VPN Flex アクティベーション キーおよびそれらの連携については次の図を参照してください。

図 1　永続アクティベーション キーと VPN Flex アクティベーション キー



1. 前述の図の例 1 では、25 の SSL セッションを使用する一時キーを適用します。VPN Flex 値は 10 セッションの永続キー値を超えているため、結果の実行キーは、25 セッションの VPN Flex 値を使用する結合キーになります。
2. 前述の例 2 では、例 1 の結合キーが永続キーに置き換えられます。VPN Flex ライセンスは無効になります。実行キーはデフォルトで 10 セッションの永続キー値に設定されます。
3. 前述の例 3 では、50 のコンテキストを含む評価ライセンスが永続キーに適用されているため、結果の実行キーは、永続キーと 50 コンテキスト ライセンスのすべての機能を含む結合キーになります。
4. 前述の例 4 では、例 3 の結合キーに VPN Flex キーが適用されています。セキュリティ アプライアンスでは一度に 1 つの一時キーだけが使用できるため、VPN Flex キーで評価キーが置き換えられます。最終的な結果は、例 1 の結合キーと同じになります。

フェールオーバー ライセンスと一時ライセンス

フェールオーバーを使用する場合は、同一のライセンスが必要になります。フェールオーバー目的では、一時ライセンスと永続ライセンスは同一に見えるため、永続ライセンスを 1 つのユニットで使用し、一時ライセンスを他のユニットで使用できます。この機能は緊急の状況で役に立ちます。たとえば、ユニットのいずれかで障害が発生したときに追加のユニットがある場合は、他のユニットを修理している間に追加のユニットを設置できます。通常 SSL VPN で追加のユニットを使用しない場合は、他のユニットの修理中に VPN Flex ライセンスを使用することを推奨します。

一時ライセンスはフェールオーバー ユニットでアクティブになっている限り、カウント ダウンを続行するため、永続フェールオーバーのインストールで一時ライセンスを使用することは推奨されません。一時ライセンスの期限が切れると、フェールオーバーは機能しなくなります。

共有ライセンス

共有ライセンスを使用すると、多数の SSL VPN セッションを購入し、必要に応じて、セキュリティ アプライアンスのグループでセッションを共有できます。これを行うには、セキュリティ アプライアンスの 1 つを共有ライセンス サーバとして設定し、残りを共有ライセンス参加ユニットとして設定します。ここでは、共有ライセンスの動作について説明します。次のトピックについて取り上げます。

共有ライセンス サーバと参加ユニットに関する情報

次の手順で、共有ライセンスの動作について説明します。

1. 共有ライセンス サーバとなるセキュリティ アプライアンスを決定し、そのデバイス シリアル番号を使用して共有ライセンス サーバ ライセンスを購入します。
2. 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ユニットとなるセキュリティ アプライアンスを決定し、各デバイスのシリアル番号を使用して各デバイスの共有ライセンス参加ユニットのライセンスを取得します。
3. （オプション）2 つ目のセキュリティ アプライアンスを共有ライセンス バックアップ サーバとして指定します。指定できるのは 1 つのバックアップ サーバだけです。

（注） 共有ライセンス バックアップ サーバには参加ユニット ライセンスだけが必要です。

4. 共有ライセンス サーバに共有秘密を設定します。共有秘密を持つすべての参加ユニットが共有ライセンスを使用できます。
5. セキュリティ アプライアンスを参加ユニットとして設定する場合は、ローカル ライセンスおよびモデル情報など、そのセキュリティ アプライアンス自身の情報を送信して、共有ライセンス サーバに登録します。

（注） 参加ユニットは、IP ネットワークを介してサーバと通信できるようにする必要があります。参加ユニットは同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加ユニットがサーバをポーリングする頻度に関する情報で応答します。
7. 参加ユニットは、ローカル ライセンスのセッションを使い切ると、共有ライセンス サーバに追加のセッション（50 セッション単位）を求める要求を送信します。
8. 共有ライセンス サーバは共有ライセンスで応答します。参加ユニットによって使用され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ることはできません。

（注） 共有ライセンス サーバは共有ライセンス プールにも参加できます。参加するためには、参加ユニット ライセンスとサーバ ライセンスは必要ありません。

   a. 共有ライセンス プールに参加ユニット用のセッションが十分に残っていない場合、サーバはできる限り多くの使用可能セッションで応答します。
   b. 参加ユニットは、サーバが要求を適切に満たすまで追加のセッションを要求する更新メッセージを送信し続けます。
9. 参加ユニットに対する負荷が減ると、その参加ユニットは共有セッションを開放するようにサーバにメッセージを送信します。

（注） セキュリティ アプライアンスは、サーバと参加ユニット間で SSL を使用してすべての通信を暗号化します。

参加ユニットとサーバ間の通信の問題

参加ユニットとサーバ間の通信の問題については次のガイドラインを参照してください。

- 参加ユニットが、3 回の更新間隔の後に更新メッセージを送信できなかった場合、サーバはセッションを開放して共有ライセンス プールに戻します。
- 参加ユニットは、更新メッセージを送信するためにライセンス サーバにアクセスできない場合、最大 24 時間、サーバから受信した共有ライセンスを使用し続けることができます。
- 24 時間が経過して参加ユニットがライセンス サーバと通信できなくなった場合、セッションが必要でも、参加ユニットは共有ライセンスを開放します。参加ユニットは既存の接続を確立したままにしますが、ライセンスの制限を超えて新しい接続を受け入れることはできません。
- 24 時間の期限前でもサーバで参加ユニット セッションの期限が切れた後であれば、参加ユニットはサーバに再接続する場合に、セッションの新しい要求を送信する必要があります。サーバは、その参加ユニットに再割り当てできる数のセッションで応答します。

ライセンス バックアップ サーバに関する情報

共有ライセンス バックアップ サーバがバックアップ ロールを引き受けるには、共有ライセンス バックアップ サーバをメインの共有ライセンス サーバに正しく登録する必要があります。登録時に、メインの共有ライセンス サーバは、サーバ設定および共有ライセンス情報（登録済み参加ユニットのリストや現在のライセンスの使用状況を含む）をバックアップと同期します。メイン サーバとバックアップ サーバは 10 秒間隔で同期します。最初の同期の後、バックアップ サーバはリロードの後であっても正常にバックアップ作業を実行できます。

メイン サーバがダウンすると、バックアップ サーバはサーバの処理を引き継ぎます。バックアップ サーバは最大 30 日間連続して動作できます。30 日が経過すると、バックアップ サーバは参加ユニットに対するセッションの発行を停止し、既存のセッションはタイムアウトします。30 日の期間内にメイン サーバを必ず元の状態に戻してください。Critical レベルの syslog メッセージが 15 日目に送信され、30 日目に再送信されます。

