IPsec Usability Enhancements

IPsec Usability Enhancements 機能では、IPsec バーチャル プライベート ネットワーク（VPN）の設定およびモニタリングを簡単にする機能が導入されています。この機能の利点としては、IPsec およびインターネット キー交換（IKE）のインテリジェントなデフォルト、および IPsec VPN を簡単に確認およびトラブルシューティングできる機能などがあります。

IPsec Usability Enhancements の前提条件

- IPsec、IKE、および暗号化の知識が必要です。
- IPsec を設定し、ルータ上の IKE をイネーブルにしておく必要があります。
- ルータ上で Cisco IOS XE k9 暗号イメージを実行する必要があります。

IPsec Usability Enhancements に関する情報

IPsec の概要

IPsec は、インターネット技術特別調査委員会（IETF）によって開発されたオープン規格のフレームワークであり、パブリック ネットワークを介して機密性の高い情報を送信する際にセキュリティを確保します。IPsec はネットワーク層で機能し、Cisco ルータなどの参加している IPsec 装置（ピア）間の IP パケットを保護および認証します。

IPsec では、2 つのピア間におけるセキュアなトンネルが提供されます。機密性の高いパケットを定義し、そのパケットをこれらのセキュアなトンネルを介して送信されるように定義できます。また、トンネルの特性を指定することによって、このように機密性の高いパケットを保護するために使用されるパラメータを定義できます。IPsec ピアによってこのように機密性の高いパケットが検出されたら、そのピアによって、適切かつセキュアなトンネルが設定され、そのパケットがトンネルからリモート ピアに送信されます。

IPsec の動作

IPsec の動作は 5 つの基本的な手順で構成されています。対象となるトラフィックの識別、IKE フェーズ 1、IKE フェーズ 2、トンネルまたは IPsec セッションの確立、そして最後にトンネルの切断です。

ステップ 1：対象となるトラフィックの識別

VPN デバイスによって、検出対象のトラフィック、つまり機密性の高いパケットが認識されます。IPsec が機密性の高いパケットに適用されるか、パケットがバイパスされるか、または、パケットが廃棄されます。トラフィックのタイプに基づき、IPsec が適用されると、IKE フェーズ 1 が開始されます。

ステップ 2：IKE フェーズ 1

IKE セキュリティ ポリシーのネゴシエーションを行い、セキュアなチャネルを確立するために、VPN デバイス間で 3 回の交換が実行されます。

最初の交換の間、VPN デバイスによって、IKE 交換を保護するための IKE トランスフォーム セットのマッチングのネゴシエーションが行われ、その結果、使用する Internet Security Association and Key Management Protocol（ISAKMP）ポリシーが確立されます。ISAKMP ポリシーは、暗号化アルゴリズム、ハッシュ アルゴリズム、認証アルゴリズム、デフィーヘルマン（DH）グループ、およびライフタイム パラメータで構成されています。

8 種類のデフォルト ISAKMP ポリシーがサポートされています。デフォルト ISAKMP ポリシーの詳細については、IKE フェーズ 1 ISAKMP デフォルト ポリシーの確認 （3 ページ） を参照してください。

2 番目の交換は Diffie-Hellman 交換です。共有秘密が確立されます。

3 番目の交換では、ピアのアイデンティティが認証されます。ピアが認証されると、IKE フェーズ 2 が開始されます。

ステップ 3：IKE フェーズ 2

VPN デバイスによって、IPsec データの保護に使用される IPsec セキュリティ ポリシーのネゴシエーションが行われます。IPsec トランスフォーム セットがネゴシエートされます。

トランスフォーム セットは、ネットワーク トラフィックのセキュリティ ポリシーを制定するアルゴリズムおよびプロトコルの組み合わせです。デフォルト トランスフォーム セットの詳細については、デフォルト IPsec トランスフォーム セットの確認 （7 ページ）を参照してください。VPN トンネル確立の準備ができました。

ステップ 4：**Tunnel--IPsec の確立**

VPNデバイスによって、セキュリティ サービスがIPsec トラフィックに適用され、次に、IPsec データが送信されます。セキュリティアソシエーション（SA）がピア間で交換されます。IPsec セッションがアクティブの間、ネゴシエートされたセキュリティ サービスがトンネル トラフィックに適用されます。

ステップ 5：**トンネルの終了**

IPsecSAライフタイムのタイムアウトが発生するか、パケットカウンタが超過すると、トンネルが切断されます。IPsec SA が削除されます。

IPsec Usability Enhancements の活用方法

IKE フェーズ 1 ISAKMP デフォルト ポリシーの確認

IKEネゴシエーションが開始されると、ピアによって共通ポリシーの検出が試行され、検出はリモートピア上で指定された最も高いプライオリティを持つポリシーから開始されます。一致が存在するまで、ピアによって、ポリシーセットのネゴシエーションが行われます。各ピアに共通のポリシーセットが複数存在する場合、最も低いプライオリティを持つ番号が使用されます。

