

ライセンス：ISA 3000 の製品認証キーライセンス

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。このマニュアルでは、ISA 3000 の製品認証キー（PAK）のライセンスについて説明します。その他のモデルについては、ライセンス：スマート ソフトウェア ライセンシング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 （11 ページ）
- PAK ライセンスの設定 （13 ページ）
- 共有ライセンスの設定（セキュアクライアント 3 以前） （18 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 （24 ページ）
- PAK ライセンスのモニタリング （26 ページ）
- PAK ライセンスの履歴 （27 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 （26 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 （2 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 セキュアクライアント Premium ライセンスを購入したり、

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 セキュアクライアント Premium ライセンスと 2500 セッション セキュアクライアント 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。

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
セキュアクライアント 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。
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 （26 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. 8 週 1000 セッションの セキュアクライアント 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）。
2. 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 セキュアクライアント 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 （17 ページ）
時間ベース ライセンスの有効期限 （4 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、ユーザー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 セキュアクライアント Premium ライセンス（アクティブ）、1000 セッションの時間ベース セキュアクライアント Premium ライセンス（非アクティブ）、500 セッションの永続 セキュアクライアント 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 （17 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。

Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス

Secure Client AdvantageまたはPremierライセンスは、ライセンスが指定するユーザープールを共有するすべての複数のASAに適用できる同時使用ライセンスです。Secure Client VPNのみライセンスは、特定のASAに適用されます。https://www.cisco.com/go/license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ベーション 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ー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 セキュアクライアント 発注ガイド
- セキュアクライアント ライセンスに関するよくある質問（FAQ）

（注） マルチコンテキストモードでサポートされている唯一のSecure Client Premierライセンスは Secure Client Premierライセンスです。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ピアには、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

- 合計VPNピアは、セキュアクライアント とその他のVPNピアを合算した、許可されるVPNピアの最大数となります。たとえば、合計が1000の場合はセキュアクライアント とその他のVPNピアを500ずつ、または セキュアクライアント を700とその他のVPNピア300を同時に許可できます。あるいは、1000すべてを セキュアクライアント に使用することも可能です。合計VPNピアが最大数を超えた場合は、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。

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、『Supplemental end User License Agreement for セキュアクライアント』を参照してください。

（注） Secure Client Premier ライセンスは、マルチコンテキストモードでサポートされる唯一のセキュアクライアントライセンスであり、デフォルトライセンスやレガシーライセンスは使用できません。

暗号化ライセンス

高度暗号化を有効にしている場合、DES を使用することはできません。

合計 TLS プロキシ セッション

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

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

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

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

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

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

接続には、SRTP 暗号化セッションを使用する場合もあります。

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

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

VLAN、最大

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

セキュアクライアント 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、AnyConnect 4 以降のライセンスではサポートされていません。セキュアクライアントライセンスは共有されるため、共有サーバーまたは参加者ライセンスは必要ありません。

共有ライセンスを使用すると、多数の セキュアクライアント 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 サーバーとして、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

いくつかの例外を除き、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。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シ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

モデル	ライセンス要件
ISA 3000	両方のユニットの Security Plus ライセンス。 （注） 各ユニットに同じ暗号化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、ISA 3000 で、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。

フェールオーバーライセンスの結合方法

フェールオーバーペアでは、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ト ダウンは同時に行われます。

  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。
  - 1 つの ASA には 1000 の TLS プロキシセッションがあり、もう 1 つには 2000 のセッションがあるとします。プラットフォームの限度は 2000 であるため、結合されたライセンスは 2000 の TLS プロキシセッションに対応できます。

- 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/制御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/データ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。

関連トピック

PAK ライセンスのモニタリング （26 ページ）

フェールオーバー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/制御ライセンスから差し引かれます。プライマリ/制御ライセンスが期限切れになるまでは、セカンダリ/データ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。

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す。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 （17 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、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。