メイン サーバはバックアップになると、バックアップ サーバと同期し、サーバの操作を引き継ぎます。

バックアップ サーバはアクティブでない場合、メインの共有ライセンス サーバの通常の参加ユニットとして機能します。

（注） メインの共有ライセンス サーバを最初に起動した場合、バックアップ サーバは 5 日間だけ単独で動作できます。動作上の制限は、30 日まで日毎に増えていきます。また、メイン サーバが後からしばらくの間ダウンした場合、バックアップ サーバの動作上の制限は日毎に減少していきます。メイン サーバがバックアップになると、バックアップ サーバの動作上の制限はまた日毎に増えていきます。たとえば、メイン サーバが 20 日間ダウンしていた場合、その期間中バックアップ サーバはアクティブになり、バックアップ サーバには 10 日間の制限しか残されなくなります。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 20 日間経過した後、最大 30 日まで「再バックアップ」します。この再バックアップ機能は、共有ライセンスの誤用を防ぐために実装されます。

フェールオーバーおよび共有ライセンス

ここでは、共有ライセンスとフェールオーバーの連携について説明します。次のトピックについて取り上げます。

- 「フェールオーバーおよび共有ライセンス サーバ」（P.15）
- 「フェールオーバーおよび共有ライセンスの参加ユニット」（P.17）

フェールオーバーおよび共有ライセンス サーバ

ここでは、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の連携について説明します。共有ライセンス サーバは、VPN ゲートウェイやファイアウォールとしての機能を実行するなど、セキュリティ アプライアンスとして通常の作業も実行するため、メインの共有ライセンス サーバとバックアップ共有ライセンス サーバにフェールオーバーを設定して信頼性を高める必要があります。

（注） バックアップ サーバ メカニズムはフェールオーバーとは異なりますが、フェールオーバーと互換性があります。

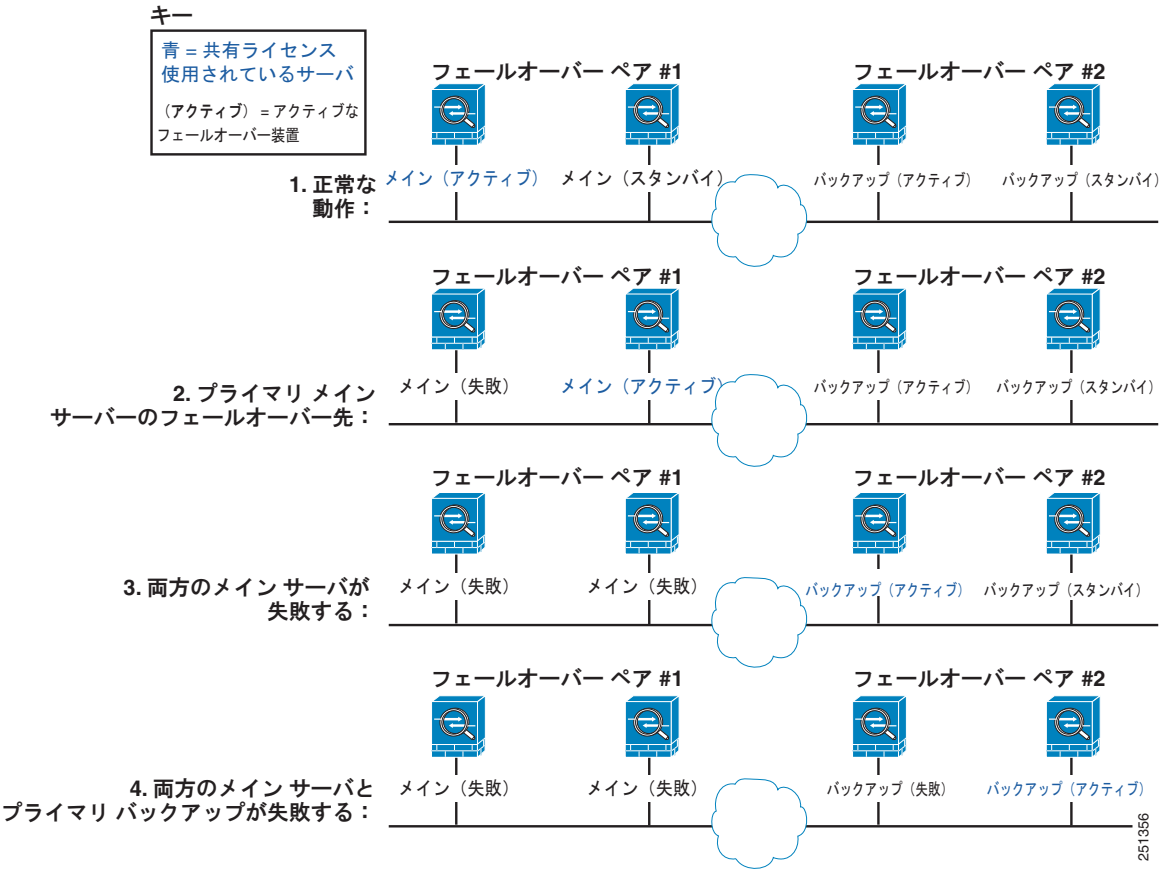
共有ライセンスは単一のコンテキスト モードだけでサポートされるため、アクティブ/アクティブ フェールオーバーはサポートされません。

フェールオーバー ペアの両方のメイン共有ライセンス サーバ ユニットには同じライセンスが必要です。そのため、プライマリ メイン サーバ ユニット用に 10,000 セッション共有ライセンスを購入した場合は、スタンバイ メイン サーバ ユニット用にも 10,000 セッション共有ライセンスを購入する必要があります。スタンバイ ユニットはスタンバイ状態のときにトラフィックを生成しないため、この例のセッションの合計数は、結合された 20,000 セッション *ではなく*、10,000 セッションのままになります。

アクティブ/スタンバイ フェールオーバーの場合、プライマリ ユニットはメインの共有ライセンス サーバとして機能し、スタンバイ ユニットがフェールオーバー後、メインの共有ライセンス サーバとして機能します。両方のユニットに同じライセンスが必要であるため、どちらのユニットもメイン ライセンス サーバとして機能できます。スタンバイ ユニットは、バックアップ共有ライセンス サーバとして機能 *しません*。代わりに、必要に応じてバックアップ サーバとして機能する 2 つ目のユニットのペアを使用できます。