IKE フェーズ 1、ISAKMP、ポリシーのプライオリティの範囲および動作によって定義された各種ポリシーの 3 つのグループがあります。

- デフォルト ISAKMP ポリシー。自動的にイネーブルにされます。
- ユーザーISAKMP設定ポリシー。**crypto isakmp policy** コマンドを使用して設定できます。
- Easy VPN ISAKMP ポリシー。Easy VPN 設定中に使用可能にされます。

このセクションでは、ISAKMP ポリシーの 3 つのグループに関して、互いの関係の中での動作、使用中のポリシーを適切な **show** コマンドを使用して特定する方法、および、デフォルト ISAKMP ポリシーをディセーブルにする方法について説明します。

デフォルト IKE フェーズ 1 ポリシー

8 種類のデフォルト IKE フェーズ 1、ISAKMP、各種ポリシーがサポートされています（下表を参照）。自動的にイネーブルにされます。**crypto isakmp policy** コマンドを使用して IKE ポリシーを手動で設定していない場合、または **no crypto isakmp default policy** コマンドを使用してデフォルト IKE ポリシーを無効にしていない場合、ピア IKE ネゴシエーション中はデフォルトの IKE ポリシーが使用されます。**show crypto isakmp policy** コマンドまたは **show crypto isakmp default policy** コマンドのいずれかを発行して、デフォルトの IKE ポリシーが使用されていることを確認できます。

（注） セキュリティに対する脅威は、脅威からの保護に役立つ暗号化技術と同様に絶え間なく変化しています。最新のシスコの暗号化に関する推奨事項については、『Next Generation Encryption』（NGE）ホワイト ペーパーを参照してください。

デフォルト IKE ポリシーによって、次のポリシー セット パラメータが定義されます。

- プライオリティ、65507 ～ 65514。65507 が最も高いプライオリティで、65514 が最も低いプライオリティ。
- 認証方式、Rivest、Shamir、および Adelman（RSA）または事前共有キー（PSK）。
- 暗号方式、Advanced Encryption Standard（AES）または Triple Data Encryption Standard（3DES）。
- ハッシュ関数、Secure Hash Algorithm（SHA-1）または Message-Digest algorithm 5（MD5）。
- DH グループ仕様 DH2 または DH5。
  - DH2 では、768 ビット DH グループが指定されます。
  - DH5 では、1536 ビット DH グループが指定されます。

（注） 3DES、MD5、および DH グループ 1、2、5 の使用は推奨しません。シスコの最新の暗号化に関する推奨事項については、『Next Generation Encryption（NGE）』ホワイト ペーパーを参照してください。IKE 設定の詳細については、『*Internet Key Exchange for IPsec VPNs Configuration Guide*』の「Configuring Internet Key Exchange for IPsec VPNs」の章を参照してください。

表 *1*: デフォルト *IKE* フェーズ *1*、*ISAKMP*、ポリシー

プライオリティ	認証	暗号化	ハッシュ	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

ユーザ設定 IKE ポリシー

crypto isakmp policy コマンドを使用して、IKE ポリシーを設定できます。ユーザ設定 IKE ポリシーは一意に識別され、1 ～ 10000 の範囲のプライオリティ番号が使用されて設定されます。1 が最も高いプライオリティで、10000 は最も低いプライオリティです。

1 ～ 10000 のプライオリティを持つ 1 つ以上の IKE ポリシーを設定した結果は次のとおりです。

- ピア IKE ネゴシエーション中にユーザ設定ポリシーが使用されます。
- ピア IKE ネゴシエーション中にデフォルト IKE ポリシーが使用されます。
- **show crypto isakmp policy** コマンドを発行することによって、ユーザー設定ポリシーを表示できます。

Easy VPN ISAKMP ポリシー

Easy VPN を設定した場合、使用中のデフォルト Easy VPN ISAKMP ポリシーは、65515 ～ 65535 の範囲のプライオリティ番号で一意に識別されます。65515 が最も高いプライオリティで、65535 は最も低いプライオリティです。

ユーザが Easy VPN を設定した結果は次のとおりです。

- ピア Easy VPN ISAKMP ネゴシエーション中に、デフォルト EzVPN ISAKMP ポリシーおよびデフォルト IKE ポリシーが使用されます。
- **show crypto isakmp policy** コマンドを発行することによって、Easy VPN ISAKMP ポリシーおよびデフォルト IKE ポリシーを表示できます。
- デフォルト ISAKMP ポリシーは、**no crypto isakmp default policy** コマンドを発行して無効にしない限り、**show crypto isakmp default policy** コマンドを発行すると表示されます。

手順の概要

1. **enable**
2. **show crypto isakmp default policy**
3. **configure terminal**
4. **no crypto isakmp default policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**show crypto isakmp default policy** 例： `Router# show crypto isakmp default policy`	（任意）1 ～ 10000 のプライオリティを持つポリシーが設定されていない場合、デフォルト ISAKMP ポリシーを表示します。
ステップ 3	**configure terminal** 例： `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 4	**no crypto isakmp default policy** 例： `Router(config)# no crypto isakmp default policy`	（任意）65507 ～ 65514 のプライオリティを持つデフォルト ISAKMP ポリシーをオフにします。

