証明書/ISAKMP プロファイルマッピング

証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに Internet Security Association and Key Management Protocol（ISAKMP）プロファイルを割り当てることができます。また、この機能では、ISAKMP プロファイルに割り当てられたピアにグループ名を割り当てることもできます。

証明書/ISAKMP プロファイルマッピングの前提条件

- 証明書マップの設定を理解している必要があります。
- ISAKMP プロファイルの設定を理解している必要があります。

証明書/ISAKMP プロファイルマッピングの制約事項

証明書を交換しないで、Rivest、Shamir、Adelman（RSA）シグニチャまたは RSA 暗号化認証を使用する場合は、この機能を適用できません。ISAKMP ピアは、証明書を使用して RSA シグニチャまたは RSA 暗号化認証を実行するように設定する必要があります。

同じ認証局（CA）サーバに登録された 2 つのトラストポイントを使用する IPsec はサポートされません。2 つ以上の ISAKMP プロファイルがあり、各プロファイルが、同じ CA サーバに登録されているが異なるトラストポイントを持っている場合、応答側は最後のグローバル トラストポイントを選択します（トラストポイントは、グローバルに定義された順序と逆の順序で選択されます）。ピアが IPsec トンネルの確立を成功させるには、発信側が選択したトラストポ

イントは、応答側が選択したトラストポイントと一致する必要があります。トラストポイントが一致しない場合、他のすべての IPsec トンネルは、接続の確立に失敗します。

証明書/ISAKMP プロファイルマッピングに関する情報

証明書/ISAKMP プロファイルマッピングの概要

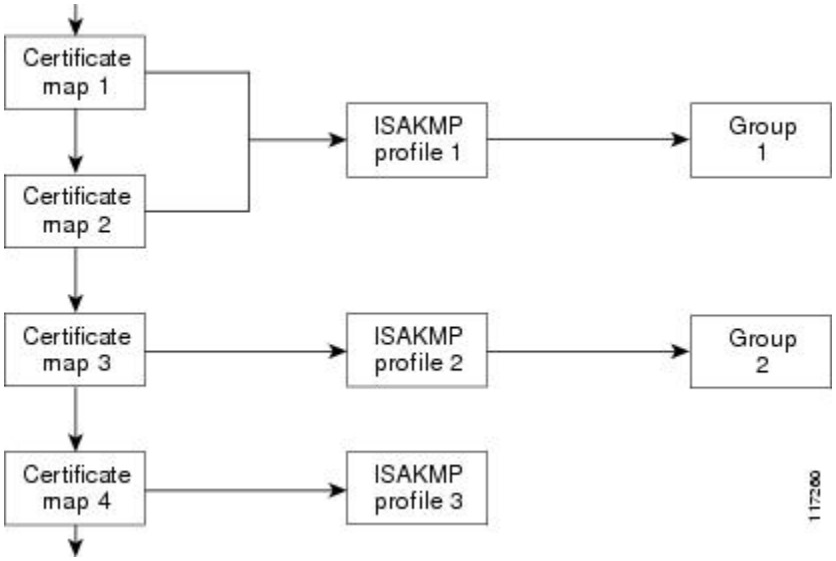
Cisco IOS Release12.3(8)T 以前では、ピアを ISAKMP プロファイルにマッピングする方法は、次の方法だけでした。ISAKMP 交換の ISAKMP ID フィールドは、ピアを ISAKMP プロファイルにマッピングするために使用されていました。証明書が認証に使用されるとき、ISAKMP ID ペイロードに証明書からの所有者名が含まれていました。CA が、要求されたグループ値を証明書の最初の組織ユニット（OU）フィールドに表示しなかった場合、ISAKMP プロファイルをピアに割り当てることはできませんでした。

Cisco IOS Release 12.3(8)T でも、上記のように、ピアをマッピングできます。証明書/ISAKMP プロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアに ISAKMP プロファイルを割り当てることができます。以前は、証明書の所有者名に基づいて ISAKMP プロファイルを割り当てるという方法しかありませんでした。また、この機能により、ISAKMP プロファイルが割り当てられたピアにグループを割り当てることができます。

証明書/ISAKMP プロファイルマッピングのしくみ

次の図に、証明書マップを ISAKMP プロファイルに接続し、証明書マップにグループ名を割り当てる方法を示します。

図 *1:* プロファイル グループ割り当てにマッピングされる証明書マップ



ISAKMP プロファイルには複数の証明書マップを接続できますが、証明書マップは 1 つの ISAKMP プロファイルにしか接続できません。

証明書マップにより、証明書を指定の一連の基準と照合できるようになります。ISAKMP プロファイルは、自身を証明書マップにバインドできます。また、提示された証明書が ISAKMP プロファイル内に存在する証明書マップと一致した場合、ピアに ISAKMP プロファイルが割り当てられます。ISAKMP プロファイルにクライアント設定グループ名が含まれている場合、同じグループ名がピアに割り当てられます。この ISAKMP プロファイル情報により、ID_KEY_ID アイデンティティまたは証明書の最初の OU フィールドの情報が上書きされます。