たとえば、2 つのフェールオーバー ペアを持つネットワークがあるとします。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 ユニットがダウンするとすぐにスタンバイ ユニットが新しいメインのライセンス サーバになります。ペア #2 のバックアップ サーバは使用されません。ペア #1 の両方のユニットがダウンした場合に限り、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ます。ペア #1 がダウンしたままで、ペア #2 のプライマリ ユニットがダウンすると、ペア #2 のスタンバイ ユニットが共有ライセンス サーバとして使用されます（図 2 を参照）。

図 2　　フェールオーバーおよび共有ライセンス 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 サーバと同じ動作上の制限を共有します。スタンバイ ユニットがアクティブになると、プライマリ ユニットが中止した時点までカウント ダウンを続行します。詳細については、「ライセンス バックアップ サーバに関する情報」（P.14）を参照してください。

フェールオーバーおよび共有ライセンスの参加ユニット

参加ユニットのペアでは、両方のユニットが個別の参加 ID を使用して共有ライセンス サーバに登録します。アクティブなユニットは、その参加ユニットの ID をスタンバイ ユニットと同期します。スタンバイ ユニットは、アクティブ ロールに切り替えるときに、この ID を使用して転送要求を生成します。この転送要求を使用して、それまでアクティブであったユニットから新しいアクティブなユニットに共有セッションを移動します。

参加ユニットの最大数

セキュリティ アプライアンスでは、共有ライセンスの参加ユニットの数に制限はありませんが、共有ネットワークの規模が非常に大きくなると、ライセンス サーバのパフォーマンスに影響を与えることがあります。この場合は、参加ユニットの更新間の遅延を大きくすることも、2 つの共有ネットワークを作成することもできます。

ライセンスに関する FAQ

Q. VPN Flex や Botnet Traffic Filter などの複数の一時ライセンスをアクティブ化できますか。

A. いいえ、できません。一度に使用できるのは 1 つの一時ライセンスだけです。最後にアクティブ化したライセンスが使用されます。複数の機能を 1 つのアクティベーション キーにグループ化した評価ライセンスの場合は、複数の機能が同時にサポートされます。ただし、シスコが販売している一時ライセンスは、アクティベーション キーごとに 1 つの機能に制限されています。

Q. 期限が切れたときに自動的に次のライセンスを使用できるように、一時ライセンスを「スタック」することはできますか。

A. いいえ、できません。複数の一時ライセンスをインストールすることはできますが、アクティブになるのは最後にアクティブ化したライセンスだけです。アクティブなライセンスが期限切れになった場合は、新しいライセンスを手動でアクティブ化する必要があります。機能が失われないように、必ず古いライセンスの期限が切れる直*前に*アクティブ化してください（古いライセンスの残り時間は未使用のままになります。たとえば、12 か月のライセンスの 10 か月分を使用し、新しい 12 か月のライセンスをアクティブ化すると、最初のライセンスの残りの 2 か月は、後でそのライセンスをアクティブ化しない限り未使用のままになります。ライセンスを最大限活用するためには、古いライセンスの失効日のできる限り近い時期に新しいライセンスをアクティブ化することを推奨します）。

Q. アクティブな一時ライセンスを保持しながら、新しい永続ライセンスをインストールできますか。

A. いいえ、できません。永続ライセンスを適用すると、一時ライセンスは非アクティブ化されます。一時ライセンスとともに新しい永続ライセンスを使用できるようにするには、永続ライセンスをアクティブ化し、次に一時ライセンスを再びアクティブ化する必要があります。この結果、一時ライセンスに依存している機能が一時的に失われます。

Q. フェールオーバー用に共有ライセンス サーバをプライマリ ユニットとして、共有ライセンス バックアップ サーバをセカンダリ ユニットとして使用できますか。

A. いいえ、できません。セカンダリ ユニットにも共有ライセンス サーバ ライセンスが必要です。参加ライセンスを持つバックアップ サーバは、2 つのバックアップ サーバで構成される個別のフェールオーバー ペアに入れることができます。

Q. フェールオーバー ペアのセカンダリ ユニットのために同じライセンスを購入する必要はありますか。共有ライセンス サーバの場合でもその必要はありますか。

A. はい。両方のユニットに同じライセンスが必要です。共有ライセンス サーバでは、両方のユニットに同じ共有ライセンス サーバ ライセンスを購入する必要があります。**注：**アクティブ/スタンバイ フェールオーバーの場合、セッション数を指定するライセンスでは、両方のユニットのセッションは互いに加算されず、アクティブなユニットのセッションだけを使用できます。たとえば、共有 SSL VPN ライセンスでは、アクティブなユニットとスタンバイ ユニットの両方に 10,000 のユーザ セッションを購入する必要があります。セッションの合計は、合わせて 20,000 *ではなく*、10,000 です。

Q. 共有 SSL VPN ライセンスに加えて VPN Flex または永続 SSL VPN ライセンスを使用できますか。

A. はい。共有ライセンスは、ローカルにインストールされたライセンス（VPN Flex または永続）を使い切った後に限り使用されます。**注**：共有ライセンス サーバでは、永続 SSL VPN ライセンスは使用されません。ただし、VPN Flex ライセンスを共有ライセンス サーバ ライセンスと同時に使用することができます。この場合は、VPN Flex ライセンス セッションをローカル SSL VPN セッションだけに使用できます。参加ユニットが使用する共有ライセンス プールには追加できません。

ガイドラインと制限事項

アクティベーション キーについては、次のガイドラインを参照してください。

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 モードでは、アクティベーション キーをシステム実行領域に適用します。
- 共有ライセンスはマルチ コンテキスト モードではサポートされません。

ファイアウォール モードのガイドライン

すべてのライセンス タイプは、ルーテッド モードとトランスペアレント モードの両方で使用できます。

フェールオーバーのガイドライン

- プライマリ ユニットとセカンダリ ユニットの両方で同じライセンスをアクティブ化している必要があります。

（注） フェールオーバーが目的の場合、2 つのユニット間でフィーチャ セットが同一である限り、永続ライセンスと一時ライセンスに違いはありません。詳細については、「フェールオーバー ライセンスと一時ライセンス」（P.13）を参照してください。

- アクティブ/アクティブ モードでは共有ライセンスはサポートされません。詳細については、「フェールオーバーおよび共有ライセンス」（P.15）を参照してください。

アップグレードのガイドライン

バージョン 8.2 以降にアップグレードする場合、また後でダウングレードする場合は、アクティベーション キーの互換性は維持されます。アップグレード後に、*8.2 以前に*導入された追加の機能ライセンスをアクティブ化した場合は、ダウングレードすると、アクティベーション キーは以前のバージョンとの互換性を維持します。ただし、*8.2 以降*に導入された機能ライセンスをアクティブ化すると、アクティベーション キーの後方互換性はなくなります。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。