例

次に、**show crypto isakmp default policy** コマンドの出力例を示します。デフォルト ポリシーがディセーブルにされていないので、デフォルト ポリシーが表示されています。

```
Router# show crypto isakmp default policy

Default IKE policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
```

```
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

次に、デフォルト IKE ポリシーがディセーブルにされてからの、**show crypto isakmp default policy** コマンドの出力結果の例を示します。ここでは、結果は空白になっています。

```
Router# configure terminal
Router(config)# no crypto isakmp default policy
Router(config)# exit
Router# show crypto isakmp default policy
Router#
!There is no output since the default IKE policies have been disabled.
```

次に、デフォルトISAKMPポリシーが使用中の時はいつでも生成されるシステム ログ メッセージの例を示します。

```
%CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

デフォルト IPsec トランスフォーム セットの確認

トランスフォーム セットは、特定のセキュリティ プロトコルとアルゴリズムを組み合わせたものです。IPsec SA のネゴシエーション中に、ピアは、特定のトランスフォームセットを使用して特定のデータ フローを保護することに合意します。

IKE とのIPsec SA のネゴシエーション中に、ピアは両方のピア上で同じトランスフォーム セットを検索します。同一のトランスフォーム セットが検出された場合、そのトランスフォーム セットが選択され、両方のピアのIPsec SA の一部として、保護するトラフィックに適用されます。

デフォルト トランスフォーム セット

他のトランスフォームセットが設定されておらず、次の条件が満たされている場合、1 つのデフォルト トランスフォームセットがすべてのクリプトマップまたはIPsecプロファイルによって使用されます。

- デフォルト トランスフォーム セットが **no crypto ipsec default transform-set** コマンドによって無効にされていない。
- 使用中の暗号化エンジンで、暗号化アルゴリズムがサポートされている。

下図に示すとおり、2 つのデフォルト トランスフォーム セットのそれぞれによって、Encapsulation Security Protocol（ESP）暗号化トランスフォーム タイプおよび ESP 認証トランスフォーム タイプが定義されます。

表 *2:* デフォルト トランスフォーム セットおよびパラメータ

デフォルト トランスフォーム名	**ESP** 暗号化トランスフォームおよび説明	**ESP** 認証トランスフォームおよび説明
#$!default_transform_set_0	esp-3des （168 ビット 3DES またはトリプル DES 暗号化アルゴリズムを持つ EDP）	esp-sha-hmac
#$!default_transform_set_1	esp-aes （128 ビット AES 暗号化アルゴリズムを持つ ESP）	esp-sha-hmac （SHA-1、ハッシュ メッセージ認証コード [HMAC] バリアント認証アルゴリズムを持つ ESP）

手順の概要

1. **enable**
2. **show crypto ipsec default transform-set**
3. **configure terminal**
4. **no crypto ipsec default transform-set**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show crypto ipsec default transform-set** 例： `Router# show crypto ipsec default transform-set`	（任意）IKE によって現在使用中のデフォルト IPsec トランスフォーム セットを表示します。
ステップ 3	**configure terminal** 例：	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Router# configure terminal`	
ステップ 4	**no crypto ipsec default transform-set** 例： `Router(config)# no crypto ipsec default transform-set`	（任意）デフォルト IPsec トランスフォーム セットを表示します。

例

```
The following example displays output from the show crypto ipsec default transform-set
 command when the default transform sets are enabled, the default setting:
Router# show crypto ipsec default transform-set
Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

次に、**no crypto ipsec default transform-set** コマンドを使用してデフォルト トランスフォーム セットを無効にした場合の、**show crypto ipsec default transform-set** コマンドの出力例を示します。

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set
! There is no output.
Router#
```

次に、IPsec SA がデフォルト トランスフォーム セットでネゴシエーションを行った時はいつでも生成されるシステム ログ メッセージ例を示します。

```
%CRYPTO-5-IPSEC_DEFAULT_TRANSFORM: Using Default IPsec transform-set
```

IPsec VPN 確認および IPsec VPN のトラブルシューティング

IKE フェーズ 1 または IKE フェーズ 2 を確認したいのか、または IPsec VPN のトラブルシューティングを行いたいのかによって、この項における次の任意の作業のいずれかを実行します。

IKE フェーズ 1 ISAKMP の確認

ISAKMP トンネルの統計情報を表示するには、次のオプション コマンドを使用します。

手順の概要

1. **show crypto mib isakmp flowmib failure [vrf** *vrf-name* **]**
2. **show crypto mib isakmp flowmib global [vrf** *vrf-name* **]**