ピアへの ISAKMP プロファイルおよびグループ名の割り当て

証明書内の任意のフィールドに基づいて、ピアに ISAKMP プロファイルを割り当てるには、ISAKMP プロファイルを定義してから、**match certificate** コマンドを使用します。

ピアに割り当てられる ISAKMP プロファイルにグループ名を関連付けるのは、同様に ISAKMP プロファイルを定義してから、**client configuration group** コマンドを使用します。

証明書/ISAKMP プロファイルマッピングの設定方法

証明書/ISAKMP プロファイル マッピング

ISAKMP プロファイルに証明書をマッピングするには、次の手順を実行します。この設定により、証明書内の任意のフィールドの内容に基づいて、ピアに ISAKMP プロファイルを割り当てることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **match certificate** *certificate-map*

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	**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 3	**crypto isakmp profile** *profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	ISAKMP プロファイルを定義し、暗号 ISAKMP プロファイル 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	**match certificate** *certificate-map* 例： `Router (conf-isa-prof)# match certificate map1`	証明書マップの名前を受け入れます。

証明書がマッピングされたことの確認

次の **show** コマンドを使って、証明書マップの所有者名が正しく設定されているか確認できます。

手順の概要

1. **enable**
2. **show crypto ca certificates**

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 ca certificates** 例： `Router# show crypto ca certificates`	証明書に関する情報を表示します。

ピアへのグループ名の割り当て

ピアを ISAKMP プロファイルにマッピングするときにグループ名をピアに関連付けるには、次の手順を実行します。

手順の概要

1. **enable**

2. **configure terminal**
3. **crypto isakmp profile** *profile-name*
4. **client configuration group** *group-name*

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	**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 3	**crypto isakmp profile** *profile-name* 例： `Router (config)# crypto isakmp profile vpnprofile`	ISAKMP プロファイルを定義し、ISAKMP プロファイル 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	**client configuration group** *group-name* 例： `Router (conf-isa-prof)# client configuration group group1`	この暗号 ISAKMP プロファイルにピアを割り当てるときに、そのピアに割り当てられるグループ名を受け入れます。

証明書/ISAKMP プロファイルマッピングのモニタおよびメンテナンス

ISAKMP プロファイルマッピングに対応する証明書をモニターしメンテナンスするには、次の **debug** コマンドを使用します。

手順の概要

1. **enable**
2. **debug crypto isakmp**

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	**debug crypto isakmp** 例： `Router# debug crypto isakmp`	証明書が、証明書マップの照合を経て、ISAKMP プロファイルと一致することを示す出力を表示します。 このコマンドは、ピアにグループが割り当てられたことを確認する場合にも使用できます。

証明書/ISAKMP プロファイルマッピングの設定例

任意のフィールドに基づいた ISAKMP プロファイルへの証明書のマッピング：例

次の設定例では、証明書に「ou = green」が含まれているときは必ず、ISAKMP プロファイル「cert_pro」がピアに割り当てられる、ということを示します。

```
crypto pki certificate map cert_map 10
 subject-name co ou = green
!
!
crypto isakmp identity dn
crypto isakmp profile cert_pro
   ca trust-point 2315
   ca trust-point LaBcA
   initiate mode aggressive
   match certificate cert_map
```

ISAKMP プロファイルに関連付けられたピアに割り当てられるグループ名の例

次の例は、グループ「some_group」が、ISAKMP プロファイルが割り当てられたピアに関連付けられていることを示しています。

```
crypto isakmp profile id_profile
   ca trust-point 2315
   match identity host domain cisco.com
   client configuration group some_group
```

ISAKMP プロファイルへの証明書のマッピング検証例

次の例は、ISAKMP プロファイルに証明書がマッピングされたことを示します。この例には、応答側および発信側の設定、証明書マップの所有者名が設定されたことを確認する **show command** 出力、および証明書が証明書マップの照合を経て ISAKMP プロファイルに一致したことを示す **debug** コマンド出力が含まれています。

応答側の設定

```
crypto pki certificate map cert_map 10
! The above line is the certificate map definition.
 subject-name co ou = green
! The above line shows that the subject name must have “ou = green.”
!
crypto isakmp profile certpro
! The above line shows that this is the ISAKMP profile that will match if the certificate
 of the peer matches cert_map (shown on third line below).
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   initiate mode aggressive
```

発信側の設定

```
crypto ca trustpoint LaBcA
 enrollment url http://10.76.82.20:80/cgi-bin/openscep
 subject-name ou=green,c=IN
! The above line ensures that the subject name “ou = green” is set.
 revocation-check none
```