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 （26 ページ）

ライセンスの FAQ

セキュアクライアント Premium とボットネット トラフィック フィルタなど、。

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 セキュアクライアント 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 セキュアクライアント 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ーでは、永続セキュアクライアント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ー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、ローカルのセキュアクライアント 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 キーを適用します。

フェールオーバーのガイドライン

フェールオーバー （8 ページ）を参照してください。

モデルのガイドライン

- スマートライセンシングは、ASA 仮想 でのみサポートされます。
- 共有ライセンスは、ASA 仮想、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、よりロバストな時間ベース 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なままです。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、（[Activation Key] ページ内）で表示されるものです。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。 [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用して、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 セキュアクライアント 発注ガイドおよび FAQ を参照してください。

- Cisco セキュアクライアント 発注ガイド

- セキュアクライアント ライセンスに関するよくある質問（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。セキュアクライアント ライセンスの場合、ユーザー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。

ステップ 2 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Activation Key]** を選択して、ご使用の ASA のシリアル番号を取得します（マルチ コンテキスト モードでは、システム実行スペースにシリアル番号を表示します）。

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。

- 製品認証キー（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。すべての製品認証キーを入力した後、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 （17 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

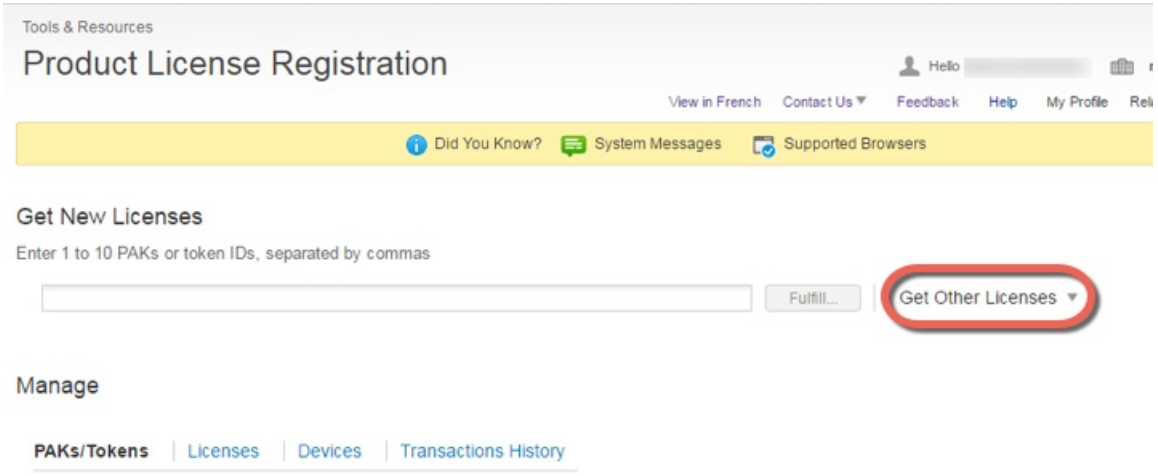
ステップ 1 次のコマンドを入力して、ASA のシリアル番号を取得します。

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。

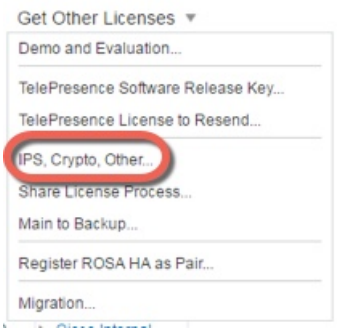
ステップ 2 Https://www.cisco.com/go/license を参照し、[Get Other Licenses] をクリックしてください。

図 *1*：他のライセンスの取得



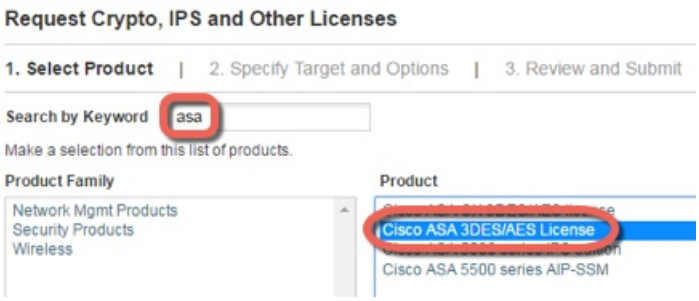
ステップ 3 [IPS、Crypto、その他（IPS, Crypto, Other）] を選択します。