3. **show crypto mib isakmp flowmib history [vrf** *vrf-name* **]**
4. **show crypto mib isakmp flowmib peer [index** *peer-mib-index* **] [vrf** *vrf-name* **]**
5. **show crypto mib isakmp flowmib tunnel [index** *tunnel-mib-index* **] [vrf** *vrf-name* **]**

手順の詳細

ステップ 1 show crypto mib isakmp flowmib failure [vrf *vrf-name*]

ISAKMP トンネルにエラーが発生した場合、このコマンドでイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib failure
 vrf Global
  Index:                       1
  Reason:                      peer lost
  Failure time since reset:    00:07:27
  Local type:                  ID_IPV4_ADDR
  Local value:                192.0.2.1
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.2.2
  Local Address:               192.0.2.1
  Remote Address:              192.0.2.2
  Index:                       2
  Reason:                      peer lost
  Failure time since reset:    00:07:27
  Local type:                  ID_IPV4_ADDR
  Local value:                192.0.3.1
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.3.2
  Local Address:               192.0.3.1
  Remote Address:              192.0.3.2
  Index:                       3
  Reason:                      peer lost
  Failure time since reset:    00:07:32
  Local type:                  ID_IPV4_ADDR
  Remote type:                 ID_IPV4_ADDR
  Remote Value:                192.0.2.2
  Local Address:               192.0.2.1
  Remote Address:              192.0.2.2
```

ステップ 2 show crypto mib isakmp flowmib global [vrf *vrf-name*]

このコマンドを発行することによって、グローバル ISAKMP トンネル統計情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib global
vrf Global
  Active Tunnels:                          3
  Previous Tunnels:                        0
  In octets:                               2856
  Out octets:                              3396
  In packets:                              16
  Out packets:                             19
  In packets drop:                         0
```

```
  Out packets drop:                       0
  In notifys:                             4
  Out notifys:                            7
  In P2 exchg:                            3
  Out P2 exchg:                           6
  In P2 exchg invalids:                   0
  Out P2 exchg invalids:                  0
  In P2 exchg rejects:                    0
  Out P2 exchg rejects:                   0
  In IPSEC delete:                        0
  Out IPSEC delete:                       0
  SAs locally initiated:                  3
  SAs locally initiated failed:           0
  SAs remotely initiated failed:          0
  System capacity failures:               0
  Authentication failures:                0
  Decrypt failures:                       0
  Hash failures:                          0
  Invalid SPI:                            0
```

ステップ 3 **show crypto mib isakmp flowmib history [vrf** *vrf-name* **]**

アクティブにならない ISAKMP トンネルの情報については、このコマンドによって、トンネルが終了した原因を含むイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib history
vrf Global
  Reason:                             peer lost
  Index:                              2
  Local type:                         ID_IPV4_ADDR
  Local address:                      192.0.2.1
  Remote type:                        ID_IPV4_ADDR
  Remote address:                     192.0.2.2
  Negotiation mode:                   Main Mode
  Diffie Hellman Grp:                 2
  Encryption algo:                    des
  Hash algo:                          sha
  Auth method:                        psk
  Lifetime:                           86400
  Active time:                        00:06:30
  Policy priority:                    1
  Keepalive enabled:                  Yes
  In octets:                          3024
  In packets:                         22
  In drops:                           0
  In notifys:                         18
  In P2 exchanges:                    1
  In P2 exchg invalids:               0
  In P2 exchg rejected:                 0
  In P2 SA delete reqs:                 0
  Out octets:                           4188
  Out packets:                          33
  Out drops:                            0
  Out notifys:                          28
  Out P2 exchgs:                        2
  Out P2 exchg invalids:                0
  Out P2 exchg rejects:                 0
  Out P2 Sa delete requests:            0
  Reason:                               peer lost
  Index:                                3
  Local type:                           ID_IPV4_ADDR
```

```
  Local address:                        192.0.3.1
  Remote type:                          ID_IPV4_ADDR
  Remote address:                       192.0.3.2
  Negotiation mode:                     Main Mode
  Diffie Hellman Grp:                   2
  Encryption algo:                      des
  Hash algo:                            sha
  Auth method:                          psk
  Lifetime:                             86400
  Active time:                          00:06:25
  Policy priority:                      1
  Keepalive enabled:                    Yes
  In octets:                            3140
  In packets:                           23
  In drops:                             0
  In notifys:                           19
  In P2 exchanges:                      1
  In P2 exchg invalids:                 0
  In P2 exchg rejected:                 0
  In P2 SA delete reqs:                 0
  Out octets:                           4304
  Out packets:                          34
  Out drops:                            0
  Out notifys:                          29
  Out P2 exchgs:                        2
  Out P2 exchg invalids:                0
  Out P2 exchg rejects:                 0
  Out P2 Sa delete requests:            0
```

ステップ 4 **show crypto mib isakmp flowmib peer [index** *peer-mib-index* **] [vrf** *vrf-name* **]**

アクティブな ISAKMP ピアアソシエーションについては、このコマンドによって、インデックス、接続タイプ、および IP アドレスを含む情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib peer
vrf Global
  Index:              1
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.2.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.2.2
  Index:              2
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.3.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.3.1
  Index:              3
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.4.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.4.1
```