- 以前に旧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、セキュリティ アプライアンス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は除く）。

- システムが新しく、以前のアクティベーション キーを持っていない場合は、旧バージョンと互換性がある新しいアクティベーション キーを請求する必要があります。

その他のガイドラインと制限事項

- 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ず、フラッシュ メモリの隠しファイルに保存されます。
- 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ています。機能ライセンスはデバイス間で転送できません（ハードウェアで障害が発生した場合を除く）。ハードウェアの障害が原因でデバイスを交換する必要がある場合は、シスコ ライセンス チームに連絡し、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要請してください。シスコ ライセンス チームに、Product Authorization Key の参照番号と既存のシリアル番号をお伝えください。
- 一度購入したライセンスは、返金またはライセンスのアップグレードの目的では返品できません。
- 同じ機能について 2 つの個別のライセンスを同時に追加できません。たとえば、25 セッションの SSL VPN ライセンスを購入し、後に 50 セッションのライセンスを購入しても、75 のセッションは使用できません。使用できるセッションの数は最大で 50 です。
- すべてのライセンス タイプをアクティブ化することはできますが、マルチ コンテキスト モードと VPN のように互換性がない機能もあります。AnyConnect Essentials ライセンスの場合、このライセンスは、フル SSL VPN ライセンス、共有 SSL VPN ライセンス、および Advanced Endpoint Assessment ライセンスとは互換性がありません。デフォルトでは、AnyConnect Essentials ライセンスがこれらのライセンスの代わりに使用されます。ただし、**no anyconnect-essentials** コマンドを使用することにより、コンフィギュレーションの AnyConnect Essentials ライセンスを無効にして、他のライセンスを再び使用することができます。

現在のライセンスの表示

ここでは、現在のライセンスを表示する方法と、一時アクティベーション キーのライセンスの残り時間を表示する方法について説明します。

詳細な手順

CLI の場合：

コマンド	目的
show activation-key detail **例：** `hostname# show activation-key detail`	一時ライセンスに関する情報など、インストールされているライセンスを表示します。

ASDM の場合：

現在のライセンスを表示するには、[Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択します。

マルチ コンテキスト モードでは、[Configuration] > [Device Management] > [Activation Key] を選択し、システム実行領域でアクティベーション キーを表示します。

例

次に **show activation-key detail** コマンドの出力例を示します。この出力は、永続アクティベーション ライセンスと 2 つの SSL VPN ピア（太字）、アクティブな一時ライセンスと 5000 の SSL VPN ピア（太字）、結合された実行ライセンスと一時ライセンスから取得した SSL VPN ピア（太字）、また、非アクティブな一時ライセンスのアクティベーション キーを示しています。

```
hostname# show activation-key detail

Serial Number:  JMX0916L0Z4

Permanent Flash Activation Key: 0xf412675d 0x48a446bc 0x8c532580 0xb000b8c4 0xcc21f48e

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
VPN Peers                    : 2
SSL VPN Peers                : 2
Total VPN Peers              : 250
Shared License               : Enabled
  Shared SSL VPN Peers       : 5000
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 24
Total UC Proxy Sessions      : 24
Botnet Traffic Filter        : Enabled

Temporary Flash Activation Key: 0xcb0367ce 0x700dd51d 0xd57b98e3 0x6ebcf553 0x0b058aac

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
SSL VPN Peers                : 5000
Total VPN Peers              : 250
Shared License               : Enabled
  Shared SSL VPN Peers       : 10000
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 24
Total UC Proxy Sessions      : 24
Botnet Traffic Filter        : Enabled

This is a time-based license that will expire in 27 day(s).

Running Activation Key: 0xcb0367ce 0x700dd51d 0xd57b98e3 0x6ebcf553 0x0b058aac

Licensed features for this platform:
```

```
Maximum Physical Interfaces  : Unlimited
Maximum VLANs                : 200
Inside Hosts                 : Unlimited
Failover                     : Active/Active
VPN-DES                      : Enabled
VPN-3DES-AES                 : Enabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
SSL VPN Peers                : 5000
Total VPN Peers              : 250
Shared License               : Enabled
  Shared SSL VPN Peers       : 10000
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 24
Total UC Proxy Sessions      : 24
Botnet Traffic Filter        : Enabled


This platform has an ASA 5540 VPN Premium license.
This is a Shared SSL VPN License server.

This is a time-based license that will expire in 27 day(s).

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

Non-active temporary keys:                                Time left
-----------------------------------------------------------------
0x2a53d6   0xfc087bfe 0x691b94fb 0x73dc8bf3 0xcc028ca2  28 day(s)
0xa13a46c2 0x7c10ec8d 0xad8a2257 0x5ec0ab7f 0x86221397  27 day(s)
```

アクティベーション キーの取得

アクティベーション キーを取得するには、シスコの代理店から購入できる Product Authorization Key が必要です。機能ライセンスごとに個別の製品アクティベーション キーを購入する必要があります。たとえば、基本ライセンスを持っている場合は、Advanced Endpoint Assessment や追加の SSL VPN セッション用に個別のキーを購入することができます。

（注） フェールオーバー ペアでは、ユニットごとに個別のアクティベーション キーが必要です。キーに含まれるライセンスが両方のユニットで同じであることを確認します。

Product Authorization Key を取得した後、次の手順に従って Cisco.com で登録します。

ステップ 1 セキュリティ アプライアンスのシリアル番号を、（ASDM の場合）[Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択して（マルチ コンテキスト モードでは、システム実行領域でシリアル番号を表示）、または次のコマンドを入力して取得します。

```
hostname# show activation-key
```

ステップ 2 次のいずれかの URL にアクセスします。

- Cisco.com の登録済みユーザであれば、次の Web サイトを使用します。

  `http://www.cisco.com/go/license`

- Cisco.com の登録済みユーザでなければ、次の Web サイトを使用します。

  `http://www.cisco.com/go/license/public`

ステップ 3 プロンプトに従って次の情報を入力します。

- Product Authorization Key（複数のキーがある場合は、いずれかのキーを最初に入力します。各キーは個別の手順を使用して入力する必要があります）。
- セキュリティ アプライアンスのシリアル番号
- E 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 E メール アドレスに送信されます。このキーには、永続ライセンスについてこれまでに登録したすべての機能が含まれます。VPN Flex ライセンスでは、各ライセンスに個別のアクティベーション キーがあります。