図 *2*：*IPS*、*Crypto*、その他



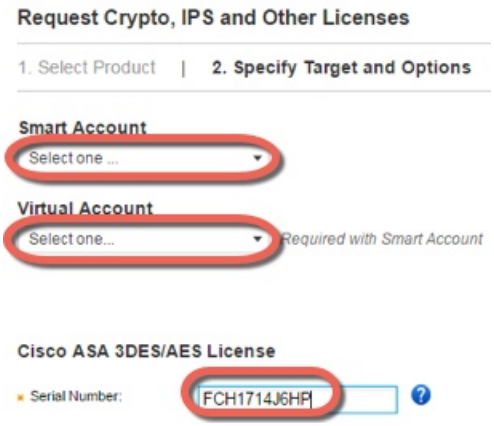
ステップ 4 [キーワード検索（Search by Keyword）] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 *3 : Cisco ASA 3DES/AES* ライセンス



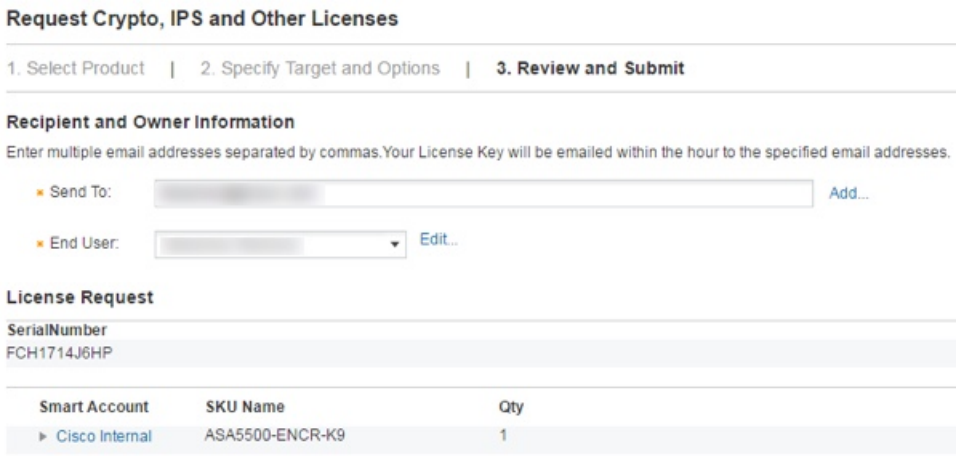
ステップ 5 [スマートアカウント（Smart Account）]、[バーチャルアカウント（Virtual Account）] を選択し、ASA の [シリアルナンバー（Serial Number）] を入力して、[次へ（Next）] をクリックします。

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



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ー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。[同意する（I Agree）] チェックボックスをオンにして、[送信（Submit）] をクリックします。

図 *5*：送信



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、**[管理（Manage）]**> **[ライセンス（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（17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 **[Configuration]** > **[Device Management]** の順に選択し、モデルに応じて、**[Licensing]** > **[Activation Key]** または [Licensing Activation Key] ペインを選択します。

ステップ 2 永続または時間ベースの新しいアクティベーション キーを入力するには、[New Activation Key] フィールドで新しいアクティベーション キーを入力します。

キーは、5 つの要素で構成される 16 進ストリングで、各要素は 1 つのスペースで区切られています。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。次に例を示します。

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

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。新しい時間ベース キーを入力した場合、デフォルトでアクティブになり、[Time-based License Keys Installed] テーブルに表示されます。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。