ステップ 5 **show crypto mib isakmp flowmib tunnel [index** *tunnel-mib-index* **] [vrf** *vrf-name* **]**

アクティブな ISAKMP トンネルについては、このコマンドによって、トンネルの統計情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib isakmp flowmib tunnel
```

```
vrf Global
  Index:                        1
  Local type:                   ID_IPV4_ADDR
  Local address:                192.0.2.1
  Remote type:                  ID_IPV4_ADDR
  Remote address:               192.0.2.2
  Negotiation mode:             Main Mode
  Diffie Hellman Grp:           2
  Encryption algo:              des
  Hash algo:                    sha
  Auth method:                  psk
  Lifetime:                     86400
  Active time:                  00:03:08
  Policy priority:              1
  Keepalive enabled:            Yes
  In octets:                    2148
  In packets:                   15
  In drops:                     0
  In notifys:                   11
  In P2 exchanges:              1
  In P2 exchg invalids:         0
  In P2 exchg rejected:         0
  In P2 SA delete reqs:         0
  Out octets:                   2328
  Out packets:                  16
  Out drops:                    0
  Out notifys:                  12
  Out P2 exchgs:                2
  Out P2 exchg invalids:        0
  Out P2 exchg rejects:         0
  Out P2 Sa delete requests:    0
```

IKE フェーズ 2 の確認

IPsec フェーズ 2 トンネルの統計情報を表示するには、次のオプション コマンドを使用します。

手順の概要

1. **show crypto mib ipsec flowmib endpoint [vrf** *vrf-name* **]**
2. **show crypto mib ipsec flowmib failure [vrf** *vrf-name* **]**
3. **show crypto mib ipsec flowmib global [vrf** *vrf-name* **]**
4. **show crypto mib ipsec flowmib history [vrf** *vrf-name* **]**
5. **show crypto mib ipsec flowmib spi [vrf** *vrf-name* **]**
6. **show crypto mib ipsec flowmib tunnel** [**index** *tunnel-mib-index*] **[vrf** *vrf-name* **]**

手順の詳細

ステップ 1 **show crypto mib ipsec flowmib endpoint [vrf** *vrf-name* **]**

このコマンドを発行することによって、IPsec フェーズ 2 トンネルに関連付けられた、各アクティブ エンドポイント、ローカルまたはリモート デバイスの情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router#  show crypto mib ipsec flowmib endpoint
vrf Global
  Index:               1
  Local type:          Single IP address
  Local address:       192.1.2.1
  Protocol:            0
  Local port:          0
  Remote type:         Single IP address
  Remote address:      192.1.2.2
  Remote port:         0
  Index:               2
  Local type:          Subnet
  Local address:       192.1.3.0 255.255.255.0
  Protocol:            0
  Local port:          0
  Remote type:         Subnet
  Remote address:      192.1.3.0 255.255.255.0
  Remote port:         0
```

ステップ 2 **show crypto mib ipsec flowmib failure [vrf** *vrf-name* **]**

ISAKMP トンネルにエラーが発生した場合、このコマンドでイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib failure
vrf Global
  Index:                       1
  Reason:                      Operation request
  Failure time since reset:    00:25:18
  Src address:                 192.1.2.1
  Destination address:         192.1.2.2
  SPI:                         0
```

ステップ 3 **show crypto mib ipsec flowmib global [vrf** *vrf-name* **]**

このコマンドを発行することによって、グローバル IKE フェーズ 2 トンネルの統計情報が表示されます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib global
 vrf Global
  Active Tunnels:                   2
  Previous Tunnels:                 0
  In octets:                        800
  Out octets:                       1408
  In packets:                       8
  Out packets:                      8
  Uncompressed encrypted bytes:    1408
  In packets drops:                 0
  Out packets drops:                2
  In replay drops:                  0
  In authentications:               8
  Out authentications:              8
  In decrypts:                      8
  Out encrypts:                     8
  Compressed bytes:                 0
  Uncompressed bytes:               0
  In uncompressed bytes:            0
```

```
  Out uncompressed bytes:             0
  In decrypt failures:                0
  Out encrypt failures:               0
  No SA failures:                     0
! Number of SA Failures.
  Protocol use failures:              0
  System capacity failures:           0
  In authentication failures:         0
  Out authentication failures:        0
```