ステップ 4 追加の Product Authorization Key がある場合は、Product Authorization Key ごとにステップ 3 を繰り返します。すべての Product Authorization Key を入力すると、提供される最終的なアクティベーション キーに登録したすべての永続機能が含まれるようになります。

新しいアクティベーション キーの入力

ここでは、新しいアクティベーション キーの入力方法について説明します。

前提条件

- アクティベーション キーを入力する前に、**show activation-key** コマンドを入力することにより、フラッシュ メモリのイメージと実行イメージが同一であることを確認します。これは、新しいアクティベーション キーを入力する前にセキュリティ アプライアンスをリロードすることで確認できます。
- すでにマルチ コンテキスト モードになっている場合は、システム実行領域にアクティベーション キーを入力します。
- 一部のライセンスでは、アクティブ化した後にセキュリティ アプライアンスをリロードする必要があります。表 8 に、リロードが必要なライセンスの一覧を示します。

表 8　　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の処理
ASA 5505 および ASA 5510	基本ライセンスと Security Plus ライセンスの切り替え
すべてのモデル	暗号化ライセンスの変更
すべてのモデル	任意のライセンスのダウングレード（コンテキスト 10 個からコンテキスト 2 個へなど）。 **（注）** 一時ライセンスが期限切れになり、永続ライセンスがダウングレードの場合は、ただちにセキュリティ アプライアンスをリロードする必要はありません。次にリロードすると、永続ライセンスが復元されます。

制限事項と制約事項

バージョン 8.2 以降にアップグレードする場合、また後でダウングレードする場合は、アクティベーション キーの互換性は維持されます。アップグレード後に、*8.2 以前に*導入された追加の機能ライセンスをアクティブ化した場合は、ダウングレードすると、アクティベーション キーは以前のバージョンとの互換性を維持します。ただし、*8.2 以降*に導入された機能ライセンスをアクティブ化すると、アクティベーション キーの後方互換性はなくなります。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。

- 以前に旧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、セキュリティ アプライアンス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は除く）。
- システムが新しく、以前のアクティベーション キーを持っていない場合は、旧バージョンと互換性がある新しいアクティベーション キーを請求する必要があります。

詳細な手順

CLI の場合：

	コマンド	目的
ステップ 1	**activation-key** *key* **例：** `hostname# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	セキュリティ アプライアンスにアクティベーション キーを適用します。このキーは、5 つの要素からなる 16 進文字列で、各要素間にスペースが入ります。先頭の 0x 指定子はオプションです。すべての値は 16 進数と見なされます。 1 つの永続キーと複数の一時キーを入力することができます。最後に入力した一時キーがアクティブな一時キーになります。詳細については、「一時ライセンス、VPN Flex ライセンス、および評価ライセンス」（P.11）を参照してください。実行アクティベーション キーを変更するには、キーの新しい値を使用して **activation-key** コマンドを入力します。
ステップ 2	**reload** **例：** `hostname# reload`	（場合によっては必要）セキュリティ アプライアンスをリロードします。一部のライセンスでは、新しいアクティベーション キーを入力した後にセキュリティ アプライアンスをリロードする必要があります。リロードが必要なライセンスの一覧は、表 8（P.23）を参照してください。リロードする必要がある場合は、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.`