ステップ 3 インストール済みの時間ベース キーをアクティブ化または非アクティブ化するには、そのキーを [Time-based License Keys Installed] テーブルで選択し、[Activate] または [Deactivate] をクリックします。

各機能でアクティブにできる時間ベース キーは 1 つのみです。

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

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。必要な場合は、リロードするよう求められます。

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（セキュアクライアント 3 以前）

（注） ASA の共有ライセンス機能は、セキュアクライアント 4 以降のライセンスではサポートされていません。セキュアクライアントライセンスは共有されるため、共有サーバーまたは参加者ライセンスは必要ありません。

この項では、共有ライセンス サーバー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 セキュアクライアント 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 サーバーとして、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ー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 サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバー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 サーバー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 サーバーとして指定します。バックアップ サーバーには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバー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 サーバー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 サーバーに登録します。

（注） 参加者は IP ネットワークを経由してサーバーと通信でき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。

6. 共有ライセンス サーバーは、参加者がサーバーにポーリングするべき頻度の情報で応答します。
7. 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 サーバーに 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。
8. 共有ライセンス サーバーは、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 サーバーは、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ー ライセンスも必要ありません。

1. 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、サーバーは使用可能な限りのセッション数で応答します。
2. 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ー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、参加者はサーバー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、サーバーと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバーの間の通信問題

参加者とサーバー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、サーバー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 サーバーに到達できない場合、参加者はサーバー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 サーバー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ーに再接続したが、サーバー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。サーバーは、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 サーバーについて

共有ライセンス バックアップ サーバーは、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 サーバー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 サーバーは共有ライセンス情報に加えてサーバー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 サーバーとバックアップ サーバーは、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 サーバー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 サーバーがダウンすると、バックアップ サーバーがサーバー動作を引き継ぎます。バックアップ サーバーは継続して最大30日間動作できます。30日を超えると、バックアップ サーバー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 サーバーをこの 30 日間中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 サーバーが復旧した場合、メイン サーバーはバックアップ サーバーと同期してから、サーバー動作を引き継ぎます。

バックアップ サーバーがアクティブでないときは、メインの共有ライセンス サーバー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 サーバーの初回起動時には、バックアップ サーバーは独立して 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、メインサーバー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ーの動作制限は日ごとに減少します。メイン サーバーが復旧した場合、バックアップ サーバーは再び日ごとに増加を開始します。たとえば、メイン サーバーが 20 日間ダウンしていて、その期間中バックアップ サーバーがアクティブであった場合、バックアップ サーバーには、10 日間の制限のみが残っています。バックアップ サーバーは、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 サーバー

この項では、メイン サーバーおよびバックアップ サーバーと、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 サーバーでは、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 サーバー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。