ステップ 4 **show crypto mib ipsec flowmib history [vrf** *vrf-name* **]**

アクティブにならない IKE フェーズ 2 トンネルの情報については、このコマンドによって、トンネルが終了した原因を含むイベント情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib history
vrf Global
  Reason:                       Operation request
  Index:                        1
  Local address:                192.1.2.1
  Remote address:               192.1.2.2
  IPSEC keying:                 IKE
  Encapsulation mode:           1
  Lifetime (KB):                4608000
  Lifetime (Sec):               3600
  Active time:                  00:24:32
  Lifetime threshold (KB):      423559168
  Lifetime threshold (Sec):     3590000
  Total number of refreshes:    0
  Expired SA instances:         4
  Current SA instances:         4
  In SA DH group:               14
  In sa encrypt algorithm       aes
  In SA auth algorithm:         rsig
  In SA ESP auth algo:          ESP_HMAC_SHA
  In SA uncompress algorithm:   None
  Out SA DH group:              14
  Out SA encryption algorithm:  aes
  Out SA auth algorithm:        ESP_HMAC_SHA
  Out SA ESP auth algorithm:    ESP_HMAC_SHA
  Out SA uncompress algorithm:  None
  In octets:                    400
  Decompressed octets:          400
  In packets:                   4
  In drops:                         0
  In replay drops:                  0
  In authentications:               4
  In authentication failures:       0
  In decrypts:                      4
  In decrypt failures:              0
  Out octets:                       704
  Out uncompressed octets:          704
  Out packets:                      4
  Out drops:                        1
  Out authentications:              4
  Out authentication failures:      0
  Out encryptions:                  4
  Out encryption failures:          0
  Compressed octets:                0
  Decompressed octets:              0
  Out uncompressed octets:          704
```

ステップ 5 **show crypto mib ipsec flowmib spi [vrf** *vrf-name* **]**

security protection index（SPI）テーブルには、アクティブおよび期限切れの各セキュリティ IKE フェーズ 2 アソシエーションのエントリが格納されます。次に、このコマンドのサンプル出力を示します。SPI テーブルが表示されています。

例：

```
Router# show crypto mib ipsec flowmib spi
vrf Global
  Tunnel Index:          1
  SPI Index:            1
  SPI Value:            0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            2
  SPI Value:            0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            3
  SPI Value:            0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active
  SPI Index:            4
  SPI Value:            0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

ステップ 6 **show crypto mib ipsec flowmib tunnel** [**index** *tunnel-mib-index*] **[vrf** *vrf-name* **]**

アクティブな IKE フェーズ 2 トンネルについては、このコマンドによって、トンネルの統計情報を表示できます。次に、このコマンドのサンプル出力を示します。

例：

```
Router# show crypto mib ipsec flowmib tunnel
vrf Global
  Index:                              1
  Local address:                      192.0.2.1
  Remote address:                     192.0.2.2
  IPSEC keying:                       IKE
  Encapsulation mode:                 1
  Lifetime (KB):                      4608000
  Lifetime (Sec):                     3600
  Active time:                        00:05:46
  Lifetime threshold (KB):            64
  Lifetime threshold (Sec):           10
  Total number of refreshes:          0
  Expired SA instances:               0
  Current SA instances:               4
  In SA DH group:                     14
  In sa encrypt algorithm:            aes
  In SA auth algorithm:               rsig
  In SA ESP auth algo:                ESP_HMAC_SHA
  In SA uncompress algorithm:         None
  Out SA DH group:                    14
  Out SA encryption algorithm:        aes
```

```
Out SA auth algorithm:              ESP_HMAC_SHA
Out SA ESP auth algorithm:          ESP_HMAC_SHA
Out SA uncompress algorithm:        None
In octets:                             400
Decompressed octets:                   400
In packets:                            4
In drops:                              0
In replay drops:                       0
In authentications:                    4
In authentication failures:            0
In decrypts:                           4
In decrypt failures:                   0
Out octets:                            704
Out uncompressed octets:               704
Out packets:                           4
Out drops:                             1
Out authentications:                   4
Out authentication failures:           0
Out encryptions:                       4
Out encryption failures:               0
Compressed octets:                     0
Decompressed octets:                   0
Out uncompressed octets:               704
```

IPsec VPN のトラブルシューティング

問題のトラブルシューティングを行う場合、**show tech-support ipsec** コマンドを使用すれば、IPsec 関連情報の収集が簡単にできます。

手順の概要

1. **show tech-support ipsec**

手順の詳細

show tech-support ipsec

show tech-support ipsec コマンドには、次の 3 つのバリエーションがあります。

- **show tech-support ipsec**
- **show tech-support ipsec peer** *ipv4address*
- **show tech-support ipsec vrf** *vrf-name*

各バリエーションについて次に示す個々の **show** コマンドに関する **show tech-support ipsec** コマンドからの出力のサンプル表示については、以下のセクションを参照してください。

show tech-support ipsec コマンドの出力

キーワードを何も指定しないで **show tech-support ipsec** コマンドを入力すると、コマンドの出力には、次の **show** コマンドが出力順に表示されます。

- **show version**

- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

show tech-support ipsec peer コマンドの出力

peer キーワードと *ipv4address* 引数を指定して **show tech-support ipsec** コマンドを入力すると、出力に次の **show** コマンドが、指定したピアの出力順に表示されます。