ASDM の場合：

ステップ 1 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択します。

ステップ 2 [New Activation Key] フィールドに新しいアクティベーション キーを入力します。

このキーは、5 つの要素からなる 16 進文字列で、各要素間にスペースが入ります。先頭の 0x 指定子はオプションです。すべての値は 16 進数と見なされます。次の例を参考にしてください。

```
0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

1 つの永続キーと複数の一時キーを入力することができます。最後に入力した一時キーがアクティブな一時キーになります。詳細については、「一時ライセンス、VPN Flex ライセンス、および評価ライセンス」（P.11）を参照してください。実行アクティベーション キーを変更するには、新しい値を入力します。

ステップ 3 [Update Activation Key] をクリックします。

フェールオーバー ペアのライセンスのアップグレード

フェールオーバー ペアのライセンスをアップグレードする必要がある場合は、ライセンスにリロードが必要かどうかに応じて、ある程度のダウンタイムが発生することがあります。リロードが必要なライセンスの詳細については、表 8（P.23）を参照してください。この項は、次の内容で構成されています。

フェールオーバーのライセンスのアップグレード（リロードは不要）

新しいライセンスにリロードが不要な場合は、次の手順に従います。リロードが必要なライセンスの詳細については、表 8（P.23）を参照してください。この手順では、ダウンタイムが発生しないことを確認します。

前提条件

ライセンスをアップグレードする前に、両方のユニットが正しく動作していること、フェールオーバー LAN インターフェイスが起動していること、フェールオーバー イベントが直後に発生しないこと（監視対象のインターフェイスが正常に動作しているなど）を確認します。

各ユニットで、**show failover** コマンドを入力するか、または ASDM の場合は [Monitoring] > [Properties] > [Failover] > [Status] を選択し、フェールオーバーの状態と監視対象のインターフェイスの状態を表示します。

詳細な手順

CLI の場合：

	コマンド	目的
	アクティブなユニットで次の手順を実行します。	
ステップ 1	**no failover** **例：** `active(config)# no failover`	アクティブなユニットでフェールオーバーをディセーブルにします。スタンバイ ユニットは擬似スタンバイ状態のままになります。アクティブなユニットでフェールオーバーを非アクティブにすると、スタンバイ ユニットは、ライセンスが一致していない間にアクティブになるよう試みません。
ステップ 2	**activation-key** *key* **例：** `active(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	アクティブなユニットに新しいライセンスをインストールします。このライセンスが、アクティブなユニットのシリアル番号のものであることを確認します。
	スタンバイ ユニットで次の手順を実行します。	
ステップ 3	**activation-key** *key* **例：** `standby# activation-key 0xc125727f 0x903de1ee 0x8c838928 0x92dc84d4 0x003a2ba0`	スタンバイ ユニットに新しいライセンスをインストールします。このライセンスがスタンバイ ユニットのシリアル番号のものであることを確認します。

	コマンド	目的
	アクティブなユニットで次の手順を実行します。	
ステップ 4	**failover** **例：** `active(config)# failover`	フェールオーバーを再びイネーブルにします。

ASDM の場合：

ステップ 1 アクティブなユニットで、[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup] を選択し、[Enable Failover] チェックボックスをオフにします。

スタンバイ ユニットは擬似スタンバイ状態のままになります。アクティブなユニットでフェールオーバーを非アクティブにすると、スタンバイ ユニットは、ライセンスが一致していない間にアクティブになるよう試みません。

ステップ 2 [Apply] をクリックします。

ステップ 3 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択し、アクティブなユニットのシリアル番号を使用して取得した新しいアクティベーション キーを入力します。

ステップ 4 [Update Activation Key] をクリックします。

ステップ 5 デバイス リストでアドレスをダブルクリックし、スタンバイ ユニットにログインします。

そのデバイスがデバイス リストにない場合は、[Add] をクリックして追加します。ログインするための認定証を求められることがあります。

ステップ 6 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択し、スタンバイ ユニットのシリアル番号を使用して取得した新しいアクティベーション キーを入力します。

ステップ 7 [Update Activation Key] をクリックします。

ステップ 8 デバイス リストでアドレスをダブルクリックし、アクティブなユニットに再びログインします。

ステップ 9 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup] を選択し、[Enable Failover] チェックボックスを再びオンにします。

ステップ 10 [Apply] をクリックします。

フェールオーバーのライセンスのアップグレード（リロードが必要）

新しいライセンスにリロードが必要な場合は、次の手順に従います。リロードが必要なライセンスの詳細については、表 8（P.23）を参照してください。フェールオーバー ペアのリロードにより、リロード中に接続が失われます。

前提条件

ライセンスをアップグレードする前に、両方のユニットが正しく動作していること、フェールオーバー LAN インターフェイスが起動していること、フェールオーバー イベントが直後に発生しないこと（監視対象のインターフェイスが正常に動作しているなど）を確認します。

各ユニットで、**show failover** コマンドを入力するか、または ASDM の場合は [Monitoring] > [Properties] > [Failover] > [Status] を選択し、フェールオーバーの状態と監視対象のインターフェイスの状態を表示します。

詳細な手順

CLI の場合：

	コマンド	目的
	アクティブなユニットで次の手順を実行します。	
ステップ 1	**no failover** **例：** `active(config)# no failover`	アクティブなユニットでフェールオーバーをディセーブルにします。スタンバイ ユニットは擬似スタンバイ状態のままになります。アクティブなユニットでフェールオーバーを非アクティブにすると、スタンバイ ユニットは、ライセンスが一致していない間にアクティブになるよう試みません。
ステップ 2	**activation-key** *key* **例：** `active(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	アクティブなユニットに新しいライセンスをインストールします。 リロードする必要がある場合は、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.` リロードする必要がない場合は、この手順ではなく「フェールオーバーのライセンスのアップグレード（リロードは不要）」（P.25）に従います。
	スタンバイ ユニットで次の手順を実行します。	
ステップ 3	**activation-key** *key* **例：** `standby# activation-key 0xc125727f 0x903de1ee 0x8c838928 0x92dc84d4 0x003a2ba0`	スタンバイ ユニットに新しいライセンスをインストールします。
ステップ 4	**reload** **例：** `standby# reload`	スタンバイ ユニットをリロードします。
	アクティブなユニットで次の手順を実行します。	
ステップ 5	**reload** **例：** `active(config)# reload`	アクティブなユニットをリロードします。リロード前に設定を保存するよう求められたら、**No** と答えます。これは、アクティブなユニットがバックアップされてもフェールオーバーがイネーブルにされることを示します。

ASDM の場合：

ステップ 1 アクティブなユニットで、[Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup] を選択し、[Enable Failover] チェックボックスをオフにします。

スタンバイ ユニットは擬似スタンバイ状態のままになります。アクティブなユニットでフェールオーバーを非アクティブにすると、スタンバイ ユニットは、ライセンスが一致していない間にアクティブになるよう試みません。

ステップ 2 [Apply] をクリックします。

ステップ 3 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択し、アクティブなユニットのシリアル番号を使用して取得した新しいアクティベーション キーを入力します。

ステップ 4 [Update Activation Key] をクリックします。

ステップ 5 デバイス リストでアドレスをダブルクリックし、スタンバイ ユニットにログインします。

そのデバイスがデバイス リストにない場合は、[Add] をクリックして追加します。ログインするための認定証を求められることがあります。

ステップ 6 [Configuration] > [Device Management] > [Licensing] > [Activation Key] を選択し、スタンバイ ユニットのシリアル番号を使用して取得した新しいアクティベーション キーを入力します。

ステップ 7 [Update Activation Key] をクリックします。

ステップ 8 デバイス リストでアドレスをダブルクリックし、アクティブなユニットに再びログインします。

ステップ 9 [Configuration] > [Device Management] > [High Availability] > [Failover] > [Setup] を選択し、[Enable Failover] チェックボックスを再びオンにします。

ステップ 10 [Apply] をクリックします。

ステップ 11 [Tools] > [System Reload] を選択して、セキュリティ アプライアンスのリロードをスケジュールします。

ステップ 12 希望の時刻にセキュリティ アプライアンスをリロードするようにリロード オプションを選択し、[Schedule Reload] をクリックします。

サービス中断の影響が最も少ない時刻を選択してください。

ステップ 13 デバイス リストでアドレスをダブルクリックし、スタンバイ ユニットに再びログインします。

ステップ 14 [Tools] > [System Reload] を選択して、セキュリティ アプライアンスのリロードをスケジュールします。

ステップ 15 アクティブなユニットについて選択した時刻と同じ時刻にセキュリティ アプライアンスをリロードするようにリロード オプションを選択し、[Schedule Reload] をクリックします。

両方のユニットが同時にリロードされ、新しいライセンスが有効になります。