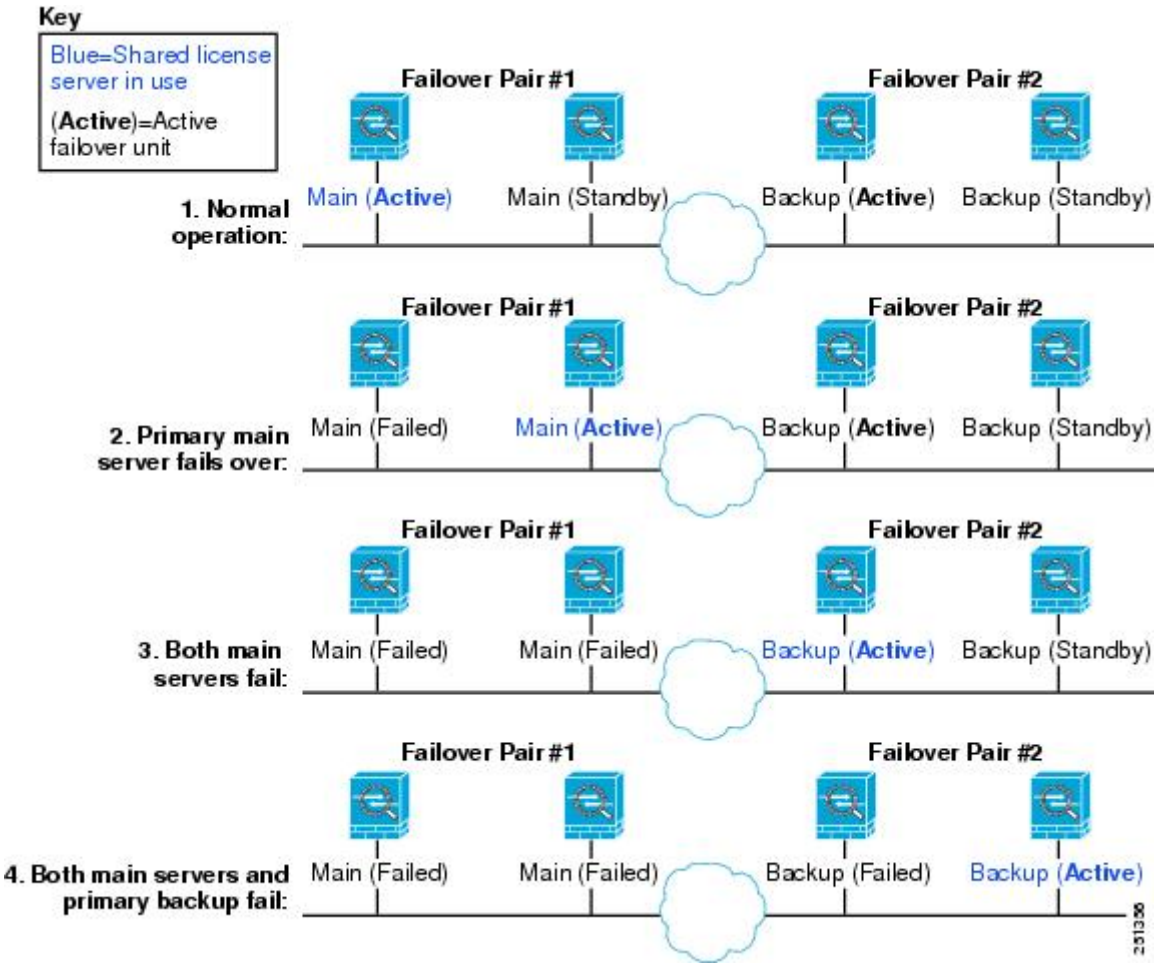
（注） バックアップ サーバー メカニズムとフェールオーバーは異なりますが、両者には互換性があります。

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 サーバーとして機能し、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 サーバーとして機能します。スタンバイ装置は、バックアップの共有ライセンス サーバーとしては機能しません。必要に応じて、バックアップ サーバー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 サーバーが含まれます。ペア #2 にはバックアップ サーバーが含まれます。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 サーバーになります。ペア #2 のバックアップ サーバー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 サーバーが共有ライセンス サーバー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 サーバー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 サーバー



スタンバイ バックアップ サーバーは、プライマリ バックアップ サーバー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 サーバーについて （20 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 サーバーに登録します。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 サーバー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 サーバーの設定

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

始める前に

サーバーが共有ライセンス サーバー キーを持っている必要があります。

手順

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

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 サーバーを使用できます。

ステップ 3 （オプション）[TCP IP Port] フィールドに、サーバー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、サーバー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。デフォルトは 30 秒です。

ステップ 5 [Interfaces that serve shared licenses] 領域で、[Shares Licenses] チェック ボックスをオンにします。パーティシパントからサーバーへの通信には、このチェックボックスに対応するインターフェイスが使用されます。

ステップ 6 （オプション）バックアップ サーバーを指定するには、[Optional backup shared SSL VPN license server] 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 サーバーの 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 サーバーのシリアル番号を入力します。
c) バックアップ サーバー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 サーバー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 7 [適用（Apply）] をクリックします。