- **show version**
- **show running-config**
- **show crypto session remote** *ipv4address* **detail**
- **show crypto isakmp sa peer** *ipv4address* **detail**
- **show crypto ipsec sa peer** *ipv4address* **detail**
- **show crypto isakmp peers** *ipv4address*
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

show tech-support ipsec vrf コマンドの出力

vrf キーワードと *vrf-name* 引数を指定して **show tech-support ipsec** コマンドを入力すると、出力に次の **show** コマンドが、指定した Virtual Routing and Forwarding（VRF）の出力順に表示されます。

- **show version**
- **show running-config**

- **show crypto isakmp sa count vrf** *vrf-name*
- **show crypto ipsec sa count vrf** *vrf-name*
- **show crypto session ivrf** *ivrf-name* **detail**
- **show crypto session fvrf** *fvrf-name* **detail**
- **show crypto isakmp sa vrf** *vrf-name* **detail**
- **show crypto ipsec sa vrf** *vrf-name* **detail**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**
- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

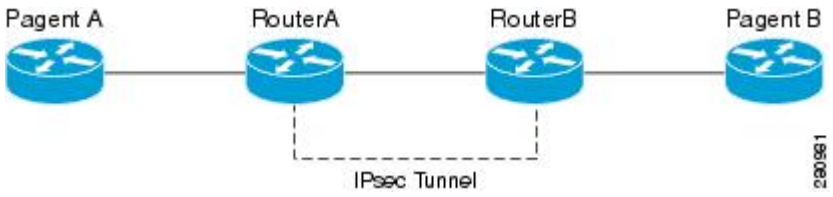
例：

IPsec Usability Enhancements の設定例

IKE デフォルト ポリシーの例

次に、クリプト マップが RouterA および RouterB 上で設定されており、デフォルト IKE ポリシーが使用中になっている例を示します。トラフィックは Pagent A から Pagent B にルーティングされます。Peer A および Peer B のシステム ログをチェックすると、デフォルトの IKE ポリシーが両方のピアで使用中であることを確認できます（下図を参照）。

図 *1:* サイトツーサイト トポロジーの例




```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identity address 209.165.200.226
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.226
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
```

```
RouterA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.226
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.225
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterA(cfg-crypto-trans)# mode tunnel
RouterA(cfg-crypto-trans)# end
RouterA(config)# crypto map testmap 10
RouterA(config-crypto-map)# set transform-set test_transf
RouterA(config-crypto-map)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.228
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.228
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto ipsec transform test_transf esp-aes esp-sha-hmac
RouterB(cfg-crypto-trans)# mode tunnel
RouterB(cfg-crypto-trans)# end
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# set transform-set test_transf
RouterB(config-crypto-map)# end
! Routing traffic from PagentA to PagentB.
PagentA(config)# ip route 209.165.200.225 255.255.255.224 209.165.200.229
PagentA(config)# end
! Routing traffic from PagentB to PagentA.
PagentB(config)# ip route 209.165.200.227 255.255.255.224 209.165.200.230
PagentB(config)# end
! Checking the system log on RouterA confirms that the default IKE policies are in use.
RouterA# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun  5 09:17:59.251 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
! Checking the system log on RouterB confirms that the default IKE policies are in use.
RouterB# show log | include %CRYPTO-6-IKMP_POLICY_DEFAULT*
Jun  5 09:17:59.979 PDT: %CRYPTO-6-IKMP_POLICY_DEFAULT: Using ISAKMP Default policies
```