共有ライセンスの設定

ここでは、共有ライセンス サーバと参加ユニットを設定する方法について説明します。共有ライセンスの詳細については、「共有ライセンス」（P.13）を参照してください。

この項は、次の内容で構成されています。

共有ライセンス サーバの設定

ここでは、共有ライセンス サーバにするようにセキュリティ アプライアンスを設定する方法について説明します。

前提条件

サーバには共有ライセンス サーバ キーが必要です。

詳細な手順

CLI の場合：

	コマンド	目的
ステップ 1	**license-server secret** *secret* **例：** `hostname(config)# license-server secret farscape`	共有秘密（4 ～ 128 文字の ASCII 文字列）を設定します。この秘密を持つすべての参加ユニットがライセンス サーバを使用できます。
ステップ 2	（オプション） **license-server refresh-interval** *seconds* **例：** `hostname(config)# license-server refresh-interval 100`	10 ～ 300 秒の更新間隔を設定します。この値は、サーバと通信する頻度を設定するために参加ユニットに提供されます。デフォルト値は 30 秒です。
ステップ 3	（オプション） **license-server port** *port* **例：** `hostname(config)# license-server port 40000`	サーバが参加ユニットからの SSL 接続を受信するポート（1 ～ 65535）を設定します。デフォルトは TCP ポート 50554 です。
ステップ 4	（オプション） **license-server backup** *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*] **例：** `hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3`	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。バックアップ サーバがフェールオーバー ペアの一部の場合は、スタンバイ ユニットのシリアル番号も指定します。1 つのバックアップ サーバとオプションのスタンバイ ユニットだけを指定できます。
ステップ 5	**license-server enable** *interface_name* **例：** `hostname(config)# license-server enable inside`	このユニットをイネーブルにし、共有ライセンス サーバにします。参加ユニット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、必要な数のインターフェイスで繰り返すことができます。

ASDM の場合：

ステップ 1 [Configuration] > [Device Management] > [Licenses] > [Shared SSL VPN Licenses] を選択します。

ステップ 2 [Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。

この秘密を持つすべての参加ユニットがライセンス サーバを使用できます。

ステップ 3 （オプション）[TCP IP Port] フィールドに、サーバが参加ユニットからの SSL 接続を受信するポート（1 ～ 65535）を入力します。

デフォルトは TCP ポート 50554 です。

ステップ 4 （オプション）[Refresh interval] フィールドで、10 ～ 300 秒の更新間隔を入力します。

この値は、サーバと通信する頻度を設定するために参加ユニットに提供されます。デフォルト値は 30 秒です。

ステップ 5 共有ライセンス領域を提供するインターフェイスで、参加ユニットがサーバと通信する任意のインターフェイスの [Shares Licenses] チェックボックスをオンにします。

ステップ 6 （オプション）バックアップ サーバを指定するには、オプションのバックアップ共有 SSL VPN ライセンス サーバ領域で次の手順を実行します。

a. [Backup server IP address] フィールドにバックアップ サーバの IP アドレスを入力します。

b. [Primary backup server serial number] フィールドにバックアップ サーバのシリアル番号を入力します。

c. バックアップ サーバがフェールオーバー ペアの一部の場合は、[Secondary backup server serial number] フィールドでスタンバイ ユニットのシリアル番号を指定します。

1 つのバックアップ サーバとオプションのスタンバイ ユニットだけを指定できます。

ステップ 7 [Apply] をクリックします。

例

次の例では、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 インターフェイスと dmz インターフェイス上の共有ライセンス サーバとしてイネーブルにします。

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

次の作業

「共有ライセンス バックアップ サーバの設定（オプション）」（P.30）（CLI の場合）、または「共有ライセンス参加ユニット、および ASDM でのオプションのバックアップ サーバの設定」（P.31）を参照してください。

共有ライセンス バックアップ サーバの設定（オプション）

（CLI の手順に限る）

ここでは、メイン サーバが停止したときにバックアップ サーバとして機能する共有ライセンス参加ユニットをイネーブルにします。

前提条件

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。

詳細な手順

	コマンド	目的
ステップ 1	**license-server address** *address* **secret** *secret* [**port** *port*] **例：** hostname(config)# license-server address 10.1.1.1 secret farscape	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。サーバの設定でデフォルトのポートを変更した場合は、それに合わせてバックアップ サーバのポートを設定します。
ステップ 2	**license-server backup enable** *interface_name* **例：** hostname(config)# license-server backup enable inside	このユニットをイネーブルにし、共有ライセンス バックアップ サーバにします。参加ユニット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、必要な数のインターフェイスで繰り返すことができます。

例

次の例では、ライセンス サーバと共有秘密を指定し、このユニットを inside インターフェイスと dmz インターフェイス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します。

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

次の作業

「共有ライセンス参加ユニット、および ASDM でのオプションのバックアップ サーバの設定」（P.31）を参照してください。

共有ライセンス参加ユニット、および ASDM でのオプションのバックアップ サーバの設定

ここでは、共有ライセンス サーバと通信するように共有ライセンス参加ユニットを設定する方法について説明します。ASDM の場合は、オプションで参加ユニットをバックアップ サーバとして設定する方法についても説明します。CLI でバックアップ サーバを設定する方法については、「共有ライセンス バックアップ サーバの設定（オプション）」（P.30）を参照してください。

前提条件

参加ユニットには共有ライセンス参加キーが必要です。

詳細な手順

CLI の場合：

	コマンド	目的
ステップ 1	**license-server address** *address* **secret** *secret* [**port** *port*] **例：** `hostname(config)# license-server address 10.1.1.1 secret farscape`	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。サーバ設定でデフォルトのポートを変更した場合は、それに合わせて参加ユニットのポートを設定します。
ステップ 2	（オプション） **license-server backup address** *address* **例：** `hostname(config)# license-server backup address 10.1.1.2`	バックアップ サーバを変更した場合は、バックアップ サーバのアドレスを入力します。

ASDM の場合：

ステップ 1 [Configuration] > [Device Management] > [Licenses] > [Shared SSL VPN Licenses] ペインの順に選択します。

ステップ 2 [Shared Secret] フィールドに、共有秘密を 4 ～ 128 ASCII 文字のストリングで入力します。

ステップ 3 （オプション）[TCP IP Port] フィールドに、SSL を使用してサーバと通信するポート（1 ～ 65535）を入力します。

デフォルトは TCP ポート 50554 です。

ステップ 4 （オプション）参加ユニットをバックアップ サーバとして指定するには、[Select backup role of participant] エリアで、次の手順を実行します。

a. [Backup Server] オプション ボタンをクリックします。

b. 参加ユニットがバックアップ サーバにアクセスするには、使用するインターフェイスの [Shares Licenses] チェックボックスをオンにします。

ステップ 5 [Apply] をクリックします。

例

次の例では、ライセンス サーバの IP アドレスと共有秘密、およびバックアップ ライセンス サーバの IP アドレスを設定します。

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

共有ライセンスの監視

共有ライセンスを監視するには、ASDM で、[Monitoring] > [VPN] > [Clientless SSL VPN] > [Shared Licenses] の順に選択するか、次のコマンドのいずれかを入力します。

コマンド	目的
show shared license [**detail** | **client** [*hostname*] | **backup**]	共有ライセンスの統計情報を表示します。オプションのキーワードはライセンス サーバに限り使用できます。**detail** キーワードを指定すると、各参加ユニットの統計情報を表示できます。表示を 1 つの参加ユニットに制限するには、**client** キーワードを使用します。**backup** キーワードを指定すると、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。
show activation-key	セキュリティ アプライアンス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 セッションに関するライセンス情報を表示します。

例

次にライセンス参加ユニットで **show shared license** コマンドを実行した場合の出力例を示します。

