CA における発信トラフィックの送信元インターフェイス選択機能

認証局を使用した発信トラフィックの送信元インターフェイスの選択機能を使用すると、指定されたトラストポイントが設定されている場合に、インターフェイスの IP アドレスを指定し、そのトラストポイントに関連付けられたすべての送信 TCP 接続の送信元アドレスとして使用できます。

CAにおける発信トラフィックの送信元インターフェイス選択機能の詳細

エンティティを識別する証明書

証明書を使用して、エンティティを識別できます。認証局（CA）とも呼ばれるトラステッドサーバにより、エンティティの ID を決定した後にエンティティに証明書が発行されます。Cisco IOS XE ソフトウェアを実行しているデバイスは、CA にネットワーク接続することでその証明書を取得します。Simple Certificate Enrollment Protocol（SCEP）を使用して、デバイスはその証明書要求を CA に送信し、許可された証明書を受信します。デバイスは、SCEP を使用した場合と同様に CA の証明書を取得します。リモートデバイスからの証明書を検証する場合、デバイスは再度 CA または Lightweight Directory Access Protocol（LDAP）サーバーあるいは HTTP サーバーに連絡して、リモートデバイスの証明書が失効しているかどうか判断できます（このプロセスは、証明書失効リスト（CRL）のチェックとも呼ばれています）。

設定によっては、デバイスは、ルーティング可能な有効なアドレスまたは IP アドレスを持たないインターフェイスを使用して発信 TCP 接続を確立する場合があります。ユーザは、異な

るインターフェイスのアドレスを発信接続の送信元 IP アドレスとして使用するよう指定する必要があります。発信ケーブルインターフェイス（RFインターフェイス）には通常、ルーティング可能な IP アドレスがないため、ケーブルモデムはこの要件の具体例です。ただし、ユーザ インターフェイス（通常はイーサネット）には有効な IP アドレスはありません。

トラストポイントに関連付けられた発信 TCP 接続の送信元インターフェイス

トラストポイントを指定するには、**crypto ca trustpoint** コマンドを使用します。インターフェイスのアドレスを、そのトラストポイントに関連付けられたすべての発信 TCP 接続の送信元アドレスとして指定する場合は、**source interface** コマンドも **crypto ca trustpoint** コマンドとともに使用します。

（注） インターフェイスアドレスが **source interface** コマンドを使用して指定されていない場合は、発信インターフェイスのアドレスが使用されます。

CAにおける発信トラフィックの送信元インターフェイス選択機能の設定方法

トラストポイントに関連付けられたすべての発信 TCP 接続のインターフェイスの設定

トラストポイントに関連付けられたすべての発信 TCP 接続の送信元アドレスとして使用するインターフェイスを設定するには、次の作業を行います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> 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**： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**crypto ca trustpoint** *name* 例： `Device(config)# crypto ca trustpoint ms-ca`	デバイスが使用する認証局（CA）を宣言し、ca-trustpoint 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	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
	例：
	`Device(ca-trustpoint)# enrollment url http://caserver.myexample.com`
	または
	`Device(ca-trustpoint)# enrollment url http://[2001:DB8:1:1::1]:80`
		CA の次の登録パラメータを指定します。
		• （任意）CA システムが登録局（RA）を提供する場合、**mode** キーワードとして RA モードを指定します。デフォルトでは、RA モードは無効です。
		• （任意）**retry period** キーワードおよび *minutes* 引数は、CA に別の証明書要求を送信するまでデバイスが待機する期間を分単位で指定します。有効値は 1 ～ 60 です。デフォルトは 1 です。
		• （任意）**retry count** キーワードおよび *number* 引数は、直前の要求に対する応答をデバイスが受信しない場合、デバイスが証明書要求を再送信する回数を指定します。有効な値は、1 ～ 100 です。デフォルトは 10 です。
		• *url* 引数は、デバイスが証明書要求を送信する CA の URL です。
		• （任意）**pem** キーワードは、証明書要求にプライバシー強化メール（PEM）の境界を追加します。

ステップ 5	**source interface** *interface-address* 例： `Device(ca-trustpoint)# source interface gigabitethernet 0/1/0`	そのトラストポイントに関連付けられたすべての発信 TCP 接続の送信元アドレスとして使用するインターフェイス。
ステップ 6	**exit** 例： `Device(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**interface** *type slot / port* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスタイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**description** *string* 例： `Device(config-if)# description inside interface`	インターフェイスの設定に説明を加えます。
ステップ 9	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 10	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードに戻ります。
ステップ 11	**interface** *type slot/port* 例： `Device(config-if)# interface gigabitethernet 1/0/2`	インターフェイスを設定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 12	**description** *string* 例： `Device(config-if)# description outside interface 10.1.1.205 255.255.255.0`	インターフェイスの設定に説明を加えます。
ステップ 13	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.2.2.205 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 14	**crypto map** *map-name* 例： `Device(config-if)# crypto map mymap`	以前に定義されたクリプトマップセットをインターフェイスに適用し、クリプトマップ設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 15	**end** 例： `Device(config-crypto-map)# end`	クリプトマップコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

CAにおける発信トラフィックの送信元インターフェイス選択機能の設定例

例：CAにおける発信元トラフィックの送信元インターフェイス選択機能

次の例では、デバイスはブランチオフィスにあります。デバイスは IPSec を使用して本社と通信します。GigabitEthernet 1/0/1 は、ISP に接続する「外部」インターフェイスです。GigabitEthernet 0/1/0 は、支社の LAN に接続されたインターフェイスです。本社に配置された CA サーバーにアクセスするには、デバイスはインターフェイス Ethernet 1（アドレス 10.2.2.205）から IPSec トンネルを使用して IP データグラムを送信する必要があります。アドレス 10.2.2.205 は ISP により割り当てられています。アドレス 10.2.2.205 は支社または本社の一部ではありません。

CA は、ファイアウォールがあるため、社外のアドレスにはアクセスできません。CA は 10.2.2.205 から着信するメッセージを認識していますが、応答できません（つまり、CA は到達可能なアドレス 10.1.1.1 にあるブランチオフィスに、デバイスが配置されていることを認識していません）。

source interface コマンドを追加すると、CA に送信する IP データグラムの送信元アドレスとして、アドレス 10.1.1.1 を使用するようにデバイスに命令が出されます。CA は 10.1.1.1 に応答できます。

このシナリオは、上記の **source interface** コマンドとインターフェイスアドレスを使用して設定されています。

```
Device> enable
Device# configure terminal
Device(config)# crypto ca trustpoint ms-ca
Device(ca-trustpoint)# enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
Device(ca-trustpoint)# source interface gigabitethernet 0/1/0
Device(ca-trustpoint)# exit
Device(onfig)# interface gigabitethernet 0/1/0
Device(config-if)# description inside interface
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# description outside interface
Device(config-if)# ip address 10.2.2.205 255.255.255.0
```

```
Device(config-if)# crypto map main-office
Device(config-if)# end
```

CAにおける発信トラフィックの送信元インターフェイス選択の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	CA における発信トラフィックの送信元インターフェイス選択機能	認証局（CA）における発信トラフィックの送信元インターフェイス選択機能により、指定のトラストポイントが設定されたときに、インターフェイスのアドレスをそのトラストポイントと関連付けられたすべての TCP 接続の送信元アドレスとして使用するよう設定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。