共有ライセンス パーティシパントとオプションのバックアップ サーバーの設定

この項では、共有ライセンス サーバーと通信する共有ライセンス参加システムを設定します。このセクションでは、オプションで参加者をバックアップ サーバーとして設定する方法も説明します。

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 **[Configuration]** > **[Device Management]** > **[Licenses]** > **[Shared SSL VPN Licenses]** ペインを選択します。

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。

ステップ 3 （任意）[TCP IP Port] フィールドに、SSL を使用してサーバーと通信するポート（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 （任意）参加ユニットをバックアップ サーバー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) [Shares Licenses] チェックボックスをオンにします。パーティシパントからバックアップ サーバーへの通信には、このチェックボックスに対応するインターフェイスが使用されます。

ステップ 5 [適用（Apply）] をクリックします。

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 （9 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 （4 ページ）を参照してください。

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				
セキュアクライアントピア	無効	オプション*Secure Client Advantage*、*Secure Client Premier*、*Secure Client VPN* のみライセンス：最大 *25*	無効	オプション*Secure Client Advantage*、*Secure Client Premier*、*Secure Client VPN* のみライセンス：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	
一般ライセンス				

ライセンス	基本ライセンス		Security Plus 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 （9 ページ）」を参照してください。

手順

ステップ 1 （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ある）実行ライセンスを表示するには、**[Configuration]** > **[Device Management]** > **[Licensing]** > **[Activation Key]** ペインを選択します。

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

フェールオーバー ペアの場合、表示される実行ライセンスは、プライマリ装置とセカンダリ装置からの結合されたライセンスです。詳細については、「フェールオーバー ライセンスの結合方法 （8 ページ）」を参照してください。数値が割り当てられた時間ベース ライセンス（期間は結合されません）の場合、[License Duration] カラムには、プライマリ装置またはセカンダリ装置からの最短の時間ベース ライセンスが表示されます。このライセンスの有効期限が切れると他の装置のライセンスの期間が表示されます。

ステップ 2 （任意）時間ベース ライセンスの詳細（ライセンスに含まれる機能やライセンス期間など）を [Time-Based License Keys Installed] 領域に表示するには、ライセンス キーを選択し、[Show License Details] をクリックします。

ステップ 3 （任意）フェールオーバーユニットで、そのユニットにインストールされている（プライマリ装置とセカンダリ装置からの結合ライセンスではない）ライセンスを [Running Licenses] 領域に表示するには、[Show information of license specifically purchased for this device alone] をクリックします。

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ーするには、[Monitoring] > [VPN] > [Clientless SSL VPN] > [Shared Licenses] を選択して。

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。 • 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 ユーザーの 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)	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 backup interface 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。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 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。
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)	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。 （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。

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)	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、ユーザー 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。 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準拠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。 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。
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セキュアクライアント 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。
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。

機能名	プラットフォームリリース	説明
Unified Communications Proxy セッション ライセンス	8.0(4)	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。 この機能は、バージョン 8.1 では使用できません。
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)	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。 （注） AnyConnect Essentials ライセンスを所有する VPN ユーザーは、Web ブラウザを使用してログインし、セキュアクライアント をダウンロードおよび起動（WebLaunch）できます。 このライセンスか AnyConnect Premium ライセンスでイネーブル化されたかに関係なく、セキュア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。 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。 デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [AnyConnect Essentials] ペインを使用すると、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。
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。

機能名	プラットフォームリリース	説明
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。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Activation Key]。
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カブルになりました。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。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Activation Key]。

機能名	プラットフォームリリース	説明
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。 次の画面が変更されました。[Configuration] > [Device Management] > [Licensing] > [Activation Key]。
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。
輸出用のペイロード暗号化なしイメージ	8.3(2)	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。 （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。
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	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。
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	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。
ASA 5580 および 5585-X での接続数の増加	8.4(1)	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。 • 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)	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。 （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。 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。
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。
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。

機能名	プラットフォームリリース	説明
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 を使用するときに VPN がサポートされるようになりました。
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す。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。

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

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

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