```
hostname>  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
```

次にライセンス参加ユニットで **show shared license detail** コマンドを実行した場合の出力例を示します。

```
hostname>  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         : XXXXXXXXXXX
  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
...
```

ライセンスの機能履歴

表 9 に、この機能のリリース履歴を示します。

表 9　　ライセンスの機能履歴

機能名	リリース	機能情報
増やされた接続数と VLAN の数	7.0(5)	次の制限が増やされました。 • ASA5510 基本ライセンス接続：32000 から 5000 へ。VLAN：0 から 10 へ。 • ASA5510 Security Plus ライセンス接続：64000 から 130000 へ。VLAN：10 から 25 へ。 • ASA5520 接続：130000 から 280000 へ。VLAN：25 から 100 へ。 • ASA5540 接続：280000 から 400000 へ。VLAN：100 から 200 へ。
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。
増やされた SSL VPN ライセンスの数	7.2(1)	5000 ユーザ SSL VPN ライセンスが ASA 5550 以上に導入されました。

表 9　ライセンスの機能履歴 （続き）

機能名	リリース	機能情報
増やされた VLAN の数	7.2(2)	ASA 5505 セキュリティ アプライアンスでは Security Plus ライセンスの VLAN の最大数が 5（3 つが完全機能、1 つはフェールオーバー、もう 1 つはバックアップ インターフェイスに制限される）から 20 の完全機能インターフェイスに増やされました。また、トランク ポートの数が 1 から 8 個に増やされました。完全機能のインターフェイスが 20 になったため、バックアップ インターフェイス コマンドを使用してバックアップ ISP インターフェイスを無効にする必要はなくなりました。この場合は完全機能のインターフェイスを使用できます。バックアップ インターフェイス コマンドは Easy VPN 設定に使用できます。 VLAN 制限についても、ASA 5510 セキュリティ アプライアンスでは基本ライセンスについては 10 から 50、Security Plus ライセンスについては 25 から 100 へ増やされ、ASA 5520 適応型セキュリティ アプライアンスでは 100 から 150 へ増やされ、ASA 5550 適応型セキュリティ アプライアンスでは 200 から 250 へ増やされました。
ASA 5510 Security Plus ライセンスでのギガビット イーサネットのサポート	7.2(3)	ASA 5510 セキュリティ アプライアンスは、Security Plus ライセンスを使用してポート 0 と 1 で Gigabit Ethernet（GE; ギガビット イーサネット）をサポートするようになりました。基本ライセンスから Security Plus にアップグレードすると、外部 Ethernet0/0 および Ethernet0/1 ポートの容量が Fast Ethernet（FE; ファースト イーサネット）（100 Mbps）から GE（1000 Mbps）に増やされます。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のまま変わりません。インターフェイスの速度を変更するには **speed** コマンドを使用し、各インターフェイスに現在設定されている速度を表示するには **show interface** コマンドを使用します。
Advanced Endpoint Assessment ライセンス	8.0(2)	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 接続の完了の条件として、リモート コンピュータはアンチウィルスと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、および関連付けられたアップデートの大幅に拡大されたコレクションをスキャンします。また、指定したレジストリ エントリ、ファイル名、およびプロセス名もスキャンします。スキャン結果は、適応型セキュリティ アプライアンスに送信されます。セキュリティ アプライアンスはユーザのログイン クレデンシャルとコンピュータのスキャン結果の両方を使用して、Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）を割り当てます。 Advanced Endpoint Assessment ライセンスでは、非適合コンピュータをバージョン要件に合わせて更新するように設定して、ホスト スキャンを拡張できます。 シスコでは、ホスト スキャンが Cisco Secure Desktop とは異なるパッケージでサポートするアプリケーションとバージョンのリストを適宜更新します。

表 9　ライセンスの機能履歴 （続き）

機能名	リリース	機能情報
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 ライセンスでは、AnyConnect クライアントを使用して Windows モバイル デバイスからセキュリティ アプライアンスに接続できます。
VPN Flex ライセンスと評価ライセンス	8.0(4)/8.1(2)	一時ライセンスのサポートが導入されました。VPN Flex ライセンスは、追加の SSL VPN セッションの一時的なサポートを提供します。
ASA 5510 基本ライセンスでのギガビット イーサネットのサポート	7.2(4)/8.0(4)	ASA 5510 セキュリティ アプライアンスは基本ライセンスでポート 0 と 1 の GE をサポートするようになりました（このサポートは以前 Security Plus ライセンスに追加されました）。外部 Ethernet0/0 および Ethernet0/1 ポートの容量が、元の FE（100 Mbps）から GE（1000 Mbps）に増やされました。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のまま変わりません。インターフェイスの速度を変更するには **speed** コマンドを使用し、各インターフェイスに現在設定されている速度を表示するには **show interface** コマンドを使用します。
ASA 5580 で増やされた VLAN の数	8.1(2)	ASA 5580 でサポートされる VLAN の数は 100 から 250 に増やされました。
ユニファイド コミュニケーション プロキシ セッション ライセンス	8.0(4)	UC プロキシ セッション ライセンスが導入されました。この機能はバージョン 8.1 では使用できません。
Botnet Traffic Filter ライセンス	8.2(1)	Botnet Traffic Filter ライセンスが導入されました。Botnet Traffic Filter は既知の不正なドメインおよび IP アドレスへの接続をトラッキングして、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。

表 9　ライセンスの機能履歴 （続き）

機能名	リリース	機能情報
AnyConnect Essentials ライセンス	8.2(1)	このライセンスでは、適応型セキュリティ アプライアンスに AnyConnect VPN クライアントからアクセスできます。このライセンスは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop をサポートしません。これらの機能を使用するには、AnyConnect Essentials ライセンスではなく、AnyConnect Premium SSL VPN ライセンスを有効にしてください。 （注） AnyConnect Essentials ライセンスを使用すると、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）できます。 AnyConnect クライアント ソフトウェアは、このライセンスで有効になっているか AnyConnect Premium SSL VPN ライセンスで有効になっているかに関係なく、同じクライアント機能セットを提供します。 AnyConnect Essentials ライセンスは、特定の適用型セキュリティ アプライアンスで AnyConnect Premium SSL VPN ライセンス（すべてのタイプ）または Advanced Endpoint Assessment ライセンスと同時にアクティブにできません。ただし、同じネットワーク内にある別の適応型セキュリティ アプライアンスで AnyConnect Essentials ライセンスと AnyConnect Premium SSL VPN ライセンスの両方を実行できます。 デフォルトでは、セキュリティ アプライアンスは AnyConnect Essentials ライセンスを使用しますが、このライセンスを無効にし、**no anyconnect-essentials** コマンドを使用して他のライセンスを使用できます。
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。複数のセキュリティ アプライアンスが SSL VPN セッションのプールを必要な単位で共有できます。