発信側の **show crypto ca certificates** コマンド出力

```
Router# show crypto ca certificates
Certificate
  Status: Available
  Certificate Serial Number: 21
  Certificate Usage: General Purpose
  Issuer:
    cn=blue-lab CA
    o=CISCO
    c=IN
  Subject:
    Name: Router1.cisco.com
    c=IN
    ou=green
! The above line is a double check that “ou = green” has been set as the subject name.
    hostname=Router1.cisco.com
  Validity Date:
    start date: 14:34:30 UTC Mar 31 2004
    end   date: 14:34:30 UTC Apr 1 2009
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: LaBcA
```

応答側の **debug crypto isakmp** コマンド出力

```
Router# debug crypto isakmp
6d23h: ISAKMP (0:268435460): received packet from 192.0.0.2 dport 500 sport 500 Global
(R) MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
```

```
6d23h: ISAKMP:(0:4:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:4:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:4:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435460): ID payload
        next-payload : 6
        type         : 2
        FQDN name    : Router1.cisco.com
        protocol     : 17
        port         : 500
        length       : 28
6d23h: ISAKMP:(0:4:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:4:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:4:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:4:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:4:HW:2): OU = green
6d23h: ISAKMP:(0:4:HW:2): certificate map matches certpro profile
! The above line shows that the certificate has gone through certificate map matching
and that it matches the “certpro” profile.
6d23h: ISAKMP:(0:4:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:4:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:4:HW:2): CERT validity confirmed.
```

ピアに割り当てられたグループ名の検証例

次の設定およびデバッグ出力は、グループがピアに割り当てられたことを示します。

発信側の設定

```
crypto isakmp profile certpro
   ca trust-point 2315
   ca trust-point LaBcA
   match certificate cert_map
   client configuration group new_group
! The statement on the above line will assign the group “new_group” to any peer that
matches the ISAKMP profile “certpro.”
   initiate mode aggressive
!
```

応答側の **debug crypto isakmp** プロファイル コマンド出力

次のデバッグ出力例は、ピアが「certpro」という ISAKMP プロファイルと照合され、「new_group」というグループが割り当てられたことを示します。

```
Router# debug crypto isakmp profile
6d23h: ISAKMP (0:268435461): received packet from 192.0.0.2 dport 500 sport 500 Global
(R) MM_KEY_EXCH
6d23h: ISAKMP: Main Mode packet contents (flags 1, len 892):
6d23h:           ID payload
6d23h:             FQDN <Router1.cisco.com> port 500 protocol 17
6d23h:           CERT payload
6d23h:           SIG payload
6d23h:           KEEPALIVE payload
6d23h:           NOTIFY payload
6d23h: ISAKMP:(0:5:HW:2):Input = IKE_MESG_FROM_PEER, IKE_MM_EXCH
6d23h: ISAKMP:(0:5:HW:2):Old State = IKE_R_MM4  New State = IKE_R_MM5
6d23h: ISAKMP:(0:5:HW:2): processing ID payload. message ID = 0
6d23h: ISAKMP (0:268435461): ID payload
        next-payload : 6
```

```
        type          : 2
        FQDN name     : Router1.cisco.com
        protocol      : 17
        port          : 500
        length        : 28
6d23h: ISAKMP:(0:5:HW:2):: peer matches *none* of the profiles
6d23h: ISAKMP:(0:5:HW:2): processing CERT payload. message ID = 0
6d23h: ISAKMP:(0:5:HW:2): processing a CT_X509_SIGNATURE cert
6d23h: ISAKMP:(0:5:HW:2): peer's pubkey isn't cached
6d23h: ISAKMP:(0:5:HW:2): OU = green
6d23h: ISAKMP:(0:5:HW:2): certificate map matches certpro profile
6d23h: ISAKMP:(0:5:HW:2): Trying to re-validate CERT using new profile
6d23h: ISAKMP:(0:5:HW:2): Creating CERT validation list: 2315, LaBcA,
6d23h: ISAKMP:(0:5:HW:2): CERT validity confirmed.
6d23h: ISAKMP:(0:5:HW:2):Profile has no keyring, aborting key search
6d23h: ISAKMP:(0:5:HW:2): Profile certpro assigned peer the group named new_group
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
ISAKMP プロファイルの設定	VRF 認識 IPSec
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア 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場合は、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
なし	--

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/cisco/web/support/index.html

証明書/ISAKMP プロファイルマッピングの機能情報

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 *1 :* 証明書*/ISAKMP* プロファイルマッピングの機能情報

機能名	リリース	機能情報
証明書/ISAKMP プロファイルマッピング	12.3(8)T 12.2(33)SRA 12.2(33)SXH	証明書/ISAKMPプロファイルマッピング機能を使用すると、証明書内の任意のフィールドの内容に基づいて、ピアにInternet Security Association and Key Management Protocol（ISAKMP）プロファイルを割り当てることができます。また、この機能では、ISAKMPプロファイルに割り当てられたピアにグループ名を割り当てることもできます。 この機能は、Cisco IOS Release12.3(8)T で導入されました。 この機能は、Cisco IOS Release 12.2(33)SRA に統合されました。 この機能は、Cisco IOS Release 12.2(33)SXH に統合されました。

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