デフォルト トランスフォーム セットの例

次に、スタティック クリプト マップが RouterA 上で設定され、ダイナミック クリプト マップが RouterB 上で設定されている例を示します。トラフィックは Pagent A から Pagent B にルーティングされます。IPsec SA はデフォルト トランスフォーム セットとネゴシエーションを行い、トラフィックは暗号化されます。両方のピアで **show crypto map** コマンドを実行すると、デフォルト トランスフォーム セットが使用中であることを確認できます。

```
! Configuring RouterA.
RouterA(config)# crypto isakmp key identify address 209.165.200.225
RouterA(config)# crypto map testmap 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
 and a valid access list have been configured.
RouterA(config-crypto-map)# set peer 209.165.200.225
RouterA(config-crypto-map)# match address 101
RouterA(config-crypto-map)# exit
RouterA(config)# ip route 209.165.200.226 255.255.255.255 209.165.200.225
RouterA(config)# access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
```

```
RouterA(config)# end
RouterA(config)# interface FastEthernet1/2
RouterA(config-if)# crypto map testmap
RouterA(config-if)# end
RouterA(config)# crypto isakmp policy 10
RouterA(config-isakmp)# encryption aes
RouterA(config-isakmp)# authentication pre-share
RouterA(config-isakmp)# hash sha
RouterA(config-isakmp)# group 5
RouterA(config-isakmp)# end
! Configuring RouterB.
RouterB(config)# crypto isakmp key identity address 209.165.200.229
RouterB(config)# crypto dynamic-map dyn_testmap 10
RouterB(config-crypto-map)# crypto map testmap 10 ipsec-isakmp dynamic dyn_testmap
RouterB(config)# ip route 209.165.200.227 255.255.255.255 209.165.200.229
RouterB(config)# end
RouterB(config)# interface GigabitEthernet0/1
RouterB(config-if)# crypto map testmap
RouterB(config-if)# end
RouterB(config)# crypto isakmp policy 10
RouterB(config-isakmp)# encryption aes
RouterB(config-isakmp)# authentication pre-share
RouterB(config-isakmp)# hash sha
RouterB(config-isakmp)# group 5
RouterB(config-isakmp)# end
! The SA is using the default transform set and traffic is encrypted on RouterA.
RouterA# show crypto isakmp sa detail | include 209.165.200.229.*209.165.200.225.*ACTIVE
13007  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  23:59:56
13006  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  0
13005  209.165.200.229     209.165.200.225     ACTIVE aes  sha  psk  5  0
! The SA is using the default transform set and traffic is encrypted on RouterB.
RouterB# show crypto isakmp sa detail | include 209.165.200.225.*209.165.200.229.*ACTIVE
7007  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  23:59:55
7006  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  0
7005  209.165.200.225      209.165.200.229      ACTIVE aes  sha  psk  5  0
! Verifying that the default transform sets are in use on RouterA.
RouterA# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
 Peer = 209.165.200.225
 Extended IP access list 101
     access-list 101 permit ip host 209.165.200.227 host 209.165.200.226
 Current peer: 209.165.200.225
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
  #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
  #$!default_transform_set_0:  { esp-3des esp-sha-hmac  } ,
 }
 Interfaces using crypto map testmap:
  FastEthernet1/2
! Verifying that the default transform sets are in use on RouterB.
RouterB# show crypto map
Crypto Map "testmap" 10 ipsec-isakmp
 Dynamic map template tag: dyn_testmap
Crypto Map "testmap" 65536 ipsec-isakmp
 Peer = 209.165.200.229
 Extended IP access list
     access-list permit ip host 209.165.200.226 host 209.165.200.227
     dynamic (created from dynamic map dyn_testmap/10)
 Current peer: 209.165.200.229
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets={
```

```
 #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
}
Interfaces using crypto map testmap:
 GigabitEthernet0/1
```

その他の参考資料

次の項では、IPsec Usability Enhancement 機能の関連資料を示します。

関連資料

関連項目	マニュアル タイトル
IKE 設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Internet Key Exchange for IPsec VPNs」モジュール
IPsec の設定	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Configuring Security for VPNs with IPsec」モジュール
Easy VPN サーバ	『*Cisco IOS XE Security Configuration Guide: Secure Connectivity*』の「Easy VPN Server」モジュール
Cisco IOS XE セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE リリース、およびフィーチャ セットの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec Usability Enhancements の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *3 : IPsec Usability Enhancements* の機能情報

機能名	リリース	機能情報
IPsec Usability Enhancements	Cisco IOS XE Release 2.4	この機能では、IKE および IPsec のインテリジェントなデフォルト、および、MIB 統計情報にアクセスするためおよびトラブルシューティングを支援するための各種**show**コマンドが導入されています。 次のコマンドが導入または変更されました。**crypto ipsec default transform-set**、**crypto isakmp default policy**、**crypto isakmp policy**、**show crypto ipsec default transform-set**、**show crypto ipsec transform-set**、**show crypto isakmp default policy**、**show crypto isakmp policy**、**show crypto map (IPsec)**、**show crypto mib ipsec flowmib endpoint**、**show crypto mib ipsec flowmib failure**、**show crypto mib ipsec flowmib global**、**show crypto mib ipsec flowmib history**、**show crypto mib ipsec flowmib spi**、**show crypto mib ipsec flowmib tunnel**、**show crypto mib isakmp flowmib failure**、**show crypto mib isakmp flowmib global**、**show crypto mib isakmp flowmib history**、**show crypto mib isakmp flowmib peer**、**show crypto mib isakmp flowmib tunnel**、**show tech-support ipsec**。

用語集

ピア：ここでのピアとは、IPsec に参加するルータまたはその他の装置です。

SA：セキュリティ アソシエーション。2 つ以上のエンティティが、特定のデータ フローにおいて安全に通信するために、特定のセキュリティ プロトコル（AH または ESP）と関連してセキュリティ サービスを使用する方法を記述します。トラフィックを保護するために、トランスフォームと共有秘密キーが使用されます。

トランスフォーム：データ認証、データ機密性、およびデータ圧縮を実現するためにデータ フローで実行される処理のリスト。たとえば、トランスフォームには、HMAC MD5 認証アルゴリズムを使用する ESP プロトコル、56 ビット DES 暗号規格アルゴリズムを使用する AH プロトコルおよび HMAC-SHA 認証アルゴリズムを使用する ESP プロトコルなどがあります。

トンネル：ここで使用するトンネルとは、2 つのピア間（2 台のルータなど）の安全な通信パスです。トンネル モードで IPsec を使用することではありません